SentinelOne

API DOCUMENTATION

SentinelOne Api Documentation Version 2.1

Get Accounts 18
Create Account 25
Get Account by ID 42
Update Account 47
Revert Policy 67
Reactivate Account 69
Expire an Account 71
Get Uninstall Password Metadata 75
Get Uninstall Password 77
Generate/Regenerate Uninstall Password 78
Revoke Uninstall Password 81
Export Accounts 83
Get Activities 84
Get Activity Types 88
Last activity as Syslog message 89
Export Activities 92
Broadcast Message 93

Connect to Network 115
Fetch Logs 136
Initiate Scan 158
Abort Scan 179
Disconnect from Network 200
Decommission 221
Uninstall 242
Restart 263
Shutdown 284
Approve Uninstall 305
Reject uninstall 326
Update Software 347
Reset Local Config 370
Set Persistent Configuration Overrides 391
Set External ID 412
Fetch Files 433
Move between Sites 435
Fetch Firewall Rules 456
Move to Console 478
Get Applications 499
Start Remote Shell 520
Can run Remote Shell 543
Terminate Remote Shell 564
Fetch Firewall Logs 585
Randomize UUID 606
Mark as up-to-date 627
Enable Ranger 648
Disable Ranger 669
Edit local upgrade site authorization 690
Disable Agent 711
Enable Agent 732
Start Remote Profiling 753

Stop Remote Profiling 774
Approve Stateless Upgrades 795
Manage endpoint tags: add, remove, override 816
Clear Remote Shell 837
Get Agents 858
Count Agents 878
Get Passphrase 888
Export Agent Logs 899
Applications 899
Processes 901
Get local upgrade agent authorization 902
Export Agents 903
Get the endpoint tags that match the filters. 912
Export Agents - Light 915
List Access Tokens 924
Create Access Token 925
Delete Access Token 927
Get alerts 927
Update Threat Incident 940
Update Alert Analyst Verdict 946
Inventory Endpoints Data Export 952
Aggregated Application Risk Data Export 953
Application Risk Data Export 954
Risk Endpoint Data Export 956
Application CVE Data Export 958
Inventory Data Export 959
Risks Data Export 960
Get Endpoint Apps 963
Get App Inventory Endpoints 965
Get Aggregated Applications With Risk 969
Get Applications With Risk 973
Get Endpoints For Vulnerable App 977

Get Application CVEs 982
Get Application Inventory 986
Get CVE data 989
Initiate scan 995
Update Application Management Settings 997
Get Application Management Settings 1000
Get Applications 1002
Get CVEs 1006
Export Applications 1009
Get Available Packages 1010
Has Policy 1012
Get Parent Policies 1014
Get Policies 1015
Deactivate Policies 1016
Policies OS Count 1017
Create Policy 1018
Update Policy 1021
Policy Action 1024
Reorder Policies 1026
Set Scope Inheriting 1028
Validate Bucket 1030
Get AWS assume role external ID. 1032
Validate Query 1033
Get cloud funnel rule 1035
Delete cloud funnel rule 1038
Post onboarding cloud funnel 1040
Create Estimator ID 1045
Get estimate size of events 1047
get cloud provider account active health events by cloud provider account id 1049
Export cloud rogue resources to csv 1051
Get cloud rogue resources 1052
Get Config Overrides 1056

Create Config Override 1060
Delete Config Overrides 1063
Delete Config Override 1066
Update Config Override 1067
Create Unified Exclusion 1070
Validate Exclusion Item 1073
Get Rules 1075
Create Rule 1082
Delete Rules 1089
Update Rule 1092
Activate Rules 1099
Disable Rules 1102
Create Query and Get QueryId 1105
Cancel Running Query 1109
Get Query Status 1111
Get Events 1113
Get Process State 1119
Get Events By Type 1119
Create a Power Query and Get QueryId 1127
Ping a Power Query if results haven't been retrieved 1129
Download source process file 1131
Get Device Rules 1132
Create Device Control Rule 1138
Delete Rules 1145
Update Device Rule 1149
Copy Rules 1156
Move rules 1161
Reorder Rules 1166
Get Configuration 1168
Update Configuration 1170
Export Rules 1174
Get Device Control Events 1175

Enable/Disable Rules 1179
Import Exclusions 1184
Get Exclusion Import Validation Report 1187
Import Blocklist Items 1187
Get Blocklist Import Validation Report 1190
Get Exclusions 1190
Create Exclusion 1196
Update Exclusions 1200
Delete Exclusions 1203
Get Blocklist 1205
Create Blocklist Item 1210
Update Blocklist Item 1213
Delete Blocklist Item 1216
Validate Exclusion Item 1218
Validate Blocklist Item 1220
Export Exclusions 1222
Export Blocklist 1224
Get Exclusions 1226
Delete Exclusions 1230
Get Filters 1232
Save Filter 1247
Update Filter 1275
Delete Filter 1302
Get Deep Visibility Filters 1303
Save Deep Visibility Filter 1304
Delete Deep Visibility Filter 1306
Update Deep Visibility Filter 1307
Upload CSV file 1311
Get Firewall Rules 1313
Create Firewall Rule 1319
Delete Rules 1326
Copy Rules 1330

Move Rules 1335
Set Location 1340
Reorder Rules 1345
Get Configuration 1347
Update Configuration 1350
Export Rules 1354
Import Rules 1355
Enable/Disable Rules 1358
Get Protocols 1363
Add Rule Tags 1365
Remove Rule Tags 1370
Get Tag Firewall Rules 1375
Update Firewall Rule 1381
Application Forensics 1388
Application Forensics - Detailed 1391
Application Connections 1394
Export Application 1395
Get Gateways 1395
Update Gateways 1403
Update Gateway 1411
Get Groups 1417
Create Group 1421
Regenerate Group Token 1438
Delete Group 1439
Update Group 1440
Get Group by ID 1457
Revert Policy 1459
Move Agents 1461
Update Ranks 1482
Get Site registration token by ID 1484
Hash Reputation Rank 1485
Hash classification 1487

Hash Reputation verdict 1488
Update sites add-ons 1489
Get Agent Merged Updates 1493
Create Location 1495
Get Locations 1503
Delete Locations 1509
Update Location 1511
Get Applications Catalog 1518
Get Installed Applications 1521
Delete Application 1526
Install Applications 1529
Update Application Configuration 1531
Get Configuration Fields 1533
Get Configuration fields for Catalog Application 1534
Enable or Disable application 1537
Activations - Resend activation link invitations 1539
Activations - Cancel user activation invitations 1540
Activations - Validate bulk user activation upload 1541
Activations - Bulk user activation import 1543
Provision - Check if tenant can be provisioned 1545
Provision - Persist MSSP partner key 1547
Provision - Update MSSP partner key 1548
Provision - Get MSSP partner key 1550
Provision - Provision tenant with admin user 1551
Provision - Get tenant with users 1553
Management - Create interim connector connection 1555
Management - Checks if connection can be created on current scope. 1558
Management - Create connector connection 1559
Activations - Create User Activation 1562
Activations - Get list of user activations 1564
Management - Test connector connection. Deprecated, use create-interim-connection + device-groups instead. 1567
Management - Get list of connections for specific scope 1570

Connectors - Get list of Connectors and their abilities 1573
Management - Get app configuration 1574
Activations - Generates a global link for anonymous device registration 1575
Activations - Return anonymous activation in the scope 1577
Incidents - Update analyst verdict 1580
Incidents - Update incident status 1582
Policy - Get global mobile policy 1584
Policy - Update global mobile policy 1586
Policy - Delete global mobile policy 1590
Incidents - Get list of incidents 1590
Devices - Get list of devices for specific scope 1595
Policy - Create mobile policy 1600
Management - Get managed groups for connection 1604
Management - Get all UEM device groups for given connection 1605
Management - Sync devices under connection 1607
Management - Patch connection group mappings 1608
Deletes MSSP partner key by client ID 1610
Management - Update connector connection 1611
Management - Delete connection 1614
Incidents - Mitigate incident 1615
Incidents - Update incident note 1617
Incidents - Delete incident note 1619
Incidents - Create incident note 1620
Policy - Get the policy for the Account given by ID 1622
Policy - Update the policy for the Account given by ID 1624
Policy - Delete the policy for the Account given by ID 1628
Policy - Get the policy for the Site given by ID 1628
Policy - Update the policy for the Group given by ID 1631
Policy - Delete the policy for the Site given by ID 1635
Policy - Update the policy for the Site given by ID 1635
Devices - Get device details by device id 1640
Get Firewall Rules 1644

Create Firewall Rule 1650
Delete Rules 1657
Copy Rules 1661
Move Rules 1666
Set Location 1671
Reorder Rules 1676
Get Configuration 1678
Update Configuration 1681
Export Rules 1685
Import Rules 1686
Enable/Disable Rules 1689
Get Protocols 1694
Add Rule Tags 1696
Remove Rule Tags 1701
Group Policy 1706
Update Group Policy 1721
Site Policy 1750
Update Site Policy 1765
Account Policy 1794
Update Account Policy 1809
Global Policy 1838
Update Global Policy 1853
Get Ranger Table 1882
Export Ranger Data 1890
JSON Raw Data 1892
Export JSON Raw Data 1894
Get Ranger Settings 1894
Update Ranger Settings 1898
Change Device Review in Bulk 1905
Change Device Review 1911
Change Device Tags 1916
Create Cred Group 1922

Get Cred groups 1925
Delete Cred Group 1928
Add cred details 1929
Get Cred group details 1931
Delete Cred Group Detail 1934
Update Cred Group Details 1935
Get Self Enablement 1938
Change Ranger or Rogues Features 1939
Change the Self-Enablement for Accounts 1942
Features Configuration for New Sites 1943
Change Feature Defaults for New Sites 1943
Get All Roles 1946
Get Specific Role Definition 1950
Update role 1953
Delete role 1956
Create new role 1958
Get template for new role 1961
Create new Destination profile. 1963
Get available Destination profiles 1965
Delete multiple Destination profiles by ID 1967
Delete Destination profile by ID 1969
Update existing Destination profile 1969
Get Destination profile by ID 1972
Set profile as default profile of the scope 1974
Get results sent to data exporter 1975
Start collection of Forensics artifacts according to specified profile 1977
Return result of collection task 1998
Returns collection file download pre-signed url 2001
Check if collection file exists for given storyline 2002
Get list of supported artifact types 2003
Get Collection profile by ID 2005
Update Collection profile by ID 2008

Delete Collection profiles 2012
Create new Collection profile 2016
Get list of available Collection profiles 2020
Run Remote Script 2024
Get Remote Scripts Tasks Status 2047
Get Script Results 2051
Get script content 2053
Get Scripts 2054
Upload New Script 2058
Delete Scripts 2064
Update a Script 2069
Get paginated pending executions 2074
Approve/decline pending execution 2080
Gets a guardrails configuration for a given scope 2082
Updates or inserts (if record does not exist) a guardrails configuration 2083
Deletes a specific guardrails configuration 2085
Check whether guardrail applies to an execution 2087
Get Rogues Table 2089
Export Rogues Data 2094
Get Rogues Settings 2096
Update Rogues Settings 2099
Get Service Users 2103
Create Service User 2106
Export Service Users 2110
Update Service User 2110
Delete Service User 2114
Bulk Delete Service Users 2115
Get SSO Settings 2117
Set SSO Settings 2120
Get SSO Service Provider Certificate 2126
Download SSO Service Provider Certificate 2128
Test SSO Settings 2128

Get Notification Settings 2133
Set Notification Settings 2136
Clear Pending Emails 2141
Get SMTP Settings 2143
Set SMTP Settings 2145
Test SMTP Settings 2149
Get Syslog Settings 2152
Set Syslog Settings 2154
Test Syslog Settings 2158
Get SMS Settings 2161
Set SMS Settings 2162
Get Notification Recipients 2164
Set Notification Recipients 2166
Delete Notification Recipient 2168
Get AD Settings 2169
Set AD Settings 2171
Test AD Settings 2174
Get AD FQDNs 2176
Set AD FQDNs 2177
Get Microsoft Settings 2179
Set Microsoft Settings 2181
Test Microsoft Settings 2184
Get Sites 2186
Create Site 2192
Export Sites 2212
Get Site by ID 2213
Update Site 2217
Delete Site 2237
Get Site registration token by ID 2238
Revert Policy 2239
Create duplicate site 2241
Create Site and User 2260

Regenerate Site Key 2280
Reactivate Site 2281
Expire Site 2283
Update Sites 2287
Get local upgrade site authorization 2291
Edit local upgrade site authorization 2292
Get a CSV file of local upgrade site authorization data 2294
System Info 2295
System Status 2296
Database Status 2297
Cache Status 2298
Get System Config 2299
Set System Config 2305
System Environment 2313
Create a new endpoint tag 2314
Delete tags 2317
Edit an existing tag 2319
Get Tags 2322
Create Tags 2325
Delete Tags 2328
Delete Tag by ID 2331
Edit Tag 2332
Get Task Configuration 2335
Create Task 2338
Has Child Scopes 2341
Get Child Scope Task Configuration 2343
Get Threat Intelligence user config 2345
Create Threat Intelligence user config 2347
Delete Threat Intelligence user config 2350
Get IOCs 2352
Create IOCs 2359
Delete IOCs 2368

Get Threat Notes 2373
Add Note to Multiple 2375
Update Threat Note 2389
Delete Threat Note 2391
Get Threats 2392
Mitigate Threats 2409
Add to Blocklist 2424
Fetch Threat File 2439
Disable Engines 2453
Exclusion Options 2455
Get Events 2456
Add to Exclusions 2462
Export Threats 2478
Add to Blocklist (Deep Visibility) 2483
Mark as Threat (Deep Visibility) 2486
Export Mitigation Report 2488
Updated Threat Incident 2488
Update Threat Analyst Verdict 2503
Update Threat External Ticket ID 2517
Download from cloud 2531
Disconnect Container 2532
Reconnect Container 2546
Get Threat Timeline 2560
Export Threat Timeline 2563
Export Events 2563
Update Exclusions 2564
Latest Packages by OS 2566
Get Latest Packages 2573
Delete Packages 2577
Update package 2579
Upload Agent Package 2583
Upload System Package 2587

Deploy System Package 2589
Download Agent Package 2590
Download Package 2590
User by token 2590
List users 2595
Create User 2602
Export Users 2608
Get User 2610
Delete User 2615
Update User 2616
Bulk Delete Users 2622
Generate iFrame Token 2626
Enable 2FA 2628
Disable 2FA 2630
Generate API Token 2632
Revoke API Token 2634
API Token by User ID 2636
API Token Details 2637
Enable 2FA App 2639
Request 2FA App 2641
Change Password 2643
Auth App 2645
Sign EULA 2647
Check Global User 2648
Check Remote Shell Permissions 2649
Check Viewer 2650
Email Verification 2651
Validate Verification Token 2653
Send Verification Email 2654
Reset 2FA 2659
Delete 2FA 2661
Enroll 2FA 2663

Redirect to SSO 2665
Redirect to SSO for re-authentication 2665
Auth by SSO 2666
Login 2666
Logout 2669
Login by API Token 2669
Login by Token 2672
Continue with login due to upcoming password expiration or SSO 2FA setup 2672
Set a New Password 2675
Prompt reset password 2677
Reset password on next login 2682

Accounts

Get Accounts

GET /web/api/v2.1/accounts

Get the Accounts, and their data, that match the filter. This command gives the Account IDs, which other commands require.
Accounts are created by a Global User or by SentinelOne. Each Account contains Sites, which can inherit assets and settings. Each Account has one or more SKUs, that you assign to the Sites. To have both Core and Complete Sites in an Account, the Account must have both SKUs.

Parameters

accountids	optional	List of Account IDs to search for. Example: "225494730938493804,225494730938493915".
accounttype	optional	Account type. Example: "Trial".
activelicenses	optional	Active licenses
billingmode	optional	Billing mode. Example: "subscription".
countonly	optional	If true, only total number of items will be returned, without any of the actual objects.
createdat	optional	Timestamp of Account creation. Example: "2018-02-27T04:49:26.257525Z".
cursor	optional	Cursor position returned by the last request. Use to iterate over more than 1000 items. Example: "YWdlbnRfaWQ6NTgwMjkzODE=".
expiration	optional	Expiration. Example: "2018-02-27T04:49:26.257525Z".
features	optional	Filter the list of Accounts for those that support this feature. Example: "firewall-control".
ids	optional	A list of Account IDs. Example: "225494730938493804,225494730938493915".
isdefault	optional	Is default
limit	optional	Limit number of returned items (1-1000). Example: "10".
name	optional	Name. Example: "My Account".
query	optional	Full text search for fields: name. (Note: on single-Account Consoles,

		the Account name will not be matched)
skip	optional	Skip first number of items (0-1000). To iterate over more than 1000 items, use "cursor". Example: "150".
skipcount	optional	If true, total number of items will not be calculated, which speeds up execution time.
sortby	optional	The column to sort the results by. Example: "id".
sortorder	optional	Sort direction. Example: "asc".
states	optional	Filter by state, such as active or expired.
totallicenses	optional	Total licenses
updatedat	optional	Timestamp of last update. Example: "2018-02-27T04:49:26.257525Z".
usagetype	optional	Usage type. Example: "customer".

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - Insufficient permissions

Response Schema

Name	Description	Required	Value
pagination	Pagination information	true	

Name	Description	Required	Value
totalItems	Total number of items found matching your query	true	integer
nextCursor	Pass this value as "cursor" on your next request, to	false	string

				get the next page of results (Will be "null" when last page reached)		
data	Response data	false	Name	Description	Required	Value
			accountType	Account type	false	string
			activeAgents	Total Agents in the Account	false	integer
			agentsInCompleteSku	[DEPRECATED] Number of Agents connected to a Complete site	false	integer
			agentsInControlSku	[DEPRECATED] Number of Agents connected to a Control site	false	integer
			agentsInCoreSku	[DEPRECATED] Number of Agents connected to a Core site	false	integer
			billingMode	Billing mode	false	enum
			completeSites	[DEPRECATED] Number of Sites in suite Complete	false	integer
			controlSites	[DEPRECATED] Number of Sites in suite Control	false	integer
			coreSites	[DEPRECATED] Number of Sites in suite	false	integer

	Core		
createdAt	Timestamp of Account creation	false	string
creator	The user that created the group	false	string
creatorId	The ID of the user that created the group	false	string
expiration	Expiration	false	string
externalId	ID of CRM external system	false	string
id	Account ID	false	string
isDefault	Is default	false	boolean
licenses	The account licenses.	false	

Name	Description	Required	Value
bundles	The licenses Bundles	false	

Name	Description	Required	Value
displayName	The Bundle display name	false	string
majorVersion	The Bundle major version	false	integer
minorVersion	The Bundle minor version	false	integer
name	The Bundle internal api name	false	string
surfaces	The Surfaces in the Bundle	false	

Name	D
count	Th co in ur co
name	Th na

									totalSurfaces	The total number of Surfaces in this Bundle. -1 indicates unlimited count.	false	integer
						modules	The licenses Add-ons	false				
									Name	Description	Required	Value
									displayName	The Add-on display name	false	string
									majorVersion	The Add-on major version	false	integer
									name	The Add-on internal api name	false	string
						settings	The licenses Settings	false				
									Name	Description	Required	Value
									displayName	[DEPRECATED] The Setting display name	false	string
									groupName	The Setting group name	false	
									setting	The Setting display name	false	
									settingGroup	[DEPRECATED] The Setting group name	false	string
									settingGroupDisplayName	The Setting group display name	false	string
			name	Name	false	string						
			numberOfSites	Total number of Sites in this Account	false	integer						
			salesforceId		false	string						
			skus	[DEPRECATE	false							

				D] The list of SKUs for the Account.		
			state	Account state	false	enum
			totalComplete	[DEPRECATED] Total Number of Complete licenses	false	integer
			totalControl	[DEPRECATED] Total Number of Control licenses	false	integer
			totalCore	[DEPRECATED] Total Number of Core licenses	false	integer
			totalLicenses	The total number of licenses on all Surfaces for all Bundles.	false	integer
			unlimitedCom	[DEPRECATE	false	boolean

Name	Description	Required	Value
agentsInSku	Total agents commissioned in this SKU.	false	integer
totalLicenses	Number of licenses for this specific SKU. Applicable only if unlimited is False	false	integer
type	The suite of product features active for this account	false	enum
unlimited	True if this is an unlimited SKU.	false	boolean

			plete	D] True if Complete licenses count is unlimited		
			unlimitedControl	[DEPRECATED] True if Control licenses count is unlimited	false	boolean
			unlimitedCore	[DEPRECATED] True if Core licenses count is unlimited	false	boolean
			unlimitedExpiration	The Account does not expire	false	boolean
			updatedAt	Timestamp of last update	false	string
			usageType	Usage type	false	enum
errors	Errors	false	array			

Create Account

POST /web/api/v2.1/accounts

Create a new Account. This command requires Global permissions and an MSSP deployment. Consult with your SE before you run this command. An Account is a logical segment with permissions to configure features for specific Sites. Multiple Accounts can be useful for deployments with multiple Sites for third-parties (such as MSSP). Each Account has one or more SKUs, that you assign to Sites. If an Account has the Complete SKU, and you create a new Site in the Account, it will automatically have the Complete SKU. Best practice: Run "name-available" first, to make sure the name is unique in your deployment.

BEST PRACTICE

Run "name-available" first, to make sure the name is unique in your deployment.

Response Messages

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Body Schema

Name	Description	Required	Value
data	Data	true	

Name	Description	Required	Value
name	Name	true	string
accountType	Account type: Trial or Paid	false	enum
billingMode	Billing mode	false	enum
expiration	Expiration	false	string
externalId	ID of CRM external system	false	string
inherits	True if the policy is inherited from Global, False if the	false	boolean

				Account has its own edited policy	
			licenses	The license configuration for the Account	false

Name	Description	Required	Value
bundles	The list of Bundles selected	false	

Name	Description	Required	Value
name		true	string
majorVersion		false	integer
surfaces		false	

Name	D
name	
count	Th of pe -1 un co

Name	Description	Required	Value
modules	The list of Add-ons selected	false	

Name	Description	Required	Value
name		true	string

Name	Description	Required	Value
settings	The list of Settings selected for the Bundle and Add-ons. If a Bundle or Add-on requires a Setting that is not defined, the default Setting is used.	false	

Name	Description	Required	Value
groupName		true	string
setting		true	string

policy	Policy is mandatory if it was edited (inherits = false), otherwise ignored.	false	

Name	Description	Required	Value
agentLoggingOn	True if logging is enabled in the agent	false	boolean
agentNotification	[DEPRECATED] Show end	false	boolean

							point notification on suspicious.Replaced by 'show_suspicious' in the agent UI section	
						agentUi	Agent ui	false

Name	Description	Required	Value
agentUiOn	Agent ui on	false	boolean
contactCompany	Contact company	false	string
contactDirectMessage	Contact direct message	false	string
contactEmail	Contact email	false	string
contactFreeText	Contact free text	false	string
contactOther	Contact other	false	string
contactPhoneNumber	Contact phone number	false	string
contactSupportWebsite	Contact support website	false	string
devicePopUpNotifications	Device pop up notifications	false	boolean
maxEventAgeDays	Max event age days	false	integer
showAgentWarnings	Show agent warnings	false	boolean
showDeviceTab	Show device tab	false	boolean
showQuarantineTab	Show quarantine tab	false	boolean

									showSupport: Show support; false; boolean showSuspicious: Show suspicious; false; boolean threatPopUpNotifications: Threat pop up notifications; false; boolean
						agentUiOn	[DEPRECATED] Show/hide Agent UI. Moved inside the agent UI section	false	boolean
						allowRemoteShell	True if Remote Shell is enabled for the scope	false	boolean
						antiTamperingOn	Anti tampering on/off	false	boolean
						autoDecommissionDays	Automatic decommission period in days	false	integer
						autoDecommissionOn	Auto decommission on	false	boolean
						autoFileUpload	Automatic file upload configuration	false	Name; Description; Required; Value enabled; Automatic file upload on/off; false; boolean includeBenignFiles; Upload benign files; false; boolean maxDailyFileUpload; Maximum size (MB) to upload daily; false; integer maxDailyFileUploadLimit; Limit for the maximum size (MB) to

										upload daily			
									maxFileSize	Maximum file size (MB) to upload	false	integer	
									maxFileSizeLimit	Limit for the maximum file size (MB) to upload	false	integer	
									maxLocalDiskUsage	Maximum local disk usage (MB) for uploaded files	false	integer	
									maxLocalDiskUsageLimit	Limit for the maximum local disk usage (MB) for uploaded files	false	integer	
							autoImmuneOn	Automatic immune on/off - this value must be true since all policies are immune by default	false	boolean			
							autoMitigationAction	Default action for auto mitigation	false	string			
							cloudValidationOn	Cloud validation on	false				
							createdAt	Timestamp of policy creation	false	string			
							driverBlocking	Suspicious driver blocking engine on/off	false	boolean			

						dvAttributesPerEventType	The DV attributes	false

Name	Description	Required	Value
autoInstallBrowserExtensions	Auto install browser extensions	false	Name: autoInstallBrowserExtensions; Description: Au br ex
behavioralIndicators	Behavioral indicators event	false	Name: dvEventTypeBehavioralIndicators; Description: Be in ev
commandScripts	Command scripts event	false	Name: dvEventTypeCommandScripts; Description: Co sc
crossProcess	Cross process event	false	Name: dvEventTypeCrossProcessDuplicateProcess; Description: Du Pr Ev Name: dvEventTypeCrossProcessDuplicateThread; Description: Du Th Ty Name: dvEventTypeCrossProcessOpenProcess; Description: Op Ev Name: dvEventTypeCrossProcessRemoteThread; Description: Re Th Ty
dataMasking	Data masking	false	Name: dataMasking; Description: Da
dllModuleLoad	DLL module load event	false	Name: dvEventTypeDllModuleLoad; Description: Dl loa

| | | |

													dvEventType NamedPipeCreation
									namedPipeExtended	Named Pipe Extended	false		
									process	Process event	false		
									registry	Registry event	false		

Name	D
namedPipeExtended	Na Co Ex Ev

Name	D
dvEventTypeProcessCreation	Pr Cr Ev
dvEventTypeProcessExit	Pr Ev
dvEventTypeProcessModification	Pr Te Ev

Name	D
dvEventTypeRegistryKeyCreated	Re Cr Ev
dvEventTypeRegistryKeyDelete	Re De Ty
dvEventTypeRegistryKeyExport	Re Ex Ty
dvEventTypeRegistryKeyImport	Re Im Ty
dvEventType RegistryKey Rename	Re Re Ev
dvEventTypeRegistryKeySecurityChange	Re Se Ch

| | | |

									forensics			
									linuxProfileName	The profile name for the linux forensics	false	string
									macosEnabled	True if macos forensics is enabled	false	boolean
									macosProfileId	The profile id for the macos forensics	false	string
									macosProfileName	The profile name for the macos forensics	false	string
									windowsEnabled	True if windows forensics is enabled	false	boolean
									windowsProfileId	The profile id for the windows forensics	false	string
									windowsProfileName	The profile name for the windows forensics	false	string
							identityEndpointReporting	Endpoint reporting level	false	enum
							identityOn	Identity module on/off	false	boolean
							identityReportInterval	Identity telemetry report interval in minutes	false	integer
							identityThrottlingInterval	Identity duplicate	false	integer

							command consolidation interval in minutes		
						identityUpdateInterval	Identity update interval in minutes	false	integer
						inheritedFrom	Indicates the parent scope from which this policy is inherited, or 'null' if it is not inherited (modified specifically for the current scope).	false	enum
						ioc	True if ioc is enabled	false	boolean
						iocAttributes	The Ioc attributes	false	

Name	Description	Required	Value
autoInstallBrowserExtensions	Update auto install browser extensions	false	boolean
behavioralIndicators	Update behavioral indicators	false	boolean
commandScripts	Update command scripts	false	boolean
crossProcess	Update cross process	false	boolean
dataMasking	Update data masking	false	boolean
dllModuleLoad	Update DLL module load	false	boolean
dns	Network	false	boolean

										event - DNS			
									driver	Driver	false	boolean	
									fds	Full disk scan	false	boolean	
									file	File event	false	boolean	
									ip	Network event - IP	false	boolean	
									login	User login/ logout event	false	boolean	
									namedPipe	Named Pipe	false	boolean	
									namedPipeExtended	Named Pipe Extended	false	boolean	
									process	Process creation event	false	boolean	
									registry	Registry event	false	boolean	
									scheduledTask	Scheduled task event	false	boolean	
									smartFileMonitoring	Smart file monitoring	false	boolean	
									url	Ioc URI	false	boolean	
									windowsEventLogs	Windows Event Log	false	boolean	
									windowsEventLogsExtended	Windows Event Log Extended	false	boolean	
							iocSupported	Ioc supported for the scope	false	boolean			
							isDefault	True if this is the tenant policy	false	boolean			
							isDvPolicyPerEventType	FE indication as to how to display DV policy	false	boolean			
							mitigationMo	Mitigation	false	enum			

						de	modes		
						mitigationModeSuspicious	Mitigation mode	false	enum
						monitorOnExecute	Monitor on execute on/off	false	boolean
						monitorOnWrite	Monitor on write	false	boolean
						networkQuarantineOn	Network quarantine on	false	boolean
						remoteOpsForensics	Remote ops forensics configuration	false	
						remoteScriptOrchestration	Remote script orchestration upload limits configuration	false	

Name	Description	Required	Value
cpuLimit	CPU resources limit for collection process	false	integer
enabled	Enabled	false	boolean
maximumDailyUpload	Maximum size to upload daily	false	integer
maximumDailyUploadLimit	Limit for the maximum size to upload daily	false	integer
maximumFileSizeUpload	Maximum size for single file	false	integer
maximumFileSizeUploadLimit	Limit for the maximum file size to upload	false	integer
parsedArtifactsDestination	Default destination of parsed artifacts	false	enum

Name	Description	Required	Value
alwaysUploadStreamToCloud	Always upload streams to	false	boolean

										cloud		
									maxDailyFileDownload	Maximum size (MB) to download daily	false	integer
									maxDailyFileDownloadLimit	Limit for the maximum size (MB) to download daily	false	integer
									maxDailyFileUpload	Maximum size (MB) to upload daily	false	integer
									maxDailyFileUploadLimit	Limit for the maximum size (MB) to upload daily	false	integer
									maxFileSize	Maximum size in bytes for single file	false	integer
									maxFileSizeLimit	Limit for the maximum file size (MB) to upload	false	integer
									maxLocalPackageDiskUsage	Maximum local disk usage (MB) for packages	false	integer
									maxLocalPackageDiskUsageLimit	Limit for the maximum local disk usage (MB) for packages	false	integer
							removeMacros	Determines if macros should be removed from macro threats	false	boolean
							researchOn	Share data	false	boolean

							with SentinelOne		
						scanNewAgents	If True initiate full disk scan upon first registration	false	boolean
						signedDriverBlockingOn	Suspicious signed driver blocking on/off	false	boolean
						snapshotsOn	True if snapshots are enabled	false	boolean
						unsignedDriverBlockingOn	Suspicious unsigned driver blocking on/off	false	boolean
						updatedAt	Time of the last update to the policy	false	string
						userFullName	The user that created the policy	false	string
						userId	The user id	false	string
			skus	[DEPRECATED] The list of allowed SKUs for the Account	false	totalLicenses	Number of licenses for this specific SKU. Applicable only if unlimited is False	false	integer
						type	The suite of product features	false	enum

							active for this Account		
						unlimited	True if this is an unlimited SKU. Total licenses will be ignored if unlimited is True	false	boolean
			unlimitedExpiration	If expiration is not unlimited, enter the expiration date	false	boolean			
			usageType	Usage type	false	enum			

Get Account by ID

GET /web/api/v2.1/accounts/{account_id}

Get Account data from a given Account ID. To get an Account ID, run "accounts".

Response Messages

200 - Success

401 - Unauthorized access - please sign in and retry.

404 - Account not found

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
accountType	Account type	false	string
activeAgents	Total Agents in the Account	false	integer
agentsInCompleteSku	[DEPRECATED] Number of Agents connected to a Complete site	false	integer
agentsInControlSku	[DEPRECATED] Number of Agents connected to a Control site	false	integer
agentsInCoreSku	[DEPRECATED] Number of Agents connected to a Core site	false	integer
billingMode	Billing mode	false	enum

			completeSites	[DEPRECATED] Number of Sites in suite Complete	false	integer
			controlSites	[DEPRECATED] Number of Sites in suite Control	false	integer
			coreSites	[DEPRECATED] Number of Sites in suite Core	false	integer
			createdAt	Timestamp of Account creation	false	string
			creator	The user that created the group	false	string
			creatorId	The ID of the user that created the group	false	string
			expiration	Expiration	false	string
			externalId	ID of CRM external system	false	string
			id	Account ID	false	string
			isDefault	Is default	false	boolean
			licenses	The account licenses.	false	

Name	Description	Required	Value
bundles	The licenses Bundles	false	

Name	Description	Required	Value
displayName	The Bundle display name	false	string
majorVersion	The Bundle major version	false	integer
minorVersion	The Bundle minor version	false	integer
name	The Bundle internal api	false	string

										name		
									surfaces	The Surfaces in the Bundle	false	
									totalSurfaces	The total number of Surfaces in this Bundle. -1 indicates unlimited count.	false	integer
						modules	The licenses Add-ons	false				
						settings	The licenses Settings	false				

Name	Description	Required	Value
displayName	The Add-on display name	false	string
majorVersion	The Add-on major version	false	integer
name	The Add-on internal api name	false	string

Name	Description	Required	Value
displayName	[DEPRECATED] The Setting display name	false	string
groupName	The Setting group name	false	
setting	The Setting display name	false	
settingGroup	[DEPRECATED] The Setting group name	false	string

Name	D
count	Th co in un co
name	Th na

										settingGroupDisplayName	The Setting group display name	false	string	
			name	Name	false	string								
			numberOfSites	Total number of Sites in this Account	false	integer								
			salesforceId		false	string								
			skus	[DEPRECATED] The list of SKUs for the Account.	false	Name	Description	Required	Value					
						agentsInSku	Total agents commissioned in this SKU.	false	integer					
						totalLicenses	Number of licenses for this specific SKU. Applicable only if unlimited is False	false	integer					
						type	The suite of product features active for this account	false	enum					
						unlimited	True if this is an unlimited SKU.	false	boolean					
			state	Account state	false	enum								
			totalComplete	[DEPRECATED] Total Number of Complete licenses	false	integer								
			totalControl	[DEPRECATED] Total Number of Control licenses	false	integer								

			totalCore	[DEPRECATED] Total Number of Core licenses	false	integer
			totalLicenses	The total number of licenses on all Surfaces for all Bundles.	false	integer
			unlimitedComplete	[DEPRECATED] True if Complete licenses count is unlimited	false	boolean
			unlimitedControl	[DEPRECATED] True if Control licenses count is unlimited	false	boolean
			unlimitedCore	[DEPRECATED] True if Core licenses count is unlimited	false	boolean
			unlimitedExpiration	The Account does not expire	false	boolean
			updatedAt	Timestamp of last update	false	string
			usageType	Usage type	false	enum
errors	Errors	false	array			

Update Account

PUT /web/api/v2.1/accounts/{account_id}

Change the data of an Account. This command requires a Global user or an Account user and Admin role. Use this command to change the name, ID, SKUs and how they are distributed among Sites and Agents, and more. (See the Body sample.) Best practice: Consult with your SentinelOne SE.

BEST PRACTICE

Consult with your SentinelOne SE.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

404 - Account not found

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
accountType	Account type	false	string
activeAgents	Total Agents in the Account	false	integer
billingMode	Billing mode	false	enum
createdAt	Timestamp of Account creation	false	string
creator	The user that created the group	false	string
creatorId	The ID of the user that	false	string

				created the group		
			expiration	Expiration	false	string
			externalId	ID of CRM external system	false	string
			id	Account ID	false	string
			isDefault	Is default	false	boolean
			licenses	The account licenses.	false	

Name	Description	Required	Value
bundles	The licenses Bundles	false	

Name	Description	Required	Value
displayName	The Bundle display name	false	string
majorVersion	The Bundle major version	false	integer
minorVersion	The Bundle minor version	false	integer
name	The Bundle internal api name	false	string
surfaces	The Surfaces in the Bundle	false	

Name	D
count	Th co in ur co
name	Th na

Name	Description	Required	Value
totalSurfaces	The total number of Surfaces in this Bundle. -1 indicates unlimited count.	false	integer

Name	Description	Required	Value
modules	The licenses Add-ons	false	

Name	Description	Required	Value
displayName	The Add-on	false	string

							product features active for this account		
						unlimited	True if this is an unlimited SKU.	false	boolean
			state	Account state	false	enum			
			totalLicenses	The total number of licenses on all Surfaces for all Bundles.	false	integer			
			unlimitedExpiration	The Account does not expire	false				
			updatedAt	Timestamp of last update	false	string			
			usageType	Usage type	false	enum			
errors	Errors	false	array						

Body Schema

Name	Description	Required	Value
data	Data	true	

Name	Description	Required	Value
accountType	Account type	false	enum
billingMode	Billing mode	false	enum
expiration	Expiration	false	string
externalId	ID of CRM external system	false	string
inherits	True if the policy is inherited from Global, False if the Account has its own edited policy	false	boolean
licenses	The license configuration for the Account	false	

Name	Description	Required	Value
bundles	The list of Bundles selected	false	
modules	The list of Add-ons selected	false	
settings	The list of Settings selected for	false	

Name	Description	Required	Value
name		true	string
majorVersion		false	integer
surfaces		false	

Name	Description	Required	Value
name		true	string

Name	Description	Required	Value
name		true	string

Name	Description	Required	Value
groupName		true	string

							the Bundle and Add-ons. If a Bundle or Add-on requires a Setting that is not defined, the default Setting is used.		setting		true	string
			name	Name	false	string						
			policy	Policy	false							

Name	Description	Required	Value
agentLoggingOn	True if logging is enabled in the agent	false	boolean
agentNotification	[DEPRECATED] Show end point notification on suspicious.Replaced by 'show_suspicious' in the agent UI section	false	boolean
agentUi	Agent ui	false	

Name	Description	Required	Value
agentUiOn	Agent ui on	false	boolean
contactCompany	Contact company	false	string
contactDirectMessage	Contact direct message	false	string
contactEmail	Contact email	false	string
contactFreeText	Contact free text	false	string
contactOther	Contact other	false	string

									contactPhoneNumber	Contact phone number	false	string	
									contactSupportWebsite	Contact support website	false	string	
									devicePopUpNotifications	Device pop up notifications	false	boolean	
									maxEventAgeDays	Max event age days	false	integer	
									showAgentWarnings	Show agent warnings	false	boolean	
									showDeviceTab	Show device tab	false	boolean	
									showQuarantineTab	Show quarantine tab	false	boolean	
									showSupport	Show support	false	boolean	
									showSuspicious	Show suspicious	false	boolean	
									threatPopUpNotifications	Threat pop up notifications	false	boolean	
							agentUiOn	[DEPRECATED] Show/hide Agent UI. Moved inside the agent UI section	false	boolean			
							allowRemoteShell	True if Remote Shell is enabled for the scope	false	boolean			
							antiTamperingOn	Anti tampering on/off	false	boolean			
							autoDecommissionDays	Automatic decommission	false	integer			

							period in days	
						autoDecommissionOn	Auto decommission on	false	boolean
						autoFileUpload	Automatic file upload configuration	false

Name	Description	Required	Value
enabled	Automatic file upload on/off	false	boolean
includeBenignFiles	Upload benign files	false	boolean
maxDailyFileUpload	Maximum size (MB) to upload daily	false	integer
maxDailyFileUploadLimit	Limit for the maximum size (MB) to upload daily	false	integer
maxFileSize	Maximum file size (MB) to upload	false	integer
maxFileSizeLimit	Limit for the maximum file size (MB) to upload	false	integer
maxLocalDiskUsage	Maximum local disk usage (MB) for uploaded files	false	integer
maxLocalDiskUsageLimit	Limit for the maximum local disk usage (MB) for uploaded files	false	integer

autoImmuneOn | Automatic immune on/off - this value must be | false | boolean

							true since all policies are immune by default	
						autoMitigationAction	Default action for auto mitigation	false	string
						cloudValidationOn	Cloud validation on	false	
						createdAt	Timestamp of policy creation	false	string
						driverBlocking	Suspicious driver blocking engine on/off	false	boolean
						dvAttributesPerEventType	The DV attributes	false	

Name	Description	Required	Value
autoInstallBrowserExtensions	Auto install browser extensions	false	
behavioralIndicators	Behavioral indicators event	false	
commandScripts	Command scripts event	false	
crossProcess	Cross process event	false	

Name	De
autoInstallBrowserExtensions	Au br ex

Name	De
dvEventTypeBehavioralIndicators	Be in ev

Name	De
dvEventTypeCommandScripts	Co sc

Name	De
dvEventTypeCrossProcessDuplicateProcess	Du Pr Ev
dvEventTypeC	Du

| | | |

										ip	Network event - IP	false	Name	D
													dvEventTypeIpConnect	IP Ev
													dvEventTypeIpListen	IP Ev
										login	User login/ logout event	false	Name	D
													dvEventTypeLoginLoggedIn	Us Ev
													dvEventTypeLoginLoggedOut	Us Ev
										namedPipe	Named Pipe	false	Name	D
													dvEventTypeNamedPipeConnection	Na Co Ev
													dvEventTypeNamedPipeCreation	Na Cr Ev
										namedPipeExtended	Named Pipe Extended	false	Name	D
													namedPipeExtended	Na Co Ex Ev
										process	Process event	false	Name	D
													dvEventTypeProcessCreation	Pr Cr Ev
													dvEventTypeProcessExit	Pr Ev
													dvEventTypeProcessModification	Pr Te Ev
										registry	Registry event	false	Name	D

												dvEventTypeRegistryKeyCreated	Re Cr Ev
												dvEventTypeRegistryKeyDelete	Re De Ty
												dvEventTypeRegistryKeyExport	Re Ex Ty
												dvEventTypeRegistryKeyImport	Re Im Ty
												dvEventTypeRegistryKeyRename	Re Re Ev
												dvEventTypeRegistryKeySecurityChanged	Re Se Ch Ev
												dvEventTypeRegistryValueCreated	Re Va Ev
												dvEventTypeRegistryValueDeleted	Re Va De Ev
												dvEventTypeRegistryValueModified	Re Va M Ev
										scheduledTask	Scheduled task event	false	Name / De
												dvEventTypeScheduledTaskDelete	Sc Ta Ev
												dvEventTypeScheduledTaskRegister	Sc Ta Ev
												dvEventTypeS	Sc

									penetration	penetration	false	enum
									preExecution	on-write	false	enum
									preExecution Suspicious	pre execution suspicious	false	enum
									pup	potentially unwanted applications (PUP)	false	enum
									remoteShell	remote shell	false	enum
									reputation	reputation	false	enum
							forensicsAuto Triggering	Forensics auto triggering configuration	false	Name	Description	Required	Value
										linuxEnabled	True if linux forensics is enabled	false	boolean
										linuxProfileId	The profile id for the linux forensics	false	string
										linuxProfileName	The profile name for the linux forensics	false	string
										macosEnabled	True if macos forensics is enabled	false	boolean
										macosProfileId	The profile id for the macos forensics	false	string
										macosProfileName	The profile name for the macos forensics	false	string
										windowsEnabled	True if windows forensics is enabled	false	boolean
										windowsProfileId	The profile id for the windows	false	string

											forensics			
										windowsProfileName	The profile name for the windows forensics	false	string	
						identityEndpointReporting	Endpoint reporting level	false	enum					
						identityOn	Identity module on/off	false	boolean					
						identityReportInterval	Identity telemetry report interval in minutes	false	integer					
						identityThrottlingInterval	Identity duplicate command consolidation interval in minutes	false	integer					
						identityUpdateInterval	Identity update interval in minutes	false	integer					
						inheritedFrom	Indicates the parent scope from which this policy is inherited, or 'null' if it is not inherited (modified specifically for the current scope).	false	enum					
						ioc	True if ioc is enabled	false	boolean					

						iocAttributes	The Ioc attributes	false

Name	Description	Required	Value
autoInstallBrowserExtensions	Update auto install browser extensions	false	boolean
behavioralIndicators	Update behavioral indicators	false	boolean
commandScripts	Update command scripts	false	boolean
crossProcess	Update cross process	false	boolean
dataMasking	Update data masking	false	boolean
dllModuleLoad	Update DLL module load	false	boolean
dns	Network event - DNS	false	boolean
driver	Driver	false	boolean
fds	Full disk scan	false	boolean
file	File event	false	boolean
ip	Network event - IP	false	boolean
login	User login/ logout event	false	boolean
namedPipe	Named Pipe	false	boolean
namedPipeExtended	Named Pipe Extended	false	boolean
process	Process creation event	false	boolean
registry	Registry event	false	boolean
scheduledTask	Scheduled task event	false	boolean

									smartFileMonitoring: Smart file monitoring; false; boolean url: Ioc URI; false; boolean windowsEventLogs: Windows Event Log; false; boolean windowsEventLogsExtended: Windows Event Log Extended; false; boolean
						iocSupported	Ioc supported for the scope	false	boolean
						isDefault	True if this is the tenant policy	false	boolean
						isDvPolicyPerEventType	FE indication as to how to display DV policy	false	boolean
						mitigationMode	Mitigation modes	false	enum
						mitigationModeSuspicious	Mitigation mode	false	enum
						monitorOnExecute	Monitor on execute on/off	false	boolean
						monitorOnWrite	Monitor on write	false	boolean
						networkQuarantineOn	Network quarantine on	false	boolean
						remoteOpsForensics	Remote ops forensics configuration	false	Name: Description; Required; Value cpuLimit: CPU resources limit for collection process; false; integer enabled: Enabled; false; boolean maximumDailyUpload: Maximum size to upload; false; integer

									daily			
									maximumDailyUploadLimit	Limit for the maximum size to upload daily	false	integer
									maximumFileSizeUpload	Maximum size for single file	false	integer
									maximumFileSizeUploadLimit	Limit for the maximum file size to upload	false	integer
									parsedArtifactsDestination	Default destination of parsed artifacts	false	enum
							remoteScriptOrchestration	Remote script orchestration upload limits configuration	false	Name	Description	Required	Value
										alwaysUploadStreamToCloud	Always upload streams to cloud	false	boolean
										maxDailyFileDownload	Maximum size (MB) to download daily	false	integer
										maxDailyFileDownloadLimit	Limit for the maximum size (MB) to download daily	false	integer
										maxDailyFileUpload	Maximum size (MB) to upload daily	false	integer
										maxDailyFileUploadLimit	Limit for the maximum size (MB) to upload daily	false	integer
										maxFileSize	Maximum size in bytes for single file	false	integer

										maxFileSizeLimit	Limit for the maximum file size (MB) to upload	false	integer	
										maxLocalPackageDiskUsage	Maximum local disk usage (MB) for packages	false	integer	
										maxLocalPackageDiskUsageLimit	Limit for the maximum local disk usage (MB) for packages	false	integer	
							removeMacros	Determines if macros should be removed from macro threats	false	boolean				
							researchOn	Share data with SentinelOne	false	boolean				
							scanNewAgents	If True initiate full disk scan upon first registration	false	boolean				
							signedDriverBlockingOn	Suspicious signed driver blocking on/off	false	boolean				
							snapshotsOn	True if snapshots are enabled	false	boolean				
							unsignedDriverBlockingOn	Suspicious unsigned driver blocking on/off	false	boolean				
							updatedAt	Time of the last update to the policy	false	string				

						userFullName: The user that created the policy; false; string userId: The user id; false; string
			salesforceId		false	string
			skus	[DEPRECATED] Use licenses instead	false	Name: totalLicenses; Description: Number of licenses for this specific SKU. Applicable only if unlimited is False; Required: false; Value: integer Name: type; Description: The suite of product features active for this Account; Required: false; Value: enum Name: unlimited; Description: True if this is an unlimited SKU. Total licenses will be ignored if unlimited is True; Required: false; Value: boolean
			unlimitedExpiration	If expiration is not limited, enter the expiration date and time yyyy-mm-ddThh:mm:ss	false	boolean
			usageType	Usage type	false	enum

Revert Policy

PUT /web/api/v2.1/accounts/{account_id}/revert-policy

The policy of the Account is based on the default Global policy and is enforced by all endpoints in the Sites and Groups of the Account (if you did not change the Site or Group policies). If you change the Account policy, you can use this command to revert it to the default Global policy.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>success</td><td>Indicates a successful operation</td><td>false</td><td>boolean</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

Name	Description	Required	Value
data	Data	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>id</td><td>Id</td><td>false</td><td>string</td></tr></table>

Reactivate Account

PUT /web/api/v2.1/accounts/{account_id}/reactivate

Reactivate an expired Account. This command requires a Global user or Support. Consult with your SentinelOne SE.

Response Messages

200 - Account reactivated

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

404 - Account not found

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td><table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>success</td><td>Indicates a successful operation</td><td>false</td><td>boolean</td></tr></table></td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>expiration</td><td>New expiration date for the Account</td><td>false</td><td>string</td></tr>
<tr><td>unlimited</td><td>If false enter an expiration date and time (yyyy-mm-ddThh:mm:ss</td><td>false</td><td>boolean</td></tr>
</table>
</td></tr>
</table>

Expire an Account

POST /web/api/v2.1/accounts/{account_id}/expire-now

Expire an Account immediately. The user must have Global access or Account acces with permissions for the Account. Best practice: Consult with Support before you use this command.

> **BEST PRACTICE**
> Consult with Support before you use this command.

Response Messages

200 - Expire account now

401 - Unauthorized access - please sign in and retry.

404 - Account not found

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
accountType	Account type	false	string
activeAgents	Total Agents in the Account	false	integer
billingMode	Billing mode	false	enum
createdAt	Timestamp of Account creation	false	string
creator	The user that created the group	false	string
creatorId	The ID of the user that created the group	false	string

			expiration	Expiration	false	string
			externalId	ID of CRM external system	false	string
			id	Account ID	false	string
			isDefault	Is default	false	boolean
			licenses	The account licenses.	false	

Name	Description	Required	Value
bundles	The licenses Bundles	false	

Name	Description	Required	Value
displayName	The Bundle display name	false	string
majorVersion	The Bundle major version	false	integer
minorVersion	The Bundle minor version	false	integer
name	The Bundle internal api name	false	string
surfaces	The Surfaces in the Bundle	false	

Name	D
count	Th co in ur co
name	Th na

Name	Description	Required	Value
totalSurfaces	The total number of Surfaces in this Bundle. -1 indicates unlimited count.	false	integer

Name	Description	Required	Value
modules	The licenses Add-ons	false	

Name	Description	Required	Value
displayName	The Add-on display name	false	string
majorVersion	The Add-on	false	integer

							active for this account		
						unlimited	True if this is an unlimited SKU.	false	boolean
			state	Account state	false	enum			
			totalLicenses	The total number of licenses on all Surfaces for all Bundles.	false	integer			
			unlimitedExpiration	The Account does not expire	false				
			updatedAt	Timestamp of last update	false	string			
			usageType	Usage type	false	enum			
errors	Errors	false	array						

Get Uninstall Password Metadata

GET /web/api/v2.1/accounts/{account_id}/uninstall-password/metadata

Get the uninstall password metadata, such as which user created and revoked it and when.

Response Messages

200 - Success

401 - Unauthorized access - please sign in and retry.

403 - Insufficient permissions

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
generatedBy Name	name of the user that generated the uninstall password	true	string
lastRevoked	uninstall password last revoked date	true	string
revokedByN ame	Revoked by name	true	string
version	Version	true	integer
createdAt	password creation date: yyyy-mm-dd	false	string
expiration	password expiration date format: yyyy-mm-dd	false	string
generatedByI d	The ID of the user that	false	integer

			generated the uninstall password		
			revokedById	The ID of the user that revoked the uninstall password	false	integer
errors	Errors	false	array

Get Uninstall Password

GET /web/api/v2.1/accounts/{account_id}/uninstall-password/view

Get the uninstall password to uninstall several Agents of one Account with one command.

Response Messages

200 - Success

401 - Unauthorized access - please sign in and retry.

403 - Insufficient permissions

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>password</td><td>msg EC signed with private key: v1.base64(data).base64(ES384(data))</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Generate/Regenerate Uninstall Password

POST /web/api/v2.1/accounts/{account_id}/uninstall-password/generate

You can uninstall all Agents of one Account with one command that requires a password. This command sets a new account-level uninstall password.
To enable this feature, submit a ticket with Support.
Best Practice: After you uninstall the Agents and install again, revoke the passphrase.
Applicable on Windows (versions 4.4+) and Linux (versions 21.7+) Agents.

BEST PRACTICE

After you uninstall the Agents and install again, revoke the passphrase.
Applicable on Windows (versions 4.4+) and Linux (versions 21.7+) Agents.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - Insufficient permissions

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
generatedBy Name	name of the user that generated the uninstall password	true	string
lastRevoked	uninstall password last revoked date	true	string
revokedByN ame	Revoked by name	true	string

			<table><tr><td>version</td><td>Version</td><td>true</td><td>integer</td></tr><tr><td>createdAt</td><td>password creation date: yyyy-mm-dd</td><td>false</td><td>string</td></tr><tr><td>expiration</td><td>password expiration date format: yyyy-mm-dd</td><td>false</td><td>string</td></tr><tr><td>generatedById</td><td>The ID of the user that generated the uninstall password</td><td>false</td><td>integer</td></tr><tr><td>revokedById</td><td>The ID of the user that revoked the uninstall password</td><td>false</td><td>integer</td></tr></table>
errors	Errors	false	array

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>expiration</td><td>password expiration date format: yyyy-mm-dd</td><td>true</td><td>string</td></tr>
</table>
</td></tr>
</table>

Revoke Uninstall Password

POST /web/api/v2.1/accounts/{account_id}/uninstall-password/revoke

Delete the account-level uninstall password. If you do not delete it, you or another Console user can mistakenly use the Account passphrase (and uninstall all Agents) when you mean to uninstall one Agent.

Response Messages

200 - Success

401 - Unauthorized access - please sign in and retry.

403 - Insufficient permissions

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
generatedBy Name	name of the user that generated the uninstall password	true	string
lastRevoked	uninstall password last revoked date	true	string
revokedByN ame	Revoked by name	true	string
version	Version	true	integer
createdAt	password creation date: yyyy-mm-dd	false	string
expiration	password expiration date format: yyyy-mm-dd	false	string
generatedByI	The ID of the	false	integer

			d user that generated the uninstall password revokedById The ID of the user that revoked the uninstall password false integer
errors	Errors	false	array

Export Accounts

GET /web/api/v2.1/export/accounts

Export Accounts data to a CSV, for Accounts that match the filter.

Parameters

accountids	optional	List of Account IDs to search for. Example: "225494730938493804,225494730938493915".
accounttype	optional	Account type. Example: "Trial".
activelicenses	optional	Active licenses
billingmode	optional	Billing mode. Example: "subscription".
createdat	optional	Timestamp of Account creation. Example: "2018-02-27T04:49:26.257525Z".
expiration	optional	Expiration. Example: "2018-02-27T04:49:26.257525Z".
features	optional	Filter the list of Accounts for those that support this feature. Example: "firewall-control".
ids	optional	A list of Account IDs. Example: "225494730938493804,225494730938493915".
isdefault	optional	Is default
name	optional	Name. Example: "My Account".
query	optional	Full text search for fields: name. (Note: on single-Account Consoles, the Account name will not be matched)
states	optional	Filter by state, such as active or expired.
totallicenses	optional	Total licenses
updatedat	optional	Timestamp of last update. Example: "2018-02-27T04:49:26.257525Z".
usagetype	optional	Usage type. Example: "customer".

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Activities

Get Activities

GET /web/api/v2.1/activities

Get the activities, and their data, that match the filters.
We recommend that you set some values for the filters. The full list will be too large to be useful.

Parameters

accountids	optional	List of Account IDs to filter by. Example: "225494730938493804,225494730938493915".
activitytypes	optional	Return only these activity codes (comma-separated list). Select a code from the drop-down, or see the id field from the Get activity types command. . Example: "52,53,71,72".
activityuuids	optional	Return activities by specific activity UUIDs. Example: "a2c8037c-e6df-436d-b92b-bc09a418717e,f15b308b-fab9-4c0b-b6f5-17d236a7bf55".
agentids	optional	Return activities related to specified agents. Example: "225494730938493804,225494730938493915".
alertids	optional	Return activities related to specified alerts. Example: "225494730938493804,225494730938493915".
countonly	optional	If true, only total number of items will be returned, without any of the actual objects.
createdat__between	optional	Get activities created in this range (inclusive) of a start timestamp and an end timestamp. Example: "1514978764288-1514978999999".
createdat__gt	optional	Get activities created after this timestamp. Example: "2018-02-27T04:49:26.257525Z".
createdat__gte	optional	Get activities created after or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
createdat__lt	optional	Get activities created before this timestamp. Example:

		"2018-02-27T04:49:26.257525Z".
createdat__lte	optional	Get activities created before or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
cursor	optional	Cursor position returned by the last request. Use to iterate over more than 1000 items. Example: "YWdlbnRfaWQ6NTgwMjkzODE=".
groupids	optional	List of Group IDs to filter by. Example: "225494730938493804,225494730938493915".
ids	optional	Filter activities by specific activity IDs. Example: "225494730938493804,225494730938493915".
includehidden	optional	Include internal activities hidden from display. Example: "False".
limit	optional	Limit number of returned items (1-1000). Example: "10".
ruleids	optional	Return activities related to specified rules. Example: "225494730938493804,225494730938493915".
siteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".
skip	optional	Skip first number of items (0-1000). To iterate over more than 1000 items, use "cursor". Example: "150".
skipcount	optional	If true, total number of items will not be calculated, which speeds up execution time.
sortby	optional	The column to sort the results by. Example: "id".
sortorder	optional	Sort direction. Example: "asc".
threatids	optional	Return activities related to specified threats. Example: "225494730938493804,225494730938493915".
useremails	optional	Email of the user who invoked the activity (If applicable)
userids	optional	The user who invoked the activity (If applicable). Example: "225494730938493804,225494730938493915".

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>pagination</td><td>Pagination information</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>totalItems</td><td>Total number of items found matching your query</td><td>true</td><td>integer</td></tr>
<tr><td>nextCursor</td><td>Pass this value as "cursor" on your next request, to get the next page of results (Will be "null" when last page reached)</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountId</td><td>Related account id (If applicable)</td><td>false</td><td>string</td></tr>
<tr><td>accountName</td><td>Related account name (If applicable)</td><td>false</td><td>string</td></tr>
<tr><td>activityType</td><td>Activity type</td><td>false</td><td>integer</td></tr>
<tr><td>activityUuid</td><td>Activity UUID</td><td>false</td><td>string</td></tr>
<tr><td>agentId</td><td>Related agent (If applicable)</td><td>false</td><td>string</td></tr>
<tr><td>agentUpdated Version</td><td>Agent's new version (If applicable)</td><td>false</td><td>string</td></tr>
<tr><td>comments</td><td>Comments</td><td>false</td><td>string</td></tr>
<tr><td>createdAt</td><td>Activity creation time</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
</table>

			(UTC)		
			data	Extra activity specific data	false	object
			description	Extra activity information	false	string
			groupId	Related group id (If applicable)	false	string
			groupName	Related group name (If applicable)	false	string
			hash	Threat file hash (If applicable)	false	string
			id	Activity ID	false	string
			osFamily	Agent's OS type (if applicable)	false	enum
			primaryDescription	Primary description	false	string
			secondaryDescription	Secondary description	false	string
			siteId	Related site id (If applicable)	false	string
			siteName	Related site name (If applicable)	false	string
			threatId	Related threat (If applicable)	false	string
			updatedAt	Activity last updated time (UTC)	false	string
			userId	The user who invoked the activity (If applicable)	false	string
errors	Errors	false	array			

Get Activity Types

GET /web/api/v2.1/activities/types

Get a list of activity types. This is useful to see valid values to filter activities in other commands.

Response Messages

200 - Success

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
data	Response data	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>action</td><td>Action described in the activity</td><td>false</td><td>string</td></tr><tr><td>descriptionTemplate</td><td>Activity description template as seen in activity page</td><td>false</td><td>string</td></tr><tr><td>id</td><td>Activity type ID</td><td>false</td><td>integer</td></tr></table>
errors	Errors	false	array

Last activity as Syslog message

GET /web/api/v2.1/last-activity-as-syslog

To see examples of Syslog messages, you can get the Syslog message that corresponds to the last activity that matches the filter. This is not intended for production purposes.
If Syslog messages that you expected to see are not in the response, make sure you selected "Syslog" for the activity type in Console > Settings > Notifications.
To see your Syslog settings, run: "settings/notifications".
To changethe settings, run: "settings/notifications" with the changes in the body of the request.

Parameters

accountids	optional	List of Account IDs to filter by. Example: "225494730938493804,225494730938493915".
activitytypes	optional	Return only these activity codes (comma-separated list). Select a code from the drop-down, or see the id field from the Get activity types command. . Example: "52,53,71,72".
activityuuids	optional	Return activities by specific activity UUIDs. Example: "a2c8037c-e6df-436d-b92b-bc09a418717e,f15b308b-fab9-4c0b-b6f5-17d236a7bf55".
agentids	optional	Return activities related to specified agents. Example: "225494730938493804,225494730938493915".
alertids	optional	Return activities related to specified alerts. Example: "225494730938493804,225494730938493915".
countonly	optional	If true, only total number of items will be returned, without any of the actual objects.
createdat__between	optional	Get activities created in this range (inclusive) of a start timestamp and an end timestamp. Example: "1514978764288-1514978999999".
createdat__gt	optional	Get activities created after this timestamp. Example: "2018-02-27T04:49:26.257525Z".
createdat__gte	optional	Get activities created after or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
createdat__lt	optional	Get activities created before this timestamp. Example: "2018-02-27T04:49:26.257525Z".
createdat__lte	optional	Get activities created before or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".

cursor	optional	Cursor position returned by the last request. Use to iterate over more than 1000 items. Example: "YWdlbnRfaWQ6NTgwMjkzODE=".
groupids	optional	List of Group IDs to filter by. Example: "225494730938493804,225494730938493915".
ids	optional	Filter activities by specific activity IDs. Example: "225494730938493804,225494730938493915".
includehidden	optional	Include internal activities hidden from display. Example: "False".
limit	optional	Limit number of returned items (1-1000). Example: "10".
ruleids	optional	Return activities related to specified rules. Example: "225494730938493804,225494730938493915".
siteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".
skip	optional	Skip first number of items (0-1000). To iterate over more than 1000 items, use "cursor". Example: "150".
skipcount	optional	If true, total number of items will not be calculated, which speeds up execution time.
sortby	optional	The column to sort the results by. Example: "id".
sortorder	optional	Sort direction. Example: "asc".
threatids	optional	Return activities related to specified threats. Example: "225494730938493804,225494730938493915".
useremails	optional	Email of the user who invoked the activity (If applicable)
userids	optional	The user who invoked the activity (If applicable). Example: "225494730938493804,225494730938493915".

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value

<table>
<tr><td>pagination</td><td>Pagination information</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>totalItems</td><td>Total number of items found matching your query</td><td>true</td><td>integer</td></tr>
<tr><td>nextCursor</td><td>Pass this value as "cursor" on your next request, to get the next page of results (Will be "null" when last page reached)</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>activityId</td><td>ID of the activity</td><td>false</td><td>string</td></tr>
<tr><td>syslogMessage</td><td>Syslog message corresponding to the activity</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Export Activities

GET /web/api/v2.1/export/activities

Export the list of activities.

Parameters

accountids	optional	List of Account IDs to filter by. Example: "225494730938493804,225494730938493915".
activitytypes	optional	Return only these activity codes (comma-separated list). Select a code from the drop-down, or see the id field from the Get activity types command. . Example: "52,53,71,72".
activityuuids	optional	Return activities by specific activity UUIDs. Example: "a2c8037c-e6df-436d-b92b-bc09a418717e,f15b308b-fab9-4c0b-b6f5-17d236a7bf55".
agentids	optional	Return activities related to specified agents. Example: "225494730938493804,225494730938493915".
alertids	optional	Return activities related to specified alerts. Example: "225494730938493804,225494730938493915".
createdat__between	optional	Get activities created in this range (inclusive) of a start timestamp and an end timestamp. Example: "1514978764288-1514978999999".
createdat__gt	optional	Get activities created after this timestamp. Example: "2018-02-27T04:49:26.257525Z".
createdat__gte	optional	Get activities created after or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
createdat__lt	optional	Get activities created before this timestamp. Example: "2018-02-27T04:49:26.257525Z".
createdat__lte	optional	Get activities created before or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
groupids	optional	List of Group IDs to filter by. Example: "225494730938493804,225494730938493915".
ids	optional	Filter activities by specific activity IDs. Example: "225494730938493804,225494730938493915".
includehidden	optional	Include internal activities hidden from display. Example: "False".

rowslimit	optional	Limit number of returned items (1-10000). Example: "100".
ruleids	optional	Return activities related to specified rules. Example: "225494730938493804,225494730938493915".
siteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".
threatids	optional	Return activities related to specified threats. Example: "225494730938493804,225494730938493915".
useremails	optional	Email of the user who invoked the activity (If applicable)
userids	optional	The user who invoked the activity (If applicable). Example: "225494730938493804,225494730938493915".

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Agent Actions

Broadcast Message

POST /web/api/v2.1/agents/actions/broadcast

You can send a message through the Agents that users can see.
This is useful for endpoints that have human users. This command is supported on Windows and macOS endpoints (not supported on Linux). The message is sent to all endpoints that match the filter.
Put the message in the data parameter: "data":{"message":"<your message>"}
The message must be 140 characters or less.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - User has insufficient permissions to perform the requested action

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>affected</td><td>Number of entities affected by the requested operation</td><td>false</td><td>integer</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>message</td><td>Message to broadcast to agents.</td><td>true</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>filter</td><td>Applied filter - only matched Agents will be affected by the requested action. Leave empty to apply the action on all applicable Agents.</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>activeThreats</td><td>Include Agents with this amount of active threats</td><td>false</td><td>integer</td></tr>
<tr><td>activeThreats__gt</td><td>Include Agents with at least this amount of active threats</td><td>false</td><td>integer</td></tr>
<tr><td>adComputerMember__contains</td><td>Free-text filter by Active Directory computer groups string (supports multiple values)</td><td>false</td><td>string []</td></tr>
<tr><td>adComputerName__contains</td><td>Free-text filter by Active Directory computer name string (supports multiple values)</td><td>false</td><td>string []</td></tr>
<tr><td>adComputerQ</td><td>Free-text</td><td>false</td><td>string []</td></tr>
</table>
</td></tr>
</table>

			uery__contains	filter by Active Directory computer name or its groups (supports multiple values)		
			adQuery	An Active Directory query string	false	string
			adQuery__contains	Free-text filter by Active Directory string (supports multiple values)	false	string []
			adUserMember__contains	Free-text filter by Active Directory user groups string (supports multiple values)	false	string []
			adUserName__contains	Free-text filter by Active Directory username string (supports multiple values)	false	string []
			adUserQuery__contains	Free-text filter by Active Directory computer name or its	false	string []

				groups (supports multiple values)		
			agentNamespace__contains	Free-text filter by agent namespace (supports multiple values)	false	string []
			agentPodName__contains	Free-text filter by agent pod name (supports multiple values)	false	string []
			agentVersion__between	Version range for agent version (format: <from_version>-<to_version>, inclusive)	false	string
			agentVersion__gt	Agents versions greater than given version	false	string
			agentVersion__gte	Agents versions greater than or equal to given version	false	string
			agentVersion__lt	Agents versions less than given version	false	string
			agentVersion__lte	Agents versions less than or equal to given version	false	string

			agentVersions	Agent versions to include	false	string []
			agentVersionsNin	Agent versions not to include	false	string []
			appsVulnerabilityStatuses	Apps vulnerability status in	false	string []
			appsVulnerabilityStatusesNin	Apps vulnerability status nin	false	string []
			awsRole__contains	Free-text filter by aws role(supports multiple values)	false	string []
			awsSecurityGroups__contains	Free-text filter by aws securityGroups(supports multiple values)	false	string []
			awsSubnetIds__contains	Free-text filter by aws subnet ids (supports multiple values)	false	string []
			azureResourceGroup__contains	Free-text filter by azure resource group(supports multiple values)	false	string []
			cloudAccount__contains	Free-text filter by cloud account (supports multiple values)	false	string []
			cloudImage__	Free-text	false	string []

			contains	filter by cloud image (supports multiple values)		
			cloudInstanceId__contains	Free-text filter by cloud instance id(supports multiple values)	false	string []
			cloudInstanceSize__contains	Free-text filter by cloud instance size(supports multiple values)	false	string []
			cloudLocation__contains	Free-text filter by cloud location (supports multiple values)	false	string []
			cloudNetwork__contains	Free-text filter by cloud network (supports multiple values)	false	string []
			cloudProvider	Agents from which cloud provider	false	string []
			cloudProviderNin	Exclude Agents from these cloud provider	false	string []
			cloudTags__contains	Free-text filter by cloud tags (supports multiple values)	false	string []

			clusterName__contains	Free-text filter by cluster name (supports multiple values)	false	string []
			computerName	Computer name	false	string
			computerName__contains	Free-text filter by computer name (supports multiple values)	false	string []
			computerName__like	Match computer name partially (substring)	false	string
			consoleMigrationStatuses	Migration status in	false	string []
			consoleMigrationStatusesNin	Migration status nin	false	string []
			coreCount__between	Possible number of CPU cores (inclusive)	false	string
			coreCount__gt	CPU cores (more than)	false	integer
			coreCount__gte	CPU cores (more than or equal)	false	integer
			coreCount__lt	CPU cores (less than)	false	integer
			coreCount__lte	CPU cores (less than or equal)	false	integer
			cpuCount__between	Possible number of	false	string

				CPU cores (inclusive)		
			cpuCount__gt	Number of CPUs (more than)	false	integer
			cpuCount__gte	Number of CPUs (more than or equal)	false	integer
			cpuCount__lt	Number of CPUs (less than)	false	integer
			cpuCount__lte	Number of CPUs (less than or equal)	false	integer
			cpuId__contains	Free-text filter by CPU name (supports multiple values)	false	string []
			createdAt__between	Date range for creation time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			createdAt__gt	Agents created after this timestamp	false	string
			createdAt__gte	Agents created after or at this timestamp	false	string
			createdAt__lt	Agents created before this timestamp	false	string
			createdAt__lte	Agents created	false	string

				before or at this timestamp		
			csvFilterId	The ID of the CSV file to filter by	false	string
			decommissionedAt__between	Date range for decommission time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			decommissionedAt__gt	Agents decommissioned after this timestamp	false	string
			decommissionedAt__gte	Agents decommissioned after or at this timestamp	false	string
			decommissionedAt__lt	Agents decommissioned before this timestamp	false	string
			decommissionedAt__lte	Agents decommissioned before this timestamp	false	string
			domains	Included network domains	false	string []
			domainsNin	Not included network domains	false	string []
			encryptedApplications	Disk encryption status	false	boolean
			externalId__c	Free-text	false	string []

			ontains	filter by external ID (Customer ID)		
			externalIp__contains	Free-text filter by visible IP (supports multiple values)	false	string []
			filteredGroupIds	List of Group IDs to filter by	false	string []
			filteredSiteIds	List of Site IDs to filter by	false	string []
			filterId	Include all Agents matching this saved filter	false	string
			firewallEnabled	The agents supports Firewall Control and it is enabled for the agent's group	false	boolean []
			gatewayIp	Gateway ip	false	string
			gcpServiceAccount__contains	Free-text filter by gcp service account (supports multiple values)	false	string []
			groupIds	List of Group IDs to filter by	false	string []
			hasContainerizedWorkload	Include only Agents protecting containerized workloads	false	boolean

			hasLocalConfiguration	Agent has a local configuration set	false	boolean
			hasTags	Include only Agents that have any tags assigned if True, or none if False	false	boolean
			ids	A list of Agent IDs	false	string []
			infected	Include only Agents with at least one active threat	false	boolean
			installerTypes	Include only Agents installed with these package types	false	string []
			installerTypesNin	Exclude Agents installed with these package types	false	string []
			isActive	Include only active Agents	false	boolean
			isDecommissioned	Include active, decommissioned or both	false	boolean []
			isPendingUninstall	Include only Agents with pending uninstall requests	false	boolean
			isUninstalled	Include installed, uninstalled or	false	boolean []

				both		
			isUpToDate	Include only Agents with updated software	false	boolean
			k8sNodeLabels__contains	Free-text filter by K8s node labels (supports multiple values)	false	string []
			k8sNodeName__contains	Free-text filter by K8s node name (supports multiple values)	false	string []
			k8sType__contains	Free-text filter by K8s type(supports multiple values)	false	string []
			k8sVersion__contains	Free-text filter by K8s version (supports multiple values)	false	string []
			lastActiveDate__between	Date range for last active date(format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			lastActiveDate__gt	Agents last active after this time	false	string
			lastActiveDate__gte	Agents last active after or at this time	false	string
			lastActiveDat	Agents last	false	string

			e__lt	active before this time		
			lastActiveDate__lte	Agents last active before or at this time	false	string
			lastLoggedInUserName__contains	Free-text filter by username (supports multiple values)	false	string []
			lastSuccessfulScanDate__between	Date range for last successful full disk scan(format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			lastSuccessfulScanDate__gt	Agents last successful full disk scan after this time	false	string
			lastSuccessfulScanDate__gte	Agents last successful full disk scan after or at this time	false	string
			lastSuccessfulScanDate__lt	Agents last successful full disk scan before this time	false	string
			lastSuccessfulScanDate__lte	Agents last successful full disk scan before or at this time	false	string
			liveUpdateId__contains	Free-text filter by live	false	string []

				update ID (supports multiple values)		
			locationEnabled	The agents supports Location Awareness and it is enabled for the agent's group	false	boolean []
			locationIds	Include only Agents reporting these locations	false	string []
			locationIdsNin	Do not include only Agents reporting these locations	false	string []
			machineTypes	Included machine types	false	string []
			machineTypesNin	Not included machine types	false	string []
			migrationStatus	Migration status	false	enum
			missingPermissions	Included missing permissions	false	string []
			missingPermissionsNin	Excluded missing permissions	false	string []
			mitigationMode	Agent mitigation mode policy	false	enum
			mitigationMo	Mitigation	false	enum

			deSuspicious	mode policy for suspicious activity		
			networkInterfaceGatewayMacAddress__contains	Free-text filter by Gateway MAC address (supports multiple values)	false	string []
			networkInterfaceInet__contains	Free-text filter by local IP (supports multiple values)	false	string []
			networkInterfacePhysical__contains	Free-text filter by MAC address (supports multiple values)	false	string []
			networkQuarantineEnabled	The agents supports Network Quarantine Control and its enabled for the agent's group	false	boolean []
			networkStatuses	Included network statuses	false	string []
			networkStatusesNin	Included network statuses	false	string []
			operationalStates	Agent operational state	false	string []
			operationalStatesNin	Do not include these Agent operational	false	string []

				states		
			osArch	OS architecture	false	enum
			osTypes	Included OS types	false	string []
			osTypesNin	Not included OS types	false	string []
			osVersion__contains	Free-text filter by OS full name and version (supports multiple values)	false	string []
			query	A free-text search term, will match applicable attributes (sub-string match). Note: Device's physical addresses will be matched if they start with the search term only (no match if they contain the term).	false	string
			rangerStatus	[DEPRECATED] Use rangerStatuses.	false	enum
			rangerStatuses	Status of Ranger	false	string []
			rangerStatusesNin	Do not include these Ranger Statuses	false	string []

			rangerVersions	Ranger versions to include	false	string []
			rangerVersionsNin	Ranger versions not to include	false	string []
			registeredAt__between	Date range for first registration time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			registeredAt__gt	Agents registered after this time	false	string
			registeredAt__gte	Agents registered after or at this time	false	string
			registeredAt__lt	Agents registered before this time	false	string
			registeredAt__lte	Agents registered before or at this time	false	string
			remoteOpsForensicsSupported	Include only agents that has Remote Ops Forensicsfeature supported	false	boolean
			remoteProfilingStates	Agent remote profiling state	false	string []
			remoteProfilingStatesNin	Do not include these Agent remote	false	string []

				profiling states		
			rsoLevel	Supported Remote Script Orchestration level	false	enum
			scanStatus	Scan status	false	enum
			scanStatuses	Included scan statuses	false	string []
			scanStatuses Nin	Not included scan statuses	false	string []
			serialNumber __contains	Free-text filter by Serial Number (supports multiple values)	false	string []
			siteIds	List of Site IDs to filter by	false	string []
			tagsData	Filter agents by their assigned tags. Given in form of a JSON where each key represents a tag key, and each value represents a list of string values to filter by. To filter by unassigned tag values, use __nin suffix in the tag key.	false	string
			threatConten	Include only	false	string

			tHash	Agents that have at least one threat with this content hash		
			threatCreatedAt__between	Agents with threats reported in a date range (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			threatCreatedAt__gt	Agents with threats reported after this time	false	string
			threatCreatedAt__gte	Agents with threats reported after or at this time	false	string
			threatCreatedAt__lt	Agents with threats reported before this time	false	string
			threatCreatedAt__lte	Agents with threats reported before or at this time	false	string
			threatHidden	Include only Agents with at least one hidden threat	false	boolean
			threatMitigationStatus	Include only Agents that have threats with this mitigation	false	enum

				status		
			threatRebootRequired	Has at least one threat with at least one mitigation action pending reboot to succeed	false	boolean []
			threatResolved	Include only Agents with at least one resolved threat	false	boolean
			totalMemory__between	Total memory range (GB, inclusive)	false	string
			totalMemory__gt	Memory size (MB, more than)	false	integer
			totalMemory__gte	Memory size (MB, more than or equal)	false	integer
			totalMemory__lt	Memory size (MB, less than)	false	integer
			totalMemory__lte	Memory size (MB, less than or equal)	false	integer
			updatedAt__between	Date range for update time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			updatedAt__gt	Agents updated after this timestamp	false	string

			updatedAt__gte	Agents updated after or at this timestamp	false	string
			updatedAt__lt	Agents updated before this timestamp	false	string
			updatedAt__lte	Agents updated before or at this timestamp	false	string
			userActionsNeeded	Included pending user actions	false	string []
			userActionsNeededNin	Excluded pending user actions	false	string []
			uuid	Agent's universally unique identifier	false	string
			uuid__contains	Free-text filter by Agent UUID (supports multiple values)	false	string []
			uuids	A list of included UUIDs	false	string []

Connect to Network

POST /web/api/v2.1/agents/actions/connect

After you run "disconnect from network" on endpoints, analyze the issue, and mitigate threats. Use this command to reconnect to the network all endpoints that match the filter. To learn more, see "Disconnect from Network".

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - User has insufficient permissions to perform the requested action

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>affected</td><td>Number of entities affected by the requested operation</td><td>false</td><td>integer</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

Name	Description	Required	Value
filter	Applied filter - only matched Agents will be affected by the requested action. Leave empty to apply the action on all applicable Agents.	true	

Name	Description	Required	Value
accountIds	List of Account IDs to filter by	false	string []
activeThreats	Include Agents with this amount of active threats	false	integer
activeThreats__gt	Include Agents with at least this amount of active threats	false	integer
adComputerMember__contains	Free-text filter by Active Directory computer groups string (supports multiple values)	false	string []
adComputerName__contains	Free-text filter by Active Directory computer name string (supports multiple values)	false	string []
adComputerQuery__contains	Free-text filter by Active Directory computer name or its groups	false	string []

				(supports multiple values)		
			adQuery	An Active Directory query string	false	string
			adQuery__contains	Free-text filter by Active Directory string (supports multiple values)	false	string []
			adUserMember__contains	Free-text filter by Active Directory user groups string (supports multiple values)	false	string []
			adUserName__contains	Free-text filter by Active Directory username string (supports multiple values)	false	string []
			adUserQuery__contains	Free-text filter by Active Directory computer name or its groups (supports multiple values)	false	string []
			agentNamespa	Free-text	false	string []

			ce__contains	filter by agent namespace (supports multiple values)		
			agentPodName__contains	Free-text filter by agent pod name (supports multiple values)	false	string []
			agentVersion__between	Version range for agent version (format: <from_version>-<to_version>, inclusive)	false	string
			agentVersion__gt	Agents versions greater than given version	false	string
			agentVersion__gte	Agents versions greater than or equal to given version	false	string
			agentVersion__lt	Agents versions less than given version	false	string
			agentVersion__lte	Agents versions less than or equal to given version	false	string
			agentVersions	Agent versions to include	false	string []
			agentVersionsNin	Agent versions not	false	string []

				to include		
			appsVulnerabilityStatuses	Apps vulnerability status in	false	string []
			appsVulnerabilityStatusesNin	Apps vulnerability status nin	false	string []
			awsRole__contains	Free-text filter by aws role(supports multiple values)	false	string []
			awsSecurityGroups__contains	Free-text filter by aws securityGroups(supports multiple values)	false	string []
			awsSubnetIds__contains	Free-text filter by aws subnet ids (supports multiple values)	false	string []
			azureResourceGroup__contains	Free-text filter by azure resource group(supports multiple values)	false	string []
			cloudAccount__contains	Free-text filter by cloud account (supports multiple values)	false	string []
			cloudImage__contains	Free-text filter by cloud image (supports multiple values)	false	string []

			cloudInstanceId__contains	Free-text filter by cloud instance id(supports multiple values)	false	string []
			cloudInstanceSize__contains	Free-text filter by cloud instance size(supports multiple values)	false	string []
			cloudLocation__contains	Free-text filter by cloud location (supports multiple values)	false	string []
			cloudNetwork__contains	Free-text filter by cloud network (supports multiple values)	false	string []
			cloudProvider	Agents from which cloud provider	false	string []
			cloudProviderNin	Exclude Agents from these cloud provider	false	string []
			cloudTags__contains	Free-text filter by cloud tags (supports multiple values)	false	string []
			clusterName__contains	Free-text filter by cluster name (supports multiple values)	false	string []

			computerName	Computer name	false	string
			computerName__contains	Free-text filter by computer name (supports multiple values)	false	string []
			computerName__like	Match computer name partially (substring)	false	string
			consoleMigrationStatuses	Migration status in	false	string []
			consoleMigrationStatusesNin	Migration status nin	false	string []
			coreCount__between	Possible number of CPU cores (inclusive)	false	string
			coreCount__gt	CPU cores (more than)	false	integer
			coreCount__gte	CPU cores (more than or equal)	false	integer
			coreCount__lt	CPU cores (less than)	false	integer
			coreCount__lte	CPU cores (less than or equal)	false	integer
			cpuCount__between	Possible number of CPU cores (inclusive)	false	string
			cpuCount__gt	Number of CPUs (more than)	false	integer

			cpuCount__gte	Number of CPUs (more than or equal)	false	integer
			cpuCount__lt	Number of CPUs (less than)	false	integer
			cpuCount__lte	Number of CPUs (less than or equal)	false	integer
			cpuId__contains	Free-text filter by CPU name (supports multiple values)	false	string []
			createdAt__between	Date range for creation time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			createdAt__gt	Agents created after this timestamp	false	string
			createdAt__gte	Agents created after or at this timestamp	false	string
			createdAt__lt	Agents created before this timestamp	false	string
			createdAt__lte	Agents created before or at this timestamp	false	string
			csvFilterId	The ID of the CSV file to filter by	false	string

			decommissionedAt__between	Date range for decommission time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			decommissionedAt__gt	Agents decommissioned after this timestamp	false	string
			decommissionedAt__gte	Agents decommissioned after or at this timestamp	false	string
			decommissionedAt__lt	Agents decommissioned before this timestamp	false	string
			decommissionedAt__lte	Agents decommissioned before this timestamp	false	string
			domains	Included network domains	false	string []
			domainsNin	Not included network domains	false	string []
			encryptedApplications	Disk encryption status	false	boolean
			externalId__contains	Free-text filter by external ID (Customer ID)	false	string []
			externalIp__contains	Free-text filter by visible IP (supports	false	string []

				multiple values)		
			filteredGroupIds	List of Group IDs to filter by	false	string []
			filteredSiteIds	List of Site IDs to filter by	false	string []
			filterId	Include all Agents matching this saved filter	false	string
			firewallEnabled	The agents supports Firewall Control and it is enabled for the agent's group	false	boolean []
			gatewayIp	Gateway ip	false	string
			gcpServiceAccount__contains	Free-text filter by gcp service account (supports multiple values)	false	string []
			groupIds	List of Group IDs to filter by	false	string []
			hasContainerizedWorkload	Include only Agents protecting containerized workloads	false	boolean
			hasLocalConfiguration	Agent has a local configuration set	false	boolean
			hasTags	Include only Agents that	false	boolean

				have any tags assigned if True, or none if False		
			ids	A list of Agent IDs	false	string []
			infected	Include only Agents with at least one active threat	false	boolean
			installerTypes	Include only Agents installed with these package types	false	string []
			installerTypesNin	Exclude Agents installed with these package types	false	string []
			isActive	Include only active Agents	false	boolean
			isDecommissioned	Include active, decommissioned or both	false	boolean []
			isPendingUninstall	Include only Agents with pending uninstall requests	false	boolean
			isUninstalled	Include installed, uninstalled or both	false	boolean []
			isUpToDate	Include only Agents with updated software	false	boolean

			k8sNodeLabels__contains	Free-text filter by K8s node labels (supports multiple values)	false	string []
			k8sNodeName__contains	Free-text filter by K8s node name (supports multiple values)	false	string []
			k8sType__contains	Free-text filter by K8s type(supports multiple values)	false	string []
			k8sVersion__contains	Free-text filter by K8s version (supports multiple values)	false	string []
			lastActiveDate__between	Date range for last active date(format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			lastActiveDate__gt	Agents last active after this time	false	string
			lastActiveDate__gte	Agents last active after or at this time	false	string
			lastActiveDate__lt	Agents last active before this time	false	string
			lastActiveDate__lte	Agents last active before or at this time	false	string

			lastLoggedInUserName__contains	Free-text filter by username (supports multiple values)	false	string []
			lastSuccessfulScanDate__between	Date range for last successful full disk scan(format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			lastSuccessfulScanDate__gt	Agents last successful full disk scan after this time	false	string
			lastSuccessfulScanDate__gte	Agents last successful full disk scan after or at this time	false	string
			lastSuccessfulScanDate__lt	Agents last successful full disk scan before this time	false	string
			lastSuccessfulScanDate__lte	Agents last successful full disk scan before or at this time	false	string
			liveUpdateId__contains	Free-text filter by live update ID (supports multiple values)	false	string []
			locationEnabled	The agents supports	false	boolean []

				Location Awareness and it is enabled for the agent's group		
			locationIds	Include only Agents reporting these locations	false	string []
			locationIdsNin	Do not include only Agents reporting these locations	false	string []
			machineTypes	Included machine types	false	string []
			machineTypesNin	Not included machine types	false	string []
			migrationStatus	Migration status	false	enum
			missingPermissions	Included missing permissions	false	string []
			missingPermissionsNin	Excluded missing permissions	false	string []
			mitigationMode	Agent mitigation mode policy	false	enum
			mitigationModeSuspicious	Mitigation mode policy for suspicious activity	false	enum
			networkInterfaceGatewayMacAddress__c	Free-text filter by Gateway	false	string []

			ontains	MAC address (supports multiple values)		
			networkInterfaceInet__contains	Free-text filter by local IP (supports multiple values)	false	string []
			networkInterfacePhysical__contains	Free-text filter by MAC address (supports multiple values)	false	string []
			networkQuarantineEnabled	The agents supports Network Quarantine Control and its enabled for the agent's group	false	boolean []
			networkStatuses	Included network statuses	false	string []
			networkStatusesNin	Included network statuses	false	string []
			operationalStates	Agent operational state	false	string []
			operationalStatesNin	Do not include these Agent operational states	false	string []
			osArch	OS architecture	false	enum
			osTypes	Included OS types	false	string []

			osTypesNin	Not included OS types	false	string []
			osVersion__contains	Free-text filter by OS full name and version (supports multiple values)	false	string []
			query	A free-text search term, will match applicable attributes (sub-string match). Note: Device's physical addresses will be matched if they start with the search term only (no match if they contain the term).	false	string
			rangerStatus	[DEPRECATED] Use rangerStatuses.	false	enum
			rangerStatuses	Status of Ranger	false	string []
			rangerStatusesNin	Do not include these Ranger Statuses	false	string []
			rangerVersions	Ranger versions to include	false	string []
			rangerVersionsNin	Ranger versions not to include	false	string []

			registeredAt__between	Date range for first registration time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			registeredAt__gt	Agents registered after this time	false	string
			registeredAt__gte	Agents registered after or at this time	false	string
			registeredAt__lt	Agents registered before this time	false	string
			registeredAt__lte	Agents registered before or at this time	false	string
			remoteOpsForensicsSupported	Include only agents that has Remote Ops Forensicsfeature supported	false	boolean
			remoteProfilingStates	Agent remote profiling state	false	string []
			remoteProfilingStatesNin	Do not include these Agent remote profiling states	false	string []
			rsoLevel	Supported Remote Script Orchestration	false	enum

				level		
			scanStatus	Scan status	false	enum
			scanStatuses	Included scan statuses	false	string []
			scanStatuses Nin	Not included scan statuses	false	string []
			serialNumber __contains	Free-text filter by Serial Number (supports multiple values)	false	string []
			siteIds	List of Site IDs to filter by	false	string []
			tagsData	Filter agents by their assigned tags. Given in form of a JSON where each key represents a tag key, and each value represents a list of string values to filter by. To filter by unassigned tag values, use __nin suffix in the tag key.	false	string
			threatConten tHash	Include only Agents that have at least one threat with this content hash	false	string
			threatCreate	Agents with	false	string

			dAt__between	threats reported in a date range (format: <from_timestamp>-<to_timestamp>, inclusive)		
			threatCreatedAt__gt	Agents with threats reported after this time	false	string
			threatCreatedAt__gte	Agents with threats reported after or at this time	false	string
			threatCreatedAt__lt	Agents with threats reported before this time	false	string
			threatCreatedAt__lte	Agents with threats reported before or at this time	false	string
			threatHidden	Include only Agents with at least one hidden threat	false	boolean
			threatMitigationStatus	Include only Agents that have threats with this mitigation status	false	enum
			threatRebootRequired	Has at least one threat with at least one mitigation	false	boolean []

				action pending reboot to succeed		
			threatResolved	Include only Agents with at least one resolved threat	false	boolean
			totalMemory__between	Total memory range (GB, inclusive)	false	string
			totalMemory__gt	Memory size (MB, more than)	false	integer
			totalMemory__gte	Memory size (MB, more than or equal)	false	integer
			totalMemory__lt	Memory size (MB, less than)	false	integer
			totalMemory__lte	Memory size (MB, less than or equal)	false	integer
			updatedAt__between	Date range for update time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			updatedAt__gt	Agents updated after this timestamp	false	string
			updatedAt__gte	Agents updated after or at this timestamp	false	string
			updatedAt__lt	Agents updated	false	string

<table>
<tr><td></td><td></td><td></td><td>
<table>
<tr><td></td><td>before this timestamp</td><td></td><td></td></tr>
<tr><td>updatedAt__lte</td><td>Agents updated before or at this timestamp</td><td>false</td><td>string</td></tr>
<tr><td>userActionsNeeded</td><td>Included pending user actions</td><td>false</td><td>string []</td></tr>
<tr><td>userActionsNeededNin</td><td>Excluded pending user actions</td><td>false</td><td>string []</td></tr>
<tr><td>uuid</td><td>Agent's universally unique identifier</td><td>false</td><td>string</td></tr>
<tr><td>uuid__contains</td><td>Free-text filter by Agent UUID (supports multiple values)</td><td>false</td><td>string []</td></tr>
<tr><td>uuids</td><td>A list of included UUIDs</td><td>false</td><td>string []</td></tr>
</table>
</td></tr>
<tr><td>data</td><td>Data</td><td>false</td><td></td></tr>
</table>

Fetch Logs

POST /web/api/v2.1/agents/actions/fetch-logs

Get the Agent and Endpoint logs from Agents that match the filter.
The Agent logs are encrypted and only Support can read them.
The Endpoint logs, for operations on the computers, laptops, or servers that have the Agent installed, are readable. The Endpoint logs are available for Windows endpoints only and require Agent version 3.6 or later. After you run this command, download the fetched logs. You can download the logs from the Console GUI or collect them.
On Windows: C:\ProgramData\Sentinel\logs.
On macOS: Run sudo sentinelctl logreport and get the log files on the desktop.
On Linux: Run sudo /opt/sentinelone/bin/sentinelctl log generate.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - User has insufficient permissions to perform the requested action

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>affected</td><td>Number of entities affected by the requested operation</td><td>false</td><td>integer</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

Name	Description	Required	Value
filter	Applied filter - only matched Agents will be affected by the requested action. Leave empty to apply the action on all applicable Agents.	true	

Name	Description	Required	Value
accountIds	List of Account IDs to filter by	false	string []
activeThreats	Include Agents with this amount of active threats	false	integer
activeThreats__gt	Include Agents with at least this amount of active threats	false	integer
adComputerMember__contains	Free-text filter by Active Directory computer groups string (supports multiple values)	false	string []
adComputerName__contains	Free-text filter by Active Directory computer name string (supports multiple values)	false	string []
adComputerQuery__contains	Free-text filter by Active Directory computer name or its groups	false	string []

				(supports multiple values)		
			adQuery	An Active Directory query string	false	string
			adQuery__contains	Free-text filter by Active Directory string (supports multiple values)	false	string []
			adUserMember__contains	Free-text filter by Active Directory user groups string (supports multiple values)	false	string []
			adUserName__contains	Free-text filter by Active Directory username string (supports multiple values)	false	string []
			adUserQuery__contains	Free-text filter by Active Directory computer name or its groups (supports multiple values)	false	string []
			agentNamespa	Free-text	false	string []

			ce__contains	filter by agent namespace (supports multiple values)		
			agentPodName__contains	Free-text filter by agent pod name (supports multiple values)	false	string []
			agentVersion__between	Version range for agent version (format: <from_version>-<to_version>, inclusive)	false	string
			agentVersion__gt	Agents versions greater than given version	false	string
			agentVersion__gte	Agents versions greater than or equal to given version	false	string
			agentVersion__lt	Agents versions less than given version	false	string
			agentVersion__lte	Agents versions less than or equal to given version	false	string
			agentVersions	Agent versions to include	false	string []
			agentVersionsNin	Agent versions not	false	string []

				to include		
			appsVulnerabilityStatuses	Apps vulnerability status in	false	string []
			appsVulnerabilityStatusesNin	Apps vulnerability status nin	false	string []
			awsRole__contains	Free-text filter by aws role(supports multiple values)	false	string []
			awsSecurityGroups__contains	Free-text filter by aws securityGroups(supports multiple values)	false	string []
			awsSubnetIds__contains	Free-text filter by aws subnet ids (supports multiple values)	false	string []
			azureResourceGroup__contains	Free-text filter by azure resource group(supports multiple values)	false	string []
			cloudAccount__contains	Free-text filter by cloud account (supports multiple values)	false	string []
			cloudImage__contains	Free-text filter by cloud image (supports multiple values)	false	string []

			cloudInstanceId__contains	Free-text filter by cloud instance id(supports multiple values)	false	string []
			cloudInstanceSize__contains	Free-text filter by cloud instance size(supports multiple values)	false	string []
			cloudLocation__contains	Free-text filter by cloud location (supports multiple values)	false	string []
			cloudNetwork__contains	Free-text filter by cloud network (supports multiple values)	false	string []
			cloudProvider	Agents from which cloud provider	false	string []
			cloudProviderNin	Exclude Agents from these cloud provider	false	string []
			cloudTags__contains	Free-text filter by cloud tags (supports multiple values)	false	string []
			clusterName__contains	Free-text filter by cluster name (supports multiple values)	false	string []

			computerName	Computer name	false	string
			computerName__contains	Free-text filter by computer name (supports multiple values)	false	string []
			computerName__like	Match computer name partially (substring)	false	string
			consoleMigrationStatuses	Migration status in	false	string []
			consoleMigrationStatusesNin	Migration status nin	false	string []
			coreCount__between	Possible number of CPU cores (inclusive)	false	string
			coreCount__gt	CPU cores (more than)	false	integer
			coreCount__gte	CPU cores (more than or equal)	false	integer
			coreCount__lt	CPU cores (less than)	false	integer
			coreCount__lte	CPU cores (less than or equal)	false	integer
			cpuCount__between	Possible number of CPU cores (inclusive)	false	string
			cpuCount__gt	Number of CPUs (more than)	false	integer

			cpuCount__gte	Number of CPUs (more than or equal)	false	integer
			cpuCount__lt	Number of CPUs (less than)	false	integer
			cpuCount__lte	Number of CPUs (less than or equal)	false	integer
			cpuId__contains	Free-text filter by CPU name (supports multiple values)	false	string []
			createdAt__between	Date range for creation time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			createdAt__gt	Agents created after this timestamp	false	string
			createdAt__gte	Agents created after or at this timestamp	false	string
			createdAt__lt	Agents created before this timestamp	false	string
			createdAt__lte	Agents created before or at this timestamp	false	string
			csvFilterId	The ID of the CSV file to filter by	false	string

			decommissionedAt__between	Date range for decommission time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			decommissionedAt__gt	Agents decommissioned after this timestamp	false	string
			decommissionedAt__gte	Agents decommissioned after or at this timestamp	false	string
			decommissionedAt__lt	Agents decommissioned before this timestamp	false	string
			decommissionedAt__lte	Agents decommissioned before this timestamp	false	string
			domains	Included network domains	false	string []
			domainsNin	Not included network domains	false	string []
			encryptedApplications	Disk encryption status	false	boolean
			externalId__contains	Free-text filter by external ID (Customer ID)	false	string []
			externalIp__contains	Free-text filter by visible IP (supports	false	string []

				multiple values)		
			filteredGroupIds	List of Group IDs to filter by	false	string []
			filteredSiteIds	List of Site IDs to filter by	false	string []
			filterId	Include all Agents matching this saved filter	false	string
			firewallEnabled	The agents supports Firewall Control and it is enabled for the agent's group	false	boolean []
			gatewayIp	Gateway ip	false	string
			gcpServiceAccount__contains	Free-text filter by gcp service account (supports multiple values)	false	string []
			groupIds	List of Group IDs to filter by	false	string []
			hasContainerizedWorkload	Include only Agents protecting containerized workloads	false	boolean
			hasLocalConfiguration	Agent has a local configuration set	false	boolean
			hasTags	Include only Agents that	false	boolean

				have any tags assigned if True, or none if False		
			ids	A list of Agent IDs	false	string []
			infected	Include only Agents with at least one active threat	false	boolean
			installerTypes	Include only Agents installed with these package types	false	string []
			installerTypesNin	Exclude Agents installed with these package types	false	string []
			isActive	Include only active Agents	false	boolean
			isDecommissioned	Include active, decommissioned or both	false	boolean []
			isPendingUninstall	Include only Agents with pending uninstall requests	false	boolean
			isUninstalled	Include installed, uninstalled or both	false	boolean []
			isUpToDate	Include only Agents with updated software	false	boolean

			k8sNodeLabels__contains	Free-text filter by K8s node labels (supports multiple values)	false	string []
			k8sNodeName__contains	Free-text filter by K8s node name (supports multiple values)	false	string []
			k8sType__contains	Free-text filter by K8s type(supports multiple values)	false	string []
			k8sVersion__contains	Free-text filter by K8s version (supports multiple values)	false	string []
			lastActiveDate__between	Date range for last active date(format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			lastActiveDate__gt	Agents last active after this time	false	string
			lastActiveDate__gte	Agents last active after or at this time	false	string
			lastActiveDate__lt	Agents last active before this time	false	string
			lastActiveDate__lte	Agents last active before or at this time	false	string

			lastLoggedInUserName__contains	Free-text filter by username (supports multiple values)	false	string []
			lastSuccessfulScanDate__between	Date range for last successful full disk scan(format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			lastSuccessfulScanDate__gt	Agents last successful full disk scan after this time	false	string
			lastSuccessfulScanDate__gte	Agents last successful full disk scan after or at this time	false	string
			lastSuccessfulScanDate__lt	Agents last successful full disk scan before this time	false	string
			lastSuccessfulScanDate__lte	Agents last successful full disk scan before or at this time	false	string
			liveUpdateId__contains	Free-text filter by live update ID (supports multiple values)	false	string []
			locationEnabled	The agents supports	false	boolean []

				Location Awareness and it is enabled for the agent's group		
			locationIds	Include only Agents reporting these locations	false	string []
			locationIdsNin	Do not include only Agents reporting these locations	false	string []
			machineTypes	Included machine types	false	string []
			machineTypesNin	Not included machine types	false	string []
			migrationStatus	Migration status	false	enum
			missingPermissions	Included missing permissions	false	string []
			missingPermissionsNin	Excluded missing permissions	false	string []
			mitigationMode	Agent mitigation mode policy	false	enum
			mitigationModeSuspicious	Mitigation mode policy for suspicious activity	false	enum
			networkInterfaceGatewayMacAddress__c	Free-text filter by Gateway	false	string []

			ontains	MAC address (supports multiple values)		
			networkInterfaceInet__contains	Free-text filter by local IP (supports multiple values)	false	string []
			networkInterfacePhysical__contains	Free-text filter by MAC address (supports multiple values)	false	string []
			networkQuarantineEnabled	The agents supports Network Quarantine Control and its enabled for the agent's group	false	boolean []
			networkStatuses	Included network statuses	false	string []
			networkStatusesNin	Included network statuses	false	string []
			operationalStates	Agent operational state	false	string []
			operationalStatesNin	Do not include these Agent operational states	false	string []
			osArch	OS architecture	false	enum
			osTypes	Included OS types	false	string []

			osTypesNin	Not included OS types	false	string []
			osVersion__contains	Free-text filter by OS full name and version (supports multiple values)	false	string []
			query	A free-text search term, will match applicable attributes (sub-string match). Note: Device's physical addresses will be matched if they start with the search term only (no match if they contain the term).	false	string
			rangerStatus	[DEPRECATED] Use rangerStatuses.	false	enum
			rangerStatuses	Status of Ranger	false	string []
			rangerStatusesNin	Do not include these Ranger Statuses	false	string []
			rangerVersions	Ranger versions to include	false	string []
			rangerVersionsNin	Ranger versions not to include	false	string []

			registeredAt__between	Date range for first registration time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			registeredAt__gt	Agents registered after this time	false	string
			registeredAt__gte	Agents registered after or at this time	false	string
			registeredAt__lt	Agents registered before this time	false	string
			registeredAt__lte	Agents registered before or at this time	false	string
			remoteOpsForensicsSupported	Include only agents that has Remote Ops Forensicsfeature supported	false	boolean
			remoteProfilingStates	Agent remote profiling state	false	string []
			remoteProfilingStatesNin	Do not include these Agent remote profiling states	false	string []
			rsoLevel	Supported Remote Script Orchestration	false	enum

				level		
			scanStatus	Scan status	false	enum
			scanStatuses	Included scan statuses	false	string []
			scanStatuses Nin	Not included scan statuses	false	string []
			serialNumber __contains	Free-text filter by Serial Number (supports multiple values)	false	string []
			siteIds	List of Site IDs to filter by	false	string []
			tagsData	Filter agents by their assigned tags. Given in form of a JSON where each key represents a tag key, and each value represents a list of string values to filter by. To filter by unassigned tag values, use __nin suffix in the tag key.	false	string
			threatConten tHash	Include only Agents that have at least one threat with this content hash	false	string
			threatCreate	Agents with	false	string

			dAt__between	threats reported in a date range (format: <from_timestamp>-<to_timestamp>, inclusive)		
			threatCreatedAt__gt	Agents with threats reported after this time	false	string
			threatCreatedAt__gte	Agents with threats reported after or at this time	false	string
			threatCreatedAt__lt	Agents with threats reported before this time	false	string
			threatCreatedAt__lte	Agents with threats reported before or at this time	false	string
			threatHidden	Include only Agents with at least one hidden threat	false	boolean
			threatMitigationStatus	Include only Agents that have threats with this mitigation status	false	enum
			threatRebootRequired	Has at least one threat with at least one mitigation	false	boolean []

				action pending reboot to succeed		
			threatResolved	Include only Agents with at least one resolved threat	false	boolean
			totalMemory__between	Total memory range (GB, inclusive)	false	string
			totalMemory__gt	Memory size (MB, more than)	false	integer
			totalMemory__gte	Memory size (MB, more than or equal)	false	integer
			totalMemory__lt	Memory size (MB, less than)	false	integer
			totalMemory__lte	Memory size (MB, less than or equal)	false	integer
			updatedAt__between	Date range for update time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			updatedAt__gt	Agents updated after this timestamp	false	string
			updatedAt__gte	Agents updated after or at this timestamp	false	string
			updatedAt__lt	Agents updated	false	string

			before this timestamp		
			updatedAt__lte	Agents updated before or at this timestamp	false	string
			userActionsNeeded	Included pending user actions	false	string []
			userActionsNeededNin	Excluded pending user actions	false	string []
			uuid	Agent's universally unique identifier	false	string
			uuid__contains	Free-text filter by Agent UUID (supports multiple values)	false	string []
			uuids	A list of included UUIDs	false	string []
data	Data	false	Name	Description	Required	Value
			agentLogs	Fetch Agent logs	false	boolean
			customerFacingLogs	Fetch customer-facing logs	false	boolean
			platformLogs	Actively fetch logs from the relevant platform: windows/	false	boolean

				mac/linux		

Initiate Scan

POST /web/api/v2.1/agents/actions/initiate-scan

Use this command to run a Full Disk Scan on Agents that match the filter.
Full Disk Scan finds dormant suspicious activity, threats, and compliance violations, that are then mitigated according to the policy. It scans the local file system.
Full Disk Scan does not inspect drives that require user credentials (such as network drives) or external drives.
Full Disk Scan does not work on hashes. It does not check each file against the blocklist.
If the Static AI determines a file is suspicious, the Agent calculates its hash and sees if the hash is in the blocklist. If a file is executed, all aspects of the process are inspected, including hash-based analysis and blocklist checks. Full Disk Scan can run when the endpoint is offline, but when it is connected to the Management, it can use the most updated Cloud data to improve detection.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - User has insufficient permissions to perform the requested action

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>affected</td><td>Number of entities affected by the requested operation</td><td>false</td><td>integer</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>filter</td><td>Applied filter - only matched Agents will be affected by the requested action. Leave empty to apply the action on all applicable Agents.</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>activeThreats</td><td>Include Agents with this amount of active threats</td><td>false</td><td>integer</td></tr>
<tr><td>activeThreats__gt</td><td>Include Agents with at least this amount of active threats</td><td>false</td><td>integer</td></tr>
<tr><td>adComputerMember__contains</td><td>Free-text filter by Active Directory computer groups string (supports multiple values)</td><td>false</td><td>string []</td></tr>
<tr><td>adComputerName__contains</td><td>Free-text filter by Active Directory computer name string (supports multiple values)</td><td>false</td><td>string []</td></tr>
<tr><td>adComputerQuery__contains</td><td>Free-text filter by Active Directory computer name or its groups</td><td>false</td><td>string []</td></tr>
</table>
</td></tr>
</table>

				(supports multiple values)		
			adQuery	An Active Directory query string	false	string
			adQuery__contains	Free-text filter by Active Directory string (supports multiple values)	false	string []
			adUserMember__contains	Free-text filter by Active Directory user groups string (supports multiple values)	false	string []
			adUserName__contains	Free-text filter by Active Directory username string (supports multiple values)	false	string []
			adUserQuery__contains	Free-text filter by Active Directory computer name or its groups (supports multiple values)	false	string []
			agentNamespa	Free-text	false	string []

			ce__contains	filter by agent namespace (supports multiple values)		
			agentPodName__contains	Free-text filter by agent pod name (supports multiple values)	false	string []
			agentVersion__between	Version range for agent version (format: <from_version>-<to_version>, inclusive)	false	string
			agentVersion__gt	Agents versions greater than given version	false	string
			agentVersion__gte	Agents versions greater than or equal to given version	false	string
			agentVersion__lt	Agents versions less than given version	false	string
			agentVersion__lte	Agents versions less than or equal to given version	false	string
			agentVersions	Agent versions to include	false	string []
			agentVersionsNin	Agent versions not	false	string []

				to include		
			appsVulnerabilityStatuses	Apps vulnerability status in	false	string []
			appsVulnerabilityStatusesNin	Apps vulnerability status nin	false	string []
			awsRole__contains	Free-text filter by aws role(supports multiple values)	false	string []
			awsSecurityGroups__contains	Free-text filter by aws securityGroups(supports multiple values)	false	string []
			awsSubnetIds__contains	Free-text filter by aws subnet ids (supports multiple values)	false	string []
			azureResourceGroup__contains	Free-text filter by azure resource group(supports multiple values)	false	string []
			cloudAccount__contains	Free-text filter by cloud account (supports multiple values)	false	string []
			cloudImage__contains	Free-text filter by cloud image (supports multiple values)	false	string []

			cloudInstanceId__contains	Free-text filter by cloud instance id(supports multiple values)	false	string []
			cloudInstanceSize__contains	Free-text filter by cloud instance size(supports multiple values)	false	string []
			cloudLocation__contains	Free-text filter by cloud location (supports multiple values)	false	string []
			cloudNetwork__contains	Free-text filter by cloud network (supports multiple values)	false	string []
			cloudProvider	Agents from which cloud provider	false	string []
			cloudProviderNin	Exclude Agents from these cloud provider	false	string []
			cloudTags__contains	Free-text filter by cloud tags (supports multiple values)	false	string []
			clusterName__contains	Free-text filter by cluster name (supports multiple values)	false	string []

			computerName	Computer name	false	string
			computerName__contains	Free-text filter by computer name (supports multiple values)	false	string []
			computerName__like	Match computer name partially (substring)	false	string
			consoleMigrationStatuses	Migration status in	false	string []
			consoleMigrationStatusesNin	Migration status nin	false	string []
			coreCount__between	Possible number of CPU cores (inclusive)	false	string
			coreCount__gt	CPU cores (more than)	false	integer
			coreCount__gte	CPU cores (more than or equal)	false	integer
			coreCount__lt	CPU cores (less than)	false	integer
			coreCount__lte	CPU cores (less than or equal)	false	integer
			cpuCount__between	Possible number of CPU cores (inclusive)	false	string
			cpuCount__gt	Number of CPUs (more than)	false	integer

			cpuCount__gte	Number of CPUs (more than or equal)	false	integer
			cpuCount__lt	Number of CPUs (less than)	false	integer
			cpuCount__lte	Number of CPUs (less than or equal)	false	integer
			cpuId__contains	Free-text filter by CPU name (supports multiple values)	false	string []
			createdAt__between	Date range for creation time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			createdAt__gt	Agents created after this timestamp	false	string
			createdAt__gte	Agents created after or at this timestamp	false	string
			createdAt__lt	Agents created before this timestamp	false	string
			createdAt__lte	Agents created before or at this timestamp	false	string
			csvFilterId	The ID of the CSV file to filter by	false	string

			decommissionedAt__between	Date range for decommission time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			decommissionedAt__gt	Agents decommissioned after this timestamp	false	string
			decommissionedAt__gte	Agents decommissioned after or at this timestamp	false	string
			decommissionedAt__lt	Agents decommissioned before this timestamp	false	string
			decommissionedAt__lte	Agents decommissioned before this timestamp	false	string
			domains	Included network domains	false	string []
			domainsNin	Not included network domains	false	string []
			encryptedApplications	Disk encryption status	false	boolean
			externalId__contains	Free-text filter by external ID (Customer ID)	false	string []
			externalIp__contains	Free-text filter by visible IP (supports	false	string []

				multiple values)		
			filteredGroupIds	List of Group IDs to filter by	false	string []
			filteredSiteIds	List of Site IDs to filter by	false	string []
			filterId	Include all Agents matching this saved filter	false	string
			firewallEnabled	The agents supports Firewall Control and it is enabled for the agent's group	false	boolean []
			gatewayIp	Gateway ip	false	string
			gcpServiceAccount__contains	Free-text filter by gcp service account (supports multiple values)	false	string []
			groupIds	List of Group IDs to filter by	false	string []
			hasContainerizedWorkload	Include only Agents protecting containerized workloads	false	boolean
			hasLocalConfiguration	Agent has a local configuration set	false	boolean
			hasTags	Include only Agents that	false	boolean

				have any tags assigned if True, or none if False		
			ids	A list of Agent IDs	false	string []
			infected	Include only Agents with at least one active threat	false	boolean
			installerTypes	Include only Agents installed with these package types	false	string []
			installerTypesNin	Exclude Agents installed with these package types	false	string []
			isActive	Include only active Agents	false	boolean
			isDecommissioned	Include active, decommissioned or both	false	boolean []
			isPendingUninstall	Include only Agents with pending uninstall requests	false	boolean
			isUninstalled	Include installed, uninstalled or both	false	boolean []
			isUpToDate	Include only Agents with updated software	false	boolean

			k8sNodeLabels__contains	Free-text filter by K8s node labels (supports multiple values)	false	string []
			k8sNodeName__contains	Free-text filter by K8s node name (supports multiple values)	false	string []
			k8sType__contains	Free-text filter by K8s type(supports multiple values)	false	string []
			k8sVersion__contains	Free-text filter by K8s version (supports multiple values)	false	string []
			lastActiveDate__between	Date range for last active date(format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			lastActiveDate__gt	Agents last active after this time	false	string
			lastActiveDate__gte	Agents last active after or at this time	false	string
			lastActiveDate__lt	Agents last active before this time	false	string
			lastActiveDate__lte	Agents last active before or at this time	false	string

			lastLoggedInUserName__contains	Free-text filter by username (supports multiple values)	false	string []
			lastSuccessfulScanDate__between	Date range for last successful full disk scan(format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			lastSuccessfulScanDate__gt	Agents last successful full disk scan after this time	false	string
			lastSuccessfulScanDate__gte	Agents last successful full disk scan after or at this time	false	string
			lastSuccessfulScanDate__lt	Agents last successful full disk scan before this time	false	string
			lastSuccessfulScanDate__lte	Agents last successful full disk scan before or at this time	false	string
			liveUpdateId__contains	Free-text filter by live update ID (supports multiple values)	false	string []
			locationEnabled	The agents supports	false	boolean []

				Location Awareness and it is enabled for the agent's group		
			locationIds	Include only Agents reporting these locations	false	string []
			locationIdsNin	Do not include only Agents reporting these locations	false	string []
			machineTypes	Included machine types	false	string []
			machineTypesNin	Not included machine types	false	string []
			migrationStatus	Migration status	false	enum
			missingPermissions	Included missing permissions	false	string []
			missingPermissionsNin	Excluded missing permissions	false	string []
			mitigationMode	Agent mitigation mode policy	false	enum
			mitigationModeSuspicious	Mitigation mode policy for suspicious activity	false	enum
			networkInterfaceGatewayMacAddress__c	Free-text filter by Gateway	false	string []

			ontains	MAC address (supports multiple values)		
			networkInterfaceInet__contains	Free-text filter by local IP (supports multiple values)	false	string []
			networkInterfacePhysical__contains	Free-text filter by MAC address (supports multiple values)	false	string []
			networkQuarantineEnabled	The agents supports Network Quarantine Control and its enabled for the agent's group	false	boolean []
			networkStatuses	Included network statuses	false	string []
			networkStatusesNin	Included network statuses	false	string []
			operationalStates	Agent operational state	false	string []
			operationalStatesNin	Do not include these Agent operational states	false	string []
			osArch	OS architecture	false	enum
			osTypes	Included OS types	false	string []

			osTypesNin	Not included OS types	false	string []
			osVersion__contains	Free-text filter by OS full name and version (supports multiple values)	false	string []
			query	A free-text search term, will match applicable attributes (sub-string match). Note: Device's physical addresses will be matched if they start with the search term only (no match if they contain the term).	false	string
			rangerStatus	[DEPRECATED] Use rangerStatuses.	false	enum
			rangerStatuses	Status of Ranger	false	string []
			rangerStatusesNin	Do not include these Ranger Statuses	false	string []
			rangerVersions	Ranger versions to include	false	string []
			rangerVersionsNin	Ranger versions not to include	false	string []

			registeredAt__between	Date range for first registration time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			registeredAt__gt	Agents registered after this time	false	string
			registeredAt__gte	Agents registered after or at this time	false	string
			registeredAt__lt	Agents registered before this time	false	string
			registeredAt__lte	Agents registered before or at this time	false	string
			remoteOpsForensicsSupported	Include only agents that has Remote Ops Forensicsfeature supported	false	boolean
			remoteProfilingStates	Agent remote profiling state	false	string []
			remoteProfilingStatesNin	Do not include these Agent remote profiling states	false	string []
			rsoLevel	Supported Remote Script Orchestration	false	enum

				level		
			scanStatus	Scan status	false	enum
			scanStatuses	Included scan statuses	false	string []
			scanStatuses Nin	Not included scan statuses	false	string []
			serialNumber __contains	Free-text filter by Serial Number (supports multiple values)	false	string []
			siteIds	List of Site IDs to filter by	false	string []
			tagsData	Filter agents by their assigned tags. Given in form of a JSON where each key represents a tag key, and each value represents a list of string values to filter by. To filter by unassigned tag values, use __nin suffix in the tag key.	false	string
			threatConten tHash	Include only Agents that have at least one threat with this content hash	false	string
			threatCreate	Agents with	false	string

			dAt__between	threats reported in a date range (format: <from_timestamp>-<to_timestamp>, inclusive)		
			threatCreatedAt__gt	Agents with threats reported after this time	false	string
			threatCreatedAt__gte	Agents with threats reported after or at this time	false	string
			threatCreatedAt__lt	Agents with threats reported before this time	false	string
			threatCreatedAt__lte	Agents with threats reported before or at this time	false	string
			threatHidden	Include only Agents with at least one hidden threat	false	boolean
			threatMitigationStatus	Include only Agents that have threats with this mitigation status	false	enum
			threatRebootRequired	Has at least one threat with at least one mitigation	false	boolean []

				action pending reboot to succeed		
			threatResolved	Include only Agents with at least one resolved threat	false	boolean
			totalMemory__between	Total memory range (GB, inclusive)	false	string
			totalMemory__gt	Memory size (MB, more than)	false	integer
			totalMemory__gte	Memory size (MB, more than or equal)	false	integer
			totalMemory__lt	Memory size (MB, less than)	false	integer
			totalMemory__lte	Memory size (MB, less than or equal)	false	integer
			updatedAt__between	Date range for update time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			updatedAt__gt	Agents updated after this timestamp	false	string
			updatedAt__gte	Agents updated after or at this timestamp	false	string
			updatedAt__lt	Agents updated	false	string

			before this timestamp		
	updatedAt__lte	Agents updated before or at this timestamp	false	string
	userActionsNeeded	Included pending user actions	false	string []
	userActionsNeededNin	Excluded pending user actions	false	string []
	uuid	Agent's universally unique identifier	false	string
	uuid__contains	Free-text filter by Agent UUID (supports multiple values)	false	string []
	uuids	A list of included UUIDs	false	string []
data	Data	false	

Abort Scan

POST /web/api/v2.1/agents/actions/abort-scan

Immediately stop a Full Disk Scan on all Agents that match the filter. See "Initiate scan" to learn more about Full Disk Scan.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - User has insufficient permissions to perform the requested action

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>affected</td><td>Number of entities affected by the requested operation</td><td>false</td><td>integer</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

Name	Description	Required	Value
filter	Applied filter - only matched Agents will be affected by the requested action. Leave empty to apply the action on all applicable Agents.	true	

Name	Description	Required	Value
accountIds	List of Account IDs to filter by	false	string []
activeThreats	Include Agents with this amount of active threats	false	integer
activeThreats__gt	Include Agents with at least this amount of active threats	false	integer
adComputerMember__contains	Free-text filter by Active Directory computer groups string (supports multiple values)	false	string []
adComputerName__contains	Free-text filter by Active Directory computer name string (supports multiple values)	false	string []
adComputerQuery__contains	Free-text filter by Active Directory computer name or its groups	false	string []

				(supports multiple values)		
			adQuery	An Active Directory query string	false	string
			adQuery__contains	Free-text filter by Active Directory string (supports multiple values)	false	string []
			adUserMember__contains	Free-text filter by Active Directory user groups string (supports multiple values)	false	string []
			adUserName__contains	Free-text filter by Active Directory username string (supports multiple values)	false	string []
			adUserQuery__contains	Free-text filter by Active Directory computer name or its groups (supports multiple values)	false	string []
			agentNamespa	Free-text	false	string []

			ce__contains	filter by agent namespace (supports multiple values)		
			agentPodName__contains	Free-text filter by agent pod name (supports multiple values)	false	string []
			agentVersion__between	Version range for agent version (format: <from_version>-<to_version>, inclusive)	false	string
			agentVersion__gt	Agents versions greater than given version	false	string
			agentVersion__gte	Agents versions greater than or equal to given version	false	string
			agentVersion__lt	Agents versions less than given version	false	string
			agentVersion__lte	Agents versions less than or equal to given version	false	string
			agentVersions	Agent versions to include	false	string []
			agentVersionsNin	Agent versions not	false	string []

				to include		
			appsVulnerabilityStatuses	Apps vulnerability status in	false	string []
			appsVulnerabilityStatusesNin	Apps vulnerability status nin	false	string []
			awsRole__contains	Free-text filter by aws role(supports multiple values)	false	string []
			awsSecurityGroups__contains	Free-text filter by aws securityGroups(supports multiple values)	false	string []
			awsSubnetIds__contains	Free-text filter by aws subnet ids (supports multiple values)	false	string []
			azureResourceGroup__contains	Free-text filter by azure resource group(supports multiple values)	false	string []
			cloudAccount__contains	Free-text filter by cloud account (supports multiple values)	false	string []
			cloudImage__contains	Free-text filter by cloud image (supports multiple values)	false	string []

			cloudInstanceId__contains	Free-text filter by cloud instance id(supports multiple values)	false	string []
			cloudInstanceSize__contains	Free-text filter by cloud instance size(supports multiple values)	false	string []
			cloudLocation__contains	Free-text filter by cloud location (supports multiple values)	false	string []
			cloudNetwork__contains	Free-text filter by cloud network (supports multiple values)	false	string []
			cloudProvider	Agents from which cloud provider	false	string []
			cloudProviderNin	Exclude Agents from these cloud provider	false	string []
			cloudTags__contains	Free-text filter by cloud tags (supports multiple values)	false	string []
			clusterName__contains	Free-text filter by cluster name (supports multiple values)	false	string []

			computerName	Computer name	false	string
			computerName__contains	Free-text filter by computer name (supports multiple values)	false	string []
			computerName__like	Match computer name partially (substring)	false	string
			consoleMigrationStatuses	Migration status in	false	string []
			consoleMigrationStatusesNin	Migration status nin	false	string []
			coreCount__between	Possible number of CPU cores (inclusive)	false	string
			coreCount__gt	CPU cores (more than)	false	integer
			coreCount__gte	CPU cores (more than or equal)	false	integer
			coreCount__lt	CPU cores (less than)	false	integer
			coreCount__lte	CPU cores (less than or equal)	false	integer
			cpuCount__between	Possible number of CPU cores (inclusive)	false	string
			cpuCount__gt	Number of CPUs (more than)	false	integer

			cpuCount__gte	Number of CPUs (more than or equal)	false	integer
			cpuCount__lt	Number of CPUs (less than)	false	integer
			cpuCount__lte	Number of CPUs (less than or equal)	false	integer
			cpuId__contains	Free-text filter by CPU name (supports multiple values)	false	string []
			createdAt__between	Date range for creation time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			createdAt__gt	Agents created after this timestamp	false	string
			createdAt__gte	Agents created after or at this timestamp	false	string
			createdAt__lt	Agents created before this timestamp	false	string
			createdAt__lte	Agents created before or at this timestamp	false	string
			csvFilterId	The ID of the CSV file to filter by	false	string

			decommissionedAt__between	Date range for decommission time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			decommissionedAt__gt	Agents decommissioned after this timestamp	false	string
			decommissionedAt__gte	Agents decommissioned after or at this timestamp	false	string
			decommissionedAt__lt	Agents decommissioned before this timestamp	false	string
			decommissionedAt__lte	Agents decommissioned before this timestamp	false	string
			domains	Included network domains	false	string []
			domainsNin	Not included network domains	false	string []
			encryptedApplications	Disk encryption status	false	boolean
			externalId__contains	Free-text filter by external ID (Customer ID)	false	string []
			externalIp__contains	Free-text filter by visible IP (supports	false	string []

				multiple values)		
			filteredGroupIds	List of Group IDs to filter by	false	string []
			filteredSiteIds	List of Site IDs to filter by	false	string []
			filterId	Include all Agents matching this saved filter	false	string
			firewallEnabled	The agents supports Firewall Control and it is enabled for the agent's group	false	boolean []
			gatewayIp	Gateway ip	false	string
			gcpServiceAccount__contains	Free-text filter by gcp service account (supports multiple values)	false	string []
			groupIds	List of Group IDs to filter by	false	string []
			hasContainerizedWorkload	Include only Agents protecting containerized workloads	false	boolean
			hasLocalConfiguration	Agent has a local configuration set	false	boolean
			hasTags	Include only Agents that	false	boolean

				have any tags assigned if True, or none if False		
			ids	A list of Agent IDs	false	string []
			infected	Include only Agents with at least one active threat	false	boolean
			installerTypes	Include only Agents installed with these package types	false	string []
			installerTypesNin	Exclude Agents installed with these package types	false	string []
			isActive	Include only active Agents	false	boolean
			isDecommissioned	Include active, decommissioned or both	false	boolean []
			isPendingUninstall	Include only Agents with pending uninstall requests	false	boolean
			isUninstalled	Include installed, uninstalled or both	false	boolean []
			isUpToDate	Include only Agents with updated software	false	boolean

			k8sNodeLabels__contains	Free-text filter by K8s node labels (supports multiple values)	false	string []
			k8sNodeName__contains	Free-text filter by K8s node name (supports multiple values)	false	string []
			k8sType__contains	Free-text filter by K8s type(supports multiple values)	false	string []
			k8sVersion__contains	Free-text filter by K8s version (supports multiple values)	false	string []
			lastActiveDate__between	Date range for last active date(format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			lastActiveDate__gt	Agents last active after this time	false	string
			lastActiveDate__gte	Agents last active after or at this time	false	string
			lastActiveDate__lt	Agents last active before this time	false	string
			lastActiveDate__lte	Agents last active before or at this time	false	string

			lastLoggedInUserName__contains	Free-text filter by username (supports multiple values)	false	string []
			lastSuccessfulScanDate__between	Date range for last successful full disk scan(format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			lastSuccessfulScanDate__gt	Agents last successful full disk scan after this time	false	string
			lastSuccessfulScanDate__gte	Agents last successful full disk scan after or at this time	false	string
			lastSuccessfulScanDate__lt	Agents last successful full disk scan before this time	false	string
			lastSuccessfulScanDate__lte	Agents last successful full disk scan before or at this time	false	string
			liveUpdateId__contains	Free-text filter by live update ID (supports multiple values)	false	string []
			locationEnabled	The agents supports	false	boolean []

				Location Awareness and it is enabled for the agent's group		
			locationIds	Include only Agents reporting these locations	false	string []
			locationIdsNin	Do not include only Agents reporting these locations	false	string []
			machineTypes	Included machine types	false	string []
			machineTypesNin	Not included machine types	false	string []
			migrationStatus	Migration status	false	enum
			missingPermissions	Included missing permissions	false	string []
			missingPermissionsNin	Excluded missing permissions	false	string []
			mitigationMode	Agent mitigation mode policy	false	enum
			mitigationModeSuspicious	Mitigation mode policy for suspicious activity	false	enum
			networkInterfaceGatewayMacAddress__c	Free-text filter by Gateway	false	string []

			ontains	MAC address (supports multiple values)		
			networkInterfaceInet__contains	Free-text filter by local IP (supports multiple values)	false	string []
			networkInterfacePhysical__contains	Free-text filter by MAC address (supports multiple values)	false	string []
			networkQuarantineEnabled	The agents supports Network Quarantine Control and its enabled for the agent's group	false	boolean []
			networkStatuses	Included network statuses	false	string []
			networkStatusesNin	Included network statuses	false	string []
			operationalStates	Agent operational state	false	string []
			operationalStatesNin	Do not include these Agent operational states	false	string []
			osArch	OS architecture	false	enum
			osTypes	Included OS types	false	string []

			osTypesNin	Not included OS types	false	string []
			osVersion__contains	Free-text filter by OS full name and version (supports multiple values)	false	string []
			query	A free-text search term, will match applicable attributes (sub-string match). Note: Device's physical addresses will be matched if they start with the search term only (no match if they contain the term).	false	string
			rangerStatus	[DEPRECATED] Use rangerStatuses.	false	enum
			rangerStatuses	Status of Ranger	false	string []
			rangerStatusesNin	Do not include these Ranger Statuses	false	string []
			rangerVersions	Ranger versions to include	false	string []
			rangerVersionsNin	Ranger versions not to include	false	string []

			registeredAt__between	Date range for first registration time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			registeredAt__gt	Agents registered after this time	false	string
			registeredAt__gte	Agents registered after or at this time	false	string
			registeredAt__lt	Agents registered before this time	false	string
			registeredAt__lte	Agents registered before or at this time	false	string
			remoteOpsForensicsSupported	Include only agents that has Remote Ops Forensicsfeature supported	false	boolean
			remoteProfilingStates	Agent remote profiling state	false	string []
			remoteProfilingStatesNin	Do not include these Agent remote profiling states	false	string []
			rsoLevel	Supported Remote Script Orchestration	false	enum

				level		
			scanStatus	Scan status	false	enum
			scanStatuses	Included scan statuses	false	string []
			scanStatuses Nin	Not included scan statuses	false	string []
			serialNumber __contains	Free-text filter by Serial Number (supports multiple values)	false	string []
			siteIds	List of Site IDs to filter by	false	string []
			tagsData	Filter agents by their assigned tags. Given in form of a JSON where each key represents a tag key, and each value represents a list of string values to filter by. To filter by unassigned tag values, use __nin suffix in the tag key.	false	string
			threatConten tHash	Include only Agents that have at least one threat with this content hash	false	string
			threatCreate	Agents with	false	string

			dAt__between	threats reported in a date range (format: <from_timestamp>-<to_timestamp>, inclusive)		
			threatCreatedAt__gt	Agents with threats reported after this time	false	string
			threatCreatedAt__gte	Agents with threats reported after or at this time	false	string
			threatCreatedAt__lt	Agents with threats reported before this time	false	string
			threatCreatedAt__lte	Agents with threats reported before or at this time	false	string
			threatHidden	Include only Agents with at least one hidden threat	false	boolean
			threatMitigationStatus	Include only Agents that have threats with this mitigation status	false	enum
			threatRebootRequired	Has at least one threat with at least one mitigation	false	boolean []

				action pending reboot to succeed		
			threatResolved	Include only Agents with at least one resolved threat	false	boolean
			totalMemory__between	Total memory range (GB, inclusive)	false	string
			totalMemory__gt	Memory size (MB, more than)	false	integer
			totalMemory__gte	Memory size (MB, more than or equal)	false	integer
			totalMemory__lt	Memory size (MB, less than)	false	integer
			totalMemory__lte	Memory size (MB, less than or equal)	false	integer
			updatedAt__between	Date range for update time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			updatedAt__gt	Agents updated after this timestamp	false	string
			updatedAt__gte	Agents updated after or at this timestamp	false	string
			updatedAt__lt	Agents updated	false	string

<table>
<tr><td></td><td></td><td></td><td><table>
<tr><td></td><td>before this timestamp</td><td></td><td></td></tr>
<tr><td>updatedAt__lte</td><td>Agents updated before or at this timestamp</td><td>false</td><td>string</td></tr>
<tr><td>userActionsNeeded</td><td>Included pending user actions</td><td>false</td><td>string []</td></tr>
<tr><td>userActionsNeededNin</td><td>Excluded pending user actions</td><td>false</td><td>string []</td></tr>
<tr><td>uuid</td><td>Agent's universally unique identifier</td><td>false</td><td>string</td></tr>
<tr><td>uuid__contains</td><td>Free-text filter by Agent UUID (supports multiple values)</td><td>false</td><td>string []</td></tr>
<tr><td>uuids</td><td>A list of included UUIDs</td><td>false</td><td>string []</td></tr>
</table></td></tr>
<tr><td>data</td><td>Data</td><td>false</td><td></td></tr>
</table>

Disconnect from Network

POST /web/api/v2.1/agents/actions/disconnect

Use this command to isolate (quarantine) endpoints from the network, if the endpoints match the filter.
The Agent can communicate with the Management, which lets you analyze and mitigate threats. Best practice: For Active threats that spread, apply "Disconnect from network" immediately. In the policy, you can set this is to be automatic. When the Agent detects a high-confidence malicious threat, it will mitigate the threat (on Protect) with the action set by the policy. Then the Agent will immediately quarantine the endpoint. To make Disconnect from network automatic in an Account policy, run the "accounts/{id} command (see "Update Account") with: "networkQuarantine":true.

BEST PRACTICE

For Active threats that spread, apply "Disconnect from network" immediately. In the policy, you can set this is to be automatic. When the Agent detects a high-confidence malicious threat, it will mitigate the threat (on Protect) with the action set by the policy. Then the Agent will immediately quarantine the endpoint. To make Disconnect from network automatic in an Account policy, run the "accounts/{id} command (see "Update Account") with: "networkQuarantine":true.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - User has insufficient permissions to perform the requested action

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>affected</td><td>Number of entities affected by the requested operation</td><td>false</td><td>integer</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>filter</td><td>Applied filter - only matched Agents will be affected by the requested action. Note: One of these filter arguments must be supplied: ids, groupIds, filterId.</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>activeThreats</td><td>Include Agents with this amount of active threats</td><td>false</td><td>integer</td></tr>
<tr><td>activeThreats__gt</td><td>Include Agents with at least this amount of active threats</td><td>false</td><td>integer</td></tr>
<tr><td>adComputerMember__contains</td><td>Free-text filter by Active Directory computer groups string (supports multiple values)</td><td>false</td><td>string []</td></tr>
<tr><td>adComputerName__contains</td><td>Free-text filter by Active Directory computer name string (supports multiple values)</td><td>false</td><td>string []</td></tr>
<tr><td>adComputerQuery__contains</td><td>Free-text filter by Active Directory computer name or its groups</td><td>false</td><td>string []</td></tr>
</table>
</td></tr>
</table>

				(supports multiple values)		
			adQuery	An Active Directory query string	false	string
			adQuery__contains	Free-text filter by Active Directory string (supports multiple values)	false	string []
			adUserMember__contains	Free-text filter by Active Directory user groups string (supports multiple values)	false	string []
			adUserName__contains	Free-text filter by Active Directory username string (supports multiple values)	false	string []
			adUserQuery__contains	Free-text filter by Active Directory computer name or its groups (supports multiple values)	false	string []
			agentNamespa	Free-text	false	string []

			ce__contains	filter by agent namespace (supports multiple values)		
			agentPodName__contains	Free-text filter by agent pod name (supports multiple values)	false	string []
			agentVersion__between	Version range for agent version (format: <from_version>-<to_version>, inclusive)	false	string
			agentVersion__gt	Agents versions greater than given version	false	string
			agentVersion__gte	Agents versions greater than or equal to given version	false	string
			agentVersion__lt	Agents versions less than given version	false	string
			agentVersion__lte	Agents versions less than or equal to given version	false	string
			agentVersions	Agent versions to include	false	string []
			agentVersionsNin	Agent versions not	false	string []

				to include		
			appsVulnerabilityStatuses	Apps vulnerability status in	false	string []
			appsVulnerabilityStatusesNin	Apps vulnerability status nin	false	string []
			awsRole__contains	Free-text filter by aws role(supports multiple values)	false	string []
			awsSecurityGroups__contains	Free-text filter by aws securityGroups(supports multiple values)	false	string []
			awsSubnetIds__contains	Free-text filter by aws subnet ids (supports multiple values)	false	string []
			azureResourceGroup__contains	Free-text filter by azure resource group(supports multiple values)	false	string []
			cloudAccount__contains	Free-text filter by cloud account (supports multiple values)	false	string []
			cloudImage__contains	Free-text filter by cloud image (supports multiple values)	false	string []

			cloudInstanceId__contains	Free-text filter by cloud instance id(supports multiple values)	false	string []
			cloudInstanceSize__contains	Free-text filter by cloud instance size(supports multiple values)	false	string []
			cloudLocation__contains	Free-text filter by cloud location (supports multiple values)	false	string []
			cloudNetwork__contains	Free-text filter by cloud network (supports multiple values)	false	string []
			cloudProvider	Agents from which cloud provider	false	string []
			cloudProviderNin	Exclude Agents from these cloud provider	false	string []
			cloudTags__contains	Free-text filter by cloud tags (supports multiple values)	false	string []
			clusterName__contains	Free-text filter by cluster name (supports multiple values)	false	string []

			computerName	Computer name	false	string
			computerName__contains	Free-text filter by computer name (supports multiple values)	false	string []
			computerName__like	Match computer name partially (substring)	false	string
			consoleMigrationStatuses	Migration status in	false	string []
			consoleMigrationStatusesNin	Migration status nin	false	string []
			coreCount__between	Possible number of CPU cores (inclusive)	false	string
			coreCount__gt	CPU cores (more than)	false	integer
			coreCount__gte	CPU cores (more than or equal)	false	integer
			coreCount__lt	CPU cores (less than)	false	integer
			coreCount__lte	CPU cores (less than or equal)	false	integer
			cpuCount__between	Possible number of CPU cores (inclusive)	false	string
			cpuCount__gt	Number of CPUs (more than)	false	integer

			cpuCount__gte	Number of CPUs (more than or equal)	false	integer
			cpuCount__lt	Number of CPUs (less than)	false	integer
			cpuCount__lte	Number of CPUs (less than or equal)	false	integer
			cpuId__contains	Free-text filter by CPU name (supports multiple values)	false	string []
			createdAt__between	Date range for creation time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			createdAt__gt	Agents created after this timestamp	false	string
			createdAt__gte	Agents created after or at this timestamp	false	string
			createdAt__lt	Agents created before this timestamp	false	string
			createdAt__lte	Agents created before or at this timestamp	false	string
			csvFilterId	The ID of the CSV file to filter by	false	string

			decommissionedAt__between	Date range for decommission time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			decommissionedAt__gt	Agents decommissioned after this timestamp	false	string
			decommissionedAt__gte	Agents decommissioned after or at this timestamp	false	string
			decommissionedAt__lt	Agents decommissioned before this timestamp	false	string
			decommissionedAt__lte	Agents decommissioned before this timestamp	false	string
			domains	Included network domains	false	string []
			domainsNin	Not included network domains	false	string []
			encryptedApplications	Disk encryption status	false	boolean
			externalId__contains	Free-text filter by external ID (Customer ID)	false	string []
			externalIp__contains	Free-text filter by visible IP (supports	false	string []

				multiple values)		
			filteredGroupIds	List of Group IDs to filter by	false	string []
			filteredSiteIds	List of Site IDs to filter by	false	string []
			filterId	Include all Agents matching this saved filter	false	string
			firewallEnabled	The agents supports Firewall Control and it is enabled for the agent's group	false	boolean []
			gatewayIp	Gateway ip	false	string
			gcpServiceAccount__contains	Free-text filter by gcp service account (supports multiple values)	false	string []
			groupIds	List of network groups	false	string []
			hasContainerizedWorkload	Include only Agents protecting containerized workloads	false	boolean
			hasLocalConfiguration	Agent has a local configuration set	false	boolean
			hasTags	Include only Agents that	false	boolean

				have any tags assigned if True, or none if False		
			ids	A list of Agent IDs	false	string []
			infected	Include only Agents with at least one active threat	false	boolean
			installerTypes	Include only Agents installed with these package types	false	string []
			installerTypesNin	Exclude Agents installed with these package types	false	string []
			isActive	Include only active Agents	false	boolean
			isDecommissioned	Include active, decommissioned or both	false	boolean []
			isPendingUninstall	Include only Agents with pending uninstall requests	false	boolean
			isUninstalled	Include installed, uninstalled or both	false	boolean []
			isUpToDate	Include only Agents with updated software	false	boolean

			k8sNodeLabels__contains	Free-text filter by K8s node labels (supports multiple values)	false	string []
			k8sNodeName__contains	Free-text filter by K8s node name (supports multiple values)	false	string []
			k8sType__contains	Free-text filter by K8s type(supports multiple values)	false	string []
			k8sVersion__contains	Free-text filter by K8s version (supports multiple values)	false	string []
			lastActiveDate__between	Date range for last active date(format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			lastActiveDate__gt	Agents last active after this time	false	string
			lastActiveDate__gte	Agents last active after or at this time	false	string
			lastActiveDate__lt	Agents last active before this time	false	string
			lastActiveDate__lte	Agents last active before or at this time	false	string

			lastLoggedInUserName__contains	Free-text filter by username (supports multiple values)	false	string []
			lastSuccessfulScanDate__between	Date range for last successful full disk scan(format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			lastSuccessfulScanDate__gt	Agents last successful full disk scan after this time	false	string
			lastSuccessfulScanDate__gte	Agents last successful full disk scan after or at this time	false	string
			lastSuccessfulScanDate__lt	Agents last successful full disk scan before this time	false	string
			lastSuccessfulScanDate__lte	Agents last successful full disk scan before or at this time	false	string
			liveUpdateId__contains	Free-text filter by live update ID (supports multiple values)	false	string []
			locationEnabled	The agents supports	false	boolean []

				Location Awareness and it is enabled for the agent's group		
			locationIds	Include only Agents reporting these locations	false	string []
			locationIdsNin	Do not include only Agents reporting these locations	false	string []
			machineTypes	Included machine types	false	string []
			machineTypesNin	Not included machine types	false	string []
			migrationStatus	Migration status	false	enum
			missingPermissions	Included missing permissions	false	string []
			missingPermissionsNin	Excluded missing permissions	false	string []
			mitigationMode	Agent mitigation mode policy	false	enum
			mitigationModeSuspicious	Mitigation mode policy for suspicious activity	false	enum
			networkInterfaceGatewayMacAddress__c	Free-text filter by Gateway	false	string []

			ontains	MAC address (supports multiple values)		
			networkInterfaceInet__contains	Free-text filter by local IP (supports multiple values)	false	string []
			networkInterfacePhysical__contains	Free-text filter by MAC address (supports multiple values)	false	string []
			networkQuarantineEnabled	The agents supports Network Quarantine Control and its enabled for the agent's group	false	boolean []
			networkStatuses	Included network statuses	false	string []
			networkStatusesNin	Included network statuses	false	string []
			operationalStates	Agent operational state	false	string []
			operationalStatesNin	Do not include these Agent operational states	false	string []
			osArch	OS architecture	false	enum
			osTypes	Included OS types	false	string []

			osTypesNin	Not included OS types	false	string []
			osVersion__contains	Free-text filter by OS full name and version (supports multiple values)	false	string []
			query	A free-text search term, will match applicable attributes (sub-string match). Note: Device's physical addresses will be matched if they start with the search term only (no match if they contain the term).	false	string
			rangerStatus	[DEPRECATED] Use rangerStatuses.	false	enum
			rangerStatuses	Status of Ranger	false	string []
			rangerStatusesNin	Do not include these Ranger Statuses	false	string []
			rangerVersions	Ranger versions to include	false	string []
			rangerVersionsNin	Ranger versions not to include	false	string []

			registeredAt__between	Date range for first registration time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			registeredAt__gt	Agents registered after this time	false	string
			registeredAt__gte	Agents registered after or at this time	false	string
			registeredAt__lt	Agents registered before this time	false	string
			registeredAt__lte	Agents registered before or at this time	false	string
			remoteOpsForensicsSupported	Include only agents that has Remote Ops Forensicsfeature supported	false	boolean
			remoteProfilingStates	Agent remote profiling state	false	string []
			remoteProfilingStatesNin	Do not include these Agent remote profiling states	false	string []
			rsoLevel	Supported Remote Script Orchestration	false	enum

				level		
			scanStatus	Scan status	false	enum
			scanStatuses	Included scan statuses	false	string []
			scanStatuses Nin	Not included scan statuses	false	string []
			serialNumber __contains	Free-text filter by Serial Number (supports multiple values)	false	string []
			siteIds	List of Site IDs to filter by	false	string []
			tagsData	Filter agents by their assigned tags. Given in form of a JSON where each key represents a tag key, and each value represents a list of string values to filter by. To filter by unassigned tag values, use __nin suffix in the tag key.	false	string
			threatConten tHash	Include only Agents that have at least one threat with this content hash	false	string
			threatCreate	Agents with	false	string

			dAt__between	threats reported in a date range (format: <from_timestamp>-<to_timestamp>, inclusive)		
			threatCreatedAt__gt	Agents with threats reported after this time	false	string
			threatCreatedAt__gte	Agents with threats reported after or at this time	false	string
			threatCreatedAt__lt	Agents with threats reported before this time	false	string
			threatCreatedAt__lte	Agents with threats reported before or at this time	false	string
			threatHidden	Include only Agents with at least one hidden threat	false	boolean
			threatMitigationStatus	Include only Agents that have threats with this mitigation status	false	enum
			threatRebootRequired	Has at least one threat with at least one mitigation	false	boolean []

				action pending reboot to succeed		
			threatResolved	Include only Agents with at least one resolved threat	false	boolean
			totalMemory__between	Total memory range (GB, inclusive)	false	string
			totalMemory__gt	Memory size (MB, more than)	false	integer
			totalMemory__gte	Memory size (MB, more than or equal)	false	integer
			totalMemory__lt	Memory size (MB, less than)	false	integer
			totalMemory__lte	Memory size (MB, less than or equal)	false	integer
			updatedAt__between	Date range for update time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			updatedAt__gt	Agents updated after this timestamp	false	string
			updatedAt__gte	Agents updated after or at this timestamp	false	string
			updatedAt__lt	Agents updated	false	string

<table>
<tr><td></td><td></td><td></td><td><table>
<tr><td></td><td>before this timestamp</td><td></td><td></td></tr>
<tr><td>updatedAt__lte</td><td>Agents updated before or at this timestamp</td><td>false</td><td>string</td></tr>
<tr><td>userActionsNeeded</td><td>Included pending user actions</td><td>false</td><td>string []</td></tr>
<tr><td>userActionsNeededNin</td><td>Excluded pending user actions</td><td>false</td><td>string []</td></tr>
<tr><td>uuid</td><td>Agent's universally unique identifier</td><td>false</td><td>string</td></tr>
<tr><td>uuid__contains</td><td>Free-text filter by Agent UUID (supports multiple values)</td><td>false</td><td>string []</td></tr>
<tr><td>uuids</td><td>A list of included UUIDs</td><td>false</td><td>string []</td></tr>
</table></td></tr>
<tr><td>data</td><td>Data</td><td>false</td><td></td></tr>
</table>

Decommission

POST /web/api/v2.1/agents/actions/decommission

If a user is scheduled for time off, or a device is scheduled for maintenance, you can decommission the Agent. This removes the Agent from the Management Console. When the Agent communicates with the Management again, the Management recommissions it and returns it to the Console. Use this command to decommission the Agents that match the filter.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - User has insufficient permissions to perform the requested action

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>affected</td><td>Number of entities affected by the requested operation</td><td>false</td><td>integer</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>filter</td><td>Applied filter - only matched Agents will be affected by the requested action. Note: One of these filter arguments must be supplied: ids, groupIds, filterId.</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>activeThreats</td><td>Include Agents with this amount of active threats</td><td>false</td><td>integer</td></tr>
<tr><td>activeThreats__gt</td><td>Include Agents with at least this amount of active threats</td><td>false</td><td>integer</td></tr>
<tr><td>adComputerMember__contains</td><td>Free-text filter by Active Directory computer groups string (supports multiple values)</td><td>false</td><td>string []</td></tr>
<tr><td>adComputerName__contains</td><td>Free-text filter by Active Directory computer name string (supports multiple values)</td><td>false</td><td>string []</td></tr>
<tr><td>adComputerQuery__contains</td><td>Free-text filter by Active Directory computer name or its groups</td><td>false</td><td>string []</td></tr>
</table>
</td></tr>
</table>

				(supports multiple values)		
			adQuery	An Active Directory query string	false	string
			adQuery__contains	Free-text filter by Active Directory string (supports multiple values)	false	string []
			adUserMember__contains	Free-text filter by Active Directory user groups string (supports multiple values)	false	string []
			adUserName__contains	Free-text filter by Active Directory username string (supports multiple values)	false	string []
			adUserQuery__contains	Free-text filter by Active Directory computer name or its groups (supports multiple values)	false	string []
			agentNamespa	Free-text	false	string []

			ce__contains	filter by agent namespace (supports multiple values)		
			agentPodName__contains	Free-text filter by agent pod name (supports multiple values)	false	string []
			agentVersion__between	Version range for agent version (format: <from_version>-<to_version>, inclusive)	false	string
			agentVersion__gt	Agents versions greater than given version	false	string
			agentVersion__gte	Agents versions greater than or equal to given version	false	string
			agentVersion__lt	Agents versions less than given version	false	string
			agentVersion__lte	Agents versions less than or equal to given version	false	string
			agentVersions	Agent versions to include	false	string []
			agentVersionsNin	Agent versions not	false	string []

				to include		
			appsVulnerabilityStatuses	Apps vulnerability status in	false	string []
			appsVulnerabilityStatusesNin	Apps vulnerability status nin	false	string []
			awsRole__contains	Free-text filter by aws role(supports multiple values)	false	string []
			awsSecurityGroups__contains	Free-text filter by aws securityGroups(supports multiple values)	false	string []
			awsSubnetIds__contains	Free-text filter by aws subnet ids (supports multiple values)	false	string []
			azureResourceGroup__contains	Free-text filter by azure resource group(supports multiple values)	false	string []
			cloudAccount__contains	Free-text filter by cloud account (supports multiple values)	false	string []
			cloudImage__contains	Free-text filter by cloud image (supports multiple values)	false	string []

			cloudInstanceId__contains	Free-text filter by cloud instance id(supports multiple values)	false	string []
			cloudInstanceSize__contains	Free-text filter by cloud instance size(supports multiple values)	false	string []
			cloudLocation__contains	Free-text filter by cloud location (supports multiple values)	false	string []
			cloudNetwork__contains	Free-text filter by cloud network (supports multiple values)	false	string []
			cloudProvider	Agents from which cloud provider	false	string []
			cloudProviderNin	Exclude Agents from these cloud provider	false	string []
			cloudTags__contains	Free-text filter by cloud tags (supports multiple values)	false	string []
			clusterName__contains	Free-text filter by cluster name (supports multiple values)	false	string []

			computerName	Computer name	false	string
			computerName__contains	Free-text filter by computer name (supports multiple values)	false	string []
			computerName__like	Match computer name partially (substring)	false	string
			consoleMigrationStatuses	Migration status in	false	string []
			consoleMigrationStatusesNin	Migration status nin	false	string []
			coreCount__between	Possible number of CPU cores (inclusive)	false	string
			coreCount__gt	CPU cores (more than)	false	integer
			coreCount__gte	CPU cores (more than or equal)	false	integer
			coreCount__lt	CPU cores (less than)	false	integer
			coreCount__lte	CPU cores (less than or equal)	false	integer
			cpuCount__between	Possible number of CPU cores (inclusive)	false	string
			cpuCount__gt	Number of CPUs (more than)	false	integer

			cpuCount__gte	Number of CPUs (more than or equal)	false	integer
			cpuCount__lt	Number of CPUs (less than)	false	integer
			cpuCount__lte	Number of CPUs (less than or equal)	false	integer
			cpuId__contains	Free-text filter by CPU name (supports multiple values)	false	string []
			createdAt__between	Date range for creation time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			createdAt__gt	Agents created after this timestamp	false	string
			createdAt__gte	Agents created after or at this timestamp	false	string
			createdAt__lt	Agents created before this timestamp	false	string
			createdAt__lte	Agents created before or at this timestamp	false	string
			csvFilterId	The ID of the CSV file to filter by	false	string

			decommissionedAt__between	Date range for decommission time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			decommissionedAt__gt	Agents decommissioned after this timestamp	false	string
			decommissionedAt__gte	Agents decommissioned after or at this timestamp	false	string
			decommissionedAt__lt	Agents decommissioned before this timestamp	false	string
			decommissionedAt__lte	Agents decommissioned before this timestamp	false	string
			domains	Included network domains	false	string []
			domainsNin	Not included network domains	false	string []
			encryptedApplications	Disk encryption status	false	boolean
			externalId__contains	Free-text filter by external ID (Customer ID)	false	string []
			externalIp__contains	Free-text filter by visible IP (supports	false	string []

				multiple values)		
			filteredGroupIds	List of Group IDs to filter by	false	string []
			filteredSiteIds	List of Site IDs to filter by	false	string []
			filterId	Include all Agents matching this saved filter	false	string
			firewallEnabled	The agents supports Firewall Control and it is enabled for the agent's group	false	boolean []
			gatewayIp	Gateway ip	false	string
			gcpServiceAccount__contains	Free-text filter by gcp service account (supports multiple values)	false	string []
			groupIds	List of network groups	false	string []
			hasContainerizedWorkload	Include only Agents protecting containerized workloads	false	boolean
			hasLocalConfiguration	Agent has a local configuration set	false	boolean
			hasTags	Include only Agents that	false	boolean

				have any tags assigned if True, or none if False		
			ids	A list of Agent IDs	false	string []
			infected	Include only Agents with at least one active threat	false	boolean
			installerTypes	Include only Agents installed with these package types	false	string []
			installerTypesNin	Exclude Agents installed with these package types	false	string []
			isActive	Include only active Agents	false	boolean
			isDecommissioned	Include active, decommissioned or both	false	boolean []
			isPendingUninstall	Include only Agents with pending uninstall requests	false	boolean
			isUninstalled	Include installed, uninstalled or both	false	boolean []
			isUpToDate	Include only Agents with updated software	false	boolean

			k8sNodeLabels__contains	Free-text filter by K8s node labels (supports multiple values)	false	string []
			k8sNodeName__contains	Free-text filter by K8s node name (supports multiple values)	false	string []
			k8sType__contains	Free-text filter by K8s type(supports multiple values)	false	string []
			k8sVersion__contains	Free-text filter by K8s version (supports multiple values)	false	string []
			lastActiveDate__between	Date range for last active date(format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			lastActiveDate__gt	Agents last active after this time	false	string
			lastActiveDate__gte	Agents last active after or at this time	false	string
			lastActiveDate__lt	Agents last active before this time	false	string
			lastActiveDate__lte	Agents last active before or at this time	false	string

			lastLoggedInUserName__contains	Free-text filter by username (supports multiple values)	false	string []
			lastSuccessfulScanDate__between	Date range for last successful full disk scan(format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			lastSuccessfulScanDate__gt	Agents last successful full disk scan after this time	false	string
			lastSuccessfulScanDate__gte	Agents last successful full disk scan after or at this time	false	string
			lastSuccessfulScanDate__lt	Agents last successful full disk scan before this time	false	string
			lastSuccessfulScanDate__lte	Agents last successful full disk scan before or at this time	false	string
			liveUpdateId__contains	Free-text filter by live update ID (supports multiple values)	false	string []
			locationEnabled	The agents supports	false	boolean []

				Location Awareness and it is enabled for the agent's group		
			locationIds	Include only Agents reporting these locations	false	string []
			locationIdsNin	Do not include only Agents reporting these locations	false	string []
			machineTypes	Included machine types	false	string []
			machineTypesNin	Not included machine types	false	string []
			migrationStatus	Migration status	false	enum
			missingPermissions	Included missing permissions	false	string []
			missingPermissionsNin	Excluded missing permissions	false	string []
			mitigationMode	Agent mitigation mode policy	false	enum
			mitigationModeSuspicious	Mitigation mode policy for suspicious activity	false	enum
			networkInterfaceGatewayMacAddress__c	Free-text filter by Gateway	false	string []

			ontains	MAC address (supports multiple values)		
			networkInterfaceInet__contains	Free-text filter by local IP (supports multiple values)	false	string []
			networkInterfacePhysical__contains	Free-text filter by MAC address (supports multiple values)	false	string []
			networkQuarantineEnabled	The agents supports Network Quarantine Control and its enabled for the agent's group	false	boolean []
			networkStatuses	Included network statuses	false	string []
			networkStatusesNin	Included network statuses	false	string []
			operationalStates	Agent operational state	false	string []
			operationalStatesNin	Do not include these Agent operational states	false	string []
			osArch	OS architecture	false	enum
			osTypes	Included OS types	false	string []

			osTypesNin	Not included OS types	false	string []
			osVersion__contains	Free-text filter by OS full name and version (supports multiple values)	false	string []
			query	A free-text search term, will match applicable attributes (sub-string match). Note: Device's physical addresses will be matched if they start with the search term only (no match if they contain the term).	false	string
			rangerStatus	[DEPRECATED] Use rangerStatuses.	false	enum
			rangerStatuses	Status of Ranger	false	string []
			rangerStatusesNin	Do not include these Ranger Statuses	false	string []
			rangerVersions	Ranger versions to include	false	string []
			rangerVersionsNin	Ranger versions not to include	false	string []

			registeredAt__between	Date range for first registration time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			registeredAt__gt	Agents registered after this time	false	string
			registeredAt__gte	Agents registered after or at this time	false	string
			registeredAt__lt	Agents registered before this time	false	string
			registeredAt__lte	Agents registered before or at this time	false	string
			remoteOpsForensicsSupported	Include only agents that has Remote Ops Forensicsfeature supported	false	boolean
			remoteProfilingStates	Agent remote profiling state	false	string []
			remoteProfilingStatesNin	Do not include these Agent remote profiling states	false	string []
			rsoLevel	Supported Remote Script Orchestration	false	enum

				level		
			scanStatus	Scan status	false	enum
			scanStatuses	Included scan statuses	false	string []
			scanStatuses Nin	Not included scan statuses	false	string []
			serialNumber __contains	Free-text filter by Serial Number (supports multiple values)	false	string []
			siteIds	List of Site IDs to filter by	false	string []
			tagsData	Filter agents by their assigned tags. Given in form of a JSON where each key represents a tag key, and each value represents a list of string values to filter by. To filter by unassigned tag values, use __nin suffix in the tag key.	false	string
			threatConten tHash	Include only Agents that have at least one threat with this content hash	false	string
			threatCreate	Agents with	false	string

			dAt__between	threats reported in a date range (format: <from_timestamp>-<to_timestamp>, inclusive)		
			threatCreatedAt__gt	Agents with threats reported after this time	false	string
			threatCreatedAt__gte	Agents with threats reported after or at this time	false	string
			threatCreatedAt__lt	Agents with threats reported before this time	false	string
			threatCreatedAt__lte	Agents with threats reported before or at this time	false	string
			threatHidden	Include only Agents with at least one hidden threat	false	boolean
			threatMitigationStatus	Include only Agents that have threats with this mitigation status	false	enum
			threatRebootRequired	Has at least one threat with at least one mitigation	false	boolean []

				action pending reboot to succeed		
			threatResolved	Include only Agents with at least one resolved threat	false	boolean
			totalMemory__between	Total memory range (GB, inclusive)	false	string
			totalMemory__gt	Memory size (MB, more than)	false	integer
			totalMemory__gte	Memory size (MB, more than or equal)	false	integer
			totalMemory__lt	Memory size (MB, less than)	false	integer
			totalMemory__lte	Memory size (MB, less than or equal)	false	integer
			updatedAt__between	Date range for update time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			updatedAt__gt	Agents updated after this timestamp	false	string
			updatedAt__gte	Agents updated after or at this timestamp	false	string
			updatedAt__lt	Agents updated	false	string

<table>
<tr><td></td><td></td><td></td><td>
<table>
<tr><td></td><td>before this timestamp</td><td></td><td></td></tr>
<tr><td>updatedAt__lte</td><td>Agents updated before or at this timestamp</td><td>false</td><td>string</td></tr>
<tr><td>userActionsNeeded</td><td>Included pending user actions</td><td>false</td><td>string []</td></tr>
<tr><td>userActionsNeededNin</td><td>Excluded pending user actions</td><td>false</td><td>string []</td></tr>
<tr><td>uuid</td><td>Agent's universally unique identifier</td><td>false</td><td>string</td></tr>
<tr><td>uuid__contains</td><td>Free-text filter by Agent UUID (supports multiple values)</td><td>false</td><td>string []</td></tr>
<tr><td>uuids</td><td>A list of included UUIDs</td><td>false</td><td>string []</td></tr>
</table>
</td></tr>
<tr><td>data</td><td>Data</td><td>false</td><td></td></tr>
</table>

Uninstall

POST /web/api/v2.1/agents/actions/uninstall

Use this command to uninstall Agents that match the filter. For Windows and macOS, make sure that all remnants of the Agent are removed: reboot the endpoints after uninstall. Use the "restart" command.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - User has insufficient permissions to perform the requested action

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>affected</td><td>Number of entities affected by the requested operation</td><td>false</td><td>integer</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>filter</td><td>Applied filter - only matched Agents will be affected by the requested action. Note: One of these filter arguments must be supplied: ids, groupIds, filterId.</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>activeThreats</td><td>Include Agents with this amount of active threats</td><td>false</td><td>integer</td></tr>
<tr><td>activeThreats__gt</td><td>Include Agents with at least this amount of active threats</td><td>false</td><td>integer</td></tr>
<tr><td>adComputerMember__contains</td><td>Free-text filter by Active Directory computer groups string (supports multiple values)</td><td>false</td><td>string []</td></tr>
<tr><td>adComputerName__contains</td><td>Free-text filter by Active Directory computer name string (supports multiple values)</td><td>false</td><td>string []</td></tr>
<tr><td>adComputerQuery__contains</td><td>Free-text filter by Active Directory computer name or its groups</td><td>false</td><td>string []</td></tr>
</table>
</td></tr>
</table>

				(supports multiple values)		
			adQuery	An Active Directory query string	false	string
			adQuery__contains	Free-text filter by Active Directory string (supports multiple values)	false	string []
			adUserMember__contains	Free-text filter by Active Directory user groups string (supports multiple values)	false	string []
			adUserName__contains	Free-text filter by Active Directory username string (supports multiple values)	false	string []
			adUserQuery__contains	Free-text filter by Active Directory computer name or its groups (supports multiple values)	false	string []
			agentNamespa	Free-text	false	string []

			ce__contains	filter by agent namespace (supports multiple values)		
			agentPodName__contains	Free-text filter by agent pod name (supports multiple values)	false	string []
			agentVersion__between	Version range for agent version (format: <from_version>-<to_version>, inclusive)	false	string
			agentVersion__gt	Agents versions greater than given version	false	string
			agentVersion__gte	Agents versions greater than or equal to given version	false	string
			agentVersion__lt	Agents versions less than given version	false	string
			agentVersion__lte	Agents versions less than or equal to given version	false	string
			agentVersions	Agent versions to include	false	string []
			agentVersionsNin	Agent versions not	false	string []

				to include		
			appsVulnerabilityStatuses	Apps vulnerability status in	false	string []
			appsVulnerabilityStatusesNin	Apps vulnerability status nin	false	string []
			awsRole__contains	Free-text filter by aws role(supports multiple values)	false	string []
			awsSecurityGroups__contains	Free-text filter by aws securityGroups(supports multiple values)	false	string []
			awsSubnetIds__contains	Free-text filter by aws subnet ids (supports multiple values)	false	string []
			azureResourceGroup__contains	Free-text filter by azure resource group(supports multiple values)	false	string []
			cloudAccount__contains	Free-text filter by cloud account (supports multiple values)	false	string []
			cloudImage__contains	Free-text filter by cloud image (supports multiple values)	false	string []

			cloudInstanceId__contains	Free-text filter by cloud instance id(supports multiple values)	false	string []
			cloudInstanceSize__contains	Free-text filter by cloud instance size(supports multiple values)	false	string []
			cloudLocation__contains	Free-text filter by cloud location (supports multiple values)	false	string []
			cloudNetwork__contains	Free-text filter by cloud network (supports multiple values)	false	string []
			cloudProvider	Agents from which cloud provider	false	string []
			cloudProviderNin	Exclude Agents from these cloud provider	false	string []
			cloudTags__contains	Free-text filter by cloud tags (supports multiple values)	false	string []
			clusterName__contains	Free-text filter by cluster name (supports multiple values)	false	string []

			computerName	Computer name	false	string
			computerName__contains	Free-text filter by computer name (supports multiple values)	false	string []
			computerName__like	Match computer name partially (substring)	false	string
			consoleMigrationStatuses	Migration status in	false	string []
			consoleMigrationStatusesNin	Migration status nin	false	string []
			coreCount__between	Possible number of CPU cores (inclusive)	false	string
			coreCount__gt	CPU cores (more than)	false	integer
			coreCount__gte	CPU cores (more than or equal)	false	integer
			coreCount__lt	CPU cores (less than)	false	integer
			coreCount__lte	CPU cores (less than or equal)	false	integer
			cpuCount__between	Possible number of CPU cores (inclusive)	false	string
			cpuCount__gt	Number of CPUs (more than)	false	integer

			cpuCount__gte	Number of CPUs (more than or equal)	false	integer
			cpuCount__lt	Number of CPUs (less than)	false	integer
			cpuCount__lte	Number of CPUs (less than or equal)	false	integer
			cpuId__contains	Free-text filter by CPU name (supports multiple values)	false	string []
			createdAt__between	Date range for creation time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			createdAt__gt	Agents created after this timestamp	false	string
			createdAt__gte	Agents created after or at this timestamp	false	string
			createdAt__lt	Agents created before this timestamp	false	string
			createdAt__lte	Agents created before or at this timestamp	false	string
			csvFilterId	The ID of the CSV file to filter by	false	string

			decommissionedAt__between	Date range for decommission time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			decommissionedAt__gt	Agents decommissioned after this timestamp	false	string
			decommissionedAt__gte	Agents decommissioned after or at this timestamp	false	string
			decommissionedAt__lt	Agents decommissioned before this timestamp	false	string
			decommissionedAt__lte	Agents decommissioned before this timestamp	false	string
			domains	Included network domains	false	string []
			domainsNin	Not included network domains	false	string []
			encryptedApplications	Disk encryption status	false	boolean
			externalId__contains	Free-text filter by external ID (Customer ID)	false	string []
			externalIp__contains	Free-text filter by visible IP (supports	false	string []

				multiple values)		
			filteredGroupIds	List of Group IDs to filter by	false	string []
			filteredSiteIds	List of Site IDs to filter by	false	string []
			filterId	Include all Agents matching this saved filter	false	string
			firewallEnabled	The agents supports Firewall Control and it is enabled for the agent's group	false	boolean []
			gatewayIp	Gateway ip	false	string
			gcpServiceAccount__contains	Free-text filter by gcp service account (supports multiple values)	false	string []
			groupIds	List of network groups	false	string []
			hasContainerizedWorkload	Include only Agents protecting containerized workloads	false	boolean
			hasLocalConfiguration	Agent has a local configuration set	false	boolean
			hasTags	Include only Agents that	false	boolean

				have any tags assigned if True, or none if False		
			ids	A list of Agent IDs	false	string []
			infected	Include only Agents with at least one active threat	false	boolean
			installerTypes	Include only Agents installed with these package types	false	string []
			installerTypesNin	Exclude Agents installed with these package types	false	string []
			isActive	Include only active Agents	false	boolean
			isDecommissioned	Include active, decommissioned or both	false	boolean []
			isPendingUninstall	Include only Agents with pending uninstall requests	false	boolean
			isUninstalled	Include installed, uninstalled or both	false	boolean []
			isUpToDate	Include only Agents with updated software	false	boolean

			k8sNodeLabels__contains	Free-text filter by K8s node labels (supports multiple values)	false	string []
			k8sNodeName__contains	Free-text filter by K8s node name (supports multiple values)	false	string []
			k8sType__contains	Free-text filter by K8s type(supports multiple values)	false	string []
			k8sVersion__contains	Free-text filter by K8s version (supports multiple values)	false	string []
			lastActiveDate__between	Date range for last active date(format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			lastActiveDate__gt	Agents last active after this time	false	string
			lastActiveDate__gte	Agents last active after or at this time	false	string
			lastActiveDate__lt	Agents last active before this time	false	string
			lastActiveDate__lte	Agents last active before or at this time	false	string

			lastLoggedInUserName__contains	Free-text filter by username (supports multiple values)	false	string []
			lastSuccessfulScanDate__between	Date range for last successful full disk scan(format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			lastSuccessfulScanDate__gt	Agents last successful full disk scan after this time	false	string
			lastSuccessfulScanDate__gte	Agents last successful full disk scan after or at this time	false	string
			lastSuccessfulScanDate__lt	Agents last successful full disk scan before this time	false	string
			lastSuccessfulScanDate__lte	Agents last successful full disk scan before or at this time	false	string
			liveUpdateId__contains	Free-text filter by live update ID (supports multiple values)	false	string []
			locationEnabled	The agents supports	false	boolean []

				Location Awareness and it is enabled for the agent's group		
			locationIds	Include only Agents reporting these locations	false	string []
			locationIdsNin	Do not include only Agents reporting these locations	false	string []
			machineTypes	Included machine types	false	string []
			machineTypesNin	Not included machine types	false	string []
			migrationStatus	Migration status	false	enum
			missingPermissions	Included missing permissions	false	string []
			missingPermissionsNin	Excluded missing permissions	false	string []
			mitigationMode	Agent mitigation mode policy	false	enum
			mitigationModeSuspicious	Mitigation mode policy for suspicious activity	false	enum
			networkInterfaceGatewayMacAddress__c	Free-text filter by Gateway	false	string []

			ontains	MAC address (supports multiple values)		
			networkInterfaceInet__contains	Free-text filter by local IP (supports multiple values)	false	string []
			networkInterfacePhysical__contains	Free-text filter by MAC address (supports multiple values)	false	string []
			networkQuarantineEnabled	The agents supports Network Quarantine Control and its enabled for the agent's group	false	boolean []
			networkStatuses	Included network statuses	false	string []
			networkStatusesNin	Included network statuses	false	string []
			operationalStates	Agent operational state	false	string []
			operationalStatesNin	Do not include these Agent operational states	false	string []
			osArch	OS architecture	false	enum
			osTypes	Included OS types	false	string []

			osTypesNin	Not included OS types	false	string []
			osVersion__contains	Free-text filter by OS full name and version (supports multiple values)	false	string []
			query	A free-text search term, will match applicable attributes (sub-string match). Note: Device's physical addresses will be matched if they start with the search term only (no match if they contain the term).	false	string
			rangerStatus	[DEPRECATED] Use rangerStatuses.	false	enum
			rangerStatuses	Status of Ranger	false	string []
			rangerStatusesNin	Do not include these Ranger Statuses	false	string []
			rangerVersions	Ranger versions to include	false	string []
			rangerVersionsNin	Ranger versions not to include	false	string []

			registeredAt__between	Date range for first registration time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			registeredAt__gt	Agents registered after this time	false	string
			registeredAt__gte	Agents registered after or at this time	false	string
			registeredAt__lt	Agents registered before this time	false	string
			registeredAt__lte	Agents registered before or at this time	false	string
			remoteOpsForensicsSupported	Include only agents that has Remote Ops Forensicsfeature supported	false	boolean
			remoteProfilingStates	Agent remote profiling state	false	string []
			remoteProfilingStatesNin	Do not include these Agent remote profiling states	false	string []
			rsoLevel	Supported Remote Script Orchestration	false	enum

				level		
			scanStatus	Scan status	false	enum
			scanStatuses	Included scan statuses	false	string []
			scanStatuses Nin	Not included scan statuses	false	string []
			serialNumber __contains	Free-text filter by Serial Number (supports multiple values)	false	string []
			siteIds	List of Site IDs to filter by	false	string []
			tagsData	Filter agents by their assigned tags. Given in form of a JSON where each key represents a tag key, and each value represents a list of string values to filter by. To filter by unassigned tag values, use __nin suffix in the tag key.	false	string
			threatConten tHash	Include only Agents that have at least one threat with this content hash	false	string
			threatCreate	Agents with	false	string

			dAt__between	threats reported in a date range (format: <from_timestamp>-<to_timestamp>, inclusive)		
			threatCreatedAt__gt	Agents with threats reported after this time	false	string
			threatCreatedAt__gte	Agents with threats reported after or at this time	false	string
			threatCreatedAt__lt	Agents with threats reported before this time	false	string
			threatCreatedAt__lte	Agents with threats reported before or at this time	false	string
			threatHidden	Include only Agents with at least one hidden threat	false	boolean
			threatMitigationStatus	Include only Agents that have threats with this mitigation status	false	enum
			threatRebootRequired	Has at least one threat with at least one mitigation	false	boolean []

				action pending reboot to succeed		
			threatResolved	Include only Agents with at least one resolved threat	false	boolean
			totalMemory__between	Total memory range (GB, inclusive)	false	string
			totalMemory__gt	Memory size (MB, more than)	false	integer
			totalMemory__gte	Memory size (MB, more than or equal)	false	integer
			totalMemory__lt	Memory size (MB, less than)	false	integer
			totalMemory__lte	Memory size (MB, less than or equal)	false	integer
			updatedAt__between	Date range for update time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			updatedAt__gt	Agents updated after this timestamp	false	string
			updatedAt__gte	Agents updated after or at this timestamp	false	string
			updatedAt__lt	Agents updated	false	string

<table>
<tr><td></td><td></td><td></td><td><table>
<tr><td></td><td>before this timestamp</td><td></td><td></td></tr>
<tr><td>updatedAt__lte</td><td>Agents updated before or at this timestamp</td><td>false</td><td>string</td></tr>
<tr><td>userActionsNeeded</td><td>Included pending user actions</td><td>false</td><td>string []</td></tr>
<tr><td>userActionsNeededNin</td><td>Excluded pending user actions</td><td>false</td><td>string []</td></tr>
<tr><td>uuid</td><td>Agent's universally unique identifier</td><td>false</td><td>string</td></tr>
<tr><td>uuid__contains</td><td>Free-text filter by Agent UUID (supports multiple values)</td><td>false</td><td>string []</td></tr>
<tr><td>uuids</td><td>A list of included UUIDs</td><td>false</td><td>string []</td></tr>
</table></td></tr>
<tr><td>data</td><td>Data</td><td>false</td><td></td></tr>
</table>

Restart

POST /web/api/v2.1/agents/actions/restart-machine

Use this command to restart endpoints that have an Agent installed and that fit the filter. We recommend that you use the "broadcast" command to send a message to users of endpoints before you restart their computers.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - User has insufficient permissions to perform the requested action

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>affected</td><td>Number of entities affected by the requested operation</td><td>false</td><td>integer</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>filter</td><td>Applied filter - only matched Agents will be affected by the requested action. Note: One of these filter arguments must be supplied: ids, groupIds, filterId.</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>activeThreats</td><td>Include Agents with this amount of active threats</td><td>false</td><td>integer</td></tr>
<tr><td>activeThreats__gt</td><td>Include Agents with at least this amount of active threats</td><td>false</td><td>integer</td></tr>
<tr><td>adComputerMember__contains</td><td>Free-text filter by Active Directory computer groups string (supports multiple values)</td><td>false</td><td>string []</td></tr>
<tr><td>adComputerName__contains</td><td>Free-text filter by Active Directory computer name string (supports multiple values)</td><td>false</td><td>string []</td></tr>
<tr><td>adComputerQuery__contains</td><td>Free-text filter by Active Directory computer name or its groups</td><td>false</td><td>string []</td></tr>
</table>
</td></tr>
</table>

				(supports multiple values)		
			adQuery	An Active Directory query string	false	string
			adQuery__contains	Free-text filter by Active Directory string (supports multiple values)	false	string []
			adUserMember__contains	Free-text filter by Active Directory user groups string (supports multiple values)	false	string []
			adUserName__contains	Free-text filter by Active Directory username string (supports multiple values)	false	string []
			adUserQuery__contains	Free-text filter by Active Directory computer name or its groups (supports multiple values)	false	string []
			agentNamespa	Free-text	false	string []

			ce__contains	filter by agent namespace (supports multiple values)		
			agentPodName__contains	Free-text filter by agent pod name (supports multiple values)	false	string []
			agentVersion__between	Version range for agent version (format: <from_version>-<to_version>, inclusive)	false	string
			agentVersion__gt	Agents versions greater than given version	false	string
			agentVersion__gte	Agents versions greater than or equal to given version	false	string
			agentVersion__lt	Agents versions less than given version	false	string
			agentVersion__lte	Agents versions less than or equal to given version	false	string
			agentVersions	Agent versions to include	false	string []
			agentVersionsNin	Agent versions not	false	string []

				to include		
			appsVulnerabilityStatuses	Apps vulnerability status in	false	string []
			appsVulnerabilityStatusesNin	Apps vulnerability status nin	false	string []
			awsRole__contains	Free-text filter by aws role(supports multiple values)	false	string []
			awsSecurityGroups__contains	Free-text filter by aws securityGroups(supports multiple values)	false	string []
			awsSubnetIds__contains	Free-text filter by aws subnet ids (supports multiple values)	false	string []
			azureResourceGroup__contains	Free-text filter by azure resource group(supports multiple values)	false	string []
			cloudAccount__contains	Free-text filter by cloud account (supports multiple values)	false	string []
			cloudImage__contains	Free-text filter by cloud image (supports multiple values)	false	string []

			cloudInstanceId__contains	Free-text filter by cloud instance id(supports multiple values)	false	string []
			cloudInstanceSize__contains	Free-text filter by cloud instance size(supports multiple values)	false	string []
			cloudLocation__contains	Free-text filter by cloud location (supports multiple values)	false	string []
			cloudNetwork__contains	Free-text filter by cloud network (supports multiple values)	false	string []
			cloudProvider	Agents from which cloud provider	false	string []
			cloudProviderNin	Exclude Agents from these cloud provider	false	string []
			cloudTags__contains	Free-text filter by cloud tags (supports multiple values)	false	string []
			clusterName__contains	Free-text filter by cluster name (supports multiple values)	false	string []

			computerName	Computer name	false	string
			computerName__contains	Free-text filter by computer name (supports multiple values)	false	string []
			computerName__like	Match computer name partially (substring)	false	string
			consoleMigrationStatuses	Migration status in	false	string []
			consoleMigrationStatusesNin	Migration status nin	false	string []
			coreCount__between	Possible number of CPU cores (inclusive)	false	string
			coreCount__gt	CPU cores (more than)	false	integer
			coreCount__gte	CPU cores (more than or equal)	false	integer
			coreCount__lt	CPU cores (less than)	false	integer
			coreCount__lte	CPU cores (less than or equal)	false	integer
			cpuCount__between	Possible number of CPU cores (inclusive)	false	string
			cpuCount__gt	Number of CPUs (more than)	false	integer

			cpuCount__gte	Number of CPUs (more than or equal)	false	integer
			cpuCount__lt	Number of CPUs (less than)	false	integer
			cpuCount__lte	Number of CPUs (less than or equal)	false	integer
			cpuId__contains	Free-text filter by CPU name (supports multiple values)	false	string []
			createdAt__between	Date range for creation time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			createdAt__gt	Agents created after this timestamp	false	string
			createdAt__gte	Agents created after or at this timestamp	false	string
			createdAt__lt	Agents created before this timestamp	false	string
			createdAt__lte	Agents created before or at this timestamp	false	string
			csvFilterId	The ID of the CSV file to filter by	false	string

			decommissionedAt__between	Date range for decommission time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			decommissionedAt__gt	Agents decommissioned after this timestamp	false	string
			decommissionedAt__gte	Agents decommissioned after or at this timestamp	false	string
			decommissionedAt__lt	Agents decommissioned before this timestamp	false	string
			decommissionedAt__lte	Agents decommissioned before this timestamp	false	string
			domains	Included network domains	false	string []
			domainsNin	Not included network domains	false	string []
			encryptedApplications	Disk encryption status	false	boolean
			externalId__contains	Free-text filter by external ID (Customer ID)	false	string []
			externalIp__contains	Free-text filter by visible IP (supports	false	string []

				multiple values)		
			filteredGroupIds	List of Group IDs to filter by	false	string []
			filteredSiteIds	List of Site IDs to filter by	false	string []
			filterId	Include all Agents matching this saved filter	false	string
			firewallEnabled	The agents supports Firewall Control and it is enabled for the agent's group	false	boolean []
			gatewayIp	Gateway ip	false	string
			gcpServiceAccount__contains	Free-text filter by gcp service account (supports multiple values)	false	string []
			groupIds	List of network groups	false	string []
			hasContainerizedWorkload	Include only Agents protecting containerized workloads	false	boolean
			hasLocalConfiguration	Agent has a local configuration set	false	boolean
			hasTags	Include only Agents that	false	boolean

				have any tags assigned if True, or none if False		
			ids	A list of Agent IDs	false	string []
			infected	Include only Agents with at least one active threat	false	boolean
			installerTypes	Include only Agents installed with these package types	false	string []
			installerTypesNin	Exclude Agents installed with these package types	false	string []
			isActive	Include only active Agents	false	boolean
			isDecommissioned	Include active, decommissioned or both	false	boolean []
			isPendingUninstall	Include only Agents with pending uninstall requests	false	boolean
			isUninstalled	Include installed, uninstalled or both	false	boolean []
			isUpToDate	Include only Agents with updated software	false	boolean

			k8sNodeLabels__contains	Free-text filter by K8s node labels (supports multiple values)	false	string []
			k8sNodeName__contains	Free-text filter by K8s node name (supports multiple values)	false	string []
			k8sType__contains	Free-text filter by K8s type(supports multiple values)	false	string []
			k8sVersion__contains	Free-text filter by K8s version (supports multiple values)	false	string []
			lastActiveDate__between	Date range for last active date(format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			lastActiveDate__gt	Agents last active after this time	false	string
			lastActiveDate__gte	Agents last active after or at this time	false	string
			lastActiveDate__lt	Agents last active before this time	false	string
			lastActiveDate__lte	Agents last active before or at this time	false	string

			lastLoggedInUserName__contains	Free-text filter by username (supports multiple values)	false	string []
			lastSuccessfulScanDate__between	Date range for last successful full disk scan(format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			lastSuccessfulScanDate__gt	Agents last successful full disk scan after this time	false	string
			lastSuccessfulScanDate__gte	Agents last successful full disk scan after or at this time	false	string
			lastSuccessfulScanDate__lt	Agents last successful full disk scan before this time	false	string
			lastSuccessfulScanDate__lte	Agents last successful full disk scan before or at this time	false	string
			liveUpdateId__contains	Free-text filter by live update ID (supports multiple values)	false	string []
			locationEnabled	The agents supports	false	boolean []

				Location Awareness and it is enabled for the agent's group		
			locationIds	Include only Agents reporting these locations	false	string []
			locationIdsNin	Do not include only Agents reporting these locations	false	string []
			machineTypes	Included machine types	false	string []
			machineTypesNin	Not included machine types	false	string []
			migrationStatus	Migration status	false	enum
			missingPermissions	Included missing permissions	false	string []
			missingPermissionsNin	Excluded missing permissions	false	string []
			mitigationMode	Agent mitigation mode policy	false	enum
			mitigationModeSuspicious	Mitigation mode policy for suspicious activity	false	enum
			networkInterfaceGatewayMacAddress__c	Free-text filter by Gateway	false	string []

			ontains	MAC address (supports multiple values)		
			networkInterfaceInet__contains	Free-text filter by local IP (supports multiple values)	false	string []
			networkInterfacePhysical__contains	Free-text filter by MAC address (supports multiple values)	false	string []
			networkQuarantineEnabled	The agents supports Network Quarantine Control and its enabled for the agent's group	false	boolean []
			networkStatuses	Included network statuses	false	string []
			networkStatusesNin	Included network statuses	false	string []
			operationalStates	Agent operational state	false	string []
			operationalStatesNin	Do not include these Agent operational states	false	string []
			osArch	OS architecture	false	enum
			osTypes	Included OS types	false	string []

			osTypesNin	Not included OS types	false	string []
			osVersion__contains	Free-text filter by OS full name and version (supports multiple values)	false	string []
			query	A free-text search term, will match applicable attributes (sub-string match). Note: Device's physical addresses will be matched if they start with the search term only (no match if they contain the term).	false	string
			rangerStatus	[DEPRECATED] Use rangerStatuses.	false	enum
			rangerStatuses	Status of Ranger	false	string []
			rangerStatusesNin	Do not include these Ranger Statuses	false	string []
			rangerVersions	Ranger versions to include	false	string []
			rangerVersionsNin	Ranger versions not to include	false	string []

			registeredAt__between	Date range for first registration time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			registeredAt__gt	Agents registered after this time	false	string
			registeredAt__gte	Agents registered after or at this time	false	string
			registeredAt__lt	Agents registered before this time	false	string
			registeredAt__lte	Agents registered before or at this time	false	string
			remoteOpsForensicsSupported	Include only agents that has Remote Ops Forensicsfeature supported	false	boolean
			remoteProfilingStates	Agent remote profiling state	false	string []
			remoteProfilingStatesNin	Do not include these Agent remote profiling states	false	string []
			rsoLevel	Supported Remote Script Orchestration	false	enum

				level		
			scanStatus	Scan status	false	enum
			scanStatuses	Included scan statuses	false	string []
			scanStatuses Nin	Not included scan statuses	false	string []
			serialNumber __contains	Free-text filter by Serial Number (supports multiple values)	false	string []
			siteIds	List of Site IDs to filter by	false	string []
			tagsData	Filter agents by their assigned tags. Given in form of a JSON where each key represents a tag key, and each value represents a list of string values to filter by. To filter by unassigned tag values, use __nin suffix in the tag key.	false	string
			threatConten tHash	Include only Agents that have at least one threat with this content hash	false	string
			threatCreate	Agents with	false	string

			dAt__between	threats reported in a date range (format: <from_timestamp>-<to_timestamp>, inclusive)		
			threatCreatedAt__gt	Agents with threats reported after this time	false	string
			threatCreatedAt__gte	Agents with threats reported after or at this time	false	string
			threatCreatedAt__lt	Agents with threats reported before this time	false	string
			threatCreatedAt__lte	Agents with threats reported before or at this time	false	string
			threatHidden	Include only Agents with at least one hidden threat	false	boolean
			threatMitigationStatus	Include only Agents that have threats with this mitigation status	false	enum
			threatRebootRequired	Has at least one threat with at least one mitigation	false	boolean []

				action pending reboot to succeed		
			threatResolved	Include only Agents with at least one resolved threat	false	boolean
			totalMemory__between	Total memory range (GB, inclusive)	false	string
			totalMemory__gt	Memory size (MB, more than)	false	integer
			totalMemory__gte	Memory size (MB, more than or equal)	false	integer
			totalMemory__lt	Memory size (MB, less than)	false	integer
			totalMemory__lte	Memory size (MB, less than or equal)	false	integer
			updatedAt__between	Date range for update time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			updatedAt__gt	Agents updated after this timestamp	false	string
			updatedAt__gte	Agents updated after or at this timestamp	false	string
			updatedAt__lt	Agents updated	false	string

<table>
<tr><td></td><td></td><td></td><td><table>
<tr><td></td><td>before this timestamp</td><td></td><td></td></tr>
<tr><td>updatedAt__lte</td><td>Agents updated before or at this timestamp</td><td>false</td><td>string</td></tr>
<tr><td>userActionsNeeded</td><td>Included pending user actions</td><td>false</td><td>string []</td></tr>
<tr><td>userActionsNeededNin</td><td>Excluded pending user actions</td><td>false</td><td>string []</td></tr>
<tr><td>uuid</td><td>Agent's universally unique identifier</td><td>false</td><td>string</td></tr>
<tr><td>uuid__contains</td><td>Free-text filter by Agent UUID (supports multiple values)</td><td>false</td><td>string []</td></tr>
<tr><td>uuids</td><td>A list of included UUIDs</td><td>false</td><td>string []</td></tr>
</table></td></tr>
<tr><td>data</td><td>Data</td><td>false</td><td></td></tr>
</table>

Shutdown

POST /web/api/v2.1/agents/actions/shutdown

You can shut down endpoints remotely for performance, maintenance, or security.
This command shuts down all endpoints that match the filter. Best Practice: If an endpoint is infected, we recommend the "disconnect" command and not the "shutdown" command. The disconnect command secures the environment from infection while you analyze the cause and best response.
If the endpoint is offline, the shutdown command is not available.

BEST PRACTICE

If an endpoint is infected, we recommend the "disconnect" command and not the "shutdown" command. The disconnect command secures the environment from infection while you analyze the cause and best response.
If the endpoint is offline, the shutdown command is not available.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - User has insufficient permissions to perform the requested action

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>affected</td><td>Number of entities affected by the requested operation</td><td>false</td><td>integer</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>filter</td><td>Applied filter - only matched Agents will be affected by the requested action. Note: One of these filter arguments must be supplied: ids, groupIds, filterId.</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>activeThreats</td><td>Include Agents with this amount of active threats</td><td>false</td><td>integer</td></tr>
<tr><td>activeThreats__gt</td><td>Include Agents with at least this amount of active threats</td><td>false</td><td>integer</td></tr>
<tr><td>adComputerMember__contains</td><td>Free-text filter by Active Directory computer groups string (supports multiple values)</td><td>false</td><td>string []</td></tr>
<tr><td>adComputerName__contains</td><td>Free-text filter by Active Directory computer name string (supports multiple values)</td><td>false</td><td>string []</td></tr>
<tr><td>adComputerQuery__contains</td><td>Free-text filter by Active Directory computer name or its groups</td><td>false</td><td>string []</td></tr>
</table>
</td></tr>
</table>

				(supports multiple values)		
			adQuery	An Active Directory query string	false	string
			adQuery__contains	Free-text filter by Active Directory string (supports multiple values)	false	string []
			adUserMember__contains	Free-text filter by Active Directory user groups string (supports multiple values)	false	string []
			adUserName__contains	Free-text filter by Active Directory username string (supports multiple values)	false	string []
			adUserQuery__contains	Free-text filter by Active Directory computer name or its groups (supports multiple values)	false	string []
			agentNamespa	Free-text	false	string []

			ce__contains	filter by agent namespace (supports multiple values)		
			agentPodName__contains	Free-text filter by agent pod name (supports multiple values)	false	string []
			agentVersion__between	Version range for agent version (format: <from_version>-<to_version>, inclusive)	false	string
			agentVersion__gt	Agents versions greater than given version	false	string
			agentVersion__gte	Agents versions greater than or equal to given version	false	string
			agentVersion__lt	Agents versions less than given version	false	string
			agentVersion__lte	Agents versions less than or equal to given version	false	string
			agentVersions	Agent versions to include	false	string []
			agentVersionsNin	Agent versions not	false	string []

				to include		
			appsVulnerabilityStatuses	Apps vulnerability status in	false	string []
			appsVulnerabilityStatusesNin	Apps vulnerability status nin	false	string []
			awsRole__contains	Free-text filter by aws role(supports multiple values)	false	string []
			awsSecurityGroups__contains	Free-text filter by aws securityGroups(supports multiple values)	false	string []
			awsSubnetIds__contains	Free-text filter by aws subnet ids (supports multiple values)	false	string []
			azureResourceGroup__contains	Free-text filter by azure resource group(supports multiple values)	false	string []
			cloudAccount__contains	Free-text filter by cloud account (supports multiple values)	false	string []
			cloudImage__contains	Free-text filter by cloud image (supports multiple values)	false	string []

			cloudInstanceId__contains	Free-text filter by cloud instance id(supports multiple values)	false	string []
			cloudInstanceSize__contains	Free-text filter by cloud instance size(supports multiple values)	false	string []
			cloudLocation__contains	Free-text filter by cloud location (supports multiple values)	false	string []
			cloudNetwork__contains	Free-text filter by cloud network (supports multiple values)	false	string []
			cloudProvider	Agents from which cloud provider	false	string []
			cloudProviderNin	Exclude Agents from these cloud provider	false	string []
			cloudTags__contains	Free-text filter by cloud tags (supports multiple values)	false	string []
			clusterName__contains	Free-text filter by cluster name (supports multiple values)	false	string []

			computerName	Computer name	false	string
			computerName__contains	Free-text filter by computer name (supports multiple values)	false	string []
			computerName__like	Match computer name partially (substring)	false	string
			consoleMigrationStatuses	Migration status in	false	string []
			consoleMigrationStatusesNin	Migration status nin	false	string []
			coreCount__between	Possible number of CPU cores (inclusive)	false	string
			coreCount__gt	CPU cores (more than)	false	integer
			coreCount__gte	CPU cores (more than or equal)	false	integer
			coreCount__lt	CPU cores (less than)	false	integer
			coreCount__lte	CPU cores (less than or equal)	false	integer
			cpuCount__between	Possible number of CPU cores (inclusive)	false	string
			cpuCount__gt	Number of CPUs (more than)	false	integer

			cpuCount__gte	Number of CPUs (more than or equal)	false	integer
			cpuCount__lt	Number of CPUs (less than)	false	integer
			cpuCount__lte	Number of CPUs (less than or equal)	false	integer
			cpuId__contains	Free-text filter by CPU name (supports multiple values)	false	string []
			createdAt__between	Date range for creation time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			createdAt__gt	Agents created after this timestamp	false	string
			createdAt__gte	Agents created after or at this timestamp	false	string
			createdAt__lt	Agents created before this timestamp	false	string
			createdAt__lte	Agents created before or at this timestamp	false	string
			csvFilterId	The ID of the CSV file to filter by	false	string

			decommissionedAt__between	Date range for decommission time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			decommissionedAt__gt	Agents decommissioned after this timestamp	false	string
			decommissionedAt__gte	Agents decommissioned after or at this timestamp	false	string
			decommissionedAt__lt	Agents decommissioned before this timestamp	false	string
			decommissionedAt__lte	Agents decommissioned before this timestamp	false	string
			domains	Included network domains	false	string []
			domainsNin	Not included network domains	false	string []
			encryptedApplications	Disk encryption status	false	boolean
			externalId__contains	Free-text filter by external ID (Customer ID)	false	string []
			externalIp__contains	Free-text filter by visible IP (supports	false	string []

				multiple values)		
			filteredGroupIds	List of Group IDs to filter by	false	string []
			filteredSiteIds	List of Site IDs to filter by	false	string []
			filterId	Include all Agents matching this saved filter	false	string
			firewallEnabled	The agents supports Firewall Control and it is enabled for the agent's group	false	boolean []
			gatewayIp	Gateway ip	false	string
			gcpServiceAccount__contains	Free-text filter by gcp service account (supports multiple values)	false	string []
			groupIds	List of network groups	false	string []
			hasContainerizedWorkload	Include only Agents protecting containerized workloads	false	boolean
			hasLocalConfiguration	Agent has a local configuration set	false	boolean
			hasTags	Include only Agents that	false	boolean

				have any tags assigned if True, or none if False		
			ids	A list of Agent IDs	false	string []
			infected	Include only Agents with at least one active threat	false	boolean
			installerTypes	Include only Agents installed with these package types	false	string []
			installerTypesNin	Exclude Agents installed with these package types	false	string []
			isActive	Include only active Agents	false	boolean
			isDecommissioned	Include active, decommissioned or both	false	boolean []
			isPendingUninstall	Include only Agents with pending uninstall requests	false	boolean
			isUninstalled	Include installed, uninstalled or both	false	boolean []
			isUpToDate	Include only Agents with updated software	false	boolean

			k8sNodeLabels__contains	Free-text filter by K8s node labels (supports multiple values)	false	string []
			k8sNodeName__contains	Free-text filter by K8s node name (supports multiple values)	false	string []
			k8sType__contains	Free-text filter by K8s type(supports multiple values)	false	string []
			k8sVersion__contains	Free-text filter by K8s version (supports multiple values)	false	string []
			lastActiveDate__between	Date range for last active date(format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			lastActiveDate__gt	Agents last active after this time	false	string
			lastActiveDate__gte	Agents last active after or at this time	false	string
			lastActiveDate__lt	Agents last active before this time	false	string
			lastActiveDate__lte	Agents last active before or at this time	false	string

			lastLoggedInUserName__contains	Free-text filter by username (supports multiple values)	false	string []
			lastSuccessfulScanDate__between	Date range for last successful full disk scan(format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			lastSuccessfulScanDate__gt	Agents last successful full disk scan after this time	false	string
			lastSuccessfulScanDate__gte	Agents last successful full disk scan after or at this time	false	string
			lastSuccessfulScanDate__lt	Agents last successful full disk scan before this time	false	string
			lastSuccessfulScanDate__lte	Agents last successful full disk scan before or at this time	false	string
			liveUpdateId__contains	Free-text filter by live update ID (supports multiple values)	false	string []
			locationEnabled	The agents supports	false	boolean []

				Location Awareness and it is enabled for the agent's group		
			locationIds	Include only Agents reporting these locations	false	string []
			locationIdsNin	Do not include only Agents reporting these locations	false	string []
			machineTypes	Included machine types	false	string []
			machineTypesNin	Not included machine types	false	string []
			migrationStatus	Migration status	false	enum
			missingPermissions	Included missing permissions	false	string []
			missingPermissionsNin	Excluded missing permissions	false	string []
			mitigationMode	Agent mitigation mode policy	false	enum
			mitigationModeSuspicious	Mitigation mode policy for suspicious activity	false	enum
			networkInterfaceGatewayMacAddress__c	Free-text filter by Gateway	false	string []

			ontains	MAC address (supports multiple values)		
			networkInterfaceInet__contains	Free-text filter by local IP (supports multiple values)	false	string []
			networkInterfacePhysical__contains	Free-text filter by MAC address (supports multiple values)	false	string []
			networkQuarantineEnabled	The agents supports Network Quarantine Control and its enabled for the agent's group	false	boolean []
			networkStatuses	Included network statuses	false	string []
			networkStatusesNin	Included network statuses	false	string []
			operationalStates	Agent operational state	false	string []
			operationalStatesNin	Do not include these Agent operational states	false	string []
			osArch	OS architecture	false	enum
			osTypes	Included OS types	false	string []

			osTypesNin	Not included OS types	false	string []
			osVersion__contains	Free-text filter by OS full name and version (supports multiple values)	false	string []
			query	A free-text search term, will match applicable attributes (sub-string match). Note: Device's physical addresses will be matched if they start with the search term only (no match if they contain the term).	false	string
			rangerStatus	[DEPRECATED] Use rangerStatuses.	false	enum
			rangerStatuses	Status of Ranger	false	string []
			rangerStatusesNin	Do not include these Ranger Statuses	false	string []
			rangerVersions	Ranger versions to include	false	string []
			rangerVersionsNin	Ranger versions not to include	false	string []

			registeredAt__between	Date range for first registration time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			registeredAt__gt	Agents registered after this time	false	string
			registeredAt__gte	Agents registered after or at this time	false	string
			registeredAt__lt	Agents registered before this time	false	string
			registeredAt__lte	Agents registered before or at this time	false	string
			remoteOpsForensicsSupported	Include only agents that has Remote Ops Forensicsfeature supported	false	boolean
			remoteProfilingStates	Agent remote profiling state	false	string []
			remoteProfilingStatesNin	Do not include these Agent remote profiling states	false	string []
			rsoLevel	Supported Remote Script Orchestration	false	enum

				level		
			scanStatus	Scan status	false	enum
			scanStatuses	Included scan statuses	false	string []
			scanStatuses Nin	Not included scan statuses	false	string []
			serialNumber __contains	Free-text filter by Serial Number (supports multiple values)	false	string []
			siteIds	List of Site IDs to filter by	false	string []
			tagsData	Filter agents by their assigned tags. Given in form of a JSON where each key represents a tag key, and each value represents a list of string values to filter by. To filter by unassigned tag values, use __nin suffix in the tag key.	false	string
			threatConten tHash	Include only Agents that have at least one threat with this content hash	false	string
			threatCreate	Agents with	false	string

			dAt__between	threats reported in a date range (format: <from_timestamp>-<to_timestamp>, inclusive)		
			threatCreatedAt__gt	Agents with threats reported after this time	false	string
			threatCreatedAt__gte	Agents with threats reported after or at this time	false	string
			threatCreatedAt__lt	Agents with threats reported before this time	false	string
			threatCreatedAt__lte	Agents with threats reported before or at this time	false	string
			threatHidden	Include only Agents with at least one hidden threat	false	boolean
			threatMitigationStatus	Include only Agents that have threats with this mitigation status	false	enum
			threatRebootRequired	Has at least one threat with at least one mitigation	false	boolean []

				action pending reboot to succeed		
			threatResolved	Include only Agents with at least one resolved threat	false	boolean
			totalMemory__between	Total memory range (GB, inclusive)	false	string
			totalMemory__gt	Memory size (MB, more than)	false	integer
			totalMemory__gte	Memory size (MB, more than or equal)	false	integer
			totalMemory__lt	Memory size (MB, less than)	false	integer
			totalMemory__lte	Memory size (MB, less than or equal)	false	integer
			updatedAt__between	Date range for update time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			updatedAt__gt	Agents updated after this timestamp	false	string
			updatedAt__gte	Agents updated after or at this timestamp	false	string
			updatedAt__lt	Agents updated	false	string

<table>
<tr><td></td><td></td><td></td><td><table>
<tr><td></td><td>before this timestamp</td><td></td><td></td></tr>
<tr><td>updatedAt__lte</td><td>Agents updated before or at this timestamp</td><td>false</td><td>string</td></tr>
<tr><td>userActionsNeeded</td><td>Included pending user actions</td><td>false</td><td>string []</td></tr>
<tr><td>userActionsNeededNin</td><td>Excluded pending user actions</td><td>false</td><td>string []</td></tr>
<tr><td>uuid</td><td>Agent's universally unique identifier</td><td>false</td><td>string</td></tr>
<tr><td>uuid__contains</td><td>Free-text filter by Agent UUID (supports multiple values)</td><td>false</td><td>string []</td></tr>
<tr><td>uuids</td><td>A list of included UUIDs</td><td>false</td><td>string []</td></tr>
</table></td></tr>
<tr><td>data</td><td>Data</td><td>false</td><td></td></tr>
</table>

Approve Uninstall

POST /web/api/v2.1/agents/actions/approve-uninstall

If a user tries to uninstall the SentinelOne Agent from an endpoint, an uninstall request is sent to the Management. You must approve the request.
After you approve a request, users see a message that the request was approved. They can restart to complete the Agent uninstall.
We recommend that you do not approve these requests until you understand the reason for the request, you agree with the request, and you have alternative security for the endpoint until you install the Agent again.
This command will approve pending uninstall requests for all Agents that match the filter.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - User has insufficient permissions to perform the requested action

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>affected</td><td>Number of entities affected by the requested operation</td><td>false</td><td>integer</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

Name	Description	Required	Value
filter	Applied filter - only matched Agents will be affected by the requested action. Leave empty to apply the action on all applicable Agents.	true	

Name	Description	Required	Value
accountIds	List of Account IDs to filter by	false	string []
activeThreats	Include Agents with this amount of active threats	false	integer
activeThreats__gt	Include Agents with at least this amount of active threats	false	integer
adComputerMember__contains	Free-text filter by Active Directory computer groups string (supports multiple values)	false	string []
adComputerName__contains	Free-text filter by Active Directory computer name string (supports multiple values)	false	string []
adComputerQuery__contains	Free-text filter by Active Directory computer name or its groups	false	string []

				(supports multiple values)		
			adQuery	An Active Directory query string	false	string
			adQuery__contains	Free-text filter by Active Directory string (supports multiple values)	false	string []
			adUserMember__contains	Free-text filter by Active Directory user groups string (supports multiple values)	false	string []
			adUserName__contains	Free-text filter by Active Directory username string (supports multiple values)	false	string []
			adUserQuery__contains	Free-text filter by Active Directory computer name or its groups (supports multiple values)	false	string []
			agentNamespa	Free-text	false	string []

			ce__contains	filter by agent namespace (supports multiple values)		
			agentPodName__contains	Free-text filter by agent pod name (supports multiple values)	false	string []
			agentVersion__between	Version range for agent version (format: <from_version>-<to_version>, inclusive)	false	string
			agentVersion__gt	Agents versions greater than given version	false	string
			agentVersion__gte	Agents versions greater than or equal to given version	false	string
			agentVersion__lt	Agents versions less than given version	false	string
			agentVersion__lte	Agents versions less than or equal to given version	false	string
			agentVersions	Agent versions to include	false	string []
			agentVersionsNin	Agent versions not	false	string []

				to include		
			appsVulnerabilityStatuses	Apps vulnerability status in	false	string []
			appsVulnerabilityStatusesNin	Apps vulnerability status nin	false	string []
			awsRole__contains	Free-text filter by aws role(supports multiple values)	false	string []
			awsSecurityGroups__contains	Free-text filter by aws securityGroups(supports multiple values)	false	string []
			awsSubnetIds__contains	Free-text filter by aws subnet ids (supports multiple values)	false	string []
			azureResourceGroup__contains	Free-text filter by azure resource group(supports multiple values)	false	string []
			cloudAccount__contains	Free-text filter by cloud account (supports multiple values)	false	string []
			cloudImage__contains	Free-text filter by cloud image (supports multiple values)	false	string []

			cloudInstanceId__contains	Free-text filter by cloud instance id(supports multiple values)	false	string []
			cloudInstanceSize__contains	Free-text filter by cloud instance size(supports multiple values)	false	string []
			cloudLocation__contains	Free-text filter by cloud location (supports multiple values)	false	string []
			cloudNetwork__contains	Free-text filter by cloud network (supports multiple values)	false	string []
			cloudProvider	Agents from which cloud provider	false	string []
			cloudProviderNin	Exclude Agents from these cloud provider	false	string []
			cloudTags__contains	Free-text filter by cloud tags (supports multiple values)	false	string []
			clusterName__contains	Free-text filter by cluster name (supports multiple values)	false	string []

			computerName	Computer name	false	string
			computerName__contains	Free-text filter by computer name (supports multiple values)	false	string []
			computerName__like	Match computer name partially (substring)	false	string
			consoleMigrationStatuses	Migration status in	false	string []
			consoleMigrationStatusesNin	Migration status nin	false	string []
			coreCount__between	Possible number of CPU cores (inclusive)	false	string
			coreCount__gt	CPU cores (more than)	false	integer
			coreCount__gte	CPU cores (more than or equal)	false	integer
			coreCount__lt	CPU cores (less than)	false	integer
			coreCount__lte	CPU cores (less than or equal)	false	integer
			cpuCount__between	Possible number of CPU cores (inclusive)	false	string
			cpuCount__gt	Number of CPUs (more than)	false	integer

			cpuCount__gte	Number of CPUs (more than or equal)	false	integer
			cpuCount__lt	Number of CPUs (less than)	false	integer
			cpuCount__lte	Number of CPUs (less than or equal)	false	integer
			cpuId__contains	Free-text filter by CPU name (supports multiple values)	false	string []
			createdAt__between	Date range for creation time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			createdAt__gt	Agents created after this timestamp	false	string
			createdAt__gte	Agents created after or at this timestamp	false	string
			createdAt__lt	Agents created before this timestamp	false	string
			createdAt__lte	Agents created before or at this timestamp	false	string
			csvFilterId	The ID of the CSV file to filter by	false	string

			decommissionedAt__between	Date range for decommission time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			decommissionedAt__gt	Agents decommissioned after this timestamp	false	string
			decommissionedAt__gte	Agents decommissioned after or at this timestamp	false	string
			decommissionedAt__lt	Agents decommissioned before this timestamp	false	string
			decommissionedAt__lte	Agents decommissioned before this timestamp	false	string
			domains	Included network domains	false	string []
			domainsNin	Not included network domains	false	string []
			encryptedApplications	Disk encryption status	false	boolean
			externalId__contains	Free-text filter by external ID (Customer ID)	false	string []
			externalIp__contains	Free-text filter by visible IP (supports	false	string []

				multiple values)		
			filteredGroupIds	List of Group IDs to filter by	false	string []
			filteredSiteIds	List of Site IDs to filter by	false	string []
			filterId	Include all Agents matching this saved filter	false	string
			firewallEnabled	The agents supports Firewall Control and it is enabled for the agent's group	false	boolean []
			gatewayIp	Gateway ip	false	string
			gcpServiceAccount__contains	Free-text filter by gcp service account (supports multiple values)	false	string []
			groupIds	List of Group IDs to filter by	false	string []
			hasContainerizedWorkload	Include only Agents protecting containerized workloads	false	boolean
			hasLocalConfiguration	Agent has a local configuration set	false	boolean
			hasTags	Include only Agents that	false	boolean

				have any tags assigned if True, or none if False		
			ids	A list of Agent IDs	false	string []
			infected	Include only Agents with at least one active threat	false	boolean
			installerTypes	Include only Agents installed with these package types	false	string []
			installerTypesNin	Exclude Agents installed with these package types	false	string []
			isActive	Include only active Agents	false	boolean
			isDecommissioned	Include active, decommissioned or both	false	boolean []
			isPendingUninstall	Include only Agents with pending uninstall requests	false	boolean
			isUninstalled	Include installed, uninstalled or both	false	boolean []
			isUpToDate	Include only Agents with updated software	false	boolean

			k8sNodeLabels__contains	Free-text filter by K8s node labels (supports multiple values)	false	string []
			k8sNodeName__contains	Free-text filter by K8s node name (supports multiple values)	false	string []
			k8sType__contains	Free-text filter by K8s type(supports multiple values)	false	string []
			k8sVersion__contains	Free-text filter by K8s version (supports multiple values)	false	string []
			lastActiveDate__between	Date range for last active date(format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			lastActiveDate__gt	Agents last active after this time	false	string
			lastActiveDate__gte	Agents last active after or at this time	false	string
			lastActiveDate__lt	Agents last active before this time	false	string
			lastActiveDate__lte	Agents last active before or at this time	false	string

			lastLoggedInUserName__contains	Free-text filter by username (supports multiple values)	false	string []
			lastSuccessfulScanDate__between	Date range for last successful full disk scan(format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			lastSuccessfulScanDate__gt	Agents last successful full disk scan after this time	false	string
			lastSuccessfulScanDate__gte	Agents last successful full disk scan after or at this time	false	string
			lastSuccessfulScanDate__lt	Agents last successful full disk scan before this time	false	string
			lastSuccessfulScanDate__lte	Agents last successful full disk scan before or at this time	false	string
			liveUpdateId__contains	Free-text filter by live update ID (supports multiple values)	false	string []
			locationEnabled	The agents supports	false	boolean []

				Location Awareness and it is enabled for the agent's group		
			locationIds	Include only Agents reporting these locations	false	string []
			locationIdsNin	Do not include only Agents reporting these locations	false	string []
			machineTypes	Included machine types	false	string []
			machineTypesNin	Not included machine types	false	string []
			migrationStatus	Migration status	false	enum
			missingPermissions	Included missing permissions	false	string []
			missingPermissionsNin	Excluded missing permissions	false	string []
			mitigationMode	Agent mitigation mode policy	false	enum
			mitigationModeSuspicious	Mitigation mode policy for suspicious activity	false	enum
			networkInterfaceGatewayMacAddress__c	Free-text filter by Gateway	false	string []

			ontains	MAC address (supports multiple values)		
			networkInterfaceInet__contains	Free-text filter by local IP (supports multiple values)	false	string []
			networkInterfacePhysical__contains	Free-text filter by MAC address (supports multiple values)	false	string []
			networkQuarantineEnabled	The agents supports Network Quarantine Control and its enabled for the agent's group	false	boolean []
			networkStatuses	Included network statuses	false	string []
			networkStatusesNin	Included network statuses	false	string []
			operationalStates	Agent operational state	false	string []
			operationalStatesNin	Do not include these Agent operational states	false	string []
			osArch	OS architecture	false	enum
			osTypes	Included OS types	false	string []

			osTypesNin	Not included OS types	false	string []
			osVersion__contains	Free-text filter by OS full name and version (supports multiple values)	false	string []
			query	A free-text search term, will match applicable attributes (sub-string match). Note: Device's physical addresses will be matched if they start with the search term only (no match if they contain the term).	false	string
			rangerStatus	[DEPRECATED] Use rangerStatuses.	false	enum
			rangerStatuses	Status of Ranger	false	string []
			rangerStatusesNin	Do not include these Ranger Statuses	false	string []
			rangerVersions	Ranger versions to include	false	string []
			rangerVersionsNin	Ranger versions not to include	false	string []

			registeredAt__between	Date range for first registration time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			registeredAt__gt	Agents registered after this time	false	string
			registeredAt__gte	Agents registered after or at this time	false	string
			registeredAt__lt	Agents registered before this time	false	string
			registeredAt__lte	Agents registered before or at this time	false	string
			remoteOpsForensicsSupported	Include only agents that has Remote Ops Forensicsfeature supported	false	boolean
			remoteProfilingStates	Agent remote profiling state	false	string []
			remoteProfilingStatesNin	Do not include these Agent remote profiling states	false	string []
			rsoLevel	Supported Remote Script Orchestration	false	enum

				level		
			scanStatus	Scan status	false	enum
			scanStatuses	Included scan statuses	false	string []
			scanStatuses Nin	Not included scan statuses	false	string []
			serialNumber __contains	Free-text filter by Serial Number (supports multiple values)	false	string []
			siteIds	List of Site IDs to filter by	false	string []
			tagsData	Filter agents by their assigned tags. Given in form of a JSON where each key represents a tag key, and each value represents a list of string values to filter by. To filter by unassigned tag values, use __nin suffix in the tag key.	false	string
			threatConten tHash	Include only Agents that have at least one threat with this content hash	false	string
			threatCreate	Agents with	false	string

			dAt__between	threats reported in a date range (format: <from_timestamp>-<to_timestamp>, inclusive)		
			threatCreatedAt__gt	Agents with threats reported after this time	false	string
			threatCreatedAt__gte	Agents with threats reported after or at this time	false	string
			threatCreatedAt__lt	Agents with threats reported before this time	false	string
			threatCreatedAt__lte	Agents with threats reported before or at this time	false	string
			threatHidden	Include only Agents with at least one hidden threat	false	boolean
			threatMitigationStatus	Include only Agents that have threats with this mitigation status	false	enum
			threatRebootRequired	Has at least one threat with at least one mitigation	false	boolean []

				action pending reboot to succeed		
			threatResolved	Include only Agents with at least one resolved threat	false	boolean
			totalMemory__between	Total memory range (GB, inclusive)	false	string
			totalMemory__gt	Memory size (MB, more than)	false	integer
			totalMemory__gte	Memory size (MB, more than or equal)	false	integer
			totalMemory__lt	Memory size (MB, less than)	false	integer
			totalMemory__lte	Memory size (MB, less than or equal)	false	integer
			updatedAt__between	Date range for update time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			updatedAt__gt	Agents updated after this timestamp	false	string
			updatedAt__gte	Agents updated after or at this timestamp	false	string
			updatedAt__lt	Agents updated	false	string

<table>
<tr><td></td><td></td><td></td><td><table>
<tr><td></td><td>before this timestamp</td><td></td><td></td></tr>
<tr><td>updatedAt__lte</td><td>Agents updated before or at this timestamp</td><td>false</td><td>string</td></tr>
<tr><td>userActionsNeeded</td><td>Included pending user actions</td><td>false</td><td>string []</td></tr>
<tr><td>userActionsNeededNin</td><td>Excluded pending user actions</td><td>false</td><td>string []</td></tr>
<tr><td>uuid</td><td>Agent's universally unique identifier</td><td>false</td><td>string</td></tr>
<tr><td>uuid__contains</td><td>Free-text filter by Agent UUID (supports multiple values)</td><td>false</td><td>string []</td></tr>
<tr><td>uuids</td><td>A list of included UUIDs</td><td>false</td><td>string []</td></tr>
</table></td></tr>
<tr><td>data</td><td>Data</td><td>false</td><td></td></tr>
</table>

Reject uninstall

POST /web/api/v2.1/agents/actions/reject-uninstall

Reject uninstall requests for all Agents that match the filter. To learn more about Uninstall Requests, see "Approve Uninstall".

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - User has insufficient permissions to perform the requested action

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>affected</td><td>Number of entities affected by the requested operation</td><td>false</td><td>integer</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>filter</td><td>Applied filter - only matched Agents will be affected by the requested action. Leave empty to apply the action on all applicable Agents.</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>activeThreats</td><td>Include Agents with this amount of active threats</td><td>false</td><td>integer</td></tr>
<tr><td>activeThreats__gt</td><td>Include Agents with at least this amount of active threats</td><td>false</td><td>integer</td></tr>
<tr><td>adComputerMember__contains</td><td>Free-text filter by Active Directory computer groups string (supports multiple values)</td><td>false</td><td>string []</td></tr>
<tr><td>adComputerName__contains</td><td>Free-text filter by Active Directory computer name string (supports multiple values)</td><td>false</td><td>string []</td></tr>
<tr><td>adComputerQuery__contains</td><td>Free-text filter by Active Directory computer name or its groups</td><td>false</td><td>string []</td></tr>
</table>
</td></tr>
</table>

				(supports multiple values)		
			adQuery	An Active Directory query string	false	string
			adQuery__contains	Free-text filter by Active Directory string (supports multiple values)	false	string []
			adUserMember__contains	Free-text filter by Active Directory user groups string (supports multiple values)	false	string []
			adUserName__contains	Free-text filter by Active Directory username string (supports multiple values)	false	string []
			adUserQuery__contains	Free-text filter by Active Directory computer name or its groups (supports multiple values)	false	string []
			agentNamespa	Free-text	false	string []

			ce__contains	filter by agent namespace (supports multiple values)		
			agentPodName__contains	Free-text filter by agent pod name (supports multiple values)	false	string []
			agentVersion__between	Version range for agent version (format: <from_version>-<to_version>, inclusive)	false	string
			agentVersion__gt	Agents versions greater than given version	false	string
			agentVersion__gte	Agents versions greater than or equal to given version	false	string
			agentVersion__lt	Agents versions less than given version	false	string
			agentVersion__lte	Agents versions less than or equal to given version	false	string
			agentVersions	Agent versions to include	false	string []
			agentVersionsNin	Agent versions not	false	string []

				to include		
			appsVulnerabilityStatuses	Apps vulnerability status in	false	string []
			appsVulnerabilityStatusesNin	Apps vulnerability status nin	false	string []
			awsRole__contains	Free-text filter by aws role(supports multiple values)	false	string []
			awsSecurityGroups__contains	Free-text filter by aws securityGroups(supports multiple values)	false	string []
			awsSubnetIds__contains	Free-text filter by aws subnet ids (supports multiple values)	false	string []
			azureResourceGroup__contains	Free-text filter by azure resource group(supports multiple values)	false	string []
			cloudAccount__contains	Free-text filter by cloud account (supports multiple values)	false	string []
			cloudImage__contains	Free-text filter by cloud image (supports multiple values)	false	string []

			cloudInstanceId__contains	Free-text filter by cloud instance id(supports multiple values)	false	string []
			cloudInstanceSize__contains	Free-text filter by cloud instance size(supports multiple values)	false	string []
			cloudLocation__contains	Free-text filter by cloud location (supports multiple values)	false	string []
			cloudNetwork__contains	Free-text filter by cloud network (supports multiple values)	false	string []
			cloudProvider	Agents from which cloud provider	false	string []
			cloudProviderNin	Exclude Agents from these cloud provider	false	string []
			cloudTags__contains	Free-text filter by cloud tags (supports multiple values)	false	string []
			clusterName__contains	Free-text filter by cluster name (supports multiple values)	false	string []

			computerName	Computer name	false	string
			computerName__contains	Free-text filter by computer name (supports multiple values)	false	string []
			computerName__like	Match computer name partially (substring)	false	string
			consoleMigrationStatuses	Migration status in	false	string []
			consoleMigrationStatusesNin	Migration status nin	false	string []
			coreCount__between	Possible number of CPU cores (inclusive)	false	string
			coreCount__gt	CPU cores (more than)	false	integer
			coreCount__gte	CPU cores (more than or equal)	false	integer
			coreCount__lt	CPU cores (less than)	false	integer
			coreCount__lte	CPU cores (less than or equal)	false	integer
			cpuCount__between	Possible number of CPU cores (inclusive)	false	string
			cpuCount__gt	Number of CPUs (more than)	false	integer

			cpuCount__gte	Number of CPUs (more than or equal)	false	integer
			cpuCount__lt	Number of CPUs (less than)	false	integer
			cpuCount__lte	Number of CPUs (less than or equal)	false	integer
			cpuId__contains	Free-text filter by CPU name (supports multiple values)	false	string []
			createdAt__between	Date range for creation time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			createdAt__gt	Agents created after this timestamp	false	string
			createdAt__gte	Agents created after or at this timestamp	false	string
			createdAt__lt	Agents created before this timestamp	false	string
			createdAt__lte	Agents created before or at this timestamp	false	string
			csvFilterId	The ID of the CSV file to filter by	false	string

			decommissionedAt__between	Date range for decommission time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			decommissionedAt__gt	Agents decommissioned after this timestamp	false	string
			decommissionedAt__gte	Agents decommissioned after or at this timestamp	false	string
			decommissionedAt__lt	Agents decommissioned before this timestamp	false	string
			decommissionedAt__lte	Agents decommissioned before this timestamp	false	string
			domains	Included network domains	false	string []
			domainsNin	Not included network domains	false	string []
			encryptedApplications	Disk encryption status	false	boolean
			externalId__contains	Free-text filter by external ID (Customer ID)	false	string []
			externalIp__contains	Free-text filter by visible IP (supports	false	string []

				multiple values)		
			filteredGroupIds	List of Group IDs to filter by	false	string []
			filteredSiteIds	List of Site IDs to filter by	false	string []
			filterId	Include all Agents matching this saved filter	false	string
			firewallEnabled	The agents supports Firewall Control and it is enabled for the agent's group	false	boolean []
			gatewayIp	Gateway ip	false	string
			gcpServiceAccount__contains	Free-text filter by gcp service account (supports multiple values)	false	string []
			groupIds	List of Group IDs to filter by	false	string []
			hasContainerizedWorkload	Include only Agents protecting containerized workloads	false	boolean
			hasLocalConfiguration	Agent has a local configuration set	false	boolean
			hasTags	Include only Agents that	false	boolean

				have any tags assigned if True, or none if False		
			ids	A list of Agent IDs	false	string []
			infected	Include only Agents with at least one active threat	false	boolean
			installerTypes	Include only Agents installed with these package types	false	string []
			installerTypesNin	Exclude Agents installed with these package types	false	string []
			isActive	Include only active Agents	false	boolean
			isDecommissioned	Include active, decommissioned or both	false	boolean []
			isPendingUninstall	Include only Agents with pending uninstall requests	false	boolean
			isUninstalled	Include installed, uninstalled or both	false	boolean []
			isUpToDate	Include only Agents with updated software	false	boolean

			k8sNodeLabels__contains	Free-text filter by K8s node labels (supports multiple values)	false	string []
			k8sNodeName__contains	Free-text filter by K8s node name (supports multiple values)	false	string []
			k8sType__contains	Free-text filter by K8s type(supports multiple values)	false	string []
			k8sVersion__contains	Free-text filter by K8s version (supports multiple values)	false	string []
			lastActiveDate__between	Date range for last active date(format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			lastActiveDate__gt	Agents last active after this time	false	string
			lastActiveDate__gte	Agents last active after or at this time	false	string
			lastActiveDate__lt	Agents last active before this time	false	string
			lastActiveDate__lte	Agents last active before or at this time	false	string

			lastLoggedInUserName__contains	Free-text filter by username (supports multiple values)	false	string []
			lastSuccessfulScanDate__between	Date range for last successful full disk scan(format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			lastSuccessfulScanDate__gt	Agents last successful full disk scan after this time	false	string
			lastSuccessfulScanDate__gte	Agents last successful full disk scan after or at this time	false	string
			lastSuccessfulScanDate__lt	Agents last successful full disk scan before this time	false	string
			lastSuccessfulScanDate__lte	Agents last successful full disk scan before or at this time	false	string
			liveUpdateId__contains	Free-text filter by live update ID (supports multiple values)	false	string []
			locationEnabled	The agents supports	false	boolean []

				Location Awareness and it is enabled for the agent's group		
			locationIds	Include only Agents reporting these locations	false	string []
			locationIdsNin	Do not include only Agents reporting these locations	false	string []
			machineTypes	Included machine types	false	string []
			machineTypesNin	Not included machine types	false	string []
			migrationStatus	Migration status	false	enum
			missingPermissions	Included missing permissions	false	string []
			missingPermissionsNin	Excluded missing permissions	false	string []
			mitigationMode	Agent mitigation mode policy	false	enum
			mitigationModeSuspicious	Mitigation mode policy for suspicious activity	false	enum
			networkInterfaceGatewayMacAddress__c	Free-text filter by Gateway	false	string []

			ontains	MAC address (supports multiple values)		
			networkInterfaceInet__contains	Free-text filter by local IP (supports multiple values)	false	string []
			networkInterfacePhysical__contains	Free-text filter by MAC address (supports multiple values)	false	string []
			networkQuarantineEnabled	The agents supports Network Quarantine Control and its enabled for the agent's group	false	boolean []
			networkStatuses	Included network statuses	false	string []
			networkStatusesNin	Included network statuses	false	string []
			operationalStates	Agent operational state	false	string []
			operationalStatesNin	Do not include these Agent operational states	false	string []
			osArch	OS architecture	false	enum
			osTypes	Included OS types	false	string []

			osTypesNin	Not included OS types	false	string []
			osVersion__contains	Free-text filter by OS full name and version (supports multiple values)	false	string []
			query	A free-text search term, will match applicable attributes (sub-string match). Note: Device's physical addresses will be matched if they start with the search term only (no match if they contain the term).	false	string
			rangerStatus	[DEPRECATED] Use rangerStatuses.	false	enum
			rangerStatuses	Status of Ranger	false	string []
			rangerStatusesNin	Do not include these Ranger Statuses	false	string []
			rangerVersions	Ranger versions to include	false	string []
			rangerVersionsNin	Ranger versions not to include	false	string []

			registeredAt__between	Date range for first registration time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			registeredAt__gt	Agents registered after this time	false	string
			registeredAt__gte	Agents registered after or at this time	false	string
			registeredAt__lt	Agents registered before this time	false	string
			registeredAt__lte	Agents registered before or at this time	false	string
			remoteOpsForensicsSupported	Include only agents that has Remote Ops Forensicsfeature supported	false	boolean
			remoteProfilingStates	Agent remote profiling state	false	string []
			remoteProfilingStatesNin	Do not include these Agent remote profiling states	false	string []
			rsoLevel	Supported Remote Script Orchestration	false	enum

				level		
			scanStatus	Scan status	false	enum
			scanStatuses	Included scan statuses	false	string []
			scanStatuses Nin	Not included scan statuses	false	string []
			serialNumber __contains	Free-text filter by Serial Number (supports multiple values)	false	string []
			siteIds	List of Site IDs to filter by	false	string []
			tagsData	Filter agents by their assigned tags. Given in form of a JSON where each key represents a tag key, and each value represents a list of string values to filter by. To filter by unassigned tag values, use __nin suffix in the tag key.	false	string
			threatConten tHash	Include only Agents that have at least one threat with this content hash	false	string
			threatCreate	Agents with	false	string

			dAt__between	threats reported in a date range (format: <from_timestamp>-<to_timestamp>, inclusive)		
			threatCreatedAt__gt	Agents with threats reported after this time	false	string
			threatCreatedAt__gte	Agents with threats reported after or at this time	false	string
			threatCreatedAt__lt	Agents with threats reported before this time	false	string
			threatCreatedAt__lte	Agents with threats reported before or at this time	false	string
			threatHidden	Include only Agents with at least one hidden threat	false	boolean
			threatMitigationStatus	Include only Agents that have threats with this mitigation status	false	enum
			threatRebootRequired	Has at least one threat with at least one mitigation	false	boolean []

				action pending reboot to succeed		
			threatResolved	Include only Agents with at least one resolved threat	false	boolean
			totalMemory__between	Total memory range (GB, inclusive)	false	string
			totalMemory__gt	Memory size (MB, more than)	false	integer
			totalMemory__gte	Memory size (MB, more than or equal)	false	integer
			totalMemory__lt	Memory size (MB, less than)	false	integer
			totalMemory__lte	Memory size (MB, less than or equal)	false	integer
			updatedAt__between	Date range for update time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			updatedAt__gt	Agents updated after this timestamp	false	string
			updatedAt__gte	Agents updated after or at this timestamp	false	string
			updatedAt__lt	Agents updated	false	string

<table>
<tr><td></td><td></td><td></td><td><table>
<tr><td></td><td>before this timestamp</td><td></td><td></td></tr>
<tr><td>updatedAt__lte</td><td>Agents updated before or at this timestamp</td><td>false</td><td>string</td></tr>
<tr><td>userActionsNeeded</td><td>Included pending user actions</td><td>false</td><td>string []</td></tr>
<tr><td>userActionsNeededNin</td><td>Excluded pending user actions</td><td>false</td><td>string []</td></tr>
<tr><td>uuid</td><td>Agent's universally unique identifier</td><td>false</td><td>string</td></tr>
<tr><td>uuid__contains</td><td>Free-text filter by Agent UUID (supports multiple values)</td><td>false</td><td>string []</td></tr>
<tr><td>uuids</td><td>A list of included UUIDs</td><td>false</td><td>string []</td></tr>
</table></td></tr>
<tr><td>data</td><td>Data</td><td>false</td><td></td></tr>
</table>

Update Software

POST /web/api/v2.1/agents/actions/update-software

Use this command to update the Agent version on endpoints that have the Agent installed and that match the filter. For a cloud-based Management, SentinelOne updates your Management Console with the latest Agent versions. For On-Prem environments, or if you need a package that is not in your Management Console, request files from SentinelOne Support.
IMPORTANT: These parameters are required:
packageType - example: "packageType": "AgentAndRanger",osType - example: "osType": "windows",fileName - example: "fileName": "SentinelInstaller-x86_windows_32bit_v4_6_12_241.exe"
Best Practice: Upgrade your SentinelOne Agents by group or OS. Note about macOS endpoints: It is important that you upgrade the Agent before the endpoint operating system is upgraded to a version that the Agent does not support. More best practices: read the Release Notes, review the system requirements, and if you decide to not upgrade Agents yet, review the Agent Lifecycle. Make sure your deployment is in the supportable bounds.

BEST PRACTICE

Upgrade your SentinelOne Agents by group or OS. Note about macOS endpoints: It is important that you upgrade the Agent before the endpoint operating system is upgraded to a version that the Agent does not support. More best practices: read the Release Notes, review the system requirements, and if you decide to not upgrade Agents yet, review the Agent Lifecycle. Make sure your deployment is in the supportable bounds.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - User has insufficient permissions to perform the requested action

409 - The Agent is automatically upgraded according to its Upgrade Policy. Manually upgrading the Agent may cause conflicts

Response Schema

Name	Description	Required	Value
data	Response data	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>affected</td><td>Number of entities affected by</td><td>false</td><td>integer</td></tr></table>

			the requested operation
errors	Errors	false	array

Body Schema

Name	Description	Required	Value
data	Data	true	

Name	Description	Required	Value
allowDowngrade	Allows or disallows downgrading the Agent version	false	boolean
fileName	Upgrade with a given uploaded package, locate package by its filename	false	string
ignoreConflicts	Ignore conflicts that may arise when you upgrade an Agent that has an active Upgrade Policy	false	boolean
isScheduled	Upgrade according to the defined scheduled in agent upgrade configuration	false	boolean
osType	Filter by specific OS type, can be used in conjunction with "fileName" or "path"	false	enum
packageId	Upgrade with a given	false	string

			uploaded package, located package by its ID		
			packageType	Package type	false	enum
			path	Upgrade from local path at the endpoint	false	string
filter	Applied filter - only matched Agents will be affected by the requested action. Leave empty to apply the action on all applicable Agents.	true	Name	Description	Required	Value
			accountIds	List of Account IDs to filter by	false	string []
			activeThreats	Include Agents with this amount of active threats	false	integer
			activeThreats__gt	Include Agents with at least this amount of active threats	false	integer
			adComputerMember__contains	Free-text filter by Active Directory computer groups string (supports multiple values)	false	string []
			adComputerName__contains	Free-text filter by Active Directory computer name string (supports multiple values)	false	string []

			adComputerQuery__contains	Free-text filter by Active Directory computer name or its groups (supports multiple values)	false	string []
			adQuery	An Active Directory query string	false	string
			adQuery__contains	Free-text filter by Active Directory string (supports multiple values)	false	string []
			adUserMember__contains	Free-text filter by Active Directory user groups string (supports multiple values)	false	string []
			adUserName__contains	Free-text filter by Active Directory username string (supports multiple values)	false	string []
			adUserQuery__contains	Free-text filter by Active Directory computer	false	string []

				name or its groups (supports multiple values)		
			agentNamespace__contains	Free-text filter by agent namespace (supports multiple values)	false	string []
			agentPodName__contains	Free-text filter by agent pod name (supports multiple values)	false	string []
			agentVersion__between	Version range for agent version (format: <from_version>-<to_version>, inclusive)	false	string
			agentVersion__gt	Agents versions greater than given version	false	string
			agentVersion__gte	Agents versions greater than or equal to given version	false	string
			agentVersion__lt	Agents versions less than given version	false	string
			agentVersion__lte	Agents versions less than or equal to given version	false	string

			agentVersions	Agent versions to include	false	string []
			agentVersionsNin	Agent versions not to include	false	string []
			appsVulnerabilityStatuses	Apps vulnerability status in	false	string []
			appsVulnerabilityStatusesNin	Apps vulnerability status nin	false	string []
			awsRole__contains	Free-text filter by aws role(supports multiple values)	false	string []
			awsSecurityGroups__contains	Free-text filter by aws securityGroups(supports multiple values)	false	string []
			awsSubnetIds__contains	Free-text filter by aws subnet ids (supports multiple values)	false	string []
			azureResourceGroup__contains	Free-text filter by azure resource group(supports multiple values)	false	string []
			cloudAccount__contains	Free-text filter by cloud account (supports multiple values)	false	string []
			cloudImage__	Free-text	false	string []

			contains	filter by cloud image (supports multiple values)		
			cloudInstanceId__contains	Free-text filter by cloud instance id(supports multiple values)	false	string []
			cloudInstanceSize__contains	Free-text filter by cloud instance size(supports multiple values)	false	string []
			cloudLocation__contains	Free-text filter by cloud location (supports multiple values)	false	string []
			cloudNetwork__contains	Free-text filter by cloud network (supports multiple values)	false	string []
			cloudProvider	Agents from which cloud provider	false	string []
			cloudProviderNin	Exclude Agents from these cloud provider	false	string []
			cloudTags__contains	Free-text filter by cloud tags (supports multiple values)	false	string []

			clusterName__contains	Free-text filter by cluster name (supports multiple values)	false	string []
			computerName	Computer name	false	string
			computerName__contains	Free-text filter by computer name (supports multiple values)	false	string []
			computerName__like	Match computer name partially (substring)	false	string
			consoleMigrationStatuses	Migration status in	false	string []
			consoleMigrationStatusesNin	Migration status nin	false	string []
			coreCount__between	Possible number of CPU cores (inclusive)	false	string
			coreCount__gt	CPU cores (more than)	false	integer
			coreCount__gte	CPU cores (more than or equal)	false	integer
			coreCount__lt	CPU cores (less than)	false	integer
			coreCount__lte	CPU cores (less than or equal)	false	integer
			cpuCount__between	Possible number of	false	string

				CPU cores (inclusive)		
			cpuCount__gt	Number of CPUs (more than)	false	integer
			cpuCount__gte	Number of CPUs (more than or equal)	false	integer
			cpuCount__lt	Number of CPUs (less than)	false	integer
			cpuCount__lte	Number of CPUs (less than or equal)	false	integer
			cpuId__contains	Free-text filter by CPU name (supports multiple values)	false	string []
			createdAt__between	Date range for creation time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			createdAt__gt	Agents created after this timestamp	false	string
			createdAt__gte	Agents created after or at this timestamp	false	string
			createdAt__lt	Agents created before this timestamp	false	string
			createdAt__lte	Agents created	false	string

				before or at this timestamp		
			csvFilterId	The ID of the CSV file to filter by	false	string
			decommissionedAt__between	Date range for decommission time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			decommissionedAt__gt	Agents decommissioned after this timestamp	false	string
			decommissionedAt__gte	Agents decommissioned after or at this timestamp	false	string
			decommissionedAt__lt	Agents decommissioned before this timestamp	false	string
			decommissionedAt__lte	Agents decommissioned before this timestamp	false	string
			domains	Included network domains	false	string []
			domainsNin	Not included network domains	false	string []
			encryptedApplications	Disk encryption status	false	boolean
			externalId__c	Free-text	false	string []

			ontains	filter by external ID (Customer ID)		
			externalIp__contains	Free-text filter by visible IP (supports multiple values)	false	string []
			filteredGroupIds	List of Group IDs to filter by	false	string []
			filteredSiteIds	List of Site IDs to filter by	false	string []
			filterId	Include all Agents matching this saved filter	false	string
			firewallEnabled	The agents supports Firewall Control and it is enabled for the agent's group	false	boolean []
			gatewayIp	Gateway ip	false	string
			gcpServiceAccount__contains	Free-text filter by gcp service account (supports multiple values)	false	string []
			groupIds	List of Group IDs to filter by	false	string []
			hasContainerizedWorkload	Include only Agents protecting containerized workloads	false	boolean

			hasLocalConfiguration	Agent has a local configuration set	false	boolean
			hasTags	Include only Agents that have any tags assigned if True, or none if False	false	boolean
			ids	A list of Agent IDs	false	string []
			infected	Include only Agents with at least one active threat	false	boolean
			installerTypes	Include only Agents installed with these package types	false	string []
			installerTypesNin	Exclude Agents installed with these package types	false	string []
			isActive	Include only active Agents	false	boolean
			isDecommissioned	Include active, decommissioned or both	false	boolean []
			isPendingUninstall	Include only Agents with pending uninstall requests	false	boolean
			isUninstalled	Include installed, uninstalled or	false	boolean []

				both		
			isUpToDate	Include only Agents with updated software	false	boolean
			k8sNodeLabels__contains	Free-text filter by K8s node labels (supports multiple values)	false	string []
			k8sNodeName__contains	Free-text filter by K8s node name (supports multiple values)	false	string []
			k8sType__contains	Free-text filter by K8s type(supports multiple values)	false	string []
			k8sVersion__contains	Free-text filter by K8s version (supports multiple values)	false	string []
			lastActiveDate__between	Date range for last active date(format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			lastActiveDate__gt	Agents last active after this time	false	string
			lastActiveDate__gte	Agents last active after or at this time	false	string
			lastActiveDat	Agents last	false	string

			e__lt	active before this time		
			lastActiveDate__lte	Agents last active before or at this time	false	string
			lastLoggedInUserName__contains	Free-text filter by username (supports multiple values)	false	string []
			lastSuccessfulScanDate__between	Date range for last successful full disk scan(format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			lastSuccessfulScanDate__gt	Agents last successful full disk scan after this time	false	string
			lastSuccessfulScanDate__gte	Agents last successful full disk scan after or at this time	false	string
			lastSuccessfulScanDate__lt	Agents last successful full disk scan before this time	false	string
			lastSuccessfulScanDate__lte	Agents last successful full disk scan before or at this time	false	string
			liveUpdateId__contains	Free-text filter by live	false	string []

				update ID (supports multiple values)		
			locationEnabled	The agents supports Location Awareness and it is enabled for the agent's group	false	boolean []
			locationIds	Include only Agents reporting these locations	false	string []
			locationIdsNin	Do not include only Agents reporting these locations	false	string []
			machineTypes	Included machine types	false	string []
			machineTypesNin	Not included machine types	false	string []
			migrationStatus	Migration status	false	enum
			missingPermissions	Included missing permissions	false	string []
			missingPermissionsNin	Excluded missing permissions	false	string []
			mitigationMode	Agent mitigation mode policy	false	enum
			mitigationMo	Mitigation	false	enum

			deSuspicious	mode policy for suspicious activity		
			networkInterfaceGatewayMacAddress__contains	Free-text filter by Gateway MAC address (supports multiple values)	false	string []
			networkInterfacelnet__contains	Free-text filter by local IP (supports multiple values)	false	string []
			networkInterfacePhysical__contains	Free-text filter by MAC address (supports multiple values)	false	string []
			networkQuarantineEnabled	The agents supports Network Quarantine Control and its enabled for the agent's group	false	boolean []
			networkStatuses	Included network statuses	false	string []
			networkStatusesNin	Included network statuses	false	string []
			operationalStates	Agent operational state	false	string []
			operationalStatesNin	Do not include these Agent operational	false	string []

				states		
			osArch	OS architecture	false	enum
			osTypes	Included OS types	false	string []
			osTypesNin	Not included OS types	false	string []
			osVersion__contains	Free-text filter by OS full name and version (supports multiple values)	false	string []
			query	A free-text search term, will match applicable attributes (sub-string match). Note: Device's physical addresses will be matched if they start with the search term only (no match if they contain the term).	false	string
			rangerStatus	[DEPRECATED] Use rangerStatuses.	false	enum
			rangerStatuses	Status of Ranger	false	string []
			rangerStatusesNin	Do not include these Ranger Statuses	false	string []

			rangerVersions	Ranger versions to include	false	string []
			rangerVersionsNin	Ranger versions not to include	false	string []
			registeredAt__between	Date range for first registration time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			registeredAt__gt	Agents registered after this time	false	string
			registeredAt__gte	Agents registered after or at this time	false	string
			registeredAt__lt	Agents registered before this time	false	string
			registeredAt__lte	Agents registered before or at this time	false	string
			remoteOpsForensicsSupported	Include only agents that has Remote Ops Forensicsfeature supported	false	boolean
			remoteProfilingStates	Agent remote profiling state	false	string []
			remoteProfilingStatesNin	Do not include these Agent remote	false	string []

				profiling states		
			rsoLevel	Supported Remote Script Orchestration level	false	enum
			scanStatus	Scan status	false	enum
			scanStatuses	Included scan statuses	false	string []
			scanStatuses Nin	Not included scan statuses	false	string []
			serialNumber __contains	Free-text filter by Serial Number (supports multiple values)	false	string []
			siteIds	List of Site IDs to filter by	false	string []
			tagsData	Filter agents by their assigned tags. Given in form of a JSON where each key represents a tag key, and each value represents a list of string values to filter by. To filter by unassigned tag values, use __nin suffix in the tag key.	false	string
			threatConten	Include only	false	string

			tHash	Agents that have at least one threat with this content hash		
			threatCreatedAt__between	Agents with threats reported in a date range (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			threatCreatedAt__gt	Agents with threats reported after this time	false	string
			threatCreatedAt__gte	Agents with threats reported after or at this time	false	string
			threatCreatedAt__lt	Agents with threats reported before this time	false	string
			threatCreatedAt__lte	Agents with threats reported before or at this time	false	string
			threatHidden	Include only Agents with at least one hidden threat	false	boolean
			threatMitigationStatus	Include only Agents that have threats with this mitigation	false	enum

				status		
			threatRebootRequired	Has at least one threat with at least one mitigation action pending reboot to succeed	false	boolean []
			threatResolved	Include only Agents with at least one resolved threat	false	boolean
			totalMemory__between	Total memory range (GB, inclusive)	false	string
			totalMemory__gt	Memory size (MB, more than)	false	integer
			totalMemory__gte	Memory size (MB, more than or equal)	false	integer
			totalMemory__lt	Memory size (MB, less than)	false	integer
			totalMemory__lte	Memory size (MB, less than or equal)	false	integer
			updatedAt__between	Date range for update time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			updatedAt__gt	Agents updated after this timestamp	false	string

			updatedAt__gte	Agents updated after or at this timestamp	false	string
			updatedAt__lt	Agents updated before this timestamp	false	string
			updatedAt__lte	Agents updated before or at this timestamp	false	string
			userActionsNeeded	Included pending user actions	false	string []
			userActionsNeededNin	Excluded pending user actions	false	string []
			uuid	Agent's universally unique identifier	false	string
			uuid__contains	Free-text filter by Agent UUID (supports multiple values)	false	string []
			uuids	A list of included UUIDs	false	string []

Reset Local Config

POST /web/api/v2.1/agents/actions/reset-local-config

SentinelCtl is the CLI for Agents. It runs commands directly on one Agent at a time. You can use this command to clear the SentinelCtl changes from all Agents that match the filter. Specific SentinelCtl settings are not cleared:
On Windows: proxy address and Management token.
On macOC: Management server address and server site key.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - User has insufficient permissions to perform the requested action

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>affected</td><td>Number of entities affected by the requested operation</td><td>false</td><td>integer</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>filter</td><td>Applied filter - only matched Agents will be affected by the requested action. Leave empty to apply the action on all applicable Agents.</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>activeThreats</td><td>Include Agents with this amount of active threats</td><td>false</td><td>integer</td></tr>
<tr><td>activeThreats__gt</td><td>Include Agents with at least this amount of active threats</td><td>false</td><td>integer</td></tr>
<tr><td>adComputerMember__contains</td><td>Free-text filter by Active Directory computer groups string (supports multiple values)</td><td>false</td><td>string []</td></tr>
<tr><td>adComputerName__contains</td><td>Free-text filter by Active Directory computer name string (supports multiple values)</td><td>false</td><td>string []</td></tr>
<tr><td>adComputerQuery__contains</td><td>Free-text filter by Active Directory computer name or its groups</td><td>false</td><td>string []</td></tr>
</table>
</td></tr>
</table>

				(supports multiple values)		
			adQuery	An Active Directory query string	false	string
			adQuery__contains	Free-text filter by Active Directory string (supports multiple values)	false	string []
			adUserMember__contains	Free-text filter by Active Directory user groups string (supports multiple values)	false	string []
			adUserName__contains	Free-text filter by Active Directory username string (supports multiple values)	false	string []
			adUserQuery__contains	Free-text filter by Active Directory computer name or its groups (supports multiple values)	false	string []
			agentNamespa	Free-text	false	string []

			ce__contains	filter by agent namespace (supports multiple values)		
			agentPodName__contains	Free-text filter by agent pod name (supports multiple values)	false	string []
			agentVersion__between	Version range for agent version (format: <from_version>-<to_version>, inclusive)	false	string
			agentVersion__gt	Agents versions greater than given version	false	string
			agentVersion__gte	Agents versions greater than or equal to given version	false	string
			agentVersion__lt	Agents versions less than given version	false	string
			agentVersion__lte	Agents versions less than or equal to given version	false	string
			agentVersions	Agent versions to include	false	string []
			agentVersionsNin	Agent versions not	false	string []

				to include		
			appsVulnerabilityStatuses	Apps vulnerability status in	false	string []
			appsVulnerabilityStatusesNin	Apps vulnerability status nin	false	string []
			awsRole__contains	Free-text filter by aws role(supports multiple values)	false	string []
			awsSecurityGroups__contains	Free-text filter by aws securityGroups(supports multiple values)	false	string []
			awsSubnetIds__contains	Free-text filter by aws subnet ids (supports multiple values)	false	string []
			azureResourceGroup__contains	Free-text filter by azure resource group(supports multiple values)	false	string []
			cloudAccount__contains	Free-text filter by cloud account (supports multiple values)	false	string []
			cloudImage__contains	Free-text filter by cloud image (supports multiple values)	false	string []

			cloudInstanceId__contains	Free-text filter by cloud instance id(supports multiple values)	false	string []
			cloudInstanceSize__contains	Free-text filter by cloud instance size(supports multiple values)	false	string []
			cloudLocation__contains	Free-text filter by cloud location (supports multiple values)	false	string []
			cloudNetwork__contains	Free-text filter by cloud network (supports multiple values)	false	string []
			cloudProvider	Agents from which cloud provider	false	string []
			cloudProviderNin	Exclude Agents from these cloud provider	false	string []
			cloudTags__contains	Free-text filter by cloud tags (supports multiple values)	false	string []
			clusterName__contains	Free-text filter by cluster name (supports multiple values)	false	string []

			computerName	Computer name	false	string
			computerName__contains	Free-text filter by computer name (supports multiple values)	false	string []
			computerName__like	Match computer name partially (substring)	false	string
			consoleMigrationStatuses	Migration status in	false	string []
			consoleMigrationStatusesNin	Migration status nin	false	string []
			coreCount__between	Possible number of CPU cores (inclusive)	false	string
			coreCount__gt	CPU cores (more than)	false	integer
			coreCount__gte	CPU cores (more than or equal)	false	integer
			coreCount__lt	CPU cores (less than)	false	integer
			coreCount__lte	CPU cores (less than or equal)	false	integer
			cpuCount__between	Possible number of CPU cores (inclusive)	false	string
			cpuCount__gt	Number of CPUs (more than)	false	integer

			cpuCount__gte	Number of CPUs (more than or equal)	false	integer
			cpuCount__lt	Number of CPUs (less than)	false	integer
			cpuCount__lte	Number of CPUs (less than or equal)	false	integer
			cpuId__contains	Free-text filter by CPU name (supports multiple values)	false	string []
			createdAt__between	Date range for creation time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			createdAt__gt	Agents created after this timestamp	false	string
			createdAt__gte	Agents created after or at this timestamp	false	string
			createdAt__lt	Agents created before this timestamp	false	string
			createdAt__lte	Agents created before or at this timestamp	false	string
			csvFilterId	The ID of the CSV file to filter by	false	string

			decommissionedAt__between	Date range for decommission time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			decommissionedAt__gt	Agents decommissioned after this timestamp	false	string
			decommissionedAt__gte	Agents decommissioned after or at this timestamp	false	string
			decommissionedAt__lt	Agents decommissioned before this timestamp	false	string
			decommissionedAt__lte	Agents decommissioned before this timestamp	false	string
			domains	Included network domains	false	string []
			domainsNin	Not included network domains	false	string []
			encryptedApplications	Disk encryption status	false	boolean
			externalId__contains	Free-text filter by external ID (Customer ID)	false	string []
			externalIp__contains	Free-text filter by visible IP (supports	false	string []

				multiple values)		
			filteredGroupIds	List of Group IDs to filter by	false	string []
			filteredSiteIds	List of Site IDs to filter by	false	string []
			filterId	Include all Agents matching this saved filter	false	string
			firewallEnabled	The agents supports Firewall Control and it is enabled for the agent's group	false	boolean []
			gatewayIp	Gateway ip	false	string
			gcpServiceAccount__contains	Free-text filter by gcp service account (supports multiple values)	false	string []
			groupIds	List of Group IDs to filter by	false	string []
			hasContainerizedWorkload	Include only Agents protecting containerized workloads	false	boolean
			hasLocalConfiguration	Agent has a local configuration set	false	boolean
			hasTags	Include only Agents that	false	boolean

				have any tags assigned if True, or none if False		
			ids	A list of Agent IDs	false	string []
			infected	Include only Agents with at least one active threat	false	boolean
			installerTypes	Include only Agents installed with these package types	false	string []
			installerTypesNin	Exclude Agents installed with these package types	false	string []
			isActive	Include only active Agents	false	boolean
			isDecommissioned	Include active, decommissioned or both	false	boolean []
			isPendingUninstall	Include only Agents with pending uninstall requests	false	boolean
			isUninstalled	Include installed, uninstalled or both	false	boolean []
			isUpToDate	Include only Agents with updated software	false	boolean

			k8sNodeLabels__contains	Free-text filter by K8s node labels (supports multiple values)	false	string []
			k8sNodeName__contains	Free-text filter by K8s node name (supports multiple values)	false	string []
			k8sType__contains	Free-text filter by K8s type(supports multiple values)	false	string []
			k8sVersion__contains	Free-text filter by K8s version (supports multiple values)	false	string []
			lastActiveDate__between	Date range for last active date(format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			lastActiveDate__gt	Agents last active after this time	false	string
			lastActiveDate__gte	Agents last active after or at this time	false	string
			lastActiveDate__lt	Agents last active before this time	false	string
			lastActiveDate__lte	Agents last active before or at this time	false	string

			lastLoggedInUserName__contains	Free-text filter by username (supports multiple values)	false	string []
			lastSuccessfulScanDate__between	Date range for last successful full disk scan(format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			lastSuccessfulScanDate__gt	Agents last successful full disk scan after this time	false	string
			lastSuccessfulScanDate__gte	Agents last successful full disk scan after or at this time	false	string
			lastSuccessfulScanDate__lt	Agents last successful full disk scan before this time	false	string
			lastSuccessfulScanDate__lte	Agents last successful full disk scan before or at this time	false	string
			liveUpdateId__contains	Free-text filter by live update ID (supports multiple values)	false	string []
			locationEnabled	The agents supports	false	boolean []

				Location Awareness and it is enabled for the agent's group		
			locationIds	Include only Agents reporting these locations	false	string []
			locationIdsNin	Do not include only Agents reporting these locations	false	string []
			machineTypes	Included machine types	false	string []
			machineTypesNin	Not included machine types	false	string []
			migrationStatus	Migration status	false	enum
			missingPermissions	Included missing permissions	false	string []
			missingPermissionsNin	Excluded missing permissions	false	string []
			mitigationMode	Agent mitigation mode policy	false	enum
			mitigationModeSuspicious	Mitigation mode policy for suspicious activity	false	enum
			networkInterfaceGatewayMacAddress__c	Free-text filter by Gateway	false	string []

			ontains	MAC address (supports multiple values)		
			networkInterfaceInet__contains	Free-text filter by local IP (supports multiple values)	false	string []
			networkInterfacePhysical__contains	Free-text filter by MAC address (supports multiple values)	false	string []
			networkQuarantineEnabled	The agents supports Network Quarantine Control and its enabled for the agent's group	false	boolean []
			networkStatuses	Included network statuses	false	string []
			networkStatusesNin	Included network statuses	false	string []
			operationalStates	Agent operational state	false	string []
			operationalStatesNin	Do not include these Agent operational states	false	string []
			osArch	OS architecture	false	enum
			osTypes	Included OS types	false	string []

			osTypesNin	Not included OS types	false	string []
			osVersion__contains	Free-text filter by OS full name and version (supports multiple values)	false	string []
			query	A free-text search term, will match applicable attributes (sub-string match). Note: Device's physical addresses will be matched if they start with the search term only (no match if they contain the term).	false	string
			rangerStatus	[DEPRECATED] Use rangerStatuses.	false	enum
			rangerStatuses	Status of Ranger	false	string []
			rangerStatusesNin	Do not include these Ranger Statuses	false	string []
			rangerVersions	Ranger versions to include	false	string []
			rangerVersionsNin	Ranger versions not to include	false	string []

			registeredAt__between	Date range for first registration time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			registeredAt__gt	Agents registered after this time	false	string
			registeredAt__gte	Agents registered after or at this time	false	string
			registeredAt__lt	Agents registered before this time	false	string
			registeredAt__lte	Agents registered before or at this time	false	string
			remoteOpsForensicsSupported	Include only agents that has Remote Ops Forensicsfeature supported	false	boolean
			remoteProfilingStates	Agent remote profiling state	false	string []
			remoteProfilingStatesNin	Do not include these Agent remote profiling states	false	string []
			rsoLevel	Supported Remote Script Orchestration	false	enum

				level		
			scanStatus	Scan status	false	enum
			scanStatuses	Included scan statuses	false	string []
			scanStatuses Nin	Not included scan statuses	false	string []
			serialNumber __contains	Free-text filter by Serial Number (supports multiple values)	false	string []
			siteIds	List of Site IDs to filter by	false	string []
			tagsData	Filter agents by their assigned tags. Given in form of a JSON where each key represents a tag key, and each value represents a list of string values to filter by. To filter by unassigned tag values, use __nin suffix in the tag key.	false	string
			threatConten tHash	Include only Agents that have at least one threat with this content hash	false	string
			threatCreate	Agents with	false	string

			dAt__between	threats reported in a date range (format: <from_timestamp>-<to_timestamp>, inclusive)		
			threatCreatedAt__gt	Agents with threats reported after this time	false	string
			threatCreatedAt__gte	Agents with threats reported after or at this time	false	string
			threatCreatedAt__lt	Agents with threats reported before this time	false	string
			threatCreatedAt__lte	Agents with threats reported before or at this time	false	string
			threatHidden	Include only Agents with at least one hidden threat	false	boolean
			threatMitigationStatus	Include only Agents that have threats with this mitigation status	false	enum
			threatRebootRequired	Has at least one threat with at least one mitigation	false	boolean []

				action pending reboot to succeed		
			threatResolved	Include only Agents with at least one resolved threat	false	boolean
			totalMemory__between	Total memory range (GB, inclusive)	false	string
			totalMemory__gt	Memory size (MB, more than)	false	integer
			totalMemory__gte	Memory size (MB, more than or equal)	false	integer
			totalMemory__lt	Memory size (MB, less than)	false	integer
			totalMemory__lte	Memory size (MB, less than or equal)	false	integer
			updatedAt__between	Date range for update time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			updatedAt__gt	Agents updated after this timestamp	false	string
			updatedAt__gte	Agents updated after or at this timestamp	false	string
			updatedAt__lt	Agents updated	false	string

			before this timestamp		
	updatedAt__lte	Agents updated before or at this timestamp	false	string
	userActionsNeeded	Included pending user actions	false	string []
	userActionsNeededNin	Excluded pending user actions	false	string []
	uuid	Agent's universally unique identifier	false	string
	uuid__contains	Free-text filter by Agent UUID (supports multiple values)	false	string []
	uuids	A list of included UUIDs	false	string []
data	Data	false	

Set Persistent Configuration Overrides

POST /web/api/v2.1/agents/actions/set-config

This command requires Global permissions or Support.
The configuration of an Agent can be changed in different ways, such as through Policy settings, Policy Override, SentinelCtl, and changes to the LocalConfig.json file.
For Windows, Policy Override overwrites policy settings, and local changes (to the file and from this command) overwrite Policy Override from the Console or with policy updates from the API.
For macOS, the Policy Override has the highest priority. If you run this command and then update a Group policy that affects both Windows and macOS endpoints, the settings of this command are applied to the Windows endpoints. But the macOS endpoints will apply the settings of the policy, for settings that are duplicated in both the policy and this command.
When you use this command, enter the filter values to set which Agents get the change. Then use the data parameter to set the actual changes. Get the JSON settings for data from the Agent Configuration or see the Knowledge Base: https://support.sentinelone.com/hc/en-us/articles/360022158673-sentinelctl

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - User has insufficient permissions to perform the requested action

Response Schema

Name	Description	Required	Value
data	Response data	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>affected</td><td>Number of entities affected by the requested operation</td><td>false</td><td>integer</td></tr></table>
errors	Errors	false	array

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>config</td><td>Config</td><td>false</td><td>object</td></tr>
</table>
</td></tr>
<tr><td>filter</td><td>Applied filter - only matched Agents will be affected by the requested action. Leave empty to apply the action on all applicable Agents.</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>activeThreats</td><td>Include Agents with this amount of active threats</td><td>false</td><td>integer</td></tr>
<tr><td>activeThreats__gt</td><td>Include Agents with at least this amount of active threats</td><td>false</td><td>integer</td></tr>
<tr><td>adComputerMember__contains</td><td>Free-text filter by Active Directory computer groups string (supports multiple values)</td><td>false</td><td>string []</td></tr>
<tr><td>adComputerName__contains</td><td>Free-text filter by Active Directory computer name string (supports multiple values)</td><td>false</td><td>string []</td></tr>
<tr><td>adComputerQuery__contains</td><td>Free-text filter by Active</td><td>false</td><td>string []</td></tr>
</table>
</td></tr>
</table>

				Directory computer name or its groups (supports multiple values)		
			adQuery	An Active Directory query string	false	string
			adQuery__contains	Free-text filter by Active Directory string (supports multiple values)	false	string []
			adUserMember__contains	Free-text filter by Active Directory user groups string (supports multiple values)	false	string []
			adUserName__contains	Free-text filter by Active Directory username string (supports multiple values)	false	string []
			adUserQuery__contains	Free-text filter by Active Directory computer name or its groups (supports	false	string []

				multiple values)		
			agentNamespace__contains	Free-text filter by agent namespace (supports multiple values)	false	string []
			agentPodName__contains	Free-text filter by agent pod name (supports multiple values)	false	string []
			agentVersion__between	Version range for agent version (format: <from_version>-<to_version>, inclusive)	false	string
			agentVersion__gt	Agents versions greater than given version	false	string
			agentVersion__gte	Agents versions greater than or equal to given version	false	string
			agentVersion__lt	Agents versions less than given version	false	string
			agentVersion__lte	Agents versions less than or equal to given version	false	string
			agentVersions	Agent versions to	false	string []

				include		
			agentVersionsNin	Agent versions not to include	false	string []
			appsVulnerabilityStatuses	Apps vulnerability status in	false	string []
			appsVulnerabilityStatusesNin	Apps vulnerability status nin	false	string []
			awsRole__contains	Free-text filter by aws role(supports multiple values)	false	string []
			awsSecurityGroups__contains	Free-text filter by aws securityGroups(supports multiple values)	false	string []
			awsSubnetIds__contains	Free-text filter by aws subnet ids (supports multiple values)	false	string []
			azureResourceGroup__contains	Free-text filter by azure resource group(supports multiple values)	false	string []
			cloudAccount__contains	Free-text filter by cloud account (supports multiple values)	false	string []
			cloudImage__contains	Free-text filter by cloud image	false	string []

				(supports multiple values)		
			cloudInstanceId__contains	Free-text filter by cloud instance id(supports multiple values)	false	string []
			cloudInstanceSize__contains	Free-text filter by cloud instance size(supports multiple values)	false	string []
			cloudLocation__contains	Free-text filter by cloud location (supports multiple values)	false	string []
			cloudNetwork__contains	Free-text filter by cloud network (supports multiple values)	false	string []
			cloudProvider	Agents from which cloud provider	false	string []
			cloudProviderNin	Exclude Agents from these cloud provider	false	string []
			cloudTags__contains	Free-text filter by cloud tags (supports multiple values)	false	string []
			clusterName__contains	Free-text filter by	false	string []

				cluster name (supports multiple values)		
			computerName	Computer name	false	string
			computerName__contains	Free-text filter by computer name (supports multiple values)	false	string []
			computerName__like	Match computer name partially (substring)	false	string
			consoleMigrationStatuses	Migration status in	false	string []
			consoleMigrationStatusesNin	Migration status nin	false	string []
			coreCount__between	Possible number of CPU cores (inclusive)	false	string
			coreCount__gt	CPU cores (more than)	false	integer
			coreCount__gte	CPU cores (more than or equal)	false	integer
			coreCount__lt	CPU cores (less than)	false	integer
			coreCount__lte	CPU cores (less than or equal)	false	integer
			cpuCount__between	Possible number of CPU cores (inclusive)	false	string

			cpuCount__gt	Number of CPUs (more than)	false	integer
			cpuCount__gte	Number of CPUs (more than or equal)	false	integer
			cpuCount__lt	Number of CPUs (less than)	false	integer
			cpuCount__lte	Number of CPUs (less than or equal)	false	integer
			cpuId__contains	Free-text filter by CPU name (supports multiple values)	false	string []
			createdAt__between	Date range for creation time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			createdAt__gt	Agents created after this timestamp	false	string
			createdAt__gte	Agents created after or at this timestamp	false	string
			createdAt__lt	Agents created before this timestamp	false	string
			createdAt__lte	Agents created before or at this timestamp	false	string

			csvFilterId	The ID of the CSV file to filter by	false	string
			decommissionedAt__between	Date range for decommission time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			decommissionedAt__gt	Agents decommissioned after this timestamp	false	string
			decommissionedAt__gte	Agents decommissioned after or at this timestamp	false	string
			decommissionedAt__lt	Agents decommissioned before this timestamp	false	string
			decommissionedAt__lte	Agents decommissioned before this timestamp	false	string
			domains	Included network domains	false	string []
			domainsNin	Not included network domains	false	string []
			encryptedApplications	Disk encryption status	false	boolean
			externalId__contains	Free-text filter by external ID (Customer ID)	false	string []

			externalIp__contains	Free-text filter by visible IP (supports multiple values)	false	string []
			filteredGroupIds	List of Group IDs to filter by	false	string []
			filteredSiteIds	List of Site IDs to filter by	false	string []
			filterId	Include all Agents matching this saved filter	false	string
			firewallEnabled	The agents supports Firewall Control and it is enabled for the agent's group	false	boolean []
			gatewayIp	Gateway ip	false	string
			gcpServiceAccount__contains	Free-text filter by gcp service account (supports multiple values)	false	string []
			groupIds	List of Group IDs to filter by	false	string []
			hasContainerizedWorkload	Include only Agents protecting containerized workloads	false	boolean
			hasLocalConfiguration	Agent has a local configuration	false	boolean

				set		
			hasTags	Include only Agents that have any tags assigned if True, or none if False	false	boolean
			ids	A list of Agent IDs	false	string []
			infected	Include only Agents with at least one active threat	false	boolean
			installerTypes	Include only Agents installed with these package types	false	string []
			installerTypesNin	Exclude Agents installed with these package types	false	string []
			isActive	Include only active Agents	false	boolean
			isDecommissioned	Include active, decommissioned or both	false	boolean []
			isPendingUninstall	Include only Agents with pending uninstall requests	false	boolean
			isUninstalled	Include installed, uninstalled or both	false	boolean []
			isUpToDate	Include only	false	boolean

				Agents with updated software		
			k8sNodeLabels__contains	Free-text filter by K8s node labels (supports multiple values)	false	string []
			k8sNodeName__contains	Free-text filter by K8s node name (supports multiple values)	false	string []
			k8sType__contains	Free-text filter by K8s type(supports multiple values)	false	string []
			k8sVersion__contains	Free-text filter by K8s version (supports multiple values)	false	string []
			lastActiveDate__between	Date range for last active date(format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			lastActiveDate__gt	Agents last active after this time	false	string
			lastActiveDate__gte	Agents last active after or at this time	false	string
			lastActiveDate__lt	Agents last active before this time	false	string

			lastActiveDate__lte	Agents last active before or at this time	false	string
			lastLoggedInUserName__contains	Free-text filter by username (supports multiple values)	false	string []
			lastSuccessfulScanDate__between	Date range for last successful full disk scan(format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			lastSuccessfulScanDate__gt	Agents last successful full disk scan after this time	false	string
			lastSuccessfulScanDate__gte	Agents last successful full disk scan after or at this time	false	string
			lastSuccessfulScanDate__lt	Agents last successful full disk scan before this time	false	string
			lastSuccessfulScanDate__lte	Agents last successful full disk scan before or at this time	false	string
			liveUpdateId__contains	Free-text filter by live update ID (supports multiple	false	string []

				values)		
			locationEnabled	The agents supports Location Awareness and it is enabled for the agent's group	false	boolean []
			locationIds	Include only Agents reporting these locations	false	string []
			locationIdsNin	Do not include only Agents reporting these locations	false	string []
			machineTypes	Included machine types	false	string []
			machineTypesNin	Not included machine types	false	string []
			migrationStatus	Migration status	false	enum
			missingPermissions	Included missing permissions	false	string []
			missingPermissionsNin	Excluded missing permissions	false	string []
			mitigationMode	Agent mitigation mode policy	false	enum
			mitigationModeSuspicious	Mitigation mode policy for suspicious activity	false	enum

			networkInterfaceGatewayMacAddress__contains	Free-text filter by Gateway MAC address (supports multiple values)	false	string []
			networkInterfaceInet__contains	Free-text filter by local IP (supports multiple values)	false	string []
			networkInterfacePhysical__contains	Free-text filter by MAC address (supports multiple values)	false	string []
			networkQuarantineEnabled	The agents supports Network Quarantine Control and its enabled for the agent's group	false	boolean []
			networkStatuses	Included network statuses	false	string []
			networkStatusesNin	Included network statuses	false	string []
			operationalStates	Agent operational state	false	string []
			operationalStatesNin	Do not include these Agent operational states	false	string []
			osArch	OS architecture	false	enum

			osTypes	Included OS types	false	string []
			osTypesNin	Not included OS types	false	string []
			osVersion__contains	Free-text filter by OS full name and version (supports multiple values)	false	string []
			query	A free-text search term, will match applicable attributes (sub-string match). Note: Device's physical addresses will be matched if they start with the search term only (no match if they contain the term).	false	string
			rangerStatus	[DEPRECATED] Use rangerStatuses.	false	enum
			rangerStatuses	Status of Ranger	false	string []
			rangerStatusesNin	Do not include these Ranger Statuses	false	string []
			rangerVersions	Ranger versions to include	false	string []

			rangerVersionsNin	Ranger versions not to include	false	string []
			registeredAt__between	Date range for first registration time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			registeredAt__gt	Agents registered after this time	false	string
			registeredAt__gte	Agents registered after or at this time	false	string
			registeredAt__lt	Agents registered before this time	false	string
			registeredAt__lte	Agents registered before or at this time	false	string
			remoteOpsForensicsSupported	Include only agents that has Remote Ops Forensicsfeature supported	false	boolean
			remoteProfilingStates	Agent remote profiling state	false	string []
			remoteProfilingStatesNin	Do not include these Agent remote profiling states	false	string []
			rsoLevel	Supported	false	enum

				Remote Script Orchestration level		
			scanStatus	Scan status	false	enum
			scanStatuses	Included scan statuses	false	string []
			scanStatuses Nin	Not included scan statuses	false	string []
			serialNumber __contains	Free-text filter by Serial Number (supports multiple values)	false	string []
			siteIds	List of Site IDs to filter by	false	string []
			tagsData	Filter agents by their assigned tags. Given in form of a JSON where each key represents a tag key, and each value represents a list of string values to filter by. To filter by unassigned tag values, use __nin suffix in the tag key.	false	string
			threatConten tHash	Include only Agents that have at least one threat with this	false	string

				content hash		
			threatCreatedAt__between	Agents with threats reported in a date range (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			threatCreatedAt__gt	Agents with threats reported after this time	false	string
			threatCreatedAt__gte	Agents with threats reported after or at this time	false	string
			threatCreatedAt__lt	Agents with threats reported before this time	false	string
			threatCreatedAt__lte	Agents with threats reported before or at this time	false	string
			threatHidden	Include only Agents with at least one hidden threat	false	boolean
			threatMitigationStatus	Include only Agents that have threats with this mitigation status	false	enum
			threatRebootRequired	Has at least one threat	false	boolean []

				with at least one mitigation action pending reboot to succeed		
			threatResolved	Include only Agents with at least one resolved threat	false	boolean
			totalMemory__between	Total memory range (GB, inclusive)	false	string
			totalMemory__gt	Memory size (MB, more than)	false	integer
			totalMemory__gte	Memory size (MB, more than or equal)	false	integer
			totalMemory__lt	Memory size (MB, less than)	false	integer
			totalMemory__lte	Memory size (MB, less than or equal)	false	integer
			updatedAt__between	Date range for update time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			updatedAt__gt	Agents updated after this timestamp	false	string
			updatedAt__gte	Agents updated after or at this timestamp	false	string

			updatedAt__lt	Agents updated before this timestamp	false	string
			updatedAt__lte	Agents updated before or at this timestamp	false	string
			userActionsNeeded	Included pending user actions	false	string []
			userActionsNeededNin	Excluded pending user actions	false	string []
			uuid	Agent's universally unique identifier	false	string
			uuid__contains	Free-text filter by Agent UUID (supports multiple values)	false	string []
			uuids	A list of included UUIDs	false	string []

Set External ID

POST /web/api/v2.1/agents/actions/set-external-id

You can add a Customer Identifier (a string) to identify each endpoint or to tag sets of endpoints. The string shows in the Endpoint Details of the Management Console. For example, you can tag endpoints based on their state, installed applications, or endpoint status. The identifier is set on all Agents that match the filter.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - User has insufficient permissions to perform the requested action

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>affected</td><td>Number of entities affected by the requested operation</td><td>false</td><td>integer</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>externalId</td><td>New external id for the agent</td><td>true</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>filter</td><td>Applied filter - only matched Agents will be affected by the requested action.</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>activeThreats</td><td>Include Agents with this amount of active threats</td><td>false</td><td>integer</td></tr>
<tr><td>activeThreats__gt</td><td>Include Agents with at least this amount of active threats</td><td>false</td><td>integer</td></tr>
<tr><td>adComputerMember__contains</td><td>Free-text filter by Active Directory computer groups string (supports multiple values)</td><td>false</td><td>string []</td></tr>
<tr><td>adComputerName__contains</td><td>Free-text filter by Active Directory computer name string (supports multiple values)</td><td>false</td><td>string []</td></tr>
<tr><td>adComputerQ</td><td>Free-text</td><td>false</td><td>string []</td></tr>
</table>
</td></tr>
</table>

			uery__contains	filter by Active Directory computer name or its groups (supports multiple values)		
			adQuery	An Active Directory query string	false	string
			adQuery__contains	Free-text filter by Active Directory string (supports multiple values)	false	string []
			adUserMember__contains	Free-text filter by Active Directory user groups string (supports multiple values)	false	string []
			adUserName__contains	Free-text filter by Active Directory username string (supports multiple values)	false	string []
			adUserQuery__contains	Free-text filter by Active Directory computer name or its	false	string []

				groups (supports multiple values)		
			agentNamespace__contains	Free-text filter by agent namespace (supports multiple values)	false	string []
			agentPodName__contains	Free-text filter by agent pod name (supports multiple values)	false	string []
			agentVersion__between	Version range for agent version (format: <from_version>-<to_version>, inclusive)	false	string
			agentVersion__gt	Agents versions greater than given version	false	string
			agentVersion__gte	Agents versions greater than or equal to given version	false	string
			agentVersion__lt	Agents versions less than given version	false	string
			agentVersion__lte	Agents versions less than or equal to given version	false	string

			agentVersions	Agent versions to include	false	string []
			agentVersionsNin	Agent versions not to include	false	string []
			appsVulnerabilityStatuses	Apps vulnerability status in	false	string []
			appsVulnerabilityStatusesNin	Apps vulnerability status nin	false	string []
			awsRole__contains	Free-text filter by aws role(supports multiple values)	false	string []
			awsSecurityGroups__contains	Free-text filter by aws securityGroups(supports multiple values)	false	string []
			awsSubnetIds__contains	Free-text filter by aws subnet ids (supports multiple values)	false	string []
			azureResourceGroup__contains	Free-text filter by azure resource group(supports multiple values)	false	string []
			cloudAccount__contains	Free-text filter by cloud account (supports multiple values)	false	string []
			cloudImage__	Free-text	false	string []

			contains	filter by cloud image (supports multiple values)		
			cloudInstanceId__contains	Free-text filter by cloud instance id(supports multiple values)	false	string []
			cloudInstanceSize__contains	Free-text filter by cloud instance size(supports multiple values)	false	string []
			cloudLocation__contains	Free-text filter by cloud location (supports multiple values)	false	string []
			cloudNetwork__contains	Free-text filter by cloud network (supports multiple values)	false	string []
			cloudProvider	Agents from which cloud provider	false	string []
			cloudProviderNin	Exclude Agents from these cloud provider	false	string []
			cloudTags__contains	Free-text filter by cloud tags (supports multiple values)	false	string []

			clusterName__contains	Free-text filter by cluster name (supports multiple values)	false	string []
			computerName	Computer name	false	string
			computerName__contains	Free-text filter by computer name (supports multiple values)	false	string []
			computerName__like	Match computer name partially (substring)	false	string
			consoleMigrationStatuses	Migration status in	false	string []
			consoleMigrationStatusesNin	Migration status nin	false	string []
			coreCount__between	Possible number of CPU cores (inclusive)	false	string
			coreCount__gt	CPU cores (more than)	false	integer
			coreCount__gte	CPU cores (more than or equal)	false	integer
			coreCount__lt	CPU cores (less than)	false	integer
			coreCount__lte	CPU cores (less than or equal)	false	integer
			cpuCount__between	Possible number of	false	string

				CPU cores (inclusive)		
			cpuCount__gt	Number of CPUs (more than)	false	integer
			cpuCount__gte	Number of CPUs (more than or equal)	false	integer
			cpuCount__lt	Number of CPUs (less than)	false	integer
			cpuCount__lte	Number of CPUs (less than or equal)	false	integer
			cpuId__contains	Free-text filter by CPU name (supports multiple values)	false	string []
			createdAt__between	Date range for creation time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			createdAt__gt	Agents created after this timestamp	false	string
			createdAt__gte	Agents created after or at this timestamp	false	string
			createdAt__lt	Agents created before this timestamp	false	string
			createdAt__lte	Agents created	false	string

				before or at this timestamp		
			csvFilterId	The ID of the CSV file to filter by	false	string
			decommissionedAt__between	Date range for decommission time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			decommissionedAt__gt	Agents decommissioned after this timestamp	false	string
			decommissionedAt__gte	Agents decommissioned after or at this timestamp	false	string
			decommissionedAt__lt	Agents decommissioned before this timestamp	false	string
			decommissionedAt__lte	Agents decommissioned before this timestamp	false	string
			domains	Included network domains	false	string []
			domainsNin	Not included network domains	false	string []
			encryptedApplications	Disk encryption status	false	boolean
			externalId__c	Free-text	false	string []

			ontains	filter by external ID (Customer ID)		
			externalIp__contains	Free-text filter by visible IP (supports multiple values)	false	string []
			filteredGroupIds	List of Group IDs to filter by	false	string []
			filteredSiteIds	List of Site IDs to filter by	false	string []
			filterId	Include all Agents matching this saved filter	false	string
			firewallEnabled	The agents supports Firewall Control and it is enabled for the agent's group	false	boolean []
			gatewayIp	Gateway ip	false	string
			gcpServiceAccount__contains	Free-text filter by gcp service account (supports multiple values)	false	string []
			groupIds	List of Group IDs to filter by	false	string []
			hasContainerizedWorkload	Include only Agents protecting containerized workloads	false	boolean

			hasLocalConfiguration	Agent has a local configuration set	false	boolean
			hasTags	Include only Agents that have any tags assigned if True, or none if False	false	boolean
			ids	A list of Agent IDs	false	string []
			infected	Include only Agents with at least one active threat	false	boolean
			installerTypes	Include only Agents installed with these package types	false	string []
			installerTypesNin	Exclude Agents installed with these package types	false	string []
			isActive	Include only active Agents	false	boolean
			isDecommissioned	Include active, decommissioned or both	false	boolean []
			isPendingUninstall	Include only Agents with pending uninstall requests	false	boolean
			isUninstalled	Include installed, uninstalled or	false	boolean []

				both		
			isUpToDate	Include only Agents with updated software	false	boolean
			k8sNodeLabels__contains	Free-text filter by K8s node labels (supports multiple values)	false	string []
			k8sNodeName__contains	Free-text filter by K8s node name (supports multiple values)	false	string []
			k8sType__contains	Free-text filter by K8s type(supports multiple values)	false	string []
			k8sVersion__contains	Free-text filter by K8s version (supports multiple values)	false	string []
			lastActiveDate__between	Date range for last active date(format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			lastActiveDate__gt	Agents last active after this time	false	string
			lastActiveDate__gte	Agents last active after or at this time	false	string
			lastActiveDat	Agents last	false	string

			e__lt	active before this time		
			lastActiveDate__lte	Agents last active before or at this time	false	string
			lastLoggedInUserName__contains	Free-text filter by username (supports multiple values)	false	string []
			lastSuccessfulScanDate__between	Date range for last successful full disk scan(format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			lastSuccessfulScanDate__gt	Agents last successful full disk scan after this time	false	string
			lastSuccessfulScanDate__gte	Agents last successful full disk scan after or at this time	false	string
			lastSuccessfulScanDate__lt	Agents last successful full disk scan before this time	false	string
			lastSuccessfulScanDate__lte	Agents last successful full disk scan before or at this time	false	string
			liveUpdateId__contains	Free-text filter by live	false	string []

				update ID (supports multiple values)		
			locationEnabled	The agents supports Location Awareness and it is enabled for the agent's group	false	boolean []
			locationIds	Include only Agents reporting these locations	false	string []
			locationIdsNin	Do not include only Agents reporting these locations	false	string []
			machineTypes	Included machine types	false	string []
			machineTypesNin	Not included machine types	false	string []
			migrationStatus	Migration status	false	enum
			missingPermissions	Included missing permissions	false	string []
			missingPermissionsNin	Excluded missing permissions	false	string []
			mitigationMode	Agent mitigation mode policy	false	enum
			mitigationMo	Mitigation	false	enum

			deSuspicious	mode policy for suspicious activity		
			networkInterfaceGatewayMacAddress__contains	Free-text filter by Gateway MAC address (supports multiple values)	false	string []
			networkInterfaceInet__contains	Free-text filter by local IP (supports multiple values)	false	string []
			networkInterfacePhysical__contains	Free-text filter by MAC address (supports multiple values)	false	string []
			networkQuarantineEnabled	The agents supports Network Quarantine Control and its enabled for the agent's group	false	boolean []
			networkStatuses	Included network statuses	false	string []
			networkStatusesNin	Included network statuses	false	string []
			operationalStates	Agent operational state	false	string []
			operationalStatesNin	Do not include these Agent operational	false	string []

				states		
			osArch	OS architecture	false	enum
			osTypes	Included OS types	false	string []
			osTypesNin	Not included OS types	false	string []
			osVersion__contains	Free-text filter by OS full name and version (supports multiple values)	false	string []
			query	A free-text search term, will match applicable attributes (sub-string match). Note: Device's physical addresses will be matched if they start with the search term only (no match if they contain the term).	false	string
			rangerStatus	[DEPRECATED] Use rangerStatuses.	false	enum
			rangerStatuses	Status of Ranger	false	string []
			rangerStatusesNin	Do not include these Ranger Statuses	false	string []

			rangerVersions	Ranger versions to include	false	string []
			rangerVersionsNin	Ranger versions not to include	false	string []
			registeredAt__between	Date range for first registration time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			registeredAt__gt	Agents registered after this time	false	string
			registeredAt__gte	Agents registered after or at this time	false	string
			registeredAt__lt	Agents registered before this time	false	string
			registeredAt__lte	Agents registered before or at this time	false	string
			remoteOpsForensicsSupported	Include only agents that has Remote Ops Forensicsfeature supported	false	boolean
			remoteProfilingStates	Agent remote profiling state	false	string []
			remoteProfilingStatesNin	Do not include these Agent remote	false	string []

				profiling states		
			rsoLevel	Supported Remote Script Orchestration level	false	enum
			scanStatus	Scan status	false	enum
			scanStatuses	Included scan statuses	false	string []
			scanStatuses Nin	Not included scan statuses	false	string []
			serialNumber __contains	Free-text filter by Serial Number (supports multiple values)	false	string []
			siteIds	List of Site IDs to filter by	false	string []
			tagsData	Filter agents by their assigned tags. Given in form of a JSON where each key represents a tag key, and each value represents a list of string values to filter by. To filter by unassigned tag values, use __nin suffix in the tag key.	false	string
			threatConten	Include only	false	string

			tHash	Agents that have at least one threat with this content hash		
			threatCreatedAt__between	Agents with threats reported in a date range (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			threatCreatedAt__gt	Agents with threats reported after this time	false	string
			threatCreatedAt__gte	Agents with threats reported after or at this time	false	string
			threatCreatedAt__lt	Agents with threats reported before this time	false	string
			threatCreatedAt__lte	Agents with threats reported before or at this time	false	string
			threatHidden	Include only Agents with at least one hidden threat	false	boolean
			threatMitigationStatus	Include only Agents that have threats with this mitigation	false	enum

				status		
			threatRebootRequired	Has at least one threat with at least one mitigation action pending reboot to succeed	false	boolean []
			threatResolved	Include only Agents with at least one resolved threat	false	boolean
			totalMemory__between	Total memory range (GB, inclusive)	false	string
			totalMemory__gt	Memory size (MB, more than)	false	integer
			totalMemory__gte	Memory size (MB, more than or equal)	false	integer
			totalMemory__lt	Memory size (MB, less than)	false	integer
			totalMemory__lte	Memory size (MB, less than or equal)	false	integer
			updatedAt__between	Date range for update time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			updatedAt__gt	Agents updated after this timestamp	false	string

			updatedAt__gte	Agents updated after or at this timestamp	false	string
			updatedAt__lt	Agents updated before this timestamp	false	string
			updatedAt__lte	Agents updated before or at this timestamp	false	string
			userActionsNeeded	Included pending user actions	false	string []
			userActionsNeededNin	Excluded pending user actions	false	string []
			uuid	Agent's universally unique identifier	false	string
			uuid__contains	Free-text filter by Agent UUID (supports multiple values)	false	string []
			uuids	A list of included UUIDs	false	string []

Fetch Files

POST /web/api/v2.1/agents/{agent_id}/actions/fetch-files

Fetch files from endpoints (up to 10 MB for each command) to analyze the root of threats (that come from files - of course, this does not help for fileless threats). Set the pathnames in the body of the request.
Regular expressions and metacharacters are not allowed. Spaces are allowed.
You must enter a new password, which you will use to open the archive of downloaded files. The password must be 10 or more characters with a mix of upper and lower case letters, numbers, and symbols.
This command collects the file and uploads them to the Management. To get the files, download them from the Management.
FedRAMP-compliant and other Managements in GovCloud require a Support ticket to enable this feature.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - User has insufficient permissions to perform the requested action

404 - Agent not found

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>success</td><td>Indicates a successful operation</td><td>false</td><td>boolean</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>password</td><td>File encryption password</td><td>true</td><td>string</td></tr>
<tr><td>files</td><td>List of files to fetch (absolute paths, up to 10 files)</td><td>false</td><td>string []</td></tr>
</table>
</td></tr>
</table>

Move between Sites

POST /web/api/v2.1/agents/actions/move-to-site

This command requires Account or Global level access.
Agents are assigned to a Site when they are first installed with a Site Token. If you have the required access level, a role with permissions (the SOC role does not allow this action), and permission for both Sites, you can move Agents from one Site to a different Site. Agents will be moved to the best matching dynamic group, or to the Default group if no dynamic group matches.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - User has insufficient permissions to perform the requested action

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>affected</td><td>Number of entities affected by the requested operation</td><td>false</td><td>integer</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>targetSiteId</td><td>Target site id</td><td>true</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>filter</td><td>Applied filter - only matched Agents will be affected by the requested action. Leave empty to apply the action on all applicable Agents.</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>activeThreats</td><td>Include Agents with this amount of active threats</td><td>false</td><td>integer</td></tr>
<tr><td>activeThreats__gt</td><td>Include Agents with at least this amount of active threats</td><td>false</td><td>integer</td></tr>
<tr><td>adComputerMember__contains</td><td>Free-text filter by Active Directory computer groups string (supports multiple values)</td><td>false</td><td>string []</td></tr>
<tr><td>adComputerName__contains</td><td>Free-text filter by Active Directory computer name string (supports multiple values)</td><td>false</td><td>string []</td></tr>
<tr><td>adComputerQuery__contains</td><td>Free-text filter by Active</td><td>false</td><td>string []</td></tr>
</table>
</td></tr>
</table>

				Directory computer name or its groups (supports multiple values)		
			adQuery	An Active Directory query string	false	string
			adQuery__contains	Free-text filter by Active Directory string (supports multiple values)	false	string []
			adUserMember__contains	Free-text filter by Active Directory user groups string (supports multiple values)	false	string []
			adUserName__contains	Free-text filter by Active Directory username string (supports multiple values)	false	string []
			adUserQuery__contains	Free-text filter by Active Directory computer name or its groups (supports	false	string []

				multiple values)		
			agentNamespace__contains	Free-text filter by agent namespace (supports multiple values)	false	string []
			agentPodName__contains	Free-text filter by agent pod name (supports multiple values)	false	string []
			agentVersion__between	Version range for agent version (format: <from_version>-<to_version>, inclusive)	false	string
			agentVersion__gt	Agents versions greater than given version	false	string
			agentVersion__gte	Agents versions greater than or equal to given version	false	string
			agentVersion__lt	Agents versions less than given version	false	string
			agentVersion__lte	Agents versions less than or equal to given version	false	string
			agentVersions	Agent versions to	false	string []

				include		
			agentVersionsNin	Agent versions not to include	false	string []
			appsVulnerabilityStatuses	Apps vulnerability status in	false	string []
			appsVulnerabilityStatusesNin	Apps vulnerability status nin	false	string []
			awsRole__contains	Free-text filter by aws role(supports multiple values)	false	string []
			awsSecurityGroups__contains	Free-text filter by aws securityGroups(supports multiple values)	false	string []
			awsSubnetIds__contains	Free-text filter by aws subnet ids (supports multiple values)	false	string []
			azureResourceGroup__contains	Free-text filter by azure resource group(supports multiple values)	false	string []
			cloudAccount__contains	Free-text filter by cloud account (supports multiple values)	false	string []
			cloudImage__contains	Free-text filter by cloud image	false	string []

				(supports multiple values)		
			cloudInstanceId__contains	Free-text filter by cloud instance id(supports multiple values)	false	string []
			cloudInstanceSize__contains	Free-text filter by cloud instance size(supports multiple values)	false	string []
			cloudLocation__contains	Free-text filter by cloud location (supports multiple values)	false	string []
			cloudNetwork__contains	Free-text filter by cloud network (supports multiple values)	false	string []
			cloudProvider	Agents from which cloud provider	false	string []
			cloudProviderNin	Exclude Agents from these cloud provider	false	string []
			cloudTags__contains	Free-text filter by cloud tags (supports multiple values)	false	string []
			clusterName__contains	Free-text filter by	false	string []

				cluster name (supports multiple values)		
			computerName	Computer name	false	string
			computerName__contains	Free-text filter by computer name (supports multiple values)	false	string []
			computerName__like	Match computer name partially (substring)	false	string
			consoleMigrationStatuses	Migration status in	false	string []
			consoleMigrationStatusesNin	Migration status nin	false	string []
			coreCount__between	Possible number of CPU cores (inclusive)	false	string
			coreCount__gt	CPU cores (more than)	false	integer
			coreCount__gte	CPU cores (more than or equal)	false	integer
			coreCount__lt	CPU cores (less than)	false	integer
			coreCount__lte	CPU cores (less than or equal)	false	integer
			cpuCount__between	Possible number of CPU cores (inclusive)	false	string

			cpuCount__gt	Number of CPUs (more than)	false	integer
			cpuCount__gte	Number of CPUs (more than or equal)	false	integer
			cpuCount__lt	Number of CPUs (less than)	false	integer
			cpuCount__lte	Number of CPUs (less than or equal)	false	integer
			cpuId__contains	Free-text filter by CPU name (supports multiple values)	false	string []
			createdAt__between	Date range for creation time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			createdAt__gt	Agents created after this timestamp	false	string
			createdAt__gte	Agents created after or at this timestamp	false	string
			createdAt__lt	Agents created before this timestamp	false	string
			createdAt__lte	Agents created before or at this timestamp	false	string

			csvFilterId	The ID of the CSV file to filter by	false	string
			decommissionedAt__between	Date range for decommission time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			decommissionedAt__gt	Agents decommissioned after this timestamp	false	string
			decommissionedAt__gte	Agents decommissioned after or at this timestamp	false	string
			decommissionedAt__lt	Agents decommissioned before this timestamp	false	string
			decommissionedAt__lte	Agents decommissioned before this timestamp	false	string
			domains	Included network domains	false	string []
			domainsNin	Not included network domains	false	string []
			encryptedApplications	Disk encryption status	false	boolean
			externalId__contains	Free-text filter by external ID (Customer ID)	false	string []

			externalIp__contains	Free-text filter by visible IP (supports multiple values)	false	string []
			filteredGroupIds	List of Group IDs to filter by	false	string []
			filteredSiteIds	List of Site IDs to filter by	false	string []
			filterId	Include all Agents matching this saved filter	false	string
			firewallEnabled	The agents supports Firewall Control and it is enabled for the agent's group	false	boolean []
			gatewayIp	Gateway ip	false	string
			gcpServiceAccount__contains	Free-text filter by gcp service account (supports multiple values)	false	string []
			groupIds	List of Group IDs to filter by	false	string []
			hasContainerizedWorkload	Include only Agents protecting containerized workloads	false	boolean
			hasLocalConfiguration	Agent has a local configuration	false	boolean

				set		
			hasTags	Include only Agents that have any tags assigned if True, or none if False	false	boolean
			ids	A list of Agent IDs	false	string []
			infected	Include only Agents with at least one active threat	false	boolean
			installerTypes	Include only Agents installed with these package types	false	string []
			installerTypesNin	Exclude Agents installed with these package types	false	string []
			isActive	Include only active Agents	false	boolean
			isDecommissioned	Include active, decommissioned or both	false	boolean []
			isPendingUninstall	Include only Agents with pending uninstall requests	false	boolean
			isUninstalled	Include installed, uninstalled or both	false	boolean []
			isUpToDate	Include only	false	boolean

				Agents with updated software		
			k8sNodeLabels__contains	Free-text filter by K8s node labels (supports multiple values)	false	string []
			k8sNodeName__contains	Free-text filter by K8s node name (supports multiple values)	false	string []
			k8sType__contains	Free-text filter by K8s type(supports multiple values)	false	string []
			k8sVersion__contains	Free-text filter by K8s version (supports multiple values)	false	string []
			lastActiveDate__between	Date range for last active date(format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			lastActiveDate__gt	Agents last active after this time	false	string
			lastActiveDate__gte	Agents last active after or at this time	false	string
			lastActiveDate__lt	Agents last active before this time	false	string

			lastActiveDate__lte	Agents last active before or at this time	false	string
			lastLoggedInUserName__contains	Free-text filter by username (supports multiple values)	false	string []
			lastSuccessfulScanDate__between	Date range for last successful full disk scan(format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			lastSuccessfulScanDate__gt	Agents last successful full disk scan after this time	false	string
			lastSuccessfulScanDate__gte	Agents last successful full disk scan after or at this time	false	string
			lastSuccessfulScanDate__lt	Agents last successful full disk scan before this time	false	string
			lastSuccessfulScanDate__lte	Agents last successful full disk scan before or at this time	false	string
			liveUpdateId__contains	Free-text filter by live update ID (supports multiple	false	string []

				values)		
			locationEnabled	The agents supports Location Awareness and it is enabled for the agent's group	false	boolean []
			locationIds	Include only Agents reporting these locations	false	string []
			locationIdsNin	Do not include only Agents reporting these locations	false	string []
			machineTypes	Included machine types	false	string []
			machineTypesNin	Not included machine types	false	string []
			migrationStatus	Migration status	false	enum
			missingPermissions	Included missing permissions	false	string []
			missingPermissionsNin	Excluded missing permissions	false	string []
			mitigationMode	Agent mitigation mode policy	false	enum
			mitigationModeSuspicious	Mitigation mode policy for suspicious activity	false	enum

			networkInterfaceGatewayMacAddress__contains	Free-text filter by Gateway MAC address (supports multiple values)	false	string []
			networkInterfaceInet__contains	Free-text filter by local IP (supports multiple values)	false	string []
			networkInterfacePhysical__contains	Free-text filter by MAC address (supports multiple values)	false	string []
			networkQuarantineEnabled	The agents supports Network Quarantine Control and its enabled for the agent's group	false	boolean []
			networkStatuses	Included network statuses	false	string []
			networkStatusesNin	Included network statuses	false	string []
			operationalStates	Agent operational state	false	string []
			operationalStatesNin	Do not include these Agent operational states	false	string []
			osArch	OS architecture	false	enum

			osTypes	Included OS types	false	string []
			osTypesNin	Not included OS types	false	string []
			osVersion__contains	Free-text filter by OS full name and version (supports multiple values)	false	string []
			query	A free-text search term, will match applicable attributes (sub-string match). Note: Device's physical addresses will be matched if they start with the search term only (no match if they contain the term).	false	string
			rangerStatus	[DEPRECATED] Use rangerStatuses.	false	enum
			rangerStatuses	Status of Ranger	false	string []
			rangerStatusesNin	Do not include these Ranger Statuses	false	string []
			rangerVersions	Ranger versions to include	false	string []

			rangerVersionsNin	Ranger versions not to include	false	string []
			registeredAt__between	Date range for first registration time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			registeredAt__gt	Agents registered after this time	false	string
			registeredAt__gte	Agents registered after or at this time	false	string
			registeredAt__lt	Agents registered before this time	false	string
			registeredAt__lte	Agents registered before or at this time	false	string
			remoteOpsForensicsSupported	Include only agents that has Remote Ops Forensicsfeature supported	false	boolean
			remoteProfilingStates	Agent remote profiling state	false	string []
			remoteProfilingStatesNin	Do not include these Agent remote profiling states	false	string []
			rsoLevel	Supported	false	enum

				Remote Script Orchestration level		
			scanStatus	Scan status	false	enum
			scanStatuses	Included scan statuses	false	string []
			scanStatuses Nin	Not included scan statuses	false	string []
			serialNumber __contains	Free-text filter by Serial Number (supports multiple values)	false	string []
			siteIds	List of Site IDs to filter by	false	string []
			tagsData	Filter agents by their assigned tags. Given in form of a JSON where each key represents a tag key, and each value represents a list of string values to filter by. To filter by unassigned tag values, use __nin suffix in the tag key.	false	string
			threatConten tHash	Include only Agents that have at least one threat with this	false	string

				content hash		
			threatCreatedAt__between	Agents with threats reported in a date range (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			threatCreatedAt__gt	Agents with threats reported after this time	false	string
			threatCreatedAt__gte	Agents with threats reported after or at this time	false	string
			threatCreatedAt__lt	Agents with threats reported before this time	false	string
			threatCreatedAt__lte	Agents with threats reported before or at this time	false	string
			threatHidden	Include only Agents with at least one hidden threat	false	boolean
			threatMitigationStatus	Include only Agents that have threats with this mitigation status	false	enum
			threatRebootRequired	Has at least one threat	false	boolean []

				with at least one mitigation action pending reboot to succeed		
			threatResolved	Include only Agents with at least one resolved threat	false	boolean
			totalMemory__between	Total memory range (GB, inclusive)	false	string
			totalMemory__gt	Memory size (MB, more than)	false	integer
			totalMemory__gte	Memory size (MB, more than or equal)	false	integer
			totalMemory__lt	Memory size (MB, less than)	false	integer
			totalMemory__lte	Memory size (MB, less than or equal)	false	integer
			updatedAt__between	Date range for update time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			updatedAt__gt	Agents updated after this timestamp	false	string
			updatedAt__gte	Agents updated after or at this timestamp	false	string

			updatedAt__lt	Agents updated before this timestamp	false	string
			updatedAt__lte	Agents updated before or at this timestamp	false	string
			userActionsNeeded	Included pending user actions	false	string []
			userActionsNeededNin	Excluded pending user actions	false	string []
			uuid	Agent's universally unique identifier	false	string
			uuid__contains	Free-text filter by Agent UUID (supports multiple values)	false	string []
			uuids	A list of included UUIDs	false	string []

Fetch Firewall Rules

POST /web/api/v2.1/agents/actions/fetch-firewall-rules

Firewall Control is disabled at the Global level. When it is first enabled, all Sites and Groups inherit the Firewall Control policy from the Global policy. Agents have Firewall Control disabled, until they connect to a Site or Group with an enabled Firewall Control policy.
After Agents get Firewall Control, if you add or change a Firewall rule, you can use this command to make sure all Agents fetch the rules, (though Agents usually update their policies every few seconds). Use the filter parameter to set which Agents will fetch the rules, if you do not want all of them to attempt it.
Firewall Control requires a Control SKU.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - Insufficient permissions

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>affected</td><td>Number of entities affected by the requested operation</td><td>false</td><td>integer</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>format</td><td>Desired firewall configuration format. Use "native" to get configuration file in native format.</td><td>false</td><td>enum</td></tr>
<tr><td>state</td><td>Desired firewall configuration state. Use "initial" to get the firewall configuration that existed before Agent installation. (Note: "initial" requires native format).</td><td>false</td><td>enum</td></tr>
</table>
</td></tr>
<tr><td>filter</td><td>Applied filter - only matched Agents will be affected by the requested action. Leave empty to apply the action on all applicable Agents.</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>activeThreats</td><td>Include Agents with this amount of active threats</td><td>false</td><td>integer</td></tr>
<tr><td>activeThreats__gt</td><td>Include Agents with at least this amount of active threats</td><td>false</td><td>integer</td></tr>
</table>
</td></tr>
</table>

			adComputerMember__contains	Free-text filter by Active Directory computer groups string (supports multiple values)	false	string []
			adComputerName__contains	Free-text filter by Active Directory computer name string (supports multiple values)	false	string []
			adComputerQuery__contains	Free-text filter by Active Directory computer name or its groups (supports multiple values)	false	string []
			adQuery	An Active Directory query string	false	string
			adQuery__contains	Free-text filter by Active Directory string (supports multiple values)	false	string []
			adUserMember__contains	Free-text filter by Active Directory user groups	false	string []

				string (supports multiple values)		
			adUserName__contains	Free-text filter by Active Directory username string (supports multiple values)	false	string []
			adUserQuery__contains	Free-text filter by Active Directory computer name or its groups (supports multiple values)	false	string []
			agentNamespace__contains	Free-text filter by agent namespace (supports multiple values)	false	string []
			agentPodName__contains	Free-text filter by agent pod name (supports multiple values)	false	string []
			agentVersion__between	Version range for agent version (format: <from_version>-<to_version>, inclusive)	false	string

			agentVersion__gt	Agents versions greater than given version	false	string
			agentVersion__gte	Agents versions greater than or equal to given version	false	string
			agentVersion__lt	Agents versions less than given version	false	string
			agentVersion__lte	Agents versions less than or equal to given version	false	string
			agentVersions	Agent versions to include	false	string []
			agentVersionsNin	Agent versions not to include	false	string []
			appsVulnerabilityStatuses	Apps vulnerability status in	false	string []
			appsVulnerabilityStatusesNin	Apps vulnerability status nin	false	string []
			awsRole__contains	Free-text filter by aws role(supports multiple values)	false	string []
			awsSecurityGroups__contains	Free-text filter by aws securityGroups(supports multiple values)	false	string []

			awsSubnetIds__contains	Free-text filter by aws subnet ids (supports multiple values)	false	string []
			azureResourceGroup__contains	Free-text filter by azure resource group(supports multiple values)	false	string []
			cloudAccount__contains	Free-text filter by cloud account (supports multiple values)	false	string []
			cloudImage__contains	Free-text filter by cloud image (supports multiple values)	false	string []
			cloudInstanceId__contains	Free-text filter by cloud instance id(supports multiple values)	false	string []
			cloudInstanceSize__contains	Free-text filter by cloud instance size(supports multiple values)	false	string []
			cloudLocation__contains	Free-text filter by cloud location (supports multiple values)	false	string []
			cloudNetwork	Free-text	false	string []

			__contains	filter by cloud network (supports multiple values)		
			cloudProvider	Agents from which cloud provider	false	string []
			cloudProvideerNin	Exclude Agents from these cloud provider	false	string []
			cloudTags__contains	Free-text filter by cloud tags (supports multiple values)	false	string []
			clusterName__contains	Free-text filter by cluster name (supports multiple values)	false	string []
			computerName	Computer name	false	string
			computerName__contains	Free-text filter by computer name (supports multiple values)	false	string []
			computerName__like	Match computer name partially (substring)	false	string
			consoleMigrationStatuses	Migration status in	false	string []
			consoleMigrationStatusesN	Migration status nin	false	string []

			in			
			coreCount__between	Possible number of CPU cores (inclusive)	false	string
			coreCount__gt	CPU cores (more than)	false	integer
			coreCount__gte	CPU cores (more than or equal)	false	integer
			coreCount__lt	CPU cores (less than)	false	integer
			coreCount__lte	CPU cores (less than or equal)	false	integer
			cpuCount__between	Possible number of CPU cores (inclusive)	false	string
			cpuCount__gt	Number of CPUs (more than)	false	integer
			cpuCount__gte	Number of CPUs (more than or equal)	false	integer
			cpuCount__lt	Number of CPUs (less than)	false	integer
			cpuCount__lte	Number of CPUs (less than or equal)	false	integer
			cpuId__contains	Free-text filter by CPU name (supports multiple values)	false	string []
			createdAt__between	Date range for creation time (format:	false	string

				<from_timestamp>-<to_timestamp>, inclusive)		
			createdAt__gt	Agents created after this timestamp	false	string
			createdAt__gte	Agents created after or at this timestamp	false	string
			createdAt__lt	Agents created before this timestamp	false	string
			createdAt__lte	Agents created before or at this timestamp	false	string
			csvFilterId	The ID of the CSV file to filter by	false	string
			decommissionedAt__between	Date range for decommission time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			decommissionedAt__gt	Agents decommissioned after this timestamp	false	string
			decommissionedAt__gte	Agents decommissioned after or at this timestamp	false	string
			decommission	Agents	false	string

			edAt__lt	decommissioned before this timestamp		
			decommissionedAt__lte	Agents decommissioned before this timestamp	false	string
			domains	Included network domains	false	string []
			domainsNin	Not included network domains	false	string []
			encryptedApplications	Disk encryption status	false	boolean
			externalId__contains	Free-text filter by external ID (Customer ID)	false	string []
			externalIp__contains	Free-text filter by visible IP (supports multiple values)	false	string []
			filteredGroupIds	List of Group IDs to filter by	false	string []
			filteredSiteIds	List of Site IDs to filter by	false	string []
			filterId	Include all Agents matching this saved filter	false	string
			firewallEnabled	The agents supports Firewall Control and it is enabled for	false	boolean []

				the agent's group		
			gatewayIp	Gateway ip	false	string
			gcpServiceAccount__contains	Free-text filter by gcp service account (supports multiple values)	false	string []
			groupIds	List of Group IDs to filter by	false	string []
			hasContainerizedWorkload	Include only Agents protecting containerized workloads	false	boolean
			hasLocalConfiguration	Agent has a local configuration set	false	boolean
			hasTags	Include only Agents that have any tags assigned if True, or none if False	false	boolean
			ids	A list of Agent IDs	false	string []
			infected	Include only Agents with at least one active threat	false	boolean
			installerTypes	Include only Agents installed with these package types	false	string []
			installerType	Exclude	false	string []

			sNin	Agents installed with these package types		
			isActive	Include only active Agents	false	boolean
			isDecommissioned	Include active, decommissioned or both	false	boolean []
			isPendingUninstall	Include only Agents with pending uninstall requests	false	boolean
			isUninstalled	Include installed, uninstalled or both	false	boolean []
			isUpToDate	Include only Agents with updated software	false	boolean
			k8sNodeLabels__contains	Free-text filter by K8s node labels (supports multiple values)	false	string []
			k8sNodeName__contains	Free-text filter by K8s node name (supports multiple values)	false	string []
			k8sType__contains	Free-text filter by K8s type(supports multiple values)	false	string []
			k8sVersion__c	Free-text	false	string []

			ontains	filter by K8s version (supports multiple values)		
			lastActiveDate__between	Date range for last active date(format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			lastActiveDate__gt	Agents last active after this time	false	string
			lastActiveDate__gte	Agents last active after or at this time	false	string
			lastActiveDate__lt	Agents last active before this time	false	string
			lastActiveDate__lte	Agents last active before or at this time	false	string
			lastLoggedInUserName__contains	Free-text filter by username (supports multiple values)	false	string []
			lastSuccessfulScanDate__between	Date range for last successful full disk scan(format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			lastSuccessfulScanDate__gt	Agents last successful full disk scan	false	string

				after this time		
			lastSuccessfulScanDate__gte	Agents last successful full disk scan after or at this time	false	string
			lastSuccessfulScanDate__lt	Agents last successful full disk scan before this time	false	string
			lastSuccessfulScanDate__lte	Agents last successful full disk scan before or at this time	false	string
			liveUpdateId__contains	Free-text filter by live update ID (supports multiple values)	false	string []
			locationEnabled	The agents supports Location Awareness and it is enabled for the agent's group	false	boolean []
			locationIds	Include only Agents reporting these locations	false	string []
			locationIdsNin	Do not include only Agents reporting these locations	false	string []

			machineTypes	Included machine types	false	string []
			machineTypesNin	Not included machine types	false	string []
			migrationStatus	Migration status	false	enum
			missingPermissions	Included missing permissions	false	string []
			missingPermissionsNin	Excluded missing permissions	false	string []
			mitigationMode	Agent mitigation mode policy	false	enum
			mitigationModeSuspicious	Mitigation mode policy for suspicious activity	false	enum
			networkInterfaceGatewayMacAddress__contains	Free-text filter by Gateway MAC address (supports multiple values)	false	string []
			networkInterfaceInet__contains	Free-text filter by local IP (supports multiple values)	false	string []
			networkInterfacePhysical__contains	Free-text filter by MAC address (supports multiple values)	false	string []
			networkQuarantineEnabled	The agents supports	false	boolean []

				Network Quarantine Control and its enabled for the agent's group		
			networkStatuses	Included network statuses	false	string []
			networkStatusesNin	Included network statuses	false	string []
			operationalStates	Agent operational state	false	string []
			operationalStatesNin	Do not include these Agent operational states	false	string []
			osArch	OS architecture	false	enum
			osTypes	Included OS types	false	string []
			osTypesNin	Not included OS types	false	string []
			osVersion__contains	Free-text filter by OS full name and version (supports multiple values)	false	string []
			query	A free-text search term, will match applicable attributes (sub-string match). Note: Device's physical	false	string

				addresses will be matched if they start with the search term only (no match if they contain the term).		
			rangerStatus	[DEPRECATED] Use rangerStatuses.	false	enum
			rangerStatuses	Status of Ranger	false	string []
			rangerStatusesNin	Do not include these Ranger Statuses	false	string []
			rangerVersions	Ranger versions to include	false	string []
			rangerVersionsNin	Ranger versions not to include	false	string []
			registeredAt__between	Date range for first registration time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			registeredAt__gt	Agents registered after this time	false	string
			registeredAt__gte	Agents registered after or at this time	false	string
			registeredAt__	Agents	false	string

			lt	registered before this time		
			registeredAt__lte	Agents registered before or at this time	false	string
			remoteOpsForensicsSupported	Include only agents that has Remote Ops Forensicsfeature supported	false	boolean
			remoteProfilingStates	Agent remote profiling state	false	string []
			remoteProfilingStatesNin	Do not include these Agent remote profiling states	false	string []
			rsoLevel	Supported Remote Script Orchestration level	false	enum
			scanStatus	Scan status	false	enum
			scanStatuses	Included scan statuses	false	string []
			scanStatuses Nin	Not included scan statuses	false	string []
			serialNumber__contains	Free-text filter by Serial Number (supports multiple values)	false	string []
			siteIds	List of Site IDs to filter by	false	string []
			tagsData	Filter agents	false	string

				by their assigned tags. Given in form of a JSON where each key represents a tag key, and each value represents a list of string values to filter by. To filter by unassigned tag values, use __nin suffix in the tag key.		
			threatContentHash	Include only Agents that have at least one threat with this content hash	false	string
			threatCreatedAt__between	Agents with threats reported in a date range (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			threatCreatedAt__gt	Agents with threats reported after this time	false	string
			threatCreatedAt__gte	Agents with threats reported after or at this time	false	string

			threatCreatedAt__lt	Agents with threats reported before this time	false	string
			threatCreatedAt__lte	Agents with threats reported before or at this time	false	string
			threatHidden	Include only Agents with at least one hidden threat	false	boolean
			threatMitigationStatus	Include only Agents that have threats with this mitigation status	false	enum
			threatRebootRequired	Has at least one threat with at least one mitigation action pending reboot to succeed	false	boolean []
			threatResolved	Include only Agents with at least one resolved threat	false	boolean
			totalMemory__between	Total memory range (GB, inclusive)	false	string
			totalMemory__gt	Memory size (MB, more than)	false	integer
			totalMemory__gte	Memory size (MB, more	false	integer

				than or equal)		
			totalMemory__lt	Memory size (MB, less than)	false	integer
			totalMemory__lte	Memory size (MB, less than or equal)	false	integer
			updatedAt__between	Date range for update time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			updatedAt__gt	Agents updated after this timestamp	false	string
			updatedAt__gte	Agents updated after or at this timestamp	false	string
			updatedAt__lt	Agents updated before this timestamp	false	string
			updatedAt__lte	Agents updated before or at this timestamp	false	string
			userActionsNeeded	Included pending user actions	false	string []
			userActionsNeededNin	Excluded pending user actions	false	string []
			uuid	Agent's universally unique identifier	false	string

			uuid__contains	Free-text filter by Agent UUID (supports multiple values)	false	string []
			uuids	A list of included UUIDs	false	string []

Move to Console

POST /web/api/v2.1/agents/actions/move-to-console

You can move Agents between Management Consoles. This command moves Agents to a target Console, Account, and Site, given the Console URL and Site token.
You must have Global permissions for the source Console and access to the Site token of the target Site.
Resolve all threats on the Agents to move before you run this command.
If the Agents have local configurations, the configurations are maintained.
If the new Management has different blocklists, exclusions, and other assets, these are applied the next time the Agent communicates with the Management.
This command works on these Agent versions: Windows 3.0 and later, macOS 3.0 and later, Linux 3.4 and later.
An Agent tries to connect to the new Management Console for 3 minutes. If the Agent cannot connect (has unresolved threats or other requirements are not met), it stays in the original Management Console.
To get the Site token, run the "sites" command (see Sites list) and take the "registrationToken" value.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - User has insufficient permissions to perform the requested action

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>affected</td><td>Number of entities affected by the requested operation</td><td>false</td><td>integer</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>token</td><td>Site token of the site to which the Agent is to be moved. This is a base-64 string that can be copied from the GUI.</td><td>true</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>filter</td><td>Applied filter - only matched Agents will be affected by the requested action. Note: One of these filter arguments must be supplied: ids, groupIds, filterId.</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>activeThreats</td><td>Include Agents with this amount of active threats</td><td>false</td><td>integer</td></tr>
<tr><td>activeThreats__gt</td><td>Include Agents with at least this amount of active threats</td><td>false</td><td>integer</td></tr>
<tr><td>adComputerMember__contains</td><td>Free-text filter by Active Directory computer groups string (supports multiple values)</td><td>false</td><td>string []</td></tr>
<tr><td>adComputerName__contains</td><td>Free-text filter by Active Directory computer</td><td>false</td><td>string []</td></tr>
</table>
</td></tr>
</table>

				name string (supports multiple values)		
			adComputerQuery__contains	Free-text filter by Active Directory computer name or its groups (supports multiple values)	false	string []
			adQuery	An Active Directory query string	false	string
			adQuery__contains	Free-text filter by Active Directory string (supports multiple values)	false	string []
			adUserMember__contains	Free-text filter by Active Directory user groups string (supports multiple values)	false	string []
			adUserName__contains	Free-text filter by Active Directory username string (supports multiple values)	false	string []

			adUserQuery__contains	Free-text filter by Active Directory computer name or its groups (supports multiple values)	false	string []
			agentNamespace__contains	Free-text filter by agent namespace (supports multiple values)	false	string []
			agentPodName__contains	Free-text filter by agent pod name (supports multiple values)	false	string []
			agentVersion__between	Version range for agent version (format: <from_version>-<to_version>, inclusive)	false	string
			agentVersion__gt	Agents versions greater than given version	false	string
			agentVersion__gte	Agents versions greater than or equal to given version	false	string
			agentVersion__lt	Agents versions less than given version	false	string

			agentVersion__lte	Agents versions less than or equal to given version	false	string
			agentVersions	Agent versions to include	false	string []
			agentVersionsNin	Agent versions not to include	false	string []
			appsVulnerabilityStatuses	Apps vulnerability status in	false	string []
			appsVulnerabilityStatusesNin	Apps vulnerability status nin	false	string []
			awsRole__contains	Free-text filter by aws role(supports multiple values)	false	string []
			awsSecurityGroups__contains	Free-text filter by aws securityGroups(supports multiple values)	false	string []
			awsSubnetIds__contains	Free-text filter by aws subnet ids (supports multiple values)	false	string []
			azureResourceGroup__contains	Free-text filter by azure resource group(supports multiple values)	false	string []
			cloudAccount__contains	Free-text filter by cloud	false	string []

				account (supports multiple values)		
			cloudImage__contains	Free-text filter by cloud image (supports multiple values)	false	string []
			cloudInstanceId__contains	Free-text filter by cloud instance id(supports multiple values)	false	string []
			cloudInstanceSize__contains	Free-text filter by cloud instance size(supports multiple values)	false	string []
			cloudLocation__contains	Free-text filter by cloud location (supports multiple values)	false	string []
			cloudNetwork__contains	Free-text filter by cloud network (supports multiple values)	false	string []
			cloudProvider	Agents from which cloud provider	false	string []
			cloudProviderNin	Exclude Agents from these cloud provider	false	string []
			cloudTags__co	Free-text	false	string []

			ntains	filter by cloud tags (supports multiple values)		
			clusterName__contains	Free-text filter by cluster name (supports multiple values)	false	string []
			computerName	Computer name	false	string
			computerName__contains	Free-text filter by computer name (supports multiple values)	false	string []
			computerName__like	Match computer name partially (substring)	false	string
			consoleMigrationStatuses	Migration status in	false	string []
			consoleMigrationStatusesNin	Migration status nin	false	string []
			coreCount__between	Possible number of CPU cores (inclusive)	false	string
			coreCount__gt	CPU cores (more than)	false	integer
			coreCount__gte	CPU cores (more than or equal)	false	integer
			coreCount__lt	CPU cores (less than)	false	integer

			coreCount__lte	CPU cores (less than or equal)	false	integer
			cpuCount__between	Possible number of CPU cores (inclusive)	false	string
			cpuCount__gt	Number of CPUs (more than)	false	integer
			cpuCount__gte	Number of CPUs (more than or equal)	false	integer
			cpuCount__lt	Number of CPUs (less than)	false	integer
			cpuCount__lte	Number of CPUs (less than or equal)	false	integer
			cpuId__contains	Free-text filter by CPU name (supports multiple values)	false	string []
			createdAt__between	Date range for creation time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			createdAt__gt	Agents created after this timestamp	false	string
			createdAt__gte	Agents created after or at this timestamp	false	string
			createdAt__lt	Agents	false	string

				created before this timestamp		
			createdAt__lte	Agents created before or at this timestamp	false	string
			csvFilterId	The ID of the CSV file to filter by	false	string
			decommissionedAt__between	Date range for decommission time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			decommissionedAt__gt	Agents decommissioned after this timestamp	false	string
			decommissionedAt__gte	Agents decommissioned after or at this timestamp	false	string
			decommissionedAt__lt	Agents decommissioned before this timestamp	false	string
			decommissionedAt__lte	Agents decommissioned before this timestamp	false	string
			domains	Included network domains	false	string []
			domainsNin	Not included network domains	false	string []

			encryptedApplications	Disk encryption status	false	boolean
			externalId__contains	Free-text filter by external ID (Customer ID)	false	string []
			externalIp__contains	Free-text filter by visible IP (supports multiple values)	false	string []
			filteredGroupIds	List of Group IDs to filter by	false	string []
			filteredSiteIds	List of Site IDs to filter by	false	string []
			filterId	Include all Agents matching this saved filter	false	string
			firewallEnabled	The agents supports Firewall Control and it is enabled for the agent's group	false	boolean []
			gatewayIp	Gateway ip	false	string
			gcpServiceAccount__contains	Free-text filter by gcp service account (supports multiple values)	false	string []
			groupIds	List of network groups	false	string []

			hasContainerizedWorkload	Include only Agents protecting containerized workloads	false	boolean
			hasLocalConfiguration	Agent has a local configuration set	false	boolean
			hasTags	Include only Agents that have any tags assigned if True, or none if False	false	boolean
			ids	A list of Agent IDs	false	string []
			infected	Include only Agents with at least one active threat	false	boolean
			installerTypes	Include only Agents installed with these package types	false	string []
			installerTypesNin	Exclude Agents installed with these package types	false	string []
			isActive	Include only active Agents	false	boolean
			isDecommissioned	Include active, decommissioned or both	false	boolean []
			isPendingUninstall	Include only Agents with pending	false	boolean

				uninstall requests		
			isUninstalled	Include installed, uninstalled or both	false	boolean []
			isUpToDate	Include only Agents with updated software	false	boolean
			k8sNodeLabels__contains	Free-text filter by K8s node labels (supports multiple values)	false	string []
			k8sNodeName__contains	Free-text filter by K8s node name (supports multiple values)	false	string []
			k8sType__contains	Free-text filter by K8s type(supports multiple values)	false	string []
			k8sVersion__contains	Free-text filter by K8s version (supports multiple values)	false	string []
			lastActiveDate__between	Date range for last active date(format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			lastActiveDate__gt	Agents last active after	false	string

				this time		
			lastActiveDate__gte	Agents last active after or at this time	false	string
			lastActiveDate__lt	Agents last active before this time	false	string
			lastActiveDate__lte	Agents last active before or at this time	false	string
			lastLoggedInUserName__contains	Free-text filter by username (supports multiple values)	false	string []
			lastSuccessfulScanDate__between	Date range for last successful full disk scan(format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			lastSuccessfulScanDate__gt	Agents last successful full disk scan after this time	false	string
			lastSuccessfulScanDate__gte	Agents last successful full disk scan after or at this time	false	string
			lastSuccessfulScanDate__lt	Agents last successful full disk scan before this time	false	string
			lastSuccessfulScanDate__lt	Agents last successful full	false	string

			e	disk scan before or at this time		
			liveUpdateId__contains	Free-text filter by live update ID (supports multiple values)	false	string []
			locationEnabled	The agents supports Location Awareness and it is enabled for the agent's group	false	boolean []
			locationIds	Include only Agents reporting these locations	false	string []
			locationIdsNin	Do not include only Agents reporting these locations	false	string []
			machineTypes	Included machine types	false	string []
			machineTypesNin	Not included machine types	false	string []
			migrationStatus	Migration status	false	enum
			missingPermissions	Included missing permissions	false	string []
			missingPermissionsNin	Excluded missing permissions	false	string []

			mitigationMode	Agent mitigation mode policy	false	enum
			mitigationModeSuspicious	Mitigation mode policy for suspicious activity	false	enum
			networkInterfaceGatewayMacAddress__contains	Free-text filter by Gateway MAC address (supports multiple values)	false	string []
			networkInterfaceInet__contains	Free-text filter by local IP (supports multiple values)	false	string []
			networkInterfacePhysical__contains	Free-text filter by MAC address (supports multiple values)	false	string []
			networkQuarantineEnabled	The agents supports Network Quarantine Control and its enabled for the agent's group	false	boolean []
			networkStatuses	Included network statuses	false	string []
			networkStatusesNin	Included network statuses	false	string []
			operationalStates	Agent operational state	false	string []

			operationalStatesNin	Do not include these Agent operational states	false	string []
			osArch	OS architecture	false	enum
			osTypes	Included OS types	false	string []
			osTypesNin	Not included OS types	false	string []
			osVersion__contains	Free-text filter by OS full name and version (supports multiple values)	false	string []
			query	A free-text search term, will match applicable attributes (sub-string match). Note: Device's physical addresses will be matched if they start with the search term only (no match if they contain the term).	false	string
			rangerStatus	[DEPRECATED] Use rangerStatuses.	false	enum
			rangerStatuses	Status of Ranger	false	string []

			rangerStatusesNin	Do not include these Ranger Statuses	false	string []
			rangerVersions	Ranger versions to include	false	string []
			rangerVersionsNin	Ranger versions not to include	false	string []
			registeredAt__between	Date range for first registration time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			registeredAt__gt	Agents registered after this time	false	string
			registeredAt__gte	Agents registered after or at this time	false	string
			registeredAt__lt	Agents registered before this time	false	string
			registeredAt__lte	Agents registered before or at this time	false	string
			remoteOpsForensicsSupported	Include only agents that has Remote Ops Forensicsfeature supported	false	boolean
			remoteProfili	Agent remote	false	string []

			ngStates	profiling state		
			remoteProfilingStatesNin	Do not include these Agent remote profiling states	false	string []
			rsoLevel	Supported Remote Script Orchestration level	false	enum
			scanStatus	Scan status	false	enum
			scanStatuses	Included scan statuses	false	string []
			scanStatuses Nin	Not included scan statuses	false	string []
			serialNumber__contains	Free-text filter by Serial Number (supports multiple values)	false	string []
			siteIds	List of Site IDs to filter by	false	string []
			tagsData	Filter agents by their assigned tags. Given in form of a JSON where each key represents a tag key, and each value represents a list of string values to filter by. To filter by unassigned tag values,	false	string

				use __nin suffix in the tag key.		
			threatContentHash	Include only Agents that have at least one threat with this content hash	false	string
			threatCreatedAt__between	Agents with threats reported in a date range (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			threatCreatedAt__gt	Agents with threats reported after this time	false	string
			threatCreatedAt__gte	Agents with threats reported after or at this time	false	string
			threatCreatedAt__lt	Agents with threats reported before this time	false	string
			threatCreatedAt__lte	Agents with threats reported before or at this time	false	string
			threatHidden	Include only Agents with at least one hidden threat	false	boolean

			threatMitigationStatus	Include only Agents that have threats with this mitigation status	false	enum
			threatRebootRequired	Has at least one threat with at least one mitigation action pending reboot to succeed	false	boolean []
			threatResolved	Include only Agents with at least one resolved threat	false	boolean
			totalMemory__between	Total memory range (GB, inclusive)	false	string
			totalMemory__gt	Memory size (MB, more than)	false	integer
			totalMemory__gte	Memory size (MB, more than or equal)	false	integer
			totalMemory__lt	Memory size (MB, less than)	false	integer
			totalMemory__lte	Memory size (MB, less than or equal)	false	integer
			updatedAt__between	Date range for update time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string

			updatedAt__gt	Agents updated after this timestamp	false	string
			updatedAt__gte	Agents updated after or at this timestamp	false	string
			updatedAt__lt	Agents updated before this timestamp	false	string
			updatedAt__lte	Agents updated before or at this timestamp	false	string
			userActionsNeeded	Included pending user actions	false	string []
			userActionsNeededNin	Excluded pending user actions	false	string []
			uuid	Agent's universally unique identifier	false	string
			uuid__contains	Free-text filter by Agent UUID (supports multiple values)	false	string []
			uuids	A list of included UUIDs	false	string []

Get Applications

POST /web/api/v2.1/agents/actions/fetch-installed-apps

Application Risk Management is an EA feature. Contact your partner or SentinelOne SE to learn how to join the EA program.
If you have this feature, you can use this command to have all Agents update the data of the applications that are installed on the endpoint. Change the filter parameter values to send this command to matching Agents only. The updated data of installed applications shows on the Console.
Some filter fields are required.
Best practice: Enter all fields in the body. Click in the Body sample to get a copy of the fields in the body form.

BEST PRACTICE

Enter all fields in the body. Click in the Body sample to get a copy of the fields in the body form.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - Insufficient permissions

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>affected</td><td>Number of entities affected by the requested operation</td><td>false</td><td>integer</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>filter</td><td>Applied filter - only matched Agents will be affected by the requested action. Note: One of these filter arguments must be supplied: ids, groupIds, filterId.</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>activeThreats</td><td>Include Agents with this amount of active threats</td><td>false</td><td>integer</td></tr>
<tr><td>activeThreats__gt</td><td>Include Agents with at least this amount of active threats</td><td>false</td><td>integer</td></tr>
<tr><td>adComputerMember__contains</td><td>Free-text filter by Active Directory computer groups string (supports multiple values)</td><td>false</td><td>string []</td></tr>
<tr><td>adComputerName__contains</td><td>Free-text filter by Active Directory computer name string (supports multiple values)</td><td>false</td><td>string []</td></tr>
<tr><td>adComputerQuery__contains</td><td>Free-text filter by Active Directory computer name or its groups</td><td>false</td><td>string []</td></tr>
</table>
</td></tr>
</table>

				(supports multiple values)		
			adQuery	An Active Directory query string	false	string
			adQuery__contains	Free-text filter by Active Directory string (supports multiple values)	false	string []
			adUserMember__contains	Free-text filter by Active Directory user groups string (supports multiple values)	false	string []
			adUserName__contains	Free-text filter by Active Directory username string (supports multiple values)	false	string []
			adUserQuery__contains	Free-text filter by Active Directory computer name or its groups (supports multiple values)	false	string []
			agentNamespa	Free-text	false	string []

			ce__contains	filter by agent namespace (supports multiple values)		
			agentPodName__contains	Free-text filter by agent pod name (supports multiple values)	false	string []
			agentVersion__between	Version range for agent version (format: <from_version>-<to_version>, inclusive)	false	string
			agentVersion__gt	Agents versions greater than given version	false	string
			agentVersion__gte	Agents versions greater than or equal to given version	false	string
			agentVersion__lt	Agents versions less than given version	false	string
			agentVersion__lte	Agents versions less than or equal to given version	false	string
			agentVersions	Agent versions to include	false	string []
			agentVersionsNin	Agent versions not	false	string []

				to include		
			appsVulnerabilityStatuses	Apps vulnerability status in	false	string []
			appsVulnerabilityStatusesNin	Apps vulnerability status nin	false	string []
			awsRole__contains	Free-text filter by aws role(supports multiple values)	false	string []
			awsSecurityGroups__contains	Free-text filter by aws securityGroups(supports multiple values)	false	string []
			awsSubnetIds__contains	Free-text filter by aws subnet ids (supports multiple values)	false	string []
			azureResourceGroup__contains	Free-text filter by azure resource group(supports multiple values)	false	string []
			cloudAccount__contains	Free-text filter by cloud account (supports multiple values)	false	string []
			cloudImage__contains	Free-text filter by cloud image (supports multiple values)	false	string []

			cloudInstanceId__contains	Free-text filter by cloud instance id(supports multiple values)	false	string []
			cloudInstanceSize__contains	Free-text filter by cloud instance size(supports multiple values)	false	string []
			cloudLocation__contains	Free-text filter by cloud location (supports multiple values)	false	string []
			cloudNetwork__contains	Free-text filter by cloud network (supports multiple values)	false	string []
			cloudProvider	Agents from which cloud provider	false	string []
			cloudProviderNin	Exclude Agents from these cloud provider	false	string []
			cloudTags__contains	Free-text filter by cloud tags (supports multiple values)	false	string []
			clusterName__contains	Free-text filter by cluster name (supports multiple values)	false	string []

			computerName	Computer name	false	string
			computerName__contains	Free-text filter by computer name (supports multiple values)	false	string []
			computerName__like	Match computer name partially (substring)	false	string
			consoleMigrationStatuses	Migration status in	false	string []
			consoleMigrationStatusesNin	Migration status nin	false	string []
			coreCount__between	Possible number of CPU cores (inclusive)	false	string
			coreCount__gt	CPU cores (more than)	false	integer
			coreCount__gte	CPU cores (more than or equal)	false	integer
			coreCount__lt	CPU cores (less than)	false	integer
			coreCount__lte	CPU cores (less than or equal)	false	integer
			cpuCount__between	Possible number of CPU cores (inclusive)	false	string
			cpuCount__gt	Number of CPUs (more than)	false	integer

			cpuCount__gte	Number of CPUs (more than or equal)	false	integer
			cpuCount__lt	Number of CPUs (less than)	false	integer
			cpuCount__lte	Number of CPUs (less than or equal)	false	integer
			cpuId__contains	Free-text filter by CPU name (supports multiple values)	false	string []
			createdAt__between	Date range for creation time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			createdAt__gt	Agents created after this timestamp	false	string
			createdAt__gte	Agents created after or at this timestamp	false	string
			createdAt__lt	Agents created before this timestamp	false	string
			createdAt__lte	Agents created before or at this timestamp	false	string
			csvFilterId	The ID of the CSV file to filter by	false	string

			decommissionedAt__between	Date range for decommission time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			decommissionedAt__gt	Agents decommissioned after this timestamp	false	string
			decommissionedAt__gte	Agents decommissioned after or at this timestamp	false	string
			decommissionedAt__lt	Agents decommissioned before this timestamp	false	string
			decommissionedAt__lte	Agents decommissioned before this timestamp	false	string
			domains	Included network domains	false	string []
			domainsNin	Not included network domains	false	string []
			encryptedApplications	Disk encryption status	false	boolean
			externalId__contains	Free-text filter by external ID (Customer ID)	false	string []
			externalIp__contains	Free-text filter by visible IP (supports	false	string []

				multiple values)		
			filteredGroupIds	List of Group IDs to filter by	false	string []
			filteredSiteIds	List of Site IDs to filter by	false	string []
			filterId	Include all Agents matching this saved filter	false	string
			firewallEnabled	The agents supports Firewall Control and it is enabled for the agent's group	false	boolean []
			gatewayIp	Gateway ip	false	string
			gcpServiceAccount__contains	Free-text filter by gcp service account (supports multiple values)	false	string []
			groupIds	List of network groups	false	string []
			hasContainerizedWorkload	Include only Agents protecting containerized workloads	false	boolean
			hasLocalConfiguration	Agent has a local configuration set	false	boolean
			hasTags	Include only Agents that	false	boolean

				have any tags assigned if True, or none if False		
			ids	A list of Agent IDs	false	string []
			infected	Include only Agents with at least one active threat	false	boolean
			installerTypes	Include only Agents installed with these package types	false	string []
			installerTypesNin	Exclude Agents installed with these package types	false	string []
			isActive	Include only active Agents	false	boolean
			isDecommissioned	Include active, decommissioned or both	false	boolean []
			isPendingUninstall	Include only Agents with pending uninstall requests	false	boolean
			isUninstalled	Include installed, uninstalled or both	false	boolean []
			isUpToDate	Include only Agents with updated software	false	boolean

			k8sNodeLabels__contains	Free-text filter by K8s node labels (supports multiple values)	false	string []
			k8sNodeName__contains	Free-text filter by K8s node name (supports multiple values)	false	string []
			k8sType__contains	Free-text filter by K8s type(supports multiple values)	false	string []
			k8sVersion__contains	Free-text filter by K8s version (supports multiple values)	false	string []
			lastActiveDate__between	Date range for last active date(format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			lastActiveDate__gt	Agents last active after this time	false	string
			lastActiveDate__gte	Agents last active after or at this time	false	string
			lastActiveDate__lt	Agents last active before this time	false	string
			lastActiveDate__lte	Agents last active before or at this time	false	string

			lastLoggedInUserName__contains	Free-text filter by username (supports multiple values)	false	string []
			lastSuccessfulScanDate__between	Date range for last successful full disk scan(format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			lastSuccessfulScanDate__gt	Agents last successful full disk scan after this time	false	string
			lastSuccessfulScanDate__gte	Agents last successful full disk scan after or at this time	false	string
			lastSuccessfulScanDate__lt	Agents last successful full disk scan before this time	false	string
			lastSuccessfulScanDate__lte	Agents last successful full disk scan before or at this time	false	string
			liveUpdateId__contains	Free-text filter by live update ID (supports multiple values)	false	string []
			locationEnabled	The agents supports	false	boolean []

				Location Awareness and it is enabled for the agent's group		
			locationIds	Include only Agents reporting these locations	false	string []
			locationIdsNin	Do not include only Agents reporting these locations	false	string []
			machineTypes	Included machine types	false	string []
			machineTypesNin	Not included machine types	false	string []
			migrationStatus	Migration status	false	enum
			missingPermissions	Included missing permissions	false	string []
			missingPermissionsNin	Excluded missing permissions	false	string []
			mitigationMode	Agent mitigation mode policy	false	enum
			mitigationModeSuspicious	Mitigation mode policy for suspicious activity	false	enum
			networkInterfaceGatewayMacAddress__c	Free-text filter by Gateway	false	string []

			ontains	MAC address (supports multiple values)		
			networkInterfaceInet__contains	Free-text filter by local IP (supports multiple values)	false	string []
			networkInterfacePhysical__contains	Free-text filter by MAC address (supports multiple values)	false	string []
			networkQuarantineEnabled	The agents supports Network Quarantine Control and its enabled for the agent's group	false	boolean []
			networkStatuses	Included network statuses	false	string []
			networkStatusesNin	Included network statuses	false	string []
			operationalStates	Agent operational state	false	string []
			operationalStatesNin	Do not include these Agent operational states	false	string []
			osArch	OS architecture	false	enum
			osTypes	Included OS types	false	string []

			osTypesNin	Not included OS types	false	string []
			osVersion__contains	Free-text filter by OS full name and version (supports multiple values)	false	string []
			query	A free-text search term, will match applicable attributes (sub-string match). Note: Device's physical addresses will be matched if they start with the search term only (no match if they contain the term).	false	string
			rangerStatus	[DEPRECATED] Use rangerStatuses.	false	enum
			rangerStatuses	Status of Ranger	false	string []
			rangerStatusesNin	Do not include these Ranger Statuses	false	string []
			rangerVersions	Ranger versions to include	false	string []
			rangerVersionsNin	Ranger versions not to include	false	string []

			registeredAt__between	Date range for first registration time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			registeredAt__gt	Agents registered after this time	false	string
			registeredAt__gte	Agents registered after or at this time	false	string
			registeredAt__lt	Agents registered before this time	false	string
			registeredAt__lte	Agents registered before or at this time	false	string
			remoteOpsForensicsSupported	Include only agents that has Remote Ops Forensicsfeature supported	false	boolean
			remoteProfilingStates	Agent remote profiling state	false	string []
			remoteProfilingStatesNin	Do not include these Agent remote profiling states	false	string []
			rsoLevel	Supported Remote Script Orchestration	false	enum

				level		
			scanStatus	Scan status	false	enum
			scanStatuses	Included scan statuses	false	string []
			scanStatuses Nin	Not included scan statuses	false	string []
			serialNumber __contains	Free-text filter by Serial Number (supports multiple values)	false	string []
			siteIds	List of Site IDs to filter by	false	string []
			tagsData	Filter agents by their assigned tags. Given in form of a JSON where each key represents a tag key, and each value represents a list of string values to filter by. To filter by unassigned tag values, use __nin suffix in the tag key.	false	string
			threatConten tHash	Include only Agents that have at least one threat with this content hash	false	string
			threatCreate	Agents with	false	string

			dAt__between	threats reported in a date range (format: <from_timestamp>-<to_timestamp>, inclusive)		
			threatCreatedAt__gt	Agents with threats reported after this time	false	string
			threatCreatedAt__gte	Agents with threats reported after or at this time	false	string
			threatCreatedAt__lt	Agents with threats reported before this time	false	string
			threatCreatedAt__lte	Agents with threats reported before or at this time	false	string
			threatHidden	Include only Agents with at least one hidden threat	false	boolean
			threatMitigationStatus	Include only Agents that have threats with this mitigation status	false	enum
			threatRebootRequired	Has at least one threat with at least one mitigation	false	boolean []

				action pending reboot to succeed		
			threatResolved	Include only Agents with at least one resolved threat	false	boolean
			totalMemory__between	Total memory range (GB, inclusive)	false	string
			totalMemory__gt	Memory size (MB, more than)	false	integer
			totalMemory__gte	Memory size (MB, more than or equal)	false	integer
			totalMemory__lt	Memory size (MB, less than)	false	integer
			totalMemory__lte	Memory size (MB, less than or equal)	false	integer
			updatedAt__between	Date range for update time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			updatedAt__gt	Agents updated after this timestamp	false	string
			updatedAt__gte	Agents updated after or at this timestamp	false	string
			updatedAt__lt	Agents updated	false	string

<table>
<tr><td></td><td></td><td></td><td><table>
<tr><td></td><td>before this timestamp</td><td></td><td></td></tr>
<tr><td>updatedAt__lte</td><td>Agents updated before or at this timestamp</td><td>false</td><td>string</td></tr>
<tr><td>userActionsNeeded</td><td>Included pending user actions</td><td>false</td><td>string []</td></tr>
<tr><td>userActionsNeededNin</td><td>Excluded pending user actions</td><td>false</td><td>string []</td></tr>
<tr><td>uuid</td><td>Agent's universally unique identifier</td><td>false</td><td>string</td></tr>
<tr><td>uuid__contains</td><td>Free-text filter by Agent UUID (supports multiple values)</td><td>false</td><td>string []</td></tr>
<tr><td>uuids</td><td>A list of included UUIDs</td><td>false</td><td>string []</td></tr>
</table></td></tr>
<tr><td>data</td><td>Data</td><td>false</td><td></td></tr>
</table>

Start Remote Shell

POST /web/api/v2.1/agents/actions/start-remote-shell

Remote shell is an opened websocket between the browser and the Agent, with a proprietary communication protocol that requires an unreasonable effort to run from the API. We recommend that you not use this call.

If you do want to use this API, you must have permission through your user role (not IT or Viewer), specific Remote Shell permissions, 2FA enabled on the username with a valid code in the twoFaCode parameter, valid code in the twoFaCode parameter, and permissions for the Account, Site, or Group on whose policy Remote Shell is enabled. To make sure you have permission to start Remote Shell, use the "can-start-remote-shell" command. Best practice: Use the UUID filter to run Remote Shell on a specific endpoint. To get the UUID, run the "agents" command.
In the body of this command, the data parameter set is mandatory.
Remote Shell requires a Control SKU.

BEST PRACTICE

Use the UUID filter to run Remote Shell on a specific endpoint. To get the UUID, run the "agents" command.
In the body of this command, the data parameter set is mandatory.
Remote Shell requires a Control SKU.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - Insufficient permissions

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
agentId	Agent that matched the filter	false	string
channelId	Name of the	false	string

				channel that will be used to communicate with the Agent		
errors	Errors	false	array			

Body Schema

Name	Description	Required	Value
data	Data	true	

Name	Description	Required	Value
columns	Number of columns of the console shell	true	integer
rows	Number of rows of the console shell	true	integer
twoFaCode	The 2FA code to authenticate the user	true	string
historyPassword	Password to zip the shell history file at end of session	false	string
passwordFromScope	Used to specify execution where a generic password is used	false	

Name	Description	Required	Value
scopeLevel	User scope	true	enum
scopeId	string repr. of scope id	false	string

filter	Applied filter - only matched Agents will be affected by the requested action. Leave empty to apply the action on all applicable Agents.	true	

Name	Description	Required	Value
accountIds	List of Account IDs to filter by	false	string []
activeThreats	Include Agents with this amount of active threats	false	integer
activeThreats__gt	Include Agents with at least this amount of	false	integer

				active threats			
			adComputerMember__contains	Free-text filter by Active Directory computer groups string (supports multiple values)	false	string []	
			adComputerName__contains	Free-text filter by Active Directory computer name string (supports multiple values)	false	string []	
			adComputerQuery__contains	Free-text filter by Active Directory computer name or its groups (supports multiple values)	false	string []	
			adQuery	An Active Directory query string	false	string	
			adQuery__contains	Free-text filter by Active Directory string (supports multiple values)	false	string []	
			adUserMember__contains	Free-text filter by Active	false	string []	

				Directory user groups string (supports multiple values)			
			adUserName__contains	Free-text filter by Active Directory username string (supports multiple values)	false	string []	
			adUserQuery__contains	Free-text filter by Active Directory computer name or its groups (supports multiple values)	false	string []	
			agentNamespace__contains	Free-text filter by agent namespace (supports multiple values)	false	string []	
			agentPodName__contains	Free-text filter by agent pod name (supports multiple values)	false	string []	
			agentVersion__between	Version range for agent version (format: <from_version>-<to_version>,	false	string	

				inclusive)			
			agentVersion__gt	Agents versions greater than given version	false	string	
			agentVersion__gte	Agents versions greater than or equal to given version	false	string	
			agentVersion__lt	Agents versions less than given version	false	string	
			agentVersion__lte	Agents versions less than or equal to given version	false	string	
			agentVersions	Agent versions to include	false	string []	
			agentVersionsNin	Agent versions not to include	false	string []	
			appsVulnerabilityStatuses	Apps vulnerability status in	false	string []	
			appsVulnerabilityStatusesNin	Apps vulnerability status nin	false	string []	
			awsRole__contains	Free-text filter by aws role(supports multiple values)	false	string []	
			awsSecurityGroups__contains	Free-text filter by aws securityGroups(supports multiple	false	string []	

				values)		
			awsSubnetIds__contains	Free-text filter by aws subnet ids (supports multiple values)	false	string []
			azureResourceGroup__contains	Free-text filter by azure resource group(supports multiple values)	false	string []
			cloudAccount__contains	Free-text filter by cloud account (supports multiple values)	false	string []
			cloudImage__contains	Free-text filter by cloud image (supports multiple values)	false	string []
			cloudInstanceId__contains	Free-text filter by cloud instance id(supports multiple values)	false	string []
			cloudInstanceSize__contains	Free-text filter by cloud instance size(supports multiple values)	false	string []
			cloudLocation__contains	Free-text filter by cloud location (supports multiple values)	false	string []

			cloudNetwork__contains	Free-text filter by cloud network (supports multiple values)	false	string []	
			cloudProvider	Agents from which cloud provider	false	string []	
			cloudProviderNin	Exclude Agents from these cloud provider	false	string []	
			cloudTags__contains	Free-text filter by cloud tags (supports multiple values)	false	string []	
			clusterName__contains	Free-text filter by cluster name (supports multiple values)	false	string []	
			computerName	Computer name	false	string	
			computerName__contains	Free-text filter by computer name (supports multiple values)	false	string []	
			computerName__like	Match computer name partially (substring)	false	string	
			consoleMigrationStatuses	Migration status in	false	string []	
			consoleMigra	Migration	false	string []	

			tionStatusesNin	status nin			
			coreCount__between	Possible number of CPU cores (inclusive)	false	string	
			coreCount__gt	CPU cores (more than)	false	integer	
			coreCount__gte	CPU cores (more than or equal)	false	integer	
			coreCount__lt	CPU cores (less than)	false	integer	
			coreCount__lte	CPU cores (less than or equal)	false	integer	
			cpuCount__between	Possible number of CPU cores (inclusive)	false	string	
			cpuCount__gt	Number of CPUs (more than)	false	integer	
			cpuCount__gte	Number of CPUs (more than or equal)	false	integer	
			cpuCount__lt	Number of CPUs (less than)	false	integer	
			cpuCount__lte	Number of CPUs (less than or equal)	false	integer	
			cpuId__contains	Free-text filter by CPU name (supports multiple values)	false	string []	
			createdAt__between	Date range for creation	false	string	

				time (format: <from_timestamp>-<to_timestamp>, inclusive)		
			createdAt__gt	Agents created after this timestamp	false	string
			createdAt__gte	Agents created after or at this timestamp	false	string
			createdAt__lt	Agents created before this timestamp	false	string
			createdAt__lte	Agents created before or at this timestamp	false	string
			csvFilterId	The ID of the CSV file to filter by	false	string
			decommissionedAt__between	Date range for decommission time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			decommissionedAt__gt	Agents decommissioned after this timestamp	false	string
			decommissionedAt__gte	Agents decommissioned after or at this timestamp	false	string

			decommissionedAt__lt	Agents decommissioned before this timestamp	false	string	
			decommissionedAt__lte	Agents decommissioned before this timestamp	false	string	
			domains	Included network domains	false	string []	
			domainsNin	Not included network domains	false	string []	
			encryptedApplications	Disk encryption status	false	boolean	
			externalId__contains	Free-text filter by external ID (Customer ID)	false	string []	
			externalIp__contains	Free-text filter by visible IP (supports multiple values)	false	string []	
			filteredGroupIds	List of Group IDs to filter by	false	string []	
			filteredSiteIds	List of Site IDs to filter by	false	string []	
			filterId	Include all Agents matching this saved filter	false	string	
			firewallEnabled	The agents supports Firewall Control and it	false	boolean []	

				is enabled for the agent's group		
			gatewayIp	Gateway ip	false	string
			gcpServiceAccount__contains	Free-text filter by gcp service account (supports multiple values)	false	string []
			groupIds	List of Group IDs to filter by	false	string []
			hasContainerizedWorkload	Include only Agents protecting containerized workloads	false	boolean
			hasLocalConfiguration	Agent has a local configuration set	false	boolean
			hasTags	Include only Agents that have any tags assigned if True, or none if False	false	boolean
			ids	A list of Agent IDs	false	string []
			infected	Include only Agents with at least one active threat	false	boolean
			installerTypes	Include only Agents installed with these package types	false	string []

			installerTypesNin	Exclude Agents installed with these package types	false	string []
			isActive	Include only active Agents	false	boolean
			isDecommissioned	Include active, decommissioned or both	false	boolean []
			isPendingUninstall	Include only Agents with pending uninstall requests	false	boolean
			isUninstalled	Include installed, uninstalled or both	false	boolean []
			isUpToDate	Include only Agents with updated software	false	boolean
			k8sNodeLabels__contains	Free-text filter by K8s node labels (supports multiple values)	false	string []
			k8sNodeName__contains	Free-text filter by K8s node name (supports multiple values)	false	string []
			k8sType__contains	Free-text filter by K8s type(supports multiple values)	false	string []

			k8sVersion__contains	Free-text filter by K8s version (supports multiple values)	false	string []	
			lastActiveDate__between	Date range for last active date(format: <from_timestamp>-<to_timestamp>, inclusive)	false	string	
			lastActiveDate__gt	Agents last active after this time	false	string	
			lastActiveDate__gte	Agents last active after or at this time	false	string	
			lastActiveDate__lt	Agents last active before this time	false	string	
			lastActiveDate__lte	Agents last active before or at this time	false	string	
			lastLoggedInUserName__contains	Free-text filter by username (supports multiple values)	false	string []	
			lastSuccessfulScanDate__between	Date range for last successful full disk scan(format: <from_timestamp>-<to_timestamp>, inclusive)	false	string	
			lastSuccessfulScanDate__g	Agents last successful full	false	string	

			t	disk scan after this time		
			lastSuccessfulScanDate__gte	Agents last successful full disk scan after or at this time	false	string
			lastSuccessfulScanDate__lt	Agents last successful full disk scan before this time	false	string
			lastSuccessfulScanDate__lte	Agents last successful full disk scan before or at this time	false	string
			liveUpdateId__contains	Free-text filter by live update ID (supports multiple values)	false	string []
			locationEnabled	The agents supports Location Awareness and it is enabled for the agent's group	false	boolean []
			locationIds	Include only Agents reporting these locations	false	string []
			locationIdsNin	Do not include only Agents reporting these locations	false	string []

			machineTypes	Included machine types	false	string []	
			machineTypesNin	Not included machine types	false	string []	
			migrationStatus	Migration status	false	enum	
			missingPermissions	Included missing permissions	false	string []	
			missingPermissionsNin	Excluded missing permissions	false	string []	
			mitigationMode	Agent mitigation mode policy	false	enum	
			mitigationModeSuspicious	Mitigation mode policy for suspicious activity	false	enum	
			networkInterfaceGatewayMacAddress__contains	Free-text filter by Gateway MAC address (supports multiple values)	false	string []	
			networkInterfaceInet__contains	Free-text filter by local IP (supports multiple values)	false	string []	
			networkInterfacePhysical__contains	Free-text filter by MAC address (supports multiple values)	false	string []	
			networkQuarantineEnabled	The agents supports	false	boolean []	

				Network Quarantine Control and its enabled for the agent's group			
			networkStatuses	Included network statuses	false	string []	
			networkStatusesNin	Included network statuses	false	string []	
			operationalStates	Agent operational state	false	string []	
			operationalStatesNin	Do not include these Agent operational states	false	string []	
			osArch	OS architecture	false	enum	
			osTypes	Included OS types	false	string []	
			osTypesNin	Not included OS types	false	string []	
			osVersion__contains	Free-text filter by OS full name and version (supports multiple values)	false	string []	
			query	A free-text search term, will match applicable attributes (sub-string match). Note: Device's physical	false	string	

				addresses will be matched if they start with the search term only (no match if they contain the term).			
			rangerStatus	[DEPRECATED] Use rangerStatuses.	false	enum	
			rangerStatuses	Status of Ranger	false	string []	
			rangerStatusesNin	Do not include these Ranger Statuses	false	string []	
			rangerVersions	Ranger versions to include	false	string []	
			rangerVersionsNin	Ranger versions not to include	false	string []	
			registeredAt__between	Date range for first registration time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string	
			registeredAt__gt	Agents registered after this time	false	string	
			registeredAt__gte	Agents registered after or at this time	false	string	
			registeredAt__	Agents	false	string	

			lt	registered before this time			
			registeredAt__lte	Agents registered before or at this time	false	string	
			remoteOpsForensicsSupported	Include only agents that has Remote Ops Forensicsfeature supported	false	boolean	
			remoteProfilingStates	Agent remote profiling state	false	string []	
			remoteProfilingStatesNin	Do not include these Agent remote profiling states	false	string []	
			rsoLevel	Supported Remote Script Orchestration level	false	enum	
			scanStatus	Scan status	false	enum	
			scanStatuses	Included scan statuses	false	string []	
			scanStatuses Nin	Not included scan statuses	false	string []	
			serialNumber__contains	Free-text filter by Serial Number (supports multiple values)	false	string []	
			siteIds	List of Site IDs to filter by	false	string []	
			tagsData	Filter agents	false	string	

			by their assigned tags. Given in form of a JSON where each key represents a tag key, and each value represents a list of string values to filter by. To filter by unassigned tag values, use __nin suffix in the tag key.			
			threatContentHash	Include only Agents that have at least one threat with this content hash	false	string
			threatCreatedAt__between	Agents with threats reported in a date range (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			threatCreatedAt__gt	Agents with threats reported after this time	false	string
			threatCreatedAt__gte	Agents with threats reported after or at this time	false	string

			threatCreatedAt__lt	Agents with threats reported before this time	false	string	
			threatCreatedAt__lte	Agents with threats reported before or at this time	false	string	
			threatHidden	Include only Agents with at least one hidden threat	false	boolean	
			threatMitigationStatus	Include only Agents that have threats with this mitigation status	false	enum	
			threatRebootRequired	Has at least one threat with at least one mitigation action pending reboot to succeed	false	boolean []	
			threatResolved	Include only Agents with at least one resolved threat	false	boolean	
			totalMemory__between	Total memory range (GB, inclusive)	false	string	
			totalMemory__gt	Memory size (MB, more than)	false	integer	
			totalMemory__gte	Memory size (MB, more	false	integer	

				than or equal)		
			totalMemory__lt	Memory size (MB, less than)	false	integer
			totalMemory__lte	Memory size (MB, less than or equal)	false	integer
			updatedAt__between	Date range for update time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			updatedAt__gt	Agents updated after this timestamp	false	string
			updatedAt__gte	Agents updated after or at this timestamp	false	string
			updatedAt__lt	Agents updated before this timestamp	false	string
			updatedAt__lte	Agents updated before or at this timestamp	false	string
			userActionsNeeded	Included pending user actions	false	string []
			userActionsNeededNin	Excluded pending user actions	false	string []
			uuid	Agent's universally unique identifier	false	string

			uuid__contains	Free-text filter by Agent UUID (supports multiple values)	false	string []	
			uuids	A list of included UUIDs	false	string []	

Can run Remote Shell

POST /web/api/v2.1/agents/actions/can-start-remote-shell

Who can run Remote Shell? Remote Shell is a powerful way to respond remotely to events on endpoints. It lets you open full shell capabilities - PowerShell on Windows and Bash on macOS and Linux. To be able to run a Remote Shell session, SentinelOne users require permissions, which are set on different levels. It can be confusing to know who has permission. Use this command to see if a username you created for someone else or the API, or your own name, has permission.
If a user does not have Remote Shell permission, how can you grant it? First, you need the Control SKU. Then, the user must have a role with permission to use Remote Shell: Admin, SOC, IR Team. The IT role does not have Remote Shell permission, and the user must be responsible for the Account, Site, or Group on whose policy Remote Shell is enabled.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - Insufficient permissions

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>affected</td><td>Number of entities affected by the requested operation</td><td>false</td><td>integer</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

Name	Description	Required	Value
filter	Applied filter - only matched Agents will be affected by the requested action. Leave empty to apply the action on all applicable Agents.	true	

Name	Description	Required	Value
accountIds	List of Account IDs to filter by	false	string []
activeThreats	Include Agents with this amount of active threats	false	integer
activeThreats__gt	Include Agents with at least this amount of active threats	false	integer
adComputerMember__contains	Free-text filter by Active Directory computer groups string (supports multiple values)	false	string []
adComputerName__contains	Free-text filter by Active Directory computer name string (supports multiple values)	false	string []
adComputerQuery__contains	Free-text filter by Active Directory computer name or its groups	false	string []

				(supports multiple values)		
			adQuery	An Active Directory query string	false	string
			adQuery__contains	Free-text filter by Active Directory string (supports multiple values)	false	string []
			adUserMember__contains	Free-text filter by Active Directory user groups string (supports multiple values)	false	string []
			adUserName__contains	Free-text filter by Active Directory username string (supports multiple values)	false	string []
			adUserQuery__contains	Free-text filter by Active Directory computer name or its groups (supports multiple values)	false	string []
			agentNamespa	Free-text	false	string []

			ce__contains	filter by agent namespace (supports multiple values)		
			agentPodName__contains	Free-text filter by agent pod name (supports multiple values)	false	string []
			agentVersion__between	Version range for agent version (format: <from_version>-<to_version>, inclusive)	false	string
			agentVersion__gt	Agents versions greater than given version	false	string
			agentVersion__gte	Agents versions greater than or equal to given version	false	string
			agentVersion__lt	Agents versions less than given version	false	string
			agentVersion__lte	Agents versions less than or equal to given version	false	string
			agentVersions	Agent versions to include	false	string []
			agentVersionsNin	Agent versions not	false	string []

				to include		
			appsVulnerabilityStatuses	Apps vulnerability status in	false	string []
			appsVulnerabilityStatusesNin	Apps vulnerability status nin	false	string []
			awsRole__contains	Free-text filter by aws role(supports multiple values)	false	string []
			awsSecurityGroups__contains	Free-text filter by aws securityGroups(supports multiple values)	false	string []
			awsSubnetIds__contains	Free-text filter by aws subnet ids (supports multiple values)	false	string []
			azureResourceGroup__contains	Free-text filter by azure resource group(supports multiple values)	false	string []
			cloudAccount__contains	Free-text filter by cloud account (supports multiple values)	false	string []
			cloudImage__contains	Free-text filter by cloud image (supports multiple values)	false	string []

			cloudInstanceId__contains	Free-text filter by cloud instance id(supports multiple values)	false	string []
			cloudInstanceSize__contains	Free-text filter by cloud instance size(supports multiple values)	false	string []
			cloudLocation__contains	Free-text filter by cloud location (supports multiple values)	false	string []
			cloudNetwork__contains	Free-text filter by cloud network (supports multiple values)	false	string []
			cloudProvider	Agents from which cloud provider	false	string []
			cloudProviderNin	Exclude Agents from these cloud provider	false	string []
			cloudTags__contains	Free-text filter by cloud tags (supports multiple values)	false	string []
			clusterName__contains	Free-text filter by cluster name (supports multiple values)	false	string []

			computerName	Computer name	false	string
			computerName__contains	Free-text filter by computer name (supports multiple values)	false	string []
			computerName__like	Match computer name partially (substring)	false	string
			consoleMigrationStatuses	Migration status in	false	string []
			consoleMigrationStatusesNin	Migration status nin	false	string []
			coreCount__between	Possible number of CPU cores (inclusive)	false	string
			coreCount__gt	CPU cores (more than)	false	integer
			coreCount__gte	CPU cores (more than or equal)	false	integer
			coreCount__lt	CPU cores (less than)	false	integer
			coreCount__lte	CPU cores (less than or equal)	false	integer
			cpuCount__between	Possible number of CPU cores (inclusive)	false	string
			cpuCount__gt	Number of CPUs (more than)	false	integer

			cpuCount__gte	Number of CPUs (more than or equal)	false	integer
			cpuCount__lt	Number of CPUs (less than)	false	integer
			cpuCount__lte	Number of CPUs (less than or equal)	false	integer
			cpuId__contains	Free-text filter by CPU name (supports multiple values)	false	string []
			createdAt__between	Date range for creation time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			createdAt__gt	Agents created after this timestamp	false	string
			createdAt__gte	Agents created after or at this timestamp	false	string
			createdAt__lt	Agents created before this timestamp	false	string
			createdAt__lte	Agents created before or at this timestamp	false	string
			csvFilterId	The ID of the CSV file to filter by	false	string

			decommissionedAt__between	Date range for decommission time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			decommissionedAt__gt	Agents decommissioned after this timestamp	false	string
			decommissionedAt__gte	Agents decommissioned after or at this timestamp	false	string
			decommissionedAt__lt	Agents decommissioned before this timestamp	false	string
			decommissionedAt__lte	Agents decommissioned before this timestamp	false	string
			domains	Included network domains	false	string []
			domainsNin	Not included network domains	false	string []
			encryptedApplications	Disk encryption status	false	boolean
			externalId__contains	Free-text filter by external ID (Customer ID)	false	string []
			externalIp__contains	Free-text filter by visible IP (supports	false	string []

				multiple values)		
			filteredGroupIds	List of Group IDs to filter by	false	string []
			filteredSiteIds	List of Site IDs to filter by	false	string []
			filterId	Include all Agents matching this saved filter	false	string
			firewallEnabled	The agents supports Firewall Control and it is enabled for the agent's group	false	boolean []
			gatewayIp	Gateway ip	false	string
			gcpServiceAccount__contains	Free-text filter by gcp service account (supports multiple values)	false	string []
			groupIds	List of Group IDs to filter by	false	string []
			hasContainerizedWorkload	Include only Agents protecting containerized workloads	false	boolean
			hasLocalConfiguration	Agent has a local configuration set	false	boolean
			hasTags	Include only Agents that	false	boolean

				have any tags assigned if True, or none if False		
			ids	A list of Agent IDs	false	string []
			infected	Include only Agents with at least one active threat	false	boolean
			installerTypes	Include only Agents installed with these package types	false	string []
			installerTypesNin	Exclude Agents installed with these package types	false	string []
			isActive	Include only active Agents	false	boolean
			isDecommissioned	Include active, decommissioned or both	false	boolean []
			isPendingUninstall	Include only Agents with pending uninstall requests	false	boolean
			isUninstalled	Include installed, uninstalled or both	false	boolean []
			isUpToDate	Include only Agents with updated software	false	boolean

			k8sNodeLabels__contains	Free-text filter by K8s node labels (supports multiple values)	false	string []
			k8sNodeName__contains	Free-text filter by K8s node name (supports multiple values)	false	string []
			k8sType__contains	Free-text filter by K8s type(supports multiple values)	false	string []
			k8sVersion__contains	Free-text filter by K8s version (supports multiple values)	false	string []
			lastActiveDate__between	Date range for last active date(format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			lastActiveDate__gt	Agents last active after this time	false	string
			lastActiveDate__gte	Agents last active after or at this time	false	string
			lastActiveDate__lt	Agents last active before this time	false	string
			lastActiveDate__lte	Agents last active before or at this time	false	string

			lastLoggedInUserName__contains	Free-text filter by username (supports multiple values)	false	string []
			lastSuccessfulScanDate__between	Date range for last successful full disk scan(format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			lastSuccessfulScanDate__gt	Agents last successful full disk scan after this time	false	string
			lastSuccessfulScanDate__gte	Agents last successful full disk scan after or at this time	false	string
			lastSuccessfulScanDate__lt	Agents last successful full disk scan before this time	false	string
			lastSuccessfulScanDate__lte	Agents last successful full disk scan before or at this time	false	string
			liveUpdateId__contains	Free-text filter by live update ID (supports multiple values)	false	string []
			locationEnabled	The agents supports	false	boolean []

				Location Awareness and it is enabled for the agent's group		
			locationIds	Include only Agents reporting these locations	false	string []
			locationIdsNin	Do not include only Agents reporting these locations	false	string []
			machineTypes	Included machine types	false	string []
			machineTypesNin	Not included machine types	false	string []
			migrationStatus	Migration status	false	enum
			missingPermissions	Included missing permissions	false	string []
			missingPermissionsNin	Excluded missing permissions	false	string []
			mitigationMode	Agent mitigation mode policy	false	enum
			mitigationModeSuspicious	Mitigation mode policy for suspicious activity	false	enum
			networkInterfaceGatewayMacAddress__c	Free-text filter by Gateway	false	string []

			ontains	MAC address (supports multiple values)		
			networkInterfaceInet__contains	Free-text filter by local IP (supports multiple values)	false	string []
			networkInterfacePhysical__contains	Free-text filter by MAC address (supports multiple values)	false	string []
			networkQuarantineEnabled	The agents supports Network Quarantine Control and its enabled for the agent's group	false	boolean []
			networkStatuses	Included network statuses	false	string []
			networkStatusesNin	Included network statuses	false	string []
			operationalStates	Agent operational state	false	string []
			operationalStatesNin	Do not include these Agent operational states	false	string []
			osArch	OS architecture	false	enum
			osTypes	Included OS types	false	string []

			osTypesNin	Not included OS types	false	string []
			osVersion__contains	Free-text filter by OS full name and version (supports multiple values)	false	string []
			query	A free-text search term, will match applicable attributes (sub-string match). Note: Device's physical addresses will be matched if they start with the search term only (no match if they contain the term).	false	string
			rangerStatus	[DEPRECATED] Use rangerStatuses.	false	enum
			rangerStatuses	Status of Ranger	false	string []
			rangerStatusesNin	Do not include these Ranger Statuses	false	string []
			rangerVersions	Ranger versions to include	false	string []
			rangerVersionsNin	Ranger versions not to include	false	string []

			registeredAt__between	Date range for first registration time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			registeredAt__gt	Agents registered after this time	false	string
			registeredAt__gte	Agents registered after or at this time	false	string
			registeredAt__lt	Agents registered before this time	false	string
			registeredAt__lte	Agents registered before or at this time	false	string
			remoteOpsForensicsSupported	Include only agents that has Remote Ops Forensicsfeature supported	false	boolean
			remoteProfilingStates	Agent remote profiling state	false	string []
			remoteProfilingStatesNin	Do not include these Agent remote profiling states	false	string []
			rsoLevel	Supported Remote Script Orchestration	false	enum

				level		
			scanStatus	Scan status	false	enum
			scanStatuses	Included scan statuses	false	string []
			scanStatuses Nin	Not included scan statuses	false	string []
			serialNumber __contains	Free-text filter by Serial Number (supports multiple values)	false	string []
			siteIds	List of Site IDs to filter by	false	string []
			tagsData	Filter agents by their assigned tags. Given in form of a JSON where each key represents a tag key, and each value represents a list of string values to filter by. To filter by unassigned tag values, use __nin suffix in the tag key.	false	string
			threatConten tHash	Include only Agents that have at least one threat with this content hash	false	string
			threatCreate	Agents with	false	string

			dAt__between	threats reported in a date range (format: <from_timestamp>-<to_timestamp>, inclusive)		
			threatCreatedAt__gt	Agents with threats reported after this time	false	string
			threatCreatedAt__gte	Agents with threats reported after or at this time	false	string
			threatCreatedAt__lt	Agents with threats reported before this time	false	string
			threatCreatedAt__lte	Agents with threats reported before or at this time	false	string
			threatHidden	Include only Agents with at least one hidden threat	false	boolean
			threatMitigationStatus	Include only Agents that have threats with this mitigation status	false	enum
			threatRebootRequired	Has at least one threat with at least one mitigation	false	boolean []

				action pending reboot to succeed		
			threatResolved	Include only Agents with at least one resolved threat	false	boolean
			totalMemory__between	Total memory range (GB, inclusive)	false	string
			totalMemory__gt	Memory size (MB, more than)	false	integer
			totalMemory__gte	Memory size (MB, more than or equal)	false	integer
			totalMemory__lt	Memory size (MB, less than)	false	integer
			totalMemory__lte	Memory size (MB, less than or equal)	false	integer
			updatedAt__between	Date range for update time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			updatedAt__gt	Agents updated after this timestamp	false	string
			updatedAt__gte	Agents updated after or at this timestamp	false	string
			updatedAt__lt	Agents updated	false	string

			before this timestamp		
	updatedAt__lte	Agents updated before or at this timestamp	false	string
	userActionsNeeded	Included pending user actions	false	string []
	userActionsNeededNin	Excluded pending user actions	false	string []
	uuid	Agent's universally unique identifier	false	string
	uuid__contains	Free-text filter by Agent UUID (supports multiple values)	false	string []
	uuids	A list of included UUIDs	false	string []
data	Data	false	

Terminate Remote Shell

POST /web/api/v2.1/agents/actions/terminate-remote-shell

Remote Shell is a powerful, full shell for Windows, macOS, and Linux. It is best practice to terminate Remote Shell sessions when they are not in use. A Remote Shell session terminates when the user closes the session, the session times out, or the session is idle longer than the idle-timeout.
Use this command terminate a session immediately.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - Insufficient permissions

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>affected</td><td>Number of entities affected by the requested operation</td><td>false</td><td>integer</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>channelId</td><td>The channel the user is closing</td><td>true</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>filter</td><td>Applied filter - only matched Agents will be affected by the requested action. Leave empty to apply the action on all applicable Agents.</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>activeThreats</td><td>Include Agents with this amount of active threats</td><td>false</td><td>integer</td></tr>
<tr><td>activeThreats__gt</td><td>Include Agents with at least this amount of active threats</td><td>false</td><td>integer</td></tr>
<tr><td>adComputerMember__contains</td><td>Free-text filter by Active Directory computer groups string (supports multiple values)</td><td>false</td><td>string []</td></tr>
<tr><td>adComputerName__contains</td><td>Free-text filter by Active Directory computer name string (supports multiple values)</td><td>false</td><td>string []</td></tr>
<tr><td>adComputerQ</td><td>Free-text</td><td>false</td><td>string []</td></tr>
</table>
</td></tr>
</table>

			uery__contains	filter by Active Directory computer name or its groups (supports multiple values)		
			adQuery	An Active Directory query string	false	string
			adQuery__contains	Free-text filter by Active Directory string (supports multiple values)	false	string []
			adUserMember__contains	Free-text filter by Active Directory user groups string (supports multiple values)	false	string []
			adUserName__contains	Free-text filter by Active Directory username string (supports multiple values)	false	string []
			adUserQuery__contains	Free-text filter by Active Directory computer name or its	false	string []

				groups (supports multiple values)		
			agentNamespace__contains	Free-text filter by agent namespace (supports multiple values)	false	string []
			agentPodName__contains	Free-text filter by agent pod name (supports multiple values)	false	string []
			agentVersion__between	Version range for agent version (format: <from_version>-<to_version>, inclusive)	false	string
			agentVersion__gt	Agents versions greater than given version	false	string
			agentVersion__gte	Agents versions greater than or equal to given version	false	string
			agentVersion__lt	Agents versions less than given version	false	string
			agentVersion__lte	Agents versions less than or equal to given version	false	string

			agentVersions	Agent versions to include	false	string []
			agentVersionsNin	Agent versions not to include	false	string []
			appsVulnerabilityStatuses	Apps vulnerability status in	false	string []
			appsVulnerabilityStatusesNin	Apps vulnerability status nin	false	string []
			awsRole__contains	Free-text filter by aws role(supports multiple values)	false	string []
			awsSecurityGroups__contains	Free-text filter by aws securityGroups(supports multiple values)	false	string []
			awsSubnetIds__contains	Free-text filter by aws subnet ids (supports multiple values)	false	string []
			azureResourceGroup__contains	Free-text filter by azure resource group(supports multiple values)	false	string []
			cloudAccount__contains	Free-text filter by cloud account (supports multiple values)	false	string []
			cloudImage__	Free-text	false	string []

			contains	filter by cloud image (supports multiple values)		
			cloudInstanceId__contains	Free-text filter by cloud instance id(supports multiple values)	false	string []
			cloudInstanceSize__contains	Free-text filter by cloud instance size(supports multiple values)	false	string []
			cloudLocation__contains	Free-text filter by cloud location (supports multiple values)	false	string []
			cloudNetwork__contains	Free-text filter by cloud network (supports multiple values)	false	string []
			cloudProvider	Agents from which cloud provider	false	string []
			cloudProviderNin	Exclude Agents from these cloud provider	false	string []
			cloudTags__contains	Free-text filter by cloud tags (supports multiple values)	false	string []

			clusterName__contains	Free-text filter by cluster name (supports multiple values)	false	string []
			computerName	Computer name	false	string
			computerName__contains	Free-text filter by computer name (supports multiple values)	false	string []
			computerName__like	Match computer name partially (substring)	false	string
			consoleMigrationStatuses	Migration status in	false	string []
			consoleMigrationStatusesNin	Migration status nin	false	string []
			coreCount__between	Possible number of CPU cores (inclusive)	false	string
			coreCount__gt	CPU cores (more than)	false	integer
			coreCount__gte	CPU cores (more than or equal)	false	integer
			coreCount__lt	CPU cores (less than)	false	integer
			coreCount__lte	CPU cores (less than or equal)	false	integer
			cpuCount__between	Possible number of	false	string

				CPU cores (inclusive)		
			cpuCount__gt	Number of CPUs (more than)	false	integer
			cpuCount__gte	Number of CPUs (more than or equal)	false	integer
			cpuCount__lt	Number of CPUs (less than)	false	integer
			cpuCount__lte	Number of CPUs (less than or equal)	false	integer
			cpuId__contains	Free-text filter by CPU name (supports multiple values)	false	string []
			createdAt__between	Date range for creation time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			createdAt__gt	Agents created after this timestamp	false	string
			createdAt__gte	Agents created after or at this timestamp	false	string
			createdAt__lt	Agents created before this timestamp	false	string
			createdAt__lte	Agents created	false	string

				before or at this timestamp		
			csvFilterId	The ID of the CSV file to filter by	false	string
			decommissionedAt__between	Date range for decommission time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			decommissionedAt__gt	Agents decommissioned after this timestamp	false	string
			decommissionedAt__gte	Agents decommissioned after or at this timestamp	false	string
			decommissionedAt__lt	Agents decommissioned before this timestamp	false	string
			decommissionedAt__lte	Agents decommissioned before this timestamp	false	string
			domains	Included network domains	false	string []
			domainsNin	Not included network domains	false	string []
			encryptedApplications	Disk encryption status	false	boolean
			externalId__c	Free-text	false	string []

			ontains	filter by external ID (Customer ID)		
			externalIp__contains	Free-text filter by visible IP (supports multiple values)	false	string []
			filteredGroupIds	List of Group IDs to filter by	false	string []
			filteredSiteIds	List of Site IDs to filter by	false	string []
			filterId	Include all Agents matching this saved filter	false	string
			firewallEnabled	The agents supports Firewall Control and it is enabled for the agent's group	false	boolean []
			gatewayIp	Gateway ip	false	string
			gcpServiceAccount__contains	Free-text filter by gcp service account (supports multiple values)	false	string []
			groupIds	List of Group IDs to filter by	false	string []
			hasContainerizedWorkload	Include only Agents protecting containerized workloads	false	boolean

			hasLocalConfiguration	Agent has a local configuration set	false	boolean
			hasTags	Include only Agents that have any tags assigned if True, or none if False	false	boolean
			ids	A list of Agent IDs	false	string []
			infected	Include only Agents with at least one active threat	false	boolean
			installerTypes	Include only Agents installed with these package types	false	string []
			installerTypesNin	Exclude Agents installed with these package types	false	string []
			isActive	Include only active Agents	false	boolean
			isDecommissioned	Include active, decommissioned or both	false	boolean []
			isPendingUninstall	Include only Agents with pending uninstall requests	false	boolean
			isUninstalled	Include installed, uninstalled or	false	boolean []

				both		
			isUpToDate	Include only Agents with updated software	false	boolean
			k8sNodeLabels__contains	Free-text filter by K8s node labels (supports multiple values)	false	string []
			k8sNodeName__contains	Free-text filter by K8s node name (supports multiple values)	false	string []
			k8sType__contains	Free-text filter by K8s type(supports multiple values)	false	string []
			k8sVersion__contains	Free-text filter by K8s version (supports multiple values)	false	string []
			lastActiveDate__between	Date range for last active date(format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			lastActiveDate__gt	Agents last active after this time	false	string
			lastActiveDate__gte	Agents last active after or at this time	false	string
			lastActiveDat	Agents last	false	string

			e__lt	active before this time		
			lastActiveDate__lte	Agents last active before or at this time	false	string
			lastLoggedInUserName__contains	Free-text filter by username (supports multiple values)	false	string []
			lastSuccessfulScanDate__between	Date range for last successful full disk scan(format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			lastSuccessfulScanDate__gt	Agents last successful full disk scan after this time	false	string
			lastSuccessfulScanDate__gte	Agents last successful full disk scan after or at this time	false	string
			lastSuccessfulScanDate__lt	Agents last successful full disk scan before this time	false	string
			lastSuccessfulScanDate__lte	Agents last successful full disk scan before or at this time	false	string
			liveUpdateId__contains	Free-text filter by live	false	string []

				update ID (supports multiple values)		
			locationEnabled	The agents supports Location Awareness and it is enabled for the agent's group	false	boolean []
			locationIds	Include only Agents reporting these locations	false	string []
			locationIdsNin	Do not include only Agents reporting these locations	false	string []
			machineTypes	Included machine types	false	string []
			machineTypesNin	Not included machine types	false	string []
			migrationStatus	Migration status	false	enum
			missingPermissions	Included missing permissions	false	string []
			missingPermissionsNin	Excluded missing permissions	false	string []
			mitigationMode	Agent mitigation mode policy	false	enum
			mitigationMo	Mitigation	false	enum

			deSuspicious	mode policy for suspicious activity		
			networkInterfaceGatewayMacAddress__contains	Free-text filter by Gateway MAC address (supports multiple values)	false	string []
			networkInterfaceInet__contains	Free-text filter by local IP (supports multiple values)	false	string []
			networkInterfacePhysical__contains	Free-text filter by MAC address (supports multiple values)	false	string []
			networkQuarantineEnabled	The agents supports Network Quarantine Control and its enabled for the agent's group	false	boolean []
			networkStatuses	Included network statuses	false	string []
			networkStatusesNin	Included network statuses	false	string []
			operationalStates	Agent operational state	false	string []
			operationalStatesNin	Do not include these Agent operational	false	string []

				states		
			osArch	OS architecture	false	enum
			osTypes	Included OS types	false	string []
			osTypesNin	Not included OS types	false	string []
			osVersion__contains	Free-text filter by OS full name and version (supports multiple values)	false	string []
			query	A free-text search term, will match applicable attributes (sub-string match). Note: Device's physical addresses will be matched if they start with the search term only (no match if they contain the term).	false	string
			rangerStatus	[DEPRECATED] Use rangerStatuses.	false	enum
			rangerStatuses	Status of Ranger	false	string []
			rangerStatusesNin	Do not include these Ranger Statuses	false	string []

			rangerVersions	Ranger versions to include	false	string []
			rangerVersionsNin	Ranger versions not to include	false	string []
			registeredAt__between	Date range for first registration time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			registeredAt__gt	Agents registered after this time	false	string
			registeredAt__gte	Agents registered after or at this time	false	string
			registeredAt__lt	Agents registered before this time	false	string
			registeredAt__lte	Agents registered before or at this time	false	string
			remoteOpsForensicsSupported	Include only agents that has Remote Ops Forensicsfeature supported	false	boolean
			remoteProfilingStates	Agent remote profiling state	false	string []
			remoteProfilingStatesNin	Do not include these Agent remote	false	string []

				profiling states		
			rsoLevel	Supported Remote Script Orchestration level	false	enum
			scanStatus	Scan status	false	enum
			scanStatuses	Included scan statuses	false	string []
			scanStatuses Nin	Not included scan statuses	false	string []
			serialNumber __contains	Free-text filter by Serial Number (supports multiple values)	false	string []
			siteIds	List of Site IDs to filter by	false	string []
			tagsData	Filter agents by their assigned tags. Given in form of a JSON where each key represents a tag key, and each value represents a list of string values to filter by. To filter by unassigned tag values, use __nin suffix in the tag key.	false	string
			threatConten	Include only	false	string

			tHash	Agents that have at least one threat with this content hash		
			threatCreatedAt__between	Agents with threats reported in a date range (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			threatCreatedAt__gt	Agents with threats reported after this time	false	string
			threatCreatedAt__gte	Agents with threats reported after or at this time	false	string
			threatCreatedAt__lt	Agents with threats reported before this time	false	string
			threatCreatedAt__lte	Agents with threats reported before or at this time	false	string
			threatHidden	Include only Agents with at least one hidden threat	false	boolean
			threatMitigationStatus	Include only Agents that have threats with this mitigation	false	enum

				status		
			threatRebootRequired	Has at least one threat with at least one mitigation action pending reboot to succeed	false	boolean []
			threatResolved	Include only Agents with at least one resolved threat	false	boolean
			totalMemory__between	Total memory range (GB, inclusive)	false	string
			totalMemory__gt	Memory size (MB, more than)	false	integer
			totalMemory__gte	Memory size (MB, more than or equal)	false	integer
			totalMemory__lt	Memory size (MB, less than)	false	integer
			totalMemory__lte	Memory size (MB, less than or equal)	false	integer
			updatedAt__between	Date range for update time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			updatedAt__gt	Agents updated after this timestamp	false	string

			updatedAt__gte	Agents updated after or at this timestamp	false	string
			updatedAt__lt	Agents updated before this timestamp	false	string
			updatedAt__lte	Agents updated before or at this timestamp	false	string
			userActionsNeeded	Included pending user actions	false	string []
			userActionsNeededNin	Excluded pending user actions	false	string []
			uuid	Agent's universally unique identifier	false	string
			uuid__contains	Free-text filter by Agent UUID (supports multiple values)	false	string []
			uuids	A list of included UUIDs	false	string []

Fetch Firewall Logs

POST /web/api/v2.1/agents/actions/firewall-logging

Get Firewall Control events in the local log file, written in clear text, for Firewall Control events of an endpoint with Firewall Control enabled. Enable the logs for Agents that match the filter.
When Firewall Logging is enabled, you can choose if blocked traffic events go only to a local log on the endpoint (reportMgmt: false, reportLog: true), or also to Console > Activity (reportMgmt: true).
Allowed traffic is not logged.
Each Agent with Firewall Control Event Logging enabled keeps five log files, for a total of 100 MB maximum. The logs cycle older lines to maintain the size threshold.
On Windows endpoints, the Firewall Control logs are in C:\ProgramData\Sentinel\logs\. Search for log files with "visible" in the filename.
On macOS, run: sudo sentinelctl log.
On Linux, run: sudo /opt/sentinelone/bin/sentinelctl log generate /output_path.
Make sure the Group and Site of the Agent has Firewall Control enabled. Firewall Control requires a Control SKU.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - Insufficient permissions

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>affected</td><td>Number of entities affected by the requested operation</td><td>false</td><td>integer</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>reportLog</td><td>Report blocking activity to log</td><td>true</td><td>boolean</td></tr>
<tr><td>reportMgmt</td><td>Report blocking activity to management</td><td>true</td><td>boolean</td></tr>
</table>
</td></tr>
<tr><td>filter</td><td>Applied filter - only matched Agents will be affected by the requested action. Leave empty to apply the action on all applicable Agents.</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>activeThreats</td><td>Include Agents with this amount of active threats</td><td>false</td><td>integer</td></tr>
<tr><td>activeThreats__gt</td><td>Include Agents with at least this amount of active threats</td><td>false</td><td>integer</td></tr>
<tr><td>adComputerMember__contains</td><td>Free-text filter by Active Directory computer groups string (supports multiple values)</td><td>false</td><td>string []</td></tr>
<tr><td>adComputerName__contains</td><td>Free-text filter by Active Directory computer name string</td><td>false</td><td>string []</td></tr>
</table>
</td></tr>
</table>

				(supports multiple values)		
			adComputerQuery__contains	Free-text filter by Active Directory computer name or its groups (supports multiple values)	false	string []
			adQuery	An Active Directory query string	false	string
			adQuery__contains	Free-text filter by Active Directory string (supports multiple values)	false	string []
			adUserMember__contains	Free-text filter by Active Directory user groups string (supports multiple values)	false	string []
			adUserName__contains	Free-text filter by Active Directory username string (supports multiple values)	false	string []
			adUserQuery_	Free-text	false	string []

			_contains	filter by Active Directory computer name or its groups (supports multiple values)		
			agentNamespace__contains	Free-text filter by agent namespace (supports multiple values)	false	string []
			agentPodName__contains	Free-text filter by agent pod name (supports multiple values)	false	string []
			agentVersion__between	Version range for agent version (format: <from_version>-<to_version>, inclusive)	false	string
			agentVersion__gt	Agents versions greater than given version	false	string
			agentVersion__gte	Agents versions greater than or equal to given version	false	string
			agentVersion__lt	Agents versions less than given version	false	string
			agentVersion_	Agents	false	string

			_lte	versions less than or equal to given version		
			agentVersions	Agent versions to include	false	string []
			agentVersionsNin	Agent versions not to include	false	string []
			appsVulnerabilityStatuses	Apps vulnerability status in	false	string []
			appsVulnerabilityStatusesNin	Apps vulnerability status nin	false	string []
			awsRole__contains	Free-text filter by aws role(supports multiple values)	false	string []
			awsSecurityGroups__contains	Free-text filter by aws securityGroups(supports multiple values)	false	string []
			awsSubnetIds__contains	Free-text filter by aws subnet ids (supports multiple values)	false	string []
			azureResourceGroup__contains	Free-text filter by azure resource group(supports multiple values)	false	string []
			cloudAccount__contains	Free-text filter by cloud account	false	string []

				(supports multiple values)		
			cloudImage__contains	Free-text filter by cloud image (supports multiple values)	false	string []
			cloudInstanceId__contains	Free-text filter by cloud instance id(supports multiple values)	false	string []
			cloudInstanceSize__contains	Free-text filter by cloud instance size(supports multiple values)	false	string []
			cloudLocation__contains	Free-text filter by cloud location (supports multiple values)	false	string []
			cloudNetwork__contains	Free-text filter by cloud network (supports multiple values)	false	string []
			cloudProvider	Agents from which cloud provider	false	string []
			cloudProviderNin	Exclude Agents from these cloud provider	false	string []
			cloudTags__contains	Free-text filter by cloud	false	string []

				tags (supports multiple values)		
			clusterName__contains	Free-text filter by cluster name (supports multiple values)	false	string []
			computerName	Computer name	false	string
			computerName__contains	Free-text filter by computer name (supports multiple values)	false	string []
			computerName__like	Match computer name partially (substring)	false	string
			consoleMigrationStatuses	Migration status in	false	string []
			consoleMigrationStatusesNin	Migration status nin	false	string []
			coreCount__between	Possible number of CPU cores (inclusive)	false	string
			coreCount__gt	CPU cores (more than)	false	integer
			coreCount__gte	CPU cores (more than or equal)	false	integer
			coreCount__lt	CPU cores (less than)	false	integer
			coreCount__l	CPU cores	false	integer

			te	(less than or equal)		
			cpuCount__between	Possible number of CPU cores (inclusive)	false	string
			cpuCount__gt	Number of CPUs (more than)	false	integer
			cpuCount__gte	Number of CPUs (more than or equal)	false	integer
			cpuCount__lt	Number of CPUs (less than)	false	integer
			cpuCount__lte	Number of CPUs (less than or equal)	false	integer
			cpuId__contains	Free-text filter by CPU name (supports multiple values)	false	string []
			createdAt__between	Date range for creation time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			createdAt__gt	Agents created after this timestamp	false	string
			createdAt__gte	Agents created after or at this timestamp	false	string
			createdAt__lt	Agents created	false	string

				before this timestamp		
			createdAt__lte	Agents created before or at this timestamp	false	string
			csvFilterId	The ID of the CSV file to filter by	false	string
			decommissionedAt__between	Date range for decommission time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			decommissionedAt__gt	Agents decommissioned after this timestamp	false	string
			decommissionedAt__gte	Agents decommissioned after or at this timestamp	false	string
			decommissionedAt__lt	Agents decommissioned before this timestamp	false	string
			decommissionedAt__lte	Agents decommissioned before this timestamp	false	string
			domains	Included network domains	false	string []
			domainsNin	Not included network domains	false	string []

			encryptedApplications	Disk encryption status	false	boolean
			externalId__contains	Free-text filter by external ID (Customer ID)	false	string []
			externalIp__contains	Free-text filter by visible IP (supports multiple values)	false	string []
			filteredGroupIds	List of Group IDs to filter by	false	string []
			filteredSiteIds	List of Site IDs to filter by	false	string []
			filterId	Include all Agents matching this saved filter	false	string
			firewallEnabled	The agents supports Firewall Control and it is enabled for the agent's group	false	boolean []
			gatewayIp	Gateway ip	false	string
			gcpServiceAccount__contains	Free-text filter by gcp service account (supports multiple values)	false	string []
			groupIds	List of Group IDs to filter by	false	string []

			hasContainerizedWorkload	Include only Agents protecting containerized workloads	false	boolean
			hasLocalConfiguration	Agent has a local configuration set	false	boolean
			hasTags	Include only Agents that have any tags assigned if True, or none if False	false	boolean
			ids	A list of Agent IDs	false	string []
			infected	Include only Agents with at least one active threat	false	boolean
			installerTypes	Include only Agents installed with these package types	false	string []
			installerTypesNin	Exclude Agents installed with these package types	false	string []
			isActive	Include only active Agents	false	boolean
			isDecommissioned	Include active, decommissioned or both	false	boolean []
			isPendingUninstall	Include only Agents with pending	false	boolean

				uninstall requests		
			isUninstalled	Include installed, uninstalled or both	false	boolean []
			isUpToDate	Include only Agents with updated software	false	boolean
			k8sNodeLabels__contains	Free-text filter by K8s node labels (supports multiple values)	false	string []
			k8sNodeName__contains	Free-text filter by K8s node name (supports multiple values)	false	string []
			k8sType__contains	Free-text filter by K8s type(supports multiple values)	false	string []
			k8sVersion__contains	Free-text filter by K8s version (supports multiple values)	false	string []
			lastActiveDate__between	Date range for last active date(format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			lastActiveDate__gt	Agents last active after	false	string

				this time		
			lastActiveDate__gte	Agents last active after or at this time	false	string
			lastActiveDate__lt	Agents last active before this time	false	string
			lastActiveDate__lte	Agents last active before or at this time	false	string
			lastLoggedInUserName__contains	Free-text filter by username (supports multiple values)	false	string []
			lastSuccessfulScanDate__between	Date range for last successful full disk scan(format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			lastSuccessfulScanDate__gt	Agents last successful full disk scan after this time	false	string
			lastSuccessfulScanDate__gte	Agents last successful full disk scan after or at this time	false	string
			lastSuccessfulScanDate__lt	Agents last successful full disk scan before this time	false	string
			lastSuccessfulScanDate__lt	Agents last successful full	false	string

			e	disk scan before or at this time		
			liveUpdateId__contains	Free-text filter by live update ID (supports multiple values)	false	string []
			locationEnabled	The agents supports Location Awareness and it is enabled for the agent's group	false	boolean []
			locationIds	Include only Agents reporting these locations	false	string []
			locationIdsNin	Do not include only Agents reporting these locations	false	string []
			machineTypes	Included machine types	false	string []
			machineTypesNin	Not included machine types	false	string []
			migrationStatus	Migration status	false	enum
			missingPermissions	Included missing permissions	false	string []
			missingPermissionsNin	Excluded missing permissions	false	string []

			mitigationMode	Agent mitigation mode policy	false	enum
			mitigationModeSuspicious	Mitigation mode policy for suspicious activity	false	enum
			networkInterfaceGatewayMacAddress__contains	Free-text filter by Gateway MAC address (supports multiple values)	false	string []
			networkInterfaceInet__contains	Free-text filter by local IP (supports multiple values)	false	string []
			networkInterfacePhysical__contains	Free-text filter by MAC address (supports multiple values)	false	string []
			networkQuarantineEnabled	The agents supports Network Quarantine Control and its enabled for the agent's group	false	boolean []
			networkStatuses	Included network statuses	false	string []
			networkStatusesNin	Included network statuses	false	string []
			operationalStates	Agent operational state	false	string []

			operationalStatesNin	Do not include these Agent operational states	false	string []
			osArch	OS architecture	false	enum
			osTypes	Included OS types	false	string []
			osTypesNin	Not included OS types	false	string []
			osVersion__contains	Free-text filter by OS full name and version (supports multiple values)	false	string []
			query	A free-text search term, will match applicable attributes (sub-string match). Note: Device's physical addresses will be matched if they start with the search term only (no match if they contain the term).	false	string
			rangerStatus	[DEPRECATED] Use rangerStatuses.	false	enum
			rangerStatuses	Status of Ranger	false	string []

			rangerStatusesNin	Do not include these Ranger Statuses	false	string []
			rangerVersions	Ranger versions to include	false	string []
			rangerVersionsNin	Ranger versions not to include	false	string []
			registeredAt__between	Date range for first registration time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			registeredAt__gt	Agents registered after this time	false	string
			registeredAt__gte	Agents registered after or at this time	false	string
			registeredAt__lt	Agents registered before this time	false	string
			registeredAt__lte	Agents registered before or at this time	false	string
			remoteOpsForensicsSupported	Include only agents that has Remote Ops Forensicsfeature supported	false	boolean
			remoteProfili	Agent remote	false	string []

			ngStates	profiling state		
			remoteProfilingStatesNin	Do not include these Agent remote profiling states	false	string []
			rsoLevel	Supported Remote Script Orchestration level	false	enum
			scanStatus	Scan status	false	enum
			scanStatuses	Included scan statuses	false	string []
			scanStatuses Nin	Not included scan statuses	false	string []
			serialNumber__contains	Free-text filter by Serial Number (supports multiple values)	false	string []
			siteIds	List of Site IDs to filter by	false	string []
			tagsData	Filter agents by their assigned tags. Given in form of a JSON where each key represents a tag key, and each value represents a list of string values to filter by. To filter by unassigned tag values,	false	string

				use __nin suffix in the tag key.		
			threatContentHash	Include only Agents that have at least one threat with this content hash	false	string
			threatCreatedAt__between	Agents with threats reported in a date range (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			threatCreatedAt__gt	Agents with threats reported after this time	false	string
			threatCreatedAt__gte	Agents with threats reported after or at this time	false	string
			threatCreatedAt__lt	Agents with threats reported before this time	false	string
			threatCreatedAt__lte	Agents with threats reported before or at this time	false	string
			threatHidden	Include only Agents with at least one hidden threat	false	boolean

			threatMitigationStatus	Include only Agents that have threats with this mitigation status	false	enum
			threatRebootRequired	Has at least one threat with at least one mitigation action pending reboot to succeed	false	boolean []
			threatResolved	Include only Agents with at least one resolved threat	false	boolean
			totalMemory__between	Total memory range (GB, inclusive)	false	string
			totalMemory__gt	Memory size (MB, more than)	false	integer
			totalMemory__gte	Memory size (MB, more than or equal)	false	integer
			totalMemory__lt	Memory size (MB, less than)	false	integer
			totalMemory__lte	Memory size (MB, less than or equal)	false	integer
			updatedAt__between	Date range for update time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string

			updatedAt__gt	Agents updated after this timestamp	false	string
			updatedAt__gte	Agents updated after or at this timestamp	false	string
			updatedAt__lt	Agents updated before this timestamp	false	string
			updatedAt__lte	Agents updated before or at this timestamp	false	string
			userActionsNeeded	Included pending user actions	false	string []
			userActionsNeededNin	Excluded pending user actions	false	string []
			uuid	Agent's universally unique identifier	false	string
			uuid__contains	Free-text filter by Agent UUID (supports multiple values)	false	string []
			uuids	A list of included UUIDs	false	string []

Randomize UUID

POST /web/api/v2.1/agents/actions/randomize-uuid

IMPORTANT: This action will assign a new UUID to Agents that match the filter.
Run it only when instructed to do so by SentinelOne Support.
If you clone the Agent on a VM or VDI without the /VDI switch, you might need to run this command. It is best to ask for Support assistance. Historical threat and Deep Visibility data will be kept in the Management, but that data will be disassociated from the Agent.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - User has insufficient permissions to perform the requested action

Response Schema

Name	Description	Required	Value
data	Response data	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>affected</td><td>Number of entities affected by the requested operation</td><td>false</td><td>integer</td></tr></table>
errors	Errors	false	array

Body Schema

Name	Description	Required	Value
filter	Applied filter - only matched Agents will be affected by the requested action. Note: One of these filter arguments must be supplied: ids, groupIds, filterId.	true	

Name	Description	Required	Value
accountIds	List of Account IDs to filter by	false	string []
activeThreats	Include Agents with this amount of active threats	false	integer
activeThreats__gt	Include Agents with at least this amount of active threats	false	integer
adComputerMember__contains	Free-text filter by Active Directory computer groups string (supports multiple values)	false	string []
adComputerName__contains	Free-text filter by Active Directory computer name string (supports multiple values)	false	string []
adComputerQuery__contains	Free-text filter by Active Directory computer name or its groups	false	string []

				(supports multiple values)		
			adQuery	An Active Directory query string	false	string
			adQuery__contains	Free-text filter by Active Directory string (supports multiple values)	false	string []
			adUserMember__contains	Free-text filter by Active Directory user groups string (supports multiple values)	false	string []
			adUserName__contains	Free-text filter by Active Directory username string (supports multiple values)	false	string []
			adUserQuery__contains	Free-text filter by Active Directory computer name or its groups (supports multiple values)	false	string []
			agentNamespa	Free-text	false	string []

			ce__contains	filter by agent namespace (supports multiple values)		
			agentPodName__contains	Free-text filter by agent pod name (supports multiple values)	false	string []
			agentVersion__between	Version range for agent version (format: <from_version>-<to_version>, inclusive)	false	string
			agentVersion__gt	Agents versions greater than given version	false	string
			agentVersion__gte	Agents versions greater than or equal to given version	false	string
			agentVersion__lt	Agents versions less than given version	false	string
			agentVersion__lte	Agents versions less than or equal to given version	false	string
			agentVersions	Agent versions to include	false	string []
			agentVersionsNin	Agent versions not	false	string []

				to include		
			appsVulnerabilityStatuses	Apps vulnerability status in	false	string []
			appsVulnerabilityStatusesNin	Apps vulnerability status nin	false	string []
			awsRole__contains	Free-text filter by aws role(supports multiple values)	false	string []
			awsSecurityGroups__contains	Free-text filter by aws securityGroups(supports multiple values)	false	string []
			awsSubnetIds__contains	Free-text filter by aws subnet ids (supports multiple values)	false	string []
			azureResourceGroup__contains	Free-text filter by azure resource group(supports multiple values)	false	string []
			cloudAccount__contains	Free-text filter by cloud account (supports multiple values)	false	string []
			cloudImage__contains	Free-text filter by cloud image (supports multiple values)	false	string []

			cloudInstanceId__contains	Free-text filter by cloud instance id(supports multiple values)	false	string []
			cloudInstanceSize__contains	Free-text filter by cloud instance size(supports multiple values)	false	string []
			cloudLocation__contains	Free-text filter by cloud location (supports multiple values)	false	string []
			cloudNetwork__contains	Free-text filter by cloud network (supports multiple values)	false	string []
			cloudProvider	Agents from which cloud provider	false	string []
			cloudProviderNin	Exclude Agents from these cloud provider	false	string []
			cloudTags__contains	Free-text filter by cloud tags (supports multiple values)	false	string []
			clusterName__contains	Free-text filter by cluster name (supports multiple values)	false	string []

			computerName	Computer name	false	string
			computerName__contains	Free-text filter by computer name (supports multiple values)	false	string []
			computerName__like	Match computer name partially (substring)	false	string
			consoleMigrationStatuses	Migration status in	false	string []
			consoleMigrationStatusesNin	Migration status nin	false	string []
			coreCount__between	Possible number of CPU cores (inclusive)	false	string
			coreCount__gt	CPU cores (more than)	false	integer
			coreCount__gte	CPU cores (more than or equal)	false	integer
			coreCount__lt	CPU cores (less than)	false	integer
			coreCount__lte	CPU cores (less than or equal)	false	integer
			cpuCount__between	Possible number of CPU cores (inclusive)	false	string
			cpuCount__gt	Number of CPUs (more than)	false	integer

			cpuCount__gte	Number of CPUs (more than or equal)	false	integer
			cpuCount__lt	Number of CPUs (less than)	false	integer
			cpuCount__lte	Number of CPUs (less than or equal)	false	integer
			cpuId__contains	Free-text filter by CPU name (supports multiple values)	false	string []
			createdAt__between	Date range for creation time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			createdAt__gt	Agents created after this timestamp	false	string
			createdAt__gte	Agents created after or at this timestamp	false	string
			createdAt__lt	Agents created before this timestamp	false	string
			createdAt__lte	Agents created before or at this timestamp	false	string
			csvFilterId	The ID of the CSV file to filter by	false	string

			decommissionedAt__between	Date range for decommission time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			decommissionedAt__gt	Agents decommissioned after this timestamp	false	string
			decommissionedAt__gte	Agents decommissioned after or at this timestamp	false	string
			decommissionedAt__lt	Agents decommissioned before this timestamp	false	string
			decommissionedAt__lte	Agents decommissioned before this timestamp	false	string
			domains	Included network domains	false	string []
			domainsNin	Not included network domains	false	string []
			encryptedApplications	Disk encryption status	false	boolean
			externalId__contains	Free-text filter by external ID (Customer ID)	false	string []
			externalIp__contains	Free-text filter by visible IP (supports	false	string []

				multiple values)		
			filteredGroupIds	List of Group IDs to filter by	false	string []
			filteredSiteIds	List of Site IDs to filter by	false	string []
			filterId	Include all Agents matching this saved filter	false	string
			firewallEnabled	The agents supports Firewall Control and it is enabled for the agent's group	false	boolean []
			gatewayIp	Gateway ip	false	string
			gcpServiceAccount__contains	Free-text filter by gcp service account (supports multiple values)	false	string []
			groupIds	List of network groups	false	string []
			hasContainerizedWorkload	Include only Agents protecting containerized workloads	false	boolean
			hasLocalConfiguration	Agent has a local configuration set	false	boolean
			hasTags	Include only Agents that	false	boolean

				have any tags assigned if True, or none if False		
			ids	A list of Agent IDs	false	string []
			infected	Include only Agents with at least one active threat	false	boolean
			installerTypes	Include only Agents installed with these package types	false	string []
			installerTypesNin	Exclude Agents installed with these package types	false	string []
			isActive	Include only active Agents	false	boolean
			isDecommissioned	Include active, decommissioned or both	false	boolean []
			isPendingUninstall	Include only Agents with pending uninstall requests	false	boolean
			isUninstalled	Include installed, uninstalled or both	false	boolean []
			isUpToDate	Include only Agents with updated software	false	boolean

			k8sNodeLabels__contains	Free-text filter by K8s node labels (supports multiple values)	false	string []
			k8sNodeName__contains	Free-text filter by K8s node name (supports multiple values)	false	string []
			k8sType__contains	Free-text filter by K8s type(supports multiple values)	false	string []
			k8sVersion__contains	Free-text filter by K8s version (supports multiple values)	false	string []
			lastActiveDate__between	Date range for last active date(format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			lastActiveDate__gt	Agents last active after this time	false	string
			lastActiveDate__gte	Agents last active after or at this time	false	string
			lastActiveDate__lt	Agents last active before this time	false	string
			lastActiveDate__lte	Agents last active before or at this time	false	string

			lastLoggedInUserName__contains	Free-text filter by username (supports multiple values)	false	string []
			lastSuccessfulScanDate__between	Date range for last successful full disk scan(format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			lastSuccessfulScanDate__gt	Agents last successful full disk scan after this time	false	string
			lastSuccessfulScanDate__gte	Agents last successful full disk scan after or at this time	false	string
			lastSuccessfulScanDate__lt	Agents last successful full disk scan before this time	false	string
			lastSuccessfulScanDate__lte	Agents last successful full disk scan before or at this time	false	string
			liveUpdateId__contains	Free-text filter by live update ID (supports multiple values)	false	string []
			locationEnabled	The agents supports	false	boolean []

				Location Awareness and it is enabled for the agent's group		
			locationIds	Include only Agents reporting these locations	false	string []
			locationIdsNin	Do not include only Agents reporting these locations	false	string []
			machineTypes	Included machine types	false	string []
			machineTypesNin	Not included machine types	false	string []
			migrationStatus	Migration status	false	enum
			missingPermissions	Included missing permissions	false	string []
			missingPermissionsNin	Excluded missing permissions	false	string []
			mitigationMode	Agent mitigation mode policy	false	enum
			mitigationModeSuspicious	Mitigation mode policy for suspicious activity	false	enum
			networkInterfaceGatewayMacAddress__c	Free-text filter by Gateway	false	string []

			ontains	MAC address (supports multiple values)		
			networkInterfaceInet__contains	Free-text filter by local IP (supports multiple values)	false	string []
			networkInterfacePhysical__contains	Free-text filter by MAC address (supports multiple values)	false	string []
			networkQuarantineEnabled	The agents supports Network Quarantine Control and its enabled for the agent's group	false	boolean []
			networkStatuses	Included network statuses	false	string []
			networkStatusesNin	Included network statuses	false	string []
			operationalStates	Agent operational state	false	string []
			operationalStatesNin	Do not include these Agent operational states	false	string []
			osArch	OS architecture	false	enum
			osTypes	Included OS types	false	string []

			osTypesNin	Not included OS types	false	string []
			osVersion__contains	Free-text filter by OS full name and version (supports multiple values)	false	string []
			query	A free-text search term, will match applicable attributes (sub-string match). Note: Device's physical addresses will be matched if they start with the search term only (no match if they contain the term).	false	string
			rangerStatus	[DEPRECATED] Use rangerStatuses.	false	enum
			rangerStatuses	Status of Ranger	false	string []
			rangerStatusesNin	Do not include these Ranger Statuses	false	string []
			rangerVersions	Ranger versions to include	false	string []
			rangerVersionsNin	Ranger versions not to include	false	string []

			registeredAt__between	Date range for first registration time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			registeredAt__gt	Agents registered after this time	false	string
			registeredAt__gte	Agents registered after or at this time	false	string
			registeredAt__lt	Agents registered before this time	false	string
			registeredAt__lte	Agents registered before or at this time	false	string
			remoteOpsForensicsSupported	Include only agents that has Remote Ops Forensicsfeature supported	false	boolean
			remoteProfilingStates	Agent remote profiling state	false	string []
			remoteProfilingStatesNin	Do not include these Agent remote profiling states	false	string []
			rsoLevel	Supported Remote Script Orchestration	false	enum

				level		
			scanStatus	Scan status	false	enum
			scanStatuses	Included scan statuses	false	string []
			scanStatuses Nin	Not included scan statuses	false	string []
			serialNumber __contains	Free-text filter by Serial Number (supports multiple values)	false	string []
			siteIds	List of Site IDs to filter by	false	string []
			tagsData	Filter agents by their assigned tags. Given in form of a JSON where each key represents a tag key, and each value represents a list of string values to filter by. To filter by unassigned tag values, use __nin suffix in the tag key.	false	string
			threatConten tHash	Include only Agents that have at least one threat with this content hash	false	string
			threatCreate	Agents with	false	string

			dAt__between	threats reported in a date range (format: <from_timestamp>-<to_timestamp>, inclusive)		
			threatCreatedAt__gt	Agents with threats reported after this time	false	string
			threatCreatedAt__gte	Agents with threats reported after or at this time	false	string
			threatCreatedAt__lt	Agents with threats reported before this time	false	string
			threatCreatedAt__lte	Agents with threats reported before or at this time	false	string
			threatHidden	Include only Agents with at least one hidden threat	false	boolean
			threatMitigationStatus	Include only Agents that have threats with this mitigation status	false	enum
			threatRebootRequired	Has at least one threat with at least one mitigation	false	boolean []

				action pending reboot to succeed		
			threatResolved	Include only Agents with at least one resolved threat	false	boolean
			totalMemory__between	Total memory range (GB, inclusive)	false	string
			totalMemory__gt	Memory size (MB, more than)	false	integer
			totalMemory__gte	Memory size (MB, more than or equal)	false	integer
			totalMemory__lt	Memory size (MB, less than)	false	integer
			totalMemory__lte	Memory size (MB, less than or equal)	false	integer
			updatedAt__between	Date range for update time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			updatedAt__gt	Agents updated after this timestamp	false	string
			updatedAt__gte	Agents updated after or at this timestamp	false	string
			updatedAt__lt	Agents updated	false	string

<table>
<tr><td></td><td></td><td></td><td><table>
<tr><td></td><td>before this timestamp</td><td></td><td></td></tr>
<tr><td>updatedAt__lte</td><td>Agents updated before or at this timestamp</td><td>false</td><td>string</td></tr>
<tr><td>userActionsNeeded</td><td>Included pending user actions</td><td>false</td><td>string []</td></tr>
<tr><td>userActionsNeededNin</td><td>Excluded pending user actions</td><td>false</td><td>string []</td></tr>
<tr><td>uuid</td><td>Agent's universally unique identifier</td><td>false</td><td>string</td></tr>
<tr><td>uuid__contains</td><td>Free-text filter by Agent UUID (supports multiple values)</td><td>false</td><td>string []</td></tr>
<tr><td>uuids</td><td>A list of included UUIDs</td><td>false</td><td>string []</td></tr>
</table></td></tr>
<tr><td>data</td><td>Data</td><td>false</td><td></td></tr>
</table>

Mark as up-to-date

POST /web/api/v2.1/agents/actions/mark-up-to-date

The value of the Agent version as "up-to-date" is a useful filter for many actions. There are scenarios where the Management does not recognize a version as latest.
For example, if Agents that were sent a new version with the update-software command did not yet report to their Management.
You can manually mark these Agents as up-to-date.
This command is not available to users with the SOC role.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - User has insufficient permissions to perform the requested action

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>affected</td><td>Number of entities affected by the requested operation</td><td>false</td><td>integer</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>filter</td><td>Applied filter - only matched Agents will be affected by the requested action. Leave empty to apply the action on all applicable Agents.</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>activeThreats</td><td>Include Agents with this amount of active threats</td><td>false</td><td>integer</td></tr>
<tr><td>activeThreats__gt</td><td>Include Agents with at least this amount of active threats</td><td>false</td><td>integer</td></tr>
<tr><td>adComputerMember__contains</td><td>Free-text filter by Active Directory computer groups string (supports multiple values)</td><td>false</td><td>string []</td></tr>
<tr><td>adComputerName__contains</td><td>Free-text filter by Active Directory computer name string (supports multiple values)</td><td>false</td><td>string []</td></tr>
<tr><td>adComputerQuery__contains</td><td>Free-text filter by Active Directory computer name or its groups</td><td>false</td><td>string []</td></tr>
</table>
</td></tr>
</table>

				(supports multiple values)		
			adQuery	An Active Directory query string	false	string
			adQuery__contains	Free-text filter by Active Directory string (supports multiple values)	false	string []
			adUserMember__contains	Free-text filter by Active Directory user groups string (supports multiple values)	false	string []
			adUserName__contains	Free-text filter by Active Directory username string (supports multiple values)	false	string []
			adUserQuery__contains	Free-text filter by Active Directory computer name or its groups (supports multiple values)	false	string []
			agentNamespa	Free-text	false	string []

			ce__contains	filter by agent namespace (supports multiple values)		
			agentPodName__contains	Free-text filter by agent pod name (supports multiple values)	false	string []
			agentVersion__between	Version range for agent version (format: <from_version>-<to_version>, inclusive)	false	string
			agentVersion__gt	Agents versions greater than given version	false	string
			agentVersion__gte	Agents versions greater than or equal to given version	false	string
			agentVersion__lt	Agents versions less than given version	false	string
			agentVersion__lte	Agents versions less than or equal to given version	false	string
			agentVersions	Agent versions to include	false	string []
			agentVersionsNin	Agent versions not	false	string []

				to include		
			appsVulnerabilityStatuses	Apps vulnerability status in	false	string []
			appsVulnerabilityStatusesNin	Apps vulnerability status nin	false	string []
			awsRole__contains	Free-text filter by aws role(supports multiple values)	false	string []
			awsSecurityGroups__contains	Free-text filter by aws securityGroups(supports multiple values)	false	string []
			awsSubnetIds__contains	Free-text filter by aws subnet ids (supports multiple values)	false	string []
			azureResourceGroup__contains	Free-text filter by azure resource group(supports multiple values)	false	string []
			cloudAccount__contains	Free-text filter by cloud account (supports multiple values)	false	string []
			cloudImage__contains	Free-text filter by cloud image (supports multiple values)	false	string []

			cloudInstanceId__contains	Free-text filter by cloud instance id(supports multiple values)	false	string []
			cloudInstanceSize__contains	Free-text filter by cloud instance size(supports multiple values)	false	string []
			cloudLocation__contains	Free-text filter by cloud location (supports multiple values)	false	string []
			cloudNetwork__contains	Free-text filter by cloud network (supports multiple values)	false	string []
			cloudProvider	Agents from which cloud provider	false	string []
			cloudProviderNin	Exclude Agents from these cloud provider	false	string []
			cloudTags__contains	Free-text filter by cloud tags (supports multiple values)	false	string []
			clusterName__contains	Free-text filter by cluster name (supports multiple values)	false	string []

			computerName	Computer name	false	string
			computerName__contains	Free-text filter by computer name (supports multiple values)	false	string []
			computerName__like	Match computer name partially (substring)	false	string
			consoleMigrationStatuses	Migration status in	false	string []
			consoleMigrationStatusesNin	Migration status nin	false	string []
			coreCount__between	Possible number of CPU cores (inclusive)	false	string
			coreCount__gt	CPU cores (more than)	false	integer
			coreCount__gte	CPU cores (more than or equal)	false	integer
			coreCount__lt	CPU cores (less than)	false	integer
			coreCount__lte	CPU cores (less than or equal)	false	integer
			cpuCount__between	Possible number of CPU cores (inclusive)	false	string
			cpuCount__gt	Number of CPUs (more than)	false	integer

			cpuCount__gte	Number of CPUs (more than or equal)	false	integer
			cpuCount__lt	Number of CPUs (less than)	false	integer
			cpuCount__lte	Number of CPUs (less than or equal)	false	integer
			cpuId__contains	Free-text filter by CPU name (supports multiple values)	false	string []
			createdAt__between	Date range for creation time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			createdAt__gt	Agents created after this timestamp	false	string
			createdAt__gte	Agents created after or at this timestamp	false	string
			createdAt__lt	Agents created before this timestamp	false	string
			createdAt__lte	Agents created before or at this timestamp	false	string
			csvFilterId	The ID of the CSV file to filter by	false	string

			decommissionedAt__between	Date range for decommission time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			decommissionedAt__gt	Agents decommissioned after this timestamp	false	string
			decommissionedAt__gte	Agents decommissioned after or at this timestamp	false	string
			decommissionedAt__lt	Agents decommissioned before this timestamp	false	string
			decommissionedAt__lte	Agents decommissioned before this timestamp	false	string
			domains	Included network domains	false	string []
			domainsNin	Not included network domains	false	string []
			encryptedApplications	Disk encryption status	false	boolean
			externalId__contains	Free-text filter by external ID (Customer ID)	false	string []
			externalIp__contains	Free-text filter by visible IP (supports	false	string []

				multiple values)		
			filteredGroupIds	List of Group IDs to filter by	false	string []
			filteredSiteIds	List of Site IDs to filter by	false	string []
			filterId	Include all Agents matching this saved filter	false	string
			firewallEnabled	The agents supports Firewall Control and it is enabled for the agent's group	false	boolean []
			gatewayIp	Gateway ip	false	string
			gcpServiceAccount__contains	Free-text filter by gcp service account (supports multiple values)	false	string []
			groupIds	List of Group IDs to filter by	false	string []
			hasContainerizedWorkload	Include only Agents protecting containerized workloads	false	boolean
			hasLocalConfiguration	Agent has a local configuration set	false	boolean
			hasTags	Include only Agents that	false	boolean

				have any tags assigned if True, or none if False		
			ids	A list of Agent IDs	false	string []
			infected	Include only Agents with at least one active threat	false	boolean
			installerTypes	Include only Agents installed with these package types	false	string []
			installerTypesNin	Exclude Agents installed with these package types	false	string []
			isActive	Include only active Agents	false	boolean
			isDecommissioned	Include active, decommissioned or both	false	boolean []
			isPendingUninstall	Include only Agents with pending uninstall requests	false	boolean
			isUninstalled	Include installed, uninstalled or both	false	boolean []
			isUpToDate	Include only Agents with updated software	false	boolean

			k8sNodeLabels__contains	Free-text filter by K8s node labels (supports multiple values)	false	string []
			k8sNodeName__contains	Free-text filter by K8s node name (supports multiple values)	false	string []
			k8sType__contains	Free-text filter by K8s type(supports multiple values)	false	string []
			k8sVersion__contains	Free-text filter by K8s version (supports multiple values)	false	string []
			lastActiveDate__between	Date range for last active date(format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			lastActiveDate__gt	Agents last active after this time	false	string
			lastActiveDate__gte	Agents last active after or at this time	false	string
			lastActiveDate__lt	Agents last active before this time	false	string
			lastActiveDate__lte	Agents last active before or at this time	false	string

			lastLoggedInUserName__contains	Free-text filter by username (supports multiple values)	false	string []
			lastSuccessfulScanDate__between	Date range for last successful full disk scan(format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			lastSuccessfulScanDate__gt	Agents last successful full disk scan after this time	false	string
			lastSuccessfulScanDate__gte	Agents last successful full disk scan after or at this time	false	string
			lastSuccessfulScanDate__lt	Agents last successful full disk scan before this time	false	string
			lastSuccessfulScanDate__lte	Agents last successful full disk scan before or at this time	false	string
			liveUpdateId__contains	Free-text filter by live update ID (supports multiple values)	false	string []
			locationEnabled	The agents supports	false	boolean []

				Location Awareness and it is enabled for the agent's group		
			locationIds	Include only Agents reporting these locations	false	string []
			locationIdsNin	Do not include only Agents reporting these locations	false	string []
			machineTypes	Included machine types	false	string []
			machineTypesNin	Not included machine types	false	string []
			migrationStatus	Migration status	false	enum
			missingPermissions	Included missing permissions	false	string []
			missingPermissionsNin	Excluded missing permissions	false	string []
			mitigationMode	Agent mitigation mode policy	false	enum
			mitigationModeSuspicious	Mitigation mode policy for suspicious activity	false	enum
			networkInterfaceGatewayMacAddress__c	Free-text filter by Gateway	false	string []

			ontains	MAC address (supports multiple values)		
			networkInterfaceInet__contains	Free-text filter by local IP (supports multiple values)	false	string []
			networkInterfacePhysical__contains	Free-text filter by MAC address (supports multiple values)	false	string []
			networkQuarantineEnabled	The agents supports Network Quarantine Control and its enabled for the agent's group	false	boolean []
			networkStatuses	Included network statuses	false	string []
			networkStatusesNin	Included network statuses	false	string []
			operationalStates	Agent operational state	false	string []
			operationalStatesNin	Do not include these Agent operational states	false	string []
			osArch	OS architecture	false	enum
			osTypes	Included OS types	false	string []

			osTypesNin	Not included OS types	false	string []
			osVersion__contains	Free-text filter by OS full name and version (supports multiple values)	false	string []
			query	A free-text search term, will match applicable attributes (sub-string match). Note: Device's physical addresses will be matched if they start with the search term only (no match if they contain the term).	false	string
			rangerStatus	[DEPRECATED] Use rangerStatuses.	false	enum
			rangerStatuses	Status of Ranger	false	string []
			rangerStatusesNin	Do not include these Ranger Statuses	false	string []
			rangerVersions	Ranger versions to include	false	string []
			rangerVersionsNin	Ranger versions not to include	false	string []

			registeredAt__between	Date range for first registration time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			registeredAt__gt	Agents registered after this time	false	string
			registeredAt__gte	Agents registered after or at this time	false	string
			registeredAt__lt	Agents registered before this time	false	string
			registeredAt__lte	Agents registered before or at this time	false	string
			remoteOpsForensicsSupported	Include only agents that has Remote Ops Forensicsfeature supported	false	boolean
			remoteProfilingStates	Agent remote profiling state	false	string []
			remoteProfilingStatesNin	Do not include these Agent remote profiling states	false	string []
			rsoLevel	Supported Remote Script Orchestration	false	enum

				level		
			scanStatus	Scan status	false	enum
			scanStatuses	Included scan statuses	false	string []
			scanStatuses Nin	Not included scan statuses	false	string []
			serialNumber __contains	Free-text filter by Serial Number (supports multiple values)	false	string []
			siteIds	List of Site IDs to filter by	false	string []
			tagsData	Filter agents by their assigned tags. Given in form of a JSON where each key represents a tag key, and each value represents a list of string values to filter by. To filter by unassigned tag values, use __nin suffix in the tag key.	false	string
			threatConten tHash	Include only Agents that have at least one threat with this content hash	false	string
			threatCreate	Agents with	false	string

			dAt__between	threats reported in a date range (format: <from_timestamp>-<to_timestamp>, inclusive)		
			threatCreatedAt__gt	Agents with threats reported after this time	false	string
			threatCreatedAt__gte	Agents with threats reported after or at this time	false	string
			threatCreatedAt__lt	Agents with threats reported before this time	false	string
			threatCreatedAt__lte	Agents with threats reported before or at this time	false	string
			threatHidden	Include only Agents with at least one hidden threat	false	boolean
			threatMitigationStatus	Include only Agents that have threats with this mitigation status	false	enum
			threatRebootRequired	Has at least one threat with at least one mitigation	false	boolean []

				action pending reboot to succeed		
			threatResolved	Include only Agents with at least one resolved threat	false	boolean
			totalMemory__between	Total memory range (GB, inclusive)	false	string
			totalMemory__gt	Memory size (MB, more than)	false	integer
			totalMemory__gte	Memory size (MB, more than or equal)	false	integer
			totalMemory__lt	Memory size (MB, less than)	false	integer
			totalMemory__lte	Memory size (MB, less than or equal)	false	integer
			updatedAt__between	Date range for update time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			updatedAt__gt	Agents updated after this timestamp	false	string
			updatedAt__gte	Agents updated after or at this timestamp	false	string
			updatedAt__lt	Agents updated	false	string

			before this timestamp		
	updatedAt__lte	Agents updated before or at this timestamp	false	string
	userActionsNeeded	Included pending user actions	false	string []
	userActionsNeededNin	Excluded pending user actions	false	string []
	uuid	Agent's universally unique identifier	false	string
	uuid__contains	Free-text filter by Agent UUID (supports multiple values)	false	string []
	uuids	A list of included UUIDs	false	string []
data	Data	false	

Enable Ranger

POST /web/api/v2.1/agents/actions/ranger-enable

SentinelOne Ranger gives full visibility of all devices connected to your network. Ranger scans your corporate environment to identify and manage connected devices, even those not protected by or supported by SentinelOne. Use this command to enable Ranger on Agents that match the filter. The Agent adds "Scanner" to its functionality.
If the given Agent cannot support Ranger, or if Ranger is already enabled, this command does nothing.
Ranger requires a special license. Consult with your SentinelOne SE.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - Insufficient permissions

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>affected</td><td>Number of entities affected by the requested operation</td><td>false</td><td>integer</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>filter</td><td>Applied filter - only matched Agents will be affected by the requested action. Leave empty to apply the action on all applicable Agents.</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>activeThreats</td><td>Include Agents with this amount of active threats</td><td>false</td><td>integer</td></tr>
<tr><td>activeThreats__gt</td><td>Include Agents with at least this amount of active threats</td><td>false</td><td>integer</td></tr>
<tr><td>adComputerMember__contains</td><td>Free-text filter by Active Directory computer groups string (supports multiple values)</td><td>false</td><td>string []</td></tr>
<tr><td>adComputerName__contains</td><td>Free-text filter by Active Directory computer name string (supports multiple values)</td><td>false</td><td>string []</td></tr>
<tr><td>adComputerQuery__contains</td><td>Free-text filter by Active Directory computer name or its groups</td><td>false</td><td>string []</td></tr>
</table>
</td></tr>
</table>

				(supports multiple values)		
			adQuery	An Active Directory query string	false	string
			adQuery__contains	Free-text filter by Active Directory string (supports multiple values)	false	string []
			adUserMember__contains	Free-text filter by Active Directory user groups string (supports multiple values)	false	string []
			adUserName__contains	Free-text filter by Active Directory username string (supports multiple values)	false	string []
			adUserQuery__contains	Free-text filter by Active Directory computer name or its groups (supports multiple values)	false	string []
			agentNamespa	Free-text	false	string []

			ce__contains	filter by agent namespace (supports multiple values)		
			agentPodName__contains	Free-text filter by agent pod name (supports multiple values)	false	string []
			agentVersion__between	Version range for agent version (format: <from_version>-<to_version>, inclusive)	false	string
			agentVersion__gt	Agents versions greater than given version	false	string
			agentVersion__gte	Agents versions greater than or equal to given version	false	string
			agentVersion__lt	Agents versions less than given version	false	string
			agentVersion__lte	Agents versions less than or equal to given version	false	string
			agentVersions	Agent versions to include	false	string []
			agentVersionsNin	Agent versions not	false	string []

				to include		
			appsVulnerabilityStatuses	Apps vulnerability status in	false	string []
			appsVulnerabilityStatusesNin	Apps vulnerability status nin	false	string []
			awsRole__contains	Free-text filter by aws role(supports multiple values)	false	string []
			awsSecurityGroups__contains	Free-text filter by aws securityGroups(supports multiple values)	false	string []
			awsSubnetIds__contains	Free-text filter by aws subnet ids (supports multiple values)	false	string []
			azureResourceGroup__contains	Free-text filter by azure resource group(supports multiple values)	false	string []
			cloudAccount__contains	Free-text filter by cloud account (supports multiple values)	false	string []
			cloudImage__contains	Free-text filter by cloud image (supports multiple values)	false	string []

			cloudInstanceId__contains	Free-text filter by cloud instance id(supports multiple values)	false	string []
			cloudInstanceSize__contains	Free-text filter by cloud instance size(supports multiple values)	false	string []
			cloudLocation__contains	Free-text filter by cloud location (supports multiple values)	false	string []
			cloudNetwork__contains	Free-text filter by cloud network (supports multiple values)	false	string []
			cloudProvider	Agents from which cloud provider	false	string []
			cloudProviderNin	Exclude Agents from these cloud provider	false	string []
			cloudTags__contains	Free-text filter by cloud tags (supports multiple values)	false	string []
			clusterName__contains	Free-text filter by cluster name (supports multiple values)	false	string []

			computerName	Computer name	false	string
			computerName__contains	Free-text filter by computer name (supports multiple values)	false	string []
			computerName__like	Match computer name partially (substring)	false	string
			consoleMigrationStatuses	Migration status in	false	string []
			consoleMigrationStatusesNin	Migration status nin	false	string []
			coreCount__between	Possible number of CPU cores (inclusive)	false	string
			coreCount__gt	CPU cores (more than)	false	integer
			coreCount__gte	CPU cores (more than or equal)	false	integer
			coreCount__lt	CPU cores (less than)	false	integer
			coreCount__lte	CPU cores (less than or equal)	false	integer
			cpuCount__between	Possible number of CPU cores (inclusive)	false	string
			cpuCount__gt	Number of CPUs (more than)	false	integer

			cpuCount__gte	Number of CPUs (more than or equal)	false	integer
			cpuCount__lt	Number of CPUs (less than)	false	integer
			cpuCount__lte	Number of CPUs (less than or equal)	false	integer
			cpuId__contains	Free-text filter by CPU name (supports multiple values)	false	string []
			createdAt__between	Date range for creation time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			createdAt__gt	Agents created after this timestamp	false	string
			createdAt__gte	Agents created after or at this timestamp	false	string
			createdAt__lt	Agents created before this timestamp	false	string
			createdAt__lte	Agents created before or at this timestamp	false	string
			csvFilterId	The ID of the CSV file to filter by	false	string

			decommissionedAt__between	Date range for decommission time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			decommissionedAt__gt	Agents decommissioned after this timestamp	false	string
			decommissionedAt__gte	Agents decommissioned after or at this timestamp	false	string
			decommissionedAt__lt	Agents decommissioned before this timestamp	false	string
			decommissionedAt__lte	Agents decommissioned before this timestamp	false	string
			domains	Included network domains	false	string []
			domainsNin	Not included network domains	false	string []
			encryptedApplications	Disk encryption status	false	boolean
			externalId__contains	Free-text filter by external ID (Customer ID)	false	string []
			externalIp__contains	Free-text filter by visible IP (supports	false	string []

				multiple values)		
			filteredGroupIds	List of Group IDs to filter by	false	string []
			filteredSiteIds	List of Site IDs to filter by	false	string []
			filterId	Include all Agents matching this saved filter	false	string
			firewallEnabled	The agents supports Firewall Control and it is enabled for the agent's group	false	boolean []
			gatewayIp	Gateway ip	false	string
			gcpServiceAccount__contains	Free-text filter by gcp service account (supports multiple values)	false	string []
			groupIds	List of Group IDs to filter by	false	string []
			hasContainerizedWorkload	Include only Agents protecting containerized workloads	false	boolean
			hasLocalConfiguration	Agent has a local configuration set	false	boolean
			hasTags	Include only Agents that	false	boolean

				have any tags assigned if True, or none if False		
			ids	A list of Agent IDs	false	string []
			infected	Include only Agents with at least one active threat	false	boolean
			installerTypes	Include only Agents installed with these package types	false	string []
			installerTypesNin	Exclude Agents installed with these package types	false	string []
			isActive	Include only active Agents	false	boolean
			isDecommissioned	Include active, decommissioned or both	false	boolean []
			isPendingUninstall	Include only Agents with pending uninstall requests	false	boolean
			isUninstalled	Include installed, uninstalled or both	false	boolean []
			isUpToDate	Include only Agents with updated software	false	boolean

			k8sNodeLabels__contains	Free-text filter by K8s node labels (supports multiple values)	false	string []
			k8sNodeName__contains	Free-text filter by K8s node name (supports multiple values)	false	string []
			k8sType__contains	Free-text filter by K8s type(supports multiple values)	false	string []
			k8sVersion__contains	Free-text filter by K8s version (supports multiple values)	false	string []
			lastActiveDate__between	Date range for last active date(format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			lastActiveDate__gt	Agents last active after this time	false	string
			lastActiveDate__gte	Agents last active after or at this time	false	string
			lastActiveDate__lt	Agents last active before this time	false	string
			lastActiveDate__lte	Agents last active before or at this time	false	string

			lastLoggedInUserName__contains	Free-text filter by username (supports multiple values)	false	string []
			lastSuccessfulScanDate__between	Date range for last successful full disk scan(format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			lastSuccessfulScanDate__gt	Agents last successful full disk scan after this time	false	string
			lastSuccessfulScanDate__gte	Agents last successful full disk scan after or at this time	false	string
			lastSuccessfulScanDate__lt	Agents last successful full disk scan before this time	false	string
			lastSuccessfulScanDate__lte	Agents last successful full disk scan before or at this time	false	string
			liveUpdateId__contains	Free-text filter by live update ID (supports multiple values)	false	string []
			locationEnabled	The agents supports	false	boolean []

				Location Awareness and it is enabled for the agent's group		
			locationIds	Include only Agents reporting these locations	false	string []
			locationIdsNin	Do not include only Agents reporting these locations	false	string []
			machineTypes	Included machine types	false	string []
			machineTypesNin	Not included machine types	false	string []
			migrationStatus	Migration status	false	enum
			missingPermissions	Included missing permissions	false	string []
			missingPermissionsNin	Excluded missing permissions	false	string []
			mitigationMode	Agent mitigation mode policy	false	enum
			mitigationModeSuspicious	Mitigation mode policy for suspicious activity	false	enum
			networkInterfaceGatewayMacAddress__c	Free-text filter by Gateway	false	string []

			ontains	MAC address (supports multiple values)		
			networkInterfaceInet__contains	Free-text filter by local IP (supports multiple values)	false	string []
			networkInterfacePhysical__contains	Free-text filter by MAC address (supports multiple values)	false	string []
			networkQuarantineEnabled	The agents supports Network Quarantine Control and its enabled for the agent's group	false	boolean []
			networkStatuses	Included network statuses	false	string []
			networkStatusesNin	Included network statuses	false	string []
			operationalStates	Agent operational state	false	string []
			operationalStatesNin	Do not include these Agent operational states	false	string []
			osArch	OS architecture	false	enum
			osTypes	Included OS types	false	string []

			osTypesNin	Not included OS types	false	string []
			osVersion__contains	Free-text filter by OS full name and version (supports multiple values)	false	string []
			query	A free-text search term, will match applicable attributes (sub-string match). Note: Device's physical addresses will be matched if they start with the search term only (no match if they contain the term).	false	string
			rangerStatus	[DEPRECATED] Use rangerStatuses.	false	enum
			rangerStatuses	Status of Ranger	false	string []
			rangerStatusesNin	Do not include these Ranger Statuses	false	string []
			rangerVersions	Ranger versions to include	false	string []
			rangerVersionsNin	Ranger versions not to include	false	string []

			registeredAt__between	Date range for first registration time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			registeredAt__gt	Agents registered after this time	false	string
			registeredAt__gte	Agents registered after or at this time	false	string
			registeredAt__lt	Agents registered before this time	false	string
			registeredAt__lte	Agents registered before or at this time	false	string
			remoteOpsForensicsSupported	Include only agents that has Remote Ops Forensicsfeature supported	false	boolean
			remoteProfilingStates	Agent remote profiling state	false	string []
			remoteProfilingStatesNin	Do not include these Agent remote profiling states	false	string []
			rsoLevel	Supported Remote Script Orchestration	false	enum

				level		
			scanStatus	Scan status	false	enum
			scanStatuses	Included scan statuses	false	string []
			scanStatuses Nin	Not included scan statuses	false	string []
			serialNumber __contains	Free-text filter by Serial Number (supports multiple values)	false	string []
			siteIds	List of Site IDs to filter by	false	string []
			tagsData	Filter agents by their assigned tags. Given in form of a JSON where each key represents a tag key, and each value represents a list of string values to filter by. To filter by unassigned tag values, use __nin suffix in the tag key.	false	string
			threatConten tHash	Include only Agents that have at least one threat with this content hash	false	string
			threatCreate	Agents with	false	string

			dAt__between	threats reported in a date range (format: <from_timestamp>-<to_timestamp>, inclusive)		
			threatCreatedAt__gt	Agents with threats reported after this time	false	string
			threatCreatedAt__gte	Agents with threats reported after or at this time	false	string
			threatCreatedAt__lt	Agents with threats reported before this time	false	string
			threatCreatedAt__lte	Agents with threats reported before or at this time	false	string
			threatHidden	Include only Agents with at least one hidden threat	false	boolean
			threatMitigationStatus	Include only Agents that have threats with this mitigation status	false	enum
			threatRebootRequired	Has at least one threat with at least one mitigation	false	boolean []

				action pending reboot to succeed		
			threatResolved	Include only Agents with at least one resolved threat	false	boolean
			totalMemory__between	Total memory range (GB, inclusive)	false	string
			totalMemory__gt	Memory size (MB, more than)	false	integer
			totalMemory__gte	Memory size (MB, more than or equal)	false	integer
			totalMemory__lt	Memory size (MB, less than)	false	integer
			totalMemory__lte	Memory size (MB, less than or equal)	false	integer
			updatedAt__between	Date range for update time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			updatedAt__gt	Agents updated after this timestamp	false	string
			updatedAt__gte	Agents updated after or at this timestamp	false	string
			updatedAt__lt	Agents updated	false	string

<table>
<tr><td></td><td></td><td></td><td><table>
<tr><td></td><td>before this timestamp</td><td></td><td></td></tr>
<tr><td>updatedAt__lte</td><td>Agents updated before or at this timestamp</td><td>false</td><td>string</td></tr>
<tr><td>userActionsNeeded</td><td>Included pending user actions</td><td>false</td><td>string []</td></tr>
<tr><td>userActionsNeededNin</td><td>Excluded pending user actions</td><td>false</td><td>string []</td></tr>
<tr><td>uuid</td><td>Agent's universally unique identifier</td><td>false</td><td>string</td></tr>
<tr><td>uuid__contains</td><td>Free-text filter by Agent UUID (supports multiple values)</td><td>false</td><td>string []</td></tr>
<tr><td>uuids</td><td>A list of included UUIDs</td><td>false</td><td>string []</td></tr>
</table></td></tr>
<tr><td>data</td><td>Data</td><td>false</td><td></td></tr>
</table>

Disable Ranger

POST /web/api/v2.1/agents/actions/ranger-disable

Disable Ranger from the Agents that match the filter.
SentinelOne Ranger gives full visibility of all devices connected to your network. Ranger scans your corporate environment to identify and manage connected devices, even those not protected by or supported by SentinelOne. When Ranger is enabled on an Agent, the Agent adds "Scanner" to its functionality. It is the starting point for the Ranger scans.
Best Practice: Disable Ranger on endpoints that are performance-sensitive and on endpoints that often connect to non-corporate networks.

BEST PRACTICE

Disable Ranger on endpoints that are performance-sensitive and on endpoints that often connect to non-corporate networks.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - Insufficient permissions

Response Schema

Name	Description	Required	Value
data	Response data	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>affected</td><td>Number of entities affected by the requested operation</td><td>false</td><td>integer</td></tr></table>
errors	Errors	false	array

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>filter</td><td>Applied filter - only matched Agents will be affected by the requested action. Leave empty to apply the action on all applicable Agents.</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>activeThreats</td><td>Include Agents with this amount of active threats</td><td>false</td><td>integer</td></tr>
<tr><td>activeThreats__gt</td><td>Include Agents with at least this amount of active threats</td><td>false</td><td>integer</td></tr>
<tr><td>adComputerMember__contains</td><td>Free-text filter by Active Directory computer groups string (supports multiple values)</td><td>false</td><td>string []</td></tr>
<tr><td>adComputerName__contains</td><td>Free-text filter by Active Directory computer name string (supports multiple values)</td><td>false</td><td>string []</td></tr>
<tr><td>adComputerQuery__contains</td><td>Free-text filter by Active Directory computer name or its groups</td><td>false</td><td>string []</td></tr>
</table>
</td></tr>
</table>

				(supports multiple values)		
			adQuery	An Active Directory query string	false	string
			adQuery__contains	Free-text filter by Active Directory string (supports multiple values)	false	string []
			adUserMember__contains	Free-text filter by Active Directory user groups string (supports multiple values)	false	string []
			adUserName__contains	Free-text filter by Active Directory username string (supports multiple values)	false	string []
			adUserQuery__contains	Free-text filter by Active Directory computer name or its groups (supports multiple values)	false	string []
			agentNamespa	Free-text	false	string []

			ce__contains	filter by agent namespace (supports multiple values)		
			agentPodName__contains	Free-text filter by agent pod name (supports multiple values)	false	string []
			agentVersion__between	Version range for agent version (format: <from_version>-<to_version>, inclusive)	false	string
			agentVersion__gt	Agents versions greater than given version	false	string
			agentVersion__gte	Agents versions greater than or equal to given version	false	string
			agentVersion__lt	Agents versions less than given version	false	string
			agentVersion__lte	Agents versions less than or equal to given version	false	string
			agentVersions	Agent versions to include	false	string []
			agentVersionsNin	Agent versions not	false	string []

				to include		
			appsVulnerabilityStatuses	Apps vulnerability status in	false	string []
			appsVulnerabilityStatusesNin	Apps vulnerability status nin	false	string []
			awsRole__contains	Free-text filter by aws role(supports multiple values)	false	string []
			awsSecurityGroups__contains	Free-text filter by aws securityGroups(supports multiple values)	false	string []
			awsSubnetIds__contains	Free-text filter by aws subnet ids (supports multiple values)	false	string []
			azureResourceGroup__contains	Free-text filter by azure resource group(supports multiple values)	false	string []
			cloudAccount__contains	Free-text filter by cloud account (supports multiple values)	false	string []
			cloudImage__contains	Free-text filter by cloud image (supports multiple values)	false	string []

			cloudInstanceId__contains	Free-text filter by cloud instance id(supports multiple values)	false	string []
			cloudInstanceSize__contains	Free-text filter by cloud instance size(supports multiple values)	false	string []
			cloudLocation__contains	Free-text filter by cloud location (supports multiple values)	false	string []
			cloudNetwork__contains	Free-text filter by cloud network (supports multiple values)	false	string []
			cloudProvider	Agents from which cloud provider	false	string []
			cloudProviderNin	Exclude Agents from these cloud provider	false	string []
			cloudTags__contains	Free-text filter by cloud tags (supports multiple values)	false	string []
			clusterName__contains	Free-text filter by cluster name (supports multiple values)	false	string []

			computerName	Computer name	false	string
			computerName__contains	Free-text filter by computer name (supports multiple values)	false	string []
			computerName__like	Match computer name partially (substring)	false	string
			consoleMigrationStatuses	Migration status in	false	string []
			consoleMigrationStatusesNin	Migration status nin	false	string []
			coreCount__between	Possible number of CPU cores (inclusive)	false	string
			coreCount__gt	CPU cores (more than)	false	integer
			coreCount__gte	CPU cores (more than or equal)	false	integer
			coreCount__lt	CPU cores (less than)	false	integer
			coreCount__lte	CPU cores (less than or equal)	false	integer
			cpuCount__between	Possible number of CPU cores (inclusive)	false	string
			cpuCount__gt	Number of CPUs (more than)	false	integer

			cpuCount__gte	Number of CPUs (more than or equal)	false	integer
			cpuCount__lt	Number of CPUs (less than)	false	integer
			cpuCount__lte	Number of CPUs (less than or equal)	false	integer
			cpuId__contains	Free-text filter by CPU name (supports multiple values)	false	string []
			createdAt__between	Date range for creation time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			createdAt__gt	Agents created after this timestamp	false	string
			createdAt__gte	Agents created after or at this timestamp	false	string
			createdAt__lt	Agents created before this timestamp	false	string
			createdAt__lte	Agents created before or at this timestamp	false	string
			csvFilterId	The ID of the CSV file to filter by	false	string

			decommissionedAt__between	Date range for decommission time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			decommissionedAt__gt	Agents decommissioned after this timestamp	false	string
			decommissionedAt__gte	Agents decommissioned after or at this timestamp	false	string
			decommissionedAt__lt	Agents decommissioned before this timestamp	false	string
			decommissionedAt__lte	Agents decommissioned before this timestamp	false	string
			domains	Included network domains	false	string []
			domainsNin	Not included network domains	false	string []
			encryptedApplications	Disk encryption status	false	boolean
			externalId__contains	Free-text filter by external ID (Customer ID)	false	string []
			externalIp__contains	Free-text filter by visible IP (supports	false	string []

				multiple values)		
			filteredGroupIds	List of Group IDs to filter by	false	string []
			filteredSiteIds	List of Site IDs to filter by	false	string []
			filterId	Include all Agents matching this saved filter	false	string
			firewallEnabled	The agents supports Firewall Control and it is enabled for the agent's group	false	boolean []
			gatewayIp	Gateway ip	false	string
			gcpServiceAccount__contains	Free-text filter by gcp service account (supports multiple values)	false	string []
			groupIds	List of Group IDs to filter by	false	string []
			hasContainerizedWorkload	Include only Agents protecting containerized workloads	false	boolean
			hasLocalConfiguration	Agent has a local configuration set	false	boolean
			hasTags	Include only Agents that	false	boolean

				have any tags assigned if True, or none if False		
			ids	A list of Agent IDs	false	string []
			infected	Include only Agents with at least one active threat	false	boolean
			installerTypes	Include only Agents installed with these package types	false	string []
			installerTypesNin	Exclude Agents installed with these package types	false	string []
			isActive	Include only active Agents	false	boolean
			isDecommissioned	Include active, decommissioned or both	false	boolean []
			isPendingUninstall	Include only Agents with pending uninstall requests	false	boolean
			isUninstalled	Include installed, uninstalled or both	false	boolean []
			isUpToDate	Include only Agents with updated software	false	boolean

			k8sNodeLabels__contains	Free-text filter by K8s node labels (supports multiple values)	false	string []
			k8sNodeName__contains	Free-text filter by K8s node name (supports multiple values)	false	string []
			k8sType__contains	Free-text filter by K8s type(supports multiple values)	false	string []
			k8sVersion__contains	Free-text filter by K8s version (supports multiple values)	false	string []
			lastActiveDate__between	Date range for last active date(format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			lastActiveDate__gt	Agents last active after this time	false	string
			lastActiveDate__gte	Agents last active after or at this time	false	string
			lastActiveDate__lt	Agents last active before this time	false	string
			lastActiveDate__lte	Agents last active before or at this time	false	string

			lastLoggedInUserName__contains	Free-text filter by username (supports multiple values)	false	string []
			lastSuccessfulScanDate__between	Date range for last successful full disk scan(format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			lastSuccessfulScanDate__gt	Agents last successful full disk scan after this time	false	string
			lastSuccessfulScanDate__gte	Agents last successful full disk scan after or at this time	false	string
			lastSuccessfulScanDate__lt	Agents last successful full disk scan before this time	false	string
			lastSuccessfulScanDate__lte	Agents last successful full disk scan before or at this time	false	string
			liveUpdateId__contains	Free-text filter by live update ID (supports multiple values)	false	string []
			locationEnabled	The agents supports	false	boolean []

				Location Awareness and it is enabled for the agent's group		
			locationIds	Include only Agents reporting these locations	false	string []
			locationIdsNin	Do not include only Agents reporting these locations	false	string []
			machineTypes	Included machine types	false	string []
			machineTypesNin	Not included machine types	false	string []
			migrationStatus	Migration status	false	enum
			missingPermissions	Included missing permissions	false	string []
			missingPermissionsNin	Excluded missing permissions	false	string []
			mitigationMode	Agent mitigation mode policy	false	enum
			mitigationModeSuspicious	Mitigation mode policy for suspicious activity	false	enum
			networkInterfaceGatewayMacAddress__c	Free-text filter by Gateway	false	string []

			ontains	MAC address (supports multiple values)		
			networkInterfaceInet__contains	Free-text filter by local IP (supports multiple values)	false	string []
			networkInterfacePhysical__contains	Free-text filter by MAC address (supports multiple values)	false	string []
			networkQuarantineEnabled	The agents supports Network Quarantine Control and its enabled for the agent's group	false	boolean []
			networkStatuses	Included network statuses	false	string []
			networkStatusesNin	Included network statuses	false	string []
			operationalStates	Agent operational state	false	string []
			operationalStatesNin	Do not include these Agent operational states	false	string []
			osArch	OS architecture	false	enum
			osTypes	Included OS types	false	string []

			osTypesNin	Not included OS types	false	string []
			osVersion__contains	Free-text filter by OS full name and version (supports multiple values)	false	string []
			query	A free-text search term, will match applicable attributes (sub-string match). Note: Device's physical addresses will be matched if they start with the search term only (no match if they contain the term).	false	string
			rangerStatus	[DEPRECATED] Use rangerStatuses.	false	enum
			rangerStatuses	Status of Ranger	false	string []
			rangerStatusesNin	Do not include these Ranger Statuses	false	string []
			rangerVersions	Ranger versions to include	false	string []
			rangerVersionsNin	Ranger versions not to include	false	string []

			registeredAt__between	Date range for first registration time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			registeredAt__gt	Agents registered after this time	false	string
			registeredAt__gte	Agents registered after or at this time	false	string
			registeredAt__lt	Agents registered before this time	false	string
			registeredAt__lte	Agents registered before or at this time	false	string
			remoteOpsForensicsSupported	Include only agents that has Remote Ops Forensicsfeature supported	false	boolean
			remoteProfilingStates	Agent remote profiling state	false	string []
			remoteProfilingStatesNin	Do not include these Agent remote profiling states	false	string []
			rsoLevel	Supported Remote Script Orchestration	false	enum

				level		
			scanStatus	Scan status	false	enum
			scanStatuses	Included scan statuses	false	string []
			scanStatuses Nin	Not included scan statuses	false	string []
			serialNumber __contains	Free-text filter by Serial Number (supports multiple values)	false	string []
			siteIds	List of Site IDs to filter by	false	string []
			tagsData	Filter agents by their assigned tags. Given in form of a JSON where each key represents a tag key, and each value represents a list of string values to filter by. To filter by unassigned tag values, use __nin suffix in the tag key.	false	string
			threatConten tHash	Include only Agents that have at least one threat with this content hash	false	string
			threatCreate	Agents with	false	string

			dAt__between	threats reported in a date range (format: <from_timestamp>-<to_timestamp>, inclusive)		
			threatCreatedAt__gt	Agents with threats reported after this time	false	string
			threatCreatedAt__gte	Agents with threats reported after or at this time	false	string
			threatCreatedAt__lt	Agents with threats reported before this time	false	string
			threatCreatedAt__lte	Agents with threats reported before or at this time	false	string
			threatHidden	Include only Agents with at least one hidden threat	false	boolean
			threatMitigationStatus	Include only Agents that have threats with this mitigation status	false	enum
			threatRebootRequired	Has at least one threat with at least one mitigation	false	boolean []

				action pending reboot to succeed		
			threatResolved	Include only Agents with at least one resolved threat	false	boolean
			totalMemory__between	Total memory range (GB, inclusive)	false	string
			totalMemory__gt	Memory size (MB, more than)	false	integer
			totalMemory__gte	Memory size (MB, more than or equal)	false	integer
			totalMemory__lt	Memory size (MB, less than)	false	integer
			totalMemory__lte	Memory size (MB, less than or equal)	false	integer
			updatedAt__between	Date range for update time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			updatedAt__gt	Agents updated after this timestamp	false	string
			updatedAt__gte	Agents updated after or at this timestamp	false	string
			updatedAt__lt	Agents updated	false	string

<table>
<tr><td></td><td></td><td></td><td><table>
<tr><td></td><td>before this timestamp</td><td></td><td></td></tr>
<tr><td>updatedAt__lte</td><td>Agents updated before or at this timestamp</td><td>false</td><td>string</td></tr>
<tr><td>userActionsNeeded</td><td>Included pending user actions</td><td>false</td><td>string []</td></tr>
<tr><td>userActionsNeededNin</td><td>Excluded pending user actions</td><td>false</td><td>string []</td></tr>
<tr><td>uuid</td><td>Agent's universally unique identifier</td><td>false</td><td>string</td></tr>
<tr><td>uuid__contains</td><td>Free-text filter by Agent UUID (supports multiple values)</td><td>false</td><td>string []</td></tr>
<tr><td>uuids</td><td>A list of included UUIDs</td><td>false</td><td>string []</td></tr>
</table></td></tr>
<tr><td>data</td><td>Data</td><td>false</td><td></td></tr>
</table>

Edit local upgrade site authorization

POST /web/api/v2.1/agents/actions/local-upgrade-authorization

Edit when authorization of local upgrades expires.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
data	Response data	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>affected</td><td>Number of entities affected by the requested operation</td><td>false</td><td>integer</td></tr></table>
errors	Errors	false	array

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>agentAuthorization</td><td>Agent approval expiration timestamp</td><td>true</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>filter</td><td>Applied filter - only matched Agents will be affected by the requested action. Leave empty to apply the action on all applicable Agents.</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>activeThreats</td><td>Include Agents with this amount of active threats</td><td>false</td><td>integer</td></tr>
<tr><td>activeThreats__gt</td><td>Include Agents with at least this amount of active threats</td><td>false</td><td>integer</td></tr>
<tr><td>adComputerMember__contains</td><td>Free-text filter by Active Directory computer groups string (supports multiple values)</td><td>false</td><td>string []</td></tr>
<tr><td>adComputerName__contains</td><td>Free-text filter by Active Directory computer name string (supports multiple values)</td><td>false</td><td>string []</td></tr>
</table>
</td></tr>
</table>

			adComputerQuery__contains	Free-text filter by Active Directory computer name or its groups (supports multiple values)	false	string []
			adQuery	An Active Directory query string	false	string
			adQuery__contains	Free-text filter by Active Directory string (supports multiple values)	false	string []
			adUserMember__contains	Free-text filter by Active Directory user groups string (supports multiple values)	false	string []
			adUserName__contains	Free-text filter by Active Directory username string (supports multiple values)	false	string []
			adUserQuery__contains	Free-text filter by Active Directory computer	false	string []

				name or its groups (supports multiple values)		
			agentNamespace__contains	Free-text filter by agent namespace (supports multiple values)	false	string []
			agentPodName__contains	Free-text filter by agent pod name (supports multiple values)	false	string []
			agentVersion__between	Version range for agent version (format: <from_version>-<to_version>, inclusive)	false	string
			agentVersion__gt	Agents versions greater than given version	false	string
			agentVersion__gte	Agents versions greater than or equal to given version	false	string
			agentVersion__lt	Agents versions less than given version	false	string
			agentVersion__lte	Agents versions less than or equal to given version	false	string

			agentVersions	Agent versions to include	false	string []
			agentVersionsNin	Agent versions not to include	false	string []
			appsVulnerabilityStatuses	Apps vulnerability status in	false	string []
			appsVulnerabilityStatusesNin	Apps vulnerability status nin	false	string []
			awsRole__contains	Free-text filter by aws role(supports multiple values)	false	string []
			awsSecurityGroups__contains	Free-text filter by aws securityGroups(supports multiple values)	false	string []
			awsSubnetIds__contains	Free-text filter by aws subnet ids (supports multiple values)	false	string []
			azureResourceGroup__contains	Free-text filter by azure resource group(supports multiple values)	false	string []
			cloudAccount__contains	Free-text filter by cloud account (supports multiple values)	false	string []
			cloudImage__	Free-text	false	string []

			contains	filter by cloud image (supports multiple values)		
			cloudInstanceId__contains	Free-text filter by cloud instance id(supports multiple values)	false	string []
			cloudInstanceSize__contains	Free-text filter by cloud instance size(supports multiple values)	false	string []
			cloudLocation__contains	Free-text filter by cloud location (supports multiple values)	false	string []
			cloudNetwork__contains	Free-text filter by cloud network (supports multiple values)	false	string []
			cloudProvider	Agents from which cloud provider	false	string []
			cloudProviderNin	Exclude Agents from these cloud provider	false	string []
			cloudTags__contains	Free-text filter by cloud tags (supports multiple values)	false	string []

			clusterName__contains	Free-text filter by cluster name (supports multiple values)	false	string []
			computerName	Computer name	false	string
			computerName__contains	Free-text filter by computer name (supports multiple values)	false	string []
			computerName__like	Match computer name partially (substring)	false	string
			consoleMigrationStatuses	Migration status in	false	string []
			consoleMigrationStatusesNin	Migration status nin	false	string []
			coreCount__between	Possible number of CPU cores (inclusive)	false	string
			coreCount__gt	CPU cores (more than)	false	integer
			coreCount__gte	CPU cores (more than or equal)	false	integer
			coreCount__lt	CPU cores (less than)	false	integer
			coreCount__lte	CPU cores (less than or equal)	false	integer
			cpuCount__between	Possible number of	false	string

				CPU cores (inclusive)		
			cpuCount__gt	Number of CPUs (more than)	false	integer
			cpuCount__gte	Number of CPUs (more than or equal)	false	integer
			cpuCount__lt	Number of CPUs (less than)	false	integer
			cpuCount__lte	Number of CPUs (less than or equal)	false	integer
			cpuId__contains	Free-text filter by CPU name (supports multiple values)	false	string []
			createdAt__between	Date range for creation time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			createdAt__gt	Agents created after this timestamp	false	string
			createdAt__gte	Agents created after or at this timestamp	false	string
			createdAt__lt	Agents created before this timestamp	false	string
			createdAt__lte	Agents created	false	string

				before or at this timestamp		
			csvFilterId	The ID of the CSV file to filter by	false	string
			decommissionedAt__between	Date range for decommission time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			decommissionedAt__gt	Agents decommissioned after this timestamp	false	string
			decommissionedAt__gte	Agents decommissioned after or at this timestamp	false	string
			decommissionedAt__lt	Agents decommissioned before this timestamp	false	string
			decommissionedAt__lte	Agents decommissioned before this timestamp	false	string
			domains	Included network domains	false	string []
			domainsNin	Not included network domains	false	string []
			encryptedApplications	Disk encryption status	false	boolean
			externalId__c	Free-text	false	string []

			ontains	filter by external ID (Customer ID)		
			externalIp__contains	Free-text filter by visible IP (supports multiple values)	false	string []
			filteredGroupIds	List of Group IDs to filter by	false	string []
			filteredSiteIds	List of Site IDs to filter by	false	string []
			filterId	Include all Agents matching this saved filter	false	string
			firewallEnabled	The agents supports Firewall Control and it is enabled for the agent's group	false	boolean []
			gatewayIp	Gateway ip	false	string
			gcpServiceAccount__contains	Free-text filter by gcp service account (supports multiple values)	false	string []
			groupIds	List of Group IDs to filter by	false	string []
			hasContainerizedWorkload	Include only Agents protecting containerized workloads	false	boolean

			hasLocalConfiguration	Agent has a local configuration set	false	boolean
			hasTags	Include only Agents that have any tags assigned if True, or none if False	false	boolean
			ids	A list of Agent IDs	false	string []
			infected	Include only Agents with at least one active threat	false	boolean
			installerTypes	Include only Agents installed with these package types	false	string []
			installerTypesNin	Exclude Agents installed with these package types	false	string []
			isActive	Include only active Agents	false	boolean
			isDecommissioned	Include active, decommissioned or both	false	boolean []
			isPendingUninstall	Include only Agents with pending uninstall requests	false	boolean
			isUninstalled	Include installed, uninstalled or	false	boolean []

				both		
			isUpToDate	Include only Agents with updated software	false	boolean
			k8sNodeLabels__contains	Free-text filter by K8s node labels (supports multiple values)	false	string []
			k8sNodeName__contains	Free-text filter by K8s node name (supports multiple values)	false	string []
			k8sType__contains	Free-text filter by K8s type(supports multiple values)	false	string []
			k8sVersion__contains	Free-text filter by K8s version (supports multiple values)	false	string []
			lastActiveDate__between	Date range for last active date(format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			lastActiveDate__gt	Agents last active after this time	false	string
			lastActiveDate__gte	Agents last active after or at this time	false	string
			lastActiveDat	Agents last	false	string

			e__lt	active before this time		
			lastActiveDate__lte	Agents last active before or at this time	false	string
			lastLoggedInUserName__contains	Free-text filter by username (supports multiple values)	false	string []
			lastSuccessfulScanDate__between	Date range for last successful full disk scan(format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			lastSuccessfulScanDate__gt	Agents last successful full disk scan after this time	false	string
			lastSuccessfulScanDate__gte	Agents last successful full disk scan after or at this time	false	string
			lastSuccessfulScanDate__lt	Agents last successful full disk scan before this time	false	string
			lastSuccessfulScanDate__lte	Agents last successful full disk scan before or at this time	false	string
			liveUpdateId__contains	Free-text filter by live	false	string []

				update ID (supports multiple values)		
			locationEnabled	The agents supports Location Awareness and it is enabled for the agent's group	false	boolean []
			locationIds	Include only Agents reporting these locations	false	string []
			locationIdsNin	Do not include only Agents reporting these locations	false	string []
			machineTypes	Included machine types	false	string []
			machineTypesNin	Not included machine types	false	string []
			migrationStatus	Migration status	false	enum
			missingPermissions	Included missing permissions	false	string []
			missingPermissionsNin	Excluded missing permissions	false	string []
			mitigationMode	Agent mitigation mode policy	false	enum
			mitigationMo	Mitigation	false	enum

			deSuspicious	mode policy for suspicious activity		
			networkInterfaceGatewayMacAddress__contains	Free-text filter by Gateway MAC address (supports multiple values)	false	string []
			networkInterfacelnet__contains	Free-text filter by local IP (supports multiple values)	false	string []
			networkInterfacePhysical__contains	Free-text filter by MAC address (supports multiple values)	false	string []
			networkQuarantineEnabled	The agents supports Network Quarantine Control and its enabled for the agent's group	false	boolean []
			networkStatuses	Included network statuses	false	string []
			networkStatusesNin	Included network statuses	false	string []
			operationalStates	Agent operational state	false	string []
			operationalStatesNin	Do not include these Agent operational	false	string []

				states		
			osArch	OS architecture	false	enum
			osTypes	Included OS types	false	string []
			osTypesNin	Not included OS types	false	string []
			osVersion__contains	Free-text filter by OS full name and version (supports multiple values)	false	string []
			query	A free-text search term, will match applicable attributes (sub-string match). Note: Device's physical addresses will be matched if they start with the search term only (no match if they contain the term).	false	string
			rangerStatus	[DEPRECATED] Use rangerStatuses.	false	enum
			rangerStatuses	Status of Ranger	false	string []
			rangerStatusesNin	Do not include these Ranger Statuses	false	string []

			rangerVersions	Ranger versions to include	false	string []
			rangerVersionsNin	Ranger versions not to include	false	string []
			registeredAt__between	Date range for first registration time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			registeredAt__gt	Agents registered after this time	false	string
			registeredAt__gte	Agents registered after or at this time	false	string
			registeredAt__lt	Agents registered before this time	false	string
			registeredAt__lte	Agents registered before or at this time	false	string
			remoteOpsForensicsSupported	Include only agents that has Remote Ops Forensicsfeature supported	false	boolean
			remoteProfilingStates	Agent remote profiling state	false	string []
			remoteProfilingStatesNin	Do not include these Agent remote	false	string []

				profiling states		
			rsoLevel	Supported Remote Script Orchestration level	false	enum
			scanStatus	Scan status	false	enum
			scanStatuses	Included scan statuses	false	string []
			scanStatuses Nin	Not included scan statuses	false	string []
			serialNumber __contains	Free-text filter by Serial Number (supports multiple values)	false	string []
			siteIds	List of Site IDs to filter by	false	string []
			tagsData	Filter agents by their assigned tags. Given in form of a JSON where each key represents a tag key, and each value represents a list of string values to filter by. To filter by unassigned tag values, use __nin suffix in the tag key.	false	string
			threatConten	Include only	false	string

			tHash	Agents that have at least one threat with this content hash		
			threatCreatedAt__between	Agents with threats reported in a date range (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			threatCreatedAt__gt	Agents with threats reported after this time	false	string
			threatCreatedAt__gte	Agents with threats reported after or at this time	false	string
			threatCreatedAt__lt	Agents with threats reported before this time	false	string
			threatCreatedAt__lte	Agents with threats reported before or at this time	false	string
			threatHidden	Include only Agents with at least one hidden threat	false	boolean
			threatMitigationStatus	Include only Agents that have threats with this mitigation	false	enum

				status		
			threatRebootRequired	Has at least one threat with at least one mitigation action pending reboot to succeed	false	boolean []
			threatResolved	Include only Agents with at least one resolved threat	false	boolean
			totalMemory__between	Total memory range (GB, inclusive)	false	string
			totalMemory__gt	Memory size (MB, more than)	false	integer
			totalMemory__gte	Memory size (MB, more than or equal)	false	integer
			totalMemory__lt	Memory size (MB, less than)	false	integer
			totalMemory__lte	Memory size (MB, less than or equal)	false	integer
			updatedAt__between	Date range for update time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			updatedAt__gt	Agents updated after this timestamp	false	string

			updatedAt__gte	Agents updated after or at this timestamp	false	string
			updatedAt__lt	Agents updated before this timestamp	false	string
			updatedAt__lte	Agents updated before or at this timestamp	false	string
			userActionsNeeded	Included pending user actions	false	string []
			userActionsNeededNin	Excluded pending user actions	false	string []
			uuid	Agent's universally unique identifier	false	string
			uuid__contains	Free-text filter by Agent UUID (supports multiple values)	false	string []
			uuids	A list of included UUIDs	false	string []

Disable Agent

POST /web/api/v2.1/agents/actions/disable-agent

Use this command to disable Agents that match the filter.
Disabled agents run with minimal footprint and do not detect or mitigate threats, but they maintain connectivity with the Management Console.
If the command returns "Insufficient permissions", make sure you have permissions for the Account, Site, or Group and a role that allows Disable Agent (Admin, IR team or IT).
In the body of this command, the data parameter set is mandatory.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - Insufficient permissions

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>affected</td><td>Number of entities affected by the requested operation</td><td>false</td><td>integer</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>shouldReboot</td><td>Reboot the endpoint</td><td>true</td><td>boolean</td></tr>
<tr><td>expiration</td><td>Agents will be re-enabled after this timestamp</td><td>false</td><td>string</td></tr>
<tr><td>expirationTimezone</td><td>Timezone for the expiration timestamp</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>filter</td><td>Applied filter - only matched Agents will be affected by the requested action. Leave empty to apply the action on all applicable Agents.</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>activeThreats</td><td>Include Agents with this amount of active threats</td><td>false</td><td>integer</td></tr>
<tr><td>activeThreats__gt</td><td>Include Agents with at least this amount of active threats</td><td>false</td><td>integer</td></tr>
<tr><td>adComputerMember__contains</td><td>Free-text filter by Active Directory computer groups string (supports multiple values)</td><td>false</td><td>string []</td></tr>
<tr><td>adComputerName__contains</td><td>Free-text filter by Active</td><td>false</td><td>string []</td></tr>
</table>
</td></tr>
</table>

				Directory computer name string (supports multiple values)		
			adComputerQuery__contains	Free-text filter by Active Directory computer name or its groups (supports multiple values)	false	string []
			adQuery	An Active Directory query string	false	string
			adQuery__contains	Free-text filter by Active Directory string (supports multiple values)	false	string []
			adUserMember__contains	Free-text filter by Active Directory user groups string (supports multiple values)	false	string []
			adUserName__contains	Free-text filter by Active Directory username string (supports multiple	false	string []

				values)		
			adUserQuery__contains	Free-text filter by Active Directory computer name or its groups (supports multiple values)	false	string []
			agentNamespace__contains	Free-text filter by agent namespace (supports multiple values)	false	string []
			agentPodName__contains	Free-text filter by agent pod name (supports multiple values)	false	string []
			agentVersion__between	Version range for agent version (format: <from_version>-<to_version>, inclusive)	false	string
			agentVersion__gt	Agents versions greater than given version	false	string
			agentVersion__gte	Agents versions greater than or equal to given version	false	string
			agentVersion__lt	Agents versions less than given	false	string

				version		
			agentVersion__lte	Agents versions less than or equal to given version	false	string
			agentVersions	Agent versions to include	false	string []
			agentVersionsNin	Agent versions not to include	false	string []
			appsVulnerabilityStatuses	Apps vulnerability status in	false	string []
			appsVulnerabilityStatusesNin	Apps vulnerability status nin	false	string []
			awsRole__contains	Free-text filter by aws role(supports multiple values)	false	string []
			awsSecurityGroups__contains	Free-text filter by aws securityGroups(supports multiple values)	false	string []
			awsSubnetIds__contains	Free-text filter by aws subnet ids (supports multiple values)	false	string []
			azureResourceGroup__contains	Free-text filter by azure resource group(supports multiple values)	false	string []

			cloudAccount__contains	Free-text filter by cloud account (supports multiple values)	false	string []
			cloudImage__contains	Free-text filter by cloud image (supports multiple values)	false	string []
			cloudInstanceId__contains	Free-text filter by cloud instance id(supports multiple values)	false	string []
			cloudInstanceSize__contains	Free-text filter by cloud instance size(supports multiple values)	false	string []
			cloudLocation__contains	Free-text filter by cloud location (supports multiple values)	false	string []
			cloudNetwork__contains	Free-text filter by cloud network (supports multiple values)	false	string []
			cloudProvider	Agents from which cloud provider	false	string []
			cloudProviderNin	Exclude Agents from these cloud provider	false	string []

			cloudTags__contains	Free-text filter by cloud tags (supports multiple values)	false	string []
			clusterName__contains	Free-text filter by cluster name (supports multiple values)	false	string []
			computerName	Computer name	false	string
			computerName__contains	Free-text filter by computer name (supports multiple values)	false	string []
			computerName__like	Match computer name partially (substring)	false	string
			consoleMigrationStatuses	Migration status in	false	string []
			consoleMigrationStatusesNin	Migration status nin	false	string []
			coreCount__between	Possible number of CPU cores (inclusive)	false	string
			coreCount__gt	CPU cores (more than)	false	integer
			coreCount__gte	CPU cores (more than or equal)	false	integer
			coreCount__lt	CPU cores	false	integer

				(less than)		
			coreCount__lte	CPU cores (less than or equal)	false	integer
			cpuCount__between	Possible number of CPU cores (inclusive)	false	string
			cpuCount__gt	Number of CPUs (more than)	false	integer
			cpuCount__gte	Number of CPUs (more than or equal)	false	integer
			cpuCount__lt	Number of CPUs (less than)	false	integer
			cpuCount__lte	Number of CPUs (less than or equal)	false	integer
			cpuId__contains	Free-text filter by CPU name (supports multiple values)	false	string []
			createdAt__between	Date range for creation time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			createdAt__gt	Agents created after this timestamp	false	string
			createdAt__gte	Agents created after or at this timestamp	false	string

			createdAt__lt	Agents created before this timestamp	false	string
			createdAt__lte	Agents created before or at this timestamp	false	string
			csvFilterId	The ID of the CSV file to filter by	false	string
			decommissionedAt__between	Date range for decommission time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			decommissionedAt__gt	Agents decommissioned after this timestamp	false	string
			decommissionedAt__gte	Agents decommissioned after or at this timestamp	false	string
			decommissionedAt__lt	Agents decommissioned before this timestamp	false	string
			decommissionedAt__lte	Agents decommissioned before this timestamp	false	string
			domains	Included network domains	false	string []
			domainsNin	Not included network	false	string []

				domains		
			encryptedApplications	Disk encryption status	false	boolean
			externalId__contains	Free-text filter by external ID (Customer ID)	false	string []
			externalIp__contains	Free-text filter by visible IP (supports multiple values)	false	string []
			filteredGroupIds	List of Group IDs to filter by	false	string []
			filteredSiteIds	List of Site IDs to filter by	false	string []
			filterId	Include all Agents matching this saved filter	false	string
			firewallEnabled	The agents supports Firewall Control and it is enabled for the agent's group	false	boolean []
			gatewayIp	Gateway ip	false	string
			gcpServiceAccount__contains	Free-text filter by gcp service account (supports multiple values)	false	string []
			groupIds	List of Group IDs to filter	false	string []

				by		
			hasContainerizedWorkload	Include only Agents protecting containerized workloads	false	boolean
			hasLocalConfiguration	Agent has a local configuration set	false	boolean
			hasTags	Include only Agents that have any tags assigned if True, or none if False	false	boolean
			ids	A list of Agent IDs	false	string []
			infected	Include only Agents with at least one active threat	false	boolean
			installerTypes	Include only Agents installed with these package types	false	string []
			installerTypesNin	Exclude Agents installed with these package types	false	string []
			isActive	Include only active Agents	false	boolean
			isDecommissioned	Include active, decommissioned or both	false	boolean []
			isPendingUnin	Include only	false	boolean

			stall	Agents with pending uninstall requests		
			isUninstalled	Include installed, uninstalled or both	false	boolean []
			isUpToDate	Include only Agents with updated software	false	boolean
			k8sNodeLabels__contains	Free-text filter by K8s node labels (supports multiple values)	false	string []
			k8sNodeName__contains	Free-text filter by K8s node name (supports multiple values)	false	string []
			k8sType__contains	Free-text filter by K8s type(supports multiple values)	false	string []
			k8sVersion__contains	Free-text filter by K8s version (supports multiple values)	false	string []
			lastActiveDate__between	Date range for last active date(format: <from_timestamp>-<to_timestamp>, inclusive)	false	string

			lastActiveDate__gt	Agents last active after this time	false	string
			lastActiveDate__gte	Agents last active after or at this time	false	string
			lastActiveDate__lt	Agents last active before this time	false	string
			lastActiveDate__lte	Agents last active before or at this time	false	string
			lastLoggedInUserName__contains	Free-text filter by username (supports multiple values)	false	string []
			lastSuccessfulScanDate__between	Date range for last successful full disk scan(format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			lastSuccessfulScanDate__gt	Agents last successful full disk scan after this time	false	string
			lastSuccessfulScanDate__gte	Agents last successful full disk scan after or at this time	false	string
			lastSuccessfulScanDate__lt	Agents last successful full disk scan before this time	false	string

			lastSuccessfulScanDate__lte	Agents last successful full disk scan before or at this time	false	string
			liveUpdateId__contains	Free-text filter by live update ID (supports multiple values)	false	string []
			locationEnabled	The agents supports Location Awareness and it is enabled for the agent's group	false	boolean []
			locationIds	Include only Agents reporting these locations	false	string []
			locationIdsNin	Do not include only Agents reporting these locations	false	string []
			machineTypes	Included machine types	false	string []
			machineTypesNin	Not included machine types	false	string []
			migrationStatus	Migration status	false	enum
			missingPermissions	Included missing permissions	false	string []
			missingPermi	Excluded	false	string []

			ssionsNin	missing permissions		
			mitigationMode	Agent mitigation mode policy	false	enum
			mitigationModeSuspicious	Mitigation mode policy for suspicious activity	false	enum
			networkInterfaceGatewayMacAddress__contains	Free-text filter by Gateway MAC address (supports multiple values)	false	string []
			networkInterfaceInet__contains	Free-text filter by local IP (supports multiple values)	false	string []
			networkInterfacePhysical__contains	Free-text filter by MAC address (supports multiple values)	false	string []
			networkQuarantineEnabled	The agents supports Network Quarantine Control and its enabled for the agent's group	false	boolean []
			networkStatuses	Included network statuses	false	string []
			networkStatusesNin	Included network statuses	false	string []
			operationalSt	Agent	false	string []

			ates	operational state		
			operationalStatesNin	Do not include these Agent operational states	false	string []
			osArch	OS architecture	false	enum
			osTypes	Included OS types	false	string []
			osTypesNin	Not included OS types	false	string []
			osVersion__contains	Free-text filter by OS full name and version (supports multiple values)	false	string []
			query	A free-text search term, will match applicable attributes (sub-string match). Note: Device's physical addresses will be matched if they start with the search term only (no match if they contain the term).	false	string
			rangerStatus	[DEPRECATED] Use rangerStatuses.	false	enum

			rangerStatuses	Status of Ranger	false	string []
			rangerStatusesNin	Do not include these Ranger Statuses	false	string []
			rangerVersions	Ranger versions to include	false	string []
			rangerVersionsNin	Ranger versions not to include	false	string []
			registeredAt__between	Date range for first registration time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			registeredAt__gt	Agents registered after this time	false	string
			registeredAt__gte	Agents registered after or at this time	false	string
			registeredAt__lt	Agents registered before this time	false	string
			registeredAt__lte	Agents registered before or at this time	false	string
			remoteOpsForensicsSupported	Include only agents that has Remote Ops Forensicsfeature	false	boolean

				supported		
			remoteProfilingStates	Agent remote profiling state	false	string []
			remoteProfilingStatesNin	Do not include these Agent remote profiling states	false	string []
			rsoLevel	Supported Remote Script Orchestration level	false	enum
			scanStatus	Scan status	false	enum
			scanStatuses	Included scan statuses	false	string []
			scanStatuses Nin	Not included scan statuses	false	string []
			serialNumber__contains	Free-text filter by Serial Number (supports multiple values)	false	string []
			siteIds	List of Site IDs to filter by	false	string []
			tagsData	Filter agents by their assigned tags. Given in form of a JSON where each key represents a tag key, and each value represents a list of string values to filter by. To filter by	false	string

				unassigned tag values, use __nin suffix in the tag key.		
			threatContentHash	Include only Agents that have at least one threat with this content hash	false	string
			threatCreatedAt__between	Agents with threats reported in a date range (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			threatCreatedAt__gt	Agents with threats reported after this time	false	string
			threatCreatedAt__gte	Agents with threats reported after or at this time	false	string
			threatCreatedAt__lt	Agents with threats reported before this time	false	string
			threatCreatedAt__lte	Agents with threats reported before or at this time	false	string
			threatHidden	Include only Agents with at least one	false	boolean

				hidden threat		
			threatMitigationStatus	Include only Agents that have threats with this mitigation status	false	enum
			threatRebootRequired	Has at least one threat with at least one mitigation action pending reboot to succeed	false	boolean []
			threatResolved	Include only Agents with at least one resolved threat	false	boolean
			totalMemory__between	Total memory range (GB, inclusive)	false	string
			totalMemory__gt	Memory size (MB, more than)	false	integer
			totalMemory__gte	Memory size (MB, more than or equal)	false	integer
			totalMemory__lt	Memory size (MB, less than)	false	integer
			totalMemory__lte	Memory size (MB, less than or equal)	false	integer
			updatedAt__between	Date range for update time (format: <from_timestamp>-<to_timestam	false	string

				p>, inclusive)		
			updatedAt__gt	Agents updated after this timestamp	false	string
			updatedAt__gte	Agents updated after or at this timestamp	false	string
			updatedAt__lt	Agents updated before this timestamp	false	string
			updatedAt__lte	Agents updated before or at this timestamp	false	string
			userActionsNeeded	Included pending user actions	false	string []
			userActionsNeededNin	Excluded pending user actions	false	string []
			uuid	Agent's universally unique identifier	false	string
			uuid__contains	Free-text filter by Agent UUID (supports multiple values)	false	string []
			uuids	A list of included UUIDs	false	string []

Enable Agent

POST /web/api/v2.1/agents/actions/enable-agent

Use this command to enable disabled Agents that match the filter.
If the command returns "Insufficient permissions", make sure you have permissions for the Account, Site, or Group and a role that allows Disable Agent (Admin, IR team or IT).
In the body of this command, the data parameter set is mandatory.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - Insufficient permissions

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>affected</td><td>Number of entities affected by the requested operation</td><td>false</td><td>integer</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

Name	Description	Required	Value
data	Data	true	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>shouldReboot</td><td>Reboot the endpoint</td><td>true</td><td>boolean</td></tr></table>
filter	Applied filter - only matched Agents will be affected by the requested action. Leave empty to apply the action on all applicable Agents.	true	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr><tr><td>activeThreats</td><td>Include Agents with this amount of active threats</td><td>false</td><td>integer</td></tr><tr><td>activeThreats__gt</td><td>Include Agents with at least this amount of active threats</td><td>false</td><td>integer</td></tr><tr><td>adComputerMember__contains</td><td>Free-text filter by Active Directory computer groups string (supports multiple values)</td><td>false</td><td>string []</td></tr><tr><td>adComputerName__contains</td><td>Free-text filter by Active Directory computer name string (supports multiple values)</td><td>false</td><td>string []</td></tr><tr><td>adComputerQuery__contain</td><td>Free-text filter by</td><td>false</td><td>string []</td></tr></table>

			s	Active Directory computer name or its groups (supports multiple values)		
			adQuery	An Active Directory query string	false	string
			adQuery__contains	Free-text filter by Active Directory string (supports multiple values)	false	string []
			adUserMember__contains	Free-text filter by Active Directory user groups string (supports multiple values)	false	string []
			adUserName__contains	Free-text filter by Active Directory username string (supports multiple values)	false	string []
			adUserQuery__contains	Free-text filter by Active Directory computer name or its groups	false	string []

				(supports multiple values)		
			agentNamespace__contains	Free-text filter by agent namespace (supports multiple values)	false	string []
			agentPodName__contains	Free-text filter by agent pod name (supports multiple values)	false	string []
			agentVersion__between	Version range for agent version (format: <from_version>-<to_version>, inclusive)	false	string
			agentVersion__gt	Agents versions greater than given version	false	string
			agentVersion__gte	Agents versions greater than or equal to given version	false	string
			agentVersion__lt	Agents versions less than given version	false	string
			agentVersion__lte	Agents versions less than or equal to given version	false	string
			agentVersion	Agent	false	string []

			s	versions to include		
			agentVersionsNin	Agent versions not to include	false	string []
			appsVulnerabilityStatuses	Apps vulnerability status in	false	string []
			appsVulnerabilityStatusesNin	Apps vulnerability status nin	false	string []
			awsRole__contains	Free-text filter by aws role(supports multiple values)	false	string []
			awsSecurityGroups__contains	Free-text filter by aws securityGroups(supports multiple values)	false	string []
			awsSubnetIds__contains	Free-text filter by aws subnet ids (supports multiple values)	false	string []
			azureResourceGroup__contains	Free-text filter by azure resource group(supports multiple values)	false	string []
			cloudAccount__contains	Free-text filter by cloud account (supports multiple values)	false	string []
			cloudImage__contains	Free-text filter by cloud	false	string []

				image (supports multiple values)		
			cloudInstanceId__contains	Free-text filter by cloud instance id(supports multiple values)	false	string []
			cloudInstanceSize__contains	Free-text filter by cloud instance size(supports multiple values)	false	string []
			cloudLocation__contains	Free-text filter by cloud location (supports multiple values)	false	string []
			cloudNetwork__contains	Free-text filter by cloud network (supports multiple values)	false	string []
			cloudProvider	Agents from which cloud provider	false	string []
			cloudProviderNin	Exclude Agents from these cloud provider	false	string []
			cloudTags__contains	Free-text filter by cloud tags (supports multiple values)	false	string []
			clusterName_	Free-text	false	string []

			_contains	filter by cluster name (supports multiple values)		
			computerName	Computer name	false	string
			computerName__contains	Free-text filter by computer name (supports multiple values)	false	string []
			computerName__like	Match computer name partially (substring)	false	string
			consoleMigrationStatuses	Migration status in	false	string []
			consoleMigrationStatusesNin	Migration status nin	false	string []
			coreCount__between	Possible number of CPU cores (inclusive)	false	string
			coreCount__gt	CPU cores (more than)	false	integer
			coreCount__gte	CPU cores (more than or equal)	false	integer
			coreCount__lt	CPU cores (less than)	false	integer
			coreCount__lte	CPU cores (less than or equal)	false	integer
			cpuCount__between	Possible number of CPU cores	false	string

				(inclusive)		
			cpuCount__gt	Number of CPUs (more than)	false	integer
			cpuCount__gte	Number of CPUs (more than or equal)	false	integer
			cpuCount__lt	Number of CPUs (less than)	false	integer
			cpuCount__lte	Number of CPUs (less than or equal)	false	integer
			cpuId__contains	Free-text filter by CPU name (supports multiple values)	false	string []
			createdAt__between	Date range for creation time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			createdAt__gt	Agents created after this timestamp	false	string
			createdAt__gte	Agents created after or at this timestamp	false	string
			createdAt__lt	Agents created before this timestamp	false	string
			createdAt__lte	Agents created before or at	false	string

				this timestamp		
			csvFilterId	The ID of the CSV file to filter by	false	string
			decommissionedAt__between	Date range for decommission time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			decommissionedAt__gt	Agents decommissioned after this timestamp	false	string
			decommissionedAt__gte	Agents decommissioned after or at this timestamp	false	string
			decommissionedAt__lt	Agents decommissioned before this timestamp	false	string
			decommissionedAt__lte	Agents decommissioned before this timestamp	false	string
			domains	Included network domains	false	string []
			domainsNin	Not included network domains	false	string []
			encryptedApplications	Disk encryption status	false	boolean
			externalId__contains	Free-text filter by	false	string []

				external ID (Customer ID)		
			externalIp__contains	Free-text filter by visible IP (supports multiple values)	false	string []
			filteredGroupIds	List of Group IDs to filter by	false	string []
			filteredSiteIds	List of Site IDs to filter by	false	string []
			filterId	Include all Agents matching this saved filter	false	string
			firewallEnabled	The agents supports Firewall Control and it is enabled for the agent's group	false	boolean []
			gatewayIp	Gateway ip	false	string
			gcpServiceAccount__contains	Free-text filter by gcp service account (supports multiple values)	false	string []
			groupIds	List of Group IDs to filter by	false	string []
			hasContainerizedWorkload	Include only Agents protecting containerized workloads	false	boolean

			hasLocalConfiguration	Agent has a local configuration set	false	boolean
			hasTags	Include only Agents that have any tags assigned if True, or none if False	false	boolean
			ids	A list of Agent IDs	false	string []
			infected	Include only Agents with at least one active threat	false	boolean
			installerTypes	Include only Agents installed with these package types	false	string []
			installerTypesNin	Exclude Agents installed with these package types	false	string []
			isActive	Include only active Agents	false	boolean
			isDecommissioned	Include active, decommissioned or both	false	boolean []
			isPendingUninstall	Include only Agents with pending uninstall requests	false	boolean
			isUninstalled	Include installed, uninstalled or	false	boolean []

				both		
			isUpToDate	Include only Agents with updated software	false	boolean
			k8sNodeLabels__contains	Free-text filter by K8s node labels (supports multiple values)	false	string []
			k8sNodeName__contains	Free-text filter by K8s node name (supports multiple values)	false	string []
			k8sType__contains	Free-text filter by K8s type(supports multiple values)	false	string []
			k8sVersion__contains	Free-text filter by K8s version (supports multiple values)	false	string []
			lastActiveDate__between	Date range for last active date(format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			lastActiveDate__gt	Agents last active after this time	false	string
			lastActiveDate__gte	Agents last active after or at this time	false	string
			lastActiveDat	Agents last	false	string

			e__lt	active before this time		
			lastActiveDate__lte	Agents last active before or at this time	false	string
			lastLoggedInUserName__contains	Free-text filter by username (supports multiple values)	false	string []
			lastSuccessfulScanDate__between	Date range for last successful full disk scan(format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			lastSuccessfulScanDate__gt	Agents last successful full disk scan after this time	false	string
			lastSuccessfulScanDate__gte	Agents last successful full disk scan after or at this time	false	string
			lastSuccessfulScanDate__lt	Agents last successful full disk scan before this time	false	string
			lastSuccessfulScanDate__lte	Agents last successful full disk scan before or at this time	false	string
			liveUpdateId__contains	Free-text filter by live	false	string []

				update ID (supports multiple values)		
			locationEnabled	The agents supports Location Awareness and it is enabled for the agent's group	false	boolean []
			locationIds	Include only Agents reporting these locations	false	string []
			locationIdsNin	Do not include only Agents reporting these locations	false	string []
			machineTypes	Included machine types	false	string []
			machineTypesNin	Not included machine types	false	string []
			migrationStatus	Migration status	false	enum
			missingPermissions	Included missing permissions	false	string []
			missingPermissionsNin	Excluded missing permissions	false	string []
			mitigationMode	Agent mitigation mode policy	false	enum
			mitigationMo	Mitigation	false	enum

			deSuspicious	mode policy for suspicious activity		
			networkInterfaceGatewayMacAddress__contains	Free-text filter by Gateway MAC address (supports multiple values)	false	string []
			networkInterfaceInet__contains	Free-text filter by local IP (supports multiple values)	false	string []
			networkInterfacePhysical__contains	Free-text filter by MAC address (supports multiple values)	false	string []
			networkQuarantineEnabled	The agents supports Network Quarantine Control and its enabled for the agent's group	false	boolean []
			networkStatuses	Included network statuses	false	string []
			networkStatusesNin	Included network statuses	false	string []
			operationalStates	Agent operational state	false	string []
			operationalStatesNin	Do not include these Agent operational	false	string []

				states		
			osArch	OS architecture	false	enum
			osTypes	Included OS types	false	string []
			osTypesNin	Not included OS types	false	string []
			osVersion__contains	Free-text filter by OS full name and version (supports multiple values)	false	string []
			query	A free-text search term, will match applicable attributes (sub-string match). Note: Device's physical addresses will be matched if they start with the search term only (no match if they contain the term).	false	string
			rangerStatus	[DEPRECATED] Use rangerStatuses.	false	enum
			rangerStatuses	Status of Ranger	false	string []
			rangerStatusesNin	Do not include these Ranger Statuses	false	string []

			rangerVersions	Ranger versions to include	false	string []
			rangerVersionsNin	Ranger versions not to include	false	string []
			registeredAt__between	Date range for first registration time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			registeredAt__gt	Agents registered after this time	false	string
			registeredAt__gte	Agents registered after or at this time	false	string
			registeredAt__lt	Agents registered before this time	false	string
			registeredAt__lte	Agents registered before or at this time	false	string
			remoteOpsForensicsSupported	Include only agents that has Remote Ops Forensicsfeature supported	false	boolean
			remoteProfilingStates	Agent remote profiling state	false	string []
			remoteProfilingStatesNin	Do not include these Agent remote	false	string []

				profiling states		
			rsoLevel	Supported Remote Script Orchestration level	false	enum
			scanStatus	Scan status	false	enum
			scanStatuses	Included scan statuses	false	string []
			scanStatuses Nin	Not included scan statuses	false	string []
			serialNumber __contains	Free-text filter by Serial Number (supports multiple values)	false	string []
			siteIds	List of Site IDs to filter by	false	string []
			tagsData	Filter agents by their assigned tags. Given in form of a JSON where each key represents a tag key, and each value represents a list of string values to filter by. To filter by unassigned tag values, use __nin suffix in the tag key.	false	string
			threatConten	Include only	false	string

			tHash	Agents that have at least one threat with this content hash		
			threatCreatedAt__between	Agents with threats reported in a date range (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			threatCreatedAt__gt	Agents with threats reported after this time	false	string
			threatCreatedAt__gte	Agents with threats reported after or at this time	false	string
			threatCreatedAt__lt	Agents with threats reported before this time	false	string
			threatCreatedAt__lte	Agents with threats reported before or at this time	false	string
			threatHidden	Include only Agents with at least one hidden threat	false	boolean
			threatMitigationStatus	Include only Agents that have threats with this mitigation	false	enum

				status		
			threatRebootRequired	Has at least one threat with at least one mitigation action pending reboot to succeed	false	boolean []
			threatResolved	Include only Agents with at least one resolved threat	false	boolean
			totalMemory__between	Total memory range (GB, inclusive)	false	string
			totalMemory__gt	Memory size (MB, more than)	false	integer
			totalMemory__gte	Memory size (MB, more than or equal)	false	integer
			totalMemory__lt	Memory size (MB, less than)	false	integer
			totalMemory__lte	Memory size (MB, less than or equal)	false	integer
			updatedAt__between	Date range for update time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			updatedAt__gt	Agents updated after this timestamp	false	string

			updatedAt__gte	Agents updated after or at this timestamp	false	string
			updatedAt__lt	Agents updated before this timestamp	false	string
			updatedAt__lte	Agents updated before or at this timestamp	false	string
			userActionsNeeded	Included pending user actions	false	string []
			userActionsNeededNin	Excluded pending user actions	false	string []
			uuid	Agent's universally unique identifier	false	string
			uuid__contains	Free-text filter by Agent UUID (supports multiple values)	false	string []
			uuids	A list of included UUIDs	false	string []

Start Remote Profiling

POST /web/api/v2.1/agents/actions/start-profiling

Use this command to start remote profiling on Agents that match the filter.
Remote profiling lets you collect runtime diagnostic information for Agents on containers.
If the command returns "Insufficient permissions", make sure you have permissions for the Account, Site, or Group and a role that allows Start Remote Profiling (Admin or IT).

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - Insufficient permissions

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>affected</td><td>Number of entities affected by the requested operation</td><td>false</td><td>integer</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

Name	Description	Required	Value
filter	Applied filter - only matched Agents will be affected by the requested action. Leave empty to apply the action on all applicable Agents.	true	

Name	Description	Required	Value
accountIds	List of Account IDs to filter by	false	string []
activeThreats	Include Agents with this amount of active threats	false	integer
activeThreats__gt	Include Agents with at least this amount of active threats	false	integer
adComputerMember__contains	Free-text filter by Active Directory computer groups string (supports multiple values)	false	string []
adComputerName__contains	Free-text filter by Active Directory computer name string (supports multiple values)	false	string []
adComputerQuery__contains	Free-text filter by Active Directory computer name or its groups	false	string []

				(supports multiple values)		
			adQuery	An Active Directory query string	false	string
			adQuery__contains	Free-text filter by Active Directory string (supports multiple values)	false	string []
			adUserMember__contains	Free-text filter by Active Directory user groups string (supports multiple values)	false	string []
			adUserName__contains	Free-text filter by Active Directory username string (supports multiple values)	false	string []
			adUserQuery__contains	Free-text filter by Active Directory computer name or its groups (supports multiple values)	false	string []
			agentNamespa	Free-text	false	string []

			ce__contains	filter by agent namespace (supports multiple values)		
			agentPodName__contains	Free-text filter by agent pod name (supports multiple values)	false	string []
			agentVersion__between	Version range for agent version (format: <from_version>-<to_version>, inclusive)	false	string
			agentVersion__gt	Agents versions greater than given version	false	string
			agentVersion__gte	Agents versions greater than or equal to given version	false	string
			agentVersion__lt	Agents versions less than given version	false	string
			agentVersion__lte	Agents versions less than or equal to given version	false	string
			agentVersions	Agent versions to include	false	string []
			agentVersionsNin	Agent versions not	false	string []

				to include		
			appsVulnerabilityStatuses	Apps vulnerability status in	false	string []
			appsVulnerabilityStatusesNin	Apps vulnerability status nin	false	string []
			awsRole__contains	Free-text filter by aws role(supports multiple values)	false	string []
			awsSecurityGroups__contains	Free-text filter by aws securityGroups(supports multiple values)	false	string []
			awsSubnetIds__contains	Free-text filter by aws subnet ids (supports multiple values)	false	string []
			azureResourceGroup__contains	Free-text filter by azure resource group(supports multiple values)	false	string []
			cloudAccount__contains	Free-text filter by cloud account (supports multiple values)	false	string []
			cloudImage__contains	Free-text filter by cloud image (supports multiple values)	false	string []

			cloudInstanceId__contains	Free-text filter by cloud instance id(supports multiple values)	false	string []
			cloudInstanceSize__contains	Free-text filter by cloud instance size(supports multiple values)	false	string []
			cloudLocation__contains	Free-text filter by cloud location (supports multiple values)	false	string []
			cloudNetwork__contains	Free-text filter by cloud network (supports multiple values)	false	string []
			cloudProvider	Agents from which cloud provider	false	string []
			cloudProviderNin	Exclude Agents from these cloud provider	false	string []
			cloudTags__contains	Free-text filter by cloud tags (supports multiple values)	false	string []
			clusterName__contains	Free-text filter by cluster name (supports multiple values)	false	string []

			computerName	Computer name	false	string
			computerName__contains	Free-text filter by computer name (supports multiple values)	false	string []
			computerName__like	Match computer name partially (substring)	false	string
			consoleMigrationStatuses	Migration status in	false	string []
			consoleMigrationStatusesNin	Migration status nin	false	string []
			coreCount__between	Possible number of CPU cores (inclusive)	false	string
			coreCount__gt	CPU cores (more than)	false	integer
			coreCount__gte	CPU cores (more than or equal)	false	integer
			coreCount__lt	CPU cores (less than)	false	integer
			coreCount__lte	CPU cores (less than or equal)	false	integer
			cpuCount__between	Possible number of CPU cores (inclusive)	false	string
			cpuCount__gt	Number of CPUs (more than)	false	integer

			cpuCount__gte	Number of CPUs (more than or equal)	false	integer
			cpuCount__lt	Number of CPUs (less than)	false	integer
			cpuCount__lte	Number of CPUs (less than or equal)	false	integer
			cpuId__contains	Free-text filter by CPU name (supports multiple values)	false	string []
			createdAt__between	Date range for creation time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			createdAt__gt	Agents created after this timestamp	false	string
			createdAt__gte	Agents created after or at this timestamp	false	string
			createdAt__lt	Agents created before this timestamp	false	string
			createdAt__lte	Agents created before or at this timestamp	false	string
			csvFilterId	The ID of the CSV file to filter by	false	string

			decommissionedAt__between	Date range for decommission time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			decommissionedAt__gt	Agents decommissioned after this timestamp	false	string
			decommissionedAt__gte	Agents decommissioned after or at this timestamp	false	string
			decommissionedAt__lt	Agents decommissioned before this timestamp	false	string
			decommissionedAt__lte	Agents decommissioned before this timestamp	false	string
			domains	Included network domains	false	string []
			domainsNin	Not included network domains	false	string []
			encryptedApplications	Disk encryption status	false	boolean
			externalId__contains	Free-text filter by external ID (Customer ID)	false	string []
			externalIp__contains	Free-text filter by visible IP (supports	false	string []

				multiple values)		
			filteredGroupIds	List of Group IDs to filter by	false	string []
			filteredSiteIds	List of Site IDs to filter by	false	string []
			filterId	Include all Agents matching this saved filter	false	string
			firewallEnabled	The agents supports Firewall Control and it is enabled for the agent's group	false	boolean []
			gatewayIp	Gateway ip	false	string
			gcpServiceAccount__contains	Free-text filter by gcp service account (supports multiple values)	false	string []
			groupIds	List of Group IDs to filter by	false	string []
			hasContainerizedWorkload	Include only Agents protecting containerized workloads	false	boolean
			hasLocalConfiguration	Agent has a local configuration set	false	boolean
			hasTags	Include only Agents that	false	boolean

				have any tags assigned if True, or none if False		
			ids	A list of Agent IDs	false	string []
			infected	Include only Agents with at least one active threat	false	boolean
			installerTypes	Include only Agents installed with these package types	false	string []
			installerTypesNin	Exclude Agents installed with these package types	false	string []
			isActive	Include only active Agents	false	boolean
			isDecommissioned	Include active, decommissioned or both	false	boolean []
			isPendingUninstall	Include only Agents with pending uninstall requests	false	boolean
			isUninstalled	Include installed, uninstalled or both	false	boolean []
			isUpToDate	Include only Agents with updated software	false	boolean

			k8sNodeLabels__contains	Free-text filter by K8s node labels (supports multiple values)	false	string []
			k8sNodeName__contains	Free-text filter by K8s node name (supports multiple values)	false	string []
			k8sType__contains	Free-text filter by K8s type(supports multiple values)	false	string []
			k8sVersion__contains	Free-text filter by K8s version (supports multiple values)	false	string []
			lastActiveDate__between	Date range for last active date(format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			lastActiveDate__gt	Agents last active after this time	false	string
			lastActiveDate__gte	Agents last active after or at this time	false	string
			lastActiveDate__lt	Agents last active before this time	false	string
			lastActiveDate__lte	Agents last active before or at this time	false	string

			lastLoggedInUserName__contains	Free-text filter by username (supports multiple values)	false	string []
			lastSuccessfulScanDate__between	Date range for last successful full disk scan(format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			lastSuccessfulScanDate__gt	Agents last successful full disk scan after this time	false	string
			lastSuccessfulScanDate__gte	Agents last successful full disk scan after or at this time	false	string
			lastSuccessfulScanDate__lt	Agents last successful full disk scan before this time	false	string
			lastSuccessfulScanDate__lte	Agents last successful full disk scan before or at this time	false	string
			liveUpdateId__contains	Free-text filter by live update ID (supports multiple values)	false	string []
			locationEnabled	The agents supports	false	boolean []

				Location Awareness and it is enabled for the agent's group		
			locationIds	Include only Agents reporting these locations	false	string []
			locationIdsNin	Do not include only Agents reporting these locations	false	string []
			machineTypes	Included machine types	false	string []
			machineTypesNin	Not included machine types	false	string []
			migrationStatus	Migration status	false	enum
			missingPermissions	Included missing permissions	false	string []
			missingPermissionsNin	Excluded missing permissions	false	string []
			mitigationMode	Agent mitigation mode policy	false	enum
			mitigationModeSuspicious	Mitigation mode policy for suspicious activity	false	enum
			networkInterfaceGatewayMacAddress__c	Free-text filter by Gateway	false	string []

			ontains	MAC address (supports multiple values)		
			networkInterfaceInet__contains	Free-text filter by local IP (supports multiple values)	false	string []
			networkInterfacePhysical__contains	Free-text filter by MAC address (supports multiple values)	false	string []
			networkQuarantineEnabled	The agents supports Network Quarantine Control and its enabled for the agent's group	false	boolean []
			networkStatuses	Included network statuses	false	string []
			networkStatusesNin	Included network statuses	false	string []
			operationalStates	Agent operational state	false	string []
			operationalStatesNin	Do not include these Agent operational states	false	string []
			osArch	OS architecture	false	enum
			osTypes	Included OS types	false	string []

			osTypesNin	Not included OS types	false	string []
			osVersion__contains	Free-text filter by OS full name and version (supports multiple values)	false	string []
			query	A free-text search term, will match applicable attributes (sub-string match). Note: Device's physical addresses will be matched if they start with the search term only (no match if they contain the term).	false	string
			rangerStatus	[DEPRECATED] Use rangerStatuses.	false	enum
			rangerStatuses	Status of Ranger	false	string []
			rangerStatusesNin	Do not include these Ranger Statuses	false	string []
			rangerVersions	Ranger versions to include	false	string []
			rangerVersionsNin	Ranger versions not to include	false	string []

			registeredAt__between	Date range for first registration time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			registeredAt__gt	Agents registered after this time	false	string
			registeredAt__gte	Agents registered after or at this time	false	string
			registeredAt__lt	Agents registered before this time	false	string
			registeredAt__lte	Agents registered before or at this time	false	string
			remoteOpsForensicsSupported	Include only agents that has Remote Ops Forensicsfeature supported	false	boolean
			remoteProfilingStates	Agent remote profiling state	false	string []
			remoteProfilingStatesNin	Do not include these Agent remote profiling states	false	string []
			rsoLevel	Supported Remote Script Orchestration	false	enum

				level		
			scanStatus	Scan status	false	enum
			scanStatuses	Included scan statuses	false	string []
			scanStatuses Nin	Not included scan statuses	false	string []
			serialNumber __contains	Free-text filter by Serial Number (supports multiple values)	false	string []
			siteIds	List of Site IDs to filter by	false	string []
			tagsData	Filter agents by their assigned tags. Given in form of a JSON where each key represents a tag key, and each value represents a list of string values to filter by. To filter by unassigned tag values, use __nin suffix in the tag key.	false	string
			threatConten tHash	Include only Agents that have at least one threat with this content hash	false	string
			threatCreate	Agents with	false	string

			dAt__between	threats reported in a date range (format: <from_timestamp>-<to_timestamp>, inclusive)		
			threatCreatedAt__gt	Agents with threats reported after this time	false	string
			threatCreatedAt__gte	Agents with threats reported after or at this time	false	string
			threatCreatedAt__lt	Agents with threats reported before this time	false	string
			threatCreatedAt__lte	Agents with threats reported before or at this time	false	string
			threatHidden	Include only Agents with at least one hidden threat	false	boolean
			threatMitigationStatus	Include only Agents that have threats with this mitigation status	false	enum
			threatRebootRequired	Has at least one threat with at least one mitigation	false	boolean []

				action pending reboot to succeed		
			threatResolved	Include only Agents with at least one resolved threat	false	boolean
			totalMemory__between	Total memory range (GB, inclusive)	false	string
			totalMemory__gt	Memory size (MB, more than)	false	integer
			totalMemory__gte	Memory size (MB, more than or equal)	false	integer
			totalMemory__lt	Memory size (MB, less than)	false	integer
			totalMemory__lte	Memory size (MB, less than or equal)	false	integer
			updatedAt__between	Date range for update time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			updatedAt__gt	Agents updated after this timestamp	false	string
			updatedAt__gte	Agents updated after or at this timestamp	false	string
			updatedAt__lt	Agents updated	false	string

<table>
<tr><td></td><td></td><td></td><td>
<table>
<tr><td></td><td>before this timestamp</td><td></td><td></td></tr>
<tr><td>updatedAt__lte</td><td>Agents updated before or at this timestamp</td><td>false</td><td>string</td></tr>
<tr><td>userActionsNeeded</td><td>Included pending user actions</td><td>false</td><td>string []</td></tr>
<tr><td>userActionsNeededNin</td><td>Excluded pending user actions</td><td>false</td><td>string []</td></tr>
<tr><td>uuid</td><td>Agent's universally unique identifier</td><td>false</td><td>string</td></tr>
<tr><td>uuid__contains</td><td>Free-text filter by Agent UUID (supports multiple values)</td><td>false</td><td>string []</td></tr>
<tr><td>uuids</td><td>A list of included UUIDs</td><td>false</td><td>string []</td></tr>
</table>
</td></tr>
<tr><td>data</td><td>Data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>timeout</td><td>Profiling will be disabled after that many seconds</td><td>false</td><td>integer</td></tr>
</table>
</td></tr>
</table>

Stop Remote Profiling

POST /web/api/v2.1/agents/actions/stop-profiling

Use this command to stop remote profiling on Agents that match the filter.
If the command returns "Insufficient permissions", make sure you have permissions for the Account, Site, or Group and a role that allows Stop Remote Profiling (Admin or IT).

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - Insufficient permissions

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>affected</td><td>Number of entities affected by the requested operation</td><td>false</td><td>integer</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

Name	Description	Required	Value
filter	Applied filter - only matched Agents will be affected by the requested action. Leave empty to apply the action on all applicable Agents.	true	

Name	Description	Required	Value
accountIds	List of Account IDs to filter by	false	string []
activeThreats	Include Agents with this amount of active threats	false	integer
activeThreats__gt	Include Agents with at least this amount of active threats	false	integer
adComputerMember__contains	Free-text filter by Active Directory computer groups string (supports multiple values)	false	string []
adComputerName__contains	Free-text filter by Active Directory computer name string (supports multiple values)	false	string []
adComputerQuery__contains	Free-text filter by Active Directory computer name or its groups	false	string []

				(supports multiple values)		
			adQuery	An Active Directory query string	false	string
			adQuery__contains	Free-text filter by Active Directory string (supports multiple values)	false	string []
			adUserMember__contains	Free-text filter by Active Directory user groups string (supports multiple values)	false	string []
			adUserName__contains	Free-text filter by Active Directory username string (supports multiple values)	false	string []
			adUserQuery__contains	Free-text filter by Active Directory computer name or its groups (supports multiple values)	false	string []
			agentNamespa	Free-text	false	string []

			ce__contains	filter by agent namespace (supports multiple values)		
			agentPodName__contains	Free-text filter by agent pod name (supports multiple values)	false	string []
			agentVersion__between	Version range for agent version (format: <from_version>-<to_version>, inclusive)	false	string
			agentVersion__gt	Agents versions greater than given version	false	string
			agentVersion__gte	Agents versions greater than or equal to given version	false	string
			agentVersion__lt	Agents versions less than given version	false	string
			agentVersion__lte	Agents versions less than or equal to given version	false	string
			agentVersions	Agent versions to include	false	string []
			agentVersionsNin	Agent versions not	false	string []

				to include		
			appsVulnerabilityStatuses	Apps vulnerability status in	false	string []
			appsVulnerabilityStatusesNin	Apps vulnerability status nin	false	string []
			awsRole__contains	Free-text filter by aws role(supports multiple values)	false	string []
			awsSecurityGroups__contains	Free-text filter by aws securityGroups(supports multiple values)	false	string []
			awsSubnetIds__contains	Free-text filter by aws subnet ids (supports multiple values)	false	string []
			azureResourceGroup__contains	Free-text filter by azure resource group(supports multiple values)	false	string []
			cloudAccount__contains	Free-text filter by cloud account (supports multiple values)	false	string []
			cloudImage__contains	Free-text filter by cloud image (supports multiple values)	false	string []

			cloudInstanceId__contains	Free-text filter by cloud instance id(supports multiple values)	false	string []
			cloudInstanceSize__contains	Free-text filter by cloud instance size(supports multiple values)	false	string []
			cloudLocation__contains	Free-text filter by cloud location (supports multiple values)	false	string []
			cloudNetwork__contains	Free-text filter by cloud network (supports multiple values)	false	string []
			cloudProvider	Agents from which cloud provider	false	string []
			cloudProviderNin	Exclude Agents from these cloud provider	false	string []
			cloudTags__contains	Free-text filter by cloud tags (supports multiple values)	false	string []
			clusterName__contains	Free-text filter by cluster name (supports multiple values)	false	string []

			computerName	Computer name	false	string
			computerName__contains	Free-text filter by computer name (supports multiple values)	false	string []
			computerName__like	Match computer name partially (substring)	false	string
			consoleMigrationStatuses	Migration status in	false	string []
			consoleMigrationStatusesNin	Migration status nin	false	string []
			coreCount__between	Possible number of CPU cores (inclusive)	false	string
			coreCount__gt	CPU cores (more than)	false	integer
			coreCount__gte	CPU cores (more than or equal)	false	integer
			coreCount__lt	CPU cores (less than)	false	integer
			coreCount__lte	CPU cores (less than or equal)	false	integer
			cpuCount__between	Possible number of CPU cores (inclusive)	false	string
			cpuCount__gt	Number of CPUs (more than)	false	integer

			cpuCount__gte	Number of CPUs (more than or equal)	false	integer
			cpuCount__lt	Number of CPUs (less than)	false	integer
			cpuCount__lte	Number of CPUs (less than or equal)	false	integer
			cpuId__contains	Free-text filter by CPU name (supports multiple values)	false	string []
			createdAt__between	Date range for creation time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			createdAt__gt	Agents created after this timestamp	false	string
			createdAt__gte	Agents created after or at this timestamp	false	string
			createdAt__lt	Agents created before this timestamp	false	string
			createdAt__lte	Agents created before or at this timestamp	false	string
			csvFilterId	The ID of the CSV file to filter by	false	string

			decommissionedAt__between	Date range for decommission time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			decommissionedAt__gt	Agents decommissioned after this timestamp	false	string
			decommissionedAt__gte	Agents decommissioned after or at this timestamp	false	string
			decommissionedAt__lt	Agents decommissioned before this timestamp	false	string
			decommissionedAt__lte	Agents decommissioned before this timestamp	false	string
			domains	Included network domains	false	string []
			domainsNin	Not included network domains	false	string []
			encryptedApplications	Disk encryption status	false	boolean
			externalId__contains	Free-text filter by external ID (Customer ID)	false	string []
			externalIp__contains	Free-text filter by visible IP (supports	false	string []

				multiple values)		
			filteredGroupIds	List of Group IDs to filter by	false	string []
			filteredSiteIds	List of Site IDs to filter by	false	string []
			filterId	Include all Agents matching this saved filter	false	string
			firewallEnabled	The agents supports Firewall Control and it is enabled for the agent's group	false	boolean []
			gatewayIp	Gateway ip	false	string
			gcpServiceAccount__contains	Free-text filter by gcp service account (supports multiple values)	false	string []
			groupIds	List of Group IDs to filter by	false	string []
			hasContainerizedWorkload	Include only Agents protecting containerized workloads	false	boolean
			hasLocalConfiguration	Agent has a local configuration set	false	boolean
			hasTags	Include only Agents that	false	boolean

				have any tags assigned if True, or none if False		
			ids	A list of Agent IDs	false	string []
			infected	Include only Agents with at least one active threat	false	boolean
			installerTypes	Include only Agents installed with these package types	false	string []
			installerTypesNin	Exclude Agents installed with these package types	false	string []
			isActive	Include only active Agents	false	boolean
			isDecommissioned	Include active, decommissioned or both	false	boolean []
			isPendingUninstall	Include only Agents with pending uninstall requests	false	boolean
			isUninstalled	Include installed, uninstalled or both	false	boolean []
			isUpToDate	Include only Agents with updated software	false	boolean

			k8sNodeLabels__contains	Free-text filter by K8s node labels (supports multiple values)	false	string []
			k8sNodeName__contains	Free-text filter by K8s node name (supports multiple values)	false	string []
			k8sType__contains	Free-text filter by K8s type(supports multiple values)	false	string []
			k8sVersion__contains	Free-text filter by K8s version (supports multiple values)	false	string []
			lastActiveDate__between	Date range for last active date(format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			lastActiveDate__gt	Agents last active after this time	false	string
			lastActiveDate__gte	Agents last active after or at this time	false	string
			lastActiveDate__lt	Agents last active before this time	false	string
			lastActiveDate__lte	Agents last active before or at this time	false	string

			lastLoggedInUserName__contains	Free-text filter by username (supports multiple values)	false	string []
			lastSuccessfulScanDate__between	Date range for last successful full disk scan(format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			lastSuccessfulScanDate__gt	Agents last successful full disk scan after this time	false	string
			lastSuccessfulScanDate__gte	Agents last successful full disk scan after or at this time	false	string
			lastSuccessfulScanDate__lt	Agents last successful full disk scan before this time	false	string
			lastSuccessfulScanDate__lte	Agents last successful full disk scan before or at this time	false	string
			liveUpdateId__contains	Free-text filter by live update ID (supports multiple values)	false	string []
			locationEnabled	The agents supports	false	boolean []

				Location Awareness and it is enabled for the agent's group		
			locationIds	Include only Agents reporting these locations	false	string []
			locationIdsNin	Do not include only Agents reporting these locations	false	string []
			machineTypes	Included machine types	false	string []
			machineTypesNin	Not included machine types	false	string []
			migrationStatus	Migration status	false	enum
			missingPermissions	Included missing permissions	false	string []
			missingPermissionsNin	Excluded missing permissions	false	string []
			mitigationMode	Agent mitigation mode policy	false	enum
			mitigationModeSuspicious	Mitigation mode policy for suspicious activity	false	enum
			networkInterfaceGatewayMacAddress__c	Free-text filter by Gateway	false	string []

			ontains	MAC address (supports multiple values)		
			networkInterfaceInet__contains	Free-text filter by local IP (supports multiple values)	false	string []
			networkInterfacePhysical__contains	Free-text filter by MAC address (supports multiple values)	false	string []
			networkQuarantineEnabled	The agents supports Network Quarantine Control and its enabled for the agent's group	false	boolean []
			networkStatuses	Included network statuses	false	string []
			networkStatusesNin	Included network statuses	false	string []
			operationalStates	Agent operational state	false	string []
			operationalStatesNin	Do not include these Agent operational states	false	string []
			osArch	OS architecture	false	enum
			osTypes	Included OS types	false	string []

			osTypesNin	Not included OS types	false	string []
			osVersion__contains	Free-text filter by OS full name and version (supports multiple values)	false	string []
			query	A free-text search term, will match applicable attributes (sub-string match). Note: Device's physical addresses will be matched if they start with the search term only (no match if they contain the term).	false	string
			rangerStatus	[DEPRECATED] Use rangerStatuses.	false	enum
			rangerStatuses	Status of Ranger	false	string []
			rangerStatusesNin	Do not include these Ranger Statuses	false	string []
			rangerVersions	Ranger versions to include	false	string []
			rangerVersionsNin	Ranger versions not to include	false	string []

			registeredAt__between	Date range for first registration time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			registeredAt__gt	Agents registered after this time	false	string
			registeredAt__gte	Agents registered after or at this time	false	string
			registeredAt__lt	Agents registered before this time	false	string
			registeredAt__lte	Agents registered before or at this time	false	string
			remoteOpsForensicsSupported	Include only agents that has Remote Ops Forensicsfeature supported	false	boolean
			remoteProfilingStates	Agent remote profiling state	false	string []
			remoteProfilingStatesNin	Do not include these Agent remote profiling states	false	string []
			rsoLevel	Supported Remote Script Orchestration	false	enum

				level		
			scanStatus	Scan status	false	enum
			scanStatuses	Included scan statuses	false	string []
			scanStatuses Nin	Not included scan statuses	false	string []
			serialNumber __contains	Free-text filter by Serial Number (supports multiple values)	false	string []
			siteIds	List of Site IDs to filter by	false	string []
			tagsData	Filter agents by their assigned tags. Given in form of a JSON where each key represents a tag key, and each value represents a list of string values to filter by. To filter by unassigned tag values, use __nin suffix in the tag key.	false	string
			threatConten tHash	Include only Agents that have at least one threat with this content hash	false	string
			threatCreate	Agents with	false	string

			dAt__between	threats reported in a date range (format: <from_timestamp>-<to_timestamp>, inclusive)		
			threatCreatedAt__gt	Agents with threats reported after this time	false	string
			threatCreatedAt__gte	Agents with threats reported after or at this time	false	string
			threatCreatedAt__lt	Agents with threats reported before this time	false	string
			threatCreatedAt__lte	Agents with threats reported before or at this time	false	string
			threatHidden	Include only Agents with at least one hidden threat	false	boolean
			threatMitigationStatus	Include only Agents that have threats with this mitigation status	false	enum
			threatRebootRequired	Has at least one threat with at least one mitigation	false	boolean []

				action pending reboot to succeed		
			threatResolved	Include only Agents with at least one resolved threat	false	boolean
			totalMemory__between	Total memory range (GB, inclusive)	false	string
			totalMemory__gt	Memory size (MB, more than)	false	integer
			totalMemory__gte	Memory size (MB, more than or equal)	false	integer
			totalMemory__lt	Memory size (MB, less than)	false	integer
			totalMemory__lte	Memory size (MB, less than or equal)	false	integer
			updatedAt__between	Date range for update time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			updatedAt__gt	Agents updated after this timestamp	false	string
			updatedAt__gte	Agents updated after or at this timestamp	false	string
			updatedAt__lt	Agents updated	false	string

<table>
<tr><td></td><td></td><td></td><td><table>
<tr><td></td><td>before this timestamp</td><td></td><td></td></tr>
<tr><td>updatedAt__lte</td><td>Agents updated before or at this timestamp</td><td>false</td><td>string</td></tr>
<tr><td>userActionsNeeded</td><td>Included pending user actions</td><td>false</td><td>string []</td></tr>
<tr><td>userActionsNeededNin</td><td>Excluded pending user actions</td><td>false</td><td>string []</td></tr>
<tr><td>uuid</td><td>Agent's universally unique identifier</td><td>false</td><td>string</td></tr>
<tr><td>uuid__contains</td><td>Free-text filter by Agent UUID (supports multiple values)</td><td>false</td><td>string []</td></tr>
<tr><td>uuids</td><td>A list of included UUIDs</td><td>false</td><td>string []</td></tr>
</table></td></tr>
<tr><td>data</td><td>Data</td><td>false</td><td></td></tr>
</table>

Approve Stateless Upgrades

POST /web/api/v2.1/agents/actions/approve-stateless-upgrade

Approve stateless upgrade for agents

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - Insufficient permissions

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>affected</td><td>Number of entities affected by the requested operation</td><td>false</td><td>integer</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

Name	Description	Required	Value
filter	Applied filter - only matched Agents will be affected by the requested action. Leave empty to apply the action on all applicable Agents.	true	

Name	Description	Required	Value
accountIds	List of Account IDs to filter by	false	string []
activeThreats	Include Agents with this amount of active threats	false	integer
activeThreats__gt	Include Agents with at least this amount of active threats	false	integer
adComputerMember__contains	Free-text filter by Active Directory computer groups string (supports multiple values)	false	string []
adComputerName__contains	Free-text filter by Active Directory computer name string (supports multiple values)	false	string []
adComputerQuery__contains	Free-text filter by Active Directory computer name or its groups	false	string []

				(supports multiple values)		
			adQuery	An Active Directory query string	false	string
			adQuery__contains	Free-text filter by Active Directory string (supports multiple values)	false	string []
			adUserMember__contains	Free-text filter by Active Directory user groups string (supports multiple values)	false	string []
			adUserName__contains	Free-text filter by Active Directory username string (supports multiple values)	false	string []
			adUserQuery__contains	Free-text filter by Active Directory computer name or its groups (supports multiple values)	false	string []
			agentNamespa	Free-text	false	string []

			ce__contains	filter by agent namespace (supports multiple values)		
			agentPodName__contains	Free-text filter by agent pod name (supports multiple values)	false	string []
			agentVersion__between	Version range for agent version (format: <from_version>-<to_version>, inclusive)	false	string
			agentVersion__gt	Agents versions greater than given version	false	string
			agentVersion__gte	Agents versions greater than or equal to given version	false	string
			agentVersion__lt	Agents versions less than given version	false	string
			agentVersion__lte	Agents versions less than or equal to given version	false	string
			agentVersions	Agent versions to include	false	string []
			agentVersionsNin	Agent versions not	false	string []

				to include		
			appsVulnerabilityStatuses	Apps vulnerability status in	false	string []
			appsVulnerabilityStatusesNin	Apps vulnerability status nin	false	string []
			awsRole__contains	Free-text filter by aws role(supports multiple values)	false	string []
			awsSecurityGroups__contains	Free-text filter by aws securityGroups(supports multiple values)	false	string []
			awsSubnetIds__contains	Free-text filter by aws subnet ids (supports multiple values)	false	string []
			azureResourceGroup__contains	Free-text filter by azure resource group(supports multiple values)	false	string []
			cloudAccount__contains	Free-text filter by cloud account (supports multiple values)	false	string []
			cloudImage__contains	Free-text filter by cloud image (supports multiple values)	false	string []

			cloudInstanceId__contains	Free-text filter by cloud instance id(supports multiple values)	false	string []
			cloudInstanceSize__contains	Free-text filter by cloud instance size(supports multiple values)	false	string []
			cloudLocation__contains	Free-text filter by cloud location (supports multiple values)	false	string []
			cloudNetwork__contains	Free-text filter by cloud network (supports multiple values)	false	string []
			cloudProvider	Agents from which cloud provider	false	string []
			cloudProviderNin	Exclude Agents from these cloud provider	false	string []
			cloudTags__contains	Free-text filter by cloud tags (supports multiple values)	false	string []
			clusterName__contains	Free-text filter by cluster name (supports multiple values)	false	string []

			computerName	Computer name	false	string
			computerName__contains	Free-text filter by computer name (supports multiple values)	false	string []
			computerName__like	Match computer name partially (substring)	false	string
			consoleMigrationStatuses	Migration status in	false	string []
			consoleMigrationStatusesNin	Migration status nin	false	string []
			coreCount__between	Possible number of CPU cores (inclusive)	false	string
			coreCount__gt	CPU cores (more than)	false	integer
			coreCount__gte	CPU cores (more than or equal)	false	integer
			coreCount__lt	CPU cores (less than)	false	integer
			coreCount__lte	CPU cores (less than or equal)	false	integer
			cpuCount__between	Possible number of CPU cores (inclusive)	false	string
			cpuCount__gt	Number of CPUs (more than)	false	integer

			cpuCount__gte	Number of CPUs (more than or equal)	false	integer
			cpuCount__lt	Number of CPUs (less than)	false	integer
			cpuCount__lte	Number of CPUs (less than or equal)	false	integer
			cpuId__contains	Free-text filter by CPU name (supports multiple values)	false	string []
			createdAt__between	Date range for creation time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			createdAt__gt	Agents created after this timestamp	false	string
			createdAt__gte	Agents created after or at this timestamp	false	string
			createdAt__lt	Agents created before this timestamp	false	string
			createdAt__lte	Agents created before or at this timestamp	false	string
			csvFilterId	The ID of the CSV file to filter by	false	string

			decommissionedAt__between	Date range for decommission time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			decommissionedAt__gt	Agents decommissioned after this timestamp	false	string
			decommissionedAt__gte	Agents decommissioned after or at this timestamp	false	string
			decommissionedAt__lt	Agents decommissioned before this timestamp	false	string
			decommissionedAt__lte	Agents decommissioned before this timestamp	false	string
			domains	Included network domains	false	string []
			domainsNin	Not included network domains	false	string []
			encryptedApplications	Disk encryption status	false	boolean
			externalId__contains	Free-text filter by external ID (Customer ID)	false	string []
			externalIp__contains	Free-text filter by visible IP (supports	false	string []

				multiple values)		
			filteredGroupIds	List of Group IDs to filter by	false	string []
			filteredSiteIds	List of Site IDs to filter by	false	string []
			filterId	Include all Agents matching this saved filter	false	string
			firewallEnabled	The agents supports Firewall Control and it is enabled for the agent's group	false	boolean []
			gatewayIp	Gateway ip	false	string
			gcpServiceAccount__contains	Free-text filter by gcp service account (supports multiple values)	false	string []
			groupIds	List of Group IDs to filter by	false	string []
			hasContainerizedWorkload	Include only Agents protecting containerized workloads	false	boolean
			hasLocalConfiguration	Agent has a local configuration set	false	boolean
			hasTags	Include only Agents that	false	boolean

				have any tags assigned if True, or none if False		
			ids	A list of Agent IDs	false	string []
			infected	Include only Agents with at least one active threat	false	boolean
			installerTypes	Include only Agents installed with these package types	false	string []
			installerTypesNin	Exclude Agents installed with these package types	false	string []
			isActive	Include only active Agents	false	boolean
			isDecommissioned	Include active, decommissioned or both	false	boolean []
			isPendingUninstall	Include only Agents with pending uninstall requests	false	boolean
			isUninstalled	Include installed, uninstalled or both	false	boolean []
			isUpToDate	Include only Agents with updated software	false	boolean

			k8sNodeLabels__contains	Free-text filter by K8s node labels (supports multiple values)	false	string []
			k8sNodeName__contains	Free-text filter by K8s node name (supports multiple values)	false	string []
			k8sType__contains	Free-text filter by K8s type(supports multiple values)	false	string []
			k8sVersion__contains	Free-text filter by K8s version (supports multiple values)	false	string []
			lastActiveDate__between	Date range for last active date(format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			lastActiveDate__gt	Agents last active after this time	false	string
			lastActiveDate__gte	Agents last active after or at this time	false	string
			lastActiveDate__lt	Agents last active before this time	false	string
			lastActiveDate__lte	Agents last active before or at this time	false	string

			lastLoggedInUserName__contains	Free-text filter by username (supports multiple values)	false	string []
			lastSuccessfulScanDate__between	Date range for last successful full disk scan(format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			lastSuccessfulScanDate__gt	Agents last successful full disk scan after this time	false	string
			lastSuccessfulScanDate__gte	Agents last successful full disk scan after or at this time	false	string
			lastSuccessfulScanDate__lt	Agents last successful full disk scan before this time	false	string
			lastSuccessfulScanDate__lte	Agents last successful full disk scan before or at this time	false	string
			liveUpdateId__contains	Free-text filter by live update ID (supports multiple values)	false	string []
			locationEnabled	The agents supports	false	boolean []

				Location Awareness and it is enabled for the agent's group		
			locationIds	Include only Agents reporting these locations	false	string []
			locationIdsNin	Do not include only Agents reporting these locations	false	string []
			machineTypes	Included machine types	false	string []
			machineTypesNin	Not included machine types	false	string []
			migrationStatus	Migration status	false	enum
			missingPermissions	Included missing permissions	false	string []
			missingPermissionsNin	Excluded missing permissions	false	string []
			mitigationMode	Agent mitigation mode policy	false	enum
			mitigationModeSuspicious	Mitigation mode policy for suspicious activity	false	enum
			networkInterfaceGatewayMacAddress__c	Free-text filter by Gateway	false	string []

			ontains	MAC address (supports multiple values)		
			networkInterfaceInet__contains	Free-text filter by local IP (supports multiple values)	false	string []
			networkInterfacePhysical__contains	Free-text filter by MAC address (supports multiple values)	false	string []
			networkQuarantineEnabled	The agents supports Network Quarantine Control and its enabled for the agent's group	false	boolean []
			networkStatuses	Included network statuses	false	string []
			networkStatusesNin	Included network statuses	false	string []
			operationalStates	Agent operational state	false	string []
			operationalStatesNin	Do not include these Agent operational states	false	string []
			osArch	OS architecture	false	enum
			osTypes	Included OS types	false	string []

			osTypesNin	Not included OS types	false	string []
			osVersion__contains	Free-text filter by OS full name and version (supports multiple values)	false	string []
			query	A free-text search term, will match applicable attributes (sub-string match). Note: Device's physical addresses will be matched if they start with the search term only (no match if they contain the term).	false	string
			rangerStatus	[DEPRECATED] Use rangerStatuses.	false	enum
			rangerStatuses	Status of Ranger	false	string []
			rangerStatusesNin	Do not include these Ranger Statuses	false	string []
			rangerVersions	Ranger versions to include	false	string []
			rangerVersionsNin	Ranger versions not to include	false	string []

			registeredAt__between	Date range for first registration time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			registeredAt__gt	Agents registered after this time	false	string
			registeredAt__gte	Agents registered after or at this time	false	string
			registeredAt__lt	Agents registered before this time	false	string
			registeredAt__lte	Agents registered before or at this time	false	string
			remoteOpsForensicsSupported	Include only agents that has Remote Ops Forensicsfeature supported	false	boolean
			remoteProfilingStates	Agent remote profiling state	false	string []
			remoteProfilingStatesNin	Do not include these Agent remote profiling states	false	string []
			rsoLevel	Supported Remote Script Orchestration	false	enum

				level		
			scanStatus	Scan status	false	enum
			scanStatuses	Included scan statuses	false	string []
			scanStatuses Nin	Not included scan statuses	false	string []
			serialNumber __contains	Free-text filter by Serial Number (supports multiple values)	false	string []
			siteIds	List of Site IDs to filter by	false	string []
			tagsData	Filter agents by their assigned tags. Given in form of a JSON where each key represents a tag key, and each value represents a list of string values to filter by. To filter by unassigned tag values, use __nin suffix in the tag key.	false	string
			threatConten tHash	Include only Agents that have at least one threat with this content hash	false	string
			threatCreate	Agents with	false	string

			dAt__between	threats reported in a date range (format: <from_timestamp>-<to_timestamp>, inclusive)		
			threatCreatedAt__gt	Agents with threats reported after this time	false	string
			threatCreatedAt__gte	Agents with threats reported after or at this time	false	string
			threatCreatedAt__lt	Agents with threats reported before this time	false	string
			threatCreatedAt__lte	Agents with threats reported before or at this time	false	string
			threatHidden	Include only Agents with at least one hidden threat	false	boolean
			threatMitigationStatus	Include only Agents that have threats with this mitigation status	false	enum
			threatRebootRequired	Has at least one threat with at least one mitigation	false	boolean []

				action pending reboot to succeed		
			threatResolved	Include only Agents with at least one resolved threat	false	boolean
			totalMemory__between	Total memory range (GB, inclusive)	false	string
			totalMemory__gt	Memory size (MB, more than)	false	integer
			totalMemory__gte	Memory size (MB, more than or equal)	false	integer
			totalMemory__lt	Memory size (MB, less than)	false	integer
			totalMemory__lte	Memory size (MB, less than or equal)	false	integer
			updatedAt__between	Date range for update time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			updatedAt__gt	Agents updated after this timestamp	false	string
			updatedAt__gte	Agents updated after or at this timestamp	false	string
			updatedAt__lt	Agents updated	false	string

			before this timestamp		
			updatedAt__lte	Agents updated before or at this timestamp	false	string
			userActionsNeeded	Included pending user actions	false	string []
			userActionsNeededNin	Excluded pending user actions	false	string []
			uuid	Agent's universally unique identifier	false	string
			uuid__contains	Free-text filter by Agent UUID (supports multiple values)	false	string []
			uuids	A list of included UUIDs	false	string []
data	Data	false	Name	Description	Required	Value
			expiration	Number of days users are authorized to upgrade Agents	true	integer

Manage endpoint tags: add, remove, override

POST /web/api/v2.1/agents/actions/manage-tags

Override forces the new key and value to be added to the endpoints. If you use add to add a key when that key already exists with a different value, it will not take effect.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>affected</td><td>Number of entities affected by the requested operation</td><td>false</td><td>integer</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>filter</td><td>Applied filter - only matched Agents will be affected by the requested action. Leave empty to apply the action on all applicable Agents.</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>activeThreats</td><td>Include Agents with this amount of active threats</td><td>false</td><td>integer</td></tr>
<tr><td>activeThreats__gt</td><td>Include Agents with at least this amount of active threats</td><td>false</td><td>integer</td></tr>
<tr><td>adComputerMember__contains</td><td>Free-text filter by Active Directory computer groups string (supports multiple values)</td><td>false</td><td>string []</td></tr>
<tr><td>adComputerName__contains</td><td>Free-text filter by Active Directory computer name string (supports multiple values)</td><td>false</td><td>string []</td></tr>
<tr><td>adComputerQuery__contains</td><td>Free-text filter by Active Directory computer name or its groups</td><td>false</td><td>string []</td></tr>
</table>
</td></tr>
</table>

				(supports multiple values)		
			adQuery	An Active Directory query string	false	string
			adQuery__contains	Free-text filter by Active Directory string (supports multiple values)	false	string []
			adUserMember__contains	Free-text filter by Active Directory user groups string (supports multiple values)	false	string []
			adUserName__contains	Free-text filter by Active Directory username string (supports multiple values)	false	string []
			adUserQuery__contains	Free-text filter by Active Directory computer name or its groups (supports multiple values)	false	string []
			agentNamespa	Free-text	false	string []

			ce__contains	filter by agent namespace (supports multiple values)		
			agentPodName__contains	Free-text filter by agent pod name (supports multiple values)	false	string []
			agentVersion__between	Version range for agent version (format: <from_version>-<to_version>, inclusive)	false	string
			agentVersion__gt	Agents versions greater than given version	false	string
			agentVersion__gte	Agents versions greater than or equal to given version	false	string
			agentVersion__lt	Agents versions less than given version	false	string
			agentVersion__lte	Agents versions less than or equal to given version	false	string
			agentVersions	Agent versions to include	false	string []
			agentVersionsNin	Agent versions not	false	string []

				to include		
			appsVulnerabilityStatuses	Apps vulnerability status in	false	string []
			appsVulnerabilityStatusesNin	Apps vulnerability status nin	false	string []
			awsRole__contains	Free-text filter by aws role(supports multiple values)	false	string []
			awsSecurityGroups__contains	Free-text filter by aws securityGroups(supports multiple values)	false	string []
			awsSubnetIds__contains	Free-text filter by aws subnet ids (supports multiple values)	false	string []
			azureResourceGroup__contains	Free-text filter by azure resource group(supports multiple values)	false	string []
			cloudAccount__contains	Free-text filter by cloud account (supports multiple values)	false	string []
			cloudImage__contains	Free-text filter by cloud image (supports multiple values)	false	string []

			cloudInstanceId__contains	Free-text filter by cloud instance id(supports multiple values)	false	string []
			cloudInstanceSize__contains	Free-text filter by cloud instance size(supports multiple values)	false	string []
			cloudLocation__contains	Free-text filter by cloud location (supports multiple values)	false	string []
			cloudNetwork__contains	Free-text filter by cloud network (supports multiple values)	false	string []
			cloudProvider	Agents from which cloud provider	false	string []
			cloudProviderNin	Exclude Agents from these cloud provider	false	string []
			cloudTags__contains	Free-text filter by cloud tags (supports multiple values)	false	string []
			clusterName__contains	Free-text filter by cluster name (supports multiple values)	false	string []

			computerName	Computer name	false	string
			computerName__contains	Free-text filter by computer name (supports multiple values)	false	string []
			computerName__like	Match computer name partially (substring)	false	string
			consoleMigrationStatuses	Migration status in	false	string []
			consoleMigrationStatusesNin	Migration status nin	false	string []
			coreCount__between	Possible number of CPU cores (inclusive)	false	string
			coreCount__gt	CPU cores (more than)	false	integer
			coreCount__gte	CPU cores (more than or equal)	false	integer
			coreCount__lt	CPU cores (less than)	false	integer
			coreCount__lte	CPU cores (less than or equal)	false	integer
			cpuCount__between	Possible number of CPU cores (inclusive)	false	string
			cpuCount__gt	Number of CPUs (more than)	false	integer

			cpuCount__gte	Number of CPUs (more than or equal)	false	integer
			cpuCount__lt	Number of CPUs (less than)	false	integer
			cpuCount__lte	Number of CPUs (less than or equal)	false	integer
			cpuId__contains	Free-text filter by CPU name (supports multiple values)	false	string []
			createdAt__between	Date range for creation time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			createdAt__gt	Agents created after this timestamp	false	string
			createdAt__gte	Agents created after or at this timestamp	false	string
			createdAt__lt	Agents created before this timestamp	false	string
			createdAt__lte	Agents created before or at this timestamp	false	string
			csvFilterId	The ID of the CSV file to filter by	false	string

			decommissionedAt__between	Date range for decommission time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			decommissionedAt__gt	Agents decommissioned after this timestamp	false	string
			decommissionedAt__gte	Agents decommissioned after or at this timestamp	false	string
			decommissionedAt__lt	Agents decommissioned before this timestamp	false	string
			decommissionedAt__lte	Agents decommissioned before this timestamp	false	string
			domains	Included network domains	false	string []
			domainsNin	Not included network domains	false	string []
			encryptedApplications	Disk encryption status	false	boolean
			externalId__contains	Free-text filter by external ID (Customer ID)	false	string []
			externalIp__contains	Free-text filter by visible IP (supports	false	string []

				multiple values)		
			filteredGroupIds	List of Group IDs to filter by	false	string []
			filteredSiteIds	List of Site IDs to filter by	false	string []
			filterId	Include all Agents matching this saved filter	false	string
			firewallEnabled	The agents supports Firewall Control and it is enabled for the agent's group	false	boolean []
			gatewayIp	Gateway ip	false	string
			gcpServiceAccount__contains	Free-text filter by gcp service account (supports multiple values)	false	string []
			groupIds	List of Group IDs to filter by	false	string []
			hasContainerizedWorkload	Include only Agents protecting containerized workloads	false	boolean
			hasLocalConfiguration	Agent has a local configuration set	false	boolean
			hasTags	Include only Agents that	false	boolean

				have any tags assigned if True, or none if False		
			ids	A list of Agent IDs	false	string []
			infected	Include only Agents with at least one active threat	false	boolean
			installerTypes	Include only Agents installed with these package types	false	string []
			installerTypesNin	Exclude Agents installed with these package types	false	string []
			isActive	Include only active Agents	false	boolean
			isDecommissioned	Include active, decommissioned or both	false	boolean []
			isPendingUninstall	Include only Agents with pending uninstall requests	false	boolean
			isUninstalled	Include installed, uninstalled or both	false	boolean []
			isUpToDate	Include only Agents with updated software	false	boolean

			k8sNodeLabels__contains	Free-text filter by K8s node labels (supports multiple values)	false	string []
			k8sNodeName__contains	Free-text filter by K8s node name (supports multiple values)	false	string []
			k8sType__contains	Free-text filter by K8s type(supports multiple values)	false	string []
			k8sVersion__contains	Free-text filter by K8s version (supports multiple values)	false	string []
			lastActiveDate__between	Date range for last active date(format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			lastActiveDate__gt	Agents last active after this time	false	string
			lastActiveDate__gte	Agents last active after or at this time	false	string
			lastActiveDate__lt	Agents last active before this time	false	string
			lastActiveDate__lte	Agents last active before or at this time	false	string

			lastLoggedInUserName__contains	Free-text filter by username (supports multiple values)	false	string []
			lastSuccessfulScanDate__between	Date range for last successful full disk scan(format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			lastSuccessfulScanDate__gt	Agents last successful full disk scan after this time	false	string
			lastSuccessfulScanDate__gte	Agents last successful full disk scan after or at this time	false	string
			lastSuccessfulScanDate__lt	Agents last successful full disk scan before this time	false	string
			lastSuccessfulScanDate__lte	Agents last successful full disk scan before or at this time	false	string
			liveUpdateId__contains	Free-text filter by live update ID (supports multiple values)	false	string []
			locationEnabled	The agents supports	false	boolean []

				Location Awareness and it is enabled for the agent's group		
			locationIds	Include only Agents reporting these locations	false	string []
			locationIdsNin	Do not include only Agents reporting these locations	false	string []
			machineTypes	Included machine types	false	string []
			machineTypesNin	Not included machine types	false	string []
			migrationStatus	Migration status	false	enum
			missingPermissions	Included missing permissions	false	string []
			missingPermissionsNin	Excluded missing permissions	false	string []
			mitigationMode	Agent mitigation mode policy	false	enum
			mitigationModeSuspicious	Mitigation mode policy for suspicious activity	false	enum
			networkInterfaceGatewayMacAddress__c	Free-text filter by Gateway	false	string []

			ontains	MAC address (supports multiple values)		
			networkInterfaceInet__contains	Free-text filter by local IP (supports multiple values)	false	string []
			networkInterfacePhysical__contains	Free-text filter by MAC address (supports multiple values)	false	string []
			networkQuarantineEnabled	The agents supports Network Quarantine Control and its enabled for the agent's group	false	boolean []
			networkStatuses	Included network statuses	false	string []
			networkStatusesNin	Included network statuses	false	string []
			operationalStates	Agent operational state	false	string []
			operationalStatesNin	Do not include these Agent operational states	false	string []
			osArch	OS architecture	false	enum
			osTypes	Included OS types	false	string []

			osTypesNin	Not included OS types	false	string []
			osVersion__contains	Free-text filter by OS full name and version (supports multiple values)	false	string []
			query	A free-text search term, will match applicable attributes (sub-string match). Note: Device's physical addresses will be matched if they start with the search term only (no match if they contain the term).	false	string
			rangerStatus	[DEPRECATED] Use rangerStatuses.	false	enum
			rangerStatuses	Status of Ranger	false	string []
			rangerStatusesNin	Do not include these Ranger Statuses	false	string []
			rangerVersions	Ranger versions to include	false	string []
			rangerVersionsNin	Ranger versions not to include	false	string []

			registeredAt__between	Date range for first registration time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			registeredAt__gt	Agents registered after this time	false	string
			registeredAt__gte	Agents registered after or at this time	false	string
			registeredAt__lt	Agents registered before this time	false	string
			registeredAt__lte	Agents registered before or at this time	false	string
			remoteOpsForensicsSupported	Include only agents that has Remote Ops Forensicsfeature supported	false	boolean
			remoteProfilingStates	Agent remote profiling state	false	string []
			remoteProfilingStatesNin	Do not include these Agent remote profiling states	false	string []
			rsoLevel	Supported Remote Script Orchestration	false	enum

				level		
			scanStatus	Scan status	false	enum
			scanStatuses	Included scan statuses	false	string []
			scanStatuses Nin	Not included scan statuses	false	string []
			serialNumber __contains	Free-text filter by Serial Number (supports multiple values)	false	string []
			siteIds	List of Site IDs to filter by	false	string []
			tagsData	Filter agents by their assigned tags. Given in form of a JSON where each key represents a tag key, and each value represents a list of string values to filter by. To filter by unassigned tag values, use __nin suffix in the tag key.	false	string
			threatConten tHash	Include only Agents that have at least one threat with this content hash	false	string
			threatCreate	Agents with	false	string

			dAt__between	threats reported in a date range (format: <from_timestamp>-<to_timestamp>, inclusive)		
			threatCreatedAt__gt	Agents with threats reported after this time	false	string
			threatCreatedAt__gte	Agents with threats reported after or at this time	false	string
			threatCreatedAt__lt	Agents with threats reported before this time	false	string
			threatCreatedAt__lte	Agents with threats reported before or at this time	false	string
			threatHidden	Include only Agents with at least one hidden threat	false	boolean
			threatMitigationStatus	Include only Agents that have threats with this mitigation status	false	enum
			threatRebootRequired	Has at least one threat with at least one mitigation	false	boolean []

				action pending reboot to succeed		
			threatResolved	Include only Agents with at least one resolved threat	false	boolean
			totalMemory__between	Total memory range (GB, inclusive)	false	string
			totalMemory__gt	Memory size (MB, more than)	false	integer
			totalMemory__gte	Memory size (MB, more than or equal)	false	integer
			totalMemory__lt	Memory size (MB, less than)	false	integer
			totalMemory__lte	Memory size (MB, less than or equal)	false	integer
			updatedAt__between	Date range for update time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			updatedAt__gt	Agents updated after this timestamp	false	string
			updatedAt__gte	Agents updated after or at this timestamp	false	string
			updatedAt__lt	Agents updated	false	string

			before this timestamp		
			updatedAt__lte	Agents updated before or at this timestamp	false	string
			userActionsNeeded	Included pending user actions	false	string []
			userActionsNeededNin	Excluded pending user actions	false	string []
			uuid	Agent's universally unique identifier	false	string
			uuid__contains	Free-text filter by Agent UUID (supports multiple values)	false	string []
			uuids	A list of included UUIDs	false	string []
data	Tags to attach	false	Name	Description	Required	Value
			operation	Operation to perform on tag	false	enum
			tagId	Tag ID	false	string

Agent Support Actions

Clear Remote Shell

POST /web/api/v2.1/agents/actions/clear-remote-shell-session

Remote Shell is a powerful way to respond remotely to events on endpoints. It lets you open full shell capabilities - PowerShell on Windows and Bash on macOS and Linux.
For best practices, a Remote Shell session can be terminated in many ways: from the UI, from Agent timeouts, from endpoint or connections issues, and so on. If a shell closes at the same time that an Agent goes offline, Remote Shell status is incorrect on the Management.
Use this command to clear the "open shell" flags on the Management.
The IT user role does not have permissions to run this command.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>affected</td><td>Number of entities affected by the requested operation</td><td>false</td><td>integer</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>filter</td><td>Applied filter - only matched Agents will be affected by the requested action. Leave empty to apply the action on all applicable Agents.</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>activeThreats</td><td>Include Agents with this amount of active threats</td><td>false</td><td>integer</td></tr>
<tr><td>activeThreats__gt</td><td>Include Agents with at least this amount of active threats</td><td>false</td><td>integer</td></tr>
<tr><td>adComputerMember__contains</td><td>Free-text filter by Active Directory computer groups string (supports multiple values)</td><td>false</td><td>string []</td></tr>
<tr><td>adComputerName__contains</td><td>Free-text filter by Active Directory computer name string (supports multiple values)</td><td>false</td><td>string []</td></tr>
<tr><td>adComputerQuery__contains</td><td>Free-text filter by Active Directory computer name or its groups</td><td>false</td><td>string []</td></tr>
</table>
</td></tr>
</table>

				(supports multiple values)		
			adQuery	An Active Directory query string	false	string
			adQuery__contains	Free-text filter by Active Directory string (supports multiple values)	false	string []
			adUserMember__contains	Free-text filter by Active Directory user groups string (supports multiple values)	false	string []
			adUserName__contains	Free-text filter by Active Directory username string (supports multiple values)	false	string []
			adUserQuery__contains	Free-text filter by Active Directory computer name or its groups (supports multiple values)	false	string []
			agentNamespa	Free-text	false	string []

			ce__contains	filter by agent namespace (supports multiple values)		
			agentPodName__contains	Free-text filter by agent pod name (supports multiple values)	false	string []
			agentVersion__between	Version range for agent version (format: <from_version>-<to_version>, inclusive)	false	string
			agentVersion__gt	Agents versions greater than given version	false	string
			agentVersion__gte	Agents versions greater than or equal to given version	false	string
			agentVersion__lt	Agents versions less than given version	false	string
			agentVersion__lte	Agents versions less than or equal to given version	false	string
			agentVersions	Agent versions to include	false	string []
			agentVersionsNin	Agent versions not	false	string []

				to include		
			appsVulnerabilityStatuses	Apps vulnerability status in	false	string []
			appsVulnerabilityStatusesNin	Apps vulnerability status nin	false	string []
			awsRole__contains	Free-text filter by aws role(supports multiple values)	false	string []
			awsSecurityGroups__contains	Free-text filter by aws securityGroups(supports multiple values)	false	string []
			awsSubnetIds__contains	Free-text filter by aws subnet ids (supports multiple values)	false	string []
			azureResourceGroup__contains	Free-text filter by azure resource group(supports multiple values)	false	string []
			cloudAccount__contains	Free-text filter by cloud account (supports multiple values)	false	string []
			cloudImage__contains	Free-text filter by cloud image (supports multiple values)	false	string []

			cloudInstanceId__contains	Free-text filter by cloud instance id(supports multiple values)	false	string []
			cloudInstanceSize__contains	Free-text filter by cloud instance size(supports multiple values)	false	string []
			cloudLocation__contains	Free-text filter by cloud location (supports multiple values)	false	string []
			cloudNetwork__contains	Free-text filter by cloud network (supports multiple values)	false	string []
			cloudProvider	Agents from which cloud provider	false	string []
			cloudProviderNin	Exclude Agents from these cloud provider	false	string []
			cloudTags__contains	Free-text filter by cloud tags (supports multiple values)	false	string []
			clusterName__contains	Free-text filter by cluster name (supports multiple values)	false	string []

			computerName	Computer name	false	string
			computerName__contains	Free-text filter by computer name (supports multiple values)	false	string []
			computerName__like	Match computer name partially (substring)	false	string
			consoleMigrationStatuses	Migration status in	false	string []
			consoleMigrationStatusesNin	Migration status nin	false	string []
			coreCount__between	Possible number of CPU cores (inclusive)	false	string
			coreCount__gt	CPU cores (more than)	false	integer
			coreCount__gte	CPU cores (more than or equal)	false	integer
			coreCount__lt	CPU cores (less than)	false	integer
			coreCount__lte	CPU cores (less than or equal)	false	integer
			cpuCount__between	Possible number of CPU cores (inclusive)	false	string
			cpuCount__gt	Number of CPUs (more than)	false	integer

			cpuCount__gte	Number of CPUs (more than or equal)	false	integer
			cpuCount__lt	Number of CPUs (less than)	false	integer
			cpuCount__lte	Number of CPUs (less than or equal)	false	integer
			cpuId__contains	Free-text filter by CPU name (supports multiple values)	false	string []
			createdAt__between	Date range for creation time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			createdAt__gt	Agents created after this timestamp	false	string
			createdAt__gte	Agents created after or at this timestamp	false	string
			createdAt__lt	Agents created before this timestamp	false	string
			createdAt__lte	Agents created before or at this timestamp	false	string
			csvFilterId	The ID of the CSV file to filter by	false	string

			decommissionedAt__between	Date range for decommission time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			decommissionedAt__gt	Agents decommissioned after this timestamp	false	string
			decommissionedAt__gte	Agents decommissioned after or at this timestamp	false	string
			decommissionedAt__lt	Agents decommissioned before this timestamp	false	string
			decommissionedAt__lte	Agents decommissioned before this timestamp	false	string
			domains	Included network domains	false	string []
			domainsNin	Not included network domains	false	string []
			encryptedApplications	Disk encryption status	false	boolean
			externalId__contains	Free-text filter by external ID (Customer ID)	false	string []
			externalIp__contains	Free-text filter by visible IP (supports	false	string []

				multiple values)		
			filteredGroupIds	List of Group IDs to filter by	false	string []
			filteredSiteIds	List of Site IDs to filter by	false	string []
			filterId	Include all Agents matching this saved filter	false	string
			firewallEnabled	The agents supports Firewall Control and it is enabled for the agent's group	false	boolean []
			gatewayIp	Gateway ip	false	string
			gcpServiceAccount__contains	Free-text filter by gcp service account (supports multiple values)	false	string []
			groupIds	List of Group IDs to filter by	false	string []
			hasContainerizedWorkload	Include only Agents protecting containerized workloads	false	boolean
			hasLocalConfiguration	Agent has a local configuration set	false	boolean
			hasTags	Include only Agents that	false	boolean

				have any tags assigned if True, or none if False		
			ids	A list of Agent IDs	false	string []
			infected	Include only Agents with at least one active threat	false	boolean
			installerTypes	Include only Agents installed with these package types	false	string []
			installerTypesNin	Exclude Agents installed with these package types	false	string []
			isActive	Include only active Agents	false	boolean
			isDecommissioned	Include active, decommissioned or both	false	boolean []
			isPendingUninstall	Include only Agents with pending uninstall requests	false	boolean
			isUninstalled	Include installed, uninstalled or both	false	boolean []
			isUpToDate	Include only Agents with updated software	false	boolean

			k8sNodeLabels__contains	Free-text filter by K8s node labels (supports multiple values)	false	string []
			k8sNodeName__contains	Free-text filter by K8s node name (supports multiple values)	false	string []
			k8sType__contains	Free-text filter by K8s type(supports multiple values)	false	string []
			k8sVersion__contains	Free-text filter by K8s version (supports multiple values)	false	string []
			lastActiveDate__between	Date range for last active date(format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			lastActiveDate__gt	Agents last active after this time	false	string
			lastActiveDate__gte	Agents last active after or at this time	false	string
			lastActiveDate__lt	Agents last active before this time	false	string
			lastActiveDate__lte	Agents last active before or at this time	false	string

			lastLoggedInUserName__contains	Free-text filter by username (supports multiple values)	false	string []
			lastSuccessfulScanDate__between	Date range for last successful full disk scan(format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			lastSuccessfulScanDate__gt	Agents last successful full disk scan after this time	false	string
			lastSuccessfulScanDate__gte	Agents last successful full disk scan after or at this time	false	string
			lastSuccessfulScanDate__lt	Agents last successful full disk scan before this time	false	string
			lastSuccessfulScanDate__lte	Agents last successful full disk scan before or at this time	false	string
			liveUpdateId__contains	Free-text filter by live update ID (supports multiple values)	false	string []
			locationEnabled	The agents supports	false	boolean []

				Location Awareness and it is enabled for the agent's group		
			locationIds	Include only Agents reporting these locations	false	string []
			locationIdsNin	Do not include only Agents reporting these locations	false	string []
			machineTypes	Included machine types	false	string []
			machineTypesNin	Not included machine types	false	string []
			migrationStatus	Migration status	false	enum
			missingPermissions	Included missing permissions	false	string []
			missingPermissionsNin	Excluded missing permissions	false	string []
			mitigationMode	Agent mitigation mode policy	false	enum
			mitigationModeSuspicious	Mitigation mode policy for suspicious activity	false	enum
			networkInterfaceGatewayMacAddress__c	Free-text filter by Gateway	false	string []

			ontains	MAC address (supports multiple values)		
			networkInterfaceInet__contains	Free-text filter by local IP (supports multiple values)	false	string []
			networkInterfacePhysical__contains	Free-text filter by MAC address (supports multiple values)	false	string []
			networkQuarantineEnabled	The agents supports Network Quarantine Control and its enabled for the agent's group	false	boolean []
			networkStatuses	Included network statuses	false	string []
			networkStatusesNin	Included network statuses	false	string []
			operationalStates	Agent operational state	false	string []
			operationalStatesNin	Do not include these Agent operational states	false	string []
			osArch	OS architecture	false	enum
			osTypes	Included OS types	false	string []

			osTypesNin	Not included OS types	false	string []
			osVersion__contains	Free-text filter by OS full name and version (supports multiple values)	false	string []
			query	A free-text search term, will match applicable attributes (sub-string match). Note: Device's physical addresses will be matched if they start with the search term only (no match if they contain the term).	false	string
			rangerStatus	[DEPRECATED] Use rangerStatuses.	false	enum
			rangerStatuses	Status of Ranger	false	string []
			rangerStatusesNin	Do not include these Ranger Statuses	false	string []
			rangerVersions	Ranger versions to include	false	string []
			rangerVersionsNin	Ranger versions not to include	false	string []

			registeredAt__between	Date range for first registration time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			registeredAt__gt	Agents registered after this time	false	string
			registeredAt__gte	Agents registered after or at this time	false	string
			registeredAt__lt	Agents registered before this time	false	string
			registeredAt__lte	Agents registered before or at this time	false	string
			remoteOpsForensicsSupported	Include only agents that has Remote Ops Forensicsfeature supported	false	boolean
			remoteProfilingStates	Agent remote profiling state	false	string []
			remoteProfilingStatesNin	Do not include these Agent remote profiling states	false	string []
			rsoLevel	Supported Remote Script Orchestration	false	enum

				level		
			scanStatus	Scan status	false	enum
			scanStatuses	Included scan statuses	false	string []
			scanStatuses Nin	Not included scan statuses	false	string []
			serialNumber __contains	Free-text filter by Serial Number (supports multiple values)	false	string []
			siteIds	List of Site IDs to filter by	false	string []
			tagsData	Filter agents by their assigned tags. Given in form of a JSON where each key represents a tag key, and each value represents a list of string values to filter by. To filter by unassigned tag values, use __nin suffix in the tag key.	false	string
			threatConten tHash	Include only Agents that have at least one threat with this content hash	false	string
			threatCreate	Agents with	false	string

			dAt__between	threats reported in a date range (format: <from_timestamp>-<to_timestamp>, inclusive)		
			threatCreatedAt__gt	Agents with threats reported after this time	false	string
			threatCreatedAt__gte	Agents with threats reported after or at this time	false	string
			threatCreatedAt__lt	Agents with threats reported before this time	false	string
			threatCreatedAt__lte	Agents with threats reported before or at this time	false	string
			threatHidden	Include only Agents with at least one hidden threat	false	boolean
			threatMitigationStatus	Include only Agents that have threats with this mitigation status	false	enum
			threatRebootRequired	Has at least one threat with at least one mitigation	false	boolean []

				action pending reboot to succeed		
			threatResolved	Include only Agents with at least one resolved threat	false	boolean
			totalMemory__between	Total memory range (GB, inclusive)	false	string
			totalMemory__gt	Memory size (MB, more than)	false	integer
			totalMemory__gte	Memory size (MB, more than or equal)	false	integer
			totalMemory__lt	Memory size (MB, less than)	false	integer
			totalMemory__lte	Memory size (MB, less than or equal)	false	integer
			updatedAt__between	Date range for update time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			updatedAt__gt	Agents updated after this timestamp	false	string
			updatedAt__gte	Agents updated after or at this timestamp	false	string
			updatedAt__lt	Agents updated	false	string

<table>
<tr><td></td><td></td><td></td><td><table>
<tr><td></td><td>before this timestamp</td><td></td><td></td></tr>
<tr><td>updatedAt__lte</td><td>Agents updated before or at this timestamp</td><td>false</td><td>string</td></tr>
<tr><td>userActionsNeeded</td><td>Included pending user actions</td><td>false</td><td>string []</td></tr>
<tr><td>userActionsNeededNin</td><td>Excluded pending user actions</td><td>false</td><td>string []</td></tr>
<tr><td>uuid</td><td>Agent's universally unique identifier</td><td>false</td><td>string</td></tr>
<tr><td>uuid__contains</td><td>Free-text filter by Agent UUID (supports multiple values)</td><td>false</td><td>string []</td></tr>
<tr><td>uuids</td><td>A list of included UUIDs</td><td>false</td><td>string []</td></tr>
</table></td></tr>
<tr><td>data</td><td>Data</td><td>false</td><td></td></tr>
</table>

Agents

Get Agents

GET /web/api/v2.1/agents

Get the Agents, and their data, that match the filter. This command gives the Agent ID, which you can use in other commands. To save the list and data to a CSV file, use "export/agents".

Parameters

accountids	optional	List of Account IDs to filter by. Example: "225494730938493804,225494730938493915".
activethreats	optional	Include Agents with this amount of active threats. Example: "3".
activethreats__gt	optional	Include Agents with at least this amount of active threats. Example: "5".
adcomputermember__contains	optional	Free-text filter by Active Directory computer groups string (supports multiple values). Example: "DC=sentinelone".
adcomputername__contains	optional	Free-text filter by Active Directory computer name string (supports multiple values). Example: "DC=sentinelone".
adcomputerquery__contains	optional	Free-text filter by Active Directory computer name or its groups (supports multiple values). Example: "DC=sentinelone,Windows".
adquery	optional	An Active Directory query string. Example: "CN=Managers,DC=sentinelone,DC=com".
adquery__contains	optional	Free-text filter by Active Directory string (supports multiple values). Example: "DC=sentinelone".
adusermember__contains	optional	Free-text filter by Active Directory user groups string (supports multiple values). Example: "DC=sentinelone".
adusername__contains	optional	Free-text filter by Active Directory username string (supports multiple values). Example: "DC=sentinelone".
aduserquery__contains	optional	Free-text filter by Active Directory computer name or its groups (supports multiple values). Example: "DC=sentinelone,John".
agentnamespace__contains	optional	Free-text filter by agent namespace (supports multiple values)

agentpodname__contains	optional	Free-text filter by agent pod name (supports multiple values)
agentversion__between	optional	Version range for agent version (format: <from_version>-<to_version>, inclusive). Example: "2.0.0.0-2.1.5.144".
agentversion__gt	optional	Agents versions greater than given version. Example: "2.5.1.1320".
agentversion__gte	optional	Agents versions greater than or equal to given version. Example: "2.5.1.1320".
agentversion__lt	optional	Agents versions less than given version. Example: "2.5.1.1320".
agentversion__lte	optional	Agents versions less than or equal to given version. Example: "2.5.1.1320".
agentversions	optional	Agent versions to include. Example: "2.0.0.0,2.1.5.144".
agentversionsnin	optional	Agent versions not to include. Example: "2.0.0.0,2.1.5.144".
appsvulnerabilitystatuses	optional	Apps vulnerability status in. Example: "patch_required".
appsvulnerabilitystatusesnin	optional	Apps vulnerability status nin. Example: "patch_required".
awsrole__contains	optional	Free-text filter by aws role(supports multiple values)
awssecuritygroups__contains	optional	Free-text filter by aws securityGroups(supports multiple values)
awssubnetids__contains	optional	Free-text filter by aws subnet ids (supports multiple values)
azureresourcegroup__contains	optional	Free-text filter by azure resource group(supports multiple values)
cloudaccount__contains	optional	Free-text filter by cloud account (supports multiple values)
cloudimage__contains	optional	Free-text filter by cloud image (supports multiple values)
cloudinstanceid__contains	optional	Free-text filter by cloud instance id(supports multiple values)
cloudinstancesize__contains	optional	Free-text filter by cloud instance size(supports multiple values)
cloudlocation__contains	optional	Free-text filter by cloud location (supports multiple values)
cloudnetwork__contains	optional	Free-text filter by cloud network (supports multiple values)

cloudprovider	optional	Agents from which cloud provider
cloudprovidernin	optional	Exclude Agents from these cloud provider
cloudtags__contains	optional	Free-text filter by cloud tags (supports multiple values)
clustername__contains	optional	Free-text filter by cluster name (supports multiple values)
computername	optional	Computer name. Example: "My Office Desktop".
computername__contains	optional	Free-text filter by computer name (supports multiple values). Example: "john-office,WIN".
computername__like	optional	Match computer name partially (substring). Example: "Lab1".
consolemigrationstatuses	optional	Migration status in. Example: "N/A".
consolemigrationstatusesnin	optional	Migration status nin. Example: "N/A".
corecount__between	optional	Possible number of CPU cores (inclusive). Example: "2-8".
corecount__gt	optional	CPU cores (more than)
corecount__gte	optional	CPU cores (more than or equal)
corecount__lt	optional	CPU cores (less than)
corecount__lte	optional	CPU cores (less than or equal)
countonly	optional	If true, only total number of items will be returned, without any of the actual objects.
cpucount__between	optional	Possible number of CPU cores (inclusive). Example: "2-8".
cpucount__gt	optional	Number of CPUs (more than)
cpucount__gte	optional	Number of CPUs (more than or equal)
cpucount__lt	optional	Number of CPUs (less than)
cpucount__lte	optional	Number of CPUs (less than or equal)
cpuid__contains	optional	Free-text filter by CPU name (supports multiple values). Example: "Intel,AMD".
createdat__between	optional	Date range for creation time (format: <from_timestamp>-<to_timestamp>, inclusive). Example: "1514978890136-1514978650130".
createdat__gt	optional	Agents created after this timestamp. Example: "2018-02-27T04:49:26.257525Z".
createdat__gte	optional	Agents created after or at this timestamp. Example:

		"2018-02-27T04:49:26.257525Z".
createdat__lt	optional	Agents created before this timestamp. Example: "2018-02-27T04:49:26.257525Z".
createdat__lte	optional	Agents created before or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
csvfilterid	optional	The ID of the CSV file to filter by. Example: "225494730938493804".
cursor	optional	Cursor position returned by the last request. Use to iterate over more than 1000 items. Example: "YWdlbnRfaWQ6NTgwMjkzODE=".
decommissionedat__between	optional	Date range for decommission time (format: <from_timestamp>-<to_timestamp>, inclusive). Example: "1514978890136-1514978650130".
decommissionedat__gt	optional	Agents decommissioned after this timestamp. Example: "2018-02-27T04:49:26.257525Z".
decommissionedat__gte	optional	Agents decommissioned after or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
decommissionedat__lt	optional	Agents decommissioned before this timestamp. Example: "2018-02-27T04:49:26.257525Z".
decommissionedat__lte	optional	Agents decommissioned before this timestamp. Example: "2018-02-27T04:49:26.257525Z".
domains	optional	Included network domains. Example: "mybusiness.net,workgroup".
domainsnin	optional	Not included network domains. Example: "mybusiness.net,workgroup".
encryptedapplications	optional	Disk encryption status
externalid__contains	optional	Free-text filter by external ID (Customer ID). Example: "Tag#1 - monitoring,Performance machine".
externalip__contains	optional	Free-text filter by visible IP (supports multiple values). Example: "205,127.0".
filteredgroupids	optional	List of Group IDs to filter by. Example: "225494730938493804,225494730938493915".
filteredsiteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".
filterid	optional	Include all Agents matching this saved filter. Example: "225494730938493804".

firewallenabled	optional	The agents supports Firewall Control and it is enabled for the agent's group
gatewayip	optional	Gateway ip. Example: "192.168.0.1".
gcpserviceaccount__contains	optional	Free-text filter by gcp service account (supports multiple values)
groupids	optional	List of Group IDs to filter by. Example: "225494730938493804,225494730938493915".
hascontainerizedworkload	optional	Include only Agents protecting containerized workloads
haslocalconfiguration	optional	Agent has a local configuration set
hastags	optional	Include only Agents that have any tags assigned if True, or none if False
ids	optional	A list of Agent IDs. Example: "225494730938493804,225494730938493915".
infected	optional	Include only Agents with at least one active threat
installertypes	optional	Include only Agents installed with these package types. Example: ".msi".
installertypesnin	optional	Exclude Agents installed with these package types. Example: ".msi".
isactive	optional	Include only active Agents
isdecommissioned	optional	Include active, decommissioned or both. Example: "True,False".
ispendinguninstall	optional	Include only Agents with pending uninstall requests
isuninstalled	optional	Include installed, uninstalled or both. Example: "True,False".
isuptodate	optional	Include only Agents with updated software
k8snodelabels__contains	optional	Free-text filter by K8s node labels (supports multiple values)
k8snodename__contains	optional	Free-text filter by K8s node name (supports multiple values)
k8stype__contains	optional	Free-text filter by K8s type(supports multiple values)
k8sversion__contains	optional	Free-text filter by K8s version (supports multiple values)
lastactivedate__between	optional	Date range for last active date(format: <from_timestamp>-<to_timestamp>, inclusive). Example: "1514978764288-1514978999999".
lastactivedate__gt	optional	Agents last active after this time. Example:

		"2018-02-27T04:49:26.257525Z".
lastactivedate__gte	optional	Agents last active after or at this time. Example: "2018-02-27T04:49:26.257525Z".
lastactivedate__lt	optional	Agents last active before this time. Example: "2018-02-27T04:49:26.257525Z".
lastactivedate__lte	optional	Agents last active before or at this time. Example: "2018-02-27T04:49:26.257525Z".
lastloggedinusername__contains	optional	Free-text filter by username (supports multiple values). Example: "admin,johnd1".
lastsuccessfulscandate__between	optional	Date range for last successful full disk scan(format: <from_timestamp>-<to_timestamp>, inclusive). Example: "1514978764288-1514978999999".
lastsuccessfulscandate__gt	optional	Agents last successful full disk scan after this time. Example: "2018-02-27T04:49:26.257525Z".
lastsuccessfulscandate__gte	optional	Agents last successful full disk scan after or at this time. Example: "2018-02-27T04:49:26.257525Z".
lastsuccessfulscandate__lt	optional	Agents last successful full disk scan before this time. Example: "2018-02-27T04:49:26.257525Z".
lastsuccessfulscandate__lte	optional	Agents last successful full disk scan before or at this time. Example: "2018-02-27T04:49:26.257525Z".
limit	optional	Limit number of returned items (1-1000). Example: "10".
liveupdateid__contains	optional	Free-text filter by live update ID (supports multiple values)
locationenabled	optional	The agents supports Location Awareness and it is enabled for the agent's group
locationids	optional	Include only Agents reporting these locations. Example: "225494730938493804,225494730938493915".
locationidsnin	optional	Do not include only Agents reporting these locations. Example: "225494730938493804,225494730938493915".
machinetypes	optional	Included machine types. Example: "laptop,desktop".
machinetypesnin	optional	Not included machine types. Example: "laptop,desktop".
migrationstatus	optional	Migration status. Example: "N/A".
missingpermissions	optional	Included missing permissions. Example: "user_action_needed_bluetooth_per,user_action_needed_fda_helper".

missingpermissionsnin	optional	Excluded missing permissions. Example: "user_action_needed_bluetooth_per,user_action_needed_fda_helper".
mitigationmode	optional	Agent mitigation mode policy. Example: "detect".
mitigationmodesuspicious	optional	Mitigation mode policy for suspicious activity. Example: "detect".
networkinterfacegatewaymacaddress__contains	optional	Free-text filter by Gateway MAC address (supports multiple values). Example: "aa:0f,:41:".
networkinterfaceinet__contains	optional	Free-text filter by local IP (supports multiple values). Example: "192,10.0.0".
networkinterfacephysical__contains	optional	Free-text filter by MAC address (supports multiple values). Example: "aa:0f,:41:".
networkquarantineenabled	optional	The agents supports Network Quarantine Control and its enabled for the agent's group
networkstatuses	optional	Included network statuses. Example: "connected,connecting".
networkstatusesnin	optional	Included network statuses. Example: "connected,connecting".
operationalstates	optional	Agent operational state
operationalstatesnin	optional	Do not include these Agent operational states
osarch	optional	OS architecture. Example: "32 bit".
ostypes	optional	Included OS types. Example: "macos".
ostypesnin	optional	Not included OS types. Example: "macos".
osversion__contains	optional	Free-text filter by OS full name and version (supports multiple values). Example: "Service Pack 1".
query	optional	A free-text search term, will match applicable attributes (sub-string match). Note: Device's physical addresses will be matched if they start with the search term only (no match if they contain the term). Example: "Linux".
rangerstatus	optional	[DEPRECATED] Use rangerStatuses. Example: "NotApplicable".
rangerstatuses	optional	Status of Ranger. Example: "NotApplicable".
rangerstatusesnin	optional	Do not include these Ranger Statuses. Example: "NotApplicable".
rangerversions	optional	Ranger versions to include. Example: "2.0.0.0,2.1.5.144".
rangerversionsnin	optional	Ranger versions not to include. Example: "2.0.0.0,2.1.5.144".

registeredat__between	optional	Date range for first registration time (format: <from_timestamp>-<to_timestamp>, inclusive). Example: "1514978764288-1514978999999".
registeredat__gt	optional	Agents registered after this time. Example: "2018-02-27T04:49:26.257525Z".
registeredat__gte	optional	Agents registered after or at this time. Example: "2018-02-27T04:49:26.257525Z".
registeredat__lt	optional	Agents registered before this time. Example: "2018-02-27T04:49:26.257525Z".
registeredat__lte	optional	Agents registered before or at this time. Example: "2018-02-27T04:49:26.257525Z".
remoteopsforensicssupported	optional	Include only agents that has Remote Ops Forensicsfeature supported
remoteprofilingstates	optional	Agent remote profiling state
remoteprofilingstatesnin	optional	Do not include these Agent remote profiling states
rsolevel	optional	Supported Remote Script Orchestration level. Example: "none".
scanstatus	optional	Scan status. Example: "none".
scanstatuses	optional	Included scan statuses. Example: "started,aborted".
scanstatusesnin	optional	Not included scan statuses. Example: "started,aborted".
serialnumber__contains	optional	Free-text filter by Serial Number (supports multiple values)
siteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".
skip	optional	Skip first number of items (0-1000). To iterate over more than 1000 items, use "cursor". Example: "150".
skipcount	optional	If true, total number of items will not be calculated, which speeds up execution time.
sortby	optional	The column to sort the results by. Example: "id".
sortorder	optional	Sort direction. Example: "asc".
tagsdata	optional	Filter agents by their assigned tags. Given in form of a JSON where each key represents a tag key, and each value represents a list of string values to filter by. To filter by unassigned tag values, use __nin suffix in the tag key. Example: "{"key1": ["value1_1", "value1_2"],

		"key2__nin": ["value2"]}".
threatcontenthash	optional	Include only Agents that have at least one threat with this content hash. Example: "cf23df2207d99a74fbe169e3eba035e633b65d94".
threatcreatedat__between	optional	Agents with threats reported in a date range (format: <from_timestamp>-<to_timestamp>, inclusive). Example: "1514978764288-1514978999999".
threatcreatedat__gt	optional	Agents with threats reported after this time. Example: "2018-02-27T04:49:26.257525Z".
threatcreatedat__gte	optional	Agents with threats reported after or at this time. Example: "2018-02-27T04:49:26.257525Z".
threatcreatedat__lt	optional	Agents with threats reported before this time. Example: "2018-02-27T04:49:26.257525Z".
threatcreatedat__lte	optional	Agents with threats reported before or at this time. Example: "2018-02-27T04:49:26.257525Z".
threathidden	optional	Include only Agents with at least one hidden threat
threatmitigationstatus	optional	Include only Agents that have threats with this mitigation status. Example: "mitigated".
threatrebootrequired	optional	Has at least one threat with at least one mitigation action pending reboot to succeed
threatresolved	optional	Include only Agents with at least one resolved threat
totalmemory__between	optional	Total memory range (GB, inclusive). Example: "4-8".
totalmemory__gt	optional	Memory size (MB, more than)
totalmemory__gte	optional	Memory size (MB, more than or equal)
totalmemory__lt	optional	Memory size (MB, less than)
totalmemory__lte	optional	Memory size (MB, less than or equal)
updatedat__between	optional	Date range for update time (format: <from_timestamp>-<to_timestamp>, inclusive). Example: "1514978890136-1514978650130".
updatedat__gt	optional	Agents updated after this timestamp. Example: "2018-02-27T04:49:26.257525Z".
updatedat__gte	optional	Agents updated after or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
updatedat__lt	optional	Agents updated before this timestamp. Example:

		"2018-02-27T04:49:26.257525Z".
updatedat__lte	optional	Agents updated before or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
useractionsneeded	optional	Included pending user actions. Example: "reboot_needed,upgrade_needed".
useractionsneedednin	optional	Excluded pending user actions. Example: "reboot_needed,upgrade_needed".
uuid	optional	Agent's universally unique identifier. Example: "ff819e70af13be381993075eb0ce5f2f6de05be2".
uuid__contains	optional	Free-text filter by Agent UUID (supports multiple values). Example: "e92-01928,b055".
uuids	optional	A list of included UUIDs. Example: "ff819e70af13be381993075eb0ce5f2f6de05b11,ff819e70af13be381993075eb0ce5f2f6de05c22".

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
pagination	Pagination information	true	

Name	Description	Required	Value
totalItems	Total number of items found matching your query	true	integer
nextCursor	Pass this value as "cursor" on your next request, to get the next	false	string

				page of results (Will be "null" when last page reached)		
data	Response data	false	Name	Description	Required	Value
			accountId	A reference to the containing account	false	string
			accountName	Name of the containing account	false	string
			activeDirectory	Active Directory data	false	

Name	Description	Required	Value
computerDistinguishedName	Computer distinguished name	false	string
computerMemberOf	Computer member of	false	string []
lastUserDistinguishedName	Last user distinguished name	false	string
lastUserMemberOf	Last user member of	false	string []
mail	Mail	false	string
userPrincipalName	User principal name	false	string

activeThreats	Current number of active threats	false	integer
agentVersion	Agent version	false	string
allowRemoteShell	Agent is capable and policy enabled for remote shell	false	boolean
appsVulnerabi	Apps	false	enum

			lityStatus	vulnerability status		
			cloudProviders	Cloud providers for this agent	false	object
			computerName	Computer name	false	string
			consoleMigrationStatus	What step the agent is at in the process of migrating to another console, if any	false	enum
			containerizedWorkloadCounts	Containerized workload counts	false	

Name	Description	Required	Value
containersCount	Number of containers the agent is currently protecting	false	integer
podsCount	Number of K8s pods the agent is currently protecting	false	integer
tasksCount	Number of tasks the agent is currently protecting	false	integer

coreCount	CPU cores	false	integer
cpuCount	Number of CPUs	false	integer
cpuId	CPU model	false	string
createdAt	Created at	false	string
detectionState	Detection State	false	string
domain	Network	false	string

				domain		
			encryptedApplications	Disk encryption status	false	boolean
			externalId	External id set by customer	false	string
			externalIp	External IPv4 address	false	string
			firewallEnabled	Firewall enabled	false	boolean
			firstFullModeTime	Date of the first time the Agent moved to full or slim detection modes	false	string
			fullDiskScanLastUpdatedAt	Last time scan status was updated	false	string
			groupId	A reference to the containing network group	false	string
			groupIp	IP Address subnet	false	string
			groupName	Name of the containing network group	false	string
			groupUpdatedAt	Group updated at	false	string
			hasContainerizedWorkload	Indicates whether the agent protects containerized workload at the moment	false	boolean

			id	Agent ID	false	string
			infected	Indicates if the Agent has active threats	false	boolean
			inRemoteShellSession	Is the Agent in a remote shell session	false	boolean
			installerType	Installer package type (file extension)	false	enum
			isActive	Indicates if the agent was recently active	false	boolean
			isDecommissioned	Is Agent decommissioned	false	boolean
			isPendingUninstall	Agent with a pending uninstall request	false	boolean
			isUninstalled	Indicates if Agent was removed from the device	false	boolean
			isUpToDate	Indicates if the agent version is up to date	false	boolean
			lastActiveDate	Last active date	false	string
			lastIpToMgmt	The last ip used to connect to the Management console	false	string
			lastLoggedInUserName	Last logged in user name	false	string

			lastSuccessfulScanDate	Last successful full disc scan time	false	string
			licenseKey	License key	false	string
			locationEnabled	Location enabled	false	boolean
			locations	A list of locations reported by the Agent	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>id</td><td>Location ID</td><td>false</td><td>string</td></tr><tr><td>name</td><td>Location name</td><td>false</td><td>string</td></tr><tr><td>scope</td><td>Location scope</td><td>false</td><td>enum</td></tr></table>
			locationType	Reported location type	false	enum
			machineType	Machine type	false	enum
			missingPermissions	A list of missing permissions. List items possible values: "user_action_needed_fda, user_action_needed_rs_fda, user_action_needed_fda_helper, user_action_needed_fda_sentineld, user_action_needed_bluetooth_per, user_action_needed_network, user_action_needed_notifications".	false	string []

			mitigationMode	Agent mitigation mode policy	false	enum
			mitigationModeSuspicious	Mitigation mode policy for suspicious activity	false	enum
			modelName	Device model	false	string
			networkInterfaces	Device's network interfaces	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>gatewayIp</td><td>The default gateway ip</td><td>false</td><td>string</td></tr><tr><td>gatewayMacAddress</td><td>The default gateway mac address</td><td>false</td><td>string</td></tr><tr><td>id</td><td>Id</td><td>false</td><td>string</td></tr><tr><td>inet</td><td>IPv4 addresses</td><td>false</td><td>string []</td></tr><tr><td>inet6</td><td>IPv6 addresses</td><td>false</td><td>string []</td></tr><tr><td>name</td><td>Name</td><td>false</td><td>string</td></tr><tr><td>physical</td><td>Interface's MAC address</td><td>false</td><td>string</td></tr></table>
			networkQuarantineEnabled	Network quarantine enabled	false	boolean
			networkStatus	Agent's network connectivity status	false	enum
			operationalState	Agent operational state	false	string
			operationalStateExpiration	Agent operational state expiration	false	string
			osArch	Os arch	false	enum
			osName	Os name	false	string

			osRevision	Os revision	false	string
			osStartTime	Last boot time	false	string
			osType	OS type	false	enum
			osUsername	Os username	false	string
			policyUpdatedAt	Policy updated at	false	string
			proxyStates	Proxy state information	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>console</td><td>Connected to Management Console using a proxy</td><td>false</td><td>boolean</td></tr><tr><td>deepVisibility</td><td>Connected to Deep Visibility using a proxy</td><td>false</td><td>boolean</td></tr></table>
			rangerStatus	Is Agent disabled as a Ranger	false	enum
			rangerVersion	The version of Ranger	false	string
			registeredAt	Time of first registration to management console (similar to createdAt)	false	string
			remoteProfilingState	Agent remote profiling state	false	string
			remoteProfilingStateExpiration	Agent remote profiling state expiration inseconds	false	string
			scanAbortedAt	Abort time of last scan (If applicable)	false	string
			scanFinishedAt	Finish time of last scan (If	false	string

				applicable)		
			scanStartedAt	Start time of last scan	false	string
			scanStatus	Last scan status	false	enum
			serialNumber	Serial Number of the endpoint	false	string
			showAlertIcon	Show alert icon in agent view and details	false	boolean
			siteId	A reference to the containing site	false	string
			siteName	Name of the containing site	false	string
			storageName	Storage Name	false	string
			storageType	Storage Type	false	string
			tags	Agent's attached tags	false	

Name	Description	Required	Value
sentinelone	SentinelOne tags section	false	

Name	Description	Required	Value
assignedAt	when tag assigned to the agent	false	string
assignedBy	full user name who assigned the tag to the agent	false	string
assignedById	user ID who assigned the tag to the agent	false	string
id	Tag ID	false	string
key	Tag key	false	string

										value	Tag value	false	string
			threatRebootRequired	Has at least one threat with at least one mitigation action that is pending reboot to succeed	false	boolean							
			totalMemory	Memory size (MB)	false	integer							
			updatedAt	Updated at	false	string							
			userActionsNeeded	A list of pending user actions. List items possible values: "none, user_action_needed, reboot_needed, upgrade_needed, incompatible_os, unprotected, rebootless_without_dynamic_detection, extended_exclusions_partially_accepted, reboot_required, pending_deprecation, ne_not_running, ne_cf_not_active".	false	string []							

			uuid	Agent's universally unique identifier	false	string
errors	Errors	false	array			

Count Agents

GET /web/api/v2.1/agents/count

Get the count of Agents that match a filter. This command is useful to run before you run other commands. You will be able to manage Agent maintenance better if you know how many Agents will get a command that takes time (such as Update Software).

Parameters

accountids	optional	List of Account IDs to filter by. Example: "225494730938493804,225494730938493915".
activethreats	optional	Include Agents with this amount of active threats. Example: "3".
activethreats__gt	optional	Include Agents with at least this amount of active threats. Example: "5".
adcomputermember__contains	optional	Free-text filter by Active Directory computer groups string (supports multiple values). Example: "DC=sentinelone".
adcomputername__contains	optional	Free-text filter by Active Directory computer name string (supports multiple values). Example: "DC=sentinelone".
adcomputerquery__contains	optional	Free-text filter by Active Directory computer name or its groups (supports multiple values). Example: "DC=sentinelone,Windows".
adquery	optional	An Active Directory query string. Example: "CN=Managers,DC=sentinelone,DC=com".
adquery__contains	optional	Free-text filter by Active Directory string (supports multiple values). Example: "DC=sentinelone".
adusermember__contains	optional	Free-text filter by Active Directory user groups string (supports multiple values). Example: "DC=sentinelone".
adusername__contains	optional	Free-text filter by Active Directory username string (supports multiple values). Example: "DC=sentinelone".
aduserquery__contains	optional	Free-text filter by Active Directory computer name or its groups (supports multiple values). Example: "DC=sentinelone,John".
agentnamespace__contains	optional	Free-text filter by agent namespace (supports multiple values)
agentpodname__contains	optional	Free-text filter by agent pod name (supports multiple values)
agentversion__between	optional	Version range for agent version (format: <from_version>-<to_version>, inclusive). Example: "2.0.0.0-2.1.5.144".

agentversion__gt	optional	Agents versions greater than given version. Example: "2.5.1.1320".
agentversion__gte	optional	Agents versions greater than or equal to given version. Example: "2.5.1.1320".
agentversion__lt	optional	Agents versions less than given version. Example: "2.5.1.1320".
agentversion__lte	optional	Agents versions less than or equal to given version. Example: "2.5.1.1320".
agentversions	optional	Agent versions to include. Example: "2.0.0.0,2.1.5.144".
agentversionsnin	optional	Agent versions not to include. Example: "2.0.0.0,2.1.5.144".
appsvulnerabilitystatuses	optional	Apps vulnerability status in. Example: "patch_required".
appsvulnerabilitystatusesnin	optional	Apps vulnerability status nin. Example: "patch_required".
awsrole__contains	optional	Free-text filter by aws role(supports multiple values)
awssecuritygroups__contains	optional	Free-text filter by aws securityGroups(supports multiple values)
awssubnetids__contains	optional	Free-text filter by aws subnet ids (supports multiple values)
azureresourcegroup__contains	optional	Free-text filter by azure resource group(supports multiple values)
cloudaccount__contains	optional	Free-text filter by cloud account (supports multiple values)
cloudimage__contains	optional	Free-text filter by cloud image (supports multiple values)
cloudinstanceid__contains	optional	Free-text filter by cloud instance id(supports multiple values)
cloudinstancesize__contains	optional	Free-text filter by cloud instance size(supports multiple values)
cloudlocation__contains	optional	Free-text filter by cloud location (supports multiple values)
cloudnetwork__contains	optional	Free-text filter by cloud network (supports multiple values)
cloudprovider	optional	Agents from which cloud provider
cloudprovidernin	optional	Exclude Agents from these cloud provider
cloudtags__contains	optional	Free-text filter by cloud tags (supports multiple values)

clustername__contains	optional	Free-text filter by cluster name (supports multiple values)
computername	optional	Computer name. Example: "My Office Desktop".
computername__contains	optional	Free-text filter by computer name (supports multiple values). Example: "john-office,WIN".
computername__like	optional	Match computer name partially (substring). Example: "Lab1".
consolemigrationstatuses	optional	Migration status in. Example: "N/A".
consolemigrationstatusesnin	optional	Migration status nin. Example: "N/A".
corecount__between	optional	Possible number of CPU cores (inclusive). Example: "2-8".
corecount__gt	optional	CPU cores (more than)
corecount__gte	optional	CPU cores (more than or equal)
corecount__lt	optional	CPU cores (less than)
corecount__lte	optional	CPU cores (less than or equal)
cpucount__between	optional	Possible number of CPU cores (inclusive). Example: "2-8".
cpucount__gt	optional	Number of CPUs (more than)
cpucount__gte	optional	Number of CPUs (more than or equal)
cpucount__lt	optional	Number of CPUs (less than)
cpucount__lte	optional	Number of CPUs (less than or equal)
cpuid__contains	optional	Free-text filter by CPU name (supports multiple values). Example: "Intel,AMD".
createdat__between	optional	Date range for creation time (format: <from_timestamp>-<to_timestamp>, inclusive). Example: "1514978890136-1514978650130".
createdat__gt	optional	Agents created after this timestamp. Example: "2018-02-27T04:49:26.257525Z".
createdat__gte	optional	Agents created after or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
createdat__lt	optional	Agents created before this timestamp. Example: "2018-02-27T04:49:26.257525Z".
createdat__lte	optional	Agents created before or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
csvfilterid	optional	The ID of the CSV file to filter by. Example:

		"225494730938493804".
decommissionedat__between	optional	Date range for decommission time (format: <from_timestamp>-<to_timestamp>, inclusive). Example: "1514978890136-1514978650130".
decommissionedat__gt	optional	Agents decommissioned after this timestamp. Example: "2018-02-27T04:49:26.257525Z".
decommissionedat__gte	optional	Agents decommissioned after or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
decommissionedat__lt	optional	Agents decommissioned before this timestamp. Example: "2018-02-27T04:49:26.257525Z".
decommissionedat__lte	optional	Agents decommissioned before this timestamp. Example: "2018-02-27T04:49:26.257525Z".
domains	optional	Included network domains. Example: "mybusiness.net,workgroup".
domainsnin	optional	Not included network domains. Example: "mybusiness.net,workgroup".
encryptedapplications	optional	Disk encryption status
externalid__contains	optional	Free-text filter by external ID (Customer ID). Example: "Tag#1 - monitoring,Performance machine".
externalip__contains	optional	Free-text filter by visible IP (supports multiple values). Example: "205,127.0".
filteredgroupids	optional	List of Group IDs to filter by. Example: "225494730938493804,225494730938493915".
filteredsiteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".
filterid	optional	Include all Agents matching this saved filter. Example: "225494730938493804".
firewallenabled	optional	The agents supports Firewall Control and it is enabled for the agent's group
gatewayip	optional	Gateway ip. Example: "192.168.0.1".
gcpserviceaccount__contains	optional	Free-text filter by gcp service account (supports multiple values)
groupids	optional	List of Group IDs to filter by. Example: "225494730938493804,225494730938493915".
hascontainerizedwork	optional	Include only Agents protecting containerized workloads

load		
haslocalconfiguration	optional	Agent has a local configuration set
hastags	optional	Include only Agents that have any tags assigned if True, or none if False
ids	optional	A list of Agent IDs. Example: "225494730938493804,225494730938493915".
infected	optional	Include only Agents with at least one active threat
installertypes	optional	Include only Agents installed with these package types. Example: ".msi".
installertypesnin	optional	Exclude Agents installed with these package types. Example: ".msi".
isactive	optional	Include only active Agents
isdecommissioned	optional	Include active, decommissioned or both. Example: "True,False".
ispendinguninstall	optional	Include only Agents with pending uninstall requests
isuninstalled	optional	Include installed, uninstalled or both. Example: "True,False".
isuptodate	optional	Include only Agents with updated software
k8snodelabels__contains	optional	Free-text filter by K8s node labels (supports multiple values)
k8snodename__contains	optional	Free-text filter by K8s node name (supports multiple values)
k8stype__contains	optional	Free-text filter by K8s type(supports multiple values)
k8sversion__contains	optional	Free-text filter by K8s version (supports multiple values)
lastactivedate__between	optional	Date range for last active date(format: <from_timestamp>-<to_timestamp>, inclusive). Example: "1514978764288-1514978999999".
lastactivedate__gt	optional	Agents last active after this time. Example: "2018-02-27T04:49:26.257525Z".
lastactivedate__gte	optional	Agents last active after or at this time. Example: "2018-02-27T04:49:26.257525Z".
lastactivedate__lt	optional	Agents last active before this time. Example: "2018-02-27T04:49:26.257525Z".
lastactivedate__lte	optional	Agents last active before or at this time. Example: "2018-02-27T04:49:26.257525Z".
lastloggedinusername_	optional	Free-text filter by username (supports multiple values). Example:

_contains		"admin,johnd1".
lastsuccessfulscandate__between	optional	Date range for last successful full disk scan(format: <from_timestamp>-<to_timestamp>, inclusive). Example: "1514978764288-1514978999999".
lastsuccessfulscandate__gt	optional	Agents last successful full disk scan after this time. Example: "2018-02-27T04:49:26.257525Z".
lastsuccessfulscandate__gte	optional	Agents last successful full disk scan after or at this time. Example: "2018-02-27T04:49:26.257525Z".
lastsuccessfulscandate__lt	optional	Agents last successful full disk scan before this time. Example: "2018-02-27T04:49:26.257525Z".
lastsuccessfulscandate__lte	optional	Agents last successful full disk scan before or at this time. Example: "2018-02-27T04:49:26.257525Z".
liveupdateid__contains	optional	Free-text filter by live update ID (supports multiple values)
locationenabled	optional	The agents supports Location Awareness and it is enabled for the agent's group
locationids	optional	Include only Agents reporting these locations. Example: "225494730938493804,225494730938493915".
locationidsnin	optional	Do not include only Agents reporting these locations. Example: "225494730938493804,225494730938493915".
machinetypes	optional	Included machine types. Example: "laptop,desktop".
machinetypesnin	optional	Not included machine types. Example: "laptop,desktop".
migrationstatus	optional	Migration status. Example: "N/A".
missingpermissions	optional	Included missing permissions. Example: "user_action_needed_bluetooth_per,user_action_needed_fda_helper".
missingpermissionsnin	optional	Excluded missing permissions. Example: "user_action_needed_bluetooth_per,user_action_needed_fda_helper".
mitigationmode	optional	Agent mitigation mode policy. Example: "detect".
mitigationmodesuspicious	optional	Mitigation mode policy for suspicious activity. Example: "detect".
networkinterfacegatewaymacaddress__contains	optional	Free-text filter by Gateway MAC address (supports multiple values). Example: "aa:0f,:41:".

networkinterfaceinet__contains	optional	Free-text filter by local IP (supports multiple values). Example: "192,10.0.0".
networkinterfacephysical__contains	optional	Free-text filter by MAC address (supports multiple values). Example: "aa:0f,:41:".
networkquarantineenabled	optional	The agents supports Network Quarantine Control and its enabled for the agent's group
networkstatuses	optional	Included network statuses. Example: "connected,connecting".
networkstatusesnin	optional	Included network statuses. Example: "connected,connecting".
operationalstates	optional	Agent operational state
operationalstatesnin	optional	Do not include these Agent operational states
osarch	optional	OS architecture. Example: "32 bit".
ostypes	optional	Included OS types. Example: "macos".
ostypesnin	optional	Not included OS types. Example: "macos".
osversion__contains	optional	Free-text filter by OS full name and version (supports multiple values). Example: "Service Pack 1".
query	optional	A free-text search term, will match applicable attributes (sub-string match). Note: Device's physical addresses will be matched if they start with the search term only (no match if they contain the term). Example: "Linux".
rangerstatus	optional	[DEPRECATED] Use rangerStatuses. Example: "NotApplicable".
rangerstatuses	optional	Status of Ranger. Example: "NotApplicable".
rangerstatusesnin	optional	Do not include these Ranger Statuses. Example: "NotApplicable".
rangerversions	optional	Ranger versions to include. Example: "2.0.0.0,2.1.5.144".
rangerversionsnin	optional	Ranger versions not to include. Example: "2.0.0.0,2.1.5.144".
registeredat__between	optional	Date range for first registration time (format: <from_timestamp>-<to_timestamp>, inclusive). Example: "1514978764288-1514978999999".
registeredat__gt	optional	Agents registered after this time. Example: "2018-02-27T04:49:26.257525Z".
registeredat__gte	optional	Agents registered after or at this time. Example: "2018-02-27T04:49:26.257525Z".
registeredat__lt	optional	Agents registered before this time. Example: "2018-02-27T04:49:26.257525Z".

registeredat__lte	optional	Agents registered before or at this time. Example: "2018-02-27T04:49:26.257525Z".
remoteopsforensicssupported	optional	Include only agents that has Remote Ops Forensicsfeature supported
remoteprofilingstates	optional	Agent remote profiling state
remoteprofilingstatesnin	optional	Do not include these Agent remote profiling states
rsolevel	optional	Supported Remote Script Orchestration level. Example: "none".
scanstatus	optional	Scan status. Example: "none".
scanstatuses	optional	Included scan statuses. Example: "started,aborted".
scanstatusesnin	optional	Not included scan statuses. Example: "started,aborted".
serialnumber__contains	optional	Free-text filter by Serial Number (supports multiple values)
siteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".
tagsdata	optional	Filter agents by their assigned tags. Given in form of a JSON where each key represents a tag key, and each value represents a list of string values to filter by. To filter by unassigned tag values, use __nin suffix in the tag key. Example: "{"key1": ["value1_1", "value1_2"], "key2__nin": ["value2"]}".
threatcontenthash	optional	Include only Agents that have at least one threat with this content hash. Example: "cf23df2207d99a74fbe169e3eba035e633b65d94".
threatcreatedat__between	optional	Agents with threats reported in a date range (format: <from_timestamp>-<to_timestamp>, inclusive). Example: "1514978764288-1514978999999".
threatcreatedat__gt	optional	Agents with threats reported after this time. Example: "2018-02-27T04:49:26.257525Z".
threatcreatedat__gte	optional	Agents with threats reported after or at this time. Example: "2018-02-27T04:49:26.257525Z".
threatcreatedat__lt	optional	Agents with threats reported before this time. Example: "2018-02-27T04:49:26.257525Z".
threatcreatedat__lte	optional	Agents with threats reported before or at this time. Example: "2018-02-27T04:49:26.257525Z".
threathidden	optional	Include only Agents with at least one hidden threat

threatmitigationstatus	optional	Include only Agents that have threats with this mitigation status. Example: "mitigated".
threatrebootrequired	optional	Has at least one threat with at least one mitigation action pending reboot to succeed
threatresolved	optional	Include only Agents with at least one resolved threat
totalmemory__between	optional	Total memory range (GB, inclusive). Example: "4-8".
totalmemory__gt	optional	Memory size (MB, more than)
totalmemory__gte	optional	Memory size (MB, more than or equal)
totalmemory__lt	optional	Memory size (MB, less than)
totalmemory__lte	optional	Memory size (MB, less than or equal)
updatedat__between	optional	Date range for update time (format: <from_timestamp>-<to_timestamp>, inclusive). Example: "1514978890136-1514978650130".
updatedat__gt	optional	Agents updated after this timestamp. Example: "2018-02-27T04:49:26.257525Z".
updatedat__gte	optional	Agents updated after or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
updatedat__lt	optional	Agents updated before this timestamp. Example: "2018-02-27T04:49:26.257525Z".
updatedat__lte	optional	Agents updated before or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
useractionsneeded	optional	Included pending user actions. Example: "reboot_needed,upgrade_needed".
useractionsneedednin	optional	Excluded pending user actions. Example: "reboot_needed,upgrade_needed".
uuid	optional	Agent's universally unique identifier. Example: "ff819e70af13be381993075eb0ce5f2f6de05be2".
uuid__contains	optional	Free-text filter by Agent UUID (supports multiple values). Example: "e92-01928,b055".
uuids	optional	A list of included UUIDs. Example: "ff819e70af13be381993075eb0ce5f2f6de05b11,ff819e70af13be381993075eb0ce5f2f6de05c22".

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>total</td><td>Number of Agents matching the input filter</td><td>false</td><td>integer</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Get Passphrase

GET /web/api/v2.1/agents/passphrases

Show the passphrase for the Agents that match the filter. This is an important command. You need the passphrase for most SentinelCtl commands and for different API commands.

Parameters

accountids	optional	List of Account IDs to filter by. Example: "225494730938493804,225494730938493915".
activethreats	optional	Include Agents with this amount of active threats. Example: "3".
activethreats__gt	optional	Include Agents with at least this amount of active threats. Example: "5".
adcomputermember__contains	optional	Free-text filter by Active Directory computer groups string (supports multiple values). Example: "DC=sentinelone".
adcomputername__contains	optional	Free-text filter by Active Directory computer name string (supports multiple values). Example: "DC=sentinelone".
adcomputerquery__contains	optional	Free-text filter by Active Directory computer name or its groups (supports multiple values). Example: "DC=sentinelone,Windows".
adquery	optional	An Active Directory query string. Example: "CN=Managers,DC=sentinelone,DC=com".
adquery__contains	optional	Free-text filter by Active Directory string (supports multiple values). Example: "DC=sentinelone".
adusermember__contains	optional	Free-text filter by Active Directory user groups string (supports multiple values). Example: "DC=sentinelone".
adusername__contains	optional	Free-text filter by Active Directory username string (supports multiple values). Example: "DC=sentinelone".
aduserquery__contains	optional	Free-text filter by Active Directory computer name or its groups (supports multiple values). Example: "DC=sentinelone,John".
agentnamespace__contains	optional	Free-text filter by agent namespace (supports multiple values)
agentpodname__contains	optional	Free-text filter by agent pod name (supports multiple values)
agentversion__between	optional	Version range for agent version (format: <from_version>-<to_version>, inclusive). Example: "2.0.0.0-2.1.5.144".

agentversion__gt	optional	Agents versions greater than given version. Example: "2.5.1.1320".
agentversion__gte	optional	Agents versions greater than or equal to given version. Example: "2.5.1.1320".
agentversion__lt	optional	Agents versions less than given version. Example: "2.5.1.1320".
agentversion__lte	optional	Agents versions less than or equal to given version. Example: "2.5.1.1320".
agentversions	optional	Agent versions to include. Example: "2.0.0.0,2.1.5.144".
agentversionsnin	optional	Agent versions not to include. Example: "2.0.0.0,2.1.5.144".
appsvulnerabilitystatuses	optional	Apps vulnerability status in. Example: "patch_required".
appsvulnerabilitystatusesnin	optional	Apps vulnerability status nin. Example: "patch_required".
awsrole__contains	optional	Free-text filter by aws role(supports multiple values)
awssecuritygroups__contains	optional	Free-text filter by aws securityGroups(supports multiple values)
awssubnetids__contains	optional	Free-text filter by aws subnet ids (supports multiple values)
azureresourcegroup__contains	optional	Free-text filter by azure resource group(supports multiple values)
cloudaccount__contains	optional	Free-text filter by cloud account (supports multiple values)
cloudimage__contains	optional	Free-text filter by cloud image (supports multiple values)
cloudinstanceid__contains	optional	Free-text filter by cloud instance id(supports multiple values)
cloudinstancesize__contains	optional	Free-text filter by cloud instance size(supports multiple values)
cloudlocation__contains	optional	Free-text filter by cloud location (supports multiple values)
cloudnetwork__contains	optional	Free-text filter by cloud network (supports multiple values)
cloudprovider	optional	Agents from which cloud provider
cloudprovidernin	optional	Exclude Agents from these cloud provider
cloudtags__contains	optional	Free-text filter by cloud tags (supports multiple values)

clustername__contains	optional	Free-text filter by cluster name (supports multiple values)
computername	optional	Computer name. Example: "My Office Desktop".
computername__contains	optional	Free-text filter by computer name (supports multiple values). Example: "john-office,WIN".
computername__like	optional	Match computer name partially (substring). Example: "Lab1".
consolemigrationstatuses	optional	Migration status in. Example: "N/A".
consolemigrationstatusesnin	optional	Migration status nin. Example: "N/A".
corecount__between	optional	Possible number of CPU cores (inclusive). Example: "2-8".
corecount__gt	optional	CPU cores (more than)
corecount__gte	optional	CPU cores (more than or equal)
corecount__lt	optional	CPU cores (less than)
corecount__lte	optional	CPU cores (less than or equal)
countonly	optional	If true, only total number of items will be returned, without any of the actual objects.
cpucount__between	optional	Possible number of CPU cores (inclusive). Example: "2-8".
cpucount__gt	optional	Number of CPUs (more than)
cpucount__gte	optional	Number of CPUs (more than or equal)
cpucount__lt	optional	Number of CPUs (less than)
cpucount__lte	optional	Number of CPUs (less than or equal)
cpuid__contains	optional	Free-text filter by CPU name (supports multiple values). Example: "Intel,AMD".
createdat__between	optional	Date range for creation time (format: <from_timestamp>-<to_timestamp>, inclusive). Example: "1514978890136-1514978650130".
createdat__gt	optional	Agents created after this timestamp. Example: "2018-02-27T04:49:26.257525Z".
createdat__gte	optional	Agents created after or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
createdat__lt	optional	Agents created before this timestamp. Example: "2018-02-27T04:49:26.257525Z".
createdat__lte	optional	Agents created before or at this timestamp. Example:

		"2018-02-27T04:49:26.257525Z".
csvfilterid	optional	The ID of the CSV file to filter by. Example: "225494730938493804".
cursor	optional	Cursor position returned by the last request. Use to iterate over more than 1000 items. Example: "YWdlbnRfaWQ6NTgwMjkzODE=".
decommissionedat__between	optional	Date range for decommission time (format: <from_timestamp>-<to_timestamp>, inclusive). Example: "1514978890136-1514978650130".
decommissionedat__gt	optional	Agents decommissioned after this timestamp. Example: "2018-02-27T04:49:26.257525Z".
decommissionedat__gte	optional	Agents decommissioned after or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
decommissionedat__lt	optional	Agents decommissioned before this timestamp. Example: "2018-02-27T04:49:26.257525Z".
decommissionedat__lte	optional	Agents decommissioned before this timestamp. Example: "2018-02-27T04:49:26.257525Z".
domains	optional	Included network domains. Example: "mybusiness.net,workgroup".
domainsnin	optional	Not included network domains. Example: "mybusiness.net,workgroup".
encryptedapplications	optional	Disk encryption status
externalid__contains	optional	Free-text filter by external ID (Customer ID). Example: "Tag#1 - monitoring,Performance machine".
externalip__contains	optional	Free-text filter by visible IP (supports multiple values). Example: "205,127.0".
filteredgroupids	optional	List of Group IDs to filter by. Example: "225494730938493804,225494730938493915".
filteredsiteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".
filterid	optional	Include all Agents matching this saved filter. Example: "225494730938493804".
firewallenabled	optional	The agents supports Firewall Control and it is enabled for the agent's group
gatewayip	optional	Gateway ip. Example: "192.168.0.1".

gcpserviceaccount__contains	optional	Free-text filter by gcp service account (supports multiple values)
groupids	optional	List of Group IDs to filter by. Example: "225494730938493804,225494730938493915".
hascontainerizedworkload	optional	Include only Agents protecting containerized workloads
haslocalconfiguration	optional	Agent has a local configuration set
hastags	optional	Include only Agents that have any tags assigned if True, or none if False
ids	optional	A list of Agent IDs. Example: "225494730938493804,225494730938493915".
infected	optional	Include only Agents with at least one active threat
installertypes	optional	Include only Agents installed with these package types. Example: ".msi".
installertypesnin	optional	Exclude Agents installed with these package types. Example: ".msi".
isactive	optional	Include only active Agents
isdecommissioned	optional	Include active, decommissioned or both. Example: "True,False".
ispendinguninstall	optional	Include only Agents with pending uninstall requests
isuninstalled	optional	Include installed, uninstalled or both. Example: "True,False".
isuptodate	optional	Include only Agents with updated software
k8snodelabels__contains	optional	Free-text filter by K8s node labels (supports multiple values)
k8snodename__contains	optional	Free-text filter by K8s node name (supports multiple values)
k8stype__contains	optional	Free-text filter by K8s type(supports multiple values)
k8sversion__contains	optional	Free-text filter by K8s version (supports multiple values)
lastactivedate__between	optional	Date range for last active date(format: <from_timestamp>-<to_timestamp>, inclusive). Example: "1514978764288-1514978999999".
lastactivedate__gt	optional	Agents last active after this time. Example: "2018-02-27T04:49:26.257525Z".
lastactivedate__gte	optional	Agents last active after or at this time. Example: "2018-02-27T04:49:26.257525Z".

lastactivedate__lt	optional	Agents last active before this time. Example: "2018-02-27T04:49:26.257525Z".
lastactivedate__lte	optional	Agents last active before or at this time. Example: "2018-02-27T04:49:26.257525Z".
lastloggedinusername__contains	optional	Free-text filter by username (supports multiple values). Example: "admin,johnd1".
lastsuccessfulscandate__between	optional	Date range for last successful full disk scan(format: <from_timestamp>-<to_timestamp>, inclusive). Example: "1514978764288-1514978999999".
lastsuccessfulscandate__gt	optional	Agents last successful full disk scan after this time. Example: "2018-02-27T04:49:26.257525Z".
lastsuccessfulscandate__gte	optional	Agents last successful full disk scan after or at this time. Example: "2018-02-27T04:49:26.257525Z".
lastsuccessfulscandate__lt	optional	Agents last successful full disk scan before this time. Example: "2018-02-27T04:49:26.257525Z".
lastsuccessfulscandate__lte	optional	Agents last successful full disk scan before or at this time. Example: "2018-02-27T04:49:26.257525Z".
limit	optional	Limit number of returned items (1-1000). Example: "10".
liveupdateid__contains	optional	Free-text filter by live update ID (supports multiple values)
locationenabled	optional	The agents supports Location Awareness and it is enabled for the agent's group
locationids	optional	Include only Agents reporting these locations. Example: "225494730938493804,225494730938493915".
locationidsnin	optional	Do not include only Agents reporting these locations. Example: "225494730938493804,225494730938493915".
machinetypes	optional	Included machine types. Example: "laptop,desktop".
machinetypesnin	optional	Not included machine types. Example: "laptop,desktop".
migrationstatus	optional	Migration status. Example: "N/A".
missingpermissions	optional	Included missing permissions. Example: "user_action_needed_bluetooth_per,user_action_needed_fda_helper".
missingpermissionsnin	optional	Excluded missing permissions. Example: "user_action_needed_bluetooth_per,user_action_needed_fda_helper".

mitigationmode	optional	Agent mitigation mode policy. Example: "detect".
mitigationmodesuspicious	optional	Mitigation mode policy for suspicious activity. Example: "detect".
networkinterfacegatewaymacaddress__contains	optional	Free-text filter by Gateway MAC address (supports multiple values). Example: "aa:0f,:41:".
networkinterfaceinet__contains	optional	Free-text filter by local IP (supports multiple values). Example: "192,10.0.0".
networkinterfacephysical__contains	optional	Free-text filter by MAC address (supports multiple values). Example: "aa:0f,:41:".
networkquarantineenabled	optional	The agents supports Network Quarantine Control and its enabled for the agent's group
networkstatuses	optional	Included network statuses. Example: "connected,connecting".
networkstatusesnin	optional	Included network statuses. Example: "connected,connecting".
operationalstates	optional	Agent operational state
operationalstatesnin	optional	Do not include these Agent operational states
osarch	optional	OS architecture. Example: "32 bit".
ostypes	optional	Included OS types. Example: "macos".
ostypesnin	optional	Not included OS types. Example: "macos".
osversion__contains	optional	Free-text filter by OS full name and version (supports multiple values). Example: "Service Pack 1".
query	optional	A free-text search term, will match applicable attributes (sub-string match). Note: Device's physical addresses will be matched if they start with the search term only (no match if they contain the term). Example: "Linux".
rangerstatus	optional	[DEPRECATED] Use rangerStatuses. Example: "NotApplicable".
rangerstatuses	optional	Status of Ranger. Example: "NotApplicable".
rangerstatusesnin	optional	Do not include these Ranger Statuses. Example: "NotApplicable".
rangerversions	optional	Ranger versions to include. Example: "2.0.0.0,2.1.5.144".
rangerversionsnin	optional	Ranger versions not to include. Example: "2.0.0.0,2.1.5.144".
registeredat__between	optional	Date range for first registration time (format: <from_timestamp>-<to_timestamp>, inclusive). Example: "1514978764288-1514978999999".

registeredat__gt	optional	Agents registered after this time. Example: "2018-02-27T04:49:26.257525Z".
registeredat__gte	optional	Agents registered after or at this time. Example: "2018-02-27T04:49:26.257525Z".
registeredat__lt	optional	Agents registered before this time. Example: "2018-02-27T04:49:26.257525Z".
registeredat__lte	optional	Agents registered before or at this time. Example: "2018-02-27T04:49:26.257525Z".
remoteopsforensicssupported	optional	Include only agents that has Remote Ops Forensicsfeature supported
remoteprofilingstates	optional	Agent remote profiling state
remoteprofilingstatesnin	optional	Do not include these Agent remote profiling states
rsolevel	optional	Supported Remote Script Orchestration level. Example: "none".
scanstatus	optional	Scan status. Example: "none".
scanstatuses	optional	Included scan statuses. Example: "started,aborted".
scanstatusesnin	optional	Not included scan statuses. Example: "started,aborted".
serialnumber__contains	optional	Free-text filter by Serial Number (supports multiple values)
siteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".
skip	optional	Skip first number of items (0-1000). To iterate over more than 1000 items, use "cursor". Example: "150".
skipcount	optional	If true, total number of items will not be calculated, which speeds up execution time.
tagsdata	optional	Filter agents by their assigned tags. Given in form of a JSON where each key represents a tag key, and each value represents a list of string values to filter by. To filter by unassigned tag values, use __nin suffix in the tag key. Example: "{"key1": ["value1_1", "value1_2"], "key2__nin": ["value2"]}".
threatcontenthash	optional	Include only Agents that have at least one threat with this content hash. Example: "cf23df2207d99a74fbe169e3eba035e633b65d94".
threatcreatedat__between	optional	Agents with threats reported in a date range (format: <from_timestamp>-<to_timestamp>, inclusive). Example: "1514978764288-1514978999999".

threatcreatedat__gt	optional	Agents with threats reported after this time. Example: "2018-02-27T04:49:26.257525Z".
threatcreatedat__gte	optional	Agents with threats reported after or at this time. Example: "2018-02-27T04:49:26.257525Z".
threatcreatedat__lt	optional	Agents with threats reported before this time. Example: "2018-02-27T04:49:26.257525Z".
threatcreatedat__lte	optional	Agents with threats reported before or at this time. Example: "2018-02-27T04:49:26.257525Z".
threathidden	optional	Include only Agents with at least one hidden threat
threatmitigationstatus	optional	Include only Agents that have threats with this mitigation status. Example: "mitigated".
threatrebootrequired	optional	Has at least one threat with at least one mitigation action pending reboot to succeed
threatresolved	optional	Include only Agents with at least one resolved threat
totalmemory__between	optional	Total memory range (GB, inclusive). Example: "4-8".
totalmemory__gt	optional	Memory size (MB, more than)
totalmemory__gte	optional	Memory size (MB, more than or equal)
totalmemory__lt	optional	Memory size (MB, less than)
totalmemory__lte	optional	Memory size (MB, less than or equal)
updatedat__between	optional	Date range for update time (format: <from_timestamp>-<to_timestamp>, inclusive). Example: "1514978890136-1514978650130".
updatedat__gt	optional	Agents updated after this timestamp. Example: "2018-02-27T04:49:26.257525Z".
updatedat__gte	optional	Agents updated after or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
updatedat__lt	optional	Agents updated before this timestamp. Example: "2018-02-27T04:49:26.257525Z".
updatedat__lte	optional	Agents updated before or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
useractionsneeded	optional	Included pending user actions. Example: "reboot_needed,upgrade_needed".
useractionsneedednin	optional	Excluded pending user actions. Example:

		"reboot_needed,upgrade_needed".
uuid	optional	Agent's universally unique identifier. Example: "ff819e70af13be381993075eb0ce5f2f6de05be2".
uuid__contains	optional	Free-text filter by Agent UUID (supports multiple values). Example: "e92-01928,b055".
uuids	optional	A list of included UUIDs. Example: "ff819e70af13be381993075eb0ce5f2f6de05b11,ff819e70af13be381993075eb0ce5f2f6de05c22".

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - Insufficient permissions

Response Schema

Name	Description	Required	Value
pagination	Pagination information	true	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>totalItems</td><td>Total number of items found matching your query</td><td>true</td><td>integer</td></tr><tr><td>nextCursor</td><td>Pass this value as "cursor" on your next request, to get the next page of results (Will be "null" when last page reached)</td><td>false</td><td>string</td></tr></table>

<table>
<tr><td>data</td><td>Response data</td><td>false</td><td><table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>computerName</td><td>Computer name</td><td>false</td><td>string</td></tr>
<tr><td>domain</td><td>Network domain</td><td>false</td><td>string</td></tr>
<tr><td>id</td><td>Agent ID</td><td>false</td><td>string</td></tr>
<tr><td>lastLoggedInUserName</td><td>Last logged in user name</td><td>false</td><td>string</td></tr>
<tr><td>passphrase</td><td>Generated passphrase for the agent</td><td>false</td><td>string</td></tr>
<tr><td>uuid</td><td>Agent's universally unique identifier</td><td>false</td><td>string</td></tr>
</table></td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Export Agent Logs

GET /web/api/v2.1/agents/{agent_id}/uploads/{activity_id}

Get Agent logs from Agents that match the filter. You can filter by Agent ID (run "agents" to get the ID) or by Activity ID (run "activities/types" to get the Activity ID). Send the logs to SentinelOne Support for assistance.

Response Messages

200 - Success

401 - Unauthorized access - please sign in and retry.

403 - Insufficient permissions

404 - Agent or activity not found

Applications

GET /web/api/v2.1/agents/applications

Get the installed applications for a specific Agent.
To get the Agent ID, run "agents".

Parameters

ids	required	Agent ID list. Example: "225494730938493804,225494730938493915".

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
data	Response data	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>installedDate</td><td>Installed date</td><td>false</td><td>string</td></tr><tr><td>name</td><td>Name</td><td>false</td><td>string</td></tr><tr><td>publisher</td><td>Publisher</td><td>false</td><td>string</td></tr><tr><td>size</td><td>Size</td><td>false</td><td>integer</td></tr><tr><td>version</td><td>Version</td><td>false</td><td>string</td></tr></table>
errors	Errors	false	array

Processes

GET /web/api/v2.1/agents/processes

[OBSOLETE] Returns empty array. To get processes of an Agent, see Applications.

Parameters

ids	required	Agent ID list. Example: "225494730938493804,225494730938493915".

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
cpuUsage	CPU Usage (%)	false	integer
executablePath	Executable path	false	string
memoryUsage	Memory usage (MB)	false	integer
pid	Process ID	false	integer
processName	Process name	false	string
startTime	Start time	false	string

errors	Errors	false	array

Get local upgrade agent authorization

GET /web/api/v2.1/agents/{agent_id}/local-upgrade-authorization

Get the time when authorization of local upgrades expires

Response Messages

200 - Success

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
data	Response data	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>agentAuthorization</td><td>Agent authorization</td><td>false</td><td>string</td></tr><tr><td>siteAuthorization</td><td>Site authorization</td><td>false</td><td>string</td></tr></table>
errors	Errors	false	array

Export Agents

GET /web/api/v2.1/export/agents

Export Agent data to a CSV, for Agents that match the filter. This command exports up to 50000 items (each datum is an item).

Parameters

accountids	optional	List of Account IDs to filter by. Example: "225494730938493804,225494730938493915".
activethreats	optional	Include Agents with this amount of active threats. Example: "3".
activethreats__gt	optional	Include Agents with at least this amount of active threats. Example: "5".
adcomputermember__contains	optional	Free-text filter by Active Directory computer groups string (supports multiple values). Example: "DC=sentinelone".
adcomputername__contains	optional	Free-text filter by Active Directory computer name string (supports multiple values). Example: "DC=sentinelone".
adcomputerquery__contains	optional	Free-text filter by Active Directory computer name or its groups (supports multiple values). Example: "DC=sentinelone,Windows".
adquery	optional	An Active Directory query string. Example: "CN=Managers,DC=sentinelone,DC=com".
adquery__contains	optional	Free-text filter by Active Directory string (supports multiple values). Example: "DC=sentinelone".
adusermember__contains	optional	Free-text filter by Active Directory user groups string (supports multiple values). Example: "DC=sentinelone".
adusername__contains	optional	Free-text filter by Active Directory username string (supports multiple values). Example: "DC=sentinelone".
aduserquery__contains	optional	Free-text filter by Active Directory computer name or its groups (supports multiple values). Example: "DC=sentinelone,John".
agentnamespace__contains	optional	Free-text filter by agent namespace (supports multiple values)
agentpodname__contains	optional	Free-text filter by agent pod name (supports multiple values)
agentversion__between	optional	Version range for agent version (format: <from_version>-<to_version>, inclusive). Example: "2.0.0.0-2.1.5.144".

agentversion__gt	optional	Agents versions greater than given version. Example: "2.5.1.1320".
agentversion__gte	optional	Agents versions greater than or equal to given version. Example: "2.5.1.1320".
agentversion__lt	optional	Agents versions less than given version. Example: "2.5.1.1320".
agentversion__lte	optional	Agents versions less than or equal to given version. Example: "2.5.1.1320".
agentversions	optional	Agent versions to include. Example: "2.0.0.0,2.1.5.144".
agentversionsnin	optional	Agent versions not to include. Example: "2.0.0.0,2.1.5.144".
appsvulnerabilitystatuses	optional	Apps vulnerability status in. Example: "patch_required".
appsvulnerabilitystatusesnin	optional	Apps vulnerability status nin. Example: "patch_required".
awsrole__contains	optional	Free-text filter by aws role(supports multiple values)
awssecuritygroups__contains	optional	Free-text filter by aws securityGroups(supports multiple values)
awssubnetids__contains	optional	Free-text filter by aws subnet ids (supports multiple values)
azureresourcegroup__contains	optional	Free-text filter by azure resource group(supports multiple values)
cloudaccount__contains	optional	Free-text filter by cloud account (supports multiple values)
cloudimage__contains	optional	Free-text filter by cloud image (supports multiple values)
cloudinstanceid__contains	optional	Free-text filter by cloud instance id(supports multiple values)
cloudinstancesize__contains	optional	Free-text filter by cloud instance size(supports multiple values)
cloudlocation__contains	optional	Free-text filter by cloud location (supports multiple values)
cloudnetwork__contains	optional	Free-text filter by cloud network (supports multiple values)
cloudprovider	optional	Agents from which cloud provider
cloudprovidernin	optional	Exclude Agents from these cloud provider
cloudtags__contains	optional	Free-text filter by cloud tags (supports multiple values)

clustername__contains	optional	Free-text filter by cluster name (supports multiple values)
computername	optional	Computer name. Example: "My Office Desktop".
computername__contains	optional	Free-text filter by computer name (supports multiple values). Example: "john-office,WIN".
computername__like	optional	Match computer name partially (substring). Example: "Lab1".
consolemigrationstatuses	optional	Migration status in. Example: "N/A".
consolemigrationstatusesnin	optional	Migration status nin. Example: "N/A".
corecount__between	optional	Possible number of CPU cores (inclusive). Example: "2-8".
corecount__gt	optional	CPU cores (more than)
corecount__gte	optional	CPU cores (more than or equal)
corecount__lt	optional	CPU cores (less than)
corecount__lte	optional	CPU cores (less than or equal)
cpucount__between	optional	Possible number of CPU cores (inclusive). Example: "2-8".
cpucount__gt	optional	Number of CPUs (more than)
cpucount__gte	optional	Number of CPUs (more than or equal)
cpucount__lt	optional	Number of CPUs (less than)
cpucount__lte	optional	Number of CPUs (less than or equal)
cpuid__contains	optional	Free-text filter by CPU name (supports multiple values). Example: "Intel,AMD".
createdat__between	optional	Date range for creation time (format: <from_timestamp>-<to_timestamp>, inclusive). Example: "1514978890136-1514978650130".
createdat__gt	optional	Agents created after this timestamp. Example: "2018-02-27T04:49:26.257525Z".
createdat__gte	optional	Agents created after or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
createdat__lt	optional	Agents created before this timestamp. Example: "2018-02-27T04:49:26.257525Z".
createdat__lte	optional	Agents created before or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
csvfilterid	optional	The ID of the CSV file to filter by. Example:

		"225494730938493804".
decommissionedat__between	optional	Date range for decommission time (format: <from_timestamp>-<to_timestamp>, inclusive). Example: "1514978890136-1514978650130".
decommissionedat__gt	optional	Agents decommissioned after this timestamp. Example: "2018-02-27T04:49:26.257525Z".
decommissionedat__gte	optional	Agents decommissioned after or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
decommissionedat__lt	optional	Agents decommissioned before this timestamp. Example: "2018-02-27T04:49:26.257525Z".
decommissionedat__lte	optional	Agents decommissioned before this timestamp. Example: "2018-02-27T04:49:26.257525Z".
domains	optional	Included network domains. Example: "mybusiness.net,workgroup".
domainsnin	optional	Not included network domains. Example: "mybusiness.net,workgroup".
encryptedapplications	optional	Disk encryption status
externalid__contains	optional	Free-text filter by external ID (Customer ID). Example: "Tag#1 - monitoring,Performance machine".
externalip__contains	optional	Free-text filter by visible IP (supports multiple values). Example: "205,127.0".
filteredgroupids	optional	List of Group IDs to filter by. Example: "225494730938493804,225494730938493915".
filteredsiteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".
filterid	optional	Include all Agents matching this saved filter. Example: "225494730938493804".
firewallenabled	optional	The agents supports Firewall Control and it is enabled for the agent's group
gatewayip	optional	Gateway ip. Example: "192.168.0.1".
gcpserviceaccount__contains	optional	Free-text filter by gcp service account (supports multiple values)
groupids	optional	List of Group IDs to filter by. Example: "225494730938493804,225494730938493915".
hascontainerizedwork	optional	Include only Agents protecting containerized workloads

load		
haslocalconfiguration	optional	Agent has a local configuration set
hastags	optional	Include only Agents that have any tags assigned if True, or none if False
ids	optional	A list of Agent IDs. Example: "225494730938493804,225494730938493915".
infected	optional	Include only Agents with at least one active threat
installertypes	optional	Include only Agents installed with these package types. Example: ".msi".
installertypesnin	optional	Exclude Agents installed with these package types. Example: ".msi".
isactive	optional	Include only active Agents
isdecommissioned	optional	Include active, decommissioned or both. Example: "True,False".
ispendinguninstall	optional	Include only Agents with pending uninstall requests
isuninstalled	optional	Include installed, uninstalled or both. Example: "True,False".
isuptodate	optional	Include only Agents with updated software
k8snodelabels__contains	optional	Free-text filter by K8s node labels (supports multiple values)
k8snodename__contains	optional	Free-text filter by K8s node name (supports multiple values)
k8stype__contains	optional	Free-text filter by K8s type(supports multiple values)
k8sversion__contains	optional	Free-text filter by K8s version (supports multiple values)
lastactivedate__between	optional	Date range for last active date(format: <from_timestamp>-<to_timestamp>, inclusive). Example: "1514978764288-1514978999999".
lastactivedate__gt	optional	Agents last active after this time. Example: "2018-02-27T04:49:26.257525Z".
lastactivedate__gte	optional	Agents last active after or at this time. Example: "2018-02-27T04:49:26.257525Z".
lastactivedate__lt	optional	Agents last active before this time. Example: "2018-02-27T04:49:26.257525Z".
lastactivedate__lte	optional	Agents last active before or at this time. Example: "2018-02-27T04:49:26.257525Z".
lastloggedinusername_	optional	Free-text filter by username (supports multiple values). Example:

_contains		"admin,johnd1".
lastsuccessfulscandate__between	optional	Date range for last successful full disk scan(format: <from_timestamp>-<to_timestamp>, inclusive). Example: "1514978764288-1514978999999".
lastsuccessfulscandate__gt	optional	Agents last successful full disk scan after this time. Example: "2018-02-27T04:49:26.257525Z".
lastsuccessfulscandate__gte	optional	Agents last successful full disk scan after or at this time. Example: "2018-02-27T04:49:26.257525Z".
lastsuccessfulscandate__lt	optional	Agents last successful full disk scan before this time. Example: "2018-02-27T04:49:26.257525Z".
lastsuccessfulscandate__lte	optional	Agents last successful full disk scan before or at this time. Example: "2018-02-27T04:49:26.257525Z".
liveupdateid__contains	optional	Free-text filter by live update ID (supports multiple values)
locationenabled	optional	The agents supports Location Awareness and it is enabled for the agent's group
locationids	optional	Include only Agents reporting these locations. Example: "225494730938493804,225494730938493915".
locationidsnin	optional	Do not include only Agents reporting these locations. Example: "225494730938493804,225494730938493915".
machinetypes	optional	Included machine types. Example: "laptop,desktop".
machinetypesnin	optional	Not included machine types. Example: "laptop,desktop".
migrationstatus	optional	Migration status. Example: "N/A".
missingpermissions	optional	Included missing permissions. Example: "user_action_needed_bluetooth_per,user_action_needed_fda_helper".
missingpermissionsnin	optional	Excluded missing permissions. Example: "user_action_needed_bluetooth_per,user_action_needed_fda_helper".
mitigationmode	optional	Agent mitigation mode policy. Example: "detect".
mitigationmodesuspicious	optional	Mitigation mode policy for suspicious activity. Example: "detect".
networkinterfacegatewaymacaddress__contains	optional	Free-text filter by Gateway MAC address (supports multiple values). Example: "aa:0f,:41:".

networkinterfaceinet__contains	optional	Free-text filter by local IP (supports multiple values). Example: "192,10.0.0".
networkinterfacephysical__contains	optional	Free-text filter by MAC address (supports multiple values). Example: "aa:0f,:41:".
networkquarantineenabled	optional	The agents supports Network Quarantine Control and its enabled for the agent's group
networkstatuses	optional	Included network statuses. Example: "connected,connecting".
networkstatusesnin	optional	Included network statuses. Example: "connected,connecting".
operationalstates	optional	Agent operational state
operationalstatesnin	optional	Do not include these Agent operational states
osarch	optional	OS architecture. Example: "32 bit".
ostypes	optional	Included OS types. Example: "macos".
ostypesnin	optional	Not included OS types. Example: "macos".
osversion__contains	optional	Free-text filter by OS full name and version (supports multiple values). Example: "Service Pack 1".
query	optional	A free-text search term, will match applicable attributes (sub-string match). Note: Device's physical addresses will be matched if they start with the search term only (no match if they contain the term). Example: "Linux".
rangerstatus	optional	[DEPRECATED] Use rangerStatuses. Example: "NotApplicable".
rangerstatuses	optional	Status of Ranger. Example: "NotApplicable".
rangerstatusesnin	optional	Do not include these Ranger Statuses. Example: "NotApplicable".
rangerversions	optional	Ranger versions to include. Example: "2.0.0.0,2.1.5.144".
rangerversionsnin	optional	Ranger versions not to include. Example: "2.0.0.0,2.1.5.144".
registeredat__between	optional	Date range for first registration time (format: <from_timestamp>-<to_timestamp>, inclusive). Example: "1514978764288-1514978999999".
registeredat__gt	optional	Agents registered after this time. Example: "2018-02-27T04:49:26.257525Z".
registeredat__gte	optional	Agents registered after or at this time. Example: "2018-02-27T04:49:26.257525Z".
registeredat__lt	optional	Agents registered before this time. Example: "2018-02-27T04:49:26.257525Z".

registeredat__lte	optional	Agents registered before or at this time. Example: "2018-02-27T04:49:26.257525Z".
remoteopsforensicssupported	optional	Include only agents that has Remote Ops Forensicsfeature supported
remoteprofilingstates	optional	Agent remote profiling state
remoteprofilingstatesnin	optional	Do not include these Agent remote profiling states
rsolevel	optional	Supported Remote Script Orchestration level. Example: "none".
scanstatus	optional	Scan status. Example: "none".
scanstatuses	optional	Included scan statuses. Example: "started,aborted".
scanstatusesnin	optional	Not included scan statuses. Example: "started,aborted".
serialnumber__contains	optional	Free-text filter by Serial Number (supports multiple values)
siteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".
tagsdata	optional	Filter agents by their assigned tags. Given in form of a JSON where each key represents a tag key, and each value represents a list of string values to filter by. To filter by unassigned tag values, use __nin suffix in the tag key. Example: "{"key1": ["value1_1", "value1_2"], "key2__nin": ["value2"]}".
threatcontenthash	optional	Include only Agents that have at least one threat with this content hash. Example: "cf23df2207d99a74fbe169e3eba035e633b65d94".
threatcreatedat__between	optional	Agents with threats reported in a date range (format: <from_timestamp>-<to_timestamp>, inclusive). Example: "1514978764288-1514978999999".
threatcreatedat__gt	optional	Agents with threats reported after this time. Example: "2018-02-27T04:49:26.257525Z".
threatcreatedat__gte	optional	Agents with threats reported after or at this time. Example: "2018-02-27T04:49:26.257525Z".
threatcreatedat__lt	optional	Agents with threats reported before this time. Example: "2018-02-27T04:49:26.257525Z".
threatcreatedat__lte	optional	Agents with threats reported before or at this time. Example: "2018-02-27T04:49:26.257525Z".
threathidden	optional	Include only Agents with at least one hidden threat

threatmitigationstatus	optional	Include only Agents that have threats with this mitigation status. Example: "mitigated".
threatrebootrequired	optional	Has at least one threat with at least one mitigation action pending reboot to succeed
threatresolved	optional	Include only Agents with at least one resolved threat
totalmemory__between	optional	Total memory range (GB, inclusive). Example: "4-8".
totalmemory__gt	optional	Memory size (MB, more than)
totalmemory__gte	optional	Memory size (MB, more than or equal)
totalmemory__lt	optional	Memory size (MB, less than)
totalmemory__lte	optional	Memory size (MB, less than or equal)
updatedat__between	optional	Date range for update time (format: <from_timestamp>-<to_timestamp>, inclusive). Example: "1514978890136-1514978650130".
updatedat__gt	optional	Agents updated after this timestamp. Example: "2018-02-27T04:49:26.257525Z".
updatedat__gte	optional	Agents updated after or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
updatedat__lt	optional	Agents updated before this timestamp. Example: "2018-02-27T04:49:26.257525Z".
updatedat__lte	optional	Agents updated before or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
useractionsneeded	optional	Included pending user actions. Example: "reboot_needed,upgrade_needed".
useractionsneedednin	optional	Excluded pending user actions. Example: "reboot_needed,upgrade_needed".
uuid	optional	Agent's universally unique identifier. Example: "ff819e70af13be381993075eb0ce5f2f6de05be2".
uuid__contains	optional	Free-text filter by Agent UUID (supports multiple values). Example: "e92-01928,b055".
uuids	optional	A list of included UUIDs. Example: "ff819e70af13be381993075eb0ce5f2f6de05b11,ff819e70af13be381993075eb0ce5f2f6de05c22".

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Get the endpoint tags that match the filters.

GET /web/api/v2.1/agents/tags

Get endpoint Tags.

Parameters

accountids	optional	List of Account IDs to filter by. Example: "225494730938493804,225494730938493915".
countonly	optional	If true, only total number of items will be returned, without any of the actual objects.
cursor	optional	Cursor position returned by the last request. Use to iterate over more than 1000 items. Example: "YWdlbnRfaWQ6NTgwMjkzODE=".
description	optional	Tag description
groupids	optional	List of Group IDs to filter by. Example: "225494730938493804,225494730938493915".
ids	optional	List of tag IDs to filter by. Example: "225494730938493804,225494730938493915".
includechildren	optional	Return tags from children scope levels
includeparents	optional	Return tags from parent scope levels
key	optional	Tag key
key__contains	optional	Free-text filter by tag key. Example: "server".
limit	optional	Limit number of returned items (1-1000). Example: "10".
query	optional	Free text search on fields key, value, description
siteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".

skip	optional	Skip first number of items (0-1000). To iterate over more than 1000 items, use "cursor". Example: "150".
skipcount	optional	If true, total number of items will not be calculated, which speeds up execution time.
sortby	optional	The column to sort the results by. Example: "id".
sortorder	optional	Sort direction. Example: "asc".
value	optional	Tag value
value__contains	optional	Free-text filter by tag value. Example: "server".

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
pagination	Pagination information	true	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>totalItems</td><td>Total number of items found matching your query</td><td>true</td><td>integer</td></tr><tr><td>nextCursor</td><td>Pass this value as "cursor" on your next request, to get the next page of results (Will be "null" when last page reached)</td><td>false</td><td>string</td></tr></table>
data	Response	false	

<table>
<tr><td></td><td>data</td><td></td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>allowEdit</td><td>indicate if user can/cant edit the tag</td><td>false</td><td>boolean</td></tr>
<tr><td>createdAt</td><td>Timestamp of creation</td><td>false</td><td>string</td></tr>
<tr><td>createdBy</td><td>Tag creator name</td><td>false</td><td>string</td></tr>
<tr><td>description</td><td>Tag description</td><td>false</td><td>string</td></tr>
<tr><td>endpointsInCurrentScope</td><td>The number of endpoints in this scope that have this tag</td><td>false</td><td>integer</td></tr>
<tr><td>id</td><td>Tag ID</td><td>false</td><td>string</td></tr>
<tr><td>key</td><td>Tag key</td><td>false</td><td>string</td></tr>
<tr><td>scopeId</td><td>Scope id</td><td>false</td><td>string</td></tr>
<tr><td>scopeLevel</td><td>Scope level</td><td>false</td><td>enum</td></tr>
<tr><td>scopePath</td><td>tag scope path</td><td>false</td><td>string</td></tr>
<tr><td>totalEndpoints</td><td>The total number of endpoints that have this tag</td><td>false</td><td>integer</td></tr>
<tr><td>type</td><td>Tag type</td><td>false</td><td>string</td></tr>
<tr><td>updatedAt</td><td>Timestamp of last update</td><td>false</td><td>string</td></tr>
<tr><td>updatedBy</td><td>Tag updater name</td><td>false</td><td>string</td></tr>
<tr><td>value</td><td>tag value</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Export Agents - Light

GET /web/api/v2.1/export/agents-light

Export Agent data to a CSV, for Agents that match the filter. This command exports up to 300000 items (each datum is an item).

Parameters

accountids	optional	List of Account IDs to filter by. Example: "225494730938493804,225494730938493915".
activethreats	optional	Include Agents with this amount of active threats. Example: "3".
activethreats__gt	optional	Include Agents with at least this amount of active threats. Example: "5".
adcomputermember__contains	optional	Free-text filter by Active Directory computer groups string (supports multiple values). Example: "DC=sentinelone".
adcomputername__contains	optional	Free-text filter by Active Directory computer name string (supports multiple values). Example: "DC=sentinelone".
adcomputerquery__contains	optional	Free-text filter by Active Directory computer name or its groups (supports multiple values). Example: "DC=sentinelone,Windows".
adquery	optional	An Active Directory query string. Example: "CN=Managers,DC=sentinelone,DC=com".
adquery__contains	optional	Free-text filter by Active Directory string (supports multiple values). Example: "DC=sentinelone".
adusermember__contains	optional	Free-text filter by Active Directory user groups string (supports multiple values). Example: "DC=sentinelone".
adusername__contains	optional	Free-text filter by Active Directory username string (supports multiple values). Example: "DC=sentinelone".
aduserquery__contains	optional	Free-text filter by Active Directory computer name or its groups (supports multiple values). Example: "DC=sentinelone,John".
agentnamespace__contains	optional	Free-text filter by agent namespace (supports multiple values)
agentpodname__contains	optional	Free-text filter by agent pod name (supports multiple values)
agentversion__between	optional	Version range for agent version (format: <from_version>-<to_version>, inclusive). Example: "2.0.0.0-2.1.5.144".

agentversion__gt	optional	Agents versions greater than given version. Example: "2.5.1.1320".
agentversion__gte	optional	Agents versions greater than or equal to given version. Example: "2.5.1.1320".
agentversion__lt	optional	Agents versions less than given version. Example: "2.5.1.1320".
agentversion__lte	optional	Agents versions less than or equal to given version. Example: "2.5.1.1320".
agentversions	optional	Agent versions to include. Example: "2.0.0.0,2.1.5.144".
agentversionsnin	optional	Agent versions not to include. Example: "2.0.0.0,2.1.5.144".
appsvulnerabilitystatuses	optional	Apps vulnerability status in. Example: "patch_required".
appsvulnerabilitystatusesnin	optional	Apps vulnerability status nin. Example: "patch_required".
awsrole__contains	optional	Free-text filter by aws role(supports multiple values)
awssecuritygroups__contains	optional	Free-text filter by aws securityGroups(supports multiple values)
awssubnetids__contains	optional	Free-text filter by aws subnet ids (supports multiple values)
azureresourcegroup__contains	optional	Free-text filter by azure resource group(supports multiple values)
cloudaccount__contains	optional	Free-text filter by cloud account (supports multiple values)
cloudimage__contains	optional	Free-text filter by cloud image (supports multiple values)
cloudinstanceid__contains	optional	Free-text filter by cloud instance id(supports multiple values)
cloudinstancesize__contains	optional	Free-text filter by cloud instance size(supports multiple values)
cloudlocation__contains	optional	Free-text filter by cloud location (supports multiple values)
cloudnetwork__contains	optional	Free-text filter by cloud network (supports multiple values)
cloudprovider	optional	Agents from which cloud provider
cloudprovidernin	optional	Exclude Agents from these cloud provider
cloudtags__contains	optional	Free-text filter by cloud tags (supports multiple values)

clustername__contains	optional	Free-text filter by cluster name (supports multiple values)
computername	optional	Computer name. Example: "My Office Desktop".
computername__contains	optional	Free-text filter by computer name (supports multiple values). Example: "john-office,WIN".
computername__like	optional	Match computer name partially (substring). Example: "Lab1".
consolemigrationstatuses	optional	Migration status in. Example: "N/A".
consolemigrationstatusesnin	optional	Migration status nin. Example: "N/A".
corecount__between	optional	Possible number of CPU cores (inclusive). Example: "2-8".
corecount__gt	optional	CPU cores (more than)
corecount__gte	optional	CPU cores (more than or equal)
corecount__lt	optional	CPU cores (less than)
corecount__lte	optional	CPU cores (less than or equal)
cpucount__between	optional	Possible number of CPU cores (inclusive). Example: "2-8".
cpucount__gt	optional	Number of CPUs (more than)
cpucount__gte	optional	Number of CPUs (more than or equal)
cpucount__lt	optional	Number of CPUs (less than)
cpucount__lte	optional	Number of CPUs (less than or equal)
cpuid__contains	optional	Free-text filter by CPU name (supports multiple values). Example: "Intel,AMD".
createdat__between	optional	Date range for creation time (format: <from_timestamp>-<to_timestamp>, inclusive). Example: "1514978890136-1514978650130".
createdat__gt	optional	Agents created after this timestamp. Example: "2018-02-27T04:49:26.257525Z".
createdat__gte	optional	Agents created after or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
createdat__lt	optional	Agents created before this timestamp. Example: "2018-02-27T04:49:26.257525Z".
createdat__lte	optional	Agents created before or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
csvfilterid	optional	The ID of the CSV file to filter by. Example:

		"225494730938493804".
decommissionedat__between	optional	Date range for decommission time (format: <from_timestamp>-<to_timestamp>, inclusive). Example: "1514978890136-1514978650130".
decommissionedat__gt	optional	Agents decommissioned after this timestamp. Example: "2018-02-27T04:49:26.257525Z".
decommissionedat__gte	optional	Agents decommissioned after or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
decommissionedat__lt	optional	Agents decommissioned before this timestamp. Example: "2018-02-27T04:49:26.257525Z".
decommissionedat__lte	optional	Agents decommissioned before this timestamp. Example: "2018-02-27T04:49:26.257525Z".
domains	optional	Included network domains. Example: "mybusiness.net,workgroup".
domainsnin	optional	Not included network domains. Example: "mybusiness.net,workgroup".
encryptedapplications	optional	Disk encryption status
externalid__contains	optional	Free-text filter by external ID (Customer ID). Example: "Tag#1 - monitoring,Performance machine".
externalip__contains	optional	Free-text filter by visible IP (supports multiple values). Example: "205,127.0".
filteredgroupids	optional	List of Group IDs to filter by. Example: "225494730938493804,225494730938493915".
filteredsiteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".
filterid	optional	Include all Agents matching this saved filter. Example: "225494730938493804".
firewallenabled	optional	The agents supports Firewall Control and it is enabled for the agent's group
gatewayip	optional	Gateway ip. Example: "192.168.0.1".
gcpserviceaccount__contains	optional	Free-text filter by gcp service account (supports multiple values)
groupids	optional	List of Group IDs to filter by. Example: "225494730938493804,225494730938493915".
hascontainerizedwork	optional	Include only Agents protecting containerized workloads

load		
haslocalconfiguration	optional	Agent has a local configuration set
hastags	optional	Include only Agents that have any tags assigned if True, or none if False
ids	optional	A list of Agent IDs. Example: "225494730938493804,225494730938493915".
infected	optional	Include only Agents with at least one active threat
installertypes	optional	Include only Agents installed with these package types. Example: ".msi".
installertypesnin	optional	Exclude Agents installed with these package types. Example: ".msi".
isactive	optional	Include only active Agents
isdecommissioned	optional	Include active, decommissioned or both. Example: "True,False".
ispendinguninstall	optional	Include only Agents with pending uninstall requests
isuninstalled	optional	Include installed, uninstalled or both. Example: "True,False".
isuptodate	optional	Include only Agents with updated software
k8snodelabels__contains	optional	Free-text filter by K8s node labels (supports multiple values)
k8snodename__contains	optional	Free-text filter by K8s node name (supports multiple values)
k8stype__contains	optional	Free-text filter by K8s type(supports multiple values)
k8sversion__contains	optional	Free-text filter by K8s version (supports multiple values)
lastactivedate__between	optional	Date range for last active date(format: <from_timestamp>-<to_timestamp>, inclusive). Example: "1514978764288-1514978999999".
lastactivedate__gt	optional	Agents last active after this time. Example: "2018-02-27T04:49:26.257525Z".
lastactivedate__gte	optional	Agents last active after or at this time. Example: "2018-02-27T04:49:26.257525Z".
lastactivedate__lt	optional	Agents last active before this time. Example: "2018-02-27T04:49:26.257525Z".
lastactivedate__lte	optional	Agents last active before or at this time. Example: "2018-02-27T04:49:26.257525Z".
lastloggedinusername_	optional	Free-text filter by username (supports multiple values). Example:

_contains		"admin,johnd1".
lastsuccessfulscandate__between	optional	Date range for last successful full disk scan(format: <from_timestamp>-<to_timestamp>, inclusive). Example: "1514978764288-1514978999999".
lastsuccessfulscandate__gt	optional	Agents last successful full disk scan after this time. Example: "2018-02-27T04:49:26.257525Z".
lastsuccessfulscandate__gte	optional	Agents last successful full disk scan after or at this time. Example: "2018-02-27T04:49:26.257525Z".
lastsuccessfulscandate__lt	optional	Agents last successful full disk scan before this time. Example: "2018-02-27T04:49:26.257525Z".
lastsuccessfulscandate__lte	optional	Agents last successful full disk scan before or at this time. Example: "2018-02-27T04:49:26.257525Z".
liveupdateid__contains	optional	Free-text filter by live update ID (supports multiple values)
locationenabled	optional	The agents supports Location Awareness and it is enabled for the agent's group
locationids	optional	Include only Agents reporting these locations. Example: "225494730938493804,225494730938493915".
locationidsnin	optional	Do not include only Agents reporting these locations. Example: "225494730938493804,225494730938493915".
machinetypes	optional	Included machine types. Example: "laptop,desktop".
machinetypesnin	optional	Not included machine types. Example: "laptop,desktop".
migrationstatus	optional	Migration status. Example: "N/A".
missingpermissions	optional	Included missing permissions. Example: "user_action_needed_bluetooth_per,user_action_needed_fda_helper".
missingpermissionsnin	optional	Excluded missing permissions. Example: "user_action_needed_bluetooth_per,user_action_needed_fda_helper".
mitigationmode	optional	Agent mitigation mode policy. Example: "detect".
mitigationmodesuspicious	optional	Mitigation mode policy for suspicious activity. Example: "detect".
networkinterfacegatewaymacaddress__contains	optional	Free-text filter by Gateway MAC address (supports multiple values). Example: "aa:0f,:41:".

networkinterfaceinet__contains	optional	Free-text filter by local IP (supports multiple values). Example: "192,10.0.0".
networkinterfacephysical__contains	optional	Free-text filter by MAC address (supports multiple values). Example: "aa:0f,:41:".
networkquarantineenabled	optional	The agents supports Network Quarantine Control and its enabled for the agent's group
networkstatuses	optional	Included network statuses. Example: "connected,connecting".
networkstatusesnin	optional	Included network statuses. Example: "connected,connecting".
operationalstates	optional	Agent operational state
operationalstatesnin	optional	Do not include these Agent operational states
osarch	optional	OS architecture. Example: "32 bit".
ostypes	optional	Included OS types. Example: "macos".
ostypesnin	optional	Not included OS types. Example: "macos".
osversion__contains	optional	Free-text filter by OS full name and version (supports multiple values). Example: "Service Pack 1".
query	optional	A free-text search term, will match applicable attributes (sub-string match). Note: Device's physical addresses will be matched if they start with the search term only (no match if they contain the term). Example: "Linux".
rangerstatus	optional	[DEPRECATED] Use rangerStatuses. Example: "NotApplicable".
rangerstatuses	optional	Status of Ranger. Example: "NotApplicable".
rangerstatusesnin	optional	Do not include these Ranger Statuses. Example: "NotApplicable".
rangerversions	optional	Ranger versions to include. Example: "2.0.0.0,2.1.5.144".
rangerversionsnin	optional	Ranger versions not to include. Example: "2.0.0.0,2.1.5.144".
registeredat__between	optional	Date range for first registration time (format: <from_timestamp>-<to_timestamp>, inclusive). Example: "1514978764288-1514978999999".
registeredat__gt	optional	Agents registered after this time. Example: "2018-02-27T04:49:26.257525Z".
registeredat__gte	optional	Agents registered after or at this time. Example: "2018-02-27T04:49:26.257525Z".
registeredat__lt	optional	Agents registered before this time. Example: "2018-02-27T04:49:26.257525Z".

registeredat__lte	optional	Agents registered before or at this time. Example: "2018-02-27T04:49:26.257525Z".
remoteopsforensicssupported	optional	Include only agents that has Remote Ops Forensicsfeature supported
remoteprofilingstates	optional	Agent remote profiling state
remoteprofilingstatesnin	optional	Do not include these Agent remote profiling states
rsolevel	optional	Supported Remote Script Orchestration level. Example: "none".
scanstatus	optional	Scan status. Example: "none".
scanstatuses	optional	Included scan statuses. Example: "started,aborted".
scanstatusesnin	optional	Not included scan statuses. Example: "started,aborted".
serialnumber__contains	optional	Free-text filter by Serial Number (supports multiple values)
siteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".
tagsdata	optional	Filter agents by their assigned tags. Given in form of a JSON where each key represents a tag key, and each value represents a list of string values to filter by. To filter by unassigned tag values, use __nin suffix in the tag key. Example: "{"key1": ["value1_1", "value1_2"], "key2__nin": ["value2"]}".
threatcontenthash	optional	Include only Agents that have at least one threat with this content hash. Example: "cf23df2207d99a74fbe169e3eba035e633b65d94".
threatcreatedat__between	optional	Agents with threats reported in a date range (format: <from_timestamp>-<to_timestamp>, inclusive). Example: "1514978764288-1514978999999".
threatcreatedat__gt	optional	Agents with threats reported after this time. Example: "2018-02-27T04:49:26.257525Z".
threatcreatedat__gte	optional	Agents with threats reported after or at this time. Example: "2018-02-27T04:49:26.257525Z".
threatcreatedat__lt	optional	Agents with threats reported before this time. Example: "2018-02-27T04:49:26.257525Z".
threatcreatedat__lte	optional	Agents with threats reported before or at this time. Example: "2018-02-27T04:49:26.257525Z".
threathidden	optional	Include only Agents with at least one hidden threat

threatmitigationstatus	optional	Include only Agents that have threats with this mitigation status. Example: "mitigated".
threatrebootrequired	optional	Has at least one threat with at least one mitigation action pending reboot to succeed
threatresolved	optional	Include only Agents with at least one resolved threat
totalmemory__between	optional	Total memory range (GB, inclusive). Example: "4-8".
totalmemory__gt	optional	Memory size (MB, more than)
totalmemory__gte	optional	Memory size (MB, more than or equal)
totalmemory__lt	optional	Memory size (MB, less than)
totalmemory__lte	optional	Memory size (MB, less than or equal)
updatedat__between	optional	Date range for update time (format: <from_timestamp>-<to_timestamp>, inclusive). Example: "1514978890136-1514978650130".
updatedat__gt	optional	Agents updated after this timestamp. Example: "2018-02-27T04:49:26.257525Z".
updatedat__gte	optional	Agents updated after or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
updatedat__lt	optional	Agents updated before this timestamp. Example: "2018-02-27T04:49:26.257525Z".
updatedat__lte	optional	Agents updated before or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
useractionsneeded	optional	Included pending user actions. Example: "reboot_needed,upgrade_needed".
useractionsneedednin	optional	Excluded pending user actions. Example: "reboot_needed,upgrade_needed".
uuid	optional	Agent's universally unique identifier. Example: "ff819e70af13be381993075eb0ce5f2f6de05be2".
uuid__contains	optional	Free-text filter by Agent UUID (supports multiple values). Example: "e92-01928,b055".
uuids	optional	A list of included UUIDs. Example: "ff819e70af13be381993075eb0ce5f2f6de05b11,ff819e70af13be381993075eb0ce5f2f6de05c22".

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Agents Repository (Beta)

List Access Tokens

GET /web/api/v2.1/agent-artifacts/token

Lists valid access tokens for the S1 Agent Artifacts Repository, with the option to filter by scope

Parameters

scope_id	optional	Scope id to list the tokens for, example: '983604236220743370'
scope_level	optional	Scope level to list the tokens for. Possible values: 'site', 'account'

Response Messages

200 - OK

400 - Invalid request

401 - Unauthorized

500 - Internal error

Response Schema

Name	Description	Required	Value
data	List of existing tokens	false	undefined []

Create Access Token

POST /web/api/v2.1/agent-artifacts/token

Creates an access token for the S1 Agent Artifacts Repository, which is needed for pulling artifacts

Response Messages

200 - OK

400 - Invalid request

401 - Unauthorized

500 - Internal Error

Response Schema

Name	Description	Required	Value
created_at	Created At timestamp of the token	false	string
description	Token description	false	string
id	Access token ID	false	integer
scope_id	Scope ID	false	string
scope_level	Scope level of the token	false	string
title	Token name	false	string
token	Access token - seen only once	false	string
username	Username of the token	false	string

Body Schema

Name	Description	Required	Value
description	Token description	false	string
scope_id	Scope ID of the specified account or site	false	string
scope_level	Scope Level of the token e.g. `account`, `site`	false	string
title	Token title	false	string

Delete Access Token

DELETE /web/api/v2.1/agent-artifacts/token

Deletes an access token for the S1 Agent Artifacts Repository

Parameters

scope_id	optional	Scope id to list the tokens for, example: '983604236220743370'
scope_level	optional	Scope level to list the tokens for. Possible values: 'site', 'account'
token_id	optional	token id of the token to be deleted, example: '42'

Response Messages

200 - Token deleted

400 - Invalid request

401 - Unauthorized

404 - Not found

500 - Internal error

alerts

Get alerts

GET /web/api/v2.1/cloud-detection/alerts

Get a list of alerts for a given scope

Parameters

accountids	optional	List of Account IDs to filter by. Example: "225494730938493804,225494730938493915".

analystverdict	optional	Filter threats by a analyst verdict. Example: "TRUE_POSITIVE".
containerimagename__contains	optional	Free-text filter by the endpoint container image name (supports multiple values)
containerlabels__contains	optional	Free-text filter by the endpoint container labels (supports multiple values)
containername__contains	optional	Free-text filter by the endpoint container name (supports multiple values)
countonly	optional	If true, only total number of items will be returned, without any of the actual objects.
createdat__gt	optional	Created at greater than. Example: "2018-02-27T04:49:26.257525Z".
createdat__gte	optional	Created at greater or equal than. Example: "2018-02-27T04:49:26.257525Z".
createdat__lt	optional	Created at lesser than. Example: "2018-02-27T04:49:26.257525Z".
createdat__lte	optional	Created at lesser or equal than. Example: "2018-02-27T04:49:26.257525Z".
cursor	optional	Cursor position returned by the last request. Use to iterate over more than 1000 items. Example: "YWdlbnRfaWQ6NTgwMjkzODE=".
disablepagination	optional	If true, all rules for requested scope will be returned
groupids	optional	List of Group IDs to filter by. Example: "225494730938493804,225494730938493915".
ids	optional	A list of Alert IDs. Example: "225494730938493804,225494730938493915".
incidentstatus	optional	Filter threats by a incident status. Example: "IN_PROGRESS".
k8scluster__contains	optional	Free-text filter by the endpoint Kubernetes cluster name (supports multiple values)
k8scontrollerlabels__contains	optional	Free-text filter by the endpoint Kubernetes controller labels (supports multiple values)
k8scontrollername__contains	optional	Free-text filter by the endpoint Kubernetes controller name (supports multiple values)
k8snamespacelabels__contains	optional	Free-text filter by the endpoint Kubernetes namespace labels (supports multiple values)
k8snamespacename__c	optional	Free-text filter by the endpoint Kubernetes namespace name

ontains		(supports multiple values)
k8snode__contains	optional	Free-text filter by the endpoint Kubernetes node name (supports multiple values)
k8spod__contains	optional	Free-text filter by the endpoint Kubernetes pod name (supports multiple values)
k8spodlabels__contains	optional	Free-text filter by the endpoint Kubernetes pod labels (supports multiple values)
limit	optional	Limit number of returned items (1-1000). Example: "10".
machinetype	optional	agent machine type
origagentname__contains	optional	Free-text filter by agent name. Example: "ilia".
origagentosrevision__contains	optional	Free-text filter by agent OS revision. Example: "win7".
origagentuuid__contains	optional	Free-text filter by agent UUID. Example: "win7".
origagentversion__contains	optional	Free-text filter by agent OS version. Example: "7.11".
ostype	optional	Included OS types
query	optional	Full text search for all fields
reportedat__gt	optional	Reported at greater than. Example: "2018-02-27T04:49:26.257525Z".
reportedat__gte	optional	Reported at greater or equal than. Example: "2018-02-27T04:49:26.257525Z".
reportedat__lt	optional	Reported at lesser than. Example: "2018-02-27T04:49:26.257525Z".
reportedat__lte	optional	Reported at lesser or equal than. Example: "2018-02-27T04:49:26.257525Z".
rulename__contains	optional	Free-text filter by rule name. Example: "rule1".
scopes	optional	Filter results by scope. Example: "account".
severity	optional	Severity. Example: "Low".
siteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".
skip	optional	Skip first number of items (0-1000). To iterate over more than 1000

		items, use "cursor". Example: "150".
skipcount	optional	If true, total number of items will not be calculated, which speeds up execution time.
sortby	optional	The column to sort the results by. Example: "id".
sortorder	optional	Sort direction. Example: "asc".
sourceprocesscommandline__contains	optional	Free-text filter by source commandline. Example: "rule1".
sourceprocessfilehashmd5__contains	optional	Free-text filter by source md5. Example: "rule1".
sourceprocessfilehashsha1__contains	optional	Free-text filter by source sha1. Example: "rule1".
sourceprocessfilehashsha256__contains	optional	Free-text filter by source sha255. Example: "rule1".
sourceprocessfilepath__contains	optional	Free-text filter by source file path. Example: "rule1".
sourceprocessname__contains	optional	Free-text filter by source process name. Example: "proc1.exe".
sourceprocessstoryline__contains	optional	Free-text filter by source storyline. Example: "rule1".
tenant	optional	Indicates a tenant scope request

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
pagination	Pagination information	true	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>totalItems</td><td>Total number of items found</td><td>true</td><td>integer</td></tr></table>

				matching your query		
			nextCursor	Pass this value as "cursor" on your next request, to get the next page of results (Will be "null" when last page reached)	false	string
data	Response data	false	Name	Description	Required	Value
			agentDetectionInfo	Agent detection time information	false	

Name	Description	Required	Value
accountId	Account id	false	string
machineType	Machine type	false	string
name	Name	false	string
osFamily	Os family	false	string
osName	Os name	false	string
osRevision	Os revision	false	string
siteId	Site id	false	string
uuid	UUID of the agent	false	string
version	Version	false	string

alertInfo	Alert information	false	

Name	Description	Required	Value
alertId	Alert ID	false	string
analystVerdict	Analyst verdict	false	enum
createdAt	Timestamp alert sent for detection	false	string
dnsRequest	Get the DNS name.	false	string

						dnsResponse	Get the DNS response information (examples: IP address, DNS, data type).	false	string		
						dstIp	Get the IP address of the destination.	false	string		
						dstPort	Get the port number of the destination.	false	string		
						dvEventId	Deep Visibility event ID	false	string		
						eventType	Event type	false	string		
						hitType	Type of hit reported from the Agent	false	enum		
						incidentStatus	Incident status	false	enum		
						indicatorCategory	Get the Indicator categories for this process.	false	string		
						indicatorDescription	Get the description of the Indicator.	false	string		
						indicatorName	Get the Indicator names for this process.	false	string		
						isEdr	True if the event is edr event	false	boolean		
						loginAccoun	Get the	false	string		

							tDomain	domain or computer name for which the login attempt was performed.						
							loginAccountSid	Get the SID of the account that attempted to log in.	false	string				
							loginIsAdministratorEquivalent	See if the login attempt was performed by an administrator equivalent.	false	string				
							loginIsSuccessful	Check if the login attempt succeeded.	false	string				
							loginsUserName	Get the login username.	false	string				
							loginType	Get the type of login that was performed.	false	string				
							modulePath	Get the paths of modules loaded by this process.	false	string				
							moduleSha1	Get the SHA1 signatures for modules loaded by this process.	false	string				
							netEventDirection	Get the direction of the connection	false	string				

								attempt (incoming or outgoing).				
							registryKeyPath	Get the full paths of registry entries modified by this process.	false	string		
							registryOldValue	Get the previous registry value if it was modified.	false	string		
							registryOldValueType	Get the previous registry value type if it was modified.	false	string		
							registryPath	Get the full path location of the registry key entry.	false	string		
							registryValue	Get the registry value	false	string		
							reportedAt	Timestamp of alert creation in STAR	false	string		
							source	Source reported from the Agent.	false	string		
							srcIp	Get the IP address of the traffic source.	false	string		
							srcMachineIp	Get the IP address of the endpoint performing	false	string		

							the login attempt.		
						srcPort	Get the port number of the traffic source.	false	string
						tiIndicatorComparisonMethod	Get the comparison method used by SentinelOne to trigger the event.	false	string
						tiIndicatorSource	Get the source of the identified Threat Intelligence indicator.	false	string
						tiIndicatorType	Get the type of the identified Threat Intelligence indicator.	false	string
						tiIndicatorValue	Get the value of the identified Threat Intelligence indicator.	false	string
						updatedAt	Date of alert updated in Star MMS	false	string
				containerInfo	Alert container information	false			
						id	Id	false	string
						image	Image	false	string
						labels	Labels	false	string
						name	Name	false	string

			kubernetesInfo	Alert kubernetes information	false

Name	Description	Required	Value
cluster	Cluster	false	string
controllerKind	Controller kind	false	string
controllerLabels	Controller labels	false	string
controllerName	Controller name	false	string
namespace	Namespace	false	string
namespaceLabels	Namespace labels	false	string
node	Node	false	string
pod	Pod	false	string
podLabels	Pod labels	false	string

			ruleInfo	Custom Detection rules like STAR indicators information	false

Name	Description	Required	Value
s1ql	The query	true	string
description	Rule description for the STAR alert	false	string
id	Rule ID for the STAR alert	false	string
name	Rule name for the STAR alert	false	string
queryLang	Defines the s1ql version query language of the rule (1.0/2.0)	false	enum
queryType	The query type	false	enum
scopeLevel	Scope level	false	enum
severity	Rule severity	false	enum

						treatAsThreat	Rule treat as threat type	false	enum
			sourceParent ProcessInfo	Source parent process info	false				
						Name	Description	Required	Value
						integrityLevel	Integrity level	true	enum
						subsystem	Subsystem	true	enum
						commandline	Commandline	false	string
						effectiveUser	Effective user	false	string
						fileHashMd5	File hash md5	false	string
						fileHashSha1	File hash sha1	false	string
						fileHashSha256	File hash sha256	false	string
						filePath	File path	false	string
						fileSignerIdentity	File signer identity	false	string
						loginUser	Login user	false	string
						name	Name	false	string
						pid	Pid	false	string
						pidStarttime	Pid starttime	false	string
						realUser	Real user	false	string
						storyline	Storyline	false	string
						uniqueId	Unique id	false	string
						user	User	false	string
			sourceProcess Info	Source process info	false				
						Name	Description	Required	Value
						integrityLevel	Integrity level	true	enum
						subsystem	Subsystem	true	enum
						commandline	Commandline	false	string
						effectiveUser	Effective user	false	string
						fileHashMd5	File hash md5	false	string
						fileHashSha1	File hash sha1	false	string
						fileHashSha2	File hash	false	string

						56	sha256			
						filePath	File path	false	string	
						fileSignerIdentity	File signer identity	false	string	
						loginUser	Login user	false	string	
						name	Name	false	string	
						pid	Pid	false	string	
						pidStarttime	Pid starttime	false	string	
						realUser	Real user	false	string	
						storyline	Storyline	false	string	
						uniqueId	Unique id	false	string	
						user	User	false	string	
				targetProcessInfo	Target process info	false	Name	Description	Required	Value
							tgtFileCreatedAt	Date and Time of File Creation	false	string
							tgtFileHashSha1	SHA1 Signature of File	false	string
							tgtFileHashSha256	SHA256 Signature of File	false	string
							tgtFileId	Unique ID of file	false	string
							tgtFileIsSigned	Is file signed	false	string
							tgtFileModifiedAt	Date and time file was modified	false	string
							tgtFileOldPath	Old path before 'Rename'	false	string
							tgtFilePath	Path and filename	false	string
							tgtProcCmdLi	Target	false	string

						ne	Process Command Line		
						tgtProcessStartTime	Target Process Start Time	false	string
						tgtProcImagePath	Target Process Image path	false	string
						tgtProcIntegrityLevel	Integrity level of target process	false	enum
						tgtProcName	Target Process Name	false	string
						tgtProcPid	Target Process ID (PID)	false	string
						tgtProcSignedStatus	Target Process Signed Status	false	string
						tgtProcStorylineId	Target Process StoryLine ID	false	string
						tgtProcUid	Target Process Unique ID	false	string
errors	Errors	false	array						

Update Threat Incident

POST /web/api/v2.1/cloud-detection/alerts/incident

Update the incident details of an alert.

Response Messages

200 - Threats incident successfully updated

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>affected</td><td>Number of entities affected by the requested operation</td><td>false</td><td>integer</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>incidentStatus</td><td>Incident status</td><td>true</td><td>enum</td></tr>
</table>
</td></tr>
<tr><td>filter</td><td>Filter</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>analystVerdict</td><td>Filter threats by a analyst verdict</td><td>false</td><td>string []</td></tr>
<tr><td>containerImageName__contains</td><td>Free-text filter by the endpoint container image name (supports multiple values)</td><td>false</td><td>string []</td></tr>
<tr><td>containerLabels__contains</td><td>Free-text filter by the endpoint container labels (supports multiple values)</td><td>false</td><td>string []</td></tr>
<tr><td>containerName__contains</td><td>Free-text filter by the endpoint container name (supports multiple values)</td><td>false</td><td>string []</td></tr>
<tr><td>createdAt__gt</td><td>Created at greater than.</td><td>false</td><td>string</td></tr>
<tr><td>createdAt__g</td><td>Created at</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
</table>

			te	greater or equal than.		
			createdAt__lt	Created at lesser than.	false	string
			createdAt__lte	Created at lesser or equal than.	false	string
			groupIds	List of Group IDs to filter by	false	string []
			ids	A list of Alert IDs	false	string []
			incidentStatus	Filter threats by a incident status	false	string []
			k8sCluster__contains	Free-text filter by the endpoint Kubernetes cluster name (supports multiple values)	false	string []
			k8sControllerLabels__contains	Free-text filter by the endpoint Kubernetes controller labels (supports multiple values)	false	string []
			k8sControllerName__contains	Free-text filter by the endpoint Kubernetes controller name (supports multiple values)	false	string []
			k8sNamespace	Free-text	false	string []

			Labels__contains	filter by the endpoint Kubernetes namespace labels (supports multiple values)		
			k8sNamespaceName__contains	Free-text filter by the endpoint Kubernetes namespace name (supports multiple values)	false	string []
			k8sNode__contains	Free-text filter by the endpoint Kubernetes node name (supports multiple values)	false	string []
			k8sPod__contains	Free-text filter by the endpoint Kubernetes pod name (supports multiple values)	false	string []
			k8sPodLabels__contains	Free-text filter by the endpoint Kubernetes pod labels (supports multiple values)	false	string []
			limit	Limit	false	integer
			machineType	agent	false	string []

				machine type		
			origAgentName__contains	Free-text filter by agent name	false	string []
			origAgentOsRevision__contains	Free-text filter by agent OS revision	false	string []
			origAgentUuid__contains	Free-text filter by agent UUID	false	string []
			origAgentVersion__contains	Free-text filter by agent OS version	false	string []
			osType	Included OS types	false	string []
			query	Full text search for all fields	false	string
			reportedAt__gt	Reported at greater than.	false	string
			reportedAt__gte	Reported at greater or equal than.	false	string
			reportedAt__lt	Reported at lesser than.	false	string
			reportedAt__lte	Reported at lesser or equal than.	false	string
			ruleName__contains	Free-text filter by rule name	false	string []
			scopes	Filter results by scope	false	string []
			severity	Severity	false	string []
			siteIds	List of Site IDs to filter by	false	string []
			sourceProcessCommandline	Free-text filter by	false	string []

			__contains	source commandline		
			sourceProcessFileHashMd5__contains	Free-text filter by source md5	false	string []
			sourceProcessFileHashSha1__contains	Free-text filter by source sha1	false	string []
			sourceProcessFileHashSha256__contains	Free-text filter by source sha255	false	string []
			sourceProcessFilePath__contains	Free-text filter by source file path	false	string []
			sourceProcessName__contains	Free-text filter by source process name	false	string []
			sourceProcessStoryline__contains	Free-text filter by source storyline	false	string []
			tenant	Indicates a tenant scope request	false	boolean

Update Alert Analyst Verdict

POST /web/api/v2.1/cloud-detection/alerts/analyst-verdict

Change the verdict of an alert

Response Messages

200 - Threats incident successfully updated

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>affected</td><td>Number of entities affected by the requested operation</td><td>false</td><td>integer</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>analystVerdict</td><td>Analyst verdict</td><td>true</td><td>enum</td></tr>
</table>
</td></tr>
<tr><td>filter</td><td>Filter</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>analystVerdict</td><td>Filter threats by a analyst verdict</td><td>false</td><td>string []</td></tr>
<tr><td>containerImageName__contains</td><td>Free-text filter by the endpoint container image name (supports multiple values)</td><td>false</td><td>string []</td></tr>
<tr><td>containerLabels__contains</td><td>Free-text filter by the endpoint container labels (supports multiple values)</td><td>false</td><td>string []</td></tr>
<tr><td>containerName__contains</td><td>Free-text filter by the endpoint container name (supports multiple values)</td><td>false</td><td>string []</td></tr>
<tr><td>createdAt__gt</td><td>Created at greater than.</td><td>false</td><td>string</td></tr>
<tr><td>createdAt__g</td><td>Created at</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
</table>

			te	greater or equal than.		
			createdAt__lt	Created at lesser than.	false	string
			createdAt__lte	Created at lesser or equal than.	false	string
			groupIds	List of Group IDs to filter by	false	string []
			ids	A list of Alert IDs	false	string []
			incidentStatus	Filter threats by a incident status	false	string []
			k8sCluster__contains	Free-text filter by the endpoint Kubernetes cluster name (supports multiple values)	false	string []
			k8sControllerLabels__contains	Free-text filter by the endpoint Kubernetes controller labels (supports multiple values)	false	string []
			k8sControllerName__contains	Free-text filter by the endpoint Kubernetes controller name (supports multiple values)	false	string []
			k8sNamespace	Free-text	false	string []

			Labels__contains	filter by the endpoint Kubernetes namespace labels (supports multiple values)		
			k8sNamespaceName__contains	Free-text filter by the endpoint Kubernetes namespace name (supports multiple values)	false	string []
			k8sNode__contains	Free-text filter by the endpoint Kubernetes node name (supports multiple values)	false	string []
			k8sPod__contains	Free-text filter by the endpoint Kubernetes pod name (supports multiple values)	false	string []
			k8sPodLabels__contains	Free-text filter by the endpoint Kubernetes pod labels (supports multiple values)	false	string []
			limit	Limit	false	integer
			machineType	agent	false	string []

				machine type		
			origAgentName__contains	Free-text filter by agent name	false	string []
			origAgentOsRevision__contains	Free-text filter by agent OS revision	false	string []
			origAgentUuid__contains	Free-text filter by agent UUID	false	string []
			origAgentVersion__contains	Free-text filter by agent OS version	false	string []
			osType	Included OS types	false	string []
			query	Full text search for all fields	false	string
			reportedAt__gt	Reported at greater than.	false	string
			reportedAt__gte	Reported at greater or equal than.	false	string
			reportedAt__lt	Reported at lesser than.	false	string
			reportedAt__lte	Reported at lesser or equal than.	false	string
			ruleName__contains	Free-text filter by rule name	false	string []
			scopes	Filter results by scope	false	string []
			severity	Severity	false	string []
			siteIds	List of Site IDs to filter by	false	string []
			sourceProcessCommandline	Free-text filter by	false	string []

			__contains	source commandline		
			sourceProcessFileHashMd5__contains	Free-text filter by source md5	false	string []
			sourceProcessFileHashSha1__contains	Free-text filter by source sha1	false	string []
			sourceProcessFileHashSha256__contains	Free-text filter by source sha255	false	string []
			sourceProcessFilePath__contains	Free-text filter by source file path	false	string []
			sourceProcessName__contains	Free-text filter by source process name	false	string []
			sourceProcessStoryline__contains	Free-text filter by source storyline	false	string []
			tenant	Indicates a tenant scope request	false	boolean

Application Management

Inventory Endpoints Data Export

GET /web/api/v2.1/application-management/inventory/endpoints/export/csv

Export application inventory endpoints data to CSV.

Parameters

applicationname	required	Name
applicationvendor	required	Vendor
accountids	optional	Single Account ID to filter by. Example: "225494730938493804".
detectiondate__between	optional	Date range for application detection date(format: <from_timestamp>-<to_timestamp>, inclusive). Example: "1514978890136-1514978650130".
detectiondate__gt	optional	Application detection date after this timestamp. Example: "2018-02-27T04:49:26.257525Z".
detectiondate__gte	optional	Application detection date after or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
detectiondate__lt	optional	Application detection date before this timestamp. Example: "2018-02-27T04:49:26.257525Z".
detectiondate__lte	optional	Application detection date before or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
endpointname__contains	optional	Free-text filter by endpoint name (supports multiple values). Example: "Office,Test".
endpointuuid__contains	optional	Free-text filter by endpoint uuid (supports multiple values)
groupids	optional	Single Group ID to filter by. Example: "225494730938493804".
osarchitectures	optional	Included OS architectures
ostypes	optional	Included OS types
osversions	optional	Included OS versions
siteids	optional	Single Site ID to filter by. Example: "225494730938493804".

versions	optional	Included application versions

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - Insufficient permissions

Aggregated Application Risk Data Export

GET /web/api/v2.1/application-management/risks/aggregated-applications/export/csv

Export aggregated application data to CSV.

Parameters

accountids	optional	Single Account ID to filter by. Example: "225494730938493804".
applicationtypes	optional	Application type. Available with Ranger Insights. Example: "A,p,p,l,i,c,a,t,i,o,n".
cveid__contains	optional	Free-text filter by CVE id (supports multiple values). Example: "CVE-1234-5678".
daysfromdetection	optional	Days from application detection, e.g. 12 days or more. Example: "12".
detectiondate__between	optional	Date range for application detection date(format: <from_timestamp>-<to_timestamp>, inclusive). Example: "1514978890136-1514978650130".
detectiondate__gt	optional	Application detection date after this timestamp. Example: "2018-02-27T04:49:26.257525Z".
detectiondate__gte	optional	Application detection date after or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
detectiondate__lt	optional	Application detection date before this timestamp. Example: "2018-02-27T04:49:26.257525Z".
detectiondate__lte	optional	Application detection date before or at this timestamp. Example:

		"2018-02-27T04:49:26.257525Z".
domains	optional	Included domains.
endpointname__contains	optional	Free-text filter by endpoint name (supports multiple values). Example: "Office,Test".
endpointtypes	optional	Included endpoint types. Example: "desktop,laptop".
endpointuuid__contains	optional	Free-text filter by endpoint uuid (supports multiple values)
exploitcodematurity	optional	Included exploit code maturity values. Available with Ranger Insights. Example: "Functional,High".
exploitedinthewild	optional	Included exploited in the wild values. Available with Ranger Insights. Example: "Unknown,Yes".
groupids	optional	Single Group ID to filter by. Example: "225494730938493804".
highestseverities	optional	Included highest severities. Example: "CRITICAL,HIGH".
mostcommonstatuses	optional	Included most common status values. Available with Ranger Insights.
name__contains	optional	Free-text filter by application name (supports multiple values). Example: "Office 1.1,Test".
ostypes	optional	Included OS types. Example: "windows,linux".
remediationlevels	optional	Included remediation level values. Available with Ranger Insights. Example: "Official Fix,Temporary Fix".
siteids	optional	Single Site ID to filter by. Example: "225494730938493804".
vendor__contains	optional	Free-text filter by vendor (supports multiple values). Example: "Microsoft,Apple".
vendors	optional	Included vendors. Example: "Microsoft,Apple".

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - Insufficient permissions

Application Risk Data Export

GET /web/api/v2.1/application-management/risks/applications/export/csv

Export application data to CSV.

Parameters

accountids	optional	Single Account ID to filter by. Example: "225494730938493804".
application__contains	optional	Free-text filter by application name and version (supports multiple values). Example: "Office 1.1,Test".
applicationtypes	optional	Application type. Available with Ranger Insights. Example: "A,p,p,l,i,c,a,t,i,o,n".
cveid__contains	optional	Free-text filter by CVE id (supports multiple values). Example: "CVE-1234-5678".
daysfromdetection	optional	Days from application detection, e.g. 12 days or more. Example: "12".
detectiondate__between	optional	Date range for application detection date(format: <from_timestamp>-<to_timestamp>, inclusive). Example: "1514978890136-1514978650130".
detectiondate__gt	optional	Application detection date after this timestamp. Example: "2018-02-27T04:49:26.257525Z".
detectiondate__gte	optional	Application detection date after or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
detectiondate__lt	optional	Application detection date before this timestamp. Example: "2018-02-27T04:49:26.257525Z".
detectiondate__lte	optional	Application detection date before or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
domains	optional	Included domains.
endpointname__contains	optional	Free-text filter by endpoint name (supports multiple values). Example: "Office,Test".
endpointtypes	optional	Included endpoint types. Example: "desktop,laptop".
endpointuuid__contains	optional	Free-text filter by endpoint uuid (supports multiple values)
exploitcodematurity	optional	Included exploit code maturity values. Available with Ranger Insights. Example: "Functional,High".
exploitedinthewild	optional	Included exploited in the wild values. Available with Ranger Insights. Example: "Unknown,Yes".

groupids	optional	Single Group ID to filter by. Example: "225494730938493804".
highestseverities	optional	Included highest severities. Example: "CRITICAL,HIGH".
mostcommonstatuses	optional	Included most common status values. Available with Ranger Insights.
ostypes	optional	Included OS types. Example: "windows,linux".
remediationlevels	optional	Included remediation level values. Available with Ranger Insights. Example: "Official Fix,Temporary Fix".
siteids	optional	Single Site ID to filter by. Example: "225494730938493804".
vendor__contains	optional	Free-text filter by vendor (supports multiple values). Example: "Microsoft,Apple".
vendors	optional	Included vendors. Example: "Microsoft,Apple".

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - Insufficient permissions

Risk Endpoint Data Export

GET /web/api/v2.1/application-management/risks/endpoints/export/csv

Export endpoint data to CSV.

Parameters

accountids	optional	Single Account ID to filter by. Example: "225494730938493804".
applicationids	optional	Included application versions by id
applicationname	optional	Application name
applicationvendor	optional	Application vendor
applicationversions	optional	Included application versions
daysfromdetection	optional	Days from application detection, e.g. 12 days or more. Example: "12".

daystomitigation__between	optional	Date range for days left to mitigation. Available with Ranger Insights when using ticket integration. Example: "1-30".
detectiondate__between	optional	Date range for application detection date(format: <from_timestamp>-<to_timestamp>, inclusive). Example: "1514978890136-1514978650130".
detectiondate__gt	optional	Application detection date after this timestamp. Example: "2018-02-27T04:49:26.257525Z".
detectiondate__gte	optional	Application detection date after or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
detectiondate__lt	optional	Application detection date before this timestamp. Example: "2018-02-27T04:49:26.257525Z".
detectiondate__lte	optional	Application detection date before or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
domain__contains	optional	Free-text filter by domain (supports multiple values). Example: "mybusiness,workgroup".
domains	optional	Included endpoint domains
endpointid__contains	optional	Free-text filter by endpoint id (supports multiple values)
endpointname__contains	optional	Free-text filter by endpoint name (supports multiple values). Example: "Office,Test".
endpointtypes	optional	Included endpoint types
endpointuuid__contains	optional	Free-text filter by endpoint uuid (supports multiple values)
groupids	optional	Single Group ID to filter by. Example: "225494730938493804".
lastscandate__between	optional	Date range for last scan date(format: <from_timestamp>-<to_timestamp>, inclusive). Example: "1514978890136-1514978650130".
lastscandate__gt	optional	Last scan date after this timestamp. Example: "2018-02-27T04:49:26.257525Z".
lastscandate__gte	optional	Last scan date after or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
lastscandate__lt	optional	Last scan date before this timestamp. Example: "2018-02-27T04:49:26.257525Z".
lastscandate__lte	optional	Last scan date before or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".

lastscanresults	optional	Included last scan results. Example: "Succeeded".
ostypes	optional	Included OS types
osversions	optional	Included OS versions
siteids	optional	Single Site ID to filter by. Example: "225494730938493804".
statuses	optional	Included statuses. Available with Ranger Insights.
statusmessage__contains	optional	Free-text filter by status message (supports multiple values). Available with Ranger Insights. Example: "assigned to john,top priority".
ticketid__contains	optional	Free-text filter by ticket id. Available with Ranger Insights when using ticket integration. Example: "ABC-123,ABCD-100".

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - Insufficient permissions

Application CVE Data Export

GET /web/api/v2.1/application-management/risks/cves/export/csv

Export CVE data to CSV.

Parameters

accountids	optional	Single Account ID to filter by. Example: "225494730938493804".
analystverdict	optional	Include Default(not edited)/ False Positives / Added CVEs for Vulnerabilities. Example: "Default,False Positive,Added CVE".
applicationids	optional	Included application versions by id
applicationname	optional	Application name
applicationvendor	optional	Application vendor
applicationversions	optional	Included application versions

cveid__contains	optional	Free-text filter by CVE id (supports multiple values). Example: "CVE-1234-5678".
exploitcodematurity	optional	Included exploit code maturity values. Available with Ranger Insights. Example: "FUNCTIONAL,HIGH".
exploitedinthewild	optional	Included exploited in the wild values. Available with Ranger Insights. Example: "EXPLOITED_UNKNOWN,YES".
groupids	optional	Single Group ID to filter by. Example: "225494730938493804".
publisheddate__between	optional	Date range for CVE publish date(format: <from_timestamp>-<to_timestamp>, inclusive). Example: "1514978890136-1514978650130".
publisheddate__gt	optional	CVE published date after this timestamp. Example: "2018-02-27T04:49:26.257525Z".
publisheddate__gte	optional	CVE published date after or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
publisheddate__lt	optional	CVE published date before this timestamp. Example: "2018-02-27T04:49:26.257525Z".
publisheddate__lte	optional	CVE published date before or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
remediationlevels	optional	Included remediation level values. Available with Ranger Insights. Example: "OFFICIAL_FIX,TEMPORARY_FIX".
reportconfidence	optional	Included report confidence values. Available with Ranger Insights. Example: "REASONABLE,CONFIRMED".
severities	optional	Included severities. Example: "CRITICAL,HIGH".
siteids	optional	Single Site ID to filter by. Example: "225494730938493804".

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - Insufficient permissions

Inventory Data Export

GET /web/api/v2.1/application-management/inventory/export/csv

Export application inventory data to CSV.

Parameters

accountids	optional	Single Account ID to filter by. Example: "225494730938493804".
endpointname__contains	optional	Free-text filter by endpoint name (supports multiple values). Example: "Office,Test".
endpointuuid__contains	optional	Free-text filter by endpoint uuid (supports multiple values)
groupids	optional	Single Group ID to filter by. Example: "225494730938493804".
name__contains	optional	Free-text filter by application name (supports multiple values). Example: "Office,Test".
osarchitectures	optional	Included OS architectures
ostypes	optional	Included OS types
osversion__contains	optional	Free-text filter by os version (supports multiple values). Example: "Windows 7 ServicePack1".
osversions	optional	Included OS versions
siteids	optional	Single Site ID to filter by. Example: "225494730938493804".
vendor__contains	optional	Free-text filter by vendor (supports multiple values). Example: "Microsoft,Apple".
vendors	optional	Included vendors. Example: "Microsoft,Apple".

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - Insufficient permissions

Risks Data Export

GET /web/api/v2.1/application-management/risks/export/csv

Export risks data to CSV.

Parameters

accountids	optional	Single Account ID to filter by. Example: "225494730938493804".
analystverdict	optional	Include Default(not edited)/ False Positives / Added CVEs for Vulnerabilities. Example: "Default,False Positive,Added CVE".
application__contains	optional	Free-text filter by application name and version (supports multiple values). Example: "Office 1.1,Test".
applicationnames	optional	Included application names. Example: "Office 1.1,Test".
applicationvendor__contains	optional	Free-text filter by vendor (supports multiple values). Example: "Microsoft,Apple".
cveid__contains	optional	Free-text filter by CVE id (supports multiple values). Example: "CVE-1234-5678".
daysfromcvedetection	optional	Days from CVE detection, e.g. 12 days or more. Example: "12".
detectiondate__between	optional	Date range for CVE detection date(format: <from_timestamp>-<to_timestamp>, inclusive). Example: "1514978890136-1514978650130".
detectiondate__gt	optional	CVE detection date after this timestamp. Example: "2018-02-27T04:49:26.257525Z".
detectiondate__gte	optional	CVE detection date after or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
detectiondate__lt	optional	CVE detection date before this timestamp. Example: "2018-02-27T04:49:26.257525Z".
detectiondate__lte	optional	CVE detection date before or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
domain__contains	optional	Free-text filter by domain (supports multiple values). Example: "mybusiness,workgroup".
domains	optional	Included network domains. Example: "mybusiness,workgroup".
endpointname__contains	optional	Free-text filter by endpoint name (supports multiple values). Example: "Office,Test".
endpointtypes	optional	Included endpoint types
exploitcodematurity	optional	Included exploit code maturity values. Available for VLN SKU. Example: "FUNCTIONAL,HIGH".
exploitedinthewild	optional	Included exploited in the wild values. Available for VLN SKU.

		Example: "EXPLOITED_UNKNOWN,YES".
groupids	optional	Single Group ID to filter by. Example: "225494730938493804".
includeremovals	optional	Include also removed CVEs in the results
lastscanresults	optional	Included last scan results. Example: "Succeeded".
mitigationstatus	optional	Filters by the application's mitigation status values.Available for VLN SKU. Example: "Not mitigated,To be patched,On hold".
ostypes	optional	Included OS types
osversions	optional	Included OS versions
publisheddate__between	optional	Date range for CVE publish date(format: <from_timestamp>-<to_timestamp>, inclusive). Example: "1514978890136-1514978650130".
publisheddate__gt	optional	CVE published date after this timestamp. Example: "2018-02-27T04:49:26.257525Z".
publisheddate__gte	optional	CVE published date after or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
publisheddate__lt	optional	CVE published date before this timestamp. Example: "2018-02-27T04:49:26.257525Z".
publisheddate__lte	optional	CVE published date before or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
remediationlevels	optional	Included remediation level values. Available for VLN SKU. Example: "OFFICIAL_FIX,TEMPORARY_FIX".
reportconfidence	optional	Included report confidence values. Available for VLN SKU. Example: "REASONABLE,CONFIRMED".
riskscore__between	optional	Risk score (inclusive). Available for VLN SKU. Example: "5-8.9".
riskupdateddate__between	optional	Significant CVE updates within this date range(format: <from_timestamp>-<to_timestamp>, inclusive). Example: "1514978890136-1514978650130".
riskupdateddate__gt	optional	Significant CVE updates after this timestamp. Example: "2018-02-27T04:49:26.257525Z".
riskupdateddate__gte	optional	Significant CVE updates after or at this timestamp. Recommended for fetching delta-changes. Example: "2018-02-27T04:49:26.257525Z".
riskupdateddate__lt	optional	Significant CVE updates before this timestamp. Example: "2018-02-27T04:49:26.257525Z".

riskupdateddate__lte	optional	Significant CVE updates before or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
severities	optional	Included severities. Example: "CRITICAL,HIGH".
siteids	optional	Single Site ID to filter by. Example: "225494730938493804".
vendors	optional	Included vendors. Example: "Microsoft,Apple".

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - Insufficient permissions

Get Endpoint Apps

GET /web/api/v2.1/application-management/inventory/applications

Get the installed applications for a specific endpoint.
To get the Agent ID, run "agents".

Parameters

ids	required	Agent ID list. Example: "225494730938493804,225494730938493915".

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value

<table>
<tr><td>data</td><td>Response data</td><td>false</td><td><table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>installedDate</td><td>Installed date</td><td>false</td><td>string</td></tr>
<tr><td>name</td><td>Name</td><td>false</td><td>string</td></tr>
<tr><td>publisher</td><td>Publisher</td><td>false</td><td>string</td></tr>
<tr><td>size</td><td>Size</td><td>false</td><td>integer</td></tr>
<tr><td>version</td><td>Version</td><td>false</td><td>string</td></tr>
</table></td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Get App Inventory Endpoints

GET /web/api/v2.1/application-management/inventory/endpoints

Get endpoint data for a specific application.

Parameters

applicationname	required	Name
applicationvendor	required	Vendor
accountids	optional	Single Account ID to filter by. Example: "225494730938493804".
countonly	optional	If true, only total number of items will be returned, without any of the actual objects.
cursor	optional	Cursor position returned by the last request. Use to iterate over more than 1000 items. Example: "YWdlbnRfaWQ6NTgwMjkzODE=".
detectiondate__between	optional	Date range for application detection date(format: <from_timestamp>-<to_timestamp>, inclusive). Example: "1514978890136-1514978650130".
detectiondate__gt	optional	Application detection date after this timestamp. Example: "2018-02-27T04:49:26.257525Z".
detectiondate__gte	optional	Application detection date after or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
detectiondate__lt	optional	Application detection date before this timestamp. Example: "2018-02-27T04:49:26.257525Z".
detectiondate__lte	optional	Application detection date before or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
endpointname__contains	optional	Free-text filter by endpoint name (supports multiple values). Example: "Office,Test".
endpointuuid__contains	optional	Free-text filter by endpoint uuid (supports multiple values)
groupids	optional	Single Group ID to filter by. Example: "225494730938493804".
limit	optional	Limit number of returned items (1-1000). Example: "10".
osarchitectures	optional	Included OS architectures
ostypes	optional	Included OS types

osversions	optional	Included OS versions
siteids	optional	Single Site ID to filter by. Example: "225494730938493804".
skip	optional	Skip first number of items (0-1000). To iterate over more than 1000 items, use "cursor". Example: "150".
skipcount	optional	If true, total number of items will not be calculated, which speeds up execution time.
sortby	optional	The column to sort the results by. Example: "id".
sortorder	optional	Sort direction. Example: "asc".
versions	optional	Included application versions

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - Insufficient permissions

Response Schema

Name	Description	Required	Value
pagination	Pagination information	true	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>totalItems</td><td>Total number of items found matching your query</td><td>true</td><td>integer</td></tr><tr><td>nextCursor</td><td>Pass this value as "cursor" on your next request, to get the next page of results (Will be "null" when last</td><td>false</td><td>string</td></tr></table>

			page reached)
data	Response data	false	

Name	Description	Required	Value
accountName	Account name	false	string
applicationInstallationDate	Application installation date	false	string
applicationInstallationPath	Application installation path	false	string
applicationName	Application name	false	string
coreCount	Core count	false	integer
cpe	Cpe	false	
cpuCount	Cpu count	false	integer
detectionDate	Detection date	false	string
endpointId	Endpoint id	false	string
endpointName	Endpoint name	false	string
endpointType	Endpoint type	false	string
endpointUuid	Endpoint uuid	false	string
fileSize	File size	false	integer
groupName	Group name	false	string
id	Id	false	string
osArch	Os arch	false	string
osName	Os name	false	string
osType	OS type	false	enum
osVersion	Os version	false	string
siteName	Site name	false	string
version	Version	false	string

errors	Errors	false	array

Get Aggregated Applications With Risk

GET /web/api/v2.1/application-management/risks/aggregated-applications

Get data for all applications. Available with Ranger Insights license.

Parameters

accountids	optional	Single Account ID to filter by. Example: "225494730938493804".
applicationtypes	optional	Application type. Available with Ranger Insights. Example: "A,p,p,l,i,c,a,t,i,o,n".
countonly	optional	If true, only total number of items will be returned, without any of the actual objects.
cursor	optional	Cursor position returned by the last request. Use to iterate over more than 1000 items. Example: "YWdlbnRfaWQ6NTgwMjkzODE=".
cveid__contains	optional	Free-text filter by CVE id (supports multiple values). Example: "CVE-1234-5678".
daysfromdetection	optional	Days from application detection, e.g. 12 days or more. Example: "12".
detectiondate__between	optional	Date range for application detection date(format: <from_timestamp>-<to_timestamp>, inclusive). Example: "1514978890136-1514978650130".
detectiondate__gt	optional	Application detection date after this timestamp. Example: "2018-02-27T04:49:26.257525Z".
detectiondate__gte	optional	Application detection date after or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
detectiondate__lt	optional	Application detection date before this timestamp. Example: "2018-02-27T04:49:26.257525Z".
detectiondate__lte	optional	Application detection date before or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
domains	optional	Included domains.
endpointname__contains	optional	Free-text filter by endpoint name (supports multiple values). Example: "Office,Test".
endpointtypes	optional	Included endpoint types. Example: "desktop,laptop".

endpointuuid__contains	optional	Free-text filter by endpoint uuid (supports multiple values)
exploitcodematurity	optional	Included exploit code maturity values. Available with Ranger Insights. Example: "Functional,High".
exploitedinthewild	optional	Included exploited in the wild values. Available with Ranger Insights. Example: "Unknown,Yes".
groupids	optional	Single Group ID to filter by. Example: "225494730938493804".
highestseverities	optional	Included highest severities. Example: "CRITICAL,HIGH".
limit	optional	Limit number of returned items (1-1000). Example: "10".
mostcommonstatuses	optional	Included most common status values. Available with Ranger Insights.
name__contains	optional	Free-text filter by application name (supports multiple values). Example: "Office 1.1,Test".
ostypes	optional	Included OS types. Example: "windows,linux".
remediationlevels	optional	Included remediation level values. Available with Ranger Insights. Example: "Official Fix,Temporary Fix".
siteids	optional	Single Site ID to filter by. Example: "225494730938493804".
skip	optional	Skip first number of items (0-1000). To iterate over more than 1000 items, use "cursor". Example: "150".
skipcount	optional	If true, total number of items will not be calculated, which speeds up execution time.
sortby	optional	The column to sort the results by. Example: "id".
sortorder	optional	Sort direction. Example: "asc".
vendor__contains	optional	Free-text filter by vendor (supports multiple values). Example: "Microsoft,Apple".
vendors	optional	Included vendors. Example: "Microsoft,Apple".

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - Insufficient permissions

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>pagination</td><td>Pagination information</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>totalItems</td><td>Total number of items found matching your query</td><td>true</td><td>integer</td></tr>
<tr><td>nextCursor</td><td>Pass this value as "cursor" on your next request, to get the next page of results (Will be "null" when last page reached)</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>applicationType</td><td>Application type</td><td>false</td><td>string</td></tr>
<tr><td>cveCount</td><td>Cve count</td><td>false</td><td>integer</td></tr>
<tr><td>daysDetected</td><td>Days detected</td><td>false</td><td></td></tr>
<tr><td>detectionDate</td><td>Detection date</td><td>false</td><td>string</td></tr>
<tr><td>endpointCount</td><td>Endpoint count</td><td>false</td><td>integer</td></tr>
<tr><td>endpointsWithoutTicket</td><td>Number of endpoints that are in an integrated scope, but don't have a ticket created. Available with Ranger</td><td>false</td><td>integer</td></tr>
</table>
</td></tr>
</table>

				Insights.		
			estimate	Estimate	false	boolean
			exploitCodeMaturity	Exploit code maturity	false	enum
			exploitedInTheWild	Exploited in the wild	false	enum
			highestNvdBaseScore	Highest nvd base score	false	string
			highestRiskScore	Highest risk score	false	string
			highestSeverity	Highest severity	false	string
			name	Name	false	string
			remediationLevel	Remediation level	false	enum
			statuses	Statuses	false	Name / Description / Required / Value count / Count / false / integer key / Key / false / label / Label / false / ticketCategory / Ticket category / false / string
			vendor	Vendor	false	string
			versionCount	Version count	false	integer
errors	Errors	false	array			

Get Applications With Risk

GET /web/api/v2.1/application-management/risks/applications

Get data for each version of all applications.

Parameters

accountids	optional	Single Account ID to filter by. Example: "225494730938493804".
application__contains	optional	Free-text filter by application name and version (supports multiple values). Example: "Office 1.1,Test".
applicationtypes	optional	Application type. Available with Ranger Insights. Example: "A,p,p,l,i,c,a,t,i,o,n".
countonly	optional	If true, only total number of items will be returned, without any of the actual objects.
cursor	optional	Cursor position returned by the last request. Use to iterate over more than 1000 items. Example: "YWdlbnRfaWQ6NTgwMjkzODE=".
cveid__contains	optional	Free-text filter by CVE id (supports multiple values). Example: "CVE-1234-5678".
daysfromdetection	optional	Days from application detection, e.g. 12 days or more. Example: "12".
detectiondate__between	optional	Date range for application detection date(format: <from_timestamp>-<to_timestamp>, inclusive). Example: "1514978890136-1514978650130".
detectiondate__gt	optional	Application detection date after this timestamp. Example: "2018-02-27T04:49:26.257525Z".
detectiondate__gte	optional	Application detection date after or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
detectiondate__lt	optional	Application detection date before this timestamp. Example: "2018-02-27T04:49:26.257525Z".
detectiondate__lte	optional	Application detection date before or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
domains	optional	Included domains.
endpointname__contains	optional	Free-text filter by endpoint name (supports multiple values). Example: "Office,Test".

endpointtypes	optional	Included endpoint types. Example: "desktop,laptop".
endpointuuid__contains	optional	Free-text filter by endpoint uuid (supports multiple values)
exploitcodematurity	optional	Included exploit code maturity values. Available with Ranger Insights. Example: "Functional,High".
exploitedinthewild	optional	Included exploited in the wild values. Available with Ranger Insights. Example: "Unknown,Yes".
groupids	optional	Single Group ID to filter by. Example: "225494730938493804".
highestseverities	optional	Included highest severities. Example: "CRITICAL,HIGH".
limit	optional	Limit number of returned items (1-1000). Example: "10".
mostcommonstatuses	optional	Included most common status values. Available with Ranger Insights.
ostypes	optional	Included OS types. Example: "windows,linux".
remediationlevels	optional	Included remediation level values. Available with Ranger Insights. Example: "Official Fix,Temporary Fix".
siteids	optional	Single Site ID to filter by. Example: "225494730938493804".
skip	optional	Skip first number of items (0-1000). To iterate over more than 1000 items, use "cursor". Example: "150".
skipcount	optional	If true, total number of items will not be calculated, which speeds up execution time.
sortby	optional	The column to sort the results by. Example: "id".
sortorder	optional	Sort direction. Example: "asc".
vendor__contains	optional	Free-text filter by vendor (supports multiple values). Example: "Microsoft,Apple".
vendors	optional	Included vendors. Example: "Microsoft,Apple".

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - Insufficient permissions

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>pagination</td><td>Pagination information</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>totalItems</td><td>Total number of items found matching your query</td><td>true</td><td>integer</td></tr>
<tr><td>nextCursor</td><td>Pass this value as "cursor" on your next request, to get the next page of results (Will be "null" when last page reached)</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>applicationId</td><td>Application id</td><td>false</td><td>string</td></tr>
<tr><td>applicationType</td><td>Available with Ranger Insights.</td><td>false</td><td>string</td></tr>
<tr><td>cveCount</td><td>Cve count</td><td>false</td><td>integer</td></tr>
<tr><td>daysDetected</td><td>Days detected</td><td>false</td><td></td></tr>
<tr><td>detectionDate</td><td>Detection date</td><td>false</td><td>string</td></tr>
<tr><td>endpointCount</td><td>Endpoint count</td><td>false</td><td>integer</td></tr>
<tr><td>endpointsWithoutTicket</td><td>Number of endpoints that are in an integrated scope, but don't have a ticket</td><td>false</td><td>integer</td></tr>
</table>
</td></tr>
</table>

				created. Available with Ranger Insights.		
			estimate	Estimate	false	boolean
			exploitCodeMaturity	Available with Ranger Insights.	false	enum
			exploitedInTheWild	Available with Ranger Insights.	false	enum
			highestNvdBaseScore	Highest nvd base score	false	string
			highestRiskScore	Available with Ranger Insights.	false	string
			highestSeverity	Highest severity	false	string
			name	Name	false	string
			remediationLevel	Available with Ranger Insights.	false	enum
			statuses	Statuses	false	
			vendor	Vendor	false	string
errors	Errors	false	array			

Name	Description	Required	Value
count	Count	false	integer
key	Key	false	
label	Label	false	
ticketCategory	Ticket category	false	string

Get Endpoints For Vulnerable App

GET /web/api/v2.1/application-management/risks/endpoints

Get a list of all endpoints installed with a specific application that contains vulnerabilities.

Parameters

accountids	optional	Single Account ID to filter by. Example: "225494730938493804".
applicationids	optional	Included application versions by id
applicationname	optional	Application name
applicationvendor	optional	Application vendor
applicationversions	optional	Included application versions
countonly	optional	If true, only total number of items will be returned, without any of the actual objects.
cursor	optional	Cursor position returned by the last request. Use to iterate over more than 1000 items. Example: "YWdlbnRfaWQ6NTgwMjkzODE=".
daysfromdetection	optional	Days from application detection, e.g. 12 days or more. Example: "12".
daystomitigation__between	optional	Date range for days left to mitigation. Available with Ranger Insights when using ticket integration. Example: "1-30".
detectiondate__between	optional	Date range for application detection date(format: <from_timestamp>-<to_timestamp>, inclusive). Example: "1514978890136-1514978650130".
detectiondate__gt	optional	Application detection date after this timestamp. Example: "2018-02-27T04:49:26.257525Z".
detectiondate__gte	optional	Application detection date after or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
detectiondate__lt	optional	Application detection date before this timestamp. Example: "2018-02-27T04:49:26.257525Z".
detectiondate__lte	optional	Application detection date before or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
domain__contains	optional	Free-text filter by domain (supports multiple values). Example: "mybusiness,workgroup".

domains	optional	Included endpoint domains
endpointid__contains	optional	Free-text filter by endpoint id (supports multiple values)
endpointname__contains	optional	Free-text filter by endpoint name (supports multiple values). Example: "Office,Test".
endpointtypes	optional	Included endpoint types
endpointuuid__contains	optional	Free-text filter by endpoint uuid (supports multiple values)
groupids	optional	Single Group ID to filter by. Example: "225494730938493804".
lastscandate__between	optional	Date range for last scan date(format: <from_timestamp>-<to_timestamp>, inclusive). Example: "1514978890136-1514978650130".
lastscandate__gt	optional	Last scan date after this timestamp. Example: "2018-02-27T04:49:26.257525Z".
lastscandate__gte	optional	Last scan date after or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
lastscandate__lt	optional	Last scan date before this timestamp. Example: "2018-02-27T04:49:26.257525Z".
lastscandate__lte	optional	Last scan date before or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
lastscanresults	optional	Included last scan results. Example: "Succeeded".
limit	optional	Limit number of returned items (1-1000). Example: "10".
ostypes	optional	Included OS types
osversions	optional	Included OS versions
siteids	optional	Single Site ID to filter by. Example: "225494730938493804".
skip	optional	Skip first number of items (0-1000). To iterate over more than 1000 items, use "cursor". Example: "150".
skipcount	optional	If true, total number of items will not be calculated, which speeds up execution time.
sortby	optional	The column to sort the results by. Example: "id".
sortorder	optional	Sort direction. Example: "asc".
statuses	optional	Included statuses. Available with Ranger Insights.
statusmessage__contains	optional	Free-text filter by status message (supports multiple values). Available with Ranger Insights. Example: "assigned to john,top

		priority".
ticketid__contains	optional	Free-text filter by ticket id. Available with Ranger Insights when using ticket integration. Example: "ABC-123,ABCD-100".

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - Insufficient permissions

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>pagination</td><td>Pagination information</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>totalItems</td><td>Total number of items found matching your query</td><td>true</td><td>integer</td></tr>
<tr><td>nextCursor</td><td>Pass this value as "cursor" on your next request, to get the next page of results (Will be "null" when last page reached)</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountName</td><td>Account name</td><td>false</td><td>string</td></tr>
<tr><td>applicationDaysDetected</td><td>Application days</td><td>false</td><td></td></tr>
</table>
</td></tr>
</table>

				detected		
			applicationDetectionDate	Detection date	false	string
			applicationVersion	Version	false	string
			domain	Domain	false	string
			endpointId	Endpoint id	false	string
			endpointName	Endpoint name	false	string
			endpointType	Endpoint type	false	string
			endpointUuid	Endpoint uuid	false	string
			externalTicketSystem	External ticket system	false	

Name	Description	Required	Value
available	Available	false	boolean
type	Type	false	string

groupName	Group name	false	string
lastScanDate	Last scan date	false	string
lastScanResult	Last scan result	false	string
osType	OS type	false	enum
osVersion	Os version	false	string
siteName	Site name	false	string
statusHistory	Available with Ranger Insights	false	

Name	Description	Required	Value
changedAt	Changed at	false	string
changedBy	Changed by	false	string
currentKey	Current key	false	string
currentLabel	Current label	false	enum
previousKey	Previous key	false	string
previousLabel	Previous label	false	enum
reason	Reason	false	string

ticket	Ticket	false	

						Name	Description	Required	Value
						analystReason	Analyst reason	false	string
						daysToMitigation	Days to mitigation	false	integer
						endpointsCount	Endpoints count	false	integer
						metaData	Meta data	false	object
						name	Name	false	string
						projectName	Project name	false	string
						reporter	Reporter	false	string
						status	Status	false	string
						statusCategory	Status category	false	string
						title	Title	false	string
						url	Url	false	string
errors	Errors	false	array						

Get Application CVEs

GET /web/api/v2.1/application-management/risks/cves

Get CVE data for a specific application.

Parameters

accountids	optional	Single Account ID to filter by. Example: "225494730938493804".
analystverdict	optional	Include Default(not edited)/ False Positives / Added CVEs for Vulnerabilities. Example: "Default,False Positive,Added CVE".
applicationids	optional	Included application versions by id
applicationname	optional	Application name
applicationvendor	optional	Application vendor
applicationversions	optional	Included application versions
countonly	optional	If true, only total number of items will be returned, without any of the actual objects.
cursor	optional	Cursor position returned by the last request. Use to iterate over more than 1000 items. Example: "YWdlbnRfaWQ6NTgwMjkzODE=".
cveid__contains	optional	Free-text filter by CVE id (supports multiple values). Example: "CVE-1234-5678".
exploitcodematurity	optional	Included exploit code maturity values. Available with Ranger Insights. Example: "FUNCTIONAL,HIGH".
exploitedinthewild	optional	Included exploited in the wild values. Available with Ranger Insights. Example: "EXPLOITED_UNKNOWN,YES".
groupids	optional	Single Group ID to filter by. Example: "225494730938493804".
limit	optional	Limit number of returned items (1-1000). Example: "10".
publisheddate__between	optional	Date range for CVE publish date(format: <from_timestamp>-<to_timestamp>, inclusive). Example: "1514978890136-1514978650130".
publisheddate__gt	optional	CVE published date after this timestamp. Example: "2018-02-27T04:49:26.257525Z".
publisheddate__gte	optional	CVE published date after or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".

publisheddate__lt	optional	CVE published date before this timestamp. Example: "2018-02-27T04:49:26.257525Z".
publisheddate__lte	optional	CVE published date before or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
remediationlevels	optional	Included remediation level values. Available with Ranger Insights. Example: "OFFICIAL_FIX,TEMPORARY_FIX".
reportconfidence	optional	Included report confidence values. Available with Ranger Insights. Example: "REASONABLE,CONFIRMED".
severities	optional	Included severities. Example: "CRITICAL,HIGH".
siteids	optional	Single Site ID to filter by. Example: "225494730938493804".
skip	optional	Skip first number of items (0-1000). To iterate over more than 1000 items, use "cursor". Example: "150".
skipcount	optional	If true, total number of items will not be calculated, which speeds up execution time.
sortby	optional	The column to sort the results by. Example: "id".
sortorder	optional	Sort direction. Example: "asc".

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - Insufficient permissions

Response Schema

Name	Description	Required	Value
pagination	Pagination information	true	

Name	Description	Required	Value
totalItems	Total number of items found matching your query	true	integer
nextCursor	Pass this	false	string

				value as "cursor" on your next request, to get the next page of results (Will be "null" when last page reached)		
data	Response data	false	Name	Description	Required	Value
			cveId	Cve id	false	string
			cvssVersion	Cvss version	false	string
			description	Description	false	
			exploitCodeMaturity	Available with Ranger Insights	false	enum
			exploitedInTheWild	Available with Ranger Insights	false	enum
			fpFnMarks	Fp fn marks	false	
			mitreUrl	Mitre url	false	
			nvdBaseScore	Nvd base score	false	string
			nvdUrl	Nvd url	false	
			publishedDat	Published	false	string

Name	Description	Required	Value
markedOnScope		true	
markedBy		false	string
markedDate		false	string
reason		false	string
type		false	

Name	Description	Required	Value
id		false	string
name		false	string
type		false	string

			e	date		
			remediationLevel	Available with Ranger Insights	false	enum
			reportConfidence	Available with Ranger Insights	false	enum
			riskScore	Available with Ranger Insights	false	string
			severity	Severity	false	
errors	Errors	false	array			

Get Application Inventory

GET /web/api/v2.1/application-management/inventory

Get application inventory data grouped by application name and vendor.

Parameters

accountids	optional	Single Account ID to filter by. Example: "225494730938493804".
countonly	optional	If true, only total number of items will be returned, without any of the actual objects.
cursor	optional	Cursor position returned by the last request. Use to iterate over more than 1000 items. Example: "YWdlbnRfaWQ6NTgwMjkzODE=".
endpointname__contains	optional	Free-text filter by endpoint name (supports multiple values). Example: "Office,Test".
endpointuuid__contains	optional	Free-text filter by endpoint uuid (supports multiple values)
groupids	optional	Single Group ID to filter by. Example: "225494730938493804".
limit	optional	Limit number of returned items (1-1000). Example: "10".
name__contains	optional	Free-text filter by application name (supports multiple values). Example: "Office,Test".
osarchitectures	optional	Included OS architectures
ostypes	optional	Included OS types
osversion__contains	optional	Free-text filter by os version (supports multiple values). Example: "Windows 7 ServicePack1".
osversions	optional	Included OS versions
siteids	optional	Single Site ID to filter by. Example: "225494730938493804".
skip	optional	Skip first number of items (0-1000). To iterate over more than 1000 items, use "cursor". Example: "150".
skipcount	optional	If true, total number of items will not be calculated, which speeds up execution time.
sortby	optional	The column to sort the results by. Example: "id".
sortorder	optional	Sort direction. Example: "asc".

vendor__contains	optional	Free-text filter by vendor (supports multiple values). Example: "Microsoft,Apple".
vendors	optional	Included vendors. Example: "Microsoft,Apple".

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - Insufficient permissions

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>pagination</td><td>Pagination information</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>totalItems</td><td>Total number of items found matching your query</td><td>true</td><td>integer</td></tr>
<tr><td>nextCursor</td><td>Pass this value as "cursor" on your next request, to get the next page of results (Will be "null" when last page reached)</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>applicationName</td><td>Name</td><td>false</td><td>string</td></tr>
<tr><td>applicationVendor</td><td>Vendor</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
</table>

			applicationVersionsCount: Application versions count; false; integer endpointsCount: Endpoints count; false; integer estimate: Estimate; false; boolean
errors	Errors	false	array

Get CVE data

GET /web/api/v2.1/application-management/risks

Get the CVE vulnerability data for each CVE.

Parameters

accountids	optional	Single Account ID to filter by. Example: "225494730938493804".
analystverdict	optional	Include Default(not edited)/ False Positives / Added CVEs for Vulnerabilities. Example: "Default,False Positive,Added CVE".
application__contains	optional	Free-text filter by application name and version (supports multiple values). Example: "Office 1.1,Test".
applicationnames	optional	Included application names. Example: "Office 1.1,Test".
applicationvendor__contains	optional	Free-text filter by vendor (supports multiple values). Example: "Microsoft,Apple".
countonly	optional	If true, only total number of items will be returned, without any of the actual objects.
cursor	optional	Cursor position returned by the last request. Use to iterate over more than 1000 items. Example: "YWdlbnRfaWQ6NTgwMjkzODE=".
cveid__contains	optional	Free-text filter by CVE id (supports multiple values). Example: "CVE-1234-5678".
daysfromcvedetection	optional	Days from CVE detection, e.g. 12 days or more. Example: "12".
detectiondate__between	optional	Date range for CVE detection date(format: <from_timestamp>-<to_timestamp>, inclusive). Example: "1514978890136-1514978650130".
detectiondate__gt	optional	CVE detection date after this timestamp. Example: "2018-02-27T04:49:26.257525Z".
detectiondate__gte	optional	CVE detection date after or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
detectiondate__lt	optional	CVE detection date before this timestamp. Example: "2018-02-27T04:49:26.257525Z".
detectiondate__lte	optional	CVE detection date before or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".

domain__contains	optional	Free-text filter by domain (supports multiple values). Example: "mybusiness,workgroup".
domains	optional	Included network domains. Example: "mybusiness,workgroup".
endpointname__contains	optional	Free-text filter by endpoint name (supports multiple values). Example: "Office,Test".
endpointtypes	optional	Included endpoint types
exploitcodematurity	optional	Included exploit code maturity values. Available for VLN SKU. Example: "FUNCTIONAL,HIGH".
exploitedinthewild	optional	Included exploited in the wild values. Available for VLN SKU. Example: "EXPLOITED_UNKNOWN,YES".
groupids	optional	Single Group ID to filter by. Example: "225494730938493804".
includeremovals	optional	Include also removed CVEs in the results
lastscanresults	optional	Included last scan results. Example: "Succeeded".
limit	optional	Limit number of returned items (1-1000). Example: "10".
mitigationstatus	optional	Filters by the application's mitigation status values.Available for VLN SKU. Example: "Not mitigated,To be patched,On hold".
ostypes	optional	Included OS types
osversions	optional	Included OS versions
publisheddate__between	optional	Date range for CVE publish date(format: <from_timestamp>-<to_timestamp>, inclusive). Example: "1514978890136-1514978650130".
publisheddate__gt	optional	CVE published date after this timestamp. Example: "2018-02-27T04:49:26.257525Z".
publisheddate__gte	optional	CVE published date after or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
publisheddate__lt	optional	CVE published date before this timestamp. Example: "2018-02-27T04:49:26.257525Z".
publisheddate__lte	optional	CVE published date before or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
remediationlevels	optional	Included remediation level values. Available for VLN SKU. Example: "OFFICIAL_FIX,TEMPORARY_FIX".
reportconfidence	optional	Included report confidence values. Available for VLN SKU. Example: "REASONABLE,CONFIRMED".
riskscore__between	optional	Risk score (inclusive). Available for VLN SKU. Example: "5-8.9".

riskupdateddate__between	optional	Significant CVE updates within this date range(format: <from_timestamp>-<to_timestamp>, inclusive). Example: "1514978890136-1514978650130".
riskupdateddate__gt	optional	Significant CVE updates after this timestamp. Example: "2018-02-27T04:49:26.257525Z".
riskupdateddate__gte	optional	Significant CVE updates after or at this timestamp. Recommended for fetching delta-changes. Example: "2018-02-27T04:49:26.257525Z".
riskupdateddate__lt	optional	Significant CVE updates before this timestamp. Example: "2018-02-27T04:49:26.257525Z".
riskupdateddate__lte	optional	Significant CVE updates before or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
severities	optional	Included severities. Example: "CRITICAL,HIGH".
siteids	optional	Single Site ID to filter by. Example: "225494730938493804".
skip	optional	Skip first number of items (0-1000). To iterate over more than 1000 items, use "cursor". Example: "150".
skipcount	optional	If true, total number of items will not be calculated, which speeds up execution time.
sortby	optional	The column to sort the results by. Example: "id".
sortorder	optional	Sort direction. Example: "asc".
vendors	optional	Included vendors. Example: "Microsoft,Apple".

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - Insufficient permissions

Response Schema

Name	Description	Required	Value
pagination	Pagination information	true	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr></table>

			totalItems: Total number of items found matching your query; true; integer nextCursor: Pass this value as "cursor" on your next request, to get the next page of results (Will be "null" when last page reached); false; string
data	Response data	false	

Name	Description	Required	Value
application	Composed application name	false	string
applicationName	Application name	false	string
applicationVendor	Application vendor	false	string
applicationVersion	Application version	false	string
baseScore	Not available with VLN SKU	false	string
cveId	CVE Id	false	string
cvssVersion	Cvss version	false	string
daysDetected	Days detected	false	integer
detectionDate	Detection date	false	string
endpointId	Endpoint id	false	string
endpointName	Endpoint name	false	string

			endpointType	Endpoint type	false	string
			exploitCodeMaturity	Available for VLN SKU	false	enum
			id	Id	false	string
			lastScanDate	Last scan date	false	string
			lastScanResult	Last scan result	false	string
			markedBy	Marked by	false	string
			markedDate	Marked date	false	string
			markType	Mark type	false	
			mitigationStatus	Risk mitigation status	false	enum
			mitigationStatusChangedBy	Mitigation status changer	false	string
			mitigationStatusChangeTime	Mitigation status change time	false	string
			mitigationStatusReason	Mitigation status reason	false	string
			nvdBaseScore	Available for VLN SKU	false	string
			nvdCvssVersion	Available for VLN SKU	false	string
			osType	OS type	false	enum
			publishedDate	Published date	false	string
			reason	Reason	false	string
			remediationLevel	Available for VLN SKU	false	enum
			reportConfidence	Available for VLN SKU	false	enum
			riskScore	Available for VLN SKU	false	string

			severity | Severity | false | string status | Risk status | false | enum
errors	Errors	false	array

Initiate scan

POST /web/api/v2.1/application-management/scan

Initiate application vulnerability scan.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>success</td><td>Indicates a successful operation</td><td>false</td><td>boolean</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>filter</td><td>Filter</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>account scope ID to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>siteIds</td><td>site scope ID to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>tenant</td><td>if the entire tenant scope should be filtered</td><td>false</td><td>boolean</td></tr>
</table>
</td></tr>
</table>

Application Management Settings

Update Application Management Settings

POST /web/api/v2.1/application-management/settings

Update Application Management Settings

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - Insufficient permissions

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
extensiveLinuxScanEnabled	Extensive linux scan enabled	false	boolean
extensiveScanEnabled	Extensive scan enabled	false	boolean
inheritedFrom	Inherited from	false	string
isDefaultPolicy	Determines if the policy is overridden on the scope level.	false	boolean
vulnerabilitiesScanEnable	Vulnerabilities scan enabled	false	boolean

			d
errors	Errors	false	array

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>extensiveLinuxScanEnabled</td><td>Extensive linux scan enabled</td><td>false</td><td>boolean</td></tr>
<tr><td>extensiveScanEnabled</td><td>Extensive scan enabled</td><td>false</td><td>boolean</td></tr>
<tr><td>isDefaultPolicy</td><td>Determines if the policy is overridden on the scope level.</td><td>false</td><td>boolean</td></tr>
<tr><td>vulnerabilitiesScanEnabled</td><td>Vulnerabilities scan enabled</td><td>false</td><td>boolean</td></tr>
</table>
</td></tr>
<tr><td>filter</td><td>Filter</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>groupIds</td><td>List of Group IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>siteIds</td><td>List of Site IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>tenant</td><td>Indicates a tenant scope request</td><td>false</td><td>boolean</td></tr>
</table>
</td></tr>
</table>

Get Application Management Settings

GET /web/api/v2.1/application-management/settings

Get Application Management settings.

Parameters

accountids	optional	account scope IDs to filter by. Example: "225494730938493804,225494730938493915".
groupids	optional	group scope to filter by. Example: "225494730938493804,225494730938493915".
siteids	optional	site scope IDs to filter by. Example: "225494730938493804,225494730938493915".

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - Insufficient permissions

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
extensiveLinuxScanEnabled	Extensive linux scan enabled	false	boolean
extensiveScanEnabled	Extensive scan enabled	false	boolean
inheritedFrom	Inherited from	false	string
isDefaultPolicy	Determines if the policy is	false	boolean

				overridden on the scope level.		
			vulnerabilitiesScanEnabled	Vulnerabilities scan enabled	false	boolean
errors	Errors	false	array			

Application Risk

Get Applications

GET /web/api/v2.1/installed-applications

Get the applications, and their data (such as risk level), installed on endpoints with Application Risk-enabled Agents that match the filter. SentinelOne Application Risk lets you monitor applications installed on endpoints. Applications not updated with the latest patches are vulnerable to exploits. With SentinelOne Application Risk you can see all applications to be patched, on all endpoints or on a specific endpoint. The Agent takes a snapshot of the endpoint application data and checks for vulnerabilities in the SentinelOne Cloud. When the Agent detects a change to the application data, it sends a diff to the Management.
Application Risk requires Complete SKU. This feature is in EA. To join the EA program, contact your SentinelOne Sales Rep.

Parameters

accountids	optional	List of Account IDs to filter by. Example: "225494730938493804,225494730938493915".
agentcomputername__contains	optional	Free-text filter by computer name (supports multiple values). Example: "john-office,WIN".
agentisdecommissioned	optional	Include active agents, decommissioned or both. Example: "True,False".
agentmachinetypes	optional	Filter by endpoint machine types. Example: "unknown".
agentmachinetypesnin	optional	Filter not by endpoint machine types. Example: "unknown".
agentosversion__contains	optional	Free-text filter by OS full name and version (supports multiple values). Example: "Service Pack 1".
agentuuid__contains	optional	Free-text filter by agent UUID (supports multiple values). Example: "e92-01928,b055".
countonly	optional	If true, only total number of items will be returned, without any of the actual objects.
cursor	optional	Cursor position returned by the last request. Use to iterate over more than 1000 items. Example: "YWdlbnRfaWQ6NTgwMjkzODE=".
groupids	optional	List of Group IDs to filter by. Example: "225494730938493804,225494730938493915".
ids	optional	Filter by application IDs. Example:

		"225494730938493804,225494730938493915".
installedat__between	optional	Filter by installation date range
limit	optional	Limit number of returned items (1-1000). Example: "10".
name__contains	optional	Free-text filter by application name (supports multiple values). Example: "calc".
ostypes	optional	Filter by OS types. Example: "macos".
ostypesnin	optional	Filter not by OS types. Example: "macos".
publisher__contains	optional	Free-text filter by application publisher (supports multiple values). Example: "Sentinel".
risklevels	optional	Filter by risk. Example: "none".
risklevelsnin	optional	Filter not by risk. Example: "none".
siteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".
size__between	optional	Filter by application size range (bytes). Example: "1024-104856".
skip	optional	Skip first number of items (0-1000). To iterate over more than 1000 items, use "cursor". Example: "150".
skipcount	optional	If true, total number of items will not be calculated, which speeds up execution time.
sortby	optional	The column to sort the results by. Example: "id".
sortorder	optional	Sort direction. Example: "asc".
types	optional	Filter by application types. Example: "app".
typesnin	optional	Filter not by application types. Example: "app".
version__contains	optional	Free-text filter by application version (supports multiple values). Example: "1.22.333,build".

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
pagination	Pagination information	true	

Name	Description	Required	Value
totalItems	Total number of items found matching your query	true	integer
nextCursor	Pass this value as "cursor" on your next request, to get the next page of results (Will be "null" when last page reached)	false	string

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
agentComputerName	Agent computer name	false	string
agentDomain	Agent domain	false	string
agentId	Agent id	false	string
agentInfected	Agent infected	false	boolean
agentIsActive	Agent is active	false	boolean
agentIsDecommissioned	Agent is decommissioned	false	boolean
agentMachineType	Agent machine type	false	enum
agentNetworkStatus	Agent network status	false	enum
agentOperati	Agent	false	string

			onalState | operational state | | | agentOsType | OS type | false | enum agentUuid | Agent uuid | false | string agentVersion | Agent version | false | string createdAt | Created at | false | string id | Application ID | false | string installedAt | Installed at | false | string name | Name | false | string osType | OS type | false | enum publisher | Publisher | false | string riskLevel | Risk level | false | enum signed | Signed | false | boolean size | Application size (bytes) | false | integer type | Type | false | enum updatedAt | Updated at | false | string version | Version | false | string
errors	Errors	false	array

Get CVEs

GET /web/api/v2.1/installed-applications/cves

Get known CVEs for applications that are installed on endpoints with Application Risk-enabled Agents.
Application Risk requires Complete SKU. This feature is in EA. To join the EA program, contact your SentinelOne Sales Rep.

Parameters

accountids	optional	List of Account IDs to filter by. Example: "225494730938493804,225494730938493915".
applicationids	optional	Filter by application IDs. Example: "225494730938493804,225494730938493915".
countonly	optional	If true, only total number of items will be returned, without any of the actual objects.
createdat__gt	optional	Created at greater than. Example: "2018-02-27T04:49:26.257525Z".
createdat__gte	optional	Created at greater or equal than. Example: "2018-02-27T04:49:26.257525Z".
createdat__lt	optional	Created at lesser than. Example: "2018-02-27T04:49:26.257525Z".
createdat__lte	optional	Created at lesser or equal than. Example: "2018-02-27T04:49:26.257525Z".
cursor	optional	Cursor position returned by the last request. Use to iterate over more than 1000 items. Example: "YWdlbnRfaWQ6NTgwMjkzODE=".
cveids	optional	Filter by global CVE ids. Example: "CVE-2018-3182,CVE-2018-1087".
groupids	optional	List of Group IDs to filter by. Example: "225494730938493804,225494730938493915".
ids	optional	Filter by internal CVE IDs. Example: "225494730938493804,225494730938493915".
limit	optional	Limit number of returned items (1-1000). Example: "10".
siteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".
skip	optional	Skip first number of items (0-1000). To iterate over more than 1000 items, use "cursor". Example: "150".

skipcount	optional	If true, total number of items will not be calculated, which speeds up execution time.
sortby	optional	The column to sort the results by. Example: "id".
sortorder	optional	Sort direction. Example: "asc".
updatedat__gt	optional	Updated at greater than. Example: "2018-02-27T04:49:26.257525Z".
updatedat__gte	optional	Updated at greater or equal than. Example: "2018-02-27T04:49:26.257525Z".
updatedat__lt	optional	Updated at lesser than. Example: "2018-02-27T04:49:26.257525Z".
updatedat__lte	optional	Updated at lesser or equal than. Example: "2018-02-27T04:49:26.257525Z".

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>pagination</td><td>Pagination information</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>totalItems</td><td>Total number of items found matching your query</td><td>true</td><td>integer</td></tr>
<tr><td>nextCursor</td><td>Pass this value as "cursor" on your next request, to get the next page of results (Will be "null" when last</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
</table>

			page reached)
data	Response data	false	array

Name	Description	Required	Value
createdAt	Created at	false	string
cveId	Global CVE ID	false	string
description	Description	false	string
id	Id	false	string
link	Link	false	string
publishedAt	Published at	false	string
riskLevel	Risk level	false	enum
score	Score	false	number
updatedAt	Updated at	false	string

errors	Errors	false	array

Export Applications

GET /web/api/v2.1/export/installed-applications

Export the list of applications installed on endpoints with Application Risk-enabled Agents and their properties, including the CVEs for each application that requires a patch. The CSV file is stored on the Management. Application Risk requires Complete SKU.
This feature is in EA. To join the EA program, contact your SentinelOne Sales Rep.

Parameters

accountids	optional	List of Account IDs to filter by. Example: "225494730938493804,225494730938493915".
agentcomputername__contains	optional	Free-text filter by computer name (supports multiple values). Example: "john-office,WIN".
agentisdecommissioned	optional	Include active agents, decommissioned or both. Example: "True,False".
agentmachinetypes	optional	Filter by endpoint machine types. Example: "unknown".
agentmachinetypesnin	optional	Filter not by endpoint machine types. Example: "unknown".
agentosversion__contains	optional	Free-text filter by OS full name and version (supports multiple values). Example: "Service Pack 1".
agentuuid__contains	optional	Free-text filter by agent UUID (supports multiple values). Example: "e92-01928,b055".
groupids	optional	List of Group IDs to filter by. Example: "225494730938493804,225494730938493915".
ids	optional	Filter by application IDs. Example: "225494730938493804,225494730938493915".
installedat__between	optional	Filter by installation date range
name__contains	optional	Free-text filter by application name (supports multiple values). Example: "calc".
ostypes	optional	Filter by OS types. Example: "macos".
ostypesnin	optional	Filter not by OS types. Example: "macos".
publisher__contains	optional	Free-text filter by application publisher (supports multiple values). Example: "Sentinel".
risklevels	optional	Filter by risk. Example: "none".
risklevelsnin	optional	Filter not by risk. Example: "none".

siteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".
size__between	optional	Filter by application size range (bytes). Example: "1024-104856".
types	optional	Filter by application types. Example: "app".
typesnin	optional	Filter not by application types. Example: "app".
version__contains	optional	Free-text filter by application version (supports multiple values). Example: "1.22.333,build".

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Auto Upgrade Policy

Get Available Packages

GET /web/api/v2.1/upgrade-policy/available-packages

Get Available Packages

Parameters

ostype	required	OS type, one of 'linux', 'macos' or 'windows'
scopelevel	required	Scope level, one of 'account', 'group', 'site' or 'tenant'
displayname__contains	optional	Partially match the name of the package, e.g. '22.1 GA'
scopeid	optional	Scope ID

Response Messages

200 - Success

400 - Bad request

Response Schema

Name	Description	Required	Value
data		false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>packages</td><td></td><td>false</td><td>undefined []</td></tr></table>

Has Policy

POST /web/api/v2.1/upgrade-policy/has-policy

Has policy

Response Messages

200 - Success

400 - Bad request

Response Schema

Name	Description	Required	Value
hasPolicies		false	boolean

Body Schema

Name	Description	Required	Value
accounts	List of Account IDs to filter by. Example: '225494730938493804,225494730938493915'.	false	string []
groups	List of Group IDs to filter by. Example: '225494730938493804,225494730938493915'.	false	string []
osType	OS type, one of 'linux', 'macos' or 'windows'	false	string
sites	List of Site IDs to filter by. Example: '225494730938493804,225494730938493915'.	false	string []

Get Parent Policies

GET /web/api/v2.1/upgrade-policy/parent-policies

Get paginated and ordered parent policies by a given scope

Parameters

limit	required	Limit number of returned items. Should be more than 1. Example: '10'.
ostype	required	OS type, one of 'linux', 'macos' or 'windows'
scopelevel	required	Scope level, one of 'account', 'group', 'site' or 'tenant'
skip	required	Skip first number of items. Example: '0'.
sortby	required	The column to sort the results by. Example: 'priority'.
sortorder	required	Sort direction. Could be 'asc' or 'desc'.
scopeid	optional	Scope ID

Response Messages

200 - Success

400 - Bad request

Response Schema

Name	Description	Required	Value
data		false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>isInherited</td><td></td><td>false</td><td>boolean</td></tr><tr><td>policies</td><td></td><td>false</td><td>undefined []</td></tr><tr><td>policiesInChildScope</td><td></td><td>false</td><td>boolean</td></tr></table>
pagination		false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>totalItems</td><td></td><td>false</td><td>integer</td></tr></table>

Get Policies

GET /web/api/v2.1/upgrade-policy/policies

Get paginated and ordered policies by a given scope

Parameters

limit	required	Limit number of returned items. Should be more than 1. Example: '10'
ostype	required	OS type, one of 'linux', 'macos' or 'windows'
scopelevel	required	Scope level, one of 'account', 'group', 'site' or 'tenant'
skip	required	Skip first number of items. Example: '0'.
sortby	required	The column to sort the results by. Example: 'priority'.
sortorder	required	Sort direction. Could be 'asc' or 'desc'.
scopeid	optional	Scope ID

Response Messages

200 - Success

400 - Bad request

Response Schema

Name	Description	Required	Value
data		false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>isInherited</td><td></td><td>false</td><td>boolean</td></tr><tr><td>policies</td><td></td><td>false</td><td>undefined []</td></tr><tr><td>policiesInChildScope</td><td></td><td>false</td><td>boolean</td></tr></table>
pagination		false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>totalItems</td><td></td><td>false</td><td>integer</td></tr></table>

Deactivate Policies

POST /web/api/v2.1/upgrade-policy/policies

Deactivate all policies

Parameters

ostype	required	OS type, one of 'linux', 'macos' or 'windows'
scopelevel	required	Scope level, one of 'account', 'group', 'site' or 'tenant'
scopeid	optional	Scope ID

Response Messages

200 - Success

400 - Bad request

Response Schema

Name	Description	Required	Value
response		false	string

Policies OS Count

GET /web/api/v2.1/upgrade-policy/policies-count

Get the number of policies for each OS, for a given scope level and id

Parameters

scopelevel	required	Scope level, one of 'account', 'group', 'site' or 'tenant'
scopeid	optional	Scope ID

Response Messages

200 - Success

400 - Bad request

Response Schema

Name	Description	Required	Value
linux		false	integer
macos		false	integer
windows		false	integer

Create Policy

POST /web/api/v2.1/upgrade-policy/policy

Add policy

Response Messages

200 - Success

400 - Bad request

Response Schema

Name	Description	Required	Value
response		false	string

Body Schema

Name	Description	Required	Value
allEndpoints	Affected endpoints. 'true' if the policy is applied to all endpoints. If 'false', tags must be provided.	false	boolean
description	Policy description	false	string
isActive	'true' if policy is active, 'false' if policy is disabled	false	boolean
isScheduled	In case of maintenance window selected, scheduling an upgrade for maintenance window	false	boolean
name	Policy name. This name will be used for creating tasks. Should be unique.	false	string
osType	OS type, one of 'linux', 'macos' or 'windows'	false	string
package		false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>build</td><td></td><td>false</td><td>string</td></tr><tr><td>fileId</td><td></td><td>false</td><td>string</td></tr><tr><td>major</td><td></td><td>false</td><td>string</td></tr></table>

			minor | | false | string
scopeId	Scope ID	false	string
scopeLevel	Scope level, one of 'account', 'group', 'site' or 'tenant'	false	string
tags	Tags for policy application. If provided, AllEndpoints should be false.	false	string []

Update Policy

PUT /web/api/v2.1/upgrade-policy/policy/:policyid

Update existing policy

Parameters

policyid	required	Policy id

Response Messages

200 - Success

400 - Bad request

Response Schema

Name	Description	Required	Value
response		false	string

Body Schema

Name	Description	Required	Value
allEndpoints	Affected endpoints. 'true' if the policy is applied to all endpoints. If 'false', tags must be provided.	false	boolean
description	Policy description	false	string
isActive	'true' if policy is active, 'false' if policy is disabled	false	boolean
isScheduled	In case of maintenance window selected, scheduling an upgrade for maintenance window	false	boolean
name	Policy name. This name will be used for creating tasks. Should be unique.	false	string
osType	OS type, one of 'linux', 'macos' or 'windows'	false	string
package		false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>build</td><td></td><td>false</td><td>string</td></tr><tr><td>fileId</td><td></td><td>false</td><td>string</td></tr><tr><td>major</td><td></td><td>false</td><td>string</td></tr></table>

			minor | | false | string
scopeId	Scope ID	false	string
scopeLevel	Scope level, one of 'account', 'group', 'site' or 'tenant'	false	string
tags	Tags for policy application. If provided, AllEndpoints should be false.	false	string []

Policy Action

POST /web/api/v2.1/upgrade-policy/policy/:policyid

Perform action on a certain policy

Parameters

policyid	required	Policy id

Response Messages

200 - Success

400 - Bad request

Response Schema

Name	Description	Required	Value
response		false	string

Body Schema

Name	Description	Required	Value
action	Policy action, one of 'delete', 'activate' or 'deactivate'	false	string

Reorder Policies

PUT /web/api/v2.1/upgrade-policy/reorder

Reorder policies

Response Messages

200 - Success

400 - Bad request

Response Schema

Name	Description	Required	Value
response		false	string

Body Schema

Name	Description	Required	Value
policies	List of policy IDs and their new order. Example: {"id":"2ad5fdd3-7f9d-4969-9d52-3560fcb482fb","order":0}, {"id":"b448ed4e-545f-442d-ad20-624876e85e84","order":1}.	false	undefined []

Set Scope Inheriting

PUT /web/api/v2.1/upgrade-policy/set-inheriting

Set Scope Inheriting

Response Messages

200 - Success

400 - Bad request

Response Schema

Name	Description	Required	Value
response		false	string

Body Schema

Name	Description	Required	Value
isInheriting	True if policies are inherited from the higher scopes, false otherwise.	false	boolean
scopeId	Scope ID	false	string
scopeLevel	Scope level, one of 'account', 'group', 'site' or 'tenant'	false	string

Cloud Funnel

Validate Bucket

POST /web/api/v2.1/cloud-funnel/validate-bucket-permissions

Validates bucket permissions.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>isValid</td><td>Bucket permissions is valid or invalid</td><td>true</td><td>boolean</td></tr>
<tr><td>error</td><td>Error message in case the bucket permissions is invalid</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>bucketUrl</td><td>Validate bucket permissions</td><td>true</td><td>string</td></tr>
<tr><td>accountId</td><td>Account id</td><td>false</td><td>string</td></tr>
<tr><td>cloudProvider</td><td>Cloud provider, default is aws</td><td>false</td><td>string</td></tr>
<tr><td>roleToAssume</td><td>The aws role to assume when using assume role functionality. Only applicable if cloud_provider is s3.</td><td>false</td><td>string</td></tr>
<tr><td>siteId</td><td>Site id</td><td>false</td><td>string</td></tr>
<tr><td>useAssumeRole</td><td>If set to true, activates the AWS AssumeRole functionality for accessing S3 buckets or other associated resources. Only applicable if cloud_provider is s3.</td><td>false</td><td>boolean</td></tr>
</table>
</td></tr>
</table>

Get AWS assume role external ID.

GET /web/api/v2.1/cloud-funnel/assume-role-external-id

Get the AWS assume role external ID.

Parameters

accountid	optional	Account id. Example: "225494730938493804".
siteid	optional	Site id. Example: "225494730938493804".

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
data	Response data	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>assumeRoleExternalId</td><td>The AWS assume role external id.</td><td>true</td><td>string</td></tr></table>
errors	Errors	false	array

Validate Query

POST /web/api/v2.1/cloud-funnel/validate-query

Verifies that a query is valid before using it as filterfor a Cloud Funnel onboarding

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>error</td><td>Error message in case the query is invalid</td><td>true</td><td>string</td></tr>
<tr><td>isValid</td><td>Query is valid or invalid</td><td>true</td><td>boolean</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

Name	Description	Required	Value
data	Data	true	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>query</td><td>Validate query</td><td>true</td><td>string</td></tr></table>

Get cloud funnel rule

GET /web/api/v2.1/cloud-funnel/onboarding

Gets cloud funnel onboarding rule details

Parameters

accountid	optional	Account id. Example: "225494730938493804".
siteid	optional	Site id. Example: "225494730938493804".

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
bucketUrl	Bucket url	true	string
disableStream	disable events stream	true	boolean
accountonboardingexists	For site scope, is account onboarding exists	false	boolean
assumeRoleExternalId	The AWS assume role external id.	false	string
cloudProvider	Cloud provider, default is aws	false	string

			desiredFields	List of desired fields to be included in the output. If not specified, all fields are included.	false	string []
			error	Error message in case the bucket permissions is invalid	false	string
			globalOnboardingExists	Is global onboarding exists in table	false	boolean
			id	log-archive-rule id, default for accounts: cloud-funnel	false	string
			isInheriting	Is inheriting global setting	false	boolean
			query	Syql query to validate	false	string
			roleToAssume	The AWS role to assume when using assume role functionality. Only applicable if cloud_provider is s3.	false	string
			useAssumeRole	If set to true, activates the AWS AssumeRole functionality for accessing S3 buckets or other	false	boolean

				associated resources. Only applicable if cloud_provider is s3.		
errors	Errors	false	array			

Delete cloud funnel rule

DELETE /web/api/v2.1/cloud-funnel/onboarding

Deletes cloud funnel onboarding rule.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>error</td><td>Error message in case the bucket permissions is invalid</td><td>true</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountId</td><td>Account id</td><td>false</td><td>string</td></tr>
<tr><td>siteIds</td><td>Site ids</td><td>false</td><td>string []</td></tr>
</table>
</td></tr>
</table>

Post onboarding cloud funnel

POST /web/api/v2.1/cloud-funnel/onboarding

Post onboarding cloud funnel rule.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>bucketUrl</td><td>Bucket url</td><td>true</td><td>string</td></tr>
<tr><td>disableStream</td><td>disable events stream</td><td>true</td><td>boolean</td></tr>
<tr><td>accountonboardingexists</td><td>For site scope, is account onboarding exists</td><td>false</td><td>boolean</td></tr>
<tr><td>assumeRoleExternalId</td><td>The AWS assume role external id.</td><td>false</td><td>string</td></tr>
<tr><td>cloudProvider</td><td>Cloud provider, default is aws</td><td>false</td><td>string</td></tr>
<tr><td>desiredFields</td><td>List of desired fields to be included in the output. If not specified,</td><td>false</td><td>string []</td></tr>
</table>
</td></tr>
</table>

				all fields are included.		
			error	Error message in case the bucket permissions is invalid	false	string
			globalOnboardingExists	Is global onboarding exists in table	false	boolean
			id	log-archive-rule id, default for accounts: cloud-funnel	false	string
			isInheriting	Is inheriting global setting	false	boolean
			query	Syql query to validate	false	string
			roleToAssume	The AWS role to assume when using assume role functionality. Only applicable if cloud_provider is s3.	false	string
			useAssumeRole	If set to true, activates the AWS AssumeRole functionality for accessing S3 buckets or other associated resources. Only applicable if cloud_provider is s3.	false	boolean

errors	Errors	false	array

Body Schema

Name	Description	Required	Value
data	Data	true	

Name	Description	Required	Value
accountId	Account id	false	string
bucketUrl	bucket url	false	string
cloudProvider	Cloud provider, default is aws	false	string
desiredFields	List of desired fields to be included in the output. If not specified, all fields are included.	false	string []
disableStream	disable events stream	false	boolean
isInheriting	Is inheriting global setting	false	boolean
query	Syql query to validate	false	string
roleToAssume	The aws role to assume when using assume role functionality. Only applicable if cloud_provider is s3.	false	string
siteIds	Site ids	false	string []
useAssumeRole	If set to true, activates the AWS AssumeRole functionality for accessing	false	boolean

				S3 buckets or other associated resources. Only applicable if cloud_provider is s3.		

Create Estimator ID

POST /web/api/v2.1/cloud-funnel/estimator

Create estimator ID. This is needed to run the API "Get Estimate Size Of Events".

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>estimatorId</td><td>Estimator query id.</td><td>true</td><td>string</td></tr>
<tr><td>error</td><td>Error message in case the estimator query is invalid</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>Account ids</td><td>false</td><td>string []</td></tr>
<tr><td>desiredFields</td><td>List of desired fields to be included in the output. If not specified, all fields are included.</td><td>false</td><td>string []</td></tr>
<tr><td>query</td><td>Query</td><td>false</td><td>string</td></tr>
<tr><td>siteIds</td><td>Site ids</td><td>false</td><td>string []</td></tr>
</table>
</td></tr>
</table>

Get estimate size of events

GET /web/api/v2.1/cloud-funnel/estimator

Get estimate size of events in the bucket. You need the estimator ID which can be generated by running the API: "Create Estimator ID".

Parameters

estimatorid	required	Estimator query id.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
isCompleted	Is estimator query status is completed.	true	boolean
compressedBytes	Estimation of compressed size.	false	string
error	Error message in case the estimator query failed	false	string
matchingEvents	Estimation of events number. string to avoid round	false	string
uncompresse	Estimation of	false	string

			dBytes	uncompressed size.		
errors	Errors	false	array			

Cloud Provider Account

get cloud provider account active health events by cloud provider account id

GET /web/api/v2.1/cloudnative/account-management/active-health-events/{cloud_provider_account_id}

get cloud provider account active health events

Parameters

accountids	optional	List of Account IDs to filter by. Example: "225494730938493804,225494730938493915".
groupids	optional	List of Group IDs to filter by. Example: "225494730938493804,225494730938493915".
siteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".
tenant	optional	Indicates a tenant scope request

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
cloudProviderAccountId	Cloud Provider Account ID	false	string
description	Description	false	string
detectedAt	Detected at	false	string

			healthStatus | Health status | false | string recommendedAction | Recommended action | false | string title | Title | false | string
errors	Errors	false	array

Cloud Resources

Export cloud rogue resources to csv

GET /web/api/v2.1/cloudnative/cloud-rogues/export

Returns the results for given cloud rogues filter in a csv format

Parameters

exportformat	required	Export format. Example: "csv".
accountids	optional	List of Account IDs to filter by. Example: "225494730938493804,225494730938493915".
cloudprovideraccountid__contains	optional	Free-text filter by cloud account id (supports multiple values)
cloudprovideraccountname	optional	Filter by cloud account (supports multiple values)
cloudprovideraccountname__contains	optional	Free-text filter by cloud account (supports multiple values)
cloudprovidername	optional	Filter by cloud provider name (supports multiple values)
countonly	optional	If true, only total number of items will be returned, without any of the actual objects.
cursor	optional	Cursor position returned by the last request. Use to iterate over more than 1000 items. Example: "YWdlbnRfaWQ6NTgwMjkzODE=".
id__contains	optional	Free-text filter by id (supports multiple values)
image__contains	optional	Free-text filter by image (supports multiple values)
limit	optional	Limit number of returned items (1-1000). Example: "10".
name__contains	optional	Free-text filter by resource name (supports multiple values)
ostypes	optional	Included OS types. Example: "macos".
region	optional	Filter by region (supports multiple values)
region__contains	optional	Free-text filter by region (supports multiple values)

siteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".
skip	optional	Skip first number of items (0-1000). To iterate over more than 1000 items, use "cursor". Example: "150".
skipcount	optional	If true, total number of items will not be calculated, which speeds up execution time.
sortby	optional	The column to sort the results by. Example: "id".
sortorder	optional	Sort direction. Example: "asc".
virtual_network_id__contains	optional	Free-text filter by network id (supports multiple values)

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Get cloud rogue resources

GET /web/api/v2.1/cloudnative/cloud-rogues

Returns the cloud rogue resources for given filter

Parameters

accountids	optional	List of Account IDs to filter by. Example: "225494730938493804,225494730938493915".
cloudprovideraccountid__contains	optional	Free-text filter by cloud account id (supports multiple values)
cloudprovideraccountname	optional	Filter by cloud account (supports multiple values)
cloudprovideraccountname__contains	optional	Free-text filter by cloud account (supports multiple values)
cloudprovidername	optional	Filter by cloud provider name (supports multiple values)

countonly	optional	If true, only total number of items will be returned, without any of the actual objects.
cursor	optional	Cursor position returned by the last request. Use to iterate over more than 1000 items. Example: "YWdlbnRfaWQ6NTgwMjkzODE=".
id__contains	optional	Free-text filter by id (supports multiple values)
image__contains	optional	Free-text filter by image (supports multiple values)
limit	optional	Limit number of returned items (1-1000). Example: "10".
name__contains	optional	Free-text filter by resource name (supports multiple values)
ostypes	optional	Included OS types. Example: "macos".
region	optional	Filter by region (supports multiple values)
region__contains	optional	Free-text filter by region (supports multiple values)
siteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".
skip	optional	Skip first number of items (0-1000). To iterate over more than 1000 items, use "cursor". Example: "150".
skipcount	optional	If true, total number of items will not be calculated, which speeds up execution time.
sortby	optional	The column to sort the results by. Example: "id".
sortorder	optional	Sort direction. Example: "asc".
virtual_network_id__contains	optional	Free-text filter by network id (supports multiple values)

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
pagination	Pagination	true	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr></table>

	information		totalItems: Total number of items found matching your query; true; integer nextCursor: Pass this value as "cursor" on your next request, to get the next page of results (Will be "null" when last page reached); false; string
data	Response data	false	Name: resources; Description: Resources; Required: false; Value:

Name	Description	Required	Value
cloudProviderAccountId		false	string
cloudProviderAccountName		false	string
cloudProviderName		false	string
cloudProviderOrganization		false	string
createdTime		false	string
id	Cloud Resource ID	false	string
name		false	string
osType		false	string
osTypeIcon		false	string
region		false	string
resourceType		false	string
tags		false	object

						virtualNetworkId		false	string
errors	Errors	false	array						

Config Overrides

Get Config Overrides

GET /web/api/v2.1/config-override

There are different ways to override the configuration of an Agent, and the priority of changes depends on the endpoint OS and the version of the installed Agent. Use this command to see the configuration values that are changed for each Agent that matches the filter.

Parameters

accountids	optional	List of Account IDs to filter by. Example: "225494730938493804,225494730938493915".
agentids	optional	List of Agent IDs to filter by. Example: "225494730938493804,225494730938493915".
agentversions	optional	Included agent versions. Example: "2.5.1.1320".
countonly	optional	If true, only total number of items will be returned, without any of the actual objects.
createdat__between	optional	Date range for creation time (format: <from_timestamp>-<to_timestamp>, inclusive). Example: "1514978890136-1514978650130".
createdat__gt	optional	Config Overrides created after this timestamp. Example: "2018-02-27T04:49:26.257525Z".
createdat__gte	optional	Config Overrides created after or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
createdat__lt	optional	Config Overrides created before this timestamp. Example: "2018-02-27T04:49:26.257525Z".
createdat__lte	optional	Config Overrides created before or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
cursor	optional	Cursor position returned by the last request. Use to iterate over more than 1000 items. Example: "YWdlbnRfaWQ6NTgwMjkzODE=".
description__like	optional	Match description partially (substring)
groupids	optional	List of Group IDs to filter by. Example:

		"225494730938493804,225494730938493915".
ids	optional	List of ids to filter by. Example: "225494730938493804,225494730938493915".
limit	optional	Limit number of returned items (1-1000). Example: "10".
name__like	optional	Match name partially (substring)
ostypes	optional	Included OS types. Example: "macos".
query	optional	Free text search on fields name, description, agent_version, os_type, config
siteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".
skip	optional	Skip first number of items (0-1000). To iterate over more than 1000 items, use "cursor". Example: "150".
skipcount	optional	If true, total number of items will not be calculated, which speeds up execution time.
sortby	optional	The column to sort the results by. Example: "id".
sortorder	optional	Sort direction. Example: "asc".
tenant	optional	Indicates a tenant scope request
versionoption	optional	Version option. Example: "ALL".

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
pagination	Pagination information	true	

Name	Description	Required	Value
totalItems	Total number of items found matching	true	integer

				your query		
			nextCursor	Pass this value as "cursor" on your next request, to get the next page of results (Will be "null" when last page reached)	false	string
data	Response data	false	Name	Description	Required	Value
			description	Description	true	string
			name	Name	true	string
			account	Account	false	Name / Description / Required / Value id / Id / true / string name / Name / false / string
			agent	Agent	false	Name / Description / Required / Value id / Id / true / string
			agentVersion	Agent version	false	string
			config	Config	false	object
			group	Group	false	Name / Description / Required / Value id / Id / true / string name / Name / false / string
			id	Id	false	string
			osType	OS type	false	enum
			scope	Scope level	false	enum
			site	Site	false	Name / Description / Required / Value id / Id / true / string name / Name / false / string
			versionOptio	Version	false	enum

			n	option		
errors	Errors	false	array			

Create Config Override

POST /web/api/v2.1/config-override

Override the configuration of Agents that match the filter. Best practice: Run "support-actions/config" to get the complete syntax. This command requires a Global user or Support.

> **BEST PRACTICE**
> Run "support-actions/config" to get the complete syntax. This command requires a Global user or Support.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - Insufficient permissions

404 - Scope not found.

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
description	Description	true	string
name	Name	true	string
account	Account	false	
agent	Agent	false	
agentVersion	Agent version	false	string

Name	Description	Required	Value
id	Id	true	string
name	Name	false	string

Name	Description	Required	Value
id	Id	true	string

<table>
<tr><td></td><td></td><td></td><td>
<table>
<tr><td>config</td><td>Config</td><td>false</td><td>object</td></tr>
<tr><td>group</td><td>Group</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>id</td><td>Id</td><td>true</td><td>string</td></tr>
<tr><td>name</td><td>Name</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>id</td><td>Id</td><td>false</td><td>string</td></tr>
<tr><td>osType</td><td>OS type</td><td>false</td><td>enum</td></tr>
<tr><td>scope</td><td>Scope level</td><td>false</td><td>enum</td></tr>
<tr><td>site</td><td>Site</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>id</td><td>Id</td><td>true</td><td>string</td></tr>
<tr><td>name</td><td>Name</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>versionOption</td><td>Version option</td><td>false</td><td>enum</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>name</td><td>Name</td><td>true</td><td>string</td></tr>
<tr><td>osType</td><td>OS type</td><td>true</td><td>enum</td></tr>
<tr><td>scope</td><td>Scope level</td><td>true</td><td>enum</td></tr>
<tr><td>account</td><td>Config override will apply to all agents in the account. This should be used with scope = 'account'</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>id</td><td>Id</td><td>true</td><td>string</td></tr>
<tr><td>name</td><td>Name</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>agentVersion</td><td>Agent version</td><td>false</td><td>string</td></tr>
<tr><td>config</td><td>Config</td><td>false</td><td>object</td></tr>
<tr><td>description</td><td>Description</td><td>false</td><td>string</td></tr>
<tr><td>group</td><td>Config override will apply to all agents in the group. This should be used with scope = 'group'</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>id</td><td>Id</td><td>true</td><td>string</td></tr>
<tr><td>name</td><td>Name</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>site</td><td>Config override will apply to all agents in the site. This should be used with scope = 'site'</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>id</td><td>Id</td><td>true</td><td>string</td></tr>
<tr><td>name</td><td>Name</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>versionOption</td><td>Version option</td><td>false</td><td>enum</td></tr>
</table>
</td></tr>
<tr><td>filter</td><td>Filter</td><td>false</td><td></td></tr>
</table>

Delete Config Overrides

DELETE /web/api/v2.1/config-override

Delete overrides value. To get the required IDs, run "config-override".

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - Insufficient permissions

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>affected</td><td>Number of entities affected by the requested operation</td><td>false</td><td>integer</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>filter</td><td>Filter</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>agentIds</td><td>List of Agent IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>agentVersions</td><td>Included agent versions</td><td>false</td><td>string []</td></tr>
<tr><td>createdAt__between</td><td>Date range for creation time (format: <from_timestamp>-<to_timestamp>, inclusive)</td><td>false</td><td>string</td></tr>
<tr><td>createdAt__gt</td><td>Config Overrides created after this timestamp</td><td>false</td><td>string</td></tr>
<tr><td>createdAt__gte</td><td>Config Overrides created after or at this timestamp</td><td>false</td><td>string</td></tr>
<tr><td>createdAt__lt</td><td>Config Overrides created before this timestamp</td><td>false</td><td>string</td></tr>
<tr><td>createdAt__lte</td><td>Config Overrides created before or at this timestamp</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
</table>

			description__like	Match description partially (substring)	false	string
			groupIds	List of Group IDs to filter by	false	string []
			ids	List of ids to filter by	false	string []
			name__like	Match name partially (substring)	false	string
			osTypes	Included OS types	false	string []
			query	Free text search on fields name, description, agent_version, os_type, config	false	string
			siteIds	List of Site IDs to filter by	false	string []
			tenant	Indicates a tenant scope request	false	boolean
			versionOption	Version option	false	enum

Delete Config Override

DELETE /web/api/v2.1/config-override/{override_id}

Delete an override value. To get the required ID, run "config-override".

Response Messages

200 - Success

401 - Unauthorized access - please sign in and retry.

403 - Insufficient permissions

404 - Override not found.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>success</td><td>Indicates a successful operation</td><td>false</td><td>boolean</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Update Config Override

PUT /web/api/v2.1/config-override/{override_id}

Use this command to change the value of one configuration value. To get the required ID, run "config-override".

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - Insufficient permissions.

404 - Override not found.

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
description	Description	true	string
name	Name	true	string
account	Account	false	
agent	Agent	false	
agentVersion	Agent version	false	string
config	Config	false	object
group	Group	false	

Name	Description	Required	Value
id	Id	true	string
name	Name	false	string

Name	Description	Required	Value
id	Id	true	string

Name	Description	Required	Value
id	Id	true	string
name	Name	false	string

<table>
<tr><td></td><td></td><td></td><td>
<table>
<tr><td>id</td><td>Id</td><td>false</td><td>string</td></tr>
<tr><td>osType</td><td>OS type</td><td>false</td><td>enum</td></tr>
<tr><td>scope</td><td>Scope level</td><td>false</td><td>enum</td></tr>
<tr><td>site</td><td>Site</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>id</td><td>Id</td><td>true</td><td>string</td></tr>
<tr><td>name</td><td>Name</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>versionOption</td><td>Version option</td><td>false</td><td>enum</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>account</td><td>Account</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>id</td><td>Id</td><td>true</td><td>string</td></tr>
<tr><td>name</td><td>Name</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>agentVersion</td><td>Agent version</td><td>false</td><td>string</td></tr>
<tr><td>config</td><td>Config</td><td>false</td><td>object</td></tr>
<tr><td>description</td><td>Description</td><td>false</td><td>string</td></tr>
<tr><td>group</td><td>Group</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>id</td><td>Id</td><td>true</td><td>string</td></tr>
<tr><td>name</td><td>Name</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>name</td><td>Name</td><td>false</td><td>string</td></tr>
<tr><td>osType</td><td>OS type</td><td>false</td><td>enum</td></tr>
<tr><td>scope</td><td>Scope level</td><td>false</td><td>enum</td></tr>
<tr><td>site</td><td>Site</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>id</td><td>Id</td><td>true</td><td>string</td></tr>
<tr><td>name</td><td>Name</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>versionOption</td><td>Version option</td><td>false</td><td>enum</td></tr>
</table>
</td></tr>
<tr><td>filter</td><td>Filter</td><td>false</td><td></td></tr>
</table>

create_exclusion

Create Unified Exclusion

POST /web/api/v2.1/unified-exclusions

Create Exclusions to make your Agents suppress alerts and mitigation for items that you consider to be benign or which you require for interoperability.
IMPORTANT! Every Exclusion is a possible security hole. Do not create Exclusions unless you are sure this hash, path, certificate signer, file type, or browser is always benign.
Of course, if you can make the Exclusion by its hash or path, that is much more secure than excluding all detections of a specific signer, file type, or browser. We do not recommend the last types for Exclusions on production endpoints. These Exclusions might be helpful in a lab or pentester group. When you create an Exclusion, make sure you set the filter to the smallest possible scope. For example, if you can exclude security for this item on a group, do not enter values for siteIds or accountIds.
We recommend that you read "Not Recommended Exclusions: https://support.sentinelone.com/hc/en-us/articles/360007532894
and Best Practices for Exclusions: https://support.sentinelone.com/hc/en-us/articles/360008709014

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
pagination	Pagination information	true	

Name	Description	Required	Value
totalItems	Total number of items found matching your query	true	integer
nextCursor	Pass this value as "cursor" on your next request, to	false	string

			get the next page of results (Will be "null" when last page reached)
data	Response data	false	
errors	Errors	false	array

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>true</td><td></td></tr>
<tr><td>filter</td><td>Filter</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>groupIds</td><td>List of Group IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>siteIds</td><td>List of Site IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>tenant</td><td>Indicates a tenant scope request</td><td>false</td><td>boolean</td></tr>
</table>
</td></tr>
</table>

Validate Exclusion Item

POST /web/api/v2.1/unified-exclusions/validate

Check if an exclusion is on the list of SentinelOne items that are "Not Allowed" or "Not Recommended". This API returns one of the following statuses:
* Not Recommended: This item is not recommended by SentinelOne because it decreases security. For example, If you accidentally exclude a path that is too broad, malware can enter your environment.
* Not Allowed: This exclusion can harm the product and lead to unexpected functionality. From version North Pole SP3 you are prevented from creating Not Allowed exclusions.* None: This item is not on the list of SentinelOne items that are "Not Allowed" or "Not Recommended".

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>status</td><td>Recommendation for the exclusion/ blocklist item</td><td>false</td><td>enum</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>exclusionType</td><td>Unified exclusion type</td><td>true</td><td>enum</td></tr>
<tr><td>osType</td><td>OS type</td><td>true</td><td>enum</td></tr>
<tr><td>type</td><td>Exclusion type</td><td>true</td><td>enum</td></tr>
<tr><td>value</td><td>Value</td><td>true</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>filter</td><td>Filter</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>groupIds</td><td>List of Group IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>siteIds</td><td>List of Site IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>tenant</td><td>Indicates a tenant scope request</td><td>false</td><td>boolean</td></tr>
</table>
</td></tr>
</table>

Custom Detection Rule

Get Rules

GET /web/api/v2.1/cloud-detection/rules

Get a list of Custom Detection Rules for a given scope.
Note: You can create and see rules only for your highest available scope. For example, if your username has an access level of scope Account, you cannot see rules created for the Global scope or rules created for a specific Site.

Parameters

accountids	optional	List of Account IDs to filter by. Example: "225494730938493804,225494730938493915".
activeresponse	optional	The active response status for the rule.
countonly	optional	If true, only total number of items will be returned, without any of the actual objects.
creator__contains	optional	Free-text filter by rule creator. You can enter multiple values, separated by commas. Example: "Service Pack 1".
cursor	optional	Cursor position returned by the last request. Use to iterate over more than 1000 items. Example: "YWdlbnRfaWQ6NTgwMjkzODE=".
description__contains	optional	Free-text filter by rule description. You can enter multiple values, separated by commas. Example: "Service Pack 1".
disablepagination	optional	If True, all rules for the requested scope will be returned.
expirationmode	optional	The expiration mode. Example: "Permanent".
expired	optional	Rule expired or not.
groupids	optional	List of Group IDs to filter by. Example: "225494730938493804,225494730938493915".
ids	optional	To filter by Rule ID, enter one or more Rule IDs, separated by commas. Example: "225494730938493804,225494730938493915".
limit	optional	Limit number of returned items (1-1000). Example: "10".

name__contains	optional	Free-text filter by rule name. You can enter multiple values, separated by commas. Example: "Service Pack 1".
query	optional	Free-text filter by S1 query. You can enter multiple values, separated by commas. Example: "Service Pack 1".
querytype	optional	The query type. Example: "events".
reachedlimit	optional	Rule reached limit or not.
s1ql__contains	optional	Free-text filter by S1 query. You can enter multiple values, separated by commas. Example: "Service Pack 1".
scopes	optional	To filter by scope, enter one or more scopes, separated by commas. Example: "account".
siteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".
skip	optional	Skip first number of items (0-1000). To iterate over more than 1000 items, use "cursor". Example: "150".
skipcount	optional	If true, total number of items will not be calculated, which speeds up execution time.
sortby	optional	The column to sort the results by. Example: "id".
sortorder	optional	Sort direction. Example: "asc".
status	optional	To filter by status, enter one or more statuses, separated by commas. Example: "Draft".

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
pagination	Pagination information	true	

Name	Description	Required	Value
totalItems	Total number of items found	true	integer

				matching your query		
			nextCursor	Pass this value as "cursor" on your next request, to get the next page of results (Will be "null" when last page reached)	false	string
data	Response data	false				

Name	Description	Required	Value
expirationMode	Whether the rule is Temporary or Permanent.	true	enum
name	The name of the custom detection rule.	true	string
queryType	The query type - Correlation (made of multiple subqueries), Event (single query), or Processes (Deprecated).	true	enum
severity	The rule severity in your environment.	true	enum
status	Enabled (Activated and sends alerts if triggered) or	true	enum

				Disabled.		
			accountId	The account ID.	false	string
			accountName	The name of the account.	false	string
			activeResponse	The Active Response status of the Rule.	false	boolean
			correlationParams	Correlation params	false	

Name	Description	Required	Value
entity	A common entity used to group matching events.	true	enum
matchInOrder	Set to True to require subqueries to match in sequence to trigger an alert.	true	boolean
subQueries	The list of subqueries for the custom detection rule.	false	

Name	Description	Required	Value
matchesRequired	The number of times a subquery must match.	true	integer
subQuery	A subquery	true	string

Name	Description	Required	Value
timeWindow	The period of time in minutes in which subqueries must match to trigger an alert.	false	

Name	Description	Required	Value
windowMinutes	The period of time in minutes in which subqueries must match to trigger an alert.	false	integer

			createdAt	The date the	false	string

				rule was created.		
			creator	The full name of the user that created the rule.	false	string
			creatorId	The ID of the user that created the rule.	false	string
			description	The description of the custom detection rule.	false	string
			editable	True if the rule can be modified at this scope level.	false	boolean
			enrichment	Enrichment	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>creator</td><td>The ID of the user that created the Rule.</td><td>false</td><td>string</td></tr><tr><td>scopeName</td><td>scope id</td><td>false</td><td>string</td></tr><tr><td>updater</td><td>The ID of the user that last updated the Rule.</td><td>false</td><td>string</td></tr></table>
			expiration	If Temporary, the expiration date for the rule.	false	string
			expired	True if the Rule has expired.	false	boolean
			generatedAlerts	The number of alerts that	false	integer

				have been generated for the Rule.		
			id	Rule ID	false	string
			lastAlertTime	The time of the last alert for the Rule.	false	string
			networkQuarantine	True if the network quarantine is on.	false	boolean
			queryLang	The s1ql version query language of the rule. Can be 1.0 or 2.0.	false	enum
			reachedLimit	True if the Rule reached the 5k/hour or 10k/day alert limit. If the limit has been reached, the Rule is disabled.	false	boolean
			s1ql	The query.	false	string
			scope	The scope of the rule. Can be Global, Account, Site, or Group.	false	enum
			scopeId	The Account, Site, or Group ID, depending on the scope. Null if the scope is Global.	false	string []
			siteId	The site ID.	false	string
			siteName	The name of	false	string

				the site.		
			statusReason	The reason why the Rule has its current status.	false	string
			treatAsThreat	The Treat as threat auto response - UNDEFINED /suspicious/ malicious	false	enum
			updatedAt	The date the rule was last updated.	false	string
			updaterId	The ID of the user that last updated the rule.	false	string
errors	Errors	false	array			

Create Rule

POST /web/api/v2.1/cloud-detection/rules

Create a Custom Detection Rule for a scope specified by ID. To get the ID, run "accounts", "sites", "groups", or set "tenant" to "true" for Global.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
expirationMode	Whether the rule is Temporary or Permanent.	true	enum
name	The name of the custom detection rule.	true	string
queryType	The query type - Correlation (made of multiple subqueries), Event (single query), or Processes (Deprecated).	true	enum
severity	The rule severity in your environment.	true	enum

			status	Enabled (Activated and sends alerts if triggered) or Disabled.	true	enum
			correlationParams	Correlation params	false	

Name	Description	Required	Value
entity	A common entity used to group matching events.	true	enum
matchInOrder	Set to True to require subqueries to match in sequence to trigger an alert.	true	boolean
subQueries	The list of subqueries for the custom detection rule.	false	
timeWindow	The period of time in minutes in which subqueries must match to trigger an alert.	false	

Name	Description	Required	Value
matchesRequired	The number of times a subquery must match.	true	integer
subQuery	A subquery	true	string

Name	Description	Required	Value
windowMinutes	The period of time in minutes in which subqueries must match to trigger an alert.	false	integer

			createdAt	The date the rule was created.	false	string
			creator	The full name of the user	false	string

				that created the rule.		
			creatorId	The ID of the user that created the rule.	false	string
			description	The description of the custom detection rule.	false	string
			editable	True if the rule can be modified at this scope level.	false	boolean
			expiration	If Temporary, the expiration date for the rule.	false	string
			expired	True if the Rule has expired.	false	boolean
			id	Rule ID	false	string
			networkQuarantine	True if the network quarantine is on.	false	boolean
			queryLang	The s1ql version query language of the rule. Can be 1.0 or 2.0.	false	enum
			reachedLimit	True if the Rule reached the 5k/hour or 10k/day alert limit. If the limit has been reached, the	false	boolean

				Rule is disabled.		
			s1ql	The query.	false	string
			scope	The scope of the rule. Can be Global, Account, Site, or Group.	false	enum
			scopeId	The Account, Site, or Group ID, depending on the scope. Null if the scope is Global.	false	string []
			statusReason	The reason why the Rule has its current status.	false	string
			treatAsThreat	The Treat as threat auto response - UNDEFINED /suspicious/ malicious	false	enum
			updatedAt	The date the rule was last updated.	false	string
			updaterId	The ID of the user that last updated the rule.	false	string
errors	Errors	false	array			

Body Schema

Name	Description	Required	Value
data	Data	true	

Name	Description	Required	Value
expirationMode	Defines the rule as Permanent or Temporary.	true	enum
name	The name of the custom detection rule.	true	string
queryType	Define the query type: Correlation (made of multiple subqueries), Event (single query), or Processes (Deprecated).	true	enum
severity	The rule severity in your environment.	true	enum
status	Defines the rule is Enabled (Activated and sends alerts if triggered) or Disabled.	true	enum
correlationParams	Correlation params	false	

Name	Description	Required	Value
entity	A common entity used to group matching events.	true	enum

						matchInOrder	Set to True to require subqueries to match in sequence to trigger an alert.	true	boolean
						subQueries	The list of subqueries for the custom detection rule.	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>matchesRequired</td><td>The number of times a subquery must match.</td><td>true</td><td>integer</td></tr><tr><td>subQuery</td><td>A subquery</td><td>true</td><td>string</td></tr></table>
						timeWindow	The period of time in minutes in which subqueries must match to trigger an alert.	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>windowMinutes</td><td>The period of time in minutes in which subqueries must match to trigger an alert.</td><td>false</td><td>integer</td></tr></table>
				description	A description of the custom detection rule.	false	string		
				expiration	If the rule is Temporary, enter the expiration date for the rule.	false	string		
				id	Rule ID	false	string		
				networkQuarantine	Set to True to automatically quarantine the alerted endpoints.	false	boolean		
				queryLang	Defines the	false	enum		

<table>
<tr><td></td><td></td><td></td><td>
<table>
<tr><td></td><td>s1ql version query language of the rule - 1.0 or 2.0.</td><td></td><td></td></tr>
<tr><td>s1ql</td><td>The query</td><td>false</td><td>string</td></tr>
<tr><td>treatAsThreat</td><td>Defines the Treat as a threat auto response. Undefined, Suspicious, or Malicious.</td><td>false</td><td>enum</td></tr>
</table>
</td></tr>
<tr><td>filter</td><td>Filter</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>groupIds</td><td>List of Group IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>siteIds</td><td>List of Site IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>tenant</td><td>Indicates a tenant scope request</td><td>false</td><td>boolean</td></tr>
</table>
</td></tr>
</table>

Delete Rules

DELETE /web/api/v2.1/cloud-detection/rules

Deletes Custom Detection Rules that match a filter.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>affected</td><td>Number of entities affected by the requested operation</td><td>false</td><td>integer</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>filter</td><td>Filter</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>activeRespon se</td><td>The active response status for the rule.</td><td>false</td><td>boolean</td></tr>
<tr><td>creator__cont ains</td><td>Free-text filter by rule creator. You can enter multiple values, separated by commas.</td><td>false</td><td>string []</td></tr>
<tr><td>description__ contains</td><td>Free-text filter by rule description. You can enter multiple values, separated by commas.</td><td>false</td><td>string []</td></tr>
<tr><td>expirationMo de</td><td>The expiration mode.</td><td>false</td><td>enum</td></tr>
<tr><td>expired</td><td>Rule expired or not.</td><td>false</td><td>boolean</td></tr>
<tr><td>groupIds</td><td>List of Group IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>ids</td><td>To filter by Rule ID, enter one or more Rule IDs, separated by commas.</td><td>false</td><td>string []</td></tr>
</table>
</td></tr>
</table>

			name__contains	Free-text filter by rule name. You can enter multiple values, separated by commas.	false	string []
			query	Free-text filter by S1 query. You can enter multiple values, separated by commas.	false	string []
			queryType	The query type.	false	enum
			reachedLimit	Rule reached limit or not.	false	boolean
			s1ql__contains	Free-text filter by S1 query. You can enter multiple values, separated by commas.	false	string []
			scopes	To filter by scope, enter one or more scopes, separated by commas.	false	string []
			siteIds	List of Site IDs to filter by	false	string []
			status	To filter by status, enter one or more statuses, separated by commas.	false	string []

Update Rule

PUT /web/api/v2.1/cloud-detection/rules/{rule_id}

Change a Custom Detection rule.
This command requires the rule ID. (See Get Rules).

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

404 - Custom Detection rule not found

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>expirationMode</td><td>Whether the rule is Temporary or Permanent.</td><td>true</td><td>enum</td></tr>
<tr><td>name</td><td>The name of the custom detection rule.</td><td>true</td><td>string</td></tr>
<tr><td>queryType</td><td>The query type - Correlation (made of multiple subqueries), Event (single query), or Processes (Deprecated).</td><td>true</td><td>enum</td></tr>
</table>
</td></tr>
</table>

			severity	The rule severity in your environment.	true	enum
			status	Enabled (Activated and sends alerts if triggered) or Disabled.	true	enum
			correlationParams	Correlation params	false	

Name	Description	Required	Value
entity	A common entity used to group matching events.	true	enum
matchInOrder	Set to True to require subqueries to match in sequence to trigger an alert.	true	boolean
subQueries	The list of subqueries for the custom detection rule.	false	

Name	Description	Required	Value
matchesRequired	The number of times a subquery must match.	true	integer
subQuery	A subquery	true	string

Name	Description	Required	Value
timeWindow	The period of time in minutes in which subqueries must match to trigger an alert.	false	

Name	Description	Required	Value
windowMinutes	The period of time in minutes in which subqueries must match to trigger an alert.	false	integer

			createdAt	The date the	false	string

				rule was created.		
			creator	The full name of the user that created the rule.	false	string
			creatorId	The ID of the user that created the rule.	false	string
			description	The description of the custom detection rule.	false	string
			editable	True if the rule can be modified at this scope level.	false	boolean
			expiration	If Temporary, the expiration date for the rule.	false	string
			expired	True if the Rule has expired.	false	boolean
			id	Rule ID	false	string
			networkQuarantine	True if the network quarantine is on.	false	boolean
			queryLang	The s1ql version query language of the rule. Can be 1.0 or 2.0.	false	enum
			reachedLimit	True if the Rule reached the 5k/hour	false	boolean

				or 10k/day alert limit. If the limit has been reached, the Rule is disabled.		
			s1ql	The query.	false	string
			scope	The scope of the rule. Can be Global, Account, Site, or Group.	false	enum
			scopeId	The Account, Site, or Group ID, depending on the scope. Null if the scope is Global.	false	string []
			statusReason	The reason why the Rule has its current status.	false	string
			treatAsThreat	The Treat as threat auto response - UNDEFINED /suspicious/ malicious	false	enum
			updatedAt	The date the rule was last updated.	false	string
			updaterId	The ID of the user that last updated the rule.	false	string
errors	Errors	false	array			

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>expirationMode</td><td>Defines the rule as Permanent or Temporary.</td><td>true</td><td>enum</td></tr>
<tr><td>name</td><td>The name of the custom detection rule.</td><td>true</td><td>string</td></tr>
<tr><td>queryType</td><td>Define the query type: Correlation (made of multiple subqueries), Event (single query), or Processes (Deprecated).</td><td>true</td><td>enum</td></tr>
<tr><td>severity</td><td>The rule severity in your environment.</td><td>true</td><td>enum</td></tr>
<tr><td>status</td><td>Defines the rule is Enabled (Activated and sends alerts if triggered) or Disabled.</td><td>true</td><td>enum</td></tr>
<tr><td>correlationParams</td><td>Correlation params</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>entity</td><td>A common entity used to group matching events.</td><td>true</td><td>enum</td></tr>
</table>
</td></tr>
</table>
</td></tr>
</table>

						matchInOrder	Set to True to require subqueries to match in sequence to trigger an alert.	true	boolean
						subQueries	The list of subqueries for the custom detection rule.	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>matchesRequired</td><td>The number of times a subquery must match.</td><td>true</td><td>integer</td></tr><tr><td>subQuery</td><td>A subquery</td><td>true</td><td>string</td></tr></table>
						timeWindow	The period of time in minutes in which subqueries must match to trigger an alert.	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>windowMinutes</td><td>The period of time in minutes in which subqueries must match to trigger an alert.</td><td>false</td><td>integer</td></tr></table>
				description	A description of the custom detection rule.	false	string		
				expiration	If the rule is Temporary, enter the expiration date for the rule.	false	string		
				id	Rule ID	false	string		
				networkQuarantine	Set to True to automatically quarantine the alerted endpoints.	false	boolean		
				queryLang	Defines the	false	enum		

<table>
<tr><td></td><td></td><td></td><td>
<table>
<tr><td></td><td>s1ql version query language of the rule - 1.0 or 2.0.</td><td></td><td></td></tr>
<tr><td>s1ql</td><td>The query</td><td>false</td><td>string</td></tr>
<tr><td>treatAsThreat</td><td>Defines the Treat as a threat auto response. Undefined, Suspicious, or Malicious.</td><td>false</td><td>enum</td></tr>
</table>
</td></tr>
<tr><td>filter</td><td>Filter</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>groupIds</td><td>List of Group IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>siteIds</td><td>List of Site IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>tenant</td><td>Indicates a tenant scope request</td><td>false</td><td>boolean</td></tr>
</table>
</td></tr>
</table>

Activate Rules

PUT /web/api/v2.1/cloud-detection/rules/enable

Activate Custom Detection Rules based on a filter.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
data	Response data	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>affected</td><td>Number of entities affected by the requested operation</td><td>false</td><td>integer</td></tr></table>
errors	Errors	false	array

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>filter</td><td>Filter</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>activeRespon se</td><td>The active response status for the rule.</td><td>false</td><td>boolean</td></tr>
<tr><td>creator__cont ains</td><td>Free-text filter by rule creator. You can enter multiple values, separated by commas.</td><td>false</td><td>string []</td></tr>
<tr><td>description__ contains</td><td>Free-text filter by rule description. You can enter multiple values, separated by commas.</td><td>false</td><td>string []</td></tr>
<tr><td>expirationMo de</td><td>The expiration mode.</td><td>false</td><td>enum</td></tr>
<tr><td>expired</td><td>Rule expired or not.</td><td>false</td><td>boolean</td></tr>
<tr><td>groupIds</td><td>List of Group IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>ids</td><td>To filter by Rule ID, enter one or more Rule IDs, separated by commas.</td><td>false</td><td>string []</td></tr>
</table>
</td></tr>
</table>

			name__contains	Free-text filter by rule name. You can enter multiple values, separated by commas.	false	string []
			query	Free-text filter by S1 query. You can enter multiple values, separated by commas.	false	string []
			queryType	The query type.	false	enum
			reachedLimit	Rule reached limit or not.	false	boolean
			s1ql__contains	Free-text filter by S1 query. You can enter multiple values, separated by commas.	false	string []
			scopes	To filter by scope, enter one or more scopes, separated by commas.	false	string []
			siteIds	List of Site IDs to filter by	false	string []
			status	To filter by status, enter one or more statuses, separated by commas.	false	string []

Disable Rules

PUT /web/api/v2.1/cloud-detection/rules/disable

Disable Custom Detection Rules based on a filter.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>affected</td><td>Number of entities affected by the requested operation</td><td>false</td><td>integer</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

Name	Description	Required	Value
filter	Filter	true	

Name	Description	Required	Value
accountIds	List of Account IDs to filter by	false	string []
activeRespon se	The active response status for the rule.	false	boolean
creator__cont ains	Free-text filter by rule creator. You can enter multiple values, separated by commas.	false	string []
description__ contains	Free-text filter by rule description. You can enter multiple values, separated by commas.	false	string []
expirationMo de	The expiration mode.	false	enum
expired	Rule expired or not.	false	boolean
groupIds	List of Group IDs to filter by	false	string []
ids	To filter by Rule ID, enter one or more Rule IDs, separated by commas.	false	string []

			name__contains	Free-text filter by rule name. You can enter multiple values, separated by commas.	false	string []
			query	Free-text filter by S1 query. You can enter multiple values, separated by commas.	false	string []
			queryType	The query type.	false	enum
			reachedLimit	Rule reached limit or not.	false	boolean
			s1ql__contains	Free-text filter by S1 query. You can enter multiple values, separated by commas.	false	string []
			scopes	To filter by scope, enter one or more scopes, separated by commas.	false	string []
			siteIds	List of Site IDs to filter by	false	string []
			status	To filter by status, enter one or more statuses, separated by commas.	false	string []

Deep Visibility

Create Query and Get QueryId

POST /web/api/v2.1/dv/init-query

Start a Deep Visibility Query and get the queryId. You can use the queryId for other commands, such as Get Events and Get Query Status. For complete query syntax, see Query Syntax in the Knowledge Base (support.sentinelone.com) or the Console Help. SentinelOne Deep Visibility extends the ActiveEDR capabilities, with full visibility into endpoint data and threat hunting. Its kernel-based monitoring searches across endpoints for all indicators of compromise (IOC).
Rate limit: 1 call per minute for each different user token.
Note: From Management version Rio (February 2022) the default of "isVerbose" is "false" instead of "true".
Deep Visibility requires Complete SKU.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
queryId	A query unique identifier	true	string
queryModeInfo	Query mode info	false	

Name	Description	Required	Value
mode	The query mode	true	string
lastActivatedAt	The query mode last_activated_at date	false	string

errors	Errors	false	array

Body Schema

Name	Description	Required	Value
fromDate	Events created after this timestamp	true	string
query	Events matching the query search term will be returned	true	string
toDate	Events created before or at this timestamp	true	string
accountIds	List of Account IDs to filter by	false	string []
isVerbose	Show all fields or just priority fields	false	boolean
limit	Limit number of returned items (1-100000)	false	integer
queryType	Query Search Type - only one is allowed	false	string []
siteIds	List of Site IDs to filter by	false	string []
timeFrame	Time frame that the query was performed on, when omitted defaults to "Last 48	false	string

	Hours"		

Cancel Running Query

POST /web/api/v2.1/dv/cancel-query

Stop a Deep Visibility Query by queryId. The body is {"queryID":"string_ID"}. Get the ID of the Deep Visibility query or Power Query from "init-query". See "Create Query and get QueryId".
Deep Visibility requires Complete SKU.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>success</td><td>request success status</td><td>true</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

Name	Description	Required	Value
queryId	QueryId obtained when creating a query under Create Query	true	string

Get Query Status

GET /web/api/v2.1/dv/query-status

Get that status of a Deep Visibility Query. When the status is FINISHED, you can get the results with the queryId in "Get Events".
Deep Visibility requires Complete SKU.
Rate limit: 1 call per second for each different user token.
responseState can return these values: EMPTY_RESULTS, EVENTS_RUNNING, FAILED, FAILED_CLIENT, FINISHED, PLANNING, PROCESS_RUNNING, QUERY_CANCEL, QUERY_EXPIRED, QUERY_NOT_FOUND, QUERY_RUNNING, RUNNING, TIMED_OUT.

Parameters

queryid	required	QueryId obtained when creating a query under Create Query. Example: "q1xx2xx3".

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
progressStatus	Query loading status in percentage	true	integer
responseState	Response state	true	enum
queryModeInfo	Query mode info	false	

Name	Description	Required	Value
mode	The query mode	true	string
lastActivatedAt	The query mode last_activated	false	string

						_at date
			responseError	Relevant only for FAILED and FAILED_CLIENT DV errors	false	string
			warnings	Warnings	false	string
errors	Errors	false	array			

Get Events

GET /web/api/v2.1/dv/events

Get all Deep Visibility events from a queryId. You can use this command to send a sub-query, a new query to run on these events. Get the ID from "init-query". See "Create Query and get QueryId".
For complete documentation, see Query Syntax in the Knowledge Base (support.sentinelone.com) or the Console Help.

Parameters

queryid	required	QueryId obtained when creating a query under Create Query. Example: "q1xx2xx3".
cursor	optional	Cursor position returned by the last request. Should be used instead of skip. cursor currently supports sort by with createdAt, pid, processStartTime
limit	optional	Limit number of returned items (1-1000). Example: "10".
skip	optional	Skip first number of items (0-1000). To iterate over more than 1000 items, use "cursor". Example: "150".
sortby	optional	Events sorted by field. Example: "createdAt".
sortorder	optional	Event sorting order. Example: "asc".
subquery	optional	Create a sub query to run on the data that was already pulled

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
pagination	Pagination information	true	

Name	Description	Required	Value
totalItems	Total number of items found	true	integer

<table>
<tr><td></td><td></td><td></td><td>
<table>
<tr><td></td><td>matching your query</td><td></td><td></td></tr>
<tr><td>nextCursor</td><td>Pass this value as "cursor" on your next request, to get the next page of results (Will be "null" when last page reached)</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>agentDomain</td><td>Agent domain</td><td>true</td><td>string</td></tr>
<tr><td>agentGroupId</td><td>Agent group id</td><td>true</td><td>string</td></tr>
<tr><td>agentId</td><td>Agent id</td><td>true</td><td>string</td></tr>
<tr><td>agentInfected</td><td>Agent infected</td><td>true</td><td>boolean</td></tr>
<tr><td>agentIp</td><td>Agent ip</td><td>true</td><td>string</td></tr>
<tr><td>agentIsActive</td><td>Agent is active</td><td>true</td><td>boolean</td></tr>
<tr><td>agentIsDecommissioned</td><td>Agent is decommissioned</td><td>true</td><td>boolean</td></tr>
<tr><td>agentMachineType</td><td>Agent machine type</td><td>true</td><td>string</td></tr>
<tr><td>agentName</td><td>Agent name</td><td>true</td><td>string</td></tr>
<tr><td>agentNetworkStatus</td><td>Agent network status</td><td>true</td><td>string</td></tr>
<tr><td>agentOs</td><td>OS type</td><td>true</td><td>enum</td></tr>
<tr><td>agentUuid</td><td>Agent uuid</td><td>true</td><td>string</td></tr>
<tr><td>agentVersion</td><td>Agent version</td><td>true</td><td>string</td></tr>
<tr><td>createdAt</td><td>Created at</td><td>true</td><td>string</td></tr>
</table>
</td></tr>
</table>

			id	Id	true	string
			objectType	Object type	true	string
			processName	Process name	true	string
			siteName	Site name	true	string
			user	User	true	string
			connectionStatus	Connection status	false	string
			direction	Direction	false	string
			dnsRequest	Dns request	false	string
			dnsResponse	Dns response	false	string
			dstIp	Dst ip	false	string
			dstPort	Dst port	false	integer
			eventType	Event type	false	string
			fileFullName	File full name	false	string
			fileId	File id	false	string
			fileMd5	File md5	false	string
			fileSha1	File sha1	false	string
			fileSha256	File sha256	false	string
			fileSize	File size	false	string
			fileType	File type	false	string
			forensicUrl	Forensic url	false	string
			indicatorCategory	Indicator category	false	string
			indicatorDescription	Indicator description	false	string
			indicatorMetadata	Indicator metadata	false	string
			indicatorName	Indicator name	false	string
			isAgentVersionFullySupportedForPg	Is agent version fully supported for pg	false	boolean
			isAgentVersi	Is agent	false	string

			onFullySupportedForPgMessage	version fully supported for pg message		
			loginsBaseType	Logins base type	false	string
			loginsUserName	Logins user name	false	string
			md5	Md5	false	string
			networkMethod	Network method	false	string
			networkSource	Network source	false	string
			networkUrl	Network url	false	string
			oldFileMd5	Old file md5	false	string
			oldFileName	Old file name	false	string
			oldFileSha1	Old file sha1	false	string
			oldFileSha256	Old file sha256	false	string
			parentPid	Parent pid	false	string
			parentProcessGroupId	Parent process group id	false	string
			parentProcessIsMalicious	Parent process is malicious	false	boolean
			parentProcessName	Parent process name	false	string
			parentProcessStartTime	Parent process start time	false	string
			parentProcessUniqueKey	Parent process unique key	false	string
			pid	Pid	false	string
			processCmd	Process cmd	false	string
			processDisplayName	Process display name	false	string

			processGroupId	Process group id	false	string
			processImagePath	Process image path	false	string
			processImageSha1Hash	Process image sha1 hash	false	string
			processIntegrityLevel	Process integrity level	false	string
			processIsMalicious	Process is malicious	false	boolean
			processIsRedirectedCommandProcessor	Process is redirected command processor	false	string
			processIsWow64	Process is wow64	false	string
			processRoot	Process root	false	string
			processSessionId	Process session id	false	string
			processStartTime	Process start time	false	string
			processSubSystem	Process sub system	false	string
			processUniqueKey	Process unique key	false	string
			processUserName	Process user name	false	string
			publisher	Publisher	false	string
			registryId	Registry id	false	string
			registryPath	Registry path	false	string
			relatedToThreat	Related to threat	false	string
			rpid	Rpid	false	string
			sha1	Sha1	false	string
			sha256	Sha256	false	string
			signatureSign	Signature	false	string

			edInvalidReason: signed invalid reason signedStatus: Signed status, false, string srcIp: Src ip, false, string srcPort: Src port, false, integer srcProcDownloadToken: Src proc download token, false, string taskName: Task name, false, string taskPath: Task path, false, string threatStatus: Threat status, false, string tid: Tid, false, string trueContext: True context, false, string verifiedStatus: Verified status, false, string
errors	Errors	false	array

Get Process State

GET /web/api/v2.1/dv/process-state

Get details of all Deep Visibility processes from a queryId.To get the ID from "init-query". See "Create Query and get QueryId".

Parameters

queryid	required	QueryId obtained when creating a query under Create Query. Example: "q1xx2xx3".
cursor	optional	Cursor position returned by the last request. Use to iterate over more than 1000 items. Example: "YWdlbnRfaWQ6NTgwMjkzODE=".
limit	optional	Limit number of returned items (1-1000). Example: "10".
skip	optional	Skip first number of items (0-1000). To iterate over more than 1000 items, use "cursor". Example: "150".
sortby	optional	Events sorted by field. Example: "SrcProcStartTime".
sortorder	optional	Event sorting order. Example: "asc".

Response Messages

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Get Events By Type

GET /web/api/v2.1/dv/events/{event_type}

Get Deep Visibility results from the query that matches the given event type. Valid values for Event Type:
Process Exit
Process Modification
Process Creation
Duplicate Process Handle
Duplicate Thread Handle
Open Remote Process Handle
Remote Thread Creation
Remote Process Termination

Command Script
IP Connect
IP Listen
File Modification
File Creation
File Scan
File Deletion
File Rename
Pre Execution Detection
Login
Logout
GET
OPTIONS
POST
PUT
DELETE
CONNECT
HEAD
DNS Resolved
DNS Unresolved
Task Register
Task Update
Task Start
Task Trigger
Task Delete
Registry Key Create
Registry Key Rename
Registry Key Delete
Registry Key Export
Registry Key Security Changed
Registry Key Import
Registry Value Modified
Registry Value Create
Registry Value Delete
Behavioral Indicators
Module Load

Parameters

queryid	required	QueryId obtained when creating a query under Create Query. Example: "q1xx2xx3".

cursor	optional	Cursor position returned by the last request. Should be used instead of skip. cursor currently supports sort by with createdAt, pid, processStartTime
limit	optional	Limit number of returned items (1-1000). Example: "10".
skip	optional	Skip first number of items (0-1000). To iterate over more than 1000 items, use "cursor". Example: "150".
sortby	optional	Events sorted by field. Example: "createdAt".
sortorder	optional	Event sorting order. Example: "asc".
subquery	optional	Create a sub query to run on the data that was already pulled

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
pagination	Pagination information	true	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>totalItems</td><td>Total number of items found matching your query</td><td>true</td><td>integer</td></tr><tr><td>nextCursor</td><td>Pass this value as "cursor" on your next request, to get the next page of results (Will be "null" when last page reached)</td><td>false</td><td>string</td></tr></table>

data	Response data	false	

Name	Description	Required	Value
agentDomain	Agent domain	true	string
agentGroupId	Agent group id	true	string
agentId	Agent id	true	string
agentInfected	Agent infected	true	boolean
agentIp	Agent ip	true	string
agentIsActive	Agent is active	true	boolean
agentIsDecommissioned	Agent is decommissioned	true	boolean
agentMachineType	Agent machine type	true	string
agentName	Agent name	true	string
agentNetworkStatus	Agent network status	true	string
agentOs	OS type	true	enum
agentUuid	Agent uuid	true	string
agentVersion	Agent version	true	string
createdAt	Created at	true	string
id	Id	true	string
objectType	Object type	true	string
processName	Process name	true	string
siteName	Site name	true	string
user	User	true	string
connectionStatus	Connection status	false	string
direction	Direction	false	string
dnsRequest	Dns request	false	string
dnsResponse	Dns response	false	string
dstIp	Dst ip	false	string

			dstPort	Dst port	false	integer
			eventType	Event type	false	string
			fileFullName	File full name	false	string
			fileId	File id	false	string
			fileMd5	File md5	false	string
			fileSha1	File sha1	false	string
			fileSha256	File sha256	false	string
			fileSize	File size	false	string
			fileType	File type	false	string
			forensicUrl	Forensic url	false	string
			indicatorCategory	Indicator category	false	string
			indicatorDescription	Indicator description	false	string
			indicatorMetadata	Indicator metadata	false	string
			indicatorName	Indicator name	false	string
			isAgentVersionFullySupportedForPg	Is agent version fully supported for pg	false	boolean
			isAgentVersionFullySupportedForPgMessage	Is agent version fully supported for pg message	false	string
			loginsBaseType	Logins base type	false	string
			loginsUserName	Logins user name	false	string
			md5	Md5	false	string
			networkMethod	Network method	false	string
			networkSource	Network source	false	string
			networkUrl	Network url	false	string

			oldFileMd5	Old file md5	false	string
			oldFileName	Old file name	false	string
			oldFileSha1	Old file sha1	false	string
			oldFileSha256	Old file sha256	false	string
			parentPid	Parent pid	false	string
			parentProcessGroupId	Parent process group id	false	string
			parentProcessIsMalicious	Parent process is malicious	false	boolean
			parentProcessName	Parent process name	false	string
			parentProcessStartTime	Parent process start time	false	string
			parentProcessUniqueKey	Parent process unique key	false	string
			pid	Pid	false	string
			processCmd	Process cmd	false	string
			processDisplayName	Process display name	false	string
			processGroupId	Process group id	false	string
			processImagePath	Process image path	false	string
			processImageSha1Hash	Process image sha1 hash	false	string
			processIntegrityLevel	Process integrity level	false	string
			processIsMalicious	Process is malicious	false	boolean
			processIsRedirectedCommandProcessor	Process is redirected command	false	string

				processor		
			processIsWow64	Process is wow64	false	string
			processRoot	Process root	false	string
			processSessionId	Process session id	false	string
			processStartTime	Process start time	false	string
			processSubSystem	Process sub system	false	string
			processUniqueKey	Process unique key	false	string
			processUserName	Process user name	false	string
			publisher	Publisher	false	string
			registryId	Registry id	false	string
			registryPath	Registry path	false	string
			relatedToThreat	Related to threat	false	string
			rpid	Rpid	false	string
			sha1	Sha1	false	string
			sha256	Sha256	false	string
			signatureSignedInvalidReason	Signature signed invalid reason	false	string
			signedStatus	Signed status	false	string
			srcIp	Src ip	false	string
			srcPort	Src port	false	integer
			srcProcDownloadToken	Src proc download token	false	string
			taskName	Task name	false	string
			taskPath	Task path	false	string
			threatStatus	Threat status	false	string
			tid	Tid	false	string

			trueContext | True context | false | string verifiedStatus | Verified status | false | string
errors	Errors	false	array

Create a Power Query and Get QueryId

POST /web/api/v2.1/dv/events/pq

Start a Deep Visibility Power Query, get back status and potential results (ping afterwards using the queryId if query has not finished)

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>progress</td><td>Query loading status in percentage</td><td>true</td><td>integer</td></tr>
<tr><td>queryId</td><td>Query Id</td><td>true</td><td>string</td></tr>
<tr><td>status</td><td>Status</td><td>true</td><td>enum</td></tr>
<tr><td>columns</td><td>includes the name of the column and its type</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td></td><td></td><td>false</td><td>object</td></tr>
</table>
</td></tr>
<tr><td>data</td><td>Includes actual searched data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td></td><td></td><td>false</td><td>undefined []</td></tr>
</table>
</td></tr>
<tr><td>externalId</td><td>External Query Id</td><td>false</td><td>string</td></tr>
<tr><td>recommendations</td><td>possible action items to improve query results</td><td>false</td><td>string []</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

Name	Description	Required	Value
fromDate	Events created after this timestamp	true	string
query	Events matching the query search term will be returned	true	string
toDate	Events created before or at this timestamp	true	string
accountIds	List of Account IDs to filter by	false	string []
limit	Limit number of returned items (1-100000)	false	integer
siteIds	List of Site IDs to filter by	false	string []

Ping a Power Query if results haven't been retrieved

GET /web/api/v2.1/dv/events/pq-ping

Ping a Deep Visibility Power Query using the queryId if results have not returned from an initial Power Query or a previous ping

Parameters

queryid	optional	QueryId query param

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
progress	Query loading status in percentage	true	integer
queryId	Query Id	true	string
status	Status	true	enum
columns	includes the name of the column and its type	false	

Name	Description	Required	Value
		false	object

Name	Description	Required	Value
data	Includes actual searched data	false	

Name	Description	Required	Value
		false	undefined []

Name	Description	Required	Value
externalId	External Query Id	false	string
recommendations	possible action items	false	string []

				to improve query results		
errors	Errors	false	array			

Download source process file

GET /web/api/v2.1/dv/fetch-file

Download the source process file associated with a Deep Visibility event.

Parameters

downloadtoken	required	Download token

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

404 - File not found

Response Schema

Name	Description	Required	Value
data	Response data	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>downloadUrl</td><td>Download link</td><td>false</td><td>string</td></tr><tr><td>fileName</td><td>File name</td><td>false</td><td>string</td></tr></table>
errors	Errors	false	array

Device Control

Get Device Rules

GET /web/api/v2.1/device-control

Get the Device Control rules of a specified Account, Site, Group or Global (tenant) that match the filter.

Parameters

accesspermissions	optional	Access permission in. Example: "Read-Only".
accountids	optional	List of Account IDs to filter by. Example: "225494730938493804,225494730938493915".
actions	optional	Return device rules with the filtered action. Example: "Allow".
bluetoothaddresses	optional	Return device rules with the filtered bluetooth addresses.
countonly	optional	If true, only total number of items will be returned, without any of the actual objects.
createdat__between	optional	Return device rules created within this range (inclusive). Example: "1514978764288-1514978999999".
createdat__gt	optional	Return device rules created after this timestamp. Example: "2018-02-27T04:49:26.257525Z".
createdat__gte	optional	Return device rules created after or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
createdat__lt	optional	Return device rules created before this timestamp. Example: "2018-02-27T04:49:26.257525Z".
createdat__lte	optional	Return device rules created before or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
cursor	optional	Cursor position returned by the last request. Use to iterate over more than 1000 items. Example: "YWdlbnRfaWQ6NTgwMjkzODE=".
deviceclasses	optional	Return device rules with the filtered device class. Example: "02h".
deviceids	optional	Return device rules with the filtered device id. Example: "02".
deviceinformationserv	optional	Return device rules with the filtered device information service info

iceinfokeys		keys.
devicenames	optional	Return device rules with the filtered device names.
disablepagination	optional	If true, all rules for requested scope will be returned
gattservices	optional	Return device rules with the filtered GATT services.
groupids	optional	List of Group IDs to filter by. Example: "225494730938493804,225494730938493915".
ids	optional	List of ids to filter by. Example: "225494730938493804,225494730938493915".
interfaces	optional	Return device rules with the filtered interface. Example: "USB".
limit	optional	Limit number of returned items (1-1000). Example: "10".
manufacturernames	optional	Return device rules with the filtered manufacturer names.
minorclasses	optional	Return device rules with the filtered minor classes.
productids	optional	Return device rules with the filtered product id. Example: "02".
query	optional	A free-text search term, will match applicable attributes.
rulename	optional	Return device rules with the filtered rule name.
scopes	optional	Return only device rules in this scope. Example: "account".
serviceclasses	optional	Return device rules with the filtered service class. Example: "02".
siteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".
skip	optional	Skip first number of items (0-1000). To iterate over more than 1000 items, use "cursor". Example: "150".
skipcount	optional	If true, total number of items will not be calculated, which speeds up execution time.
sortby	optional	The column to sort the results by. Example: "id".
sortorder	optional	Sort direction. Example: "asc".
statuses	optional	Return device rules with the filtered status. Example: "Enabled".
tenant	optional	Indicates a tenant scope request
uids	optional	Return device rules with the filtered uId.
vendorids	optional	Return device rules with the filtered vendor id.
versions	optional	Return device rules with the filtered versions.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>pagination</td><td>Pagination information</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>totalItems</td><td>Total number of items found matching your query</td><td>true</td><td>integer</td></tr>
<tr><td>nextCursor</td><td>Pass this value as "cursor" on your next request, to get the next page of results (Will be "null" when last page reached)</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accessPermission</td><td>Access permission</td><td>false</td><td>enum</td></tr>
<tr><td>action</td><td>Defines if agent shall Block or Allow use of devices which matches the rule parameters.</td><td>false</td><td>enum</td></tr>
</table>
</td></tr>
</table>

			bluetoothAddress	Bluetooth Address	false	string
			createdAt	Date of rule creation	false	string
			creator	Full name of the creating user	false	string
			creatorId	Id of the creating user	false	string
			deviceClass	The Device Class key. Valid for all rule types.	false	string
			deviceClassName	The Device Class name. Valid for all rule types.	false	
			deviceId	The id of the physical device connected to the interface.	false	string
			deviceInformationServiceInfoKey	Device Information Service Info Key	false	string
			deviceInformationServiceInfoValue	Device Information Service Info Value	false	string
			deviceName	Device Name	false	string
			editable	True if the rule can be modified at this scope level	false	boolean
			gattService	GATT Service IDs	false	string []
			id	Rule ID	false	string
			interface	The physical	false	enum

				bus type of the device.		
			manufacturerName	Manufacturer Name	false	string
			minorClasses	List of Bluetooth minor classes	false	string []
			order	Position in the list of rules	false	integer
			productId	Product identifier. Unique for a specific product module, per vendor ID, Interface.	false	string
			ruleName	The name of the device rule.	false	string
			ruleType	Defines a set of fields that are mandatory.	false	enum
			scope	Scope of the rule	false	enum
			scopeId	The id representing a group or a site dependent on the scope	false	string
			scopeName	Extended name of the scope	false	string
			status	Defines if rule is Enabled or Disabled.	false	enum
			uid	Relevant USB	false	string

			Mass storage devices only (Interface=USB, Class=mass storage).		
			updatedAt	Date of last update	false	string
			vendorId	Vendor identifier. Mandatory when rule type is vendor id or product id.	false	string
			version	Vendor identifier. Mandatory when rule type is vendor id or product id.	false	string
errors	Errors	false	array			

Create Device Control Rule

POST /web/api/v2.1/device-control

Use this command to create a new Device Control rule. These rules allow or block devices, based on device identifiers. Rules apply to a scope: Global (tenant), Account, Site, or Group. To learn details of the fields, see https://support.sentinelone.com/hc/en-us/articles/360023338494.
Recommended: Before you begin, see Device Control Known Limitations: https://support.sentinelone.com/hc/en-us/articles/360021104114.
Device Control requires Control SKU. Linux Agents do not support Device Control.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
accessPermission	Access permission	false	enum
action	Defines if agent shall Block or Allow use of devices which matches the rule parameters.	false	enum
bluetoothAddress	Bluetooth Address	false	string
createdAt	Date of rule creation	false	string
creator	Full name of the creating user	false	string

			creatorId	Id of the creating user	false	string
			deviceClass	The Device Class key. Valid for all rule types.	false	string
			deviceClass Name	The Device Class name. Valid for all rule types.	false	
			deviceId	The id of the physical device connected to the interface.	false	string
			deviceInformationServiceInfoKey	Device Information Service Info Key	false	string
			deviceInformationServiceInfoValue	Device Information Service Info Value	false	string
			deviceName	Device Name	false	string
			editable	True if the rule can be modified at this scope level	false	boolean
			gattService	GATT Service IDs	false	string []
			id	Rule ID	false	string
			interface	The physical bus type of the device.	false	enum
			manufacturerName	Manufacturer Name	false	string
			minorClasses	List of Bluetooth minor classes	false	string []

			order	Position in the list of rules	false	integer
			productId	Product identifier. Unique for a specific product module, per vendor ID, Interface.	false	string
			ruleName	The name of the device rule.	false	string
			ruleType	Defines a set of fields that are mandatory.	false	enum
			scope	Scope of the rule	false	enum
			scopeId	The id representing a group or a site dependent on the scope	false	string
			scopeName	Extended name of the scope	false	string
			status	Defines if rule is Enabled or Disabled.	false	enum
			uid	Relevant USB Mass storage devices only (Interface=USB, Class=mass storage).	false	string
			updatedAt	Date of last update	false	string

			vendorId: Vendor identifier. Mandatory when rule type is vendor id or product id. — false — string version: Vendor identifier. Mandatory when rule type is vendor id or product id. — false — string
errors	Errors	false	array

Body Schema

Name	Description	Required	Value
data	Data	true	

Name	Description	Required	Value
action	Defines if agent shall Block or Allow use of devices which matches the rule parameters.	true	enum
interface	The physical bus type of the device.	true	enum
ruleName	The name of the device rule.	true	string
ruleType	Rule type. Depending on the type, each rule requires different parameters.	true	enum
status	Defines if rule is Enabled or Disabled.	true	enum
accessPermission	Access permission	false	enum
bluetoothAddress	Bluetooth Address	false	string
deviceClass	The Device Class	false	string
deviceId	Physical device identifier. Mandatory when rule	false	string

				type is device id.		
			deviceInformationServiceInfoKey	Device Information Service Info Key	false	string
			deviceInformationServiceInfoValue	Device Information Service Info Value	false	string
			deviceName	Device Name	false	string
			gattService	Gatt service	false	string []
			manufacturerName	Manufacturer Name	false	string
			minorClasses	Minor classes	false	string []
			productId	Product identifier. Unique for a specific product module, per vendor ID, Interface.	false	string
			serviceClass	Relevant for Bluetooth devices only	false	string
			uid	Relevant USB Mass storage devices only (Interface=USB, Class=mass storage).	false	string
			vendorId	Vendor identifier. Mandatory when rule type is vendor id or product id.	false	string
			version	The version	false	string

			of the device.
filter	Filter	true	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr><tr><td>groupIds</td><td>List of Group IDs to filter by</td><td>false</td><td>string []</td></tr><tr><td>siteIds</td><td>List of Site IDs to filter by</td><td>false</td><td>string []</td></tr><tr><td>tenant</td><td>Indicates a tenant scope request</td><td>false</td><td>boolean</td></tr></table>

Delete Rules

DELETE /web/api/v2.1/device-control

Delete Device Control rules that match the filter.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>affected</td><td>Number of entities affected by the requested operation</td><td>false</td><td>integer</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>filter</td><td>Filter</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accessPermissions</td><td>Access permission in</td><td>false</td><td>string []</td></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>actions</td><td>Return device rules with the filtered action.</td><td>false</td><td>string []</td></tr>
<tr><td>bluetoothAddresses</td><td>Return device rules with the filtered bluetooth addresses.</td><td>false</td><td>string []</td></tr>
<tr><td>createdAt__between</td><td>Return device rules created within this range (inclusive)</td><td>false</td><td>string</td></tr>
<tr><td>createdAt__gt</td><td>Return device rules created after this timestamp.</td><td>false</td><td>string</td></tr>
<tr><td>createdAt__gte</td><td>Return device rules created after or at this timestamp.</td><td>false</td><td>string</td></tr>
<tr><td>createdAt__lt</td><td>Return device rules created before this timestamp.</td><td>false</td><td>string</td></tr>
<tr><td>createdAt__lte</td><td>Return device rules created before or at this timestamp.</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
</table>

			deviceClasses	Return device rules with the filtered device class.	false	string []
			deviceIds	Return device rules with the filtered device id.	false	string []
			deviceInformationServiceInfoKeys	Return device rules with the filtered device information service info keys.	false	string []
			deviceNames	Return device rules with the filtered device names.	false	string []
			gattServices	Return device rules with the filtered GATT services.	false	string []
			groupIds	List of Group IDs to filter by	false	string []
			ids	List of ids to filter by	false	string []
			interfaces	Return device rules with the filtered interface.	false	string []
			manufacturerNames	Return device rules with the filtered manufacturer names.	false	string []
			minorClasses	Return device rules with the filtered minor classes.	false	string []

	productIds	Return device rules with the filtered product id.	false	string []
	query	A free-text search term, will match applicable attributes.	false	string
	ruleName	Return device rules with the filtered rule name.	false	string
	scopes	Return only device rules in this scope	false	string []
	serviceClasses	Return device rules with the filtered service class.	false	string []
	siteIds	List of Site IDs to filter by	false	string []
	statuses	Return device rules with the filtered status.	false	string []
	tenant	Indicates a tenant scope request	false	boolean
	uids	Return device rules with the filtered uId.	false	string []
	vendorIds	Return device rules with the filtered vendor id.	false	string []
	versions	Return device rules with the filtered versions.	false	string []

Update Device Rule

PUT /web/api/v2.1/device-control/{rule_id}

Change the Device Control rule that matches the filter. To learn more about the fields, see https://support.sentinelone.com/hc/en-us/articles/360023338494.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

404 - Device rule not found

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
accessPermission	Access permission	false	enum
action	Defines if agent shall Block or Allow use of devices which matches the rule parameters.	false	enum
bluetoothAddress	Bluetooth Address	false	string
createdAt	Date of rule creation	false	string
creator	Full name of the creating user	false	string
creatorId	Id of the	false	string

				creating user		
			deviceClass	The Device Class key. Valid for all rule types.	false	string
			deviceClass Name	The Device Class name. Valid for all rule types.	false	
			deviceId	The id of the physical device connected to the interface.	false	string
			deviceInformationServiceInfoKey	Device Information Service Info Key	false	string
			deviceInformationServiceInfoValue	Device Information Service Info Value	false	string
			deviceName	Device Name	false	string
			editable	True if the rule can be modified at this scope level	false	boolean
			gattService	GATT Service IDs	false	string []
			id	Rule ID	false	string
			interface	The physical bus type of the device.	false	enum
			manufacturerName	Manufacturer Name	false	string
			minorClasses	List of Bluetooth minor classes	false	string []
			order	Position in	false	integer

				the list of rules		
			productId	Product identifier. Unique for a specific product module, per vendor ID, Interface.	false	string
			ruleName	The name of the device rule.	false	string
			ruleType	Defines a set of fields that are mandatory.	false	enum
			scope	Scope of the rule	false	enum
			scopeId	The id representing a group or a site dependent on the scope	false	string
			scopeName	Extended name of the scope	false	string
			status	Defines if rule is Enabled or Disabled.	false	enum
			uid	Relevant USB Mass storage devices only (Interface=USB, Class=mass storage).	false	string
			updatedAt	Date of last update	false	string

			vendorId	Vendor identifier. Mandatory when rule type is vendor id or product id.	false	string
			version	Vendor identifier. Mandatory when rule type is vendor id or product id.	false	string
errors	Errors	false	array			

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accessPermission</td><td>Access permission</td><td>false</td><td>enum</td></tr>
<tr><td>action</td><td>Defines if agent shall Block or Allow use of devices which matches the rule parameters.</td><td>false</td><td>enum</td></tr>
<tr><td>bluetoothAddress</td><td>Bluetooth Address</td><td>false</td><td>string</td></tr>
<tr><td>deviceClass</td><td>The Device Class</td><td>false</td><td>string</td></tr>
<tr><td>deviceId</td><td>Physical device identifier. Mandatory when rule type is device id.</td><td>false</td><td>string</td></tr>
<tr><td>deviceInformationServiceInfoKey</td><td>Device Information Service Info Key</td><td>false</td><td>string</td></tr>
<tr><td>deviceInformationServiceInfoValue</td><td>Device Information Service Info Value</td><td>false</td><td>string</td></tr>
<tr><td>deviceName</td><td>Device Name</td><td>false</td><td>string</td></tr>
<tr><td>gattService</td><td>Gatt service</td><td>false</td><td>string []</td></tr>
<tr><td>interface</td><td>Defines the Physical bus type of the Device.</td><td>false</td><td>enum</td></tr>
</table>
</td></tr>
</table>

			manufacturerName	Manufacturer Name	false	string
			minorClasses	Minor classes	false	string []
			productId	Product identifier. Unique for a specific product module, per vendor ID, Interface.	false	string
			ruleName	The name of the device rule.	false	string
			ruleType	Rule type. Depending on the type, each rule requires different parameters.	false	enum
			serviceClass	Relevant for Bluetooth devices only	false	string
			status	Defines if rule is Enabled or Disabled.	false	enum
			uid	Relevant USB Mass storage devices only (Interface=USB, Class=mass storage).	false	string
			vendorId	Vendor identifier. Mandatory when rule type is vendor id or product id.	false	string

			version	The version of the device.	false	string

Copy Rules

POST /web/api/v2.1/device-control/copy-rules

You can copy a set of Device Control rules to use in other Accounts, Sites, or Groups. Copy the rules from a source Group, Site, or Account to target Groups, Sites, or Accounts.
Define the rules to copy with the filters. To get the values for devices, run "unscoped". To get Account IDs, run "accounts". To get Site IDs, run "sites".
Device Control requires Control SKU. Linux Agents do not support Device Control.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>affected</td><td>Number of entities affected by the requested operation</td><td>false</td><td>integer</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>filter</td><td>Filter</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accessPermissions</td><td>Access permission in</td><td>false</td><td>string []</td></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>actions</td><td>Return device rules with the filtered action.</td><td>false</td><td>string []</td></tr>
<tr><td>bluetoothAddresses</td><td>Return device rules with the filtered bluetooth addresses.</td><td>false</td><td>string []</td></tr>
<tr><td>createdAt__between</td><td>Return device rules created within this range (inclusive)</td><td>false</td><td>string</td></tr>
<tr><td>createdAt__gt</td><td>Return device rules created after this timestamp.</td><td>false</td><td>string</td></tr>
<tr><td>createdAt__gte</td><td>Return device rules created after or at this timestamp.</td><td>false</td><td>string</td></tr>
<tr><td>createdAt__lt</td><td>Return device rules created before this timestamp.</td><td>false</td><td>string</td></tr>
<tr><td>createdAt__lte</td><td>Return device rules created before or at this timestamp.</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
</table>

			deviceClasses	Return device rules with the filtered device class.	false	string []
			deviceIds	Return device rules with the filtered device id.	false	string []
			deviceInformationServiceInfoKeys	Return device rules with the filtered device information service info keys.	false	string []
			deviceNames	Return device rules with the filtered device names.	false	string []
			gattServices	Return device rules with the filtered GATT services.	false	string []
			groupIds	List of Group IDs to filter by	false	string []
			ids	List of ids to filter by	false	string []
			interfaces	Return device rules with the filtered interface.	false	string []
			manufacturerNames	Return device rules with the filtered manufacturer names.	false	string []
			minorClasses	Return device rules with the filtered minor classes.	false	string []

			productIds	Return device rules with the filtered product id.	false	string []
			query	A free-text search term, will match applicable attributes.	false	string
			ruleName	Return device rules with the filtered rule name.	false	string
			scopes	Return only device rules in this scope	false	string []
			serviceClasses	Return device rules with the filtered service class.	false	string []
			siteIds	List of Site IDs to filter by	false	string []
			statuses	Return device rules with the filtered status.	false	string []
			tenant	Indicates a tenant scope request	false	boolean
			uids	Return device rules with the filtered uId.	false	string []
			vendorIds	Return device rules with the filtered vendor id.	false	string []
			versions	Return device rules with the filtered versions.	false	string []

data	Data	false	

Name	Description	Required	Value
accountId	Target account (or "null" for global scope)	false	string
groupIds	Target group(s)	false	string []
siteId	Target site (or "null" for global scope)	false	string

Move rules

POST /web/api/v2.1/device-control/move-rules

You can move a set of Device Control rules to other Accounts, Sites, or Groups. This command removes the rule from the source and copies to the targets. Define the rules to copy with the filters. To get the values for devices, run "unscoped". To get Account IDs, run "accounts". To get Site IDs, run "sites". Device Control requires Control SKU. Linux Agents do not support Device Control.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>affected</td><td>Number of entities affected by the requested operation</td><td>false</td><td>integer</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

Name	Description	Required	Value
filter	Filter	true	

Name	Description	Required	Value
accessPermissions	Access permission in	false	string []
accountIds	List of Account IDs to filter by	false	string []
actions	Return device rules with the filtered action.	false	string []
bluetoothAddresses	Return device rules with the filtered bluetooth addresses.	false	string []
createdAt__between	Return device rules created within this range (inclusive)	false	string
createdAt__gt	Return device rules created after this timestamp.	false	string
createdAt__gte	Return device rules created after or at this timestamp.	false	string
createdAt__lt	Return device rules created before this timestamp.	false	string
createdAt__lte	Return device rules created before or at this timestamp.	false	string

			deviceClasses	Return device rules with the filtered device class.	false	string []
			deviceIds	Return device rules with the filtered device id.	false	string []
			deviceInformationServiceInfoKeys	Return device rules with the filtered device information service info keys.	false	string []
			deviceNames	Return device rules with the filtered device names.	false	string []
			gattServices	Return device rules with the filtered GATT services.	false	string []
			groupIds	List of Group IDs to filter by	false	string []
			ids	List of ids to filter by	false	string []
			interfaces	Return device rules with the filtered interface.	false	string []
			manufacturerNames	Return device rules with the filtered manufacturer names.	false	string []
			minorClasses	Return device rules with the filtered minor classes.	false	string []

			productIds	Return device rules with the filtered product id.	false	string []
			query	A free-text search term, will match applicable attributes.	false	string
			ruleName	Return device rules with the filtered rule name.	false	string
			scopes	Return only device rules in this scope	false	string []
			serviceClasses	Return device rules with the filtered service class.	false	string []
			siteIds	List of Site IDs to filter by	false	string []
			statuses	Return device rules with the filtered status.	false	string []
			tenant	Indicates a tenant scope request	false	boolean
			uids	Return device rules with the filtered uId.	false	string []
			vendorIds	Return device rules with the filtered vendor id.	false	string []
			versions	Return device rules with the filtered versions.	false	string []

data	Data	false	

Name	Description	Required	Value
accountId	Target account (or "null" for global scope)	false	string
groupIds	Target group(s)	false	string []
siteId	Target site (or "null" for global scope)	false	string

Reorder Rules

PUT /web/api/v2.1/device-control/reorder

When an external device connects to an endpoint, the SentinelOne Agent looks at the rules based on their order in the Device Control policy, from the top to the bottom. When the Agent finds a rule that matches the device identifiers of a connected device, that rule is applied. The Agent does not continue to the lower rules in the list.
Use this command to change the order of rules for a specific scope.
Device Control requires Control SKU. Linux Agents do not support Device Control.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
data	Response data	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>success</td><td>Indicates a successful operation</td><td>false</td><td>boolean</td></tr></table>
errors	Errors	false	array

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>filter</td><td>Filter</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>interface</td><td>The physical bus type of the device.</td><td>true</td><td>enum</td></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>groupIds</td><td>List of Group IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>siteIds</td><td>List of Site IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>tenant</td><td>Indicates a tenant scope request</td><td>false</td><td>boolean</td></tr>
</table>
</td></tr>
<tr><td>data</td><td>Data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>id</td><td>Rule ID</td><td>true</td><td>string</td></tr>
<tr><td>order</td><td>Desired position in the list of rules</td><td>true</td><td>integer</td></tr>
</table>
</td></tr>
</table>

Get Configuration

GET /web/api/v2.1/device-control/configuration

Get Device Control configuration for a given scope.
To filter the results for a scope:
* Global - Make sure "tenant" is "true" and no other scope ID is given.
* Account - Make sure "tenant" is "false" and at least one Account ID is given.
* Site - Make sure "tenant" is "false" and at least one Site ID is given.<brDevice Control requires Control SKU. It is not supported on Linux.

Parameters

accountids	optional	List of Account IDs to filter by. Example: "225494730938493804,225494730938493915".
groupids	optional	List of Group IDs to filter by. Example: "225494730938493804,225494730938493915".
siteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".
tenant	optional	Indicates a tenant scope request

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
disableBleCommunication	Disable Bluetooth LE Communication	false	boolean
disableRfcomm	Disable RFCOMM for	false	boolean

			Bluetooth devices		
			disallowAccessPermissionControl	Disallow access permission control (i.e. treat Read-Only rules as Read-Write)	false	boolean
			enabled	Device control enabled for the scope	false	boolean
			inheritedFrom	If null it means it is own policy else it will be site or global to state which policy is being inherited.	false	string
			inherits	True if rules are decoupled from parent rules	false	boolean
			reportApproved	Agent should report connected/disconnected events	false	boolean
			reportBlocked	Agent should report blocked events	false	boolean
			reportReadOnly	Agent should report 'connected as read-only' events	false	boolean
errors	Errors	false	array

Update Configuration

PUT /web/api/v2.1/device-control/configuration

Use this command to change the Device Control configuration. Enter a Group ID, Site ID, Account ID, or "tenant = true". If you select only tenant, and the other scopes are empty, the change is applied to the Global policy.
Device Control requires Control SKU. It is not supported on Linux.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>disableBleCommunication</td><td>Disable Bluetooth LE Communication</td><td>false</td><td>boolean</td></tr>
<tr><td>disableRfcomm</td><td>Disable RFCOMM for Bluetooth devices</td><td>false</td><td>boolean</td></tr>
<tr><td>disallowAccessPermissionControl</td><td>Disallow access permission control (i.e. treat Read-Only rules as Read-Write)</td><td>false</td><td>boolean</td></tr>
<tr><td>enabled</td><td>Device control enabled for the scope</td><td>false</td><td>boolean</td></tr>
</table>
</td></tr>
</table>

			inheritedFrom: If null it means it is own policy else it will be site or global to state which policy is being inherited. — false — string inherits: True if rules are decoupled from parent rules — false — boolean reportApproved: Agent should report connected/disconnected events — false — boolean reportBlocked: Agent should report blocked events — false — boolean reportReadOnly: Agent should report 'connected as read-only' events — false — boolean
errors	Errors	false	array

Body Schema

Name	Description	Required	Value
data	Data	true	

Name	Description	Required	Value
disableBleCommunication	Disable Bluetooth LE Communication	false	boolean
disableRfcomm	Disable RFCOMM for Bluetooth devices	false	boolean
disallowAccessPermissionControl	Disallow access permission control (i.e. treat Read-Only rules as Read-Write)	false	boolean
enabled	Device control enabled for the scope	false	boolean
inheritedFrom	If null it means it is own policy else it will be site or global to state which policy is being inherited.	false	string
inherits	True if rules are decoupled from parent rules	false	boolean
reportApproved	Agent should report connected/disconnected events	false	boolean

			reportBlocked: Agent should report blocked events — false — boolean reportReadOnly: Agent should report 'connected as read-only' events — false — boolean
filter	Filter	true	accountIds: List of Account IDs to filter by — false — string [] groupIds: List of Group IDs to filter by — false — string [] siteIds: List of Site IDs to filter by — false — string [] tenant: Indicates a tenant scope request — false — boolean

Export Rules

GET /web/api/v2.1/device-control/export

Export Device Control rules to a CSV file.

Parameters

accesspermissions	optional	Access permission in. Example: "Read-Only".
accountids	optional	List of Account IDs to filter by. Example: "225494730938493804,225494730938493915".
actions	optional	Return device rules with the filtered action. Example: "Allow".
bluetoothaddresses	optional	Return device rules with the filtered bluetooth addresses.
createdat__between	optional	Return device rules created within this range (inclusive). Example: "1514978764288-1514978999999".
createdat__gt	optional	Return device rules created after this timestamp. Example: "2018-02-27T04:49:26.257525Z".
createdat__gte	optional	Return device rules created after or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
createdat__lt	optional	Return device rules created before this timestamp. Example: "2018-02-27T04:49:26.257525Z".
createdat__lte	optional	Return device rules created before or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
deviceclasses	optional	Return device rules with the filtered device class. Example: "02h".
deviceids	optional	Return device rules with the filtered device id. Example: "02".
deviceinformationserviceinfokeys	optional	Return device rules with the filtered device information service info keys.
devicenames	optional	Return device rules with the filtered device names.
gattservices	optional	Return device rules with the filtered GATT services.
groupids	optional	List of Group IDs to filter by. Example: "225494730938493804,225494730938493915".
ids	optional	List of ids to filter by. Example: "225494730938493804,225494730938493915".
interfaces	optional	Return device rules with the filtered interface. Example: "USB".

manufacturernames	optional	Return device rules with the filtered manufacturer names.
minorclasses	optional	Return device rules with the filtered minor classes.
productids	optional	Return device rules with the filtered product id. Example: "02".
query	optional	A free-text search term, will match applicable attributes.
rulename	optional	Return device rules with the filtered rule name.
scopes	optional	Return only device rules in this scope. Example: "account".
serviceclasses	optional	Return device rules with the filtered service class. Example: "02".
siteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".
statuses	optional	Return device rules with the filtered status. Example: "Enabled".
tenant	optional	Indicates a tenant scope request
uids	optional	Return device rules with the filtered uId.
vendorids	optional	Return device rules with the filtered vendor id.
versions	optional	Return device rules with the filtered versions.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Get Device Control Events

GET /web/api/v2.1/device-control/events

Get the data of Device Control events on Windows and macOS endpoints with Device Control-enabled Agents that match the filter. Device Control requires Control SKU. Linux Agents do not support Device Control.

Parameters

access_permissions	optional	Access permission in. Example: "Read-Only".
accountids	optional	List of Account IDs to filter by. Example: "225494730938493804,225494730938493915".

agentids	optional	List of agent Ids to filter by
countonly	optional	If true, only total number of items will be returned, without any of the actual objects.
cursor	optional	Cursor position returned by the last request. Use to iterate over more than 1000 items. Example: "YWdlbnRfaWQ6NTgwMjkzODE=".
deviceclasses	optional	List of device classes to filter by. Example: "02h".
deviceids	optional	List of device IDs to filter by
eventids	optional	List of event IDs to filter by
eventtime__between	optional	Return events created within this range (inclusive). Example: "1514978764288-1514978999999".
eventtime__gt	optional	Return events generated after this time. Example: "2018-02-27T04:49:26.257525Z".
eventtime__gte	optional	Return events generated after or at this time. Example: "2018-02-27T04:49:26.257525Z".
eventtime__lt	optional	Return events generated before this time. Example: "2018-02-27T04:49:26.257525Z".
eventtime__lte	optional	Return events generated before or at this time. Example: "2018-02-27T04:49:26.257525Z".
eventtypes	optional	List of event types to filter by.
groupids	optional	List of Group IDs to filter by. Example: "225494730938493804,225494730938493915".
ids	optional	List of IDs to filter by. Example: "225494730938493804,225494730938493915".
interfaces	optional	List of interfaces to filter by. Example: "USB".
limit	optional	Limit number of returned items (1-1000). Example: "10".
productids	optional	List of product IDs to filter by. Example: "02".
query	optional	A free-text search term, will match applicable attributes.
serviceclasses	optional	List of service classes to filter by. Example: "02".
siteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".
skip	optional	Skip first number of items (0-1000). To iterate over more than 1000 items, use "cursor". Example: "150".

skipcount	optional	If true, total number of items will not be calculated, which speeds up execution time.
sortby	optional	The column to sort the results by. Example: "id".
sortorder	optional	Sort direction. Example: "asc".
tenant	optional	Indicates a tenant scope request
uids	optional	List of uIds to filter by.
vendorids	optional	List of vendor IDs to filter by.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
pagination	Pagination information	true	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>totalItems</td><td>Total number of items found matching your query</td><td>true</td><td>integer</td></tr><tr><td>nextCursor</td><td>Pass this value as "cursor" on your next request, to get the next page of results (Will be "null" when last page reached)</td><td>false</td><td>string</td></tr></table>
data	Response data	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr></table>

			accessPermission: Access permission, false, enum agentId: Agent id, false, string computerName: Computer name, false, string createdAt: Created at, false, string deviceClass: Device class, false, string deviceId: Device id, false, string deviceName: Device name, false, string eventId: Event id, false, string eventTime: Event time, false, string eventType: Event type, false, string id: Id, false, string interface: Interface, false, enum lastLoggedInUserName: Last logged in user name, false, string lmpVersion: Lmp version, false, string minorClass: Minor class, false, string productId: Product id, false, string profileUuids: Profile uuids, false, string ruleId: Rule id, false, string serviceClass: Service class, false, string uId: U id, false, string updatedAt: Updated at, false, string vendorId: Vendor id, false, string
errors	Errors	false	array

Enable/Disable Rules

PUT /web/api/v2.1/device-control/enable

It is best practice to disable a rule rather than delete it. Use this command to change the status of a rule between Enabled and Disabled.
Note: On Windows, if a USB device is already connected to an endpoint, new rules and rule changes do not affect it. USB rules will apply the next time the device connects to the endpoint. For Windows Bluetooth rules, the device and endpoint must be paired after the SentinelOne Agent that supports Bluetooth is installed or upgraded. If the endpoint and device were already paired before the Agent supported bluetooth, reboot the endpoint to activate the rule, or re-pair the endpoint and device.
On macOS, changes apply to devices that are already connected to an endpoint.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>affected</td><td>Number of entities affected by the requested operation</td><td>false</td><td>integer</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

Name	Description	Required	Value
data	Data	true	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>status</td><td>should the rules be enabled/ disabled</td><td>true</td><td>enum</td></tr></table>
filter	Filter	true	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>accessPermissions</td><td>Access permission in</td><td>false</td><td>string []</td></tr><tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr><tr><td>actions</td><td>Return device rules with the filtered action.</td><td>false</td><td>string []</td></tr><tr><td>bluetoothAddresses</td><td>Return device rules with the filtered bluetooth addresses.</td><td>false</td><td>string []</td></tr><tr><td>createdAt__between</td><td>Return device rules created within this range (inclusive)</td><td>false</td><td>string</td></tr><tr><td>createdAt__gt</td><td>Return device rules created after this timestamp.</td><td>false</td><td>string</td></tr><tr><td>createdAt__gte</td><td>Return device rules created after or at this timestamp.</td><td>false</td><td>string</td></tr><tr><td>createdAt__lt</td><td>Return device rules created</td><td>false</td><td>string</td></tr></table>

				before this timestamp.		
			createdAt__lte	Return device rules created before or at this timestamp.	false	string
			deviceClasses	Return device rules with the filtered device class.	false	string []
			deviceIds	Return device rules with the filtered device id.	false	string []
			deviceInformationServiceInfoKeys	Return device rules with the filtered device information service info keys.	false	string []
			deviceNames	Return device rules with the filtered device names.	false	string []
			gattServices	Return device rules with the filtered GATT services.	false	string []
			groupIds	List of Group IDs to filter by	false	string []
			ids	List of ids to filter by	false	string []
			interfaces	Return device rules with the filtered interface.	false	string []
			manufacture	Return device	false	string []

			rNames	rules with the filtered manufacturer names.		
			minorClasses	Return device rules with the filtered minor classes.	false	string []
			productIds	Return device rules with the filtered product id.	false	string []
			query	A free-text search term, will match applicable attributes.	false	string
			ruleName	Return device rules with the filtered rule name.	false	string
			scopes	Return only device rules in this scope	false	string []
			serviceClasses	Return device rules with the filtered service class.	false	string []
			siteIds	List of Site IDs to filter by	false	string []
			statuses	Return device rules with the filtered status.	false	string []
			tenant	Indicates a tenant scope request	false	boolean
			uids	Return device rules with the filtered uId.	false	string []

			vendorIds	Return device rules with the filtered vendor id.	false	string []
			versions	Return device rules with the filtered versions.	false	string []

Exclusions and Blocklist

Import Exclusions

POST /web/api/v2.1/exclusions/import

Upload a CSV file that contains exclusion entries to import to a scope in your Management

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
reportId	The ID of the Validation Report generated for the import. It can help you fix entries that did not import successfully.	false	string
succeeded	The number of entries that imported successfully	false	integer
total	The number of rows in the file	false	integer

errors	Errors	false	array

Body Schema

Name	Description	Required	Value
formData		false	

Name	Description	Required	Value
file	The input CSV file	true	file
filter	The details of the scope where the entities will be imported, for example: For Global - '{"tenant":true}' For an Account - '{"accountIds": ["225494730938493804"]}' For a Site - '{"siteIds": ["225494730938493804"]}' For a Group - '{"groupIds": ["225494730938493804"]}'	false	string

Get Exclusion Import Validation Report

GET /web/api/v2.1/exclusions/report/{report_id}

Get the Validation Report generated for the import to help you fix entries that did not import successfully

Response Messages

200 - Success

401 - Unauthorized access - please sign in and retry.

Import Blocklist Items

POST /web/api/v2.1/restrictions/import

Upload a CSV file that contains blocklist entries to import to a scope in your Management

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
data	Response data	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>reportId</td><td>The ID of the Validation Report generated for the import. It can help you fix entries that did not</td><td>false</td><td>string</td></tr></table>

errors	Errors	false	array

	import successfully.		
succeeded	The number of entries that imported successfully	false	integer
total	The number of rows in the file	false	integer

Body Schema

Name	Description	Required	Value
formData		false	

Name	Description	Required	Value
file	The input CSV file	true	file
filter	The details of the scope where the entities will be imported, for example: For Global - '{"tenant":true}' For an Account - '{"accountIds": ["225494730938493804"]}' For a Site - '{"siteIds": ["225494730938493804"]}' For a Group - '{"groupIds": ["225494730938493804"]}'	false	string

Get Blocklist Import Validation Report

GET /web/api/v2.1/restrictions/report/{report_id}

Get the Validation Report generated for the import to help you fix entries that did not import successfully

Response Messages

200 - Success

401 - Unauthorized access - please sign in and retry.

Get Exclusions

GET /web/api/v2.1/exclusions

Get a list of all the Exclusions that match the filter.
Note: To filter the results for a scope:
* Global - Make sure "tenant" is "true" and no other scope ID is given.
* Account - Make sure "tenant" is "false" and at least one Account ID is given.
* Site - Make sure "tenant" is "false" and at least one Site ID is given.

Parameters

accountids	optional	List of Account IDs to filter by. Example: "225494730938493804,225494730938493915".
applicationname__contains	optional	Free-text filter by application name
countonly	optional	If true, only total number of items will be returned, without any of the actual objects.
createdat__between	optional	Date range for creation time (format: <from_timestamp>-<to_timestamp>, inclusive). Example: "1514978890136-1514978650130".
createdat__gt	optional	Created after this timestamp. Example: "2018-02-27T04:49:26.257525Z".
createdat__gte	optional	Created after or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".

createdat__lt	optional	Created before this timestamp. Example: "2018-02-27T04:49:26.257525Z".
createdat__lte	optional	Created before or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
cursor	optional	Cursor position returned by the last request. Use to iterate over more than 1000 items. Example: "YWdlbnRfaWQ6NTgwMjkzODE=".
description__contains	optional	Free-text filter by description
groupids	optional	List of Group IDs to filter by. Example: "225494730938493804,225494730938493915".
ids	optional	List of IDs to filter by. Example: "225494730938493804,225494730938493915".
imported	optional	indication whether the exclusion was imported by a bulk operation or not
inappinventory	optional	Found or Not found - indicates if this exclusion is related to an application found in the scope's Application Inventory.
includechildren	optional	Return filters from children scope levels (Default: false)
includeparents	optional	Return filters from parent scope levels (Default: false)
limit	optional	Limit number of returned items (1-1000). Example: "10".
modes	optional	List of modes to filter by (Path exclusions only). Example: "suppress".
modetype	optional	Agent interaction \ Suppression. Example: "all".
ostypes	optional	List of Os types to filter by. Example: "macos".
pathexclusiontypes	optional	List of excluded paths in an exclusion (Path exclusions only). Example: "file".
query	optional	A free-text search term, will match applicable attributes
recommendations	optional	List of recommendations to filter by. Example: "Not recommended".
siteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".
skip	optional	Skip first number of items (0-1000). To iterate over more than 1000 items, use "cursor". Example: "150".
skipcount	optional	If true, total number of items will not be calculated, which speeds up execution time.
sortby	optional	The column to sort the results by. Example: "id".

sortorder	optional	Sort direction. Example: "asc".
source	optional	List sources to filter by. Example: "user".
tenant	optional	Indicates a tenant scope request
type	optional	Type. Example: "path".
types	optional	Type in. Example: "path".
unified	optional	Unified
updatedat__between	optional	Date range for update time (format: <from_timestamp>-<to_timestamp>, inclusive). Example: "1514978890136-1514978650130".
updatedat__gt	optional	Updated after this timestamp. Example: "2018-02-27T04:49:26.257525Z".
updatedat__gte	optional	Updated after or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
updatedat__lt	optional	Updated before this timestamp. Example: "2018-02-27T04:49:26.257525Z".
updatedat__lte	optional	Updated before or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
user__contains	optional	Free-text filter by user name
userids	optional	List of user ids to filter by. Example: "225494730938493804,225494730938493915".
value	optional	Value
value__contains	optional	Free-text filter by value

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
pagination	Pagination	true	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr></table>

	information		totalItems: Total number of items found matching your query; true; integer nextCursor: Pass this value as "cursor" on your next request, to get the next page of results (Will be "null" when last page reached); false; string
data	Response data	false	

Name	Description	Required	Value
actions	Actions to perform	false	string []
applicationName	The Application name of exclusions created from the Exclusion Catalog.	false	string
createdAt	Timestamp of item creation	false	string
description	Description	false	string
id	Id	false	string
imported	indication whether the exclusion was imported by a bulk operation or not	false	boolean
inAppInventory	Found or Not found - indicates if	false	boolean

				this exclusion is related to an application found in the scope's Application Inventory.		
			includeChildren	Return filters from children scope levels (Default: false)	false	boolean
			includeParents	Return filters from parent scope levels (Default: false)	false	boolean
			inject	[DEPRECATED] Path exclusion monitor mode	false	boolean
			mode	Exclusion mode (path exclusion only)	false	enum
			notRecommended	Not recommended	false	string
			osType	os_type	false	enum
			pathExclusionType	Excluded path for a path exclusion list	false	enum
			scope	Scope	false	

Name	Description	Required	Value
accountIds	Account ids	false	string []
groupIds	Group ids	false	string []
siteIds	Site ids	false	string []
tenant	Tenant	false	boolean

			scopeName | Scope name | false | string scopePath | Scope path | false | string source | Source: cloud, user, action_from_threat, or catalog | false | enum type | type | false | string updatedAt | Timestamp of item update | false | string userId | ID of the creating user | false | string userName | Name of the creating user | false | string value | Sha1 if hash type or value according to the exclusion list type | false | string
errors	Errors	false	array

Create Exclusion

POST /web/api/v2.1/exclusions

Create Exclusions to make your Agents suppress alerts and mitigation for items that you consider to be benign or which you require for interoperability.
IMPORTANT! Every Exclusion is a possible security hole. Do not create Exclusions unless you are sure this hash, path, certificate signer, file type, or browser is always benign.
Of course, if you can make the Exclusion by its hash or path, that is much more secure than excluding all detections of a specific signer, file type, or browser. We do not recommend the last types for Exclusions on production endpoints. These Exclusions might be helpful in a lab or pentester group. When you create an Exclusion, make sure you set the filter to the smallest possible scope. For example, if you can exclude security for this item on a group, do not enter values for siteIds or accountIds.
We recommend that you read "Not Recommended Exclusions: https://support.sentinelone.com/hc/en-us/articles/360007532894
and Best Practices for Exclusions: https://support.sentinelone.com/hc/en-us/articles/360008709014

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
scope	Scope	true	

Name	Description	Required	Value
accountIds	Account ids	false	string []
groupIds	Group ids	false	string []
siteIds	Site ids	false	string []
tenant	Tenant	false	boolean

Name	Description	Required	Value
actions	Actions to perform	false	string []
createdAt	Timestamp of exclusion item creation	false	string
description	Description	false	string

			id | Id | false | string inject | [DEPRECATED] Path exclusion monitor mode | false | boolean mode | Exclusion mode (path exclusion only) | false | enum notRecommended | Not recommended | false | string osType | OS type | false | enum pathExclusionType | Excluded path for a path exclusion list | false | enum scopeName | Scope name | false | string source | Source: cloud, user, action_from_threat, or catalog | false | enum type | Type | false | string updatedAt | Timestamp of exclusion item update | false | string userId | ID of the creating user | false | string userName | Name of the creating user | false | string value | Sha1 if hash type or value according to the exclusion list type | false | string
errors	Errors	false	array

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>osType</td><td>OS type</td><td>true</td><td>enum</td></tr>
<tr><td>type</td><td>Exclusion item type</td><td>true</td><td>enum</td></tr>
<tr><td>value</td><td>Valid values depend on the item type</td><td>true</td><td></td></tr>
<tr><td>actions</td><td>Actions to perform</td><td>false</td><td>string []</td></tr>
<tr><td>description</td><td>Description</td><td>false</td><td>string</td></tr>
<tr><td>inject</td><td>[DEPRECATED] Path exclusion monitor mode</td><td>false</td><td>boolean</td></tr>
<tr><td>mode</td><td>Exclusion mode (path exclusion only)</td><td>false</td><td>enum</td></tr>
<tr><td>pathExclusionType</td><td>Excluded path for a path exclusion list</td><td>false</td><td>string</td></tr>
<tr><td>source</td><td>Source</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>filter</td><td>Filter</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>groupIds</td><td>List of Group IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>siteIds</td><td>List of Site IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>tenant</td><td>Indicates a</td><td>false</td><td>boolean</td></tr>
</table>
</td></tr>
</table>

				tenant scope request		

Update Exclusions

PUT /web/api/v2.1/exclusions

Change the properties of an Exclusion through the data fields. To get the original data, run "exclusions" with a filter to give the item you want.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

404 - Exclusion not found

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
scope	Scope	true	

Name	Description	Required	Value
accountIds	Account ids	false	string []
groupIds	Group ids	false	string []
siteIds	Site ids	false	string []
tenant	Tenant	false	boolean

Name	Description	Required	Value
actions	Actions to perform	false	string []
createdAt	Timestamp of exclusion item creation	false	string
description	Description	false	string
id	Id	false	string
inject	[DEPRECATED] Path exclusion monitor	false	boolean

			mode	false	
			mode	Exclusion mode (path exclusion only)	false	enum
			notRecommended	Not recommended	false	string
			osType	OS type	false	enum
			pathExclusionType	Excluded path for a path exclusion list	false	enum
			scopeName	Scope name	false	string
			source	Source: cloud, user, action_from_threat, or catalog	false	enum
			type	Type	false	string
			updatedAt	Timestamp of exclusion item update	false	string
			userId	ID of the creating user	false	string
			userName	Name of the creating user	false	string
			value	Sha1 if hash type or value according to the exclusion list type	false	string
errors	Errors	false	array			

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>id</td><td>Id</td><td>true</td><td>string</td></tr>
<tr><td>osType</td><td>OS type</td><td>true</td><td>enum</td></tr>
<tr><td>type</td><td>Exclusion item type</td><td>true</td><td>enum</td></tr>
<tr><td>actions</td><td>Actions to perform</td><td>false</td><td>string []</td></tr>
<tr><td>description</td><td>Description</td><td>false</td><td>string</td></tr>
<tr><td>inject</td><td>[DEPRECATED] Path exclusion monitor mode</td><td>false</td><td>boolean</td></tr>
<tr><td>mode</td><td>Exclusion mode (path exclusion only)</td><td>false</td><td>enum</td></tr>
<tr><td>pathExclusionType</td><td>Excluded path for a path exclusion list</td><td>false</td><td>string</td></tr>
<tr><td>source</td><td>Source</td><td>false</td><td>string</td></tr>
<tr><td>value</td><td>Value</td><td>false</td><td></td></tr>
</table>
</td></tr>
</table>

Delete Exclusions

DELETE /web/api/v2.1/exclusions

Every Exclusion opens a possible security hole. If you decide that an Exclusion (or multiple Exclusions) is not required, use this command to delete it. To get the ID of the Exclusion to delete, run the "exclusions" command.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>affected</td><td>Number of entities affected by the requested operation</td><td>false</td><td>integer</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

Name	Description	Required	Value
data	Data	true	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>ids</td><td>Ids</td><td>false</td><td>string []</td></tr><tr><td>type</td><td>Type</td><td>false</td><td>enum</td></tr></table>

Get Blocklist

GET /web/api/v2.1/restrictions

Get a list of all the items in the Blocklist that match the filter.
To filter the results for a scope:
* Global - Make sure "tenant" is "true" and no other scope ID is given.
* Account - Make sure "tenant" is "false" and at least one Account ID is given.
* Site - Make sure "tenant" is "false" and at least one Site ID is given.

Parameters

accountids	optional	List of Account IDs to filter by. Example: "225494730938493804,225494730938493915".
countonly	optional	If true, only total number of items will be returned, without any of the actual objects.
createdat__between	optional	Date range for creation time (format: <from_timestamp>-<to_timestamp>, inclusive). Example: "1514978890136-1514978650130".
createdat__gt	optional	Created after this timestamp. Example: "2018-02-27T04:49:26.257525Z".
createdat__gte	optional	Created after or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
createdat__lt	optional	Created before this timestamp. Example: "2018-02-27T04:49:26.257525Z".
createdat__lte	optional	Created before or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
cursor	optional	Cursor position returned by the last request. Use to iterate over more than 1000 items. Example: "YWdlbnRfaWQ6NTgwMjkzODE=".
description__contains	optional	Free-text filter by description
groupids	optional	List of Group IDs to filter by. Example: "225494730938493804,225494730938493915".
ids	optional	List of IDs to filter by. Example: "225494730938493804,225494730938493915".
imported	optional	indication whether the hash was imported by a bulk operation or

		not
includechildren	optional	Return filters from children scope levels (Default: false)
includeparents	optional	Return filters from parent scope levels (Default: false)
limit	optional	Limit number of returned items (1-1000). Example: "10".
modes	optional	List of modes to filter by (Path exclusions only). Example: "suppress".
ostypes	optional	List of Os types to filter by. Example: "macos".
query	optional	A free-text search term, will match applicable attributes
recommendations	optional	List of recommendations to filter by. Example: "Not recommended".
siteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".
skip	optional	Skip first number of items (0-1000). To iterate over more than 1000 items, use "cursor". Example: "150".
skipcount	optional	If true, total number of items will not be calculated, which speeds up execution time.
sortby	optional	The column to sort the results by. Example: "id".
sortorder	optional	Sort direction. Example: "asc".
source	optional	List sources to filter by. Example: "user".
tenant	optional	Indicates a tenant scope request
type	optional	Type. Example: "black_hash".
types	optional	Type in. Example: "black_hash".
unified	optional	Unified
updatedat__between	optional	Date range for update time (format: <from_timestamp>-<to_timestamp>, inclusive). Example: "1514978890136-1514978650130".
updatedat__gt	optional	Updated after this timestamp. Example: "2018-02-27T04:49:26.257525Z".
updatedat__gte	optional	Updated after or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
updatedat__lt	optional	Updated before this timestamp. Example: "2018-02-27T04:49:26.257525Z".
updatedat__lte	optional	Updated before or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".

user__contains	optional	Free-text filter by user name
userids	optional	List of user ids to filter by. Example: "225494730938493804,225494730938493915".
value	optional	Value
value__contains	optional	Free-text filter by value

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
pagination	Pagination information	true	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>totalItems</td><td>Total number of items found matching your query</td><td>true</td><td>integer</td></tr><tr><td>nextCursor</td><td>Pass this value as "cursor" on your next request, to get the next page of results (Will be "null" when last page reached)</td><td>false</td><td>string</td></tr></table>
data	Response data	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>createdAt</td><td>Timestamp of item creation</td><td>false</td><td>string</td></tr><tr><td>description</td><td>Description</td><td>false</td><td>string</td></tr></table>

			id	Id	false	string
			imported	indication whether the exclusion was imported by a bulk operation or not	false	boolean
			includeChildren	Return filters from children scope levels (Default: false)	false	boolean
			includeParents	Return filters from parent scope levels (Default: false)	false	boolean
			notRecommended	Not recommended	false	string
			osType	os_type	false	enum
			scope	Scope	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>accountIds</td><td>Account ids</td><td>false</td><td>string []</td></tr><tr><td>groupIds</td><td>Group ids</td><td>false</td><td>string []</td></tr><tr><td>siteIds</td><td>Site ids</td><td>false</td><td>string []</td></tr><tr><td>tenant</td><td>Tenant</td><td>false</td><td>boolean</td></tr></table>
			scopeName	Scope name	false	string
			scopePath	Scope path	false	string
			source	Source: cloud, user, or action_from_threat	false	enum
			type	type	false	string
			updatedAt	Timestamp of item update	false	string
			userId	ID of the	false	string

				creating user		
			userName	Name of the creating user	false	string
			value	SHA1 hash	false	string
errors	Errors	false	array			

Create Blocklist Item

POST /web/api/v2.1/restrictions

Create a blocklist item for a SHA1 hash, for the scopes you enter in the filter fields. You can add the hash to multiple Groups, Sites, Accounts, and to the Global list.
IMPORTANT: The type must be "black_hash" - any other value will create an Exclusion rather than a Blocklist item.
Users with the IT role do not have permissions to run this.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
scope	Scope	true	

Name	Description	Required	Value
accountIds	Account ids	false	string []
groupIds	Group ids	false	string []
siteIds	Site ids	false	string []
tenant	Tenant	false	boolean

Name	Description	Required	Value
createdAt	Timestamp of blocklist item creation	false	string
description	Description	false	string
id	Id	false	string
notRecommended	Not recommended	false	string
osType	OS type	false	enum
scopeName	Scope name	false	string

			source: Source: cloud, user, or action_from_threat; false; enum
			type: Type; false; string
			updatedAt: Timestamp of blocklist item update; false; string
			userId: ID of the creating user; false; string
			userName: Name of the creating user; false; string
			value: SHA1 hash; false; string
errors	Errors	false	array

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>osType</td><td>OS type</td><td>true</td><td>enum</td></tr>
<tr><td>type</td><td>Restriction type</td><td>true</td><td>enum</td></tr>
<tr><td>value</td><td>SHA1 of the file to add to the blocklist</td><td>true</td><td></td></tr>
<tr><td>description</td><td>Description</td><td>false</td><td>string</td></tr>
<tr><td>source</td><td>Source</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>filter</td><td>Filter</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>groupIds</td><td>List of Group IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>siteIds</td><td>List of Site IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>tenant</td><td>Indicates a tenant scope request</td><td>false</td><td>boolean</td></tr>
</table>
</td></tr>
</table>

Update Blocklist Item

PUT /web/api/v2.1/restrictions

Change the properties of a Blocklist item through the data fields. To get the original data, run "restrictions" with a filter to give the item you want.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

404 - Blocklist not found

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>scope</td><td>Scope</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>Account ids</td><td>false</td><td>string []</td></tr>
<tr><td>groupIds</td><td>Group ids</td><td>false</td><td>string []</td></tr>
<tr><td>siteIds</td><td>Site ids</td><td>false</td><td>string []</td></tr>
<tr><td>tenant</td><td>Tenant</td><td>false</td><td>boolean</td></tr>
</table>
</td></tr>
<tr><td>createdAt</td><td>Timestamp of blocklist item creation</td><td>false</td><td>string</td></tr>
<tr><td>description</td><td>Description</td><td>false</td><td>string</td></tr>
<tr><td>id</td><td>Id</td><td>false</td><td>string</td></tr>
<tr><td>notRecommended</td><td>Not recommended</td><td>false</td><td>string</td></tr>
<tr><td>osType</td><td>OS type</td><td>false</td><td>enum</td></tr>
<tr><td>scopeName</td><td>Scope name</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
</table>

			source: Source: cloud, user, or action_from_threat; false; enum
			type: Type; false; string
			updatedAt: Timestamp of blocklist item update; false; string
			userId: ID of the creating user; false; string
			userName: Name of the creating user; false; string
			value: SHA1 hash; false; string
errors	Errors	false	array

Body Schema

Name	Description	Required	Value
data	Data	true	

Name	Description	Required	Value
id	Id	true	string
osType	OS type	true	enum
type	Restrictions type (black_hash)	true	enum
description	Description	false	string
source	Source	false	string
value	Value	false	

Delete Blocklist Item

DELETE /web/api/v2.1/restrictions

Agents immediately identify files on the blocklist and block them from executing. Agents identify files on the blocklist before they look at exclusions. If there is a conflict - for example, if a hash is blocklisted from the Cloud Intelligence, and you have an exclusion to run an application that requires this hash - you can delete the hash from the Blocklist. Users with the IT role do not have permissions to run this command.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>affected</td><td>Number of entities affected by the requested operation</td><td>false</td><td>integer</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

Name	Description	Required	Value
data	Data	true	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>ids</td><td>Ids</td><td>false</td><td>string []</td></tr><tr><td>type</td><td>Type</td><td>false</td><td>enum</td></tr></table>

Validate Exclusion Item

POST /web/api/v2.1/exclusions/validate

Check if an exclusion is on the list of SentinelOne items that are "Not Allowed" or "Not Recommended". This API returns one of the following statuses:
* Not Recommended: This item is not recommended by SentinelOne because it decreases security. For example, If you accidentally exclude a path that is too broad, malware can enter your environment.
* Not Allowed: This exclusion can harm the product and lead to unexpected functionality. From version North Pole SP3 you are prevented from creating Not Allowed exclusions.* None: This item is not on the list of SentinelOne items that are "Not Allowed" or "Not Recommended".

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>status</td><td>Recommendation for the exclusion/ blocklist item</td><td>false</td><td>enum</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>exclusionType</td><td>Exclusion type</td><td>false</td><td>enum</td></tr>
<tr><td>osType</td><td>OS type</td><td>false</td><td>enum</td></tr>
<tr><td>value</td><td>Value</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
</table>

Validate Blocklist Item

POST /web/api/v2.1/restrictions/validate

Check if a hash is on the list of SentinelOne items that are "Not Allowed" or "Not Recommended". This API returns one of the following statuses:
* Not Recommended: This item is not recommended by SentinelOne because it decreases security.
* Not Allowed: This item can harm the product and lead to unexpected functionality. From version North Pole SP3 you are prevented from creating Not Allowed blocklist item. * None: This item is not on the list of SentinelOne items that are "Not Allowed" or "Not Recommended".

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>status</td><td>Recommendation for the exclusion/ blocklist item</td><td>false</td><td>enum</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

Name	Description	Required	Value
data	Data	true	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>osType</td><td>OS type</td><td>false</td><td>enum</td></tr><tr><td>value</td><td>Value</td><td>false</td><td>string</td></tr></table>

Export Exclusions

GET /web/api/v2.1/export/exclusions

Get a csv of all the items in the Exclusions that match the filter.
Note: To see items from the Global Exclusion scope, make sure "tenant" is "true" and no other scope ID is given.

Parameters

accountids	optional	List of Account IDs to filter by. Example: "225494730938493804,225494730938493915".
applicationname__contains	optional	Free-text filter by application name
createdat__between	optional	Date range for creation time (format: <from_timestamp>-<to_timestamp>, inclusive). Example: "1514978890136-1514978650130".
createdat__gt	optional	Created after this timestamp. Example: "2018-02-27T04:49:26.257525Z".
createdat__gte	optional	Created after or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
createdat__lt	optional	Created before this timestamp. Example: "2018-02-27T04:49:26.257525Z".
createdat__lte	optional	Created before or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
description__contains	optional	Free-text filter by description
groupids	optional	List of Group IDs to filter by. Example: "225494730938493804,225494730938493915".
ids	optional	List of IDs to filter by. Example: "225494730938493804,225494730938493915".
imported	optional	indication whether the exclusion was imported by a bulk operation or not
inappinventory	optional	Found or Not found - indicates if this exclusion is related to an application found in the scope's Application Inventory.
includechildren	optional	Return filters from children scope levels (Default: false)
includeparents	optional	Return filters from parent scope levels (Default: false)

modes	optional	List of modes to filter by (Path exclusions only). Example: "suppress".
modetype	optional	Agent interaction \ Suppression. Example: "all".
ostypes	optional	List of Os types to filter by. Example: "macos".
pathexclusiontypes	optional	List of excluded paths in an exclusion (Path exclusions only). Example: "file".
query	optional	A free-text search term, will match applicable attributes
recommendations	optional	List of recommendations to filter by. Example: "Not recommended".
siteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".
source	optional	List sources to filter by. Example: "user".
tenant	optional	Indicates a tenant scope request
type	optional	Type. Example: "path".
types	optional	Type in. Example: "path".
unified	optional	Unified
updatedat__between	optional	Date range for update time (format: <from_timestamp>-<to_timestamp>, inclusive). Example: "1514978890136-1514978650130".
updatedat__gt	optional	Updated after this timestamp. Example: "2018-02-27T04:49:26.257525Z".
updatedat__gte	optional	Updated after or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
updatedat__lt	optional	Updated before this timestamp. Example: "2018-02-27T04:49:26.257525Z".
updatedat__lte	optional	Updated before or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
user__contains	optional	Free-text filter by user name
userids	optional	List of user ids to filter by. Example: "225494730938493804,225494730938493915".
value	optional	Value
value__contains	optional	Free-text filter by value

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Export Blocklist

GET /web/api/v2.1/export/restrictions

Get a csv of all the items in the Blocklist that match the filter.
Note: To see items from the Global Blocklist, make sure "tenant" is "true" and no other scope ID is given.

Parameters

accountids	optional	List of Account IDs to filter by. Example: "225494730938493804,225494730938493915".
createdat__between	optional	Date range for creation time (format: <from_timestamp>-<to_timestamp>, inclusive). Example: "1514978890136-1514978650130".
createdat__gt	optional	Created after this timestamp. Example: "2018-02-27T04:49:26.257525Z".
createdat__gte	optional	Created after or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
createdat__lt	optional	Created before this timestamp. Example: "2018-02-27T04:49:26.257525Z".
createdat__lte	optional	Created before or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
description__contains	optional	Free-text filter by description
groupids	optional	List of Group IDs to filter by. Example: "225494730938493804,225494730938493915".
ids	optional	List of IDs to filter by. Example: "225494730938493804,225494730938493915".
imported	optional	indication whether the hash was imported by a bulk operation or not
includechildren	optional	Return filters from children scope levels (Default: false)
includeparents	optional	Return filters from parent scope levels (Default: false)

ostypes	optional	List of Os types to filter by. Example: "macos".
query	optional	A free-text search term, will match applicable attributes
recommendations	optional	List of recommendations to filter by. Example: "Not recommended".
siteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".
source	optional	List sources to filter by. Example: "user".
tenant	optional	Indicates a tenant scope request
type	optional	Type. Example: "black_hash".
types	optional	Type in. Example: "black_hash".
unified	optional	Unified
updatedat__between	optional	Date range for update time (format: <from_timestamp>-<to_timestamp>, inclusive). Example: "1514978890136-1514978650130".
updatedat__gt	optional	Updated after this timestamp. Example: "2018-02-27T04:49:26.257525Z".
updatedat__gte	optional	Updated after or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
updatedat__lt	optional	Updated before this timestamp. Example: "2018-02-27T04:49:26.257525Z".
updatedat__lte	optional	Updated before or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
user__contains	optional	Free-text filter by user name
userids	optional	List of user ids to filter by. Example: "225494730938493804,225494730938493915".
value	optional	Value
value__contains	optional	Free-text filter by value

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Exclusions v2.1

Get Exclusions

GET /web/api/v2.1/unified-exclusions

Get a list of all the Exclusions that match the filter.
Note: To filter the results for a scope:
* Global - Make sure "tenant" is "true" and no other scope ID is given.
* Account - Make sure "tenant" is "false" and at least one Account ID is given.
* Site - Make sure "tenant" is "false" and at least one Site ID is given.

Parameters

accountids	optional	List of Account IDs to filter by. Example: "225494730938493804,225494730938493915".
applicationname__contains	optional	Free-text filter by application name
conditions	optional	List of conditions to filter by. Example: "white_hash".
countonly	optional	If true, only total number of items will be returned, without any of the actual objects.
createdat__between	optional	Date range for creation time (format: <from_timestamp>-<to_timestamp>, inclusive). Example: "1514978890136-1514978650130".
createdat__gt	optional	Created after this timestamp. Example: "2018-02-27T04:49:26.257525Z".
createdat__gte	optional	Created after or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
createdat__lt	optional	Created before this timestamp. Example: "2018-02-27T04:49:26.257525Z".
createdat__lte	optional	Created before or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
cursor	optional	Cursor position returned by the last request. Use to iterate over more than 1000 items. Example: "YWdlbnRfaWQ6NTgwMjkzODE=".
description__contains	optional	Free-text filter by description

engines	optional	List of engines to filter by. Example: "suppress".
exclusionname__contains	optional	Free-text filter by exclusion name
groupids	optional	List of Group IDs to filter by. Example: "225494730938493804,225494730938493915".
ids	optional	List of IDs to filter by. Example: "225494730938493804,225494730938493915".
imported	optional	indication whether the exclusion was imported by a bulk operation or not
includechildren	optional	Return filters from children scope levels (Default: false)
includeparents	optional	Return filters from parent scope levels (Default: false)
interactionlevel	optional	List of interaction levels to filter by. Example: "disable_all_monitors".
limit	optional	Limit number of returned items (1-1000). Example: "10".
modetype	optional	Agent interaction \ Suppression. Example: "suppression".
notrecommended	optional	List of recommendations to filter by. Example: "Not recommended".
ostypes	optional	List of Os types to filter by. Example: "macos".
pathexclusiontypes	optional	List of excluded paths in an exclusion (Path exclusions only). Example: "file".
scopepath__contains	optional	Free-text filter by scope path
siteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".
skip	optional	Skip first number of items (0-1000). To iterate over more than 1000 items, use "cursor". Example: "150".
skipcount	optional	If true, total number of items will not be calculated, which speeds up execution time.
sortby	optional	The column to sort the results by. Example: "id".
sortorder	optional	Sort direction. Example: "asc".
source	optional	List sources to filter by. Example: "user".
tenant	optional	Indicates a tenant scope request
threattype	optional	List of threat types to filter by. Example: "EDR".
updatedat__between	optional	Date range for update time (format: <from_timestamp>-<to_timestamp>, inclusive). Example: "1514978890136-1514978650130".

updatedat__gt	optional	Updated after this timestamp. Example: "2018-02-27T04:49:26.257525Z".
updatedat__gte	optional	Updated after or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
updatedat__lt	optional	Updated before this timestamp. Example: "2018-02-27T04:49:26.257525Z".
updatedat__lte	optional	Updated before or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
user__contains	optional	Free-text filter by user name
userids	optional	List of user ids to filter by. Example: "225494730938493804,225494730938493915".
value__contains	optional	Free-text filter by value

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
pagination	Pagination information	true	

Name	Description	Required	Value
totalItems	Total number of items found matching your query	true	integer
nextCursor	Pass this value as "cursor" on your next request, to get the next page of results (Will	false	string

			be "null" when last page reached)
data	Response data	false	
errors	Errors	false	array

Delete Exclusions

DELETE /web/api/v2.1/unified-exclusions

Response Messages

200 - Exclusions successfully deleted.

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - User is not allowed to perform this operation.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>affected</td><td>Number of entities affected by the requested operation</td><td>false</td><td>integer</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

Name	Description	Required	Value
data	Data	true	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>exclusions</td><td>Exclusions</td><td>false</td><td><table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>exclusionType</td><td>Exclusion type</td><td>true</td><td>enum</td></tr><tr><td>id</td><td>Id</td><td>true</td><td>string</td></tr></table></td></tr></table>

Filters

Get Filters

GET /web/api/v2.1/filters

Get the list of saved filters. See Save Filter. The response includes the ID of the filter, which you can use in other commands.

Parameters

accountids	optional	List of Account IDs to filter by. Example: "225494730938493804,225494730938493915".
countonly	optional	If true, only total number of items will be returned, without any of the actual objects.
cursor	optional	Cursor position returned by the last request. Use to iterate over more than 1000 items. Example: "YWdlbnRfaWQ6NTgwMjkzODE=".
ids	optional	A list of Filter IDs. Example: "225494730938493804,225494730938493915".
includechildren	optional	Return filters from children scope levels (Default: false)
includeglobal	optional	[DEPRECATED] Return global filters even when specific sites are selected
includeparents	optional	Return filters from parent scope levels (Default: false)
limit	optional	Limit number of returned items (1-1000). Example: "10".
query	optional	Text query for filter's name. Example: "MyFilter".
siteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".
skip	optional	Skip first number of items (0-1000). To iterate over more than 1000 items, use "cursor". Example: "150".
skipcount	optional	If true, total number of items will not be calculated, which speeds up execution time.
sortby	optional	The column to sort the results by. Example: "id".
sortorder	optional	Sort direction. Example: "asc".

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>pagination</td><td>Pagination information</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>totalItems</td><td>Total number of items found matching your query</td><td>true</td><td>integer</td></tr>
<tr><td>nextCursor</td><td>Pass this value as "cursor" on your next request, to get the next page of results (Will be "null" when last page reached)</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>createdAt</td><td>Created at</td><td>true</td><td>string</td></tr>
<tr><td>id</td><td>Id</td><td>true</td><td>string</td></tr>
<tr><td>name</td><td>Name</td><td>true</td><td>string</td></tr>
<tr><td>scopeLevel</td><td>Filter scope</td><td>true</td><td>enum</td></tr>
<tr><td>updatedAt</td><td>Updated at</td><td>true</td><td>string</td></tr>
<tr><td>filterFields</td><td>A set of arguments composing the filter</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>adComputerMember__contains</td><td>Free-text filter by Active</td><td>false</td><td>string []</td></tr>
</table>
</td></tr>
</table>
</td></tr>
</table>

									Directory computer groups string (supports multiple values)					
								adComputerName__contains	Free-text filter by Active Directory computer name string (supports multiple values)	false	string []			
								adComputerQuery__contains	Free-text filter by Active Directory computer name or its groups (supports multiple values)	false	string []			
								adQuery	An Active Directory query string	false	string			
								adQuery__contains	Free-text filter by Active Directory string (supports multiple values)	false	string []			
								adUserMember__contains	Free-text filter by Active Directory user groups string (supports	false	string []			

							multiple values)		
						adUserName__contains	Free-text filter by Active Directory username string (supports multiple values)	false	string []
						adUserQuery__contains	Free-text filter by Active Directory computer name or its groups (supports multiple values)	false	string []
						agentNamespace__contains	Free-text filter by agent namespace (supports multiple values)	false	string []
						agentPodName__contains	Free-text filter by agent pod name (supports multiple values)	false	string []
						agentVersions	Agent versions to include	false	string []
						agentVersionsNin	Agent versions not to include	false	string []
						appsVulnerabilityStatuses	Apps vulnerability status in	false	string []

								appsVulnerabilityStatusesNin	Apps vulnerability status nin	false	string []						
								awsRole__contains	Free-text filter by aws role(supports multiple values)	false	string []						
								awsSecurityGroups__contains	Free-text filter by aws securityGroups(supports multiple values)	false	string []						
								awsSubnetIds__contains	Free-text filter by aws subnet ids (supports multiple values)	false	string []						
								azureResourceGroup__contains	Free-text filter by azure resource group(supports multiple values)	false	string []						
								cloudAccount__contains	Free-text filter by cloud account (supports multiple values)	false	string []						
								cloudImage__contains	Free-text filter by cloud image (supports multiple values)	false	string []						
								cloudInstanceId__contains	Free-text filter by cloud instance id(supports	false	string []						

									multiple values)						
								cloudInstanceSize__contains	Free-text filter by cloud instance size(supports multiple values)	false	string []				
								cloudLocation__contains	Free-text filter by cloud location (supports multiple values)	false	string []				
								cloudNetwork__contains	Free-text filter by cloud network (supports multiple values)	false	string []				
								cloudProvider	Agents from which cloud provider	false	string []				
								cloudProviderNin	Exclude Agents from these cloud provider	false	string []				
								cloudTags__contains	Free-text filter by cloud tags (supports multiple values)	false	string []				
								clusterName__contains	Free-text filter by cluster name (supports multiple values)	false	string []				
								computerName__contains	Free-text filter by computer	false	string []				

									name (supports multiple values)					
								consoleMigrationStatuses	Migration status in	false	string []			
								consoleMigrationStatusesNin	Migration status nin	false	string []			
								coreCount__between	Possible number of CPU cores (inclusive)	false	string			
								cpuCount__between	Possible number of CPU cores (inclusive)	false	string			
								cpuId__contains	Free-text filter by CPU name (supports multiple values)	false	string []			
								domains	Included network domains	false	string []			
								domainsNin	Not included network domains	false	string []			
								encryptedApplications	Disk encryption status	false	boolean			
								externalId__contains	Free-text filter by external ID (Customer ID)	false	string []			
								externalIp__contains	Free-text filter by visible IP (supports multiple	false	string []			

								values)				
							filteredGroupIds	List of Group IDs to filter by	false	string []		
							filteredSiteIds	List of Site IDs to filter by	false	string []		
							firewallEnabled	The agents supports Firewall Control and it is enabled for the agent's group	false	boolean []		
							gcpServiceAccount__contains	Free-text filter by gcp service account (supports multiple values)	false	string []		
							hasLocalConfiguration	Agent has a local configuration set	false	boolean		
							hasTags	Include only Agents that have any tags assigned if True, or none if False	false	boolean		
							infected	Include only Agents with at least one active threat	false	boolean		
							installerTypes	Include only Agents installed with these package types	false	string []		

						installerTypesNin	Exclude Agents installed with these package types	false	string []
						isActive	Include only active Agents	false	boolean
						isDecommissioned	Include active, decommissioned or both	false	boolean []
						isPendingUninstall	Include only Agents with pending uninstall requests	false	boolean
						isUninstalled	Include installed, uninstalled or both	false	boolean []
						isUpToDate	Include only Agents with updated software	false	boolean
						k8sNodeLabels__contains	Free-text filter by K8s node labels (supports multiple values)	false	string []
						k8sNodeName__contains	Free-text filter by K8s node name (supports multiple values)	false	string []
						k8sType__contains	Free-text filter by K8s type(supports multiple values)	false	string []

							k8sVersion__contains	Free-text filter by K8s version (supports multiple values)	false	string []		
							lastActiveDate__between	Date range for last active date(format: <from_timestamp>-<to_timestamp>, inclusive)	false	string		
							lastLoggedInUserName__contains	Free-text filter by username (supports multiple values)	false	string []		
							lastSuccessfulScanDate__between	Date range for last successful full disk scan(format: <from_timestamp>-<to_timestamp>, inclusive)	false	string		
							liveUpdateId__contains	Free-text filter by live update ID (supports multiple values)	false	string []		
							locationEnabled	The agents supports Location Awareness and it is enabled for the agent's group	false	boolean []		
							locationIds	Include only	false	string []		

									Agents reporting these locations					
								locationIdsNin	Do not include only Agents reporting these locations	false	string []			
								machineTypes	Included machine types	false	string []			
								machineTypesNin	Not included machine types	false	string []			
								missingPermissions	Included missing permissions	false	string []			
								missingPermissionsNin	Excluded missing permissions	false	string []			
								networkInterfaceGatewayMacAddress__contains	Free-text filter by Gateway MAC address (supports multiple values)	false	string []			
								networkInterfaceInet__contains	Free-text filter by local IP (supports multiple values)	false	string []			
								networkInterfacePhysical__contains	Free-text filter by MAC address (supports multiple values)	false	string []			
								networkQuara	The agents	false	boolean []			

							ntineEnabled	supports Network Quarantine Control and its enabled for the agent's group						
							networkStatuses	Included network statuses	false	string []				
							networkStatusesNin	Included network statuses	false	string []				
							operationalStates	Agent operational state	false	string []				
							operationalStatesNin	Do not include these Agent operational states	false	string []				
							osArch	OS architecture	false	enum				
							osTypes	Included OS types	false	string []				
							osTypesNin	Not included OS types	false	string []				
							osVersion__contains	Free-text filter by OS full name and version (supports multiple values)	false	string []				
							query	A free-text search term, will match applicable attributes (sub-string match). Note:	false	string				

							Device's physical addresses will be matched if they start with the search term only (no match if they contain the term).		
						rangerStatus	[DEPRECATED] Use rangerStatuses.	false	enum
						rangerStatuses	Status of Ranger	false	string []
						rangerStatusesNin	Do not include these Ranger Statuses	false	string []
						rangerVersions	Ranger versions to include	false	string []
						rangerVersionsNin	Ranger versions not to include	false	string []
						registeredAt__between	Date range for first registration time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
						remoteProfilingStates	Agent remote profiling state	false	string []
						remoteProfilingStatesNin	Do not include these Agent remote profiling states	false	string []

							scanStatuses	Included scan statuses	false	string []		
							scanStatuses Nin	Not included scan statuses	false	string []		
							serialNumber __contains	Free-text filter by Serial Number (supports multiple values)	false	string []		
							tagsData	Filter agents by their assigned tags. Given in form of a JSON where each key represents a tag key, and each value represents a list of string values to filter by. To filter by unassigned tag values, use __nin suffix in the tag key.	false	string		
							threatReboot Required	Has at least one threat with at least one mitigation action pending reboot to succeed	false	boolean []		
							totalMemory __between	Total memory range (GB, inclusive)	false	string		
							userActionsN	Included	false	string []		

						eeded	pending user actions		
						userActionsNeededNin	Excluded pending user actions	false	string []
						uuid__contains	Free-text filter by Agent UUID (supports multiple values)	false	string []
			scopeId	Associated site/account	false	string			
			siteId	[DEPRECATED] Use scopeId instead	false	string			
errors	Errors	false	array						

Save Filter

POST /web/api/v2.1/filters

Save a new filter to get a list of matching endpoints. When you save a filter, you can run actions on the Agents as a set of objects or create a dynamic group (automatically adds new Agents that match the filter and drops Agents if they change to not match).
For example, you can save a filter with {"data":{"filterFields":{"infected":true}}} to run kill and quarantine commands on all the Agents at once, or to create a group that holds currently infected endpoints. Best Practice: Set a scope for the new Saved Filter. Run "accounts", "sites", or "groups" to get the IDs for the scope.

BEST PRACTICE

Set a scope for the new Saved Filter. Run "accounts", "sites", or "groups" to get the IDs for the scope.

Response Messages

200 - Filter successfully saved. Returns created object.

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - User is not allowed to perform this operation.

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
createdAt	Created at	true	string
id	Id	true	string
name	Name	true	string
scopeLevel	Filter scope	true	enum
updatedAt	Updated at	true	string
filterFields	A set of arguments composing the filter	false	

Name	Description	Required	Value
adComputerMember__contains	Free-text filter by Active	false	string []

									Directory computer groups string (supports multiple values)					
								adComputerName__contains	Free-text filter by Active Directory computer name string (supports multiple values)	false	string []			
								adComputerQuery__contains	Free-text filter by Active Directory computer name or its groups (supports multiple values)	false	string []			
								adQuery	An Active Directory query string	false	string			
								adQuery__contains	Free-text filter by Active Directory string (supports multiple values)	false	string []			
								adUserMember__contains	Free-text filter by Active Directory user groups string (supports	false	string []			

							multiple values)		
						adUserName__contains	Free-text filter by Active Directory username string (supports multiple values)	false	string []
						adUserQuery__contains	Free-text filter by Active Directory computer name or its groups (supports multiple values)	false	string []
						agentNamespace__contains	Free-text filter by agent namespace (supports multiple values)	false	string []
						agentPodName__contains	Free-text filter by agent pod name (supports multiple values)	false	string []
						agentVersions	Agent versions to include	false	string []
						agentVersionsNin	Agent versions not to include	false	string []
						appsVulnerabilityStatuses	Apps vulnerability status in	false	string []

							appsVulnerabilityStatusesNin	Apps vulnerability status nin	false	string []						
							awsRole__contains	Free-text filter by aws role(supports multiple values)	false	string []						
							awsSecurityGroups__contains	Free-text filter by aws securityGroups(supports multiple values)	false	string []						
							awsSubnetIds__contains	Free-text filter by aws subnet ids (supports multiple values)	false	string []						
							azureResourceGroup__contains	Free-text filter by azure resource group(supports multiple values)	false	string []						
							cloudAccount__contains	Free-text filter by cloud account (supports multiple values)	false	string []						
							cloudImage__contains	Free-text filter by cloud image (supports multiple values)	false	string []						
							cloudInstanceId__contains	Free-text filter by cloud instance id(supports	false	string []						

									multiple values)							
								cloudInstanceSize__contains	Free-text filter by cloud instance size(supports multiple values)	false	string []					
								cloudLocation__contains	Free-text filter by cloud location (supports multiple values)	false	string []					
								cloudNetwork__contains	Free-text filter by cloud network (supports multiple values)	false	string []					
								cloudProvider	Agents from which cloud provider	false	string []					
								cloudProviderNin	Exclude Agents from these cloud provider	false	string []					
								cloudTags__contains	Free-text filter by cloud tags (supports multiple values)	false	string []					
								clusterName__contains	Free-text filter by cluster name (supports multiple values)	false	string []					
								computerName__contains	Free-text filter by computer	false	string []					

									name (supports multiple values)					
								consoleMigrationStatuses	Migration status in	false	string []			
								consoleMigrationStatusesNin	Migration status nin	false	string []			
								coreCount__between	Possible number of CPU cores (inclusive)	false	string			
								cpuCount__between	Possible number of CPU cores (inclusive)	false	string			
								cpuId__contains	Free-text filter by CPU name (supports multiple values)	false	string []			
								domains	Included network domains	false	string []			
								domainsNin	Not included network domains	false	string []			
								encryptedApplications	Disk encryption status	false	boolean			
								externalId__contains	Free-text filter by external ID (Customer ID)	false	string []			
								externalIp__contains	Free-text filter by visible IP (supports multiple	false	string []			

								values)				
							filteredGroupIds	List of Group IDs to filter by	false	string []		
							filteredSiteIds	List of Site IDs to filter by	false	string []		
							firewallEnabled	The agents supports Firewall Control and it is enabled for the agent's group	false	boolean []		
							gcpServiceAccount__contains	Free-text filter by gcp service account (supports multiple values)	false	string []		
							hasLocalConfiguration	Agent has a local configuration set	false	boolean		
							hasTags	Include only Agents that have any tags assigned if True, or none if False	false	boolean		
							infected	Include only Agents with at least one active threat	false	boolean		
							installerTypes	Include only Agents installed with these package types	false	string []		

						installerTypesNin	Exclude Agents installed with these package types	false	string []
						isActive	Include only active Agents	false	boolean
						isDecommissioned	Include active, decommissioned or both	false	boolean []
						isPendingUninstall	Include only Agents with pending uninstall requests	false	boolean
						isUninstalled	Include installed, uninstalled or both	false	boolean []
						isUpToDate	Include only Agents with updated software	false	boolean
						k8sNodeLabels__contains	Free-text filter by K8s node labels (supports multiple values)	false	string []
						k8sNodeName__contains	Free-text filter by K8s node name (supports multiple values)	false	string []
						k8sType__contains	Free-text filter by K8s type(supports multiple values)	false	string []

							k8sVersion__contains	Free-text filter by K8s version (supports multiple values)	false	string []		
							lastActiveDate__between	Date range for last active date(format: <from_timestamp>-<to_timestamp>, inclusive)	false	string		
							lastLoggedInUserName__contains	Free-text filter by username (supports multiple values)	false	string []		
							lastSuccessfulScanDate__between	Date range for last successful full disk scan(format: <from_timestamp>-<to_timestamp>, inclusive)	false	string		
							liveUpdateId__contains	Free-text filter by live update ID (supports multiple values)	false	string []		
							locationEnabled	The agents supports Location Awareness and it is enabled for the agent's group	false	boolean []		
							locationIds	Include only	false	string []		

								Agents reporting these locations					
							locationIdsNin	Do not include only Agents reporting these locations	false	string []			
							machineTypes	Included machine types	false	string []			
							machineTypesNin	Not included machine types	false	string []			
							missingPermissions	Included missing permissions	false	string []			
							missingPermissionsNin	Excluded missing permissions	false	string []			
							networkInterfaceGatewayMacAddress__contains	Free-text filter by Gateway MAC address (supports multiple values)	false	string []			
							networkInterfaceInet__contains	Free-text filter by local IP (supports multiple values)	false	string []			
							networkInterfacePhysical__contains	Free-text filter by MAC address (supports multiple values)	false	string []			
							networkQuara	The agents	false	boolean []			

							ntineEnabled	supports Network Quarantine Control and its enabled for the agent's group						
							networkStatuses	Included network statuses	false	string []				
							networkStatusesNin	Included network statuses	false	string []				
							operationalStates	Agent operational state	false	string []				
							operationalStatesNin	Do not include these Agent operational states	false	string []				
							osArch	OS architecture	false	enum				
							osTypes	Included OS types	false	string []				
							osTypesNin	Not included OS types	false	string []				
							osVersion__contains	Free-text filter by OS full name and version (supports multiple values)	false	string []				
							query	A free-text search term, will match applicable attributes (sub-string match). Note:	false	string				

							Device's physical addresses will be matched if they start with the search term only (no match if they contain the term).		
						rangerStatus	[DEPRECATED] Use rangerStatuses.	false	enum
						rangerStatuses	Status of Ranger	false	string []
						rangerStatusesNin	Do not include these Ranger Statuses	false	string []
						rangerVersions	Ranger versions to include	false	string []
						rangerVersionsNin	Ranger versions not to include	false	string []
						registeredAt__between	Date range for first registration time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
						remoteProfilingStates	Agent remote profiling state	false	string []
						remoteProfilingStatesNin	Do not include these Agent remote profiling states	false	string []

							scanStatuses	Included scan statuses	false	string []		
							scanStatuses Nin	Not included scan statuses	false	string []		
							serialNumber __contains	Free-text filter by Serial Number (supports multiple values)	false	string []		
							tagsData	Filter agents by their assigned tags. Given in form of a JSON where each key represents a tag key, and each value represents a list of string values to filter by. To filter by unassigned tag values, use __nin suffix in the tag key.	false	string		
							threatReboot Required	Has at least one threat with at least one mitigation action pending reboot to succeed	false	boolean []		
							totalMemory __between	Total memory range (GB, inclusive)	false	string		
							userActionsN	Included	false	string []		

						eeded	pending user actions		
						userActionsNeededNin	Excluded pending user actions	false	string []
						uuid__contains	Free-text filter by Agent UUID (supports multiple values)	false	string []
			scopeId	Associated site/account	false	string			
			siteId	[DEPRECATED] Use scopeId instead	false	string			
errors	Errors	false	array						

Body Schema

Name	Description	Required	Value
data	Data	true	

Name	Description	Required	Value
filterFields	A set of parameters to filter by	true	

Name	Description	Required	Value
adComputerMember__contains	Free-text filter by Active Directory computer groups string (supports multiple values)	false	string []
adComputerName__contains	Free-text filter by Active Directory computer name string (supports multiple values)	false	string []
adComputerQuery__contains	Free-text filter by Active Directory computer name or its groups (supports multiple values)	false	string []
adQuery	An Active Directory query string	false	string
adQuery__contains	Free-text filter by Active Directory string	false	string []

							(supports multiple values)		
						adUserMember__contains	Free-text filter by Active Directory user groups string (supports multiple values)	false	string []
						adUserName__contains	Free-text filter by Active Directory username string (supports multiple values)	false	string []
						adUserQuery__contains	Free-text filter by Active Directory computer name or its groups (supports multiple values)	false	string []
						agentNamespace__contains	Free-text filter by agent namespace (supports multiple values)	false	string []
						agentPodName__contains	Free-text filter by agent pod name (supports multiple values)	false	string []

						agentVersions	Agent versions to include	false	string []
						agentVersionsNin	Agent versions not to include	false	string []
						appsVulnerabilityStatuses	Apps vulnerability status in	false	string []
						appsVulnerabilityStatusesNin	Apps vulnerability status nin	false	string []
						awsRole__contains	Free-text filter by aws role(supports multiple values)	false	string []
						awsSecurityGroups__contains	Free-text filter by aws securityGroups(supports multiple values)	false	string []
						awsSubnetIds__contains	Free-text filter by aws subnet ids (supports multiple values)	false	string []
						azureResourceGroup__contains	Free-text filter by azure resource group(supports multiple values)	false	string []
						cloudAccount__contains	Free-text filter by cloud account (supports multiple values)	false	string []

							cloudImage__contains	Free-text filter by cloud image (supports multiple values)	false	string []				
							cloudInstanceId__contains	Free-text filter by cloud instance id(supports multiple values)	false	string []				
							cloudInstanceSize__contains	Free-text filter by cloud instance size(supports multiple values)	false	string []				
							cloudLocation__contains	Free-text filter by cloud location (supports multiple values)	false	string []				
							cloudNetwork__contains	Free-text filter by cloud network (supports multiple values)	false	string []				
							cloudProvider	Agents from which cloud provider	false	string []				
							cloudProviderNin	Exclude Agents from these cloud provider	false	string []				
							cloudTags__contains	Free-text filter by cloud tags (supports multiple	false	string []				

									values)								
								clusterName__contains	Free-text filter by cluster name (supports multiple values)	false	string []						
								computerName__contains	Free-text filter by computer name (supports multiple values)	false	string []						
								consoleMigrationStatuses	Migration status in	false	string []						
								consoleMigrationStatusesNin	Migration status nin	false	string []						
								coreCount__between	Possible number of CPU cores (inclusive)	false	string						
								cpuCount__between	Possible number of CPU cores (inclusive)	false	string						
								cpuId__contains	Free-text filter by CPU name (supports multiple values)	false	string []						
								domains	Included network domains	false	string []						
								domainsNin	Not included network domains	false	string []						
								encryptedApplications	Disk encryption	false	boolean						

							status		
						externalId__contains	Free-text filter by external ID (Customer ID)	false	string []
						externalIp__contains	Free-text filter by visible IP (supports multiple values)	false	string []
						filteredGroupIds	List of Group IDs to filter by	false	string []
						filteredSiteIds	List of Site IDs to filter by	false	string []
						firewallEnabled	The agents supports Firewall Control and it is enabled for the agent's group	false	boolean []
						gcpServiceAccount__contains	Free-text filter by gcp service account (supports multiple values)	false	string []
						hasLocalConfiguration	Agent has a local configuration set	false	boolean
						hasTags	Include only Agents that have any tags assigned if True, or none if False	false	boolean

						infected	Include only Agents with at least one active threat	false	boolean		
						installerTypes	Include only Agents installed with these package types	false	string []		
						installerTypesNin	Exclude Agents installed with these package types	false	string []		
						isActive	Include only active Agents	false	boolean		
						isDecommissioned	Include active, decommissioned or both	false	boolean []		
						isPendingUninstall	Include only Agents with pending uninstall requests	false	boolean		
						isUninstalled	Include installed, uninstalled or both	false	boolean []		
						isUpToDate	Include only Agents with updated software	false	boolean		
						k8sNodeLabels__contains	Free-text filter by K8s node labels (supports multiple values)	false	string []		

							k8sNodeName__contains	Free-text filter by K8s node name (supports multiple values)	false	string []			
							k8sType__contains	Free-text filter by K8s type(supports multiple values)	false	string []			
							k8sVersion__contains	Free-text filter by K8s version (supports multiple values)	false	string []			
							lastActiveDate__between	Date range for last active date(format: <from_timestamp>-<to_timestamp>, inclusive)	false	string			
							lastLoggedInUserName__contains	Free-text filter by username (supports multiple values)	false	string []			
							lastSuccessfulScanDate__between	Date range for last successful full disk scan(format: <from_timestamp>-<to_timestamp>, inclusive)	false	string			
							liveUpdateId__contains	Free-text filter by live update ID (supports	false	string []			

									multiple values)					
								locationEnabled	The agents supports Location Awareness and it is enabled for the agent's group	false	boolean []			
								locationIds	Include only Agents reporting these locations	false	string []			
								locationIdsNin	Do not include only Agents reporting these locations	false	string []			
								machineTypes	Included machine types	false	string []			
								machineTypesNin	Not included machine types	false	string []			
								missingPermissions	Included missing permissions	false	string []			
								missingPermissionsNin	Excluded missing permissions	false	string []			
								networkInterfaceGatewayMacAddress__contains	Free-text filter by Gateway MAC address (supports multiple values)	false	string []			
								networkInterf	Free-text	false	string []			

							aceInet__contains	filter by local IP (supports multiple values)						
							networkInterfacePhysical__contains	Free-text filter by MAC address (supports multiple values)	false	string []				
							networkQuarantineEnabled	The agents supports Network Quarantine Control and its enabled for the agent's group	false	boolean []				
							networkStatuses	Included network statuses	false	string []				
							networkStatusesNin	Included network statuses	false	string []				
							operationalStates	Agent operational state	false	string []				
							operationalStatesNin	Do not include these Agent operational states	false	string []				
							osArch	OS architecture	false	enum				
							osTypes	Included OS types	false	string []				
							osTypesNin	Not included OS types	false	string []				
							osVersion__contains	Free-text filter by OS full name and	false	string []				

								version (supports multiple values)					
							query	A free-text search term, will match applicable attributes (sub-string match). Note: Device's physical addresses will be matched if they start with the search term only (no match if they contain the term).	false	string			
							rangerStatus	[DEPRECATED] Use rangerStatuses.	false	enum			
							rangerStatuses	Status of Ranger	false	string []			
							rangerStatusesNin	Do not include these Ranger Statuses	false	string []			
							rangerVersions	Ranger versions to include	false	string []			
							rangerVersionsNin	Ranger versions not to include	false	string []			
							registeredAt__between	Date range for first registration time (format:	false	string			

								<from_timestamp>-<to_timestamp>, inclusive)				
							remoteProfilingStates	Agent remote profiling state	false	string []		
							remoteProfilingStatesNin	Do not include these Agent remote profiling states	false	string []		
							scanStatuses	Included scan statuses	false	string []		
							scanStatusesNin	Not included scan statuses	false	string []		
							serialNumber__contains	Free-text filter by Serial Number (supports multiple values)	false	string []		
							tagsData	Filter agents by their assigned tags. Given in form of a JSON where each key represents a tag key, and each value represents a list of string values to filter by. To filter by unassigned tag values, use __nin suffix in the tag key.	false	string		
							threatReboot	Has at least	false	boolean []		

						Required: one threat with at least one mitigation action pending reboot to succeed
						totalMemory__between: Total memory range (GB, inclusive) — false — string
						userActionsNeeded: Included pending user actions — false — string []
						userActionsNeededNin: Excluded pending user actions — false — string []
						uuid__contains: Free-text filter by Agent UUID (supports multiple values) — false — string []
			name	New filter name	true	string
			scopeLevel	[DEPRECATED] Use the "filter" object instead.	false	enum
			siteId	[DEPRECATED] Use the "filter" object instead.	false	string
filter	Target scope for the new filter	false				

Name	Description	Required	Value
accountIds	List of Account IDs	false	string []

				to filter by			
			siteIds	List of Site IDs to filter by	false	string []	

Update Filter

PUT /web/api/v2.1/filters/{filter_id}

Update an existing filter

Response Messages

200 - Filter successfully updated. Returns updated object.

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - User is not allowed to perform this operation.

404 - Filter not found

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
createdAt	Created at	true	string
id	Id	true	string
name	Name	true	string
scopeLevel	Filter scope	true	enum
updatedAt	Updated at	true	string
filterFields	A set of arguments composing the filter	false	

Name	Description	Required	Value
adComputerMember__contains	Free-text filter by Active Directory computer groups string (supports multiple values)	false	string []

							adComputerName__contains	Free-text filter by Active Directory computer name string (supports multiple values)	false	string []		
							adComputerQuery__contains	Free-text filter by Active Directory computer name or its groups (supports multiple values)	false	string []		
							adQuery	An Active Directory query string	false	string		
							adQuery__contains	Free-text filter by Active Directory string (supports multiple values)	false	string []		
							adUserMember__contains	Free-text filter by Active Directory user groups string (supports multiple values)	false	string []		
							adUserName__contains	Free-text filter by Active Directory	false	string []		

									multiple values)					
								awsSecurityGroups__contains	Free-text filter by aws securityGroups(supports multiple values)	false	string []			
								awsSubnetIds__contains	Free-text filter by aws subnet ids (supports multiple values)	false	string []			
								azureResourceGroup__contains	Free-text filter by azure resource group(supports multiple values)	false	string []			
								cloudAccount__contains	Free-text filter by cloud account (supports multiple values)	false	string []			
								cloudImage__contains	Free-text filter by cloud image (supports multiple values)	false	string []			
								cloudInstanceId__contains	Free-text filter by cloud instance id(supports multiple values)	false	string []			
								cloudInstanceSize__contains	Free-text filter by cloud instance size(supports	false	string []			

							multiple values)		
						cloudLocation__contains	Free-text filter by cloud location (supports multiple values)	false	string []
						cloudNetwork__contains	Free-text filter by cloud network (supports multiple values)	false	string []
						cloudProvider	Agents from which cloud provider	false	string []
						cloudProviderNin	Exclude Agents from these cloud provider	false	string []
						cloudTags__contains	Free-text filter by cloud tags (supports multiple values)	false	string []
						clusterName__contains	Free-text filter by cluster name (supports multiple values)	false	string []
						computerName__contains	Free-text filter by computer name (supports multiple values)	false	string []
						consoleMigrationStatuses	Migration status in	false	string []

							consoleMigrationStatusesNin	Migration status nin	false	string []						
							coreCount__between	Possible number of CPU cores (inclusive)	false	string						
							cpuCount__between	Possible number of CPU cores (inclusive)	false	string						
							cpuId__contains	Free-text filter by CPU name (supports multiple values)	false	string []						
							domains	Included network domains	false	string []						
							domainsNin	Not included network domains	false	string []						
							encryptedApplications	Disk encryption status	false	boolean						
							externalId__contains	Free-text filter by external ID (Customer ID)	false	string []						
							externalIp__contains	Free-text filter by visible IP (supports multiple values)	false	string []						
							filteredGroupIds	List of Group IDs to filter by	false	string []						
							filteredSiteIds	List of Site IDs to filter	false	string []						

								by				
							firewallEnabled	The agents supports Firewall Control and it is enabled for the agent's group	false	boolean []		
							gcpServiceAccount__contains	Free-text filter by gcp service account (supports multiple values)	false	string []		
							hasLocalConfiguration	Agent has a local configuration set	false	boolean		
							hasTags	Include only Agents that have any tags assigned if True, or none if False	false	boolean		
							infected	Include only Agents with at least one active threat	false	boolean		
							installerTypes	Include only Agents installed with these package types	false	string []		
							installerTypesNin	Exclude Agents installed with these package types	false	string []		
							isActive	Include only	false	boolean		

							active Agents		
						isDecommissioned	Include active, decommissioned or both	false	boolean []
						isPendingUninstall	Include only Agents with pending uninstall requests	false	boolean
						isUninstalled	Include installed, uninstalled or both	false	boolean []
						isUpToDate	Include only Agents with updated software	false	boolean
						k8sNodeLabels__contains	Free-text filter by K8s node labels (supports multiple values)	false	string []
						k8sNodeName__contains	Free-text filter by K8s node name (supports multiple values)	false	string []
						k8sType__contains	Free-text filter by K8s type(supports multiple values)	false	string []
						k8sVersion__contains	Free-text filter by K8s version (supports multiple values)	false	string []

							lastActiveDate__between	Date range for last active date(format: <from_timestamp>-<to_timestamp>, inclusive)	false	string		
							lastLoggedInUserName__contains	Free-text filter by username (supports multiple values)	false	string []		
							lastSuccessfulScanDate__between	Date range for last successful full disk scan(format: <from_timestamp>-<to_timestamp>, inclusive)	false	string		
							liveUpdateId__contains	Free-text filter by live update ID (supports multiple values)	false	string []		
							locationEnabled	The agents supports Location Awareness and it is enabled for the agent's group	false	boolean []		
							locationIds	Include only Agents reporting these locations	false	string []		
							locationIdsNin	Do not include only	false	string []		

								Agents reporting these locations			
							machineTypes	Included machine types	false	string []	
							machineTypesNin	Not included machine types	false	string []	
							missingPermissions	Included missing permissions	false	string []	
							missingPermissionsNin	Excluded missing permissions	false	string []	
							networkInterfaceGatewayMacAddress__contains	Free-text filter by Gateway MAC address (supports multiple values)	false	string []	
							networkInterfaceInet__contains	Free-text filter by local IP (supports multiple values)	false	string []	
							networkInterfacePhysical__contains	Free-text filter by MAC address (supports multiple values)	false	string []	
							networkQuarantineEnabled	The agents supports Network Quarantine Control and its enabled for the agent's group	false	boolean []	

							networkStatuses	Included network statuses	false	string []				
							networkStatusesNin	Included network statuses	false	string []				
							operationalStates	Agent operational state	false	string []				
							operationalStatesNin	Do not include these Agent operational states	false	string []				
							osArch	OS architecture	false	enum				
							osTypes	Included OS types	false	string []				
							osTypesNin	Not included OS types	false	string []				
							osVersion__contains	Free-text filter by OS full name and version (supports multiple values)	false	string []				
							query	A free-text search term, will match applicable attributes (sub-string match). Note: Device's physical addresses will be matched if they start with the search term only (no	false	string				

								match if they contain the term).						
							rangerStatus	[DEPRECATED] Use rangerStatuses.	false	enum				
							rangerStatuses	Status of Ranger	false	string []				
							rangerStatusesNin	Do not include these Ranger Statuses	false	string []				
							rangerVersions	Ranger versions to include	false	string []				
							rangerVersionsNin	Ranger versions not to include	false	string []				
							registeredAt__between	Date range for first registration time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string				
							remoteProfilingStates	Agent remote profiling state	false	string []				
							remoteProfilingStatesNin	Do not include these Agent remote profiling states	false	string []				
							scanStatuses	Included scan statuses	false	string []				
							scanStatusesNin	Not included scan statuses	false	string []				
							serialNumber__contains	Free-text filter by Serial	false	string []				

									Number (supports multiple values)					
								tagsData	Filter agents by their assigned tags. Given in form of a JSON where each key represents a tag key, and each value represents a list of string values to filter by. To filter by unassigned tag values, use __nin suffix in the tag key.	false	string			
								threatRebootRequired	Has at least one threat with at least one mitigation action pending reboot to succeed	false	boolean []			
								totalMemory__between	Total memory range (GB, inclusive)	false	string			
								userActionsNeeded	Included pending user actions	false	string []			
								userActionsNeededNin	Excluded pending user actions	false	string []			
								uuid__contain	Free-text	false	string []			

						s	filter by Agent UUID (supports multiple values)		
			scopeId	Associated site/account	false	string			
			siteId	[DEPRECATED] Use scopeId instead	false	string			
errors	Errors	false	array						

Body Schema

Name	Description	Required	Value
data	Data	true	

Name	Description	Required	Value
filterFields	A set of parameters to filter by (If supplied, replaces existing parameter set	false	

Name	Description	Required	Value
adComputerMember__contains	Free-text filter by Active Directory computer groups string (supports multiple values)	false	string []
adComputerName__contains	Free-text filter by Active Directory computer name string (supports multiple values)	false	string []
adComputerQuery__contains	Free-text filter by Active Directory computer name or its groups (supports multiple values)	false	string []
adQuery	An Active Directory query string	false	string
adQuery__contains	Free-text filter by Active Directory string	false	string []

							(supports multiple values)		
						adUserMember__contains	Free-text filter by Active Directory user groups string (supports multiple values)	false	string []
						adUserName__contains	Free-text filter by Active Directory username string (supports multiple values)	false	string []
						adUserQuery__contains	Free-text filter by Active Directory computer name or its groups (supports multiple values)	false	string []
						agentNamespace__contains	Free-text filter by agent namespace (supports multiple values)	false	string []
						agentPodName__contains	Free-text filter by agent pod name (supports multiple values)	false	string []

							agentVersions	Agent versions to include	false	string []	
							agentVersionsNin	Agent versions not to include	false	string []	
							appsVulnerabilityStatuses	Apps vulnerability status in	false	string []	
							appsVulnerabilityStatusesNin	Apps vulnerability status nin	false	string []	
							awsRole__contains	Free-text filter by aws role(supports multiple values)	false	string []	
							awsSecurityGroups__contains	Free-text filter by aws securityGroups(supports multiple values)	false	string []	
							awsSubnetIds__contains	Free-text filter by aws subnet ids (supports multiple values)	false	string []	
							azureResourceGroup__contains	Free-text filter by azure resource group(supports multiple values)	false	string []	
							cloudAccount__contains	Free-text filter by cloud account (supports multiple values)	false	string []	

									values)								
								clusterName__contains	Free-text filter by cluster name (supports multiple values)	false	string []						
								computerName__contains	Free-text filter by computer name (supports multiple values)	false	string []						
								consoleMigrationStatuses	Migration status in	false	string []						
								consoleMigrationStatusesNin	Migration status nin	false	string []						
								coreCount__between	Possible number of CPU cores (inclusive)	false	string						
								cpuCount__between	Possible number of CPU cores (inclusive)	false	string						
								cpuId__contains	Free-text filter by CPU name (supports multiple values)	false	string []						
								domains	Included network domains	false	string []						
								domainsNin	Not included network domains	false	string []						
								encryptedApplications	Disk encryption	false	boolean						

							status		
						externalId__contains	Free-text filter by external ID (Customer ID)	false	string []
						externalIp__contains	Free-text filter by visible IP (supports multiple values)	false	string []
						filteredGroupIds	List of Group IDs to filter by	false	string []
						filteredSiteIds	List of Site IDs to filter by	false	string []
						firewallEnabled	The agents supports Firewall Control and it is enabled for the agent's group	false	boolean []
						gcpServiceAccount__contains	Free-text filter by gcp service account (supports multiple values)	false	string []
						hasLocalConfiguration	Agent has a local configuration set	false	boolean
						hasTags	Include only Agents that have any tags assigned if True, or none if False	false	boolean

						infected	Include only Agents with at least one active threat	false	boolean
						installerTypes	Include only Agents installed with these package types	false	string []
						installerTypesNin	Exclude Agents installed with these package types	false	string []
						isActive	Include only active Agents	false	boolean
						isDecommissioned	Include active, decommissioned or both	false	boolean []
						isPendingUninstall	Include only Agents with pending uninstall requests	false	boolean
						isUninstalled	Include installed, uninstalled or both	false	boolean []
						isUpToDate	Include only Agents with updated software	false	boolean
						k8sNodeLabels__contains	Free-text filter by K8s node labels (supports multiple values)	false	string []

							k8sNodeName__contains	Free-text filter by K8s node name (supports multiple values)	false	string []				
							k8sType__contains	Free-text filter by K8s type(supports multiple values)	false	string []				
							k8sVersion__contains	Free-text filter by K8s version (supports multiple values)	false	string []				
							lastActiveDate__between	Date range for last active date(format: <from_timestamp>-<to_timestamp>, inclusive)	false	string				
							lastLoggedInUserName__contains	Free-text filter by username (supports multiple values)	false	string []				
							lastSuccessfulScanDate__between	Date range for last successful full disk scan(format: <from_timestamp>-<to_timestamp>, inclusive)	false	string				
							liveUpdateId__contains	Free-text filter by live update ID (supports	false	string []				

									multiple values)					
								locationEnabled	The agents supports Location Awareness and it is enabled for the agent's group	false	boolean []			
								locationIds	Include only Agents reporting these locations	false	string []			
								locationIdsNin	Do not include only Agents reporting these locations	false	string []			
								machineTypes	Included machine types	false	string []			
								machineTypesNin	Not included machine types	false	string []			
								missingPermissions	Included missing permissions	false	string []			
								missingPermissionsNin	Excluded missing permissions	false	string []			
								networkInterfaceGatewayMacAddress__contains	Free-text filter by Gateway MAC address (supports multiple values)	false	string []			
								networkInterf	Free-text	false	string []			

							aceInet__contains	filter by local IP (supports multiple values)						
							networkInterfacePhysical__contains	Free-text filter by MAC address (supports multiple values)	false	string []				
							networkQuarantineEnabled	The agents supports Network Quarantine Control and its enabled for the agent's group	false	boolean []				
							networkStatuses	Included network statuses	false	string []				
							networkStatusesNin	Included network statuses	false	string []				
							operationalStates	Agent operational state	false	string []				
							operationalStatesNin	Do not include these Agent operational states	false	string []				
							osArch	OS architecture	false	enum				
							osTypes	Included OS types	false	string []				
							osTypesNin	Not included OS types	false	string []				
							osVersion__contains	Free-text filter by OS full name and	false	string []				

									version (supports multiple values)					
								query	A free-text search term, will match applicable attributes (sub-string match). Note: Device's physical addresses will be matched if they start with the search term only (no match if they contain the term).	false	string			
								rangerStatus	[DEPRECATED] Use rangerStatuses.	false	enum			
								rangerStatuses	Status of Ranger	false	string []			
								rangerStatusesNin	Do not include these Ranger Statuses	false	string []			
								rangerVersions	Ranger versions to include	false	string []			
								rangerVersionsNin	Ranger versions not to include	false	string []			
								registeredAt__between	Date range for first registration time (format:	false	string			

								<from_timestamp>-<to_timestamp>, inclusive)				
							remoteProfilingStates	Agent remote profiling state	false	string []		
							remoteProfilingStatesNin	Do not include these Agent remote profiling states	false	string []		
							scanStatuses	Included scan statuses	false	string []		
							scanStatusesNin	Not included scan statuses	false	string []		
							serialNumber__contains	Free-text filter by Serial Number (supports multiple values)	false	string []		
							tagsData	Filter agents by their assigned tags. Given in form of a JSON where each key represents a tag key, and each value represents a list of string values to filter by. To filter by unassigned tag values, use __nin suffix in the tag key.	false	string		
							threatReboot	Has at least	false	boolean []		

						Required	one threat with at least one mitigation action pending reboot to succeed		
						totalMemory__between	Total memory range (GB, inclusive)	false	string
						userActionsNeeded	Included pending user actions	false	string []
						userActionsNeededNin	Excluded pending user actions	false	string []
						uuid__contains	Free-text filter by Agent UUID (supports multiple values)	false	string []
			name	Updated filter name	false	string			

Delete Filter

DELETE /web/api/v2.1/filters/{filter_id}

Delete a saved filter.

Response Messages

200 - Filter successfully deleted.

401 - Unauthorized access - please sign in and retry.

403 - User is not allowed to perform this operation.

404 - Filter not found

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>success</td><td>Indicates a successful operation</td><td>false</td><td>boolean</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Get Deep Visibility Filters

GET /web/api/v2.1/filters/dv

Get saved Deep Visibility queries with full data. See Save Deep Visibility Filters.The response includes the ID of the filter, which you can use in other commands.

Parameters

accountids	optional	List of Account IDs to filter by. Example: "225494730938493804,225494730938493915".
countonly	optional	If true, only total number of items will be returned, without any of the actual objects.
cursor	optional	Cursor position returned by the last request. Use to iterate over more than 1000 items. Example: "YWdlbnRfaWQ6NTgwMjkzODE=".
groupids	optional	List of Group IDs to filter by. Example: "225494730938493804,225494730938493915".
ids	optional	A list of Filter IDs. Example: "225494730938493804,225494730938493915".
includechildren	optional	Return filters from children scope levels (Default: false)
includeglobal	optional	[DEPRECATED] Return global filters even when specific sites are selected
includeparents	optional	Return filters from parent scope levels (Default: false)
limit	optional	Limit number of returned items (1-1000). Example: "10".
query	optional	Text query for filter's name. Example: "MyFilter".
siteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".
skip	optional	Skip first number of items (0-1000). To iterate over more than 1000 items, use "cursor". Example: "150".
skipcount	optional	If true, total number of items will not be calculated, which speeds up execution time.
sortby	optional	The column to sort the results by. Example: "id".
sortorder	optional	Sort direction. Example: "asc".

Response Messages

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Save Deep Visibility Filter

POST /web/api/v2.1/filters/dv

Save a Deep Visibility query with data as a filter, to get notifications of specific events sent to named recipients on a given frequency. The recipients must be Console users with permissions on the scope of the query. Notifications are sent through email: you must have an SMTP server configured in the SentinelOne solution (/settings/smtp see Set SMTP Settings).
Deep Visibility requires a Complete SKU.

Response Messages

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Body Schema

Name	Description	Required	Value
data	Data	true	

Name	Description	Required	Value
filterFields	A set of parameters to filter by	true	

Name	Description	Required	Value
accountIds	List of Account IDs to filter by	false	string []
groupIds	List of Group IDs to filter by	false	string []
query	The query to be saved	false	string
queryType	Query Search Type	false	string
siteIds	List of Site IDs to filter	false	string []

<table>
<tr><td></td><td></td><td></td><td>
<table>
<tr><td></td><td></td><td></td><td>
<table>
<tr><td></td><td>by</td><td></td><td></td></tr>
<tr><td>timeRange</td><td>The timeframe in which events occurred</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>name</td><td>New filter name</td><td>true</td><td>string</td></tr>
<tr><td>frequency</td><td>Frequency</td><td>false</td><td>integer</td></tr>
<tr><td>notifications</td><td>Notifications</td><td>false</td><td>boolean</td></tr>
<tr><td>recipients</td><td>List of recipients</td><td>false</td><td>string []</td></tr>
</table>
</td></tr>
<tr><td>filter</td><td>Filter</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>groupIds</td><td>List of Group IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>scope_level</td><td>Filter scope</td><td>false</td><td>enum</td></tr>
<tr><td>siteIds</td><td>List of Site IDs to filter by</td><td>false</td><td>string []</td></tr>
</table>
</td></tr>
</table>

Delete Deep Visibility Filter

DELETE /web/api/v2.1/filters/dv/{filter_id}

Delete a saved Deep Visibility query.

Response Messages

200 - Filter successfully deleted.

401 - Unauthorized access - please sign in and retry.

403 - User is not allowed to perform this operation.

404 - Filter not found

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>success</td><td>Indicates a successful operation</td><td>false</td><td>boolean</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Update Deep Visibility Filter

PUT /web/api/v2.1/filters/dv/{filter_id}

Change a saved Deep Visibility filter. To get the ID and fields to change, run Get Deep Visibility Filters.

Response Messages

200 - Filter successfully updated. Returns updated object.

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - User is not allowed to perform this operation.

404 - Filter not found

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
createdAt	Created at	true	string
id	Id	true	string
name	Name	true	string
scopeLevel	Filter scope	true	enum
updatedAt	Updated at	true	string
filterFields	A set of parameters to filter by	false	

Name	Description	Required	Value
query	Deep visibility query	false	string
queryType	Either powerquery or events/processes/None	false	string

						timeRange | Deep visibility query time range | false | string
			frequency	Frequency	false	integer
			notifications	Notifications	false	boolean
			recipients	List of recipients	false	string []
			scopeId	Associated site/account	false	string
			scopeLevelName	Filter scope name	false	string
			siteId	[DEPRECATED] Use scopeId instead	false	string
errors	Errors	false	array			

Body Schema

Name	Description	Required	Value
data	Data	true	

Name	Description	Required	Value
filterFields	A set of parameters to filter by	true	

Name	Description	Required	Value
accountIds	List of Account IDs to filter by	false	string []
groupIds	List of Group IDs to filter by	false	string []
query	The query to be saved	false	string
queryType	Query Search Type	false	string
siteIds	List of Site IDs to filter by	false	string []
timeRange	The timeframe in which events occurred	false	string

Name	Description	Required	Value
name	New filter name	true	string
frequency	Frequency	false	integer
notifications	Notifications	false	boolean
recipients	List of recipients	false	string []

Name	Description	Required	Value
filter	Filter	true	

Name	Description	Required	Value
accountIds	List of Account IDs to filter by	false	string []
groupIds	List of Group IDs to filter by	false	string []
scope_level	Filter scope	false	enum

			siteIds	List of Site IDs to filter by	false	string []	

Upload CSV file

POST /web/api/v2.1/filters/csv-filter

Upload CSV file

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
data	Response data	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>endpointFoundCount</td><td>Number of endpoints found with these values</td><td>false</td><td>integer</td></tr><tr><td>filterId</td><td>ID of the filter</td><td>false</td><td>string</td></tr><tr><td>notFoundEndpoints</td><td>Not found endpoints</td><td>false</td><td>string []</td></tr><tr><td>rowsCount</td><td>Number of rows in the CSV file</td><td>false</td><td>integer</td></tr><tr><td>uniqueInputValuesCount</td><td>Number of unique values in the file</td><td>false</td><td>integer</td></tr></table>
errors	Errors	false	array

Body Schema

Name	Description	Required	Value
formData		false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>agentFilterField</td><td>The property of the endpoint to filter by</td><td>true</td><td>string</td></tr><tr><td>excludeHeader</td><td>Set to True to exclude the column header</td><td>true</td><td>boolean</td></tr><tr><td>file</td><td>File</td><td>true</td><td>file</td></tr></table>

Firewall Control

Get Firewall Rules

GET /web/api/v2.1/firewall-control

Get the Firewall Control rules for a scope specified by ID (run "accounts", "sites, "groups", or set "tenant" to "true") that match the filter.
The response will be quite long because it includes all the rule properties, thus at least one of these filters is required: action, status, osType, name, or scope ID.

Parameters

accountids	optional	List of Account IDs to filter by. Example: "225494730938493804,225494730938493915".
actions	optional	Return firewall rules with the filtered action. Example: "Allow".
application__contains	optional	Free-text filter by application (supports multiple values)
applications	optional	Return firewall rules with the filtered firewall class.
countonly	optional	If true, only total number of items will be returned, without any of the actual objects.
createdat__between	optional	Return firewall rules created within this range (inclusive). Example: "1514978764288-1514978999999".
createdat__gt	optional	Return firewall rules created after this timestamp. Example: "2018-02-27T04:49:26.257525Z".
createdat__gte	optional	Return firewall rules created after or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
createdat__lt	optional	Return firewall rules created before this timestamp. Example: "2018-02-27T04:49:26.257525Z".
createdat__lte	optional	Return firewall rules created before or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
cursor	optional	Cursor position returned by the last request. Use to iterate over more than 1000 items. Example: "YWdlbnRfaWQ6NTgwMjkzODE=".
directions	optional	Return firewall rules with the filtered directions. Example: "any".
disablepagination	optional	If true, all rules for requested scope will be returned

groupids	optional	List of Group IDs to filter by. Example: "225494730938493804,225494730938493915".
ids	optional	List of ids to filter by. Example: "225494730938493804,225494730938493915".
limit	optional	Limit number of returned items (1-1000). Example: "10".
locationids	optional	Filter by associated locations. Example: "225494730938493804,225494730938493915".
name	optional	Return firewall rules with the filtered name.
name__contains	optional	Free-text filter by the Rule name (supports multiple values)
ostypes	optional	Return firewall rules with the filtered os_type. Example: "macos".
protocol__contains	optional	Free-text filter by protocol (supports multiple values)
protocols	optional	Return firewall rules with the filtered protocols.
query	optional	Free text search on name, tag, application, protocol
scopes	optional	Return only firewall rules in this scope. Example: "account".
service__contains	optional	Free-text filter by service (supports multiple values)
siteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".
skip	optional	Skip first number of items (0-1000). To iterate over more than 1000 items, use "cursor". Example: "150".
skipcount	optional	If true, total number of items will not be calculated, which speeds up execution time.
sortby	optional	The column to sort the results by. Example: "id".
sortorder	optional	Sort direction. Example: "asc".
statuses	optional	Return firewall rules with the filtered status. Example: "Enabled".
tagids	optional	Filter by associated tags. Example: "225494730938493804,225494730938493915".
tagname__contains	optional	Free-text filter by the Tag name (supports multiple values)
tenant	optional	Indicates a tenant scope request

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>pagination</td><td>Pagination information</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>totalItems</td><td>Total number of items found matching your query</td><td>true</td><td>integer</td></tr>
<tr><td>nextCursor</td><td>Pass this value as "cursor" on your next request, to get the next page of results (Will be "null" when last page reached)</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>action</td><td>Defines if agent shall Block or Allow use of firewalls which matches the rule parameters.</td><td>false</td><td>enum</td></tr>
<tr><td>application</td><td>Application for the rule</td><td>false</td><td></td></tr>
<tr><td>createdAt</td><td>Date of rule creation</td><td>false</td><td>string</td></tr>
<tr><td>creator</td><td>Full name of the creating</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
</table>

				user		
			creatorId	Id of the creating user	false	string
			description	Description	false	string
			direction	Defines the Direction of the Firewall rule.	false	enum
			editable	True if the rule can be modified at this scope level	false	boolean
			id	Rule ID	false	string
			localHost	Local host	false	
			localPort	Local ports	false	
			location	Location associated with the rule	false	

Name	Description	Required	Value
type	Location type	true	enum
values	Location IDs (applicable for the "specific" location type only)	false	

Name	Description	Required	Value
id	Location ID	true	string
name	Location name	false	string
scope	Location scope	false	enum

name	The name of the firewall rule.	false	string
order	Position in the list of rules	false	integer
osType	[DEPRECATED] Please use os_types since multiple os types are supported.This field will	false	enum

	return the first os_type, not necessarily the only one.		
osTypes	Os types	false	string []
productId	Product identifier. Unique for a specific product module, per vendor ID, Interface.	false	string
protocol	The protocol.	false	string
remoteHost	[DEPRECATED] First remote host in the rule. Full list in remote_hosts	false	
remoteHosts	List of remote hosts	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>type</td><td>Type of the host</td><td>false</td><td>enum</td></tr><tr><td>values</td><td>Value of the host</td><td>false</td><td>string []</td></tr></table>
remotePort	Remote ports	false	
ruleCategory	Network quarantine rule or standard firewall rule	false	enum
scope	Scope of the rule	false	enum
scopeId	The group or site id depending on the scope. null if it is global.	false	string

<table>
<tr><td></td><td></td><td></td><td>
<table>
<tr><td>status</td><td>Defines if rule is Enabled or Disabled</td><td>false</td><td>enum</td></tr>
<tr><td>tag</td><td>[DEPRECATED] Free text to describe the rule. Please use description instead.</td><td>false</td><td>string</td></tr>
<tr><td>tagIds</td><td>Tag ids</td><td>false</td><td>string []</td></tr>
<tr><td>tagNames</td><td>Tag names</td><td>false</td><td>string []</td></tr>
<tr><td>tags</td><td>Tags</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>id</td><td></td><td>false</td><td>string</td></tr>
<tr><td>name</td><td></td><td>false</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>updatedAt</td><td>Date of last update</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Create Firewall Rule

POST /web/api/v2.1/firewall-control

Create a Firewall Control rule for a scope specified by ID (run "accounts", "sites", "groups", or set "tenant" to "true") and specific OS, to allow or block network traffic to matching endpoints.
You can create one clean-up rule, with the Action of Allow or Block and with no other parameters defined explicitly. Make this the default rule at the end of your rule list. Traffic that does not match other rules first will match this rule. If you do not have a clean-up rule to match all traffic, the default Firewall Control behavior is to allow traffic that is not explicitly blocked.
Firewall Control requires Control SKU.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
action	Defines if agent shall Block or Allow use of firewalls which matches the rule parameters.	false	enum
application	Application for the rule	false	
createdAt	Date of rule creation	false	string
creator	Full name of the creating user	false	string

			creatorId	Id of the creating user	false	string
			description	Description	false	string
			direction	Defines the Direction of the Firewall rule.	false	enum
			editable	True if the rule can be modified at this scope level	false	boolean
			id	Rule ID	false	string
			localHost	Local host	false	
			localPort	Local ports	false	
			location	Location associated with the rule	false	

Name	Description	Required	Value
type	Location type	true	enum
values	Location IDs (applicable for the "specific" location type only)	false	

Name	Description	Required	Value
id	Location ID	true	string
name	Location name	false	string
scope	Location scope	false	enum

name	The name of the firewall rule.	false	string
order	Position in the list of rules	false	integer
osType	[DEPRECATED] Please use os_types since multiple os types are supported.This field will return the first os_type,	false	enum

				not necessarily the only one.		
			osTypes	Os types	false	string []
			productId	Product identifier. Unique for a specific product module, per vendor ID, Interface.	false	string
			protocol	The protocol.	false	string
			remoteHost	[DEPRECATED] First remote host in the rule. Full list in remote_hosts	false	
			remoteHosts	List of remote hosts	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>type</td><td>Type of the host</td><td>false</td><td>enum</td></tr><tr><td>values</td><td>Value of the host</td><td>false</td><td>string []</td></tr></table>
			remotePort	Remote ports	false	
			ruleCategory	Network quarantine rule or standard firewall rule	false	enum
			scope	Scope of the rule	false	enum
			scopeId	The group or site id depending on the scope. null if it is global.	false	string
			status	Defines if rule is	false	enum

<table>
<tr><td></td><td></td><td></td><td>
<table>
<tr><td></td><td>Enabled or Disabled</td><td></td><td></td></tr>
<tr><td>tag</td><td>[DEPRECATED] Free text to describe the rule. Please use description instead.</td><td>false</td><td>string</td></tr>
<tr><td>tagIds</td><td>Tag ids</td><td>false</td><td>string []</td></tr>
<tr><td>tagNames</td><td>Tag names</td><td>false</td><td>string []</td></tr>
<tr><td>tags</td><td>Tags</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>id</td><td></td><td>false</td><td>string</td></tr>
<tr><td>name</td><td></td><td>false</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>updatedAt</td><td>Date of last update</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

Name	Description	Required	Value
data	Data	true	

Name	Description	Required	Value
action	Defines if agent shall Block or Allow use of firewalls which matches the rule parameters.	true	enum
name	The name of the firewall rule.	true	string
status	Defines if rule is Enabled or Disabled	true	enum
application	Application for the rule	false	
description	Description	false	string
direction	Defines the Direction of the Firewall rule.	false	enum
localHost	Local host structure with a type and a set of values	false	
localPort	Local ports structure with a type	false	

Name	Description	Required	Value
type	Type of the application	false	enum
values	Value of the application	false	string []

Name	Description	Required	Value
type	Type of the host	false	enum
values	Value of the host	false	string []

Name	Description	Required	Value
type	Type of the	false	enum

				and a set of values		

<table>
<tr><td></td><td></td><td></td><td>
<table>
<tr><td></td><td>values</td><td></td><td>
<table>
<tr><td></td><td>host</td><td></td><td></td></tr>
</table>
</td></tr>
<tr><td>remotePort</td><td>Remote ports structure with a type and a set of values</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>type</td><td>Type of the ports</td><td>false</td><td>enum</td></tr>
<tr><td>values</td><td>A list of port numbers</td><td>false</td><td>integer []</td></tr>
</table>
</td></tr>
<tr><td>tag</td><td>[DEPRECATED] Free text to describe the rule. Please use description instead.</td><td>false</td><td>string</td></tr>
<tr><td>tagIds</td><td>Tag ids</td><td>false</td><td>string []</td></tr>
</table>
</td></tr>
<tr><td>filter</td><td>Filter</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>groupIds</td><td>List of Group IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>siteIds</td><td>List of Site IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>tenant</td><td>Indicates a tenant scope request</td><td>false</td><td>boolean</td></tr>
</table>
</td></tr>
</table>

Delete Rules

DELETE /web/api/v2.1/firewall-control

Delete Firewall Control rules that match the filter.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
data	Response data	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>affected</td><td>Number of entities affected by the requested operation</td><td>false</td><td>integer</td></tr></table>
errors	Errors	false	array

Body Schema

Name	Description	Required	Value
filter	Filter	false	

Name	Description	Required	Value
accountIds	List of Account IDs to filter by	false	string []
actions	Return firewall rules with the filtered action.	false	string []
application__contains	Free-text filter by application (supports multiple values)	false	string []
applications	Return firewall rules with the filtered firewall class.	false	string []
createdAt__between	Return firewall rules created within this range (inclusive)	false	string
createdAt__gt	Return firewall rules created after this timestamp.	false	string
createdAt__gte	Return firewall rules created after or at this timestamp.	false	string
createdAt__lt	Return firewall rules	false	string

				created before this timestamp.		
			createdAt__lte	Return firewall rules created before or at this timestamp.	false	string
			directions	Return firewall rules with the filtered directions.	false	string []
			groupIds	List of Group IDs to filter by	false	string []
			ids	List of ids to filter by	false	string []
			locationIds	Filter by associated locations	false	string []
			name	Return firewall rules with the filtered name.	false	string
			name__contains	Free-text filter by the Rule name (supports multiple values)	false	string []
			osTypes	Return firewall rules with the filtered os_type.	false	string []
			protocol__contains	Free-text filter by protocol (supports multiple	false	string []

				values)		
			protocols	Return firewall rules with the filtered protocols.	false	string []
			query	Free text search on name, tag, application, protocol	false	string
			scopes	Return only firewall rules in this scope	false	string []
			service__contains	Free-text filter by service (supports multiple values)	false	string []
			siteIds	List of Site IDs to filter by	false	string []
			statuses	Return firewall rules with the filtered status.	false	string []
			tagIds	Filter by associated tags	false	string []
			tagName__contains	Free-text filter by the Tag name (supports multiple values)	false	string []
			tenant	Indicates a tenant scope request	false	boolean

Copy Rules

POST /web/api/v2.1/firewall-control/copy-rules

Copy a set of rules to other scopes.
In the filter of the body, enter the properties to define the source. In the data field of the body, define the targets by ID. To get a scope ID, run 'accounts', 'sites', or 'groups'.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>affected</td><td>Number of entities affected by the requested operation</td><td>false</td><td>integer</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountId</td><td>Target account</td><td>false</td><td>string</td></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>groupId</td><td>Target group</td><td>false</td><td>string</td></tr>
<tr><td>groupIds</td><td>[DEPRECATED] Target group(s)</td><td>false</td><td>string []</td></tr>
<tr><td>siteId</td><td>Target site</td><td>false</td><td>string</td></tr>
<tr><td>siteIds</td><td>List of Site IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>tenant</td><td>Indicates a tenant scope request</td><td>false</td><td>boolean</td></tr>
</table>
</td></tr>
<tr><td>filter</td><td>Filter</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>actions</td><td>Return firewall rules with the filtered action.</td><td>false</td><td>string []</td></tr>
<tr><td>application__contains</td><td>Free-text filter by application (supports multiple values)</td><td>false</td><td>string []</td></tr>
<tr><td>applications</td><td>Return firewall rules with the filtered</td><td>false</td><td>string []</td></tr>
</table>
</td></tr>
</table>

				firewall class.		
			createdAt__between	Return firewall rules created within this range (inclusive)	false	string
			createdAt__gt	Return firewall rules created after this timestamp.	false	string
			createdAt__gte	Return firewall rules created after or at this timestamp.	false	string
			createdAt__lt	Return firewall rules created before this timestamp.	false	string
			createdAt__lte	Return firewall rules created before or at this timestamp.	false	string
			directions	Return firewall rules with the filtered directions.	false	string []
			groupIds	List of Group IDs to filter by	false	string []
			ids	List of ids to filter by	false	string []
			locationIds	Filter by associated locations	false	string []

			name	Return firewall rules with the filtered name.	false	string
			name__contains	Free-text filter by the Rule name (supports multiple values)	false	string []
			osTypes	Return firewall rules with the filtered os_type.	false	string []
			protocol__contains	Free-text filter by protocol (supports multiple values)	false	string []
			protocols	Return firewall rules with the filtered protocols.	false	string []
			query	Free text search on name, tag, application, protocol	false	string
			scopes	Return only firewall rules in this scope	false	string []
			service__contains	Free-text filter by service (supports multiple values)	false	string []
			siteIds	List of Site IDs to filter	false	string []

				by		
			statuses	Return firewall rules with the filtered status.	false	string []
			tagIds	Filter by associated tags	false	string []
			tagName__contains	Free-text filter by the Tag name (supports multiple values)	false	string []
			tenant	Indicates a tenant scope request	false	boolean

Move Rules

POST /web/api/v2.1/firewall-control/move-rules

Remove Firewall Rules, defined with the ID of the rules (run 'firewall-control'), from scopes specified by ID (run 'accounts', 'sites', or 'groups') and add the rules to the scope IDs in the data field.
Firewall Control requires Control SKU.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>affected</td><td>Number of entities affected by the requested operation</td><td>false</td><td>integer</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountId</td><td>Target account</td><td>false</td><td>string</td></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>groupId</td><td>Target group</td><td>false</td><td>string</td></tr>
<tr><td>groupIds</td><td>[DEPRECATED] Target group(s)</td><td>false</td><td>string []</td></tr>
<tr><td>siteId</td><td>Target site</td><td>false</td><td>string</td></tr>
<tr><td>siteIds</td><td>List of Site IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>tenant</td><td>Indicates a tenant scope request</td><td>false</td><td>boolean</td></tr>
</table>
</td></tr>
<tr><td>filter</td><td>Filter</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>actions</td><td>Return firewall rules with the filtered action.</td><td>false</td><td>string []</td></tr>
<tr><td>application__contains</td><td>Free-text filter by application (supports multiple values)</td><td>false</td><td>string []</td></tr>
<tr><td>applications</td><td>Return firewall rules with the filtered</td><td>false</td><td>string []</td></tr>
</table>
</td></tr>
</table>

				firewall class.		
			createdAt__between	Return firewall rules created within this range (inclusive)	false	string
			createdAt__gt	Return firewall rules created after this timestamp.	false	string
			createdAt__gte	Return firewall rules created after or at this timestamp.	false	string
			createdAt__lt	Return firewall rules created before this timestamp.	false	string
			createdAt__lte	Return firewall rules created before or at this timestamp.	false	string
			directions	Return firewall rules with the filtered directions.	false	string []
			groupIds	List of Group IDs to filter by	false	string []
			ids	List of ids to filter by	false	string []
			locationIds	Filter by associated locations	false	string []

			name	Return firewall rules with the filtered name.	false	string
			name__contains	Free-text filter by the Rule name (supports multiple values)	false	string []
			osTypes	Return firewall rules with the filtered os_type.	false	string []
			protocol__contains	Free-text filter by protocol (supports multiple values)	false	string []
			protocols	Return firewall rules with the filtered protocols.	false	string []
			query	Free text search on name, tag, application, protocol	false	string
			scopes	Return only firewall rules in this scope	false	string []
			service__contains	Free-text filter by service (supports multiple values)	false	string []
			siteIds	List of Site IDs to filter	false	string []

				by		
			statuses	Return firewall rules with the filtered status.	false	string []
			tagIds	Filter by associated tags	false	string []
			tagName__contains	Free-text filter by the Tag name (supports multiple values)	false	string []
			tenant	Indicates a tenant scope request	false	boolean

Set Location

POST /web/api/v2.1/firewall-control/set-location

Set location attributes for a Location Aware Firewall Control rule. These rules are applied by Agents only if the network parameters of the endpoint match the properties of the location definition. To get a Location ID, run "locations".
Firewall Control requires Control SKU.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
data	Response data	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>affected</td><td>Number of entities affected by the requested operation</td><td>false</td><td>integer</td></tr></table>
errors	Errors	false	array

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>type</td><td>Location type</td><td>true</td><td>enum</td></tr>
<tr><td>values</td><td>Location IDs (applicable for the "specific" location type only)</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>id</td><td>Location ID</td><td>true</td><td>string</td></tr>
<tr><td>name</td><td>Location name</td><td>false</td><td>string</td></tr>
<tr><td>scope</td><td>Location scope</td><td>false</td><td>enum</td></tr>
</table>
</td></tr>
</table>
</td></tr>
<tr><td>filter</td><td>Filter</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>actions</td><td>Return firewall rules with the filtered action.</td><td>false</td><td>string []</td></tr>
<tr><td>application__contains</td><td>Free-text filter by application (supports multiple values)</td><td>false</td><td>string []</td></tr>
<tr><td>applications</td><td>Return firewall rules with the filtered firewall class.</td><td>false</td><td>string []</td></tr>
<tr><td>createdAt__between</td><td>Return firewall rules created within this range (inclusive)</td><td>false</td><td>string</td></tr>
<tr><td>createdAt__g</td><td>Return</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
</table>

			t	firewall rules created after this timestamp.			
			createdAt__gte	Return firewall rules created after or at this timestamp.	false	string	
			createdAt__lt	Return firewall rules created before this timestamp.	false	string	
			createdAt__lte	Return firewall rules created before or at this timestamp.	false	string	
			directions	Return firewall rules with the filtered directions.	false	string []	
			groupIds	List of Group IDs to filter by	false	string []	
			ids	List of ids to filter by	false	string []	
			locationIds	Filter by associated locations	false	string []	
			name	Return firewall rules with the filtered name.	false	string	
			name__contains	Free-text filter by the Rule name (supports multiple	false	string []	

				values)		
			osTypes	Return firewall rules with the filtered os_type.	false	string []
			protocol__contains	Free-text filter by protocol (supports multiple values)	false	string []
			protocols	Return firewall rules with the filtered protocols.	false	string []
			query	Free text search on name, tag, application, protocol	false	string
			scopes	Return only firewall rules in this scope	false	string []
			service__contains	Free-text filter by service (supports multiple values)	false	string []
			siteIds	List of Site IDs to filter by	false	string []
			statuses	Return firewall rules with the filtered status.	false	string []
			tagIds	Filter by associated tags	false	string []

			tagName__contains	Free-text filter by the Tag name (supports multiple values)	false	string []	
			tenant	Indicates a tenant scope request	false	boolean	

Reorder Rules

PUT /web/api/v2.1/firewall-control/reorder

Change the order of rules for a scope specified by ID (run "accounts", "sites", or "groups").
The Agent looks at the rules based on their order in the Firewall Control policy, from the top to the bottom. First it goes through the Group rules, then the Site rules, then the Account rules, then the Global rules. When the Agent finds a rule that matches the parameters of the traffic, that rule is applied. The Agent does not continue to the lower rules in the list. Thus, the scope and the order of the rules is important.
Firewall Control requires Control SKU.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>success</td><td>Indicates a successful operation</td><td>false</td><td>boolean</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>filter</td><td>Filter</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>groupIds</td><td>List of Group IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>osTypes</td><td>[DEPRECATED] Rules OS type (was relevant for when each OS type had its own rule order)</td><td>false</td><td>string []</td></tr>
<tr><td>siteIds</td><td>List of Site IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>tenant</td><td>Indicates a tenant scope request</td><td>false</td><td>boolean</td></tr>
</table>
</td></tr>
<tr><td>data</td><td>Data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>id</td><td>Rule ID</td><td>true</td><td>string</td></tr>
<tr><td>order</td><td>Desired position in the list of rules</td><td>true</td><td>integer</td></tr>
</table>
</td></tr>
</table>

Get Configuration

GET /web/api/v2.1/firewall-control/configuration

Get the Firewall Control configuration for a given scope.
To filter the results for a scope:
* Global - Make sure "tenant" is "true" and no other scope ID is given.
* Account - Make sure "tenant" is "false" and at least one Account ID is given.
* Site - Make sure "tenant" is "false" and at least one Site ID is given.
The response shows if Firewall Control is enabled for the scope, if Location Awareness is enabled, the higher scope from which this scope inherited the configuration, and whether a lower scope inherits this configuration.
Firewall Control requires Control SKU.

Parameters

accountids	optional	List of Account IDs to filter by. Example: "225494730938493804,225494730938493915".
groupids	optional	List of Group IDs to filter by. Example: "225494730938493804,225494730938493915".
siteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".
tenant	optional	Indicates a tenant scope request

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
enabled	Firewall control enabled for	false	boolean

				the scope		
			inheritAllFirewallRules	Inherit all the rules and tags from the parent scope. Expands on 'inherits' value.	false	boolean
			inheritedFrom	If null it means it is own policy else it tells the ancestor for the policy.For groups options are null/Site/Global, for site options are null/Global.	false	string
			inherits	True if rules are decoupled from parent rules	false	boolean
			inheritSettings	Inherit firewall settings from parent scope	false	boolean
			locationAware	Firewall control supports location awareness for the scope	false	boolean
			reportBlocked	Agent should report blocked events	false	boolean
			selectedTags	Selected tags	false	string []

errors	Errors	false	array

Update Configuration

PUT /web/api/v2.1/firewall-control/configuration

Change the Firewall Control configuration for a given scope.
To get the ID of a scope, run "accounts", "sites", or "groups". To change the Global configuration, leave the filters empty and set "tenant" to "true". In the Body, you can set if Firewall Control is enabled for the scope, if Location Awareness is enabled, the higher scope from which this scope inherits the configuration ("Global" or a scope ID), whether the lower scopes inherit this configuration, and whether blocked actions are reported.
Firewall Control requires Control SKU.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>enabled</td><td>Firewall control enabled for the scope</td><td>false</td><td>boolean</td></tr>
<tr><td>inheritAllFirewallRules</td><td>Inherit all the rules and tags from the parent scope. Expands on 'inherits' value.</td><td>false</td><td>boolean</td></tr>
<tr><td>inheritedFrom</td><td>If null it means it is own policy else it tells the ancestor for the policy.For</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
</table>

			groups options are null/Site/Global, for site options are null/Global.
			inherits: True if rules are decoupled from parent rules — false — boolean
			inheritSettings: Inherit firewall settings from parent scope — false — boolean
			locationAware: Firewall control supports location awareness for the scope — false — boolean
			reportBlocked: Agent should report blocked events — false — boolean
			selectedTags: Selected tags — false — string []
errors	Errors	false	array

Body Schema

Name	Description	Required	Value
data	Data	true	

Name	Description	Required	Value
enabled	Firewall control enabled for the scope	false	boolean
inheritAllFirewallRules	Inherit all the rules and tags from the parent scope. Expands on 'inherits' value.	false	boolean
inheritedFrom	If null it means it is own policy else it tells the ancestor for the policy.For groups options are null/Site/Global, for site options are null/Global.	false	string
inherits	True if rules are decoupled from parent rules	false	boolean
inheritSettings	Inherit firewall settings from parent scope	false	boolean
locationAware	Firewall control supports location	false	boolean

filter	Filter	true	

	awareness for the scope		
reportBlocked	Agent should report blocked events	false	boolean
selectedTags	Selected tags	false	string []

Name	Description	Required	Value
accountIds	List of Account IDs to filter by	false	string []
groupIds	List of Group IDs to filter by	false	string []
siteIds	List of Site IDs to filter by	false	string []
tenant	Indicates a tenant scope request	false	boolean

Export Rules

GET /web/api/v2.1/firewall-control/export

Export Firewall Control rules that match the filter to a JSON file from a scope specified by ID (run "accounts", "sites", "groups", or leave the scope empty and set "tenant" to "true") and import them to another scope (with the "import" command.
Firewall Control requires Control SKU.

Parameters

accountids	optional	List of Account IDs to filter by. Example: "225494730938493804,225494730938493915".
actions	optional	Return firewall rules with the filtered action. Example: "Allow".
application__contains	optional	Free-text filter by application (supports multiple values)
applications	optional	Return firewall rules with the filtered firewall class.
createdat__between	optional	Return firewall rules created within this range (inclusive). Example: "1514978764288-1514978999999".
createdat__gt	optional	Return firewall rules created after this timestamp. Example: "2018-02-27T04:49:26.257525Z".
createdat__gte	optional	Return firewall rules created after or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
createdat__lt	optional	Return firewall rules created before this timestamp. Example: "2018-02-27T04:49:26.257525Z".
createdat__lte	optional	Return firewall rules created before or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
directions	optional	Return firewall rules with the filtered directions. Example: "any".
groupids	optional	List of Group IDs to filter by. Example: "225494730938493804,225494730938493915".
ids	optional	List of ids to filter by. Example: "225494730938493804,225494730938493915".
locationids	optional	Filter by associated locations. Example: "225494730938493804,225494730938493915".
name	optional	Return firewall rules with the filtered name.
name__contains	optional	Free-text filter by the Rule name (supports multiple values)
ostypes	optional	Return firewall rules with the filtered os_type. Example: "macos".

protocol__contains	optional	Free-text filter by protocol (supports multiple values)
protocols	optional	Return firewall rules with the filtered protocols.
query	optional	Free text search on name, tag, application, protocol
scopes	optional	Return only firewall rules in this scope. Example: "account".
service__contains	optional	Free-text filter by service (supports multiple values)
siteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".
statuses	optional	Return firewall rules with the filtered status. Example: "Enabled".
tagids	optional	Filter by associated tags. Example: "225494730938493804,225494730938493915".
tagname__contains	optional	Free-text filter by the Tag name (supports multiple values)
tenant	optional	Indicates a tenant scope request

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Import Rules

POST /web/api/v2.1/firewall-control/import

Import Firewall Control rules from an exported JSON file to scopes specified by ID (run "accounts", "sites", "groups", or leave the scope empty and set "tenant" to "true"). Firewall Control requires Control SKU, in the target and in the source.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
data	Response data	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>success</td><td>Indicates a successful operation</td><td>false</td><td>boolean</td></tr></table>
errors	Errors	false	array

Body Schema

Name	Description	Required	Value
formData		false	

Name	Description	Required	Value
file	File	true	file
accountIds	List of Account IDs to filter by. Example: "225494730938493804,225494730938493915".	false	string []
groupIds	List of Group IDs to filter by. Example: "225494730938493804,225494730938493915".	false	string []
siteIds	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".	false	string []
tenant	Indicates a tenant scope request	false	boolean

Enable/Disable Rules

PUT /web/api/v2.1/firewall-control/enable

Change the status of a set of Firewall Control rules that match the filter to "Enabled" or "Disabled". In one request, you can set one status or the other.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>affected</td><td>Number of entities affected by the requested operation</td><td>false</td><td>integer</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>status</td><td>should the rules be enabled/ disabled</td><td>true</td><td>enum</td></tr>
</table>
</td></tr>
<tr><td>filter</td><td>Filter</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>actions</td><td>Return firewall rules with the filtered action.</td><td>false</td><td>string []</td></tr>
<tr><td>application__contains</td><td>Free-text filter by application (supports multiple values)</td><td>false</td><td>string []</td></tr>
<tr><td>applications</td><td>Return firewall rules with the filtered firewall class.</td><td>false</td><td>string []</td></tr>
<tr><td>createdAt__between</td><td>Return firewall rules created within this range (inclusive)</td><td>false</td><td>string</td></tr>
<tr><td>createdAt__gt</td><td>Return firewall rules created after this timestamp.</td><td>false</td><td>string</td></tr>
<tr><td>createdAt__g</td><td>Return</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
</table>

			te	firewall rules created after or at this timestamp.		
			createdAt__lt	Return firewall rules created before this timestamp.	false	string
			createdAt__lte	Return firewall rules created before or at this timestamp.	false	string
			directions	Return firewall rules with the filtered directions.	false	string []
			groupIds	List of Group IDs to filter by	false	string []
			ids	List of ids to filter by	false	string []
			locationIds	Filter by associated locations	false	string []
			name	Return firewall rules with the filtered name.	false	string
			name__contains	Free-text filter by the Rule name (supports multiple values)	false	string []
			osTypes	Return firewall rules with the filtered	false	string []

				os_type.		
			protocol__contains	Free-text filter by protocol (supports multiple values)	false	string []
			protocols	Return firewall rules with the filtered protocols.	false	string []
			query	Free text search on name, tag, application, protocol	false	string
			scopes	Return only firewall rules in this scope	false	string []
			service__contains	Free-text filter by service (supports multiple values)	false	string []
			siteIds	List of Site IDs to filter by	false	string []
			statuses	Return firewall rules with the filtered status.	false	string []
			tagIds	Filter by associated tags	false	string []
			tagName__contains	Free-text filter by the Tag name (supports multiple	false	string []

				values)		
			tenant	Indicates a tenant scope request	false	boolean

Get Protocols

GET /web/api/v2.1/firewall-control/protocols

Get a list of protocols that can be used in Firewall Control rules.

Parameters

countonly	optional	If true, only total number of items will be returned, without any of the actual objects.
cursor	optional	Cursor position returned by the last request. Use to iterate over more than 1000 items. Example: "YWdlbnRfaWQ6NTgwMjkzODE=".
disablepagination	optional	If true, all rules for requested scope will be returned
limit	optional	Limit number of returned items (1-1000). Example: "10".
query	optional	Full text search on protocols
skip	optional	Skip first number of items (0-1000). To iterate over more than 1000 items, use "cursor". Example: "150".
skipcount	optional	If true, total number of items will not be calculated, which speeds up execution time.
sortby	optional	The column to sort the results by. Example: "id".
sortorder	optional	Sort direction. Example: "asc".

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
pagination	Pagination information	true	

Name	Description	Required	Value
totalItems	Total number	true	integer

			of items found matching your query		
			nextCursor	Pass this value as "cursor" on your next request, to get the next page of results (Will be "null" when last page reached)	false	string
data	Response data	false	Name	Description	Required	Value
			accountIds	List of Account IDs to filter by	false	string []
			groupIds	List of Group IDs to filter by	false	string []
			name	Description of the protocol	false	string
			siteIds	List of Site IDs to filter by	false	string []
			tenant	Indicates a tenant scope request	false	boolean
			value	Short code identifying the protocol	false	string
errors	Errors	false	array			

Add Rule Tags

POST /web/api/v2.1/firewall-control/add-tags

Create a Firewall Rule tag.
Create tags to represent Firewall policies - a set of rules in a specific order. After you create the tag, add rules to it.
Notes:
* Tags apply to a scope and cannot be linked to rules from different scopes.
* Tags must be 2 to 256 characters.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>affected</td><td>Number of entities affected by the requested operation</td><td>false</td><td>integer</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>tagIds</td><td>Tag ids</td><td>false</td><td>string []</td></tr>
</table>
</td></tr>
<tr><td>filter</td><td>Filter</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>actions</td><td>Return firewall rules with the filtered action.</td><td>false</td><td>string []</td></tr>
<tr><td>application__contains</td><td>Free-text filter by application (supports multiple values)</td><td>false</td><td>string []</td></tr>
<tr><td>applications</td><td>Return firewall rules with the filtered firewall class.</td><td>false</td><td>string []</td></tr>
<tr><td>createdAt__between</td><td>Return firewall rules created within this range (inclusive)</td><td>false</td><td>string</td></tr>
<tr><td>createdAt__gt</td><td>Return firewall rules created after this timestamp.</td><td>false</td><td>string</td></tr>
<tr><td>createdAt__gte</td><td>Return firewall rules created after or at this</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
</table>

				timestamp.		
			createdAt__lt	Return firewall rules created before this timestamp.	false	string
			createdAt__lte	Return firewall rules created before or at this timestamp.	false	string
			directions	Return firewall rules with the filtered directions.	false	string []
			groupIds	List of Group IDs to filter by	false	string []
			ids	List of ids to filter by	false	string []
			locationIds	Filter by associated locations	false	string []
			name	Return firewall rules with the filtered name.	false	string
			name__contains	Free-text filter by the Rule name (supports multiple values)	false	string []
			osTypes	Return firewall rules with the filtered os_type.	false	string []
			protocol__con	Free-text	false	string []

			tains	filter by protocol (supports multiple values)		
			protocols	Return firewall rules with the filtered protocols.	false	string []
			query	Free text search on name, tag, application, protocol	false	string
			scopes	Return only firewall rules in this scope	false	string []
			service__contains	Free-text filter by service (supports multiple values)	false	string []
			siteIds	List of Site IDs to filter by	false	string []
			statuses	Return firewall rules with the filtered status.	false	string []
			tagIds	Filter by associated tags	false	string []
			tagName__contains	Free-text filter by the Tag name (supports multiple values)	false	string []
			tenant	Indicates a	false	boolean

				tenant scope request		

Remove Rule Tags

POST /web/api/v2.1/firewall-control/remove-tags

Remove firewall tags from rules matching the filter.
Tags represent Firewall policies - a set of rules in a specific order. When you remove a rule with a tag, all scopes that subscribe to the tag get the change.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>affected</td><td>Number of entities affected by the requested operation</td><td>false</td><td>integer</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>tagIds</td><td>Tag ids</td><td>false</td><td>string []</td></tr>
</table>
</td></tr>
<tr><td>filter</td><td>Filter</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>actions</td><td>Return firewall rules with the filtered action.</td><td>false</td><td>string []</td></tr>
<tr><td>application__contains</td><td>Free-text filter by application (supports multiple values)</td><td>false</td><td>string []</td></tr>
<tr><td>applications</td><td>Return firewall rules with the filtered firewall class.</td><td>false</td><td>string []</td></tr>
<tr><td>createdAt__between</td><td>Return firewall rules created within this range (inclusive)</td><td>false</td><td>string</td></tr>
<tr><td>createdAt__gt</td><td>Return firewall rules created after this timestamp.</td><td>false</td><td>string</td></tr>
<tr><td>createdAt__gte</td><td>Return firewall rules created after or at this</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
</table>

				timestamp.		
			createdAt__lt	Return firewall rules created before this timestamp.	false	string
			createdAt__lte	Return firewall rules created before or at this timestamp.	false	string
			directions	Return firewall rules with the filtered directions.	false	string []
			groupIds	List of Group IDs to filter by	false	string []
			ids	List of ids to filter by	false	string []
			locationIds	Filter by associated locations	false	string []
			name	Return firewall rules with the filtered name.	false	string
			name__contains	Free-text filter by the Rule name (supports multiple values)	false	string []
			osTypes	Return firewall rules with the filtered os_type.	false	string []
			protocol__con	Free-text	false	string []

			tains	filter by protocol (supports multiple values)		
			protocols	Return firewall rules with the filtered protocols.	false	string []
			query	Free text search on name, tag, application, protocol	false	string
			scopes	Return only firewall rules in this scope	false	string []
			service__contains	Free-text filter by service (supports multiple values)	false	string []
			siteIds	List of Site IDs to filter by	false	string []
			statuses	Return firewall rules with the filtered status.	false	string []
			tagIds	Filter by associated tags	false	string []
			tagName__contains	Free-text filter by the Tag name (supports multiple values)	false	string []
			tenant	Indicates a	false	boolean

				tenant scope request		

Get Tag Firewall Rules

GET /web/api/v2.1/firewall-control/tag-rules/{tag_id}

Get all Firewall rules linked to tag, regardless of inheritance mode.
To get the ID of a tag, run the firewall-control API (see Get Firewall Rules) and see tagIDs in the response.

Parameters

accountids	optional	List of Account IDs to filter by. Example: "225494730938493804,225494730938493915".
actions	optional	Return firewall rules with the filtered action. Example: "Allow".
application__contains	optional	Free-text filter by application (supports multiple values)
applications	optional	Return firewall rules with the filtered firewall class.
countonly	optional	If true, only total number of items will be returned, without any of the actual objects.
createdat__between	optional	Return firewall rules created within this range (inclusive). Example: "1514978764288-1514978999999".
createdat__gt	optional	Return firewall rules created after this timestamp. Example: "2018-02-27T04:49:26.257525Z".
createdat__gte	optional	Return firewall rules created after or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
createdat__lt	optional	Return firewall rules created before this timestamp. Example: "2018-02-27T04:49:26.257525Z".
createdat__lte	optional	Return firewall rules created before or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
cursor	optional	Cursor position returned by the last request. Use to iterate over more than 1000 items. Example: "YWdlbnRfaWQ6NTgwMjkzODE=".
directions	optional	Return firewall rules with the filtered directions. Example: "any".
disablepagination	optional	If true, all rules for requested scope will be returned
groupids	optional	List of Group IDs to filter by. Example: "225494730938493804,225494730938493915".
ids	optional	List of ids to filter by. Example: "225494730938493804,225494730938493915".

limit	optional	Limit number of returned items (1-1000). Example: "10".
locationids	optional	Filter by associated locations. Example: "225494730938493804,225494730938493915".
name	optional	Return firewall rules with the filtered name.
name__contains	optional	Free-text filter by the Rule name (supports multiple values)
ostypes	optional	Return firewall rules with the filtered os_type. Example: "macos".
protocol__contains	optional	Free-text filter by protocol (supports multiple values)
protocols	optional	Return firewall rules with the filtered protocols.
query	optional	Free text search on name, tag, application, protocol
scopes	optional	Return only firewall rules in this scope. Example: "account".
service__contains	optional	Free-text filter by service (supports multiple values)
siteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".
skip	optional	Skip first number of items (0-1000). To iterate over more than 1000 items, use "cursor". Example: "150".
skipcount	optional	If true, total number of items will not be calculated, which speeds up execution time.
sortby	optional	The column to sort the results by. Example: "id".
sortorder	optional	Sort direction. Example: "asc".
statuses	optional	Return firewall rules with the filtered status. Example: "Enabled".
tagids	optional	Filter by associated tags. Example: "225494730938493804,225494730938493915".
tagname__contains	optional	Free-text filter by the Tag name (supports multiple values)
tenant	optional	Indicates a tenant scope request

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>pagination</td><td>Pagination information</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>totalItems</td><td>Total number of items found matching your query</td><td>true</td><td>integer</td></tr>
<tr><td>nextCursor</td><td>Pass this value as "cursor" on your next request, to get the next page of results (Will be "null" when last page reached)</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>action</td><td>Defines if agent shall Block or Allow use of firewalls which matches the rule parameters.</td><td>false</td><td>enum</td></tr>
<tr><td>application</td><td>Application for the rule</td><td>false</td><td></td></tr>
<tr><td>createdAt</td><td>Date of rule creation</td><td>false</td><td>string</td></tr>
<tr><td>creator</td><td>Full name of the creating user</td><td>false</td><td>string</td></tr>
<tr><td>creatorId</td><td>Id of the creating user</td><td>false</td><td>string</td></tr>
<tr><td>description</td><td>Description</td><td>false</td><td>string</td></tr>
<tr><td>direction</td><td>Defines the</td><td>false</td><td>enum</td></tr>
</table>
</td></tr>
</table>

	Direction of the Firewall rule.	
editable	True if the rule can be modified at this scope level	false
id	Rule ID	false
localHost	Local host	false
localPort	Local ports	false
location	Location associated with the rule	false

Name	Description	Required	Value
type	Location type	true	enum
values	Location IDs (applicable for the "specific" location type only)	false	

Name	Description	Required	Value
id	Location ID	true	string
name	Location name	false	string
scope	Location scope	false	enum

name	The name of the firewall rule.	false	string
order	Position in the list of rules	false	integer
osType	[DEPRECATED] Please use os_types since multiple os types are supported.This field will return the first os_type, not necessarily the only one.	false	enum
osTypes	Os types	false	string []

			productId	Product identifier. Unique for a specific product module, per vendor ID, Interface.	false	string
			protocol	The protocol.	false	string
			remoteHost	[DEPRECATED] First remote host in the rule. Full list in remote_hosts	false	
			remoteHosts	List of remote hosts	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>type</td><td>Type of the host</td><td>false</td><td>enum</td></tr><tr><td>values</td><td>Value of the host</td><td>false</td><td>string []</td></tr></table>
			remotePort	Remote ports	false	
			ruleCategory	Network quarantine rule or standard firewall rule	false	enum
			scope	Scope of the rule	false	enum
			scopeId	The group or site id depending on the scope. null if it is global.	false	string
			status	Defines if rule is Enabled or Disabled	false	enum
			tag	[DEPRECATED] Free text	false	string

<table>
<tr><td></td><td></td><td></td><td>
<table>
<tr><td></td><td>to describe the rule. Please use description instead.</td><td></td><td></td></tr>
<tr><td>tagIds</td><td>Tag ids</td><td>false</td><td>string []</td></tr>
<tr><td>tagNames</td><td>Tag names</td><td>false</td><td>string []</td></tr>
<tr><td>tags</td><td>Tags</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>id</td><td></td><td>false</td><td>string</td></tr>
<tr><td>name</td><td></td><td>false</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>updatedAt</td><td>Date of last update</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Update Firewall Rule

PUT /web/api/v2.1/firewall-control/{firewall_rule_category}

Change a Firewall Control rule.
This command requires the rule ID, which you can get from "firewall-control" (see Get Firewall Rules) or "firewall-control/unscoped" (see Get Unscoped Rules).

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

404 - Firewall rule not found

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
action	Defines if agent shall Block or Allow use of firewalls which matches the rule parameters.	false	enum
application	Application for the rule	false	
createdAt	Date of rule creation	false	string
creator	Full name of the creating user	false	string
creatorId	Id of the creating user	false	string

			description	Description	false	string
			direction	Defines the Direction of the Firewall rule.	false	enum
			editable	True if the rule can be modified at this scope level	false	boolean
			id	Rule ID	false	string
			localHost	Local host	false	
			localPort	Local ports	false	
			location	Location associated with the rule	false	

Name	Description	Required	Value
type	Location type	true	enum
values	Location IDs (applicable for the "specific" location type only)	false	

Name	Description	Required	Value
id	Location ID	true	string
name	Location name	false	string
scope	Location scope	false	enum

name	The name of the firewall rule.	false	string
order	Position in the list of rules	false	integer
osType	[DEPRECATED] Please use os_types since multiple os types are supported.This field will return the first os_type, not necessarily	false	enum

	the only one.		
osTypes	Os types	false	string []
productId	Product identifier. Unique for a specific product module, per vendor ID, Interface.	false	string
protocol	The protocol.	false	string
remoteHost	[DEPRECATED] First remote host in the rule. Full list in remote_hosts	false	
remoteHosts	List of remote hosts	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>type</td><td>Type of the host</td><td>false</td><td>enum</td></tr><tr><td>values</td><td>Value of the host</td><td>false</td><td>string []</td></tr></table>
remotePort	Remote ports	false	
ruleCategory	Network quarantine rule or standard firewall rule	false	enum
scope	Scope of the rule	false	enum
scopeId	The group or site id depending on the scope. null if it is global.	false	string
status	Defines if rule is Enabled or Disabled	false	enum

<table>
<tr><td></td><td></td><td></td><td>
<table>
<tr><td>tag</td><td>[DEPRECATED] Free text to describe the rule. Please use description instead.</td><td>false</td><td>string</td></tr>
<tr><td>tagIds</td><td>Tag ids</td><td>false</td><td>string []</td></tr>
<tr><td>tagNames</td><td>Tag names</td><td>false</td><td>string []</td></tr>
<tr><td>tags</td><td>Tags</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>id</td><td></td><td>false</td><td>string</td></tr>
<tr><td>name</td><td></td><td>false</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>updatedAt</td><td>Date of last update</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

Name	Description	Required	Value
data	Data	true	

Name	Description	Required	Value
action	Defines if agent shall Block or Allow use of firewalls which matches the rule parameters.	false	enum
application	Application for the rule	false	

Name	Description	Required	Value
type	Type of the application	false	enum
values	Value of the application	false	string []

Name	Description	Required	Value
description	Description	false	string
direction	Defines the Direction of the Firewall rule.	false	enum
localHost	Local host structure with a type and a set of values	false	

Name	Description	Required	Value
type	Type of the host	false	enum
values	Value of the host	false	string []

Name	Description	Required	Value
localPort	Local ports structure with a type and a set of values	false	

Name	Description	Required	Value
type	Type of the ports	false	enum
values	A list of port numbers	false	integer []

Name	Description	Required	Value
location	Location structure with a type and a set of	false	

Name	Description	Required	Value
type	Location type	true	enum

				values		values	Location IDs (applicable for the "specific" location type only)	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>id</td><td>Location ID</td><td>true</td><td>string</td></tr><tr><td>name</td><td>Location name</td><td>false</td><td>string</td></tr><tr><td>scope</td><td>Location scope</td><td>false</td><td>enum</td></tr></table>
				name	The name of the firewall rule.	false	string		
				osType	[DEPRECATED] Please use os_types since multiple os types are supported.This field will return the first os_type, not necessarily the only one.	false	enum		
				osTypes	Os types	false	string []		
				protocol	The protocol	false	string		
				remoteHost	[DEPRECATED] Please use remote_hosts .Remote host structure with a type and a set of values.	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>type</td><td>Type of the host</td><td>false</td><td>enum</td></tr><tr><td>values</td><td>Value of the host</td><td>false</td><td>string []</td></tr></table>		
				remoteHosts	List of remote hosts, each structured with a type and a set of values	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>type</td><td>Type of the host</td><td>false</td><td>enum</td></tr><tr><td>values</td><td>Value of the host</td><td>false</td><td>string []</td></tr></table>		
				remotePort	Remote ports structure	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr></table>		

				with a type and a set of values		type: Type of the ports; false; enum values: A list of port numbers; false; integer []
			status	Defines if rule is Enabled or Disabled	false	enum
			tag	[DEPRECATED] Free text to describe the rule. Please use description instead.	false	string
			tagIds	Tag ids	false	string []

Forensics

Application Forensics

GET /web/api/v2.1/applications/{application_id}/forensics

DEPRECATED

Parameters

accountids	optional	List of Account IDs to filter by. Example: "225494730938493804,225494730938493915".
groupids	optional	List of Group IDs to filter by. Example: "225494730938493804,225494730938493915".
siteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

404 - Not found

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
result	Result	false	

Name	Description	Required	Value
agent	Agent	false	string
application_created	Application created	false	string

application_id	Application id	false	string
fetch_story_status	Fetch story status	false	string
file	File	false	

Name	Description	Required	Value
content_hash	Content hash	false	string
created_date	Created date	false	string
display_name	Display name	false	string
is_system	Is system	false	boolean
object_id	Object id	false	string
path	Path	false	string
permission	Permission	false	string
size	Size	false	integer

malicious_process_arguments	Malicious process arguments	false	string
process	Process	false	

Name	Description	Required	Value
bundle_id	Bundle id	false	string
created_date	Created date	false	string
display_name	Display name	false	string
executable_file_id	Executable file id	false	string
is_primary	Is primary	false	boolean
is_root	Is root	false	boolean
object_id	Object id	false	string
pid	Pid	false	integer
username	Username	false	string

process_created_at	Process created at	false	string
process_display_name	Process display name	false	string
seen_on_network	Seen on network	false	integer

			success | Success | false | boolean
errors	Errors	false	array

Application Forensics - Detailed

GET /web/api/v2.1/applications/{application_id}/forensics/details

[DEPRECATED] Returns an empty array

Parameters

accountids	optional	List of Account IDs to filter by. Example: "225494730938493804,225494730938493915".
groupids	optional	List of Group IDs to filter by. Example: "225494730938493804,225494730938493915".
siteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

404 - Not found

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
result	Result	false	

Name	Description	Required	Value
agent	Agent	false	string
application_created	Application created	false	string
application_duration	Application duration	false	string
application_id	Application id	false	string

						category_scores	Category scores	false	
						fetch_story_error_at	Fetch story error at	false	string
						fetch_story_sent_at	Fetch story sent at	false	string
						fetch_story_status	Fetch story status	false	string
						file	File	false	
						graph	Graph	false	
						last_event_seen_at	Last event seen at	false	string
						process	Process	false	
						process_created_at	Process created at	false	string

Name	Description	Required	Value
content_hash	Content hash	false	string
created_date	Created date	false	string
display_name	Display name	false	string
is_system	Is system	false	boolean
object_id	Object id	false	string
path	Path	false	string
permission	Permission	false	string
size	Size	false	integer

Name	Description	Required	Value
bundle_id	Bundle id	false	string
created_date	Created date	false	string
display_name	Display name	false	string
executable_file_id	Executable file id	false	string
is_primary	Is primary	false	boolean
is_root	Is root	false	boolean
object_id	Object id	false	string
pid	Pid	false	integer
username	Username	false	string

						process_display_name	Process display name	false	string
						raw_data	Raw data	false	
						seen_on_network	Seen on network	false	integer
						summary	Summary	false	
						summary_overview	Summary overview	false	

Name	Description	Required	Value
file	File	false	
network	Network	false	
registry	Registry	false	

Name	D
create	Cr
delete	De
write	W

Name	D
connections	Co
dns	Dn

Name	D
persistence	Pe
security	Se
stealth	St

			success	Success	false	boolean
errors	Errors	false	array			

Application Connections

GET /web/api/v2.1/applications/{application_id}/forensics/connections

[DEPRECATED] Returns an empty array

Parameters

accountids	optional	List of Account IDs to filter by. Example: "225494730938493804,225494730938493915".
country_code	optional	Country code
groupids	optional	List of Group IDs to filter by. Example: "225494730938493804,225494730938493915".
siteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

404 - Not found

Response Schema

Name	Description	Required	Value
data	Response data	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>data</td><td>Data</td><td>false</td><td><table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td></td><td></td><td>false</td><td>object</td></tr></table></td></tr></table>
errors	Errors	false	array

Export Application

GET /web/api/v2.1/applications/{application_id}/forensics/export/{export_format}

[DEPRECATED] Returns an empty array

Parameters

accountids	optional	List of Account IDs to filter by. Example: "225494730938493804,225494730938493915".
groupids	optional	List of Group IDs to filter by. Example: "225494730938493804,225494730938493915".
siteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

404 - Not found

Gateways

Get Gateways

GET /web/api/v2.1/ranger/gateways

Get the gateways in your deployment that match the filter from a Ranger scan.
Ranger requires a Ranger license.

Parameters

accountids	optional	List of Account IDs to filter by. Example:

		"225494730938493804,225494730938493915".
agentpercentage__between	optional	Percentage of agents of the account in this network calculated as numberOfAgents/totalAgents * 100. Example: "70-80".
agentpercentage__gt	optional	Agent percentage (more than)
agentpercentage__gte	optional	Agent percentage (more than or equal)
agentpercentage__lt	optional	Agent percentage (less than)
agentpercentage__lte	optional	Agent percentage (less than or equal)
allowscan	optional	Do we allow scanning in this network
archived	optional	Archived network
connectedrangers__between	optional	The total of non decommissioned agents in the account. Example: "2-8".
connectedrangers__gt	optional	Total agents (more than)
connectedrangers__gte	optional	Total agents (more than or equal)
connectedrangers__lt	optional	Total agents (less than)
connectedrangers__lte	optional	Total agents (less than or equal)
countonly	optional	If true, only total number of items will be returned, without any of the actual objects.
createdat__between	optional	Date range for creation time (format: <from_timestamp>-<to_timestamp>, inclusive). Example: "1514978890136-1514978650130".
createdat__gt	optional	Gateway created after this timestamp. Example: "2018-02-27T04:49:26.257525Z".
createdat__gte	optional	Gateway created after or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
createdat__lt	optional	Gateway created before this timestamp. Example: "2018-02-27T04:49:26.257525Z".
createdat__lte	optional	Gateway created before or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
cursor	optional	Cursor position returned by the last request. Use to iterate over more than 1000 items. Example: "YWdlbnRfaWQ6NTgwMjkzODE=".
externalip	optional	Search external ip using a CIDR expression or exact IP

externalip__contains	optional	Free-text filter by visible IP (supports multiple values). Example: "192.168.0.1/24,10.1".
icmpscan	optional	ICMP scan enabled
ids	optional	List of gateway ids. Example: "225494730938493804,225494730938493915".
ip	optional	Search ip using a CIDR expression exact IP
ip__contains	optional	Free-text filter by IP Address (supports multiple values). Example: "192.168.0.1/24,10.1".
limit	optional	Limit number of returned items (1-1000). Example: "10".
macaddress	optional	The gateway mac address
macaddress__contains	optional	Free-text filter by mac address (supports multiple values). Example: "aa:ee:b1".
manufacturer	optional	The gateway manufacturer obtained from the mac address
manufacturer__contains	optional	Free-text filter by manufacturer (supports multiple values). Example: "Company".
mdnsscan	optional	MDNS scan enabled
networkname__contains	optional	Free-text filter by network name (supports multiple values). Example: "Network1".
new	optional	True if this is network was first seen some days ago, 3 by default
numberofagents__between	optional	The number of non decommissioned agents in this network. Example: "2-8".
numberofagents__gt	optional	Agent count (more than)
numberofagents__gte	optional	Agent count (more than or equal)
numberofagents__lt	optional	Agent count (less than)
numberofagents__lte	optional	Agent count (less than or equal)
numberofrangers__between	optional	The number of non decommissioned agents in this network. Example: "2-8".
numberofrangers__gt	optional	Ranger count (more than)
numberofrangers__gte	optional	Ranger count (more than or equal)
numberofrangers__lt	optional	Ranger count (less than)
numberofrangers__lte	optional	Ranger count (less than or equal)
query	optional	Free text query

rdnsscan	optional	RDNS scan enabled
scanonlylocalsubnets	optional	Allow remote tasks form this network
siteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".
skip	optional	Skip first number of items (0-1000). To iterate over more than 1000 items, use "cursor". Example: "150".
skipcount	optional	If true, total number of items will not be calculated, which speeds up execution time.
smbscan	optional	SMB scan enabled
snmpscan	optional	SNMP scan enabled
sortby	optional	The column to sort the results by. Example: "id".
sortorder	optional	Sort direction. Example: "asc".
tcpports__contains	optional	Free-text filter by tcp port (supports multiple values). Example: "80,24".
totalagents__between	optional	The total of non decommissioned agents in the account. Example: "2-8".
totalagents__gt	optional	Total agents (more than)
totalagents__gte	optional	Total agents (more than or equal)
totalagents__lt	optional	Total agents (less than)
totalagents__lte	optional	Total agents (less than or equal)
udpports__contains	optional	Free-text filter by udp port (supports multiple values). Example: "137,2002".
updatedat__between	optional	Date range for update time (format: <from_timestamp>-<to_timestamp>, inclusive). Example: "1514978890136-1514978650130".
updatedat__gt	optional	Gateway updated after this timestamp. Example: "2018-02-27T04:49:26.257525Z".
updatedat__gte	optional	Gateway updated after or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
updatedat__lt	optional	Gateway updated before this timestamp. Example: "2018-02-27T04:49:26.257525Z".
updatedat__lte	optional	Gateway updated before or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - Insufficient permissions

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>pagination</td><td>Pagination information</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>totalItems</td><td>Total number of items found matching your query</td><td>true</td><td>integer</td></tr>
<tr><td>nextCursor</td><td>Pass this value as "cursor" on your next request, to get the next page of results (Will be "null" when last page reached)</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountId</td><td>The Account Id</td><td>false</td><td>integer</td></tr>
<tr><td>accountName</td><td>Account name</td><td>false</td><td>string</td></tr>
<tr><td>agentPercentage</td><td>Percentage of agents of the account in this network calculated as</td><td>false</td><td>number</td></tr>
</table>
</td></tr>
</table>

				numberOfAgents/ totalAgents * 100		
			allowScan	Do we allow scanning in this network	false	boolean
			archived	Archived network	false	boolean
			connectedRangers	The number of active rangers	false	integer
			createdAt	Created at	false	string
			discoveryMethod	Discovery method	false	enum
			expiryDate	Date when this network will expire, null if it won't expire	false	string
			externalIp	The gateway external Ip	false	string
			icmpScan	ICMP scan enabled	false	boolean
			id	The gateway id	false	string
			inheritSettings	True if inherited values are taken from account settings	false	boolean
			ip	The gateway local ip	false	string
			macAddress	The gateway mac address	false	string
			manufacturer	The gateway manufacturer obtained from the mac	false	string

	address		
mdnsScan	MDNS scan enabled	false	boolean
multiScanSsdp	Multicast SSDP scan enabled	false	boolean
networkName	The network name	false	string
new	True if this is network was first seen some days ago, 3 by default	false	boolean
numberOfAgents	The number of non decommissioned agents in this network	false	integer
numberOfRangers	The number of rangers in this network	false	integer
rdnsScan	RDNS scan enabled	false	boolean
restrictions	A set of IP addresses that should not be scanned in the specific network	false	

Name	Description	Required	Value
annotation	An optional note with the reason for the restriction	false	string
type		false	enum
values	It will be one IP or one CIDR or two values for a Range	false	string []

scanOnlyLocalSubnets	Allow remote tasks form this network	false	boolean

			siteId: The Site Id; false; integer smbScan: SMB scan enabled; false; boolean snmpScan: SNMP scan enabled; false; boolean tcpPorts: Allowed TCP ports; false; integer [] tcpPortScan: TCP Port scan enabled; false; boolean totalAgents: The total of non decommissioned agents in the account; false; integer udpPorts: Allowed UDP ports; false; integer [] udpPortScan: UDP Port scan enabled; false; boolean
errors	Errors	false	array

Update Gateways

POST /web/api/v2.1/ranger/gateways/update

Change the status of filtered gateways discovered by Ranger. You can set the archived status, whether the network behind the gateway may be scanned by Ranger, and whether Ranger will scan only local networks.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - Insufficient permissions

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>affected</td><td>Number of entities affected by the requested operation</td><td>false</td><td>integer</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>allowScan</td><td>Do we allow scanning in this network</td><td>false</td><td>boolean</td></tr>
<tr><td>archived</td><td>True if we should archive the network, valid for networks that are not allowed to scan only</td><td>false</td><td>boolean</td></tr>
<tr><td>inheritSettings</td><td>True if inherited values are taken from account settings</td><td>false</td><td>boolean</td></tr>
<tr><td>scanOnlyLocalSubnets</td><td>Allow remote tasks form this network</td><td>false</td><td>boolean</td></tr>
</table>
</td></tr>
<tr><td>filter</td><td>Filter</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>agentPercentage__between</td><td>Percentage of agents of the account in this network calculated as numberOfAgents/ totalAgents * 100</td><td>false</td><td>string</td></tr>
<tr><td>agentPercentage__gt</td><td>Agent percentage</td><td>false</td><td>number</td></tr>
</table>
</td></tr>
</table>

				(more than)		
			agentPercentage__gte	Agent percentage (more than or equal)	false	number
			agentPercentage__lt	Agent percentage (less than)	false	number
			agentPercentage__lte	Agent percentage (less than or equal)	false	number
			allowScan	Do we allow scanning in this network	false	string
			archived	Archived network	false	boolean
			connectedRangers__between	The total of non decommissioned agents in the account	false	string
			connectedRangers__gt	Total agents (more than)	false	integer
			connectedRangers__gte	Total agents (more than or equal)	false	integer
			connectedRangers__lt	Total agents (less than)	false	integer
			connectedRangers__lte	Total agents (less than or equal)	false	integer
			createdAt__between	Date range for creation time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			createdAt__g	Gateway	false	string

			t	created after this timestamp		
			createdAt__gte	Gateway created after or at this timestamp	false	string
			createdAt__lt	Gateway created before this timestamp	false	string
			createdAt__lte	Gateway created before or at this timestamp	false	string
			externalIp	Search external ip using a CIDR expression or exact IP	false	string
			externalIp__contains	Free-text filter by visible IP (supports multiple values)	false	string []
			icmpScan	ICMP scan enabled	false	boolean
			ids	List of gateway ids	false	string []
			ip	Search ip using a CIDR expression exact IP	false	string
			ip__contains	Free-text filter by IP Address (supports multiple values)	false	string []

			macAddress	The gateway mac address	false	string
			macAddress__contains	Free-text filter by mac address (supports multiple values)	false	string []
			manufacturer	The gateway manufacturer obtained from the mac address	false	string
			manufacturer__contains	Free-text filter by manufacturer (supports multiple values)	false	string []
			mdnsScan	MDNS scan enabled	false	boolean
			networkName__contains	Free-text filter by network name (supports multiple values)	false	string []
			new	True if this is network was first seen some days ago, 3 by default	false	boolean
			numberOfAgents__between	The number of non decommissioned agents in this network	false	string
			numberOfAgents__gt	Agent count (more than)	false	integer
			numberOfAge	Agent count	false	integer

			nts__gte	(more than or equal)		
			numberOfAgents__lt	Agent count (less than)	false	integer
			numberOfAgents__lte	Agent count (less than or equal)	false	integer
			numberOfRangers__between	The number of non decommissioned agents in this network	false	string
			numberOfRangers__gt	Ranger count (more than)	false	integer
			numberOfRangers__gte	Ranger count (more than or equal)	false	integer
			numberOfRangers__lt	Ranger count (less than)	false	integer
			numberOfRangers__lte	Ranger count (less than or equal)	false	integer
			query	Free text query	false	string
			rdnsScan	RDNS scan enabled	false	boolean
			scanOnlyLocalSubnets	Allow remote tasks form this network	false	boolean
			siteIds	List of Site IDs to filter by	false	string []
			smbScan	SMB scan enabled	false	boolean
			snmpScan	SNMP scan enabled	false	boolean
			tcpPorts__contains	Free-text filter by tcp port	false	integer []

				(supports multiple values)		
			totalAgents__between	The total of non decommissioned agents in the account	false	string
			totalAgents__gt	Total agents (more than)	false	integer
			totalAgents__gte	Total agents (more than or equal)	false	integer
			totalAgents__lt	Total agents (less than)	false	integer
			totalAgents__lte	Total agents (less than or equal)	false	integer
			udpPorts__contains	Free-text filter by udp port (supports multiple values)	false	integer []
			updatedAt__between	Date range for update time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			updatedAt__gt	Gateway updated after this timestamp	false	string
			updatedAt__gte	Gateway updated after or at this timestamp	false	string
			updatedAt__lt	Gateway updated	false	string

				before this timestamp		
			updatedAt__lte	Gateway updated before or at this timestamp	false	string

Update Gateway

PUT /web/api/v2.1/ranger/gateways/{gateway_id}

Change the Ranger scan configuration for a gateway that Ranger discovered

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - Insufficient permissions

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
accountId	The Account Id	false	integer
accountName	Account name	false	string
agentPercentage	Percentage of agents of the account in this network calculated as numberOfAgents/ totalAgents * 100	false	number
allowScan	Do we allow scanning in this network	false	boolean
archived	Archived network	false	boolean
connectedRan	The number	false	integer

			gers	of active rangers		
			createdAt	Created at	false	string
			discoveryMethod	Discovery method	false	enum
			expiryDate	Date when this network will expire, null if it won't expire	false	string
			externalIp	The gateway external Ip	false	string
			icmpScan	ICMP scan enabled	false	boolean
			id	The gateway id	false	string
			inheritSettings	True if inherited values are taken from account settings	false	boolean
			ip	The gateway local ip	false	string
			macAddress	The gateway mac address	false	string
			manufacturer	The gateway manufacturer obtained from the mac address	false	string
			mdnsScan	MDNS scan enabled	false	boolean
			multiScanSsdp	Multicast SSDP scan enabled	false	boolean
			networkName	The network name	false	string
			new	True if this is	false	boolean

				network was first seen some days ago, 3 by default		
			numberOfAgents	The number of non decommissioned agents in this network	false	integer
			numberOfRangers	The number of rangers in this network	false	integer
			rdnsScan	RDNS scan enabled	false	boolean
			restrictions	A set of IP addresses that should not be scanned in the specific network	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>annotation</td><td>An optional note with the reason for the restriction</td><td>false</td><td>string</td></tr><tr><td>type</td><td></td><td>false</td><td>enum</td></tr><tr><td>values</td><td>It will be one IP or one CIDR or two values for a Range</td><td>false</td><td>string []</td></tr></table>
			scanOnlyLocalSubnets	Allow remote tasks form this network	false	boolean
			siteId	The Site Id	false	integer
			smbScan	SMB scan enabled	false	boolean
			snmpScan	SNMP scan enabled	false	boolean
			tcpPorts	Allowed TCP ports	false	integer []
			tcpPortScan	TCP Port scan enabled	false	boolean

			totalAgents: The total of non decommissioned agents in the account — false — integer udpPorts: Allowed UDP ports — false — integer [] udpPortScan: UDP Port scan enabled — false — boolean
errors	Errors	false	array

Body Schema

Name	Description	Required	Value
data	Data	true	

Name	Description	Required	Value
accountId	The Account Id	false	integer
allowScan	Do we allow scanning in this network	false	boolean
archived	Archived network	false	boolean
icmpScan	ICMP scan enabled	false	boolean
inheritSettings	True if inherited values are taken from account settings	false	boolean
mdnsScan	MDNS scan enabled	false	boolean
multiCastSsdpScan	Multicast SSDP scan enabled	false	boolean
networkName	The network name	false	string
rdnsScan	RDNS scan enabled	false	boolean
restrictions	A set of IP addresses that should not be scanned in the specific network	false	

Name	Description	Required	Value
annotation	An optional note with the reason for the restriction	false	string
type		false	enum
values	It will be one IP or one CIDR or two	false	string []

							values for a Range		
			scanOnlyLocalSubnets	Can we scan remote networks from this gateway	false	boolean			
			siteId	The Site Id	false	integer			
			smbScan	SMB scan enabled	false	boolean			
			snmpScan	SNMP scan enabled	false	boolean			
			tcpPorts	Allowed TCP ports	false	integer []			
			tcpPortScan	TCP Port scan enabled	false	boolean			
			udpPorts	Allowed UDP ports	false	integer []			
			udpPortScan	UDP Port scan enabled	false	boolean			

Groups

Get Groups

GET /web/api/v2.1/groups

Get data of groups that match the filter. Best practice: use as narrow a filter as you can. The data can be quite long for many groups. The response returns the ID of each group, which you can use in other commands.

> **BEST PRACTICE**
> use as narrow a filter as you can. The data can be quite long for many groups. The response returns the ID of each group, which you can use in other commands.

Parameters

accountids	optional	List of Account IDs to filter by. Example: "225494730938493804,225494730938493915".
countonly	optional	If true, only total number of items will be returned, without any of the actual objects.
cursor	optional	Cursor position returned by the last request. Use to iterate over more than 1000 items. Example: "YWdlbnRfaWQ6NTgwMjkzODE=".
description	optional	The description for the Group
groupids	optional	List of Group IDs to filter by. Example: "225494730938493804,225494730938493915".
id	optional	Id. Example: "225494730938493804".
isdefault	optional	Is this the default group?
limit	optional	Limit number of returned items (1-300). Example: "10".
name	optional	Name
query	optional	Free text search on fields name, description
rank	optional	The rank sets the priority of a dynamic group over others. Example: "1".
registrationtoken	optional	Registration token. Example: "eyJ1cmwiOiAiaHR0cHM6Ly9jb25zb2xlLnNlbnRpbmVsb25lLm5ldCIs

		ICJzaXRlX2tleSI6ICIwNzhkYjliMWUyOTA1Y2NhIn0=".
siteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".
skip	optional	Skip first number of items (0-1000). To iterate over more than 1000 items, use "cursor". Example: "150".
skipcount	optional	If true, total number of items will not be calculated, which speeds up execution time.
sortby	optional	The column to sort the results by. Example: "id".
sortorder	optional	Sort direction. Example: "asc".
type	optional	Group type. Example: "static".
types	optional	A list of Group types. Example: "static".
updatedat__gt	optional	Updated at greater than. Example: "2018-02-27T04:49:26.257525Z".
updatedat__gte	optional	Updated at greater or equal than. Example: "2018-02-27T04:49:26.257525Z".
updatedat__lt	optional	Updated at lesser than. Example: "2018-02-27T04:49:26.257525Z".
updatedat__lte	optional	Updated at lesser or equal than. Example: "2018-02-27T04:49:26.257525Z".

Response Messages

200 - Data retrieved successfully

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
pagination	Pagination information	true	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>totalItems</td><td>Total number of items found matching your query</td><td>true</td><td>integer</td></tr></table>

			nextCursor: Pass this value as "cursor" on your next request, to get the next page of results (Will be "null" when last page reached) — false — string
data	Response data	false	

Name	Description	Required	Value
createdAt	Timestamp of group creation	false	string
creator	The user that created the group	false	string
creatorId	The ID of the user that created the group	false	string
description	The user-defined description for the Group	false	string
filterId	If the group is dynamic id of the filter which is used to associate agents	false	string
filterName	If the group is dynamic the name of the filter which is used to associate agents	false	string
id	Id	false	string

			inherits: True if the policy is inherited from Site, False if the group has its own edited policy — false — boolean isDefault: True only for the default group of the Site — false — boolean name: Name — false — string rank: The rank sets the priority of a dynamic group over others — false — integer registrationToken: [DEPRECATED] token generation in dedicated endpoint - /groups/<group_id>/token — false — siteId: The id of the site this group is part of — false — string totalAgents: Count of agents in the group — false — integer type: Group type — false — enum updatedAt: Timestamp of last update — false — string
errors	Errors	false	array

Create Group

POST /web/api/v2.1/groups

Create a new group. You must create the Group in a Site (run "sites" to get the Site ID) for which you have permissions. If you create a dynamic Group, you must have the ID of a filter saved in the Site (run "filters?siteIds=<id from sites>").

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - Insufficient permissions

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
createdAt	Timestamp of group creation	false	string
creator	The user that created the group	false	string
creatorId	The ID of the user that created the group	false	string
description	The user-defined description for the Group	false	string
filterId	If the group is dynamic id of the filter which is used	false	string

			to associate agents		
			id	Id	false	string
			isDefault	True only for the default group of the Site	false	boolean
			name	Name	false	string
			rank	The rank sets the priority of a dynamic group over others	false	integer
			registrationToken	[DEPRECATED] token generation in dedicated endpoint - /groups/<group_id>/token	false	
			siteId	The id of the site this group is part of	false	string
			type	Group type	false	enum
			updatedAt	Timestamp of last update	false	string
errors	Errors	false	array			

Body Schema

Name	Description	Required	Value
data	Data	true	

Name	Description	Required	Value
inherits	True to inherit from site policy.	true	boolean
name	Name	true	string
siteId	The site this group should be part of	true	string
description	The user-defined description for the Group	false	string
filterId	If supplied this group will be dynamic using the filter to associate agents.	false	string
isDefault	Obsolete for POST, always false	false	boolean
policy	The group policy, it is required only if inherits is False, ignored else.	false	

Name	Description	Required	Value
agentLoggingOn	True if logging is enabled in the agent	false	boolean
agentNotification	[DEPRECATED] Show end point notification on suspicious.Replaced by 'show_suspicious' in the	false	boolean

							agent UI section	
						agentUi	Agent ui	false

Name	Description	Required	Value
agentUiOn	Agent ui on	false	boolean
contactCompany	Contact company	false	string
contactDirectMessage	Contact direct message	false	string
contactEmail	Contact email	false	string
contactFreeText	Contact free text	false	string
contactOther	Contact other	false	string
contactPhoneNumber	Contact phone number	false	string
contactSupportWebsite	Contact support website	false	string
devicePopUpNotifications	Device pop up notifications	false	boolean
maxEventAgeDays	Max event age days	false	integer
showAgentWarnings	Show agent warnings	false	boolean
showDeviceTab	Show device tab	false	boolean
showQuarantineTab	Show quarantine tab	false	boolean
showSupport	Show support	false	boolean
showSuspicious	Show suspicious	false	boolean
threatPopUpNotifications	Threat pop up notifications	false	boolean

						agentUiOn	[DEPRECATED] Show/hide Agent UI. Moved inside the agent UI section	false	boolean
						allowRemoteShell	True if Remote Shell is enabled for the scope	false	boolean
						antiTamperingOn	Anti tampering on/off	false	boolean
						autoDecommissionDays	Automatic decommission period in days	false	integer
						autoDecommissionOn	Auto decommission on	false	boolean
						autoFileUpload	Automatic file upload configuration	false	

Name	Description	Required	Value
enabled	Automatic file upload on/off	false	boolean
includeBenignFiles	Upload benign files	false	boolean
maxDailyFileUpload	Maximum size (MB) to upload daily	false	integer
maxDailyFileUploadLimit	Limit for the maximum size (MB) to upload daily	false	integer
maxFileSize	Maximum file size (MB) to upload	false	integer
maxFileSizeLimit	Limit for the maximum file size (MB) to upload	false	integer

										maxLocalDiskUsage	Maximum local disk usage (MB) for uploaded files	false	integer		
										maxLocalDiskUsageLimit	Limit for the maximum local disk usage (MB) for uploaded files	false	integer		
							autoImmuneOn	Automatic immune on/off - this value must be true since all policies are immune by default	false	boolean					
							autoMitigationAction	Default action for auto mitigation	false	string					
							cloudValidationOn	Cloud validation on	false						
							createdAt	Timestamp of policy creation	false	string					
							driverBlocking	Suspicious driver blocking engine on/off	false	boolean					
							dvAttributesPerEventType	The DV attributes	false	Name	Description	Required	Value		
										autoInstallBrowserExtensions	Auto install browser extensions	false	Name	D	
													autoInstallBrowserExtensions	Au br ex	
										behavioralIndicators	Behavioral indicators	false	Name	D	

| | | |

												riverLoad
									file	File event	false	Name dvEventTypeFileCreation dvEventTypeFileDeletion dvEventTypeFileModification dvEventTypeFileRename fullDiskScan
									ip	Network event - IP	false	Name dvEventTypeIpConnect dvEventTypeIpListen
									login	User login/ logout event	false	Name dvEventTypeLoginLoggedIn dvEventTypeLoginLoggedOut
									namedPipe	Named Pipe	false	Name dvEventTypeNamedPipeConnection dvEventTypeNamedPipeCreation
									namedPipeExtended	Named Pipe Extended	false	Name namedPipeEx

														tended
									process	Process event	false			Name
														dvEventTypeProcessCreation
														dvEventTypeProcessExit
														dvEventTypeProcessModification
									registry	Registry event	false			Name
														dvEventTypeRegistryKeyCreated
														dvEventTypeRegistryKeyDelete
														dvEventTypeRegistryKeyExport
														dvEventTypeRegistryKeyImport
														dvEventTypeRegistryKeyRename
														dvEventTypeRegistryKeySecurityChanged
														dvEventTypeRegistryValueCreated
														dvEventTypeRegistryValueD

| | | |

| | | |

									d	forensics is enabled			
									macosProfileId	The profile id for the macos forensics	false	string	
									macosProfileName	The profile name for the macos forensics	false	string	
									windowsEnabled	True if windows forensics is enabled	false	boolean	
									windowsProfileId	The profile id for the windows forensics	false	string	
									windowsProfileName	The profile name for the windows forensics	false	string	
							identityEndpointReporting	Endpoint reporting level	false	enum			
							identityOn	Identity module on/off	false	boolean			
							identityReportInterval	Identity telemetry report interval in minutes	false	integer			
							identityThrottlingInterval	Identity duplicate command consolidation interval in minutes	false	integer			
							identityUpdateInterval	Identity update	false	integer			

							interval in minutes	
						inheritedFrom	Indicates the parent scope from which this policy is inherited, or 'null' if it is not inherited (modified specifically for the current scope).	false	enum
						ioc	True if ioc is enabled	false	boolean
						iocAttributes	The Ioc attributes	false	

Name	Description	Required	Value
autoInstallBrowserExtensions	Update auto install browser extensions	false	boolean
behavioralIndicators	Update behavioral indicators	false	boolean
commandScripts	Update command scripts	false	boolean
crossProcess	Update cross process	false	boolean
dataMasking	Update data masking	false	boolean
dllModuleLoad	Update DLL module load	false	boolean
dns	Network event - DNS	false	boolean
driver	Driver	false	boolean
fds	Full disk scan	false	boolean
file	File event	false	boolean

									ip	Network event - IP	false	boolean	
									login	User login/ logout event	false	boolean	
									namedPipe	Named Pipe	false	boolean	
									namedPipeExtended	Named Pipe Extended	false	boolean	
									process	Process creation event	false	boolean	
									registry	Registry event	false	boolean	
									scheduledTask	Scheduled task event	false	boolean	
									smartFileMonitoring	Smart file monitoring	false	boolean	
									url	Ioc URI	false	boolean	
									windowsEventLogs	Windows Event Log	false	boolean	
									windowsEventLogsExtended	Windows Event Log Extended	false	boolean	
							iocSupported	Ioc supported for the scope	false	boolean			
							isDefault	True if this is the tenant policy	false	boolean			
							isDvPolicyPerEventType	FE indication as to how to display DV policy	false	boolean			
							mitigationMode	Mitigation modes	false	enum			
							mitigationModeSuspicious	Mitigation mode	false	enum			
							monitorOnExecute	Monitor on execute on/	false	boolean			

							off	
						monitorOnWrite	Monitor on write	false	boolean
						networkQuarantineOn	Network quarantine on	false	boolean
						remoteOpsForensics	Remote ops forensics configuration	false	

Name	Description	Required	Value
cpuLimit	CPU resources limit for collection process	false	integer
enabled	Enabled	false	boolean
maximumDailyUpload	Maximum size to upload daily	false	integer
maximumDailyUploadLimit	Limit for the maximum size to upload daily	false	integer
maximumFileSizeUpload	Maximum size for single file	false	integer
maximumFileSizeUploadLimit	Limit for the maximum file size to upload	false	integer
parsedArtifactsDestination	Default destination of parsed artifacts	false	enum

remoteScriptOrchestration	Remote script orchestration upload limits configuration	false	

Name	Description	Required	Value
alwaysUploadStreamToCloud	Always upload streams to cloud	false	boolean
maxDailyFileDownload	Maximum size (MB) to download daily	false	integer

									maxDailyFileDownloadLimit	Limit for the maximum size (MB) to download daily	false	integer	
									maxDailyFileUpload	Maximum size (MB) to upload daily	false	integer	
									maxDailyFileUploadLimit	Limit for the maximum size (MB) to upload daily	false	integer	
									maxFileSize	Maximum size in bytes for single file	false	integer	
									maxFileSizeLimit	Limit for the maximum file size (MB) to upload	false	integer	
									maxLocalPackageDiskUsage	Maximum local disk usage (MB) for packages	false	integer	
									maxLocalPackageDiskUsageLimit	Limit for the maximum local disk usage (MB) for packages	false	integer	
							removeMacros	Determines if macros should be removed from macro threats	false	boolean			
							researchOn	Share data with SentinelOne	false	boolean			
							scanNewAgents	If True initiate full disk scan upon first registration	false	boolean			

						signedDriverBlockingOn	Suspicious signed driver blocking on/off	false	boolean
						snapshotsOn	True if snapshots are enabled	false	boolean
						unsignedDriverBlockingOn	Suspicious unsigned driver blocking on/off	false	boolean
						updatedAt	Time of the last update to the policy	false	string
						userFullName	The user that created the policy	false	string
						userId	The user id	false	string
			rank	Obsolete for post - The rank of the group	false	integer			
			source	Obsolete - Always MGMT	false	string			
			type	Type of Group: Static, Dynamic, or Pinned	false	enum			

Regenerate Group Token

PUT /web/api/v2.1/groups/{group_id}/regenerate-key

Get a new Group Token for a static Group. This command requires the Group ID ("groups") and you must have permissions for the Group. If you run this command on a dynamic Group, it ends in an error. If you use the API in scripts to add new endpoints with a Group Token rather than a Site Token, be aware that you must update the token value in your scripts.

Response Messages

200 - Success

401 - Unauthorized access - please sign in and retry.

403 - No permission for regenerating a key.

404 - Group not found

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>registrationToken</td><td>Registration token</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Delete Group

DELETE /web/api/v2.1/groups/{group_id}

Delete a Group given by the required Group ID (run "groups"). If there are Agents in the Group, and the Group is dynamic, the next dynamic Groups will collect matching Agents, and unmatched Agents will go to the Default Group. If this is a static Group with Agents, all the Agents will go to the Default Group. (Agents always go to matching dynamic Groups. If a static Group holds Agents, there are no matching dynamic Groups.)

Response Messages

200 - Success

401 - Unauthorized access - please sign in and retry.

404 - Group not found.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>success</td><td>Indicates a successful operation</td><td>false</td><td>boolean</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Update Group

PUT /web/api/v2.1/groups/{group_id}

Change properties of a Group specified by its ID (run "groups"). The body of the request holds all the properties of a Group. You must have access permissions on the Site. Note: iocAttributes refers to Deep Visibility. If you do not have a Complete SKU, you can remove this set.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - Insufficient permissions.

404 - Group not found.

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
createdAt	Timestamp of group creation	false	string
creator	The user that created the group	false	string
creatorId	The ID of the user that created the group	false	string
description	The user-defined description for the Group	false	string
filterId	If the group is dynamic id of	false	string

			the filter which is used to associate agents		
			id	Id	false	string
			isDefault	True only for the default group of the Site	false	boolean
			name	Name	false	string
			rank	The rank sets the priority of a dynamic group over others	false	integer
			registrationToken	[DEPRECATED] token generation in dedicated endpoint - /groups/<group_id>/token	false	
			siteId	The id of the site this group is part of	false	string
			type	Group type	false	enum
			updatedAt	Timestamp of last update	false	string
errors	Errors	false	array			

Body Schema

Name	Description	Required	Value
data	Data	false	

Name	Description	Required	Value
description	The user-defined description for the Group	false	string
filterId	If supplied this group will be dynamic using the filter to associate agents.	false	string
id	Id	false	string
inherits	True to inherit from Site Policy.	false	boolean
isDefault	Obsolete for POST, always false	false	boolean
name	Name	false	string
policy	The group policy, it is required only if inherits is False, ignored else.	false	

Name	Description	Required	Value
agentLoggingOn	True if logging is enabled in the agent	false	boolean
agentNotification	[DEPRECATED] Show end point notification on suspicious.Replaced by 'show_suspicious' in the agent UI section	false	boolean

						agentUi	Agent ui	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>agentUiOn</td><td>Agent ui on</td><td>false</td><td>boolean</td></tr><tr><td>contactCompany</td><td>Contact company</td><td>false</td><td>string</td></tr><tr><td>contactDirectMessage</td><td>Contact direct message</td><td>false</td><td>string</td></tr><tr><td>contactEmail</td><td>Contact email</td><td>false</td><td>string</td></tr><tr><td>contactFreeText</td><td>Contact free text</td><td>false</td><td>string</td></tr><tr><td>contactOther</td><td>Contact other</td><td>false</td><td>string</td></tr><tr><td>contactPhoneNumber</td><td>Contact phone number</td><td>false</td><td>string</td></tr><tr><td>contactSupportWebsite</td><td>Contact support website</td><td>false</td><td>string</td></tr><tr><td>devicePopUpNotifications</td><td>Device pop up notifications</td><td>false</td><td>boolean</td></tr><tr><td>maxEventAgeDays</td><td>Max event age days</td><td>false</td><td>integer</td></tr><tr><td>showAgentWarnings</td><td>Show agent warnings</td><td>false</td><td>boolean</td></tr><tr><td>showDeviceTab</td><td>Show device tab</td><td>false</td><td>boolean</td></tr><tr><td>showQuarantineTab</td><td>Show quarantine tab</td><td>false</td><td>boolean</td></tr><tr><td>showSupport</td><td>Show support</td><td>false</td><td>boolean</td></tr><tr><td>showSuspicious</td><td>Show suspicious</td><td>false</td><td>boolean</td></tr><tr><td>threatPopUpNotifications</td><td>Threat pop up notifications</td><td>false</td><td>boolean</td></tr></table>
						agentUiOn	[DEPRECATED] Show/hide	false	boolean

						Agent UI. Moved inside the agent UI section		
					allowRemoteShell	True if Remote Shell is enabled for the scope	false	boolean
					antiTamperingOn	Anti tampering on/off	false	boolean
					autoDecommissionDays	Automatic decommission period in days	false	integer
					autoDecommissionOn	Auto decommission on	false	boolean
					autoFileUpload	Automatic file upload configuration	false	

Name	Description	Required	Value
enabled	Automatic file upload on/off	false	boolean
includeBenignFiles	Upload benign files	false	boolean
maxDailyFileUpload	Maximum size (MB) to upload daily	false	integer
maxDailyFileUploadLimit	Limit for the maximum size (MB) to upload daily	false	integer
maxFileSize	Maximum file size (MB) to upload	false	integer
maxFileSizeLimit	Limit for the maximum file size (MB) to upload	false	integer
maxLocalDis	Maximum	false	integer

									kUsage: local disk usage (MB) for uploaded files maxLocalDiskUsageLimit: Limit for the maximum local disk usage (MB) for uploaded files (false, integer)
						autoImmuneOn	Automatic immune on/off - this value must be true since all policies are immune by default	false	boolean
						autoMitigationAction	Default action for auto mitigation	false	string
						cloudValidationOn	Cloud validation on	false	
						createdAt	Timestamp of policy creation	false	string
						driverBlocking	Suspicious driver blocking engine on/off	false	boolean
						dvAttributesPerEventType	The DV attributes	false	Name: autoInstallBrowserExtensions — Description: Auto install browser extensions — Required: false — Value: Name: autoInstallBrowserExtensions Name: behavioralIndicators — Description: Behavioral indicators event — Required: false — Value: Name: dvEventTypeBe

| | | |

										file	File event	false	Name	D	
													dvEventTypeFileCreation	Fil Ev	
													dvEventTypeFileDeletion	Fil Ev	
													dvEventTypeFileModification	Fil M Ev	
													dvEventTypeFileRename	Fil Ev	
													fullDiskScan	Fil Ev	
										ip	Network event - IP	false	Name	D	
													dvEventTypeIpConnect	IP Ev	
													dvEventTypeIpListen	IP Ev	
										login	User login/ logout event	false	Name	D	
													dvEventTypeLoginLoggedIn	Us Ev	
													dvEventTypeLoginLoggedOut	Us Ev	
										namedPipe	Named Pipe	false	Name	D	
													dvEventTypeNamedPipeConnection	Na Co Ev	
													dvEventTypeNamedPipeCreation	Na Cr Ev	
										namedPipeExtended	Named Pipe Extended	false	Name	D	
													namedPipeExtended	Na Co Ex	

													Ev
									process	Process event	false	Name dvEventTypeProcessCreation dvEventTypeProcessExit dvEventTypeProcessModification	De Pr Cr Ev Pr Ev Pr Te Ev
									registry	Registry event	false	Name dvEventTypeRegistryKeyCreated dvEventTypeRegistryKeyDelete dvEventTypeRegistryKeyExport dvEventTypeRegistryKeyImport dvEventTypeRegistryKeyRename dvEventTypeRegistryKeySecurityChanged dvEventTypeRegistryValueCreated dvEventTypeRegistryValueDeleted	De Re Cr Ev Re De Ty Re Ex Ty Re Im Ty Re Re Ev Re Se Ch Ev Re Va Ev Re Va De Ev

													dvEventTypeRegistryValueModified	Re Va M Ev
									scheduledTask	Scheduled task event	false		Name	De
													dvEventTypeScheduledTaskDelete	Sc Ta Ev
													dvEventTypeScheduledTaskRegister	Sc Ta Ev
													dvEventTypeScheduledTaskStart	Sc Ta Ev
													dvEventTypeScheduledTaskTrigger	Sc Ta Ev
													dvEventTypeScheduledTaskUpdate	Sc Ta Ev
									smartFileMonitoring	Smart file monitoring	false		Name	De
													smartFileMonitoring	Sm mo
									url	URL Actions event	false		Name	De
													dvEventTypeUrl	UR ev
									windowsEventLogs	Windows Event Log	false		Name	De
													dvEventTypeWindowsEventLogCreation	W Ev Cr Ev
									windowsEventLogsExtended	Windows Event Log Extended	false		Name	De
													windowsEventLogsExtende	W Ev

												d	Ex Ev
						engines	The engines statuses	false					

Name	Description	Required	Value
applicationControl	application control	false	enum
dataFiles	data files	false	enum
executables	executables	false	enum
exploits	exploits	false	enum
lateralMovement	lateral movement	false	enum
penetration	penetration	false	enum
preExecution	on-write	false	enum
preExecutionSuspicious	pre execution suspicious	false	enum
pup	potentially unwanted applications (PUP)	false	enum
remoteShell	remote shell	false	enum
reputation	reputation	false	enum

forensicsAutoTriggering	Forensics auto triggering configuration	false	

Name	Description	Required	Value
linuxEnabled	True if linux forensics is enabled	false	boolean
linuxProfileId	The profile id for the linux forensics	false	string
linuxProfileName	The profile name for the linux forensics	false	string
macosEnabled	True if macos forensics is enabled	false	boolean

										macosProfileId	The profile id for the macos forensics	false	string	
										macosProfileName	The profile name for the macos forensics	false	string	
										windowsEnabled	True if windows forensics is enabled	false	boolean	
										windowsProfileId	The profile id for the windows forensics	false	string	
										windowsProfileName	The profile name for the windows forensics	false	string	
							identityEndpointReporting	Endpoint reporting level	false	enum				
							identityOn	Identity module on/off	false	boolean				
							identityReportInterval	Identity telemetry report interval in minutes	false	integer				
							identityThrottlingInterval	Identity duplicate command consolidation interval in minutes	false	integer				
							identityUpdateInterval	Identity update interval in minutes	false	integer				

						inheritedFrom	Indicates the parent scope from which this policy is inherited, or 'null' if it is not inherited (modified specifically for the current scope).	false	enum
						ioc	True if ioc is enabled	false	boolean
						iocAttributes	The Ioc attributes	false	

Name	Description	Required	Value
autoInstallBrowserExtensions	Update auto install browser extensions	false	boolean
behavioralIndicators	Update behavioral indicators	false	boolean
commandScripts	Update command scripts	false	boolean
crossProcess	Update cross process	false	boolean
dataMasking	Update data masking	false	boolean
dllModuleLoad	Update DLL module load	false	boolean
dns	Network event - DNS	false	boolean
driver	Driver	false	boolean
fds	Full disk scan	false	boolean
file	File event	false	boolean
ip	Network event - IP	false	boolean

									login	User login/ logout event	false	boolean	
									namedPipe	Named Pipe	false	boolean	
									namedPipeExtended	Named Pipe Extended	false	boolean	
									process	Process creation event	false	boolean	
									registry	Registry event	false	boolean	
									scheduledTask	Scheduled task event	false	boolean	
									smartFileMonitoring	Smart file monitoring	false	boolean	
									url	Ioc URI	false	boolean	
									windowsEventLogs	Windows Event Log	false	boolean	
									windowsEventLogsExtended	Windows Event Log Extended	false	boolean	
							iocSupported	Ioc supported for the scope	false	boolean			
							isDefault	True if this is the tenant policy	false	boolean			
							isDvPolicyPerEventType	FE indication as to how to display DV policy	false	boolean			
							mitigationMode	Mitigation modes	false	enum			
							mitigationModeSuspicious	Mitigation mode	false	enum			
							monitorOnExecute	Monitor on execute on/ off	false	boolean			
							monitorOnWr	Monitor on	false	boolean			

						ite	write		
						networkQuarantineOn	Network quarantine on	false	boolean
						remoteOpsForensics	Remote ops forensics configuration	false	

Name	Description	Required	Value
cpuLimit	CPU resources limit for collection process	false	integer
enabled	Enabled	false	boolean
maximumDailyUpload	Maximum size to upload daily	false	integer
maximumDailyUploadLimit	Limit for the maximum size to upload daily	false	integer
maximumFileSizeUpload	Maximum size for single file	false	integer
maximumFileSizeUploadLimit	Limit for the maximum file size to upload	false	integer
parsedArtifactsDestination	Default destination of parsed artifacts	false	enum

remoteScriptOrchestration	Remote script orchestration upload limits configuration	false	

Name	Description	Required	Value
alwaysUploadStreamToCloud	Always upload streams to cloud	false	boolean
maxDailyFileDownload	Maximum size (MB) to download daily	false	integer
maxDailyFileDownloadLim	Limit for the maximum	false	integer

									it	size (MB) to download daily			
									maxDailyFileUpload	Maximum size (MB) to upload daily	false	integer	
									maxDailyFileUploadLimit	Limit for the maximum size (MB) to upload daily	false	integer	
									maxFileSize	Maximum size in bytes for single file	false	integer	
									maxFileSizeLimit	Limit for the maximum file size (MB) to upload	false	integer	
									maxLocalPackageDiskUsage	Maximum local disk usage (MB) for packages	false	integer	
									maxLocalPackageDiskUsageLimit	Limit for the maximum local disk usage (MB) for packages	false	integer	
							removeMacros	Determines if macros should be removed from macro threats	false	boolean			
							researchOn	Share data with SentinelOne	false	boolean			
							scanNewAgents	If True initiate full disk scan upon first registration	false	boolean			
							signedDriver	Suspicious	false	boolean			

						BlockingOn	signed driver blocking on/off		
						snapshotsOn	True if snapshots are enabled	false	boolean
						unsignedDriverBlockingOn	Suspicious unsigned driver blocking on/off	false	boolean
						updatedAt	Time of the last update to the policy	false	string
						userFullName	The user that created the policy	false	string
						userId	The user id	false	string
			rank	Obsolete for post - The rank of the group	false	integer			
			siteId	The site this group should be part of	false	string			
			source	Obsolete	false	string			

Get Group by ID

GET /web/api/v2.1/groups/{group_id}

Get data of a given Group. To get a Group ID, run "groups". This command responds with the ID of the Site of the Group, Group name, type (dynamic or static), and similar data. Your username must permissions for the Site.

Response Messages

200 - Success

401 - Unauthorized access - please sign in and retry.

403 - Insufficient permissions

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
createdAt	Timestamp of group creation	false	string
creator	The user that created the group	false	string
creatorId	The ID of the user that created the group	false	string
description	The user-defined description for the Group	false	string
filterId	If the group is dynamic id of the filter which is used to associate agents	false	string

			id | Id | false | string isDefault | True only for the default group of the Site | false | boolean name | Name | false | string rank | The rank sets the priority of a dynamic group over others | false | integer registrationToken | [DEPRECATED] token generation in dedicated endpoint - /groups/<group_id>/token | false | siteId | The id of the site this group is part of | false | string type | Group type | false | enum updatedAt | Timestamp of last update | false | string
errors	Errors	false	array

Revert Policy

PUT /web/api/v2.1/groups/{group_id}/revert-policy

A Group can have a policy that is different from its Site policy. Use this command to revert the changes on the Group policy to inherit the Site policy. Your user must have permissions on the Site.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - Insufficient permissions

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>success</td><td>Indicates a successful operation</td><td>false</td><td>boolean</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

Name	Description	Required	Value
data	Data	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>id</td><td>Id</td><td>false</td><td>string</td></tr></table>

Move Agents

PUT /web/api/v2.1/groups/{group_id}/move-agents

Move Agents that match the filter to a Group. The Group ID (run "groups") is required and there can be only one. This will move the matched Agents that are in the same Site as the given Group.

Response Messages

204 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - Insufficient permissions

409 - Conflict

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>filter</td><td>Specification of which agents should be moved</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>activeThreats</td><td>Include Agents with this amount of active threats</td><td>false</td><td>integer</td></tr>
<tr><td>activeThreats__gt</td><td>Include Agents with at least this amount of active threats</td><td>false</td><td>integer</td></tr>
<tr><td>adComputerMember__contains</td><td>Free-text filter by Active</td><td>false</td><td>string []</td></tr>
</table>
</td></tr>
</table>

				Directory computer groups string (supports multiple values)		
			adComputerName__contains	Free-text filter by Active Directory computer name string (supports multiple values)	false	string []
			adComputerQuery__contains	Free-text filter by Active Directory computer name or its groups (supports multiple values)	false	string []
			adQuery	An Active Directory query string	false	string
			adQuery__contains	Free-text filter by Active Directory string (supports multiple values)	false	string []
			adUserMember__contains	Free-text filter by Active Directory user groups string (supports multiple	false	string []

				values)		
			adUserName__contains	Free-text filter by Active Directory username string (supports multiple values)	false	string []
			adUserQuery__contains	Free-text filter by Active Directory computer name or its groups (supports multiple values)	false	string []
			agentIds	(DEPRECATED; use 'ids' instead) List of agent ids to move to a new group	false	string []
			agentNamespace__contains	Free-text filter by agent namespace (supports multiple values)	false	string []
			agentPodName__contains	Free-text filter by agent pod name (supports multiple values)	false	string []
			agentVersion__between	Version range for agent version (format: <from_versio	false	string

				n>-<to_version>, inclusive)		
			agentVersion__gt	Agents versions greater than given version	false	string
			agentVersion__gte	Agents versions greater than or equal to given version	false	string
			agentVersion__lt	Agents versions less than given version	false	string
			agentVersion__lte	Agents versions less than or equal to given version	false	string
			agentVersions	Agent versions to include	false	string []
			agentVersionsNin	Agent versions not to include	false	string []
			appsVulnerabilityStatuses	Apps vulnerability status in	false	string []
			appsVulnerabilityStatusesNin	Apps vulnerability status nin	false	string []
			awsRole__contains	Free-text filter by aws role(supports multiple values)	false	string []
			awsSecurityGroups__contains	Free-text filter by aws securityGroup	false	string []

				s(supports multiple values)		
			awsSubnetIds__contains	Free-text filter by aws subnet ids (supports multiple values)	false	string []
			azureResourceGroup__contains	Free-text filter by azure resource group(supports multiple values)	false	string []
			cloudAccount__contains	Free-text filter by cloud account (supports multiple values)	false	string []
			cloudImage__contains	Free-text filter by cloud image (supports multiple values)	false	string []
			cloudInstanceId__contains	Free-text filter by cloud instance id(supports multiple values)	false	string []
			cloudInstanceSize__contains	Free-text filter by cloud instance size(supports multiple values)	false	string []
			cloudLocation__contains	Free-text filter by cloud location (supports	false	string []

				multiple values)		
			cloudNetwork__contains	Free-text filter by cloud network (supports multiple values)	false	string []
			cloudProvider	Agents from which cloud provider	false	string []
			cloudProvideRNin	Exclude Agents from these cloud provider	false	string []
			cloudTags__contains	Free-text filter by cloud tags (supports multiple values)	false	string []
			clusterName__contains	Free-text filter by cluster name (supports multiple values)	false	string []
			computerName	Computer name	false	string
			computerName__contains	Free-text filter by computer name (supports multiple values)	false	string []
			computerName__like	Match computer name partially (substring)	false	string
			consoleMigra	Migration	false	string []

			tionStatuses	status in		
			consoleMigrationStatusesNin	Migration status nin	false	string []
			coreCount__between	Possible number of CPU cores (inclusive)	false	string
			coreCount__gt	CPU cores (more than)	false	integer
			coreCount__gte	CPU cores (more than or equal)	false	integer
			coreCount__lt	CPU cores (less than)	false	integer
			coreCount__lte	CPU cores (less than or equal)	false	integer
			cpuCount__between	Possible number of CPU cores (inclusive)	false	string
			cpuCount__gt	Number of CPUs (more than)	false	integer
			cpuCount__gte	Number of CPUs (more than or equal)	false	integer
			cpuCount__lt	Number of CPUs (less than)	false	integer
			cpuCount__lte	Number of CPUs (less than or equal)	false	integer
			cpuId__contains	Free-text filter by CPU name (supports multiple values)	false	string []

			createdAt__between	Date range for creation time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			createdAt__gt	Agents created after this timestamp	false	string
			createdAt__gte	Agents created after or at this timestamp	false	string
			createdAt__lt	Agents created before this timestamp	false	string
			createdAt__lte	Agents created before or at this timestamp	false	string
			csvFilterId	The ID of the CSV file to filter by	false	string
			decommissionedAt__between	Date range for decommission time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			decommissionedAt__gt	Agents decommissioned after this timestamp	false	string
			decommissionedAt__gte	Agents decommissioned after or at	false	string

				this timestamp		
			decommissionedAt__lt	Agents decommissioned before this timestamp	false	string
			decommissionedAt__lte	Agents decommissioned before this timestamp	false	string
			domains	Included network domains	false	string []
			domainsNin	Not included network domains	false	string []
			encryptedApplications	Disk encryption status	false	boolean
			externalId__contains	Free-text filter by external ID (Customer ID)	false	string []
			externalIp__contains	Free-text filter by visible IP (supports multiple values)	false	string []
			filteredGroupIds	List of Group IDs to filter by	false	string []
			filteredSiteIds	List of Site IDs to filter by	false	string []
			filterId	Include all Agents matching this saved filter	false	string
			firewallEnabled	The agents supports	false	boolean []

				Firewall Control and it is enabled for the agent's group		
			gatewayIp	Gateway ip	false	string
			gcpServiceAccount__contains	Free-text filter by gcp service account (supports multiple values)	false	string []
			groupIds	List of Group IDs to filter by	false	string []
			hasContainerizedWorkload	Include only Agents protecting containerized workloads	false	boolean
			hasLocalConfiguration	Agent has a local configuration set	false	boolean
			hasTags	Include only Agents that have any tags assigned if True, or none if False	false	boolean
			ids	A list of Agent IDs	false	string []
			infected	Include only Agents with at least one active threat	false	boolean
			installerTypes	Include only Agents installed with these package	false	string []

				types		
			installerTypesNin	Exclude Agents installed with these package types	false	string []
			isActive	Include only active Agents	false	boolean
			isDecommissioned	Include active, decommissioned or both	false	boolean []
			isPendingUninstall	Include only Agents with pending uninstall requests	false	boolean
			isUninstalled	Include installed, uninstalled or both	false	boolean []
			isUpToDate	Include only Agents with updated software	false	boolean
			k8sNodeLabels__contains	Free-text filter by K8s node labels (supports multiple values)	false	string []
			k8sNodeName__contains	Free-text filter by K8s node name (supports multiple values)	false	string []
			k8sType__contains	Free-text filter by K8s type(supports multiple	false	string []

				values)		
			k8sVersion__contains	Free-text filter by K8s version (supports multiple values)	false	string []
			lastActiveDate__between	Date range for last active date(format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			lastActiveDate__gt	Agents last active after this time	false	string
			lastActiveDate__gte	Agents last active after or at this time	false	string
			lastActiveDate__lt	Agents last active before this time	false	string
			lastActiveDate__lte	Agents last active before or at this time	false	string
			lastLoggedInUserName__contains	Free-text filter by username (supports multiple values)	false	string []
			lastSuccessfulScanDate__between	Date range for last successful full disk scan(format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			lastSuccessfu	Agents last	false	string

			lScanDate__gt	successful full disk scan after this time		
			lastSuccessfulScanDate__gte	Agents last successful full disk scan after or at this time	false	string
			lastSuccessfulScanDate__lt	Agents last successful full disk scan before this time	false	string
			lastSuccessfulScanDate__lte	Agents last successful full disk scan before or at this time	false	string
			liveUpdateId__contains	Free-text filter by live update ID (supports multiple values)	false	string []
			locationEnabled	The agents supports Location Awareness and it is enabled for the agent's group	false	boolean []
			locationIds	Include only Agents reporting these locations	false	string []
			locationIdsNin	Do not include only Agents reporting these	false	string []

				locations		
			machineTypes	Included machine types	false	string []
			machineTypesNin	Not included machine types	false	string []
			migrationStatus	Migration status	false	enum
			missingPermissions	Included missing permissions	false	string []
			missingPermissionsNin	Excluded missing permissions	false	string []
			mitigationMode	Agent mitigation mode policy	false	enum
			mitigationModeSuspicious	Mitigation mode policy for suspicious activity	false	enum
			networkInterfaceGatewayMacAddress__contains	Free-text filter by Gateway MAC address (supports multiple values)	false	string []
			networkInterfaceInet__contains	Free-text filter by local IP (supports multiple values)	false	string []
			networkInterfacePhysical__contains	Free-text filter by MAC address (supports multiple values)	false	string []
			networkQuara	The agents	false	boolean []

			ntineEnabled	supports Network Quarantine Control and its enabled for the agent's group		
			networkStatuses	Included network statuses	false	string []
			networkStatusesNin	Included network statuses	false	string []
			operationalStates	Agent operational state	false	string []
			operationalStatesNin	Do not include these Agent operational states	false	string []
			osArch	OS architecture	false	enum
			osTypes	Included OS types	false	string []
			osTypesNin	Not included OS types	false	string []
			osVersion__contains	Free-text filter by OS full name and version (supports multiple values)	false	string []
			query	A free-text search term, will match applicable attributes (sub-string match). Note: Device's	false	string

				physical addresses will be matched if they start with the search term only (no match if they contain the term).		
			rangerStatus	[DEPRECATED] Use rangerStatuses.	false	enum
			rangerStatuses	Status of Ranger	false	string []
			rangerStatusesNin	Do not include these Ranger Statuses	false	string []
			rangerVersions	Ranger versions to include	false	string []
			rangerVersionsNin	Ranger versions not to include	false	string []
			registeredAt__between	Date range for first registration time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			registeredAt__gt	Agents registered after this time	false	string
			registeredAt__gte	Agents registered after or at this time	false	string

			registeredAt__lt	Agents registered before this time	false	string
			registeredAt__lte	Agents registered before or at this time	false	string
			remoteOpsForensicsSupported	Include only agents that has Remote Ops Forensicsfeature supported	false	boolean
			remoteProfilingStates	Agent remote profiling state	false	string []
			remoteProfilingStatesNin	Do not include these Agent remote profiling states	false	string []
			rsoLevel	Supported Remote Script Orchestration level	false	enum
			scanStatus	Scan status	false	enum
			scanStatuses	Included scan statuses	false	string []
			scanStatusesNin	Not included scan statuses	false	string []
			serialNumber__contains	Free-text filter by Serial Number (supports multiple values)	false	string []
			siteIds	List of Site IDs to filter by	false	string []

			tagsData	Filter agents by their assigned tags. Given in form of a JSON where each key represents a tag key, and each value represents a list of string values to filter by. To filter by unassigned tag values, use __nin suffix in the tag key.	false	string
			threatContentHash	Include only Agents that have at least one threat with this content hash	false	string
			threatCreatedAt__between	Agents with threats reported in a date range (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			threatCreatedAt__gt	Agents with threats reported after this time	false	string
			threatCreatedAt__gte	Agents with threats reported after or at	false	string

				this time		
			threatCreated At__lt	Agents with threats reported before this time	false	string
			threatCreated At__lte	Agents with threats reported before or at this time	false	string
			threatHidden	Include only Agents with at least one hidden threat	false	boolean
			threatMitigat ionStatus	Include only Agents that have threats with this mitigation status	false	enum
			threatReboot Required	Has at least one threat with at least one mitigation action pending reboot to succeed	false	boolean []
			threatResolv ed	Include only Agents with at least one resolved threat	false	boolean
			totalMemory __between	Total memory range (GB, inclusive)	false	string
			totalMemory_ _gt	Memory size (MB, more than)	false	integer
			totalMemory_	Memory size	false	integer

			_gte	(MB, more than or equal)		
			totalMemory__lt	Memory size (MB, less than)	false	integer
			totalMemory__lte	Memory size (MB, less than or equal)	false	integer
			updatedAt__between	Date range for update time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			updatedAt__gt	Agents updated after this timestamp	false	string
			updatedAt__gte	Agents updated after or at this timestamp	false	string
			updatedAt__lt	Agents updated before this timestamp	false	string
			updatedAt__lte	Agents updated before or at this timestamp	false	string
			userActionsNeeded	Included pending user actions	false	string []
			userActionsNeededNin	Excluded pending user actions	false	string []
			uuid	Agent's universally unique	false	string

				identifier		
			uuid__contains	Free-text filter by Agent UUID (supports multiple values)	false	string []
			uuids	A list of included UUIDs	false	string []

Update Ranks

PUT /web/api/v2.1/groups/ranks

An Agent can belong to only one Group. If the Agent matches multiple Dynamic Groups, it goes to the Group with the highest rank. The "rank" parameter has a minimum of "1". The lower the integer, the higher priority it has to collect Agents. Make sure the IDs of the groups in this command are for Dynamic groups.

Response Messages

204 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - Insufficient permissions

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>ranks</td><td>List of ranks to update</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>id</td><td>Id</td><td>false</td><td>string</td></tr>
<tr><td>rank</td><td>The new rank for the group</td><td>false</td><td>integer</td></tr>
</table>
</td></tr>
</table>
</td></tr>
<tr><td>filter</td><td>Filter</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>siteIds</td><td>List of Site IDs to filter by</td><td>false</td><td>string []</td></tr>
</table>
</td></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>siteIds</td><td>List of Site</td><td>false</td><td>string []</td></tr>
</table>

	IDs to filter by		

Get Site registration token by ID

GET /web/api/v2.1/groups/{group_id}/token

Get the registration token of the Group of the ID.

Response Messages

200 - Success

401 - Unauthorized access - please sign in and retry.

403 - Insufficient permissions

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td><table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>token</td><td>Token</td><td>false</td><td>string</td></tr></table></td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Hashes

Hash Reputation Rank

GET /web/api/v2.1/hashes/{hash}/reputation

[DEPRECATED] Please use the /verdict endpoint.
Get the reputation rank of the of a hash, given the required SHA1. To get a hash, run "threats" (best if filtered for a Group or Site) and take the fileContentHash value.
Rank is a number measured on a scale of 1-10, where 10 is definitely malicious and 1 is definitely not malicious. 5-10 shows a status of malicious. 1-4 shows a status of not malicious. 0 is status unknown. Example response for a malicious hash looks like this: {"data": {"rank": "5"}}.
Important: This endpoint only returns the rank of the hash if it is known to the management (stored in mgmt DB). For unknown hashes it returns an empty response {"data": {}}

Response Messages

200 - Rank of the hash known to the management. If the hash is unknown, the response is an empty "data" field in the response.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
rank	The hash reputation measured on a scale of 1-10, where 10 is definitely malicious and 1 is definitely not malicious. 5-10 shows a status of malicious. 1-4 shows a	false	string

			status of not malicious. 0 is status unknown.
errors	Errors	false	array

Hash classification

GET /web/api/v2.1/hashes/{hash}/classification

[DEPRECATED] Returns hash classification.

Response Messages

200 - Hash classification received from cloud

401 - Unauthorized access - please sign in and retry.

404 - Hash classification wasn't received from cloud

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>classification</td><td>The hash classification</td><td>false</td><td>string</td></tr>
<tr><td>classificationSource</td><td>The source deciding the most current classification</td><td>false</td><td>enum</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Hash Reputation verdict

GET /web/api/v2.1/hashes/{hash}/verdict

Get the verdict of the of a hash, given the required SHA1.
A hash, either malicious or non-malicious, means it has been marked as such by the Reputation's sources.
An unknown answer is given for hashes that are not yet known by Reputation.

Response Messages

200 - Verdict of the hash known to the management

401 - Unauthorized access - please sign in and retry.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>verdict</td><td>The hash verdict, could be malicious, non-malicious or unknown</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

licenses

Update sites add-ons

PUT /web/api/v2.1/licenses/update-sites-modules

Change the add-ons of the sites by a given filter

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
data	Response data	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>affected</td><td>Number of entities affected by the requested operation</td><td>false</td><td>integer</td></tr></table>
errors	Errors	false	array

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>operation</td><td>Operation</td><td>true</td><td>enum</td></tr>
<tr><td>modules</td><td>Modules</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>name</td><td>Name</td><td>true</td><td>string</td></tr>
</table>
</td></tr>
</table>
</td></tr>
<tr><td>filter</td><td>Filter</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountId</td><td>Account id</td><td>false</td><td>string</td></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>accountName__contains</td><td>Free-text filter by account name (supports multiple values)</td><td>false</td><td>string []</td></tr>
<tr><td>activeLicenses</td><td>Active licenses</td><td>false</td><td>integer</td></tr>
<tr><td>adminOnly</td><td>Show sites the user has Admin privileges to</td><td>false</td><td>boolean</td></tr>
<tr><td>availableMoveSites</td><td>Only return sites the user can move agents to</td><td>false</td><td>boolean</td></tr>
<tr><td>createdAt</td><td>Timestamp of site creation</td><td>false</td><td>string</td></tr>
<tr><td>description</td><td>The description for the Site</td><td>false</td><td>string</td></tr>
<tr><td>description__contains</td><td>Free-text filter by site description</td><td>false</td><td>string []</td></tr>
</table>
</td></tr>
</table>

				(supports multiple values)		
			expiration	Expiration	false	string
			externalId	Id in a CRM external system	false	string
			features	If sent return only sites that support this features	false	string []
			healthStatus	Health status	false	boolean
			isDefault	Is default	false	boolean
			module	Module	false	string
			name	Name	false	string
			name__contains	Free-text filter by site name (supports multiple values)	false	string []
			query	Full text search for fields: name, account_name, description. (Note: on single-account consoles account name will not be matched)	false	string
			registrationToken	Registration token	false	string
			siteIds	List of Site IDs to filter by	false	string []
			siteType	Site type	false	enum
			sku	Sku	false	string

			state	Site state	false	enum	
			states	List of states to filter	false	string []	
			suite	[DEPRECATED] Use sku instead	false	enum	
			totalLicenses	Total licenses	false	integer	
			updatedAt	Timestamp of last update	false	string	

Live Updates

Get Agent Merged Updates

GET /web/api/v2.1/content-updates-inventory

Get Agent's merged updates.

Parameters

agentid	required	The ID of the Agent. Example: "225494730938493804".
countonly	optional	If true, only total number of items will be returned, without any of the actual objects.
cursor	optional	Cursor position returned by the last request. Use to iterate over more than 1000 items. Example: "YWdlbnRfaWQ6NTgwMjkzODE=".
limit	optional	Limit number of returned items (1-1000). Example: "10".
skip	optional	Skip first number of items (0-1000). To iterate over more than 1000 items, use "cursor". Example: "150".
skipcount	optional	If true, total number of items will not be calculated, which speeds up execution time.
sortby	optional	The column to sort the results by. Example: "id".
sortorder	optional	Sort direction. Example: "asc".

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value

<table>
<tr><td>pagination</td><td>Pagination information</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>totalItems</td><td>Total number of items found matching your query</td><td>true</td><td>integer</td></tr>
<tr><td>nextCursor</td><td>Pass this value as "cursor" on your next request, to get the next page of results (Will be "null" when last page reached)</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>appliedAt</td><td>Timestamp of when the update was applied</td><td>false</td><td>string</td></tr>
<tr><td>assetFamilyType</td><td>Live update category</td><td>false</td><td>string</td></tr>
<tr><td>displayName</td><td>Live update type name</td><td>false</td><td>string</td></tr>
<tr><td>liveUpdateId</td><td>Live update ID</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Locations

Create Location

POST /web/api/v2.1/locations

Create a location that defines parameters of Agents in a scope filter. Parameters include:
* ipAddresses - The Agent compares the endpoint active IPv4 or IPv6 addresses to the IP addresses, ranges, and CIDRs defined for the location.
* dnsServers - The Agent compares the configured DNS servers of the endpoint to the DNS servers defined for the location.
* dnsLookup - The Agent resolves the FQDN of the endpoint to IPv4 or IPv6 addresses and compares them to the addresses configured in the location setting.
* networkInterfaces - The Agent determines if the endpoint is connected to the network over a wireless connection. If one connected interface is wireless, the endpoint is considered wireless.
* serverConnectivity - The Agent reports if it is connected to its Management.
* registryKeys - The Agent compares the endpoint registry keys in HKEY_LOCAL_MACHINE\SOFTWARE with the registry key of the location definition.
When you set a location parameter, also set the operator to ALL, NONE, or at least 1.
The serverConnectivity parameter takes "enabled" (true or false) and "value" (connected or disconnected).
The networkInterfaces parameter takes "enabled" (true or false) and "value" (wired or wireless).

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - Insufficient permissions

Response Schema

Name	Description	Required	Value
data	Response data	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>name</td><td>Location name (should be unique per scope)</td><td>true</td><td>string</td></tr></table>

			operator	Logical operator to apply between the set of identifiers	true	enum
			activeFirewallRules	Number of active firewall rules defined in the location	false	integer
			createdAt	Created at	false	string
			creator	Location creator name	false	string
			creatorId	Location creator ID	false	string
			description	Location description	false	string
			dnsLookup	Identify a location by DNS lookup results	false	

Name	Description	Required	Value
operator	Logical operator to apply between the set of identifiers	true	enum
identifiers	A list of DNS lookup identifiers	false	

Name	Description	Required	Value
host	Hostname to resolve	true	string
ip	Resolved IP address	true	string

dnsServers	Identify a location by DNS servers defined on the endpoint	false	

Name	Description	Required	Value
operator	Logical operator to apply between the set of identifiers	true	enum
identifiers	A list of	false	

							identifiers		Name	Description	Required	Value
									type	Address type	true	enum
									values	IP address, CIDR or range of two addresses. May be either IPv4 or IPv6	false	string []
			editable	Is location editable in current scope	false	boolean						
			id	Id	false	string						
			ipAddresses	Identify a location the assigned IP addresses	false	Name	Description	Required	Value			
						operator	Logical operator to apply between the set of identifiers	true	enum			
						identifiers	A list of identifiers	false	Name	Description	Required	Value
									type	Address type	true	enum
									values	IP address, CIDR or range of two addresses. May be either IPv4 or IPv6	false	string []
			isFallback	Is fallback	false	boolean						
			networkInterfaces	Identify a location by available network interface types	false	Name	Description	Required	Value			
						enabled	Use or discard this location identifier	true	boolean			
						value	Network interface type	false	enum			
			registryKeys	Identify a	false							

				location by a registry key or value		<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>key</td><td>Registry key path to match. Must start with "HKEY_LOCAL_MACHINE\SOFTWARE\".</td><td>true</td><td>string</td></tr><tr><td>data</td><td>Content of the value to match (may be a string or a 64-bit integer, optional)</td><td>false</td><td>string</td></tr><tr><td>value</td><td>Value name in the registry key path to match (optional)</td><td>false</td><td>string</td></tr></table>
			reportingAgents	Number of agents in the location	false	integer
			scope	Scope	false	enum
			scopeId	Scope id	false	string
			scopeName	Scope name	false	string
			serverConnectivity	Identify a location by connectivity to the management server	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>enabled</td><td>Use or discard this location identifier</td><td>true</td><td>boolean</td></tr><tr><td>value</td><td>Server connectivity status</td><td>false</td><td>enum</td></tr></table>
			updatedAt	Updated at	false	string
			updater	Location updater name	false	string

			updaterId	Location updater	false	string
errors	Errors	false	array			

Body Schema

Name	Description	Required	Value
data	Location data	true	

Name	Description	Required	Value
name	Location name (should be unique per scope)	true	string
operator	Logical operator to apply between the set of identifiers	true	enum
description	Location description	false	string
dnsLookup	Identify a location by DNS lookup results	false	
dnsServers	Identify a location by DNS servers defined on the endpoint	false	

Name	Description	Required	Value
operator	Logical operator to apply between the set of identifiers	true	enum
identifiers	A list of DNS lookup identifiers	false	

Name	Description	Required	Value
host	Hostname to resolve	true	string
ip	Resolved IP address	true	string

Name	Description	Required	Value
operator	Logical operator to apply between the set of identifiers	true	enum
identifiers	A list of identifiers	false	

Name	Description	Required	Value
type	Address type	true	enum

									values	IP address, CIDR or range of two addresses. May be either IPv4 or IPv6	false	string []
			ipAddresses	Identify a location the assigned IP addresses	false	Name	Description	Required	Value			
						operator	Logical operator to apply between the set of identifiers	true	enum			
						identifiers	A list of identifiers	false	Name	Description	Required	Value
									type	Address type	true	enum
									values	IP address, CIDR or range of two addresses. May be either IPv4 or IPv6	false	string []
			networkInterfaces	Identify a location by available network interface types	false	Name	Description	Required	Value			
						enabled	Use or discard this location identifier	true	boolean			
						value	Network interface type	false	enum			
			registryKeys	Identify a location by a registry key or value	false	Name	Description	Required	Value			
						key	Registry key path to match. Must start with "HKEY_LOCAL_MACHINE\SOFTWARE\".	true	string			

<table>
<tr><td></td><td></td><td></td><td>
<table>
<tr><td></td><td></td><td></td><td>
<table>
<tr><td>data</td><td>Content of the value to match (may be a string or a 64-bit integer, optional)</td><td>false</td><td>string</td></tr>
<tr><td>value</td><td>Value name in the registry key path to match (optional)</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>serverConnectivity</td><td>Identify a location by connectivity to the management server</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>enabled</td><td>Use or discard this location identifier</td><td>true</td><td>boolean</td></tr>
<tr><td>value</td><td>Server connectivity status</td><td>false</td><td>enum</td></tr>
</table>
</td></tr>
</table>
</td></tr>
<tr><td>filter</td><td>Location scope</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>siteIds</td><td>List of Site IDs to filter by</td><td>false</td><td>string []</td></tr>
</table>
</td></tr>
</table>

Get Locations

GET /web/api/v2.1/locations

Get the locations of Agents in a given scope that match the filter. Agent locations are based on endpoint network parameters (IP, DNS, NIC, Registry Key, or SentinelOne connection set for all true, at least one true, or none true and applied to a Site, Account, or Global). Agents detect their location settings and apply Firewall Control rules that have Location Aware parameters that match the Agent location. Agents can be in multiple locations at the same time. If an Agent that supports Locations does not detect that it is in a defined location, it uses the Firewall rules assigned to the Fallback location.
Use this command with a filter for "hasFirewallRules" to find Locations that do not have matching Firewall Control rules. The response to this request includes the ID of the location, which you can use in other commands.
Firewall Control and Location Awareness require Control SKU.

Parameters

accountids	optional	List of Account IDs to filter by. Example: "225494730938493804,225494730938493915".
countonly	optional	If true, only total number of items will be returned, without any of the actual objects.
creator__contains	optional	Free-text filter by creator of the location (supports multiple values). Example: "max,mike".
cursor	optional	Cursor position returned by the last request. Use to iterate over more than 1000 items. Example: "YWdlbnRfaWQ6NTgwMjkzODE=".
description__contains	optional	Free-text filter by description (supports multiple values). Example: "out of office".
groupids	optional	List of Group IDs to filter by. Example: "225494730938493804,225494730938493915".
hasfirewallrules	optional	Filter by locations with/without firewall rules associated to them
hostname__contains	optional	Free-text filter by hostname (supports multiple values). Example: "sentinelone.com,localhost".
ids	optional	Filter results by location IDs. Example: "225494730938493804,225494730938493915".
ipaddress__contains	optional	Free-text filter by IP address (supports multiple values). Example: "29.213.22.17".
limit	optional	Limit number of returned items (1-1000). Example: "10".
name__contains	optional	Free-text filter by location name (supports multiple values). Example:

		"office".
registrykey__contains	optional	Free-text filter by registry key (supports multiple values). Example: "system\software,sentinel".
scopename__contains	optional	Free-text filter by scope name (supports multiple values). Example: "my_group,my_site".
scopes	optional	Filter results by scope. Example: "account".
siteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".
skip	optional	Skip first number of items (0-1000). To iterate over more than 1000 items, use "cursor". Example: "150".
skipcount	optional	If true, total number of items will not be calculated, which speeds up execution time.
sortby	optional	The column to sort the results by. Example: "id".
sortorder	optional	Sort direction. Example: "asc".

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
pagination	Pagination information	true	

Name	Description	Required	Value
totalItems	Total number of items found matching your query	true	integer
nextCursor	Pass this value as "cursor" on your next request, to	false	string

				get the next page of results (Will be "null" when last page reached)		
data	Response data	false	Name	Description	Required	Value
			name	Location name (should be unique per scope)	true	string
			operator	Logical operator to apply between the set of identifiers	true	enum
			activeFirewallRules	Number of active firewall rules defined in the location	false	integer
			createdAt	Created at	false	string
			creator	Location creator name	false	string
			creatorId	Location creator ID	false	string
			description	Location description	false	string
			dnsLookup	Identify a location by DNS lookup results	false	Name / Description / Required / Value
						operator / Logical operator to apply between the set of identifiers / true / enum
						identifiers / A list of DNS lookup / false / Name / Description / Required / Value

							identifiers		host	Hostname to resolve	true	string
									ip	Resolved IP address	true	string
			dnsServers	Identify a location by DNS servers defined on the endpoint	false	Name	Description	Required	Value			
						operator	Logical operator to apply between the set of identifiers	true	enum			
						identifiers	A list of identifiers	false	Name	Description	Required	Value
									type	Address type	true	enum
									values	IP address, CIDR or range of two addresses. May be either IPv4 or IPv6	false	string []
			editable	Is location editable in current scope	false	boolean						
			id	Id	false	string						
			ipAddresses	Identify a location the assigned IP addresses	false	Name	Description	Required	Value			
						operator	Logical operator to apply between the set of identifiers	true	enum			
						identifiers	A list of identifiers	false	Name	Description	Required	Value
									type	Address type	true	enum
									values	IP address, CIDR or range of two addresses.	false	string []

										May be either IPv4 or IPv6		
			isFallback	Is fallback	false	boolean						
			networkInterfaces	Identify a location by available network interface types	false	Name	Description	Required	Value			
						enabled	Use or discard this location identifier	true	boolean			
						value	Network interface type	false	enum			
			registryKeys	Identify a location by a registry key or value	false	Name	Description	Required	Value			
						key	Registry key path to match. Must start with "HKEY_LOCAL_MACHINE\SOFTWARE\".	true	string			
						data	Content of the value to match (may be a string or a 64-bit integer, optional)	false	string			
						value	Value name in the registry key path to match (optional)	false	string			
			reportingAgents	Number of agents in the location	false	integer						
			scope	Scope	false	enum						
			scopeId	Scope id	false	string						
			scopeName	Scope name	false	string						

<table>
<tr><td></td><td></td><td></td><td>
<table>
<tr><td>serverConnectivity</td><td>Identify a location by connectivity to the management server</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>enabled</td><td>Use or discard this location identifier</td><td>true</td><td>boolean</td></tr>
<tr><td>value</td><td>Server connectivity status</td><td>false</td><td>enum</td></tr>
</table>
</td></tr>
<tr><td>updatedAt</td><td>Updated at</td><td>false</td><td>string</td></tr>
<tr><td>updater</td><td>Location updater name</td><td>false</td><td>string</td></tr>
<tr><td>updaterId</td><td>Location updater</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Delete Locations

DELETE /web/api/v2.1/locations

Delete location definitions of a given location. To get location IDs, run "locations".

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - Insufficient permissions

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>affected</td><td>Number of entities affected by the requested operation</td><td>false</td><td>integer</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

Name	Description	Required	Value
data	Data	true	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>ids</td><td>List of location IDs to delete</td><td>false</td><td>string []</td></tr></table>

Update Location

PUT /web/api/v2.1/locations/{location_id}

Change the parameter values of a location definition. See Create Location.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - Insufficient permissions

404 - Location not found

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
name	Location name (should be unique per scope)	true	string
operator	Logical operator to apply between the set of identifiers	true	enum
activeFirewallRules	Number of active firewall rules defined in the location	false	integer
createdAt	Created at	false	string
creator	Location	false	string

	creator name		
creatorId	Location creator ID	false	string
description	Location description	false	string
dnsLookup	Identify a location by DNS lookup results	false	

Name	Description	Required	Value
operator	Logical operator to apply between the set of identifiers	true	enum
identifiers	A list of DNS lookup identifiers	false	

Name	Description	Required	Value
host	Hostname to resolve	true	string
ip	Resolved IP address	true	string

dnsServers	Identify a location by DNS servers defined on the endpoint	false	

Name	Description	Required	Value
operator	Logical operator to apply between the set of identifiers	true	enum
identifiers	A list of identifiers	false	

Name	Description	Required	Value
type	Address type	true	enum
values	IP address, CIDR or range of two addresses. May be either IPv4 or IPv6	false	string []

editable	Is location editable in current scope	false	boolean
id	Id	false	string

			ipAddresses	Identify a location the assigned IP addresses	false

Name	Description	Required	Value
operator	Logical operator to apply between the set of identifiers	true	enum
identifiers	A list of identifiers	false	

Name	Description	Required	Value
type	Address type	true	enum
values	IP address, CIDR or range of two addresses. May be either IPv4 or IPv6	false	string []

isFallback	Is fallback	false	boolean
networkInterfaces	Identify a location by available network interface types	false	

Name	Description	Required	Value
enabled	Use or discard this location identifier	true	boolean
value	Network interface type	false	enum

registryKeys	Identify a location by a registry key or value	false	

Name	Description	Required	Value
key	Registry key path to match. Must start with "HKEY_LOCAL_MACHINE\SOFTWARE\".	true	string
data	Content of the value to match (may be a string or a 64-bit integer,	false	string

<table>
<tr><td></td><td></td><td></td><td>
<table>
<tr><td></td><td></td><td></td><td>
<table>
<tr><td></td><td>optional)</td><td></td><td></td></tr>
<tr><td>value</td><td>Value name in the registry key path to match (optional)</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>reportingAgents</td><td>Number of agents in the location</td><td>false</td><td>integer</td></tr>
<tr><td>scope</td><td>Scope</td><td>false</td><td>enum</td></tr>
<tr><td>scopeId</td><td>Scope id</td><td>false</td><td>string</td></tr>
<tr><td>scopeName</td><td>Scope name</td><td>false</td><td>string</td></tr>
<tr><td>serverConnectivity</td><td>Identify a location by connectivity to the management server</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>enabled</td><td>Use or discard this location identifier</td><td>true</td><td>boolean</td></tr>
<tr><td>value</td><td>Server connectivity status</td><td>false</td><td>enum</td></tr>
</table>
</td></tr>
<tr><td>updatedAt</td><td>Updated at</td><td>false</td><td>string</td></tr>
<tr><td>updater</td><td>Location updater name</td><td>false</td><td>string</td></tr>
<tr><td>updaterId</td><td>Location updater</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

Name	Description	Required	Value
data	Data	true	

Name	Description	Required	Value
name	Location name (should be unique per scope)	true	string
description	Location description	false	string
dnsLookup	Identify a location by DNS lookup results	false	
dnsServers	Identify a location by DNS servers defined on the endpoint	false	

Name	Description	Required	Value
operator	Logical operator to apply between the set of identifiers	true	enum
identifiers	A list of DNS lookup identifiers	false	

Name	Description	Required	Value
host	Hostname to resolve	true	string
ip	Resolved IP address	true	string

Name	Description	Required	Value
operator	Logical operator to apply between the set of identifiers	true	enum
identifiers	A list of identifiers	false	

Name	Description	Required	Value
type	Address type	true	enum
values	IP address, CIDR or range of two addresses. May be either IPv4 or IPv6	false	string []

			ipAddresses	Identify a location the assigned IP addresses	false

Name	Description	Required	Value
operator	Logical operator to apply between the set of identifiers	true	enum
identifiers	A list of identifiers	false	

Name	Description	Required	Value
type	Address type	true	enum
values	IP address, CIDR or range of two addresses. May be either IPv4 or IPv6	false	string []

networkInterfaces	Identify a location by available network interface types	false	

Name	Description	Required	Value
enabled	Use or discard this location identifier	true	boolean
value	Network interface type	false	enum

operator	Logical operator to apply between the set of identifiers	false	enum
registryKeys	Identify a location by a registry key or value	false	

Name	Description	Required	Value
key	Registry key path to match. Must start with "HKEY_LOCAL_MACHINE\SOFTWARE\".	true	string
data	Content of	false	string

							the value to match (may be a string or a 64-bit integer, optional)		
						value	Value name in the registry key path to match (optional)	false	string
			serverConnectivity	Identify a location by connectivity to the management server	false	Name	Description	Required	Value
						enabled	Use or discard this location identifier	true	boolean
						value	Server connectivity status	false	enum

marketplace

Get Applications Catalog

GET /web/api/v2.1/singularity-marketplace/applications-catalog

Get the Marketplace Application Catalog.

Parameters

category__contains	optional	Free-text filter by catalog application category (supports multiple values). Example: "Service Pack 1".
description__contains	optional	Free-text filter by catalog application description (supports multiple values). Example: "Service Pack 1".
id	optional	Filter results by application catalog id. Example: "225494730938493804,225494730938493915".
name__contains	optional	Free-text filter by catalog application name (supports multiple values). Example: "Service Pack 1".
query	optional	Free-text filter by S1 query (supports multiple values). Example: "Service Pack 1".

Response Messages

200 - Success

400 - Invalid user input received, See error details for further information

401 - Unauthorized access - please sign in and retry

Response Schema

Name	Description	Required	Value
data	Response data	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>name</td><td>Application's name</td><td>true</td><td>string</td></tr></table>

			availablePlugins	Available Plugins for the Application	false	string
			category	Application's category	false	string
			createdAt	Date of Application's installation	false	string
			deletedAt	Deleted Application Date of Deletion	false	string
			description	The description of the Application	false	string
			externalUrl	External URL in case the app type is not openfaas	false	string
			icon	Application's icon	false	string
			id	Application ID	false	string
			installed	True if the application is installed for requested user	false	boolean
			key	The application's unique key	false	string
			oauthUrl	OAuth URL in case the app supports OIDC flows	false	string
			retryPolicy	The number of seconds to retry until in case of app	false	integer

			error
			summary: Application's summary (false, string)
			type: Type of triggered application (false, string)
			updatedAt: Date of last update (false, string)
			viewPolicy: Policy for whether to show or hide and application in the catalog (false, string)
errors	Errors	false	array

Get Installed Applications

GET /web/api/v2.1/singularity-marketplace/applications

Get the installed Marketplace applications for a scope specified.

Parameters

accountids	optional	List of Account IDs to filter by. Example: "225494730938493804,225494730938493915".
application_catalog_id	optional	A list of catalog applications IDs. Example: "225494730938493804,225494730938493915".
countonly	optional	If true, only total number of items will be returned, without any of the actual objects.
creator__contains	optional	Free-text filter by application creator (supports multiple values). Example: "Service Pack 1".
cursor	optional	Cursor position returned by the last request. Should be used for iterating over more than 1000 items. Example: "YWdlbnRfaWQ6NTgwMjkzODE=".
disablepagination	optional	If true, all installed applications for requested scope will be returned
groupids	optional	List of Group IDs to filter by. Example: "225494730938493804,225494730938493915".
id	optional	A list of applications IDs. Example: "225494730938493804,225494730938493915".
limit	optional	Limit number of returned items (1-1000). Example: "10".
name__contains	optional	Free-text filter by application name (supports multiple values). Example: "Service Pack 1".
query	optional	Free-text filter by S1 query (supports multiple values). Example: "Service Pack 1".
scopes	optional	Filter results by scope. Example: "global".
siteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".
skip	optional	Skip first number of items (0-1000). For iterating over more than a 1000 items please use "cursor" instead. Example: "150".
skipcount	optional	If true, total number of items will not be calculated, which speeds up

		execution time
sortby	optional	The column to sort the results by. Example: "id".
sortorder	optional	Sort direction. Example: "asc".

Response Messages

200 - Success

400 - Invalid user input received, See error details for further information

401 - Unauthorized access - please sign in and retry

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>pagination</td><td>Pagination information</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>totalItems</td><td>Total number of items found matching your query</td><td>true</td><td>integer</td></tr>
<tr><td>nextCursor</td><td>Pass this value as "cursor" on your next request, to get the next page of results (Will be "null" when last page has been reached)</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>name</td><td>Application's name</td><td>true</td><td>string</td></tr>
<tr><td>applicationCatalogId</td><td>Application Catalog ID</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
</table>

			hasAlert	True if the any installed application has any issues	false	boolean
			icon	Application's icon	false	string
			lastInstalledAt	Last time an Application was installed	false	string
			scopes	Scopes	false	

Name	Description	Required	Value
desiredStatus	Desired status	true	enum
status	Status	true	enum
account	Application's scope account name	false	string
accountId	Account ID of the scope the application was installed for	false	string
alertMessage	Application's alert message, in case of an alert	false	string
createdAt	Date application was installed	false	string
creator	Application's creator name	false	string
creatorId	The ID of the user who installed the application	false	string
group	Application's scope group name	false	string

							groupId	Group ID of the scope the application was installed for	false	string		
							hasAlert	True if the application has any issues	false	boolean		
							id	Application ID	false	string		
							lastEntityCreatedAt	Date of the last entity processed by the application	false	string		
							modifier	Application's last modifier name	false	string		
							modifierId	The ID of the user who modified last the application	false	string		
							retryUntil	In case the application receives errors, the field will be populated with the last date and time the application can retry	false	string		
							scopeId	Scope ID of the scope the application was installed for	false	string		
							scopeLevel	Scope the application	false	enum		

							was installed for		
						site	Application's scope site name	false	string
						siteId	Site ID of the scope the application was installed for	false	string
						updatedAt	Date of last update	false	string
errors	Errors	false	array						

Delete Application

DELETE /web/api/v2.1/singularity-marketplace/applications

Delete application integration from your Marketplace.

Response Messages

200 - Delete Application successfully

400 - Invalid user input received, See error details for further information

401 - Unauthorized access - please sign in and retry

Response Schema

Name	Description	Required	Value
data	Response data	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>affected</td><td>Number of entities affected by the requested operation</td><td>false</td><td>integer</td></tr></table>
errors	Errors	false	array

Body Schema

Name	Description	Required	Value
filter	Filter	true	

Name	Description	Required	Value
accountIds	List of Account IDs to filter by	false	string []
application_catalog_id	A list of catalog applications IDs	false	string []
creator__contains	Free-text filter by application creator (supports multiple values)	false	string []
groupIds	List of Group IDs to filter by	false	string []
id	A list of applications IDs	false	string []
name__contains	Free-text filter by application name (supports multiple values)	false	string []
query	Free-text filter by S1 query (supports multiple values)	false	string []
scopes	Filter results by scope	false	string []
siteIds	List of Site IDs to filter	false	string []

				by		

Install Applications

POST /web/api/v2.1/singularity-marketplace/applications

Install application from the Application Catalog.

Response Messages

200 - Installed application successfully

400 - Invalid user input received, See error details for further information

401 - Unauthorized access - please sign in and retry

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>affected</td><td>Number of entities affected by the requested operation</td><td>false</td><td>integer</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>configurations</td><td>Configurations</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>id</td><td>Id</td><td>false</td><td>string</td></tr>
<tr><td>value</td><td>Value</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
</table>
</td></tr>
<tr><td>filter</td><td>Filter</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>applicationCatalogId</td><td>Install Application for requested Application Catalog ID</td><td>false</td><td>string</td></tr>
<tr><td>groupIds</td><td>List of Group IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>siteIds</td><td>List of Site IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>tenant</td><td>Indicates a tenant scope request</td><td>false</td><td>boolean</td></tr>
</table>
</td></tr>
</table>

Update Application Configuration

PUT /web/api/v2.1/singularity-marketplace/applications

Update installed application configuration.

Response Messages

200 - Success

400 - Invalid user input received, See error details for further information

401 - Unauthorized access - please sign in and retry

Response Schema

Name	Description	Required	Value
data	Response data	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>affected</td><td>Number of entities affected by the requested operation</td><td>false</td><td>integer</td></tr></table>
errors	Errors	false	array

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>configurations</td><td>Configurations</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>id</td><td>Id</td><td>false</td><td>string</td></tr>
<tr><td>value</td><td>Value</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
</table>
</td></tr>
<tr><td>filter</td><td>Filter</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>groupIds</td><td>List of Group IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>ids</td><td>A list of applications IDs</td><td>false</td><td>string []</td></tr>
<tr><td>siteIds</td><td>List of Site IDs to filter by</td><td>false</td><td>string []</td></tr>
</table>
</td></tr>
</table>

Get Configuration Fields

GET /web/api/v2.1/singularity-marketplace/applications-catalog/{application_catalog_id}/config

Get the Catalog Application Configuration Fields.

Response Messages

200 - Success

401 - Unauthorized access - please sign in and retry

404 - Application Catalog not found

Response Schema

Name	Description	Required	Value
data	Response data	false	
errors	Errors	false	array

Name	Description	Required	Value
fields	Fields	false	

Name	Description	Required	Value
defaultValue	Default value	false	string
enum	Enum	false	string []
id	Id	false	string
label	Label	false	string
placeHolder	Place holder	false	string
required	Required	false	boolean
type	Type	false	string
value	Value	false	string

Get Configuration fields for Catalog Application

GET /web/api/v2.1/singularity-marketplace/applications/{application_id}/config

Returns The configuration schema for a requested Application Catalog.

Response Messages

200 - Success

401 - Unauthorized access - please sign in and retry

404 - Application not found

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
desiredStatus	Desired status	true	enum
status	Status	true	enum
account	Application's scope account name	false	string
accountId	Account ID of the scope the application was installed for	false	string
alertMessage	Application's alert message, in case of an alert	false	string
createdAt	Date application was installed	false	string

			creator	Application's creator name	false	string
			creatorId	The ID of the user who installed the application	false	string
			fields	Fields	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>defaultValue</td><td>Default value</td><td>false</td><td>string</td></tr><tr><td>enum</td><td>Enum</td><td>false</td><td>string []</td></tr><tr><td>id</td><td>Id</td><td>false</td><td>string</td></tr><tr><td>label</td><td>Label</td><td>false</td><td>string</td></tr><tr><td>placeHolder</td><td>Place holder</td><td>false</td><td>string</td></tr><tr><td>required</td><td>Required</td><td>false</td><td>boolean</td></tr><tr><td>type</td><td>Type</td><td>false</td><td>string</td></tr><tr><td>value</td><td>Value</td><td>false</td><td>string</td></tr></table>
			group	Application's scope group name	false	string
			groupId	Group ID of the scope the application was installed for	false	string
			hasAlert	True if the application has any issues	false	boolean
			id	Application ID	false	string
			lastEntityCreatedAt	Date of the last entity processed by the application	false	string
			modifier	Application's last modifier name	false	string

			modifierId: The ID of the user who modified last the application; false; string retryUntil: In case the application receives errors, the field will be populated with the last date and time the application can retry; false; string scopeId: Scope ID of the scope the application was installed for; false; string scopeLevel: Scope the application was installed for; false; enum site: Application's scope site name; false; string siteId: Site ID of the scope the application was installed for; false; string updatedAt: Date of last update; false; string
errors	Errors	false	array

Enable or Disable application

POST /web/api/v2.1/singularity-marketplace/applications/{mode}

Use this command to enable or disable application integrations that match the filter.

Response Messages

200 - Updated application mode successfully

400 - Invalid user input received, See error details for further information

401 - Unauthorized access - please sign in and retry

404 - Application not found

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>affected</td><td>Number of entities affected by the requested operation</td><td>false</td><td>integer</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>filter</td><td>Filter</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>applicationId</td><td>Enable or Disable Application for requested Application by ID</td><td>false</td><td>string</td></tr>
<tr><td>groupIds</td><td>List of Group IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>siteIds</td><td>List of Site IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>tenant</td><td>Indicates a tenant scope request</td><td>false</td><td>boolean</td></tr>
</table>
</td></tr>
</table>

Mobile Integration

Activations - Resend activation link invitations

PUT /web/api/v2.1/mobile-integration/activation/user-activation/resend-activations

Activations - Resend activation link invitations

Response Messages

200 - Activation links resend

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - 403 - You do not have authorization to complete request.

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>false</td><td>string []</td></tr>
<tr><td>filter</td><td>Filter</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>groupIds</td><td>List of Group IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>siteIds</td><td>List of Site IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>tenant</td><td>Indicates a tenant scope request</td><td>false</td><td>boolean</td></tr>
</table>
</td></tr>
</table>

Activations - Cancel user activation invitations

PUT /web/api/v2.1/mobile-integration/activation/user-activation/cancel-activations

Activations - Cancel user activation invitations

Response Messages

200 - Activation links cancelled

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - 403 - You do not have authorization to complete request.

Body Schema

Name	Description	Required	Value
data	Data	false	string []
filter	Filter	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr><tr><td>groupIds</td><td>List of Group IDs to filter by</td><td>false</td><td>string []</td></tr><tr><td>siteIds</td><td>List of Site IDs to filter by</td><td>false</td><td>string []</td></tr><tr><td>tenant</td><td>Indicates a tenant scope request</td><td>false</td><td>boolean</td></tr></table>

Activations - Validate bulk user activation upload

POST /web/api/v2.1/mobile-integration/activation/user-activation/validate-import

Check the validity of uploaded CSV file and its content

Response Messages

200 - Validation result

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - 403 - You do not have authorization to complete request.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>total</td><td>The number of rows in the file</td><td>true</td><td>integer</td></tr>
<tr><td>errors</td><td>Validation errors</td><td>false</td><td>array</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>formData</td><td></td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>file</td><td>The input CSV file with user activations</td><td>true</td><td>file</td></tr>
<tr><td>filter</td><td>The details of the scope where the entities will be imported, for example:
For Global - '{"tenant":true}'
For an Account - '{"accountIds":

["225494730938493804"]}'
For a Site - '{"siteIds": ["225494730938493804"]}'
For a Group - '{"groupIds": ["225494730938493804"]}'</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
</table>

Activations - Bulk user activation import

POST /web/api/v2.1/mobile-integration/activation/user-activation/import

Import user activations from uploaded CSV file

Response Messages

200 - Import completed

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - 403 - You do not have authorization to complete request.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>total</td><td>The number of rows in the file</td><td>true</td><td>integer</td></tr>
<tr><td>errors</td><td>Validation errors</td><td>false</td><td>array</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

Name	Description	Required	Value
formData		false	

Name	Description	Required	Value
file	The input CSV file with user activations	true	file
filter	The details of the scope where the entities will be imported, for example: For Global - '{"tenant":true}' For an Account - '{"accountIds": ["225494730938493804"]}' For a Site - '{"siteIds": ["225494730938493804"]}' For a Group - '{"groupIds": ["225494730938493804"]}'	false	string
mgmtGroupId	Group identifier of a group where new devices will be activated	false	string

Provision - Check if tenant can be provisioned

GET /web/api/v2.1/mobile-integration/provisioning/can-provision-tenant

Checks if tenant can be provisioned by scope

Parameters

accountids	optional	List of Account IDs to filter by. Example: "225494730938493804,225494730938493915".
groupids	optional	List of Group IDs to filter by. Example: "225494730938493804,225494730938493915".
siteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".
tenant	optional	Indicates a tenant scope request

Response Messages

200 - Tenant retrieved

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
canProvision	Can provision tenant	true	boolean
affectingScopes	Affectingscopes	false	

Name	Description	Required	Value
id	Scope ID	true	string
level	Scope level	true	string

Name	Description	Required	Value
msspScope	Is MSSP scope	false	boolean
reason	Reason for	false	string

				not being able to provision tenant		
			reasonCode	Reason code for not being able to provision tenant	false	string
			underMSSPScope	Is under MSSP scope	false	boolean
errors	Errors	false	array			

Provision - Persist MSSP partner key

POST /web/api/v2.1/mobile-integration/provisioning/partner-key

Persists MSSP partner key - client ID and secret - for future customer provisioning.

Response Messages

201 - Partner key persisted successfully.

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - 403 - You do not have authorization to complete request.

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>clientId</td><td>Partner client ID</td><td>true</td><td>string</td></tr>
<tr><td>secret</td><td>Partner secret</td><td>true</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>filter</td><td>Filter</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>groupIds</td><td>List of Group IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>siteIds</td><td>List of Site IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>tenant</td><td>Indicates a tenant scope request</td><td>false</td><td>boolean</td></tr>
</table>
</td></tr>
</table>

Provision - Update MSSP partner key

PUT /web/api/v2.1/mobile-integration/provisioning/partner-key

Updates MSSP partner key - client ID and secret - for future customer provisioning.

Response Messages

201 - Partner key updated successfully.

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - 403 - You do not have authorization to complete request.

404 - 404 - Partner key not found.

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>clientId</td><td>Partner client ID</td><td>true</td><td>string</td></tr>
<tr><td>secret</td><td>Partner secret</td><td>true</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>filter</td><td>Filter</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>groupIds</td><td>List of Group IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>siteIds</td><td>List of Site IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>tenant</td><td>Indicates a</td><td>false</td><td>boolean</td></tr>
</table>
</td></tr>
</table>

				tenant scope request		

Provision - Get MSSP partner key

GET /web/api/v2.1/mobile-integration/provisioning/partner-key

Gets MSSP partner key by scope

Parameters

accountids	optional	List of Account IDs to filter by. Example: "225494730938493804,225494730938493915".
groupids	optional	List of Group IDs to filter by. Example: "225494730938493804,225494730938493915".
siteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".
tenant	optional	Indicates a tenant scope request

Response Messages

200 - Partner key retrieved successfully.

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
data	Response data	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>clientId</td><td>Partner client ID</td><td>true</td><td>string</td></tr></table>
errors	Errors	false	array

Provision - Provision tenant with admin user

POST /web/api/v2.1/mobile-integration/provisioning/tenant

Provision a new tenant and create an admin user for the tenant account

Response Messages

201 - Tenant provisioned and admin user created

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - 403 - You do not have authorization to complete request.

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>adminEmail</td><td>User's email address</td><td>true</td><td>string</td></tr>
<tr><td>adminFirstName</td><td>User's first name</td><td>true</td><td>string</td></tr>
<tr><td>adminLastName</td><td>User's last name</td><td>true</td><td>string</td></tr>
<tr><td>adminNotificationEmail</td><td>Notification email for sending details</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>filter</td><td>Filter</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>groupIds</td><td>List of Group IDs to filter by</td><td>false</td><td>string []</td></tr>
</table>
</td></tr>
</table>

			siteIds	List of Site IDs to filter by	false	string []
			tenant	Indicates a tenant scope request	false	boolean

Provision - Get tenant with users

GET /web/api/v2.1/mobile-integration/provisioning/tenant

Gets tenant with users by scope

Parameters

accountids	optional	List of Account IDs to filter by. Example: "225494730938493804,225494730938493915".
groupids	optional	List of Group IDs to filter by. Example: "225494730938493804,225494730938493915".
siteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".
tenant	optional	Indicates a tenant scope request

Response Messages

200 - Tenant retrieved

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
id	Tenant ID	true	string
name	Tenant name	true	string
adminUser	Tenant admin user	false	

Name	Description	Required	Value
created	User's creation date	true	string
email	User's email address	true	string
firstName	User's first	true	string

							name		
						id	User ID	true	string
						lastName	User's last name	true	string
						role	User's role	true	Name | Description | Required | Value id | Role ID | true | string name | Role name | true | string
						notificationEmail	Notification email for sending details	false	string
			users	Tenant users	false	Name	Description	Required	Value
						created	User's creation date	true	string
						email	User's email address	true	string
						firstName	User's first name	true	string
						id	User ID	true	string
						lastName	User's last name	true	string
						role	User's role	true	Name | Description | Required | Value id | Role ID | true | string name | Role name | true | string
						notificationEmail	Notification email for sending details	false	string
errors	Errors	false	array						

Management - Create interim connector connection

POST /web/api/v2.1/mobile-integration/management/create-interim-connection

Management - Create interim connector connection.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td><table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>connectionId</td><td>Connectionid</td><td>true</td><td>string</td></tr></table></td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

Name	Description	Required	Value
data	Data	true	

Name	Description	Required	Value
MicrosoftEndpointManagerConnector	Microsoftendpointmanagerconnector	false	

Name	Description	Required	Value
auth	Auth	true	

Name	Description	Required	Value
oauth	Oauth	false	

Name	D
cloud	Cl
tenantId	Te

Name	Description	Required	Value
baseUrl	Baseurl	true	string
backgroundSync	Enable background syncing	false	boolean
maskUserInformation	Enable masking user information	false	boolean
mode	Supported mode	false	enum

Name	Description	Required	Value
MobileIronCloudConnector	Mobileironcloudconnector	false	

Name	Description	Required	Value
auth	Auth	true	

Name	Description	Required	Value
basic	Basic	true	

Name	D
password	Pa
userId	Us

Name	Description	Required	Value
baseUrl	Baseurl	true	string

Name	Description	Required	Value
MobileIronCoreConnector	Mobileironcoreconnector	false	

Name	Description	Required	Value
auth	Auth	true	

Name	Description	Required	Value
basic	Basic	true	

Name	D
password	Pa
userId	Us

						baseUrl	Baseurl	true	string
			WorkspaceOneConnector	Workspaceoneconnector	false	Name	Description	Required	Value
						auth	Auth	true	Name / Description / Required / Value
									basic / Basic / false / Name / Description: apiKey / Ap; password / Pa; userId / Us
									certificate / Certificate / false / Name / Description: apiKey / Ap; certificate / Ce; passphrase / Pa
						baseUrl	Baseurl	true	string
filter	Filter	true	Name	Description	Required	Value			
			accountIds	List of Account IDs to filter by	false	string []			
			groupIds	List of Group IDs to filter by	false	string []			
			siteIds	List of Site IDs to filter by	false	string []			
			tenant	Indicates a tenant scope request	false	boolean			

Management - Checks if connection can be created on current scope.

GET /web/api/v2.1/mobile-integration/management/can-create-connection

Management - Checks if connection can be created on current scope.

Parameters

accountids	optional	List of Account IDs to filter by. Example: "225494730938493804,225494730938493915".
groupids	optional	List of Group IDs to filter by. Example: "225494730938493804,225494730938493915".
siteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".
tenant	optional	Indicates a tenant scope request

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
data	Response data	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>canCreateConnection</td><td>Cancreateconnection</td><td>true</td><td>boolean</td></tr><tr><td>reason</td><td>Reason</td><td>true</td><td>string</td></tr><tr><td>affectingScopes</td><td>Affectingscopes</td><td>false</td><td><table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>scopeId</td><td></td><td>true</td><td>string</td></tr><tr><td>scopeLevel</td><td></td><td>true</td><td>string</td></tr></table></td></tr></table>
errors	Errors	false	array

Management - Create connector connection

POST /web/api/v2.1/mobile-integration/management/create-connection

Management - Create connector connection.

Response Messages

201 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Body Schema

Name	Description	Required	Value
data	Data	true	

Name	Description	Required	Value
connector	Connector	true	

Name	Description	Required	Value
MicrosoftEndpointManagerConnector	Microsoftendpointmanagerconnector	false	
MobileIronCl	Mobileironcl	false	

Name	Description	Required	Value
auth	Auth	true	
baseUrl	Baseurl	true	string
backgroundSync	Enable background syncing	false	boolean
maskUserInformation	Enable masking user information	false	boolean
mode	Supported mode	false	enum

Name	D
oauth	Oa

						oudConnector	oudconnector		Name / Description / Required / Value auth / Auth / true / Name: basic, D: Ba baseUrl / Baseurl / true / string
						MobileIronCoreConnector	Mobileironcoreconnector	false	Name / Description / Required / Value auth / Auth / true / Name: basic, D: Ba baseUrl / Baseurl / true / string
						WorkspaceOneConnector	Workspaceoneconnector	false	Name / Description / Required / Value auth / Auth / true / Name: basic, D: Ba; Name: certificate, D: Ce baseUrl / Baseurl / true / string
			name	Name	true	string			
			connectionId	Connectionid	false	string			
			defaultS1GroupId	Defaults1groupid	false	string			

<table>
<tr><td></td><td></td><td></td><td>
<table>
<tr><td>deviceGroup Mappings</td><td>Devicegroup mappings</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>mdmGroupId</td><td></td><td>true</td><td>string</td></tr>
<tr><td>s1GroupId</td><td></td><td>true</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>responseGroupIds</td><td>Responsegroupids</td><td>false</td><td>string []</td></tr>
</table>
</td></tr>
<tr><td>filter</td><td>Filter</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>groupIds</td><td>List of Group IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>siteIds</td><td>List of Site IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>tenant</td><td>Indicates a tenant scope request</td><td>false</td><td>boolean</td></tr>
</table>
</td></tr>
</table>

Activations - Create User Activation

POST /web/api/v2.1/mobile-integration/activation/user-activation

Generate bulk of end user links for device registration

Response Messages

201 - Bulk of user activation links created

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - 403 - You do not have authorization to complete request.

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>mgmtGroupId</td><td>Group identifier of a group where new devices will be activated</td><td>true</td><td>string</td></tr>
<tr><td>details</td><td>Details</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>email</td><td>This is the email for the new user and the new user uses it to log into the console.</td><td>true</td><td>string</td></tr>
<tr><td>firstName</td><td>This is the first name that you want for the new user</td><td>true</td><td>string</td></tr>
</table>
</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><td></td><td></td><td></td><td>
<table>
<tr><td></td><td></td><td></td><td>
<table>
<tr><td>lastName</td><td>This is the last name that you want for the new user</td><td>true</td><td>string</td></tr>
<tr><td>activationLimit</td><td>This is the count of how many activations are allowed</td><td>false</td><td>integer</td></tr>
</table>
</td></tr>
</table>
</td></tr>
<tr><td>filter</td><td>Filter</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>groupIds</td><td>List of Group IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>siteIds</td><td>List of Site IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>tenant</td><td>Indicates a tenant scope request</td><td>false</td><td>boolean</td></tr>
</table>
</td></tr>
</table>

Activations - Get list of user activations

GET /web/api/v2.1/mobile-integration/activation/user-activation

Activations - Get list of user activations

Parameters

accountids	optional	List of Account IDs to filter by. Example: "225494730938493804,225494730938493915".
countonly	optional	If true, only total number of items will be returned, without any of the actual objects.
cursor	optional	Cursor position returned by the last request. Use to iterate over more than 1000 items. Example: "YWdlbnRfaWQ6NTgwMjkzODE=".
groupids	optional	List of Group IDs to filter by. Example: "225494730938493804,225494730938493915".
limit	optional	Limit number of returned items (1-1000). Example: "10".
siteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".
skip	optional	Skip first number of items (0-1000). To iterate over more than 1000 items, use "cursor". Example: "150".
skipcount	optional	If true, total number of items will not be calculated, which speeds up execution time.
sortby	optional	The column to sort the results by. Example: "id".
sortorder	optional	Sort direction. Example: "asc".
status__in	optional	Include user activations only with given status. Example: "created".
tenant	optional	Indicates a tenant scope request

Response Messages

200 - Paged list of user activations

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - 403 - You do not have authorization to complete request.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>pagination</td><td>Pagination information</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>totalItems</td><td>Total number of items found matching your query</td><td>true</td><td>integer</td></tr>
<tr><td>nextCursor</td><td>Pass this value as "cursor" on your next request, to get the next page of results (Will be "null" when last page reached)</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>activationCount</td><td>Counter of devices registered through the group activation link</td><td>true</td><td>integer</td></tr>
<tr><td>activationLimit</td><td>This is the number of activations available with this group activation link.</td><td>true</td><td>integer</td></tr>
<tr><td>createdAt</td><td>User invite creation date</td><td>true</td><td>string</td></tr>
<tr><td>createdBy</td><td>Username,</td><td>true</td><td>string</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><td></td><td></td><td></td><td>
<table>
<tr><td></td><td>who sent the invitation</td><td></td><td></td></tr>
<tr><td>email</td><td>User email</td><td>true</td><td>string</td></tr>
<tr><td>id</td><td>User activation identifier</td><td>true</td><td>string</td></tr>
<tr><td>name</td><td>User name</td><td>true</td><td>string</td></tr>
<tr><td>mgmtGroupName</td><td>Name of the group, where a new device is registered</td><td>false</td><td>string</td></tr>
<tr><td>scope</td><td>Scope hierarchy, where the user activation is assigned</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountName</td><td>Accountname</td><td>false</td><td>string</td></tr>
<tr><td>groupName</td><td>Groupname</td><td>false</td><td>string</td></tr>
<tr><td>siteName</td><td>Sitename</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Management - Test connector connection. Deprecated, use create-interim-connection + device-groups instead.

POST /web/api/v2.1/mobile-integration/management/test-connection

Management - Test connector connection. Deprecated, use create-interim-connection + device-groups instead.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>managedGroups</td><td>Managedgroups</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>id</td><td></td><td>true</td><td>string</td></tr>
<tr><td>name</td><td></td><td>true</td><td>string</td></tr>
</table>
</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

Name	Description	Required	Value
data	Data	true	

Name	Description	Required	Value
MicrosoftEndpointManagerConnector	Microsoftendpointmanagerconnector	false	

Name	Description	Required	Value
auth	Auth	true	

Name	Description	Required	Value
oauth	Oauth	false	

Name	D
cloud	Cl
tenantId	Te

Name	Description	Required	Value
baseUrl	Baseurl	true	string
backgroundSync	Enable background syncing	false	boolean
maskUserInformation	Enable masking user information	false	boolean
mode	Supported mode	false	enum

Name	Description	Required	Value
MobileIronCloudConnector	Mobileironcloudconnector	false	

Name	Description	Required	Value
auth	Auth	true	

Name	Description	Required	Value
basic	Basic	true	

Name	D
password	Pa
userId	Us

Name	Description	Required	Value
baseUrl	Baseurl	true	string

Name	Description	Required	Value
MobileIronCoreConnector	Mobileironcoreconnector	false	

Name	Description	Required	Value
auth	Auth	true	

Name	Description	Required	Value
basic	Basic	true	

Name	D
password	Pa
userId	Us

						baseUrl	Baseurl	true	string
			WorkspaceOneConnector	Workspaceoneconnector	false	Name	Description	Required	Value
						auth	Auth	true	Name / Description / Required / Value
									basic / Basic / false / Name / Description / Required / Value
									apiKey / Ap
									password / Pa
									userId / Us
									certificate / Certificate / false / Name / Description / Required / Value
									apiKey / Ap
									certificate / Ce
									passphrase / Pa
						baseUrl	Baseurl	true	string
filter	Filter	true	Name / Description / Required / Value						
			accountIds / List of Account IDs to filter by / false / string []						
			groupIds / List of Group IDs to filter by / false / string []						
			siteIds / List of Site IDs to filter by / false / string []						
			tenant / Indicates a tenant scope request / false / boolean						

Management - Get list of connections for specific scope

GET /web/api/v2.1/mobile-integration/management/connections

Management - Get list of connections for specific scope

Parameters

accountids	optional	List of Account IDs to filter by. Example: "225494730938493804,225494730938493915".
groupids	optional	List of Group IDs to filter by. Example: "225494730938493804,225494730938493915".
siteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".
tenant	optional	Indicates a tenant scope request

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
connectionId	Connectionid	true	string
connector	Connector	true	

Name	Description	Required	Value
MicrosoftEndpointManagerConnector	Microsoftendpointmanagerconnector	false	

Name	Description	Required	Value
auth	Auth	true	

Name	D
oauth	Oa

									baseUrl	Baseurl	true	string	
									backgroundSync	Enable background syncing	false	boolean	
									maskUserInformation	Enable masking user information	false	boolean	
									mode	Supported mode	false	enum	
						MobileIronCloudConnector	Mobileironcloudconnector	false	Name	Description	Required	Value	
									auth	Auth	true	Name	D
												basic	Ba
									baseUrl	Baseurl	true	string	
						MobileIronCoreConnector	Mobileironcoreconnector	false	Name	Description	Required	Value	
									auth	Auth	true	Name	D
												basic	Ba
									baseUrl	Baseurl	true	string	
						WorkspaceOneConnector	Workspaceoneconnector	false	Name	Description	Required	Value	
									auth	Auth	true	Name	D
												basic	Ba

										baseUrl	Baseurl	true	string	
													certificate	Ce
			name	Name	true	string								
			scopeId	Scopeid	true	string								
			scopeLevel	Scopelevel	true	string								
			defaultS1GroupId	Defaults1groupid	false	string								
			details	Details	false	Name	Description	Required	Value					
						lastSyncOn	When the connection sync happened last time	true	string					
						syncStatus	Connection sync status	true	enum					
						syncErrorMessage	Syncerrormessage	false	string					
			deviceGroupMappings	Devicegroupmappings	false	Name	Description	Required	Value					
						mdmGroupId		true	string					
						s1GroupId		true	string					
			responseGroupIds	Responsegroupids	false	string []								
errors	Errors	false	array											

Connectors - Get list of Connectors and their abilities

GET /web/api/v2.1/mobile-integration/management/connectors

Connectors - Get list of Connectors and their abilities

Response Messages

200 - Success

401 - Unauthorized access - please sign in and retry.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>id</td><td>Id</td><td>true</td><td>string</td></tr>
<tr><td>logo</td><td>Logo</td><td>true</td><td>string</td></tr>
<tr><td>azureApps</td><td>Azureapps</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>clientId</td><td></td><td>true</td><td>string</td></tr>
<tr><td>id</td><td></td><td>true</td><td>string</td></tr>
<tr><td>requestUri</td><td></td><td>true</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>supportedModes</td><td>Supportedmodes</td><td>false</td><td>string []</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Management - Get app configuration

GET /web/api/v2.1/mobile-integration/management/app-config

Management - Get app configuration

Parameters

accountids	optional	List of Account IDs to filter by. Example: "225494730938493804,225494730938493915".
groupids	optional	List of Group IDs to filter by. Example: "225494730938493804,225494730938493915".
siteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".
tenant	optional	Indicates a tenant scope request

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

404 - Credentials not found for scope

Response Schema

Name	Description	Required	Value
data	Response data	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>defaultChannel</td><td>Defaultchannel</td><td>true</td><td>string</td></tr><tr><td>tenantId</td><td>Tenantid</td><td>true</td><td>string</td></tr></table>
errors	Errors	false	array

Activations - Generates a global link for anonymous device registration

POST /web/api/v2.1/mobile-integration/activation/anonymous

Activations - Generates a global link for anonymous device registration

Response Messages

201 - Link for anonymous activation was generated and can be shared

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - 403 - You do not have authorization to complete request.

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>activationLimit</td><td>This is the number of activations available with this group activation link.</td><td>true</td><td>integer</td></tr>
<tr><td>description</td><td>This is the description for the group activation</td><td>false</td><td>string</td></tr>
<tr><td>expiryDays</td><td>This is the link expiration days</td><td>false</td><td>integer</td></tr>
<tr><td>mgmtGroupId</td><td>Group identifier of a group where new devices</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
</table>

			will be activated		
			name	This is the name that you want for the group activation. This has to be unique.	false	string
filter	Filter	false	Name	Description	Required	Value
			accountIds	List of Account IDs to filter by	false	string []
			groupIds	List of Group IDs to filter by	false	string []
			siteIds	List of Site IDs to filter by	false	string []
			tenant	Indicates a tenant scope request	false	boolean

Activations - Return anonymous activation in the scope

GET /web/api/v2.1/mobile-integration/activation/anonymous

Activations - Return anonymous activation in the scope

Parameters

accountids	optional	List of Account IDs to filter by. Example: "225494730938493804,225494730938493915".
countonly	optional	If true, only total number of items will be returned, without any of the actual objects.
cursor	optional	Cursor position returned by the last request. Use to iterate over more than 1000 items. Example: "YWdlbnRfaWQ6NTgwMjkzODE=".
groupids	optional	List of Group IDs to filter by. Example: "225494730938493804,225494730938493915".
limit	optional	Limit number of returned items (1-1000). Example: "10".
siteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".
skip	optional	Skip first number of items (0-1000). To iterate over more than 1000 items, use "cursor". Example: "150".
skipcount	optional	If true, total number of items will not be calculated, which speeds up execution time.
sortby	optional	The column to sort the results by. Example: "id".
sortorder	optional	Sort direction. Example: "asc".
tenant	optional	Indicates a tenant scope request

Response Messages

200 - Active links for anonymous activation in the scope

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>pagination</td><td>Pagination information</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>totalItems</td><td>Total number of items found matching your query</td><td>true</td><td>integer</td></tr>
<tr><td>nextCursor</td><td>Pass this value as "cursor" on your next request, to get the next page of results (Will be "null" when last page reached)</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>activationCount</td><td>Counter of devices registered through the group activation link</td><td>true</td><td>integer</td></tr>
<tr><td>activationLimit</td><td>This is the number of activations available with this group activation link.</td><td>true</td><td>integer</td></tr>
<tr><td>activationLink</td><td>Anonymous group link to register devices</td><td>true</td><td>string</td></tr>
<tr><td>createdAt</td><td>Request timestamp</td><td>true</td><td>string</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><td></td><td></td><td></td><td>
<table>
<tr><td>id</td><td>Anonymous activation identifier</td><td>true</td><td>string</td></tr>
<tr><td>createdBy</td><td>Identifier of the user, who created the anonymous activation</td><td>false</td><td>string</td></tr>
<tr><td>linkExpiry</td><td>This is the link expiration date</td><td>false</td><td>string</td></tr>
<tr><td>mgmtGroupName</td><td>Name of the group, where a new device is registered</td><td>false</td><td>string</td></tr>
<tr><td>scope</td><td>Scope hierarchy, where the anonymous activation is assigned</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountName</td><td>Accountname</td><td>false</td><td>string</td></tr>
<tr><td>groupName</td><td>Groupname</td><td>false</td><td>string</td></tr>
<tr><td>siteName</td><td>Sitename</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Incidents - Update analyst verdict

POST /web/api/v2.1/mobile-integration/incidents/analyst-verdict

Incidents - Update analyst verdict

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td><table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>affected</td><td>Affected</td><td>true</td><td>integer</td></tr></table></td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>analystVerdict</td><td>Analystverdict</td><td>true</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>filter</td><td>Filter</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>groupIds</td><td>List of Group IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>ids</td><td>Ids</td><td>false</td><td>integer []</td></tr>
<tr><td>siteIds</td><td>List of Site IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>tenant</td><td>Indicates a tenant scope request</td><td>false</td><td>boolean</td></tr>
</table>
</td></tr>
</table>

Incidents - Update incident status

POST /web/api/v2.1/mobile-integration/incidents/incident-status

Incidents - Update incident status

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td><table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>affected</td><td>Affected</td><td>true</td><td>integer</td></tr></table></td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>incidentStatus</td><td>Incidentstatus</td><td>true</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>filter</td><td>Filter</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>groupIds</td><td>List of Group IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>ids</td><td>Ids</td><td>false</td><td>integer []</td></tr>
<tr><td>siteIds</td><td>List of Site IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>tenant</td><td>Indicates a tenant scope request</td><td>false</td><td>boolean</td></tr>
</table>
</td></tr>
</table>

Policy - Get global mobile policy

GET /web/api/v2.1/mobile-integration/tenant/policy

Policy - Get global mobile policy

Response Messages

200 - Success

401 - Unauthorized access - please sign in and retry.

404 - Policy not found

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
alertOnDeviceAlert	Alertondevice alert	true	string
alerts	Alerts	true	string
default	Default	true	boolean
engines	Engines	true	

Name	Description	Required	Value
appBehaviorallAi	Appbehaviorallai	true	string
appStaticAi	Appstaticai	true	string
networkAnalysis	Networkanalysis	true	string
phishingScanner	Phishingscanner	true	string
systemBehaviorallAi	Systembehaviorallai	true	string
systemStaticAi	Systemstaticai	true	string
vulnerabilityScanner	Vulnerabilityscanner	true	string

			responseActions	Responseactions	true	string
			threatOnDeviceAlert	Threatondevicealert	true	string
			threatPhishingPrevention	Threatphishingprevention	true	string
			threats	Threats	true	string
			updatedAt	Updatedat	true	string
			alertResponseGroupId	Alertresponsegroupid	false	string
			connectionId	Connectionid	false	string
			connectionScopeId	Connectionscopeid	false	string
			connectionScopeLevel	Connectionscopelevel	false	string
			inheritedFrom	Inheritedfrom	false	string
			threatResponseGroupId	Threatresponsegroupid	false	string
			updatedBy	Updatedby	false	string
			userFullName	Userfullname	false	string
errors	Errors	false	array			

Policy - Update global mobile policy

PUT /web/api/v2.1/mobile-integration/tenant/policy

Policy - Update global mobile policy

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

404 - Policy not found

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
alertOnDeviceAlert	Alertondevicealert	true	string
alerts	Alerts	true	string
default	Default	true	boolean
engines	Engines	true	

Name	Description	Required	Value
appBehaviioralAi	Appbehavioralai	true	string
appStaticAi	Appstaticai	true	string
networkAnalysis	Networkanalysis	true	string
phishingScanner	Phishingscanner	true	string
systemBehaviioralAi	Systembehavioralai	true	string
systemStaticAi	Systemstaticai	true	string

						vulnerability Scanner	Vulnerability scanner	true	string
			responseActions	Responseactions	true	string			
			threatOnDeviceAlert	Threatondevicealert	true	string			
			threatPhishingPrevention	Threatphishingprevention	true	string			
			threats	Threats	true	string			
			updatedAt	Updatedat	true	string			
			alertResponseGroupId	Alertresponsegroupid	false	string			
			connectionId	Connectionid	false	string			
			connectionScopeId	Connectionscopeid	false	string			
			connectionScopeLevel	Connectionscopelevel	false	string			
			inheritedFrom	Inheritedfrom	false	string			
			threatResponseGroupId	Threatresponsegroupid	false	string			
			updatedBy	Updatedby	false	string			
			userFullName	Userfullname	false	string			
errors	Errors	false	array						

Body Schema

Name	Description	Required	Value
data	Data	true	

Name	Description	Required	Value
alertOnDeviceAlert	Alertondevicealert	true	string
alerts	Alerts	true	string
engines	Engines	true	

Name	Description	Required	Value
appBehavioralAi	Appbehavioralai	true	string
appStaticAi	Appstaticai	true	string
networkAnalysis	Networkanalysis	true	string
phishingScanner	Phishingscanner	true	string
systemBehavioralAi	Systembehavioralai	true	string
systemStaticAi	Systemstaticai	true	string
vulnerabilityScanner	Vulnerabilityscanner	true	string

Name	Description	Required	Value
threatOnDeviceAlert	Threatondevicealert	true	string
threatPhishingPrevention	Threatphishingprevention	true	string
threats	Threats	true	string
alertResponseGroupId	Alertresponsegroupid	false	string
threatResponseGroupId	Threatresponsegroupid	false	string

Name	Description	Required	Value
filter	Filter	false	

Name	Description	Required	Value
accountIds	List of Account IDs to filter by	false	string []
groupIds	List of Group	false	string []

				IDs to filter by			
			siteIds	List of Site IDs to filter by	false	string []	
			tenant	Indicates a tenant scope request	false	boolean	

Policy - Delete global mobile policy

DELETE /web/api/v2.1/mobile-integration/tenant/policy

Policy - Delete global mobile policy

Response Messages

204 - Success

401 - Unauthorized access - please sign in and retry.

404 - Policy not found

Incidents - Get list of incidents

GET /web/api/v2.1/mobile-integration/incidents

Incidents - Get list of incidents

Parameters

accountids	optional	List of Account IDs to filter by. Example: "225494730938493804,225494730938493915".
analystverdict__in	optional	Include incident only of given analyst verdicts. Example: "true_positive".
countonly	optional	If true, only total number of items will be returned, without any of the actual objects.
cursor	optional	Cursor position returned by the last request. Use to iterate over more than 1000 items. Example: "YWdlbnRfaWQ6NTgwMjkzODE=".
deviceid__contains	optional	Include incidents by device IDs that contain text
deviceid__in	optional	Include incidents only of given device ids. Example: "a,b,c,-,1,2,3,-,4,5,6".
groupids	optional	List of Group IDs to filter by. Example: "225494730938493804,225494730938493915".

incidentstatus__in	optional	Include incident only of given incident statuses. Example: "unresolved".
kind__in	optional	Include incidents only of given kinds. Example: "t,h,r,e,a,t".
limit	optional	Limit number of returned items (1-1000). Example: "10".
severity__in	optional	Include incident only of given severities. Example: "low".
siteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".
skip	optional	Skip first number of items (0-1000). To iterate over more than 1000 items, use "cursor". Example: "150".
skipcount	optional	If true, total number of items will not be calculated, which speeds up execution time.
sortby	optional	The column to sort the results by. Example: "id".
sortorder	optional	Sort direction. Example: "asc".
status__in	optional	Include incident only of given statuses. Example: "not_mitigated".
statusaction__in	optional	Include incident only of given status actions. Example: "conditional_access".
tenant	optional	Indicates a tenant scope request
user__contains	optional	Include incidents by user email that contain text

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
pagination	Pagination information	true	

Name	Description	Required	Value
totalItems	Total number of items found matching	true	integer

				your query		
			nextCursor	Pass this value as "cursor" on your next request, to get the next page of results (Will be "null" when last page reached)	false	string
data	Response data	false	accountId	A reference to the containing account	true	string
			accountName	Name of the containing account	true	string
			analystVerdict	Analystverdict	true	string
			description	Description	true	string
			details	Details	true	

Name	Description	Required	Value
applicationDeveloper	Applicationdeveloper	true	string
applicationName	Applicationname	true	string
applicationPackage	Applicationpackage	true	string
deviceTime	Devicetime	true	string
fileHash	Filehash	true	string
fileName	Filename	true	string
installerSource	Installersource	true	string
malwareThre	Malwarethre	true	string

						atName networkInterface processName routerBSSID routerSSID suspectedUrl
						atname Networkinterface Processname Routerbssid Routerssid Suspectedurl
						 true true true true true
						 string string string string string
			detectionEngine	Detectionengine	true	string
			detectionType	Detectiontype	true	string
			deviceId	Deviceid	true	string
			groupId	A reference to the containing network group	true	string
			groupName	Name of the containing network group	true	string
			id	Id	true	integer
			incidentStatus	Incidentstatus	true	string
			investigation	Investigation	true	string
			kind	Kind	true	string
			osType	Ostype	true	string
			osVersion	Osversion	true	string
			remediationStep	Remediationstep	true	string
			reportedTime	Reportedtime	true	string
			severity	Severity	true	string
			siteId	A reference to the containing site	true	string

<table>
<tr><td></td><td></td><td></td><td>
<table>
<tr><td>siteName</td><td>Name of the containing site</td><td>true</td><td>string</td></tr>
<tr><td>status</td><td>Status</td><td>true</td><td>string</td></tr>
<tr><td>statusAction</td><td>Statusaction</td><td>true</td><td>string</td></tr>
<tr><td>trackingId1</td><td>Trackingid1</td><td>true</td><td>string</td></tr>
<tr><td>trackingId2</td><td>Trackingid2</td><td>true</td><td>string</td></tr>
<tr><td>type</td><td>Type</td><td>true</td><td>string</td></tr>
<tr><td>userEmail</td><td>Useremail</td><td>true</td><td>string</td></tr>
<tr><td>userNotified</td><td>Usernotified</td><td>true</td><td>boolean</td></tr>
<tr><td>detail</td><td>Detail</td><td>false</td><td>string</td></tr>
<tr><td>network</td><td>Network</td><td>false</td><td>string</td></tr>
<tr><td>notes</td><td>Notes</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>author</td><td></td><td>true</td><td>string</td></tr>
<tr><td>authorId</td><td></td><td>true</td><td>string</td></tr>
<tr><td>createdAt</td><td></td><td>true</td><td>string</td></tr>
<tr><td>edited</td><td></td><td>true</td><td>boolean</td></tr>
<tr><td>id</td><td></td><td>true</td><td>integer</td></tr>
<tr><td>text</td><td></td><td>true</td><td>string</td></tr>
<tr><td>updatedAt</td><td></td><td>true</td><td>string</td></tr>
</table>
</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Devices - Get list of devices for specific scope

GET /web/api/v2.1/mobile-integration/devices

Devices - Get list devices for specific scope

Parameters

accountids	optional	List of Account IDs to filter by. Example: "225494730938493804,225494730938493915".
appversion__in	optional	Include devices with given app versions. Example: "2.5.1.1320".
countonly	optional	If true, only total number of items will be returned, without any of the actual objects.
cursor	optional	Cursor position returned by the last request. Use to iterate over more than 1000 items. Example: "YWdlbnRfaWQ6NTgwMjkzODE=".
deviceid__contains	optional	Include devices by device IDs that contain text
groupids	optional	List of Group IDs to filter by. Example: "225494730938493804,225494730938493915".
healthstate__in	optional	Include devices only with given health state. Example: "normal".
limit	optional	Limit number of returned items (1-1000). Example: "10".
model__contains	optional	Include devices by models that contain text
osversion__contains	optional	Include devices by os version that contain text
platform__in	optional	Include devices only of given platforms. Example: "android".
privileges__in	optional	Include devices only with given privileges. Example: "none".
siteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".
skip	optional	Skip first number of items (0-1000). To iterate over more than 1000 items, use "cursor". Example: "150".
skipcount	optional	If true, total number of items will not be calculated, which speeds up execution time.
sortby	optional	The column to sort the results by. Example: "id".
sortorder	optional	Sort direction. Example: "asc".
tenant	optional	Indicates a tenant scope request

trackingid1__contains	optional	Include devices by external tracking IDs that contain text
trackingid2__contains	optional	Include devices by another external tracking IDs that contain text
user__contains	optional	Include devices by users that contain text

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
pagination	Pagination information	true	
data	Response data	false	

Name	Description	Required	Value
totalItems	Total number of items found matching your query	true	integer
nextCursor	Pass this value as "cursor" on your next request, to get the next page of results (Will be "null" when last page reached)	false	string

Name	Description	Required	Value
accountId	A reference to the containing account	true	string
accountName	Name of the	true	string

				containing account		
			alertCounts	Alertcounts	true	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>adminResolvedCount</td><td>How many threats are resolved by admin</td><td>true</td><td>integer</td></tr><tr><td>conditionalAccessCount</td><td>How many threats is in conditional access</td><td>true</td><td>integer</td></tr><tr><td>mitigatedCount</td><td>How many threats are mitigated</td><td>true</td><td>integer</td></tr><tr><td>notMitigatedCount</td><td>How many threats are not mitigated</td><td>true</td><td>integer</td></tr></table>
			deviceId	MDM device ID	true	string
			groupId	A reference to the containing network group	true	string
			groupName	Name of the containing network group	true	string
			id	Id	true	integer
			registrationSource	MDM name or initiator in case of activations	true	string
			registrationType	Registration type	true	enum
			siteId	A reference to the containing site	true	string

			siteName	Name of the containing site	true	string
			threatCounts	Threatcounts	true	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>adminResolvedCount</td><td>How many threats are resolved by admin</td><td>true</td><td>integer</td></tr><tr><td>conditionalAccessCount</td><td>How many threats is in conditional access</td><td>true</td><td>integer</td></tr><tr><td>mitigatedCount</td><td>How many threats are mitigated</td><td>true</td><td>integer</td></tr><tr><td>notMitigatedCount</td><td>How many threats are not mitigated</td><td>true</td><td>integer</td></tr></table>
			appState	ZipApp state	false	enum
			appVersion	Version of the ZippApp	false	string
			debugMode	Debugmode	false	boolean
			developerMode	Developermode	false	boolean
			encrypted	Encrypted	false	boolean
			healthState	Highest health state of the device	false	enum
			lastActiveOn	When we received last heartbeat	false	string
			managedState	UEM state of the device	false	enum
			model	Device manufacturer and model	false	string
			osVersion	Device os version	false	string

			owner: User email; false; string platform: Device platform; false; enum policyUpdatedAt: When the corresponding policy was updated; false; string privileges: Either rooted or jailbroken for devices with privileges. Otherwise none; false; enum protected: Protected; false; boolean registeredOn: When the ZippApp registered; false; string registrationDate: When the activation for this device was created; false; string screenLocked: Screenlocked; false; boolean stagefreightVulnerable: Stagefreightvulnerable; false; boolean trackingId1: External tracking ID of device; false; string trackingId2: Another external tracking ID of device; false; string unofficialAppstore: Unofficialappstore; false; boolean
errors	Errors	false	array

Policy - Create mobile policy

POST /web/api/v2.1/mobile-integration/policy

Policy - Create mobile policy

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

404 - Policy not found

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
alertOnDeviceAlert	Alertondevice alert	true	string
alerts	Alerts	true	string
default	Default	true	boolean
engines	Engines	true	

Name	Description	Required	Value
appBehaviorallAi	Appbehaviorallai	true	string
appStaticAi	Appstaticai	true	string
networkAnalysis	Networkanalysis	true	string
phishingScanner	Phishingscanner	true	string
systemBehaviorallAi	Systembehaviorallai	true	string
systemStaticAi	Systemstaticai	true	string

						vulnerabilityScanner	Vulnerabilityscanner	true	string
			responseActions	Responseactions	true	string			
			threatOnDeviceAlert	Threatondevicealert	true	string			
			threatPhishingPrevention	Threatphishingprevention	true	string			
			threats	Threats	true	string			
			updatedAt	Updatedat	true	string			
			alertResponseGroupId	Alertresponsegroupid	false	string			
			connectionId	Connectionid	false	string			
			connectionScopeId	Connectionscopeid	false	string			
			connectionScopeLevel	Connectionscopelevel	false	string			
			inheritedFrom	Inheritedfrom	false	string			
			threatResponseGroupId	Threatresponsegroupid	false	string			
			updatedBy	Updatedby	false	string			
			userFullName	Userfullname	false	string			
errors	Errors	false	array						

Body Schema

Name	Description	Required	Value
data	Data	true	

Name	Description	Required	Value
alertOnDeviceAlert	Alertondevicealert	true	string
alerts	Alerts	true	string
engines	Engines	true	

Name	Description	Required	Value
appBehavioralAi	Appbehavioralai	true	string
appStaticAi	Appstaticai	true	string
networkAnalysis	Networkanalysis	true	string
phishingScanner	Phishingscanner	true	string
systemBehavioralAi	Systembehavioralai	true	string
systemStaticAi	Systemstaticai	true	string
vulnerabilityScanner	Vulnerabilityscanner	true	string

Name	Description	Required	Value
threatOnDeviceAlert	Threatondevicealert	true	string
threatPhishingPrevention	Threatphishingprevention	true	string
threats	Threats	true	string
alertResponseGroupId	Alertresponsegroupid	false	string
threatResponseGroupId	Threatresponsegroupid	false	string

Name	Description	Required	Value
filter	Filter	false	

Name	Description	Required	Value
accountIds	List of Account IDs to filter by	false	string []
groupIds	List of Group	false	string []

				IDs to filter by			
			siteIds	List of Site IDs to filter by	false	string []	
			tenant	Indicates a tenant scope request	false	boolean	

Management - Get managed groups for connection

GET /web/api/v2.1/mobile-integration/management/connections/{conn_id}/managed-groups

Management - Get managed groups for connection

Parameters

accountids	optional	List of Account IDs to filter by. Example: "225494730938493804,225494730938493915".
groupids	optional	List of Group IDs to filter by. Example: "225494730938493804,225494730938493915".
siteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".
tenant	optional	Indicates a tenant scope request

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
data	Response data	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>managedGroups</td><td>Managedgroups</td><td>false</td><td><table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>id</td><td></td><td>true</td><td>string</td></tr><tr><td>name</td><td></td><td>true</td><td>string</td></tr></table></td></tr></table>
errors	Errors	false	array

Management - Get all UEM device groups for given connection

GET /web/api/v2.1/mobile-integration/management/connections/{conn_id}/device-groups

Management - Get all UEM device groups for given connection

Parameters

accountids	optional	List of Account IDs to filter by. Example: "225494730938493804,225494730938493915".
countonly	optional	If true, only total number of items will be returned, without any of the actual objects.
cursor	optional	Cursor position returned by the last request. Use to iterate over more than 1000 items. Example: "YWdlbnRfaWQ6NTgwMjkzODE=".
groupids	optional	List of Group IDs to filter by. Example: "225494730938493804,225494730938493915".
limit	optional	Limit number of returned items (1-1000). Example: "10".
query	optional	Search for groups with names containing this value
siteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".
skip	optional	Skip first number of items (0-1000). To iterate over more than 1000 items, use "cursor". Example: "150".
skipcount	optional	If true, total number of items will not be calculated, which speeds up execution time.
sortby	optional	The column to sort the results by. Example: "id".
sortorder	optional	Sort direction. Example: "asc".
tenant	optional	Indicates a tenant scope request

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>pagination</td><td>Pagination information</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>totalItems</td><td>Total number of items found matching your query</td><td>true</td><td>integer</td></tr>
<tr><td>nextCursor</td><td>Pass this value as "cursor" on your next request, to get the next page of results (Will be "null" when last page reached)</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>id</td><td>Id</td><td>true</td><td>string</td></tr>
<tr><td>name</td><td>Name</td><td>true</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Management - Sync devices under connection

POST /web/api/v2.1/mobile-integration/management/connections/{connection_id}/sync-devices

Management - Sync devices under connection

Response Messages

204 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Body Schema

Name	Description	Required	Value
filter	Filter	true	

Name	Description	Required	Value
accountIds	List of Account IDs to filter by	false	string []
groupIds	List of Group IDs to filter by	false	string []
siteIds	List of Site IDs to filter by	false	string []
tenant	Indicates a tenant scope request	false	boolean

Management - Patch connection group mappings

PUT /web/api/v2.1/mobile-integration/management/connections/{connection_id}/groups

Management - Patch connection group mappings

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

404 - Connection not found

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>defaultS1GroupId</td><td>Defaults1groupid</td><td>false</td><td>string</td></tr>
<tr><td>deviceGroupMappings</td><td>Devicegroup mappings</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>mdmGroupId</td><td></td><td>true</td><td>string</td></tr>
<tr><td>s1GroupId</td><td></td><td>true</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>responseGroupIds</td><td>Responsegroupids</td><td>false</td><td>string []</td></tr>
</table>
</td></tr>
<tr><td>filter</td><td>Filter</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>groupIds</td><td>List of Group IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>siteIds</td><td>List of Site IDs to filter</td><td>false</td><td>string []</td></tr>
</table>
</td></tr>
</table>

				by			
			tenant	Indicates a tenant scope request	false	boolean	

Deletes MSSP partner key by client ID

DELETE /web/api/v2.1/mobile-integration/provisioning/partner-key/{client_id}

Provision - Delete MSSP partner key

Response Messages

204 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

404 - Partner key not found

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>filter</td><td>Filter</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>groupIds</td><td>List of Group IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>siteIds</td><td>List of Site IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>tenant</td><td>Indicates a tenant scope request</td><td>false</td><td>boolean</td></tr>
</table>
</td></tr>
</table>

Management - Update connector connection

PUT /web/api/v2.1/mobile-integration/management/connections/{connection_id}

Management - Update connector connection.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

404 - Connection not found

Body Schema

Name	Description	Required	Value
data	Data	true	

Name	Description	Required	Value
connector	Connector	true	

Name	Description	Required	Value
MicrosoftEndpointManagerConnector	Microsoftendpointmanagerconnector	false	

Name	Description	Required	Value
auth	Auth	true	
baseUrl	Baseurl	true	string
backgroundSync	Enable background syncing	false	boolean
maskUserInformation	Enable masking user information	false	boolean
mode	Supported	false	enum

Name	D
oauth	Oa

											mode	
						MobileIronCloudConnector	Mobileironcloudconnector	false	Name	Description	Required	Value
									auth	Auth	true	Name: basic; D: Ba
									baseUrl	Baseurl	true	string
						MobileIronCoreConnector	Mobileironcoreconnector	false	Name	Description	Required	Value
									auth	Auth	true	Name: basic; D: Ba
									baseUrl	Baseurl	true	string
						WorkspaceOneConnector	Workspaceoneconnector	false	Name	Description	Required	Value
									auth	Auth	true	Name: basic; D: Ba Name: certificate; D: Ce
									baseUrl	Baseurl	true	string
			name	Name	true	string						
			defaultS1Gro	Defaults1gro	false	string						

<table>
<tr><td></td><td></td><td></td><td>
<table>
<tr><td>upId</td><td>upid</td><td></td><td></td></tr>
<tr><td>deviceGroup Mappings</td><td>Devicegroup mappings</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>mdmGroupId</td><td></td><td>true</td><td>string</td></tr>
<tr><td>s1GroupId</td><td></td><td>true</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>responseGroupIds</td><td>Responsegroupids</td><td>false</td><td>string []</td></tr>
</table>
</td></tr>
<tr><td>filter</td><td>Filter</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>groupIds</td><td>List of Group IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>siteIds</td><td>List of Site IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>tenant</td><td>Indicates a tenant scope request</td><td>false</td><td>boolean</td></tr>
</table>
</td></tr>
</table>

Management - Delete connection

DELETE /web/api/v2.1/mobile-integration/management/connections/{connection_id}

Management - Delete connection

Response Messages

204 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Body Schema

Name	Description	Required	Value
filter	Filter	true	

Name	Description	Required	Value
accountIds	List of Account IDs to filter by	false	string []
groupIds	List of Group IDs to filter by	false	string []
siteIds	List of Site IDs to filter by	false	string []
tenant	Indicates a tenant scope request	false	boolean

Incidents - Mitigate incident

POST /web/api/v2.1/mobile-integration/incidents/mitigate/{mitigation_action}

Incidents - Mitigate incident

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td><table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>affected</td><td>Affected</td><td>true</td><td>integer</td></tr></table></td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

Name	Description	Required	Value
filter	Filter	true	

Name	Description	Required	Value
accountIds	List of Account IDs to filter by	false	string []
groupIds	List of Group IDs to filter by	false	string []
ids	Ids	false	integer []
siteIds	List of Site IDs to filter by	false	string []
tenant	Indicates a tenant scope request	false	boolean

Incidents - Update incident note

PUT /web/api/v2.1/mobile-integration/incidents/{incident_id}/notes/{note_id}

Incidents - Update incident note

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
data	Response data	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>author</td><td>Author</td><td>true</td><td>string</td></tr><tr><td>authorId</td><td>Authorid</td><td>true</td><td>string</td></tr><tr><td>createdAt</td><td>Createdat</td><td>true</td><td>string</td></tr><tr><td>edited</td><td>Edited</td><td>true</td><td>boolean</td></tr><tr><td>id</td><td>Id</td><td>true</td><td>integer</td></tr><tr><td>text</td><td>Text</td><td>true</td><td>string</td></tr><tr><td>updatedAt</td><td>Updatedat</td><td>true</td><td>string</td></tr></table>
errors	Errors	false	array

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>text</td><td>Text field</td><td>true</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>filter</td><td>Filter</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>groupIds</td><td>List of Group IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>siteIds</td><td>List of Site IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>tenant</td><td>Indicates a tenant scope request</td><td>false</td><td>boolean</td></tr>
</table>
</td></tr>
</table>

Incidents - Delete incident note

DELETE /web/api/v2.1/mobile-integration/incidents/{incident_id}/notes/{note_id}

Incidents - Delete incident note

Response Messages

204 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Body Schema

Name	Description	Required	Value
filter	Filter	true	

Name	Description	Required	Value
accountIds	List of Account IDs to filter by	false	string []
groupIds	List of Group IDs to filter by	false	string []
siteIds	List of Site IDs to filter by	false	string []
tenant	Indicates a tenant scope request	false	boolean

Incidents - Create incident note

POST /web/api/v2.1/mobile-integration/incidents/{incident_id}/notes

Incidents - Create incident note

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
data	Response data	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>author</td><td>Author</td><td>true</td><td>string</td></tr><tr><td>authorId</td><td>Authorid</td><td>true</td><td>string</td></tr><tr><td>createdAt</td><td>Createdat</td><td>true</td><td>string</td></tr><tr><td>edited</td><td>Edited</td><td>true</td><td>boolean</td></tr><tr><td>id</td><td>Id</td><td>true</td><td>integer</td></tr><tr><td>text</td><td>Text</td><td>true</td><td>string</td></tr><tr><td>updatedAt</td><td>Updatedat</td><td>true</td><td>string</td></tr></table>
errors	Errors	false	array

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>text</td><td>Text field</td><td>true</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>filter</td><td>Filter</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>groupIds</td><td>List of Group IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>siteIds</td><td>List of Site IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>tenant</td><td>Indicates a tenant scope request</td><td>false</td><td>boolean</td></tr>
</table>
</td></tr>
</table>

Policy - Get the policy for the Account given by ID

GET /web/api/v2.1/mobile-integration/accounts/{account_id}/policy

Policy - Get the policy for the Account given by ID

Response Messages

200 - Success

401 - Unauthorized access - please sign in and retry.

404 - Policy not found

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
alertOnDeviceAlert	Alertondevice alert	true	string
alerts	Alerts	true	string
default	Default	true	boolean
engines	Engines	true	

Name	Description	Required	Value
appBehaviorallAi	Appbehaviorallai	true	string
appStaticAi	Appstaticai	true	string
networkAnalysis	Networkanalysis	true	string
phishingScanner	Phishingscanner	true	string
systemBehaviorallAi	Systembehaviorallai	true	string
systemStaticAi	Systemstaticai	true	string
vulnerabilityScanner	Vulnerabilityscanner	true	string

			responseActions | Responseactions | true | string threatOnDeviceAlert | Threatondevicealert | true | string threatPhishingPrevention | Threatphishingprevention | true | string threats | Threats | true | string updatedAt | Updatedat | true | string alertResponseGroupId | Alertresponsegroupid | false | string connectionId | Connectionid | false | string connectionScopeId | Connectionscopeid | false | string connectionScopeLevel | Connectionscopelevel | false | string inheritedFrom | Inheritedfrom | false | string threatResponseGroupId | Threatresponsegroupid | false | string updatedBy | Updatedby | false | string userFullName | Userfullname | false | string
errors	Errors	false	array

Policy - Update the policy for the Account given by ID

PUT /web/api/v2.1/mobile-integration/accounts/{account_id}/policy

Policy - Update the policy for the Account given by ID

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

404 - Policy not found

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>alertOnDeviceAlert</td><td>Alertondevicealert</td><td>true</td><td>string</td></tr>
<tr><td>alerts</td><td>Alerts</td><td>true</td><td>string</td></tr>
<tr><td>default</td><td>Default</td><td>true</td><td>boolean</td></tr>
<tr><td>engines</td><td>Engines</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>appBehaviorallAi</td><td>Appbehaviorallai</td><td>true</td><td>string</td></tr>
<tr><td>appStaticAi</td><td>Appstaticai</td><td>true</td><td>string</td></tr>
<tr><td>networkAnalysis</td><td>Networkanalysis</td><td>true</td><td>string</td></tr>
<tr><td>phishingScanner</td><td>Phishingscanner</td><td>true</td><td>string</td></tr>
<tr><td>systemBehavioralAi</td><td>Systembehavioralai</td><td>true</td><td>string</td></tr>
<tr><td>systemStaticAi</td><td>Systemstaticai</td><td>true</td><td>string</td></tr>
</table>
</td></tr>
</table>
</td></tr>
</table>

						vulnerabilityScanner | Vulnerabilityscanner | true | string
			responseActions	Responseactions	true	string
			threatOnDeviceAlert	Threatondevicealert	true	string
			threatPhishingPrevention	Threatphishingprevention	true	string
			threats	Threats	true	string
			updatedAt	Updatedat	true	string
			alertResponseGroupId	Alertresponsegroupid	false	string
			connectionId	Connectionid	false	string
			connectionScopeId	Connectionscopeid	false	string
			connectionScopeLevel	Connectionscopelevel	false	string
			inheritedFrom	Inheritedfrom	false	string
			threatResponseGroupId	Threatresponsegroupid	false	string
			updatedBy	Updatedby	false	string
			userFullName	Userfullname	false	string
errors	Errors	false	array			

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>alertOnDeviceAlert</td><td>Alertondevice alert</td><td>true</td><td>string</td></tr>
<tr><td>alerts</td><td>Alerts</td><td>true</td><td>string</td></tr>
<tr><td>engines</td><td>Engines</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>appBehaviorallAi</td><td>Appbehavioralai</td><td>true</td><td>string</td></tr>
<tr><td>appStaticAi</td><td>Appstaticai</td><td>true</td><td>string</td></tr>
<tr><td>networkAnalysis</td><td>Networkanalysis</td><td>true</td><td>string</td></tr>
<tr><td>phishingScanner</td><td>Phishingscanner</td><td>true</td><td>string</td></tr>
<tr><td>systemBehavioralAi</td><td>Systembehavioralai</td><td>true</td><td>string</td></tr>
<tr><td>systemStaticAi</td><td>Systemstaticai</td><td>true</td><td>string</td></tr>
<tr><td>vulnerabilityScanner</td><td>Vulnerabilityscanner</td><td>true</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>threatOnDeviceAlert</td><td>Threatondevicealert</td><td>true</td><td>string</td></tr>
<tr><td>threatPhishingPrevention</td><td>Threatphishingprevention</td><td>true</td><td>string</td></tr>
<tr><td>threats</td><td>Threats</td><td>true</td><td>string</td></tr>
<tr><td>alertResponseGroupId</td><td>Alertresponsegroupid</td><td>false</td><td>string</td></tr>
<tr><td>threatResponseGroupId</td><td>Threatresponsegroupid</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>filter</td><td>Filter</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>groupIds</td><td>List of Group</td><td>false</td><td>string []</td></tr>
</table>
</td></tr>
</table>

				IDs to filter by			
			siteIds	List of Site IDs to filter by	false	string []	
			tenant	Indicates a tenant scope request	false	boolean	

Policy - Delete the policy for the Account given by ID

DELETE /web/api/v2.1/mobile-integration/accounts/{account_id}/policy

Policy - Delete the policy for the Account given by ID

Response Messages

200 - Success

401 - Unauthorized access - please sign in and retry.

404 - Policy not found

Policy - Get the policy for the Site given by ID

GET /web/api/v2.1/mobile-integration/sites/{site_id}/policy

Policy - Get the policy for the Site given by ID

Response Messages

200 - Success

401 - Unauthorized access - please sign in and retry.

404 - Policy not found

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
alertOnDeviceAlert	Alertondevice alert	true	string
alerts	Alerts	true	string
default	Default	true	boolean

			engines	Engines	true	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>appBehaviorallAi</td><td>Appbehavioralai</td><td>true</td><td>string</td></tr><tr><td>appStaticAi</td><td>Appstaticai</td><td>true</td><td>string</td></tr><tr><td>networkAnalysis</td><td>Networkanalysis</td><td>true</td><td>string</td></tr><tr><td>phishingScanner</td><td>Phishingscanner</td><td>true</td><td>string</td></tr><tr><td>systemBehaviorralAi</td><td>Systembehavioralai</td><td>true</td><td>string</td></tr><tr><td>systemStaticAi</td><td>Systemstaticai</td><td>true</td><td>string</td></tr><tr><td>vulnerabilityScanner</td><td>Vulnerabilityscanner</td><td>true</td><td>string</td></tr></table>
			responseActions	Responseactions	true	string
			threatOnDeviceAlert	Threatondevicealert	true	string
			threatPhishingPrevention	Threatphishingprevention	true	string
			threats	Threats	true	string
			updatedAt	Updatedat	true	string
			alertResponseGroupId	Alertresponsegroupid	false	string
			connectionId	Connectionid	false	string
			connectionScopeId	Connectionscopeid	false	string
			connectionScopeLevel	Connectionscopelevel	false	string
			inheritedFrom	Inheritedfrom	false	string
			threatResponseGroupId	Threatresponsegroupid	false	string
			updatedBy	Updatedby	false	string
			userFullName	Userfullname	false	string

errors	Errors	false	array

Policy - Update the policy for the Group given by ID

PUT /web/api/v2.1/mobile-integration/groups/{group_id}/policy

Policy - Update the policy for the Group given by ID

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

404 - Policy not found

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
alertOnDeviceAlert	Alertondevicealert	true	string
alerts	Alerts	true	string
default	Default	true	boolean
engines	Engines	true	

Name	Description	Required	Value
appBehaviioralAi	Appbehavioralai	true	string
appStaticAi	Appstaticai	true	string
networkAnalysis	Networkanalysis	true	string
phishingScanner	Phishingscanner	true	string
systemBehaviioralAi	Systembehavioralai	true	string
systemStaticAi	Systemstaticai	true	string

						vulnerabilityScanner | Vulnerabilityscanner | true | string
			responseActions	Responseactions	true	string
			threatOnDeviceAlert	Threatondevicealert	true	string
			threatPhishingPrevention	Threatphishingprevention	true	string
			threats	Threats	true	string
			updatedAt	Updatedat	true	string
			alertResponseGroupId	Alertresponsegroupid	false	string
			connectionId	Connectionid	false	string
			connectionScopeId	Connectionscopeid	false	string
			connectionScopeLevel	Connectionscopelevel	false	string
			inheritedFrom	Inheritedfrom	false	string
			threatResponseGroupId	Threatresponsegroupid	false	string
			updatedBy	Updatedby	false	string
			userFullName	Userfullname	false	string
errors	Errors	false	array			

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>alertOnDeviceAlert</td><td>Alertondevice alert</td><td>true</td><td>string</td></tr>
<tr><td>alerts</td><td>Alerts</td><td>true</td><td>string</td></tr>
<tr><td>engines</td><td>Engines</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>appBehaviorallAi</td><td>Appbehavioralai</td><td>true</td><td>string</td></tr>
<tr><td>appStaticAi</td><td>Appstaticai</td><td>true</td><td>string</td></tr>
<tr><td>networkAnalysis</td><td>Networkanalysis</td><td>true</td><td>string</td></tr>
<tr><td>phishingScanner</td><td>Phishingscanner</td><td>true</td><td>string</td></tr>
<tr><td>systemBehaviorralAi</td><td>Systembehavioralai</td><td>true</td><td>string</td></tr>
<tr><td>systemStaticAi</td><td>Systemstaticai</td><td>true</td><td>string</td></tr>
<tr><td>vulnerabilityScanner</td><td>Vulnerabilityscanner</td><td>true</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>threatOnDeviceAlert</td><td>Threatondevicealert</td><td>true</td><td>string</td></tr>
<tr><td>threatPhishingPrevention</td><td>Threatphishingprevention</td><td>true</td><td>string</td></tr>
<tr><td>threats</td><td>Threats</td><td>true</td><td>string</td></tr>
<tr><td>alertResponseGroupId</td><td>Alertresponsegroupid</td><td>false</td><td>string</td></tr>
<tr><td>threatResponseGroupId</td><td>Threatresponsegroupid</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>filter</td><td>Filter</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>groupIds</td><td>List of Group</td><td>false</td><td>string []</td></tr>
</table>
</td></tr>
</table>

				IDs to filter by			
			siteIds	List of Site IDs to filter by	false	string []	
			tenant	Indicates a tenant scope request	false	boolean	

Policy - Delete the policy for the Site given by ID

DELETE /web/api/v2.1/mobile-integration/sites/{site_id}/policy

Policy - Delete the policy for the Site given by ID

Response Messages

200 - Success

401 - Unauthorized access - please sign in and retry.

404 - Policy not found

Policy - Update the policy for the Site given by ID

PUT /web/api/v2.1/mobile-integration/sites/{site_id}/policy

Policy - Update the policy for the Site given by ID

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

404 - Policy not found

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
alertOnDeviceAlert	Alertondevice alert	true	string
alerts	Alerts	true	string

			default	Default	true	boolean
			engines	Engines	true	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>appBehavioralAi</td><td>Appbehavioralai</td><td>true</td><td>string</td></tr><tr><td>appStaticAi</td><td>Appstaticai</td><td>true</td><td>string</td></tr><tr><td>networkAnalysis</td><td>Networkanalysis</td><td>true</td><td>string</td></tr><tr><td>phishingScanner</td><td>Phishingscanner</td><td>true</td><td>string</td></tr><tr><td>systemBehavioralAi</td><td>Systembehavioralai</td><td>true</td><td>string</td></tr><tr><td>systemStaticAi</td><td>Systemstaticai</td><td>true</td><td>string</td></tr><tr><td>vulnerabilityScanner</td><td>Vulnerabilityscanner</td><td>true</td><td>string</td></tr></table>
			responseActions	Responseactions	true	string
			threatOnDeviceAlert	Threatondevicealert	true	string
			threatPhishingPrevention	Threatphishingprevention	true	string
			threats	Threats	true	string
			updatedAt	Updatedat	true	string
			alertResponseGroupId	Alertresponsegroupid	false	string
			connectionId	Connectionid	false	string
			connectionScopeId	Connectionscopeid	false	string
			connectionScopeLevel	Connectionscopelevel	false	string
			inheritedFrom	Inheritedfrom	false	string
			threatResponseGroupId	Threatresponsegroupid	false	string
			updatedBy	Updatedby	false	string
			userFullName	Userfullname	false	string

errors	Errors	false	array

Body Schema

Name	Description	Required	Value
data	Data	true	

Name	Description	Required	Value
alertOnDeviceAlert	Alertondevicealert	true	string
alerts	Alerts	true	string
engines	Engines	true	

Name	Description	Required	Value
appBehavioralAi	Appbehavioralai	true	string
appStaticAi	Appstaticai	true	string
networkAnalysis	Networkanalysis	true	string
phishingScanner	Phishingscanner	true	string
systemBehavioralAi	Systembehavioralai	true	string
systemStaticAi	Systemstaticai	true	string
vulnerabilityScanner	Vulnerabilityscanner	true	string

Name	Description	Required	Value
threatOnDeviceAlert	Threatondevicealert	true	string
threatPhishingPrevention	Threatphishingprevention	true	string
threats	Threats	true	string
alertResponseGroupId	Alertresponsegroupid	false	string
threatResponseGroupId	Threatresponsegroupid	false	string

Name	Description	Required	Value
filter	Filter	false	

Name	Description	Required	Value
accountIds	List of Account IDs to filter by	false	string []
groupIds	List of Group	false	string []

				IDs to filter by			
			siteIds	List of Site IDs to filter by	false	string []	
			tenant	Indicates a tenant scope request	false	boolean	

Devices - Get device details by device id

GET /web/api/v2.1/mobile-integration/devices/{device_id}

Devices - Get device details by device id

Parameters

accountids	optional	List of Account IDs to filter by. Example: "225494730938493804,225494730938493915".
groupids	optional	List of Group IDs to filter by. Example: "225494730938493804,225494730938493915".
siteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".
tenant	optional	Indicates a tenant scope request

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

404 - Device not found

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
accountId	A reference to the containing account	true	string
accountName	Name of the containing account	true	string
alertCounts	Alertcounts	true	

						Name: adminResolvedCount; Description: How many threats are resolved by admin; Required: true; Value: integer Name: conditionalAccessCount; Description: How many threats is in conditional access; Required: true; Value: integer Name: mitigatedCount; Description: How many threats are mitigated; Required: true; Value: integer Name: notMitigatedCount; Description: How many threats are not mitigated; Required: true; Value: integer
			deviceId	MDM device ID	true	string
			groupId	A reference to the containing network group	true	string
			groupName	Name of the containing network group	true	string
			id	Id	true	integer
			registrationSource	MDM name or initiator in case of activations	true	string
			registrationType	Registration type	true	enum
			siteId	A reference to the containing site	true	string
			siteName	Name of the containing site	true	string

			threatCounts	Threatcounts	true	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>adminResolvedCount</td><td>How many threats are resolved by admin</td><td>true</td><td>integer</td></tr><tr><td>conditionalAccessCount</td><td>How many threats is in conditional access</td><td>true</td><td>integer</td></tr><tr><td>mitigatedCount</td><td>How many threats are mitigated</td><td>true</td><td>integer</td></tr><tr><td>notMitigatedCount</td><td>How many threats are not mitigated</td><td>true</td><td>integer</td></tr></table>
			appState	ZipApp state	false	enum
			appVersion	Version of the ZippApp	false	string
			debugMode	Debugmode	false	boolean
			developerMode	Developermode	false	boolean
			encrypted	Encrypted	false	boolean
			healthState	Highest health state of the device	false	enum
			lastActiveOn	When we received last heartbeat	false	string
			managedState	UEM state of the device	false	enum
			model	Device manufacturer and model	false	string
			osVersion	Device os version	false	string
			owner	User email	false	string
			platform	Device platform	false	enum

			policyUpdatedAt: When the corresponding policy was updated; false; string
			privileges: Either rooted or jailbroken for devices with privileges. Otherwise none; false; enum
			protected: Protected; false; boolean
			registeredOn: When the ZippApp registered; false; string
			registrationDate: When the activation for this device was created; false; string
			screenLocked: Screenlocked; false; boolean
			stagefreightVulnerable: Stagefreightvulnerable; false; boolean
			trackingId1: External tracking ID of device; false; string
			trackingId2: Another external tracking ID of device; false; string
			unofficialAppstore: Unofficialappstore; false; boolean
errors	Errors	false	array

Network Quarantine Control

Get Firewall Rules

GET /web/api/v2.1/firewall-control/{firewall_rule_category}

Get the Firewall Control rules for a scope specified by ID (run "accounts", "sites, "groups", or set "tenant" to "true") that match the filter.
The response will be quite long because it includes all the rule properties, thus at least one of these filters is required: action, status, osType, name, or scope ID.

Parameters

accountids	optional	List of Account IDs to filter by. Example: "225494730938493804,225494730938493915".
actions	optional	Return firewall rules with the filtered action. Example: "Allow".
application__contains	optional	Free-text filter by application (supports multiple values)
applications	optional	Return firewall rules with the filtered firewall class.
countonly	optional	If true, only total number of items will be returned, without any of the actual objects.
createdat__between	optional	Return firewall rules created within this range (inclusive). Example: "1514978764288-1514978999999".
createdat__gt	optional	Return firewall rules created after this timestamp. Example: "2018-02-27T04:49:26.257525Z".
createdat__gte	optional	Return firewall rules created after or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
createdat__lt	optional	Return firewall rules created before this timestamp. Example: "2018-02-27T04:49:26.257525Z".
createdat__lte	optional	Return firewall rules created before or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
cursor	optional	Cursor position returned by the last request. Use to iterate over more than 1000 items. Example: "YWdlbnRfaWQ6NTgwMjkzODE=".
directions	optional	Return firewall rules with the filtered directions. Example: "any".
disablepagination	optional	If true, all rules for requested scope will be returned

groupids	optional	List of Group IDs to filter by. Example: "225494730938493804,225494730938493915".
ids	optional	List of ids to filter by. Example: "225494730938493804,225494730938493915".
limit	optional	Limit number of returned items (1-1000). Example: "10".
locationids	optional	Filter by associated locations. Example: "225494730938493804,225494730938493915".
name	optional	Return firewall rules with the filtered name.
name__contains	optional	Free-text filter by the Rule name (supports multiple values)
ostypes	optional	Return firewall rules with the filtered os_type. Example: "macos".
protocol__contains	optional	Free-text filter by protocol (supports multiple values)
protocols	optional	Return firewall rules with the filtered protocols.
query	optional	Free text search on name, tag, application, protocol
scopes	optional	Return only firewall rules in this scope. Example: "account".
service__contains	optional	Free-text filter by service (supports multiple values)
siteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".
skip	optional	Skip first number of items (0-1000). To iterate over more than 1000 items, use "cursor". Example: "150".
skipcount	optional	If true, total number of items will not be calculated, which speeds up execution time.
sortby	optional	The column to sort the results by. Example: "id".
sortorder	optional	Sort direction. Example: "asc".
statuses	optional	Return firewall rules with the filtered status. Example: "Enabled".
tagids	optional	Filter by associated tags. Example: "225494730938493804,225494730938493915".
tagname__contains	optional	Free-text filter by the Tag name (supports multiple values)
tenant	optional	Indicates a tenant scope request

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>pagination</td><td>Pagination information</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>totalItems</td><td>Total number of items found matching your query</td><td>true</td><td>integer</td></tr>
<tr><td>nextCursor</td><td>Pass this value as "cursor" on your next request, to get the next page of results (Will be "null" when last page reached)</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>action</td><td>Defines if agent shall Block or Allow use of firewalls which matches the rule parameters.</td><td>false</td><td>enum</td></tr>
<tr><td>application</td><td>Application for the rule</td><td>false</td><td></td></tr>
<tr><td>createdAt</td><td>Date of rule creation</td><td>false</td><td>string</td></tr>
<tr><td>creator</td><td>Full name of the creating</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
</table>

				user		
			creatorId	Id of the creating user	false	string
			description	Description	false	string
			direction	Defines the Direction of the Firewall rule.	false	enum
			editable	True if the rule can be modified at this scope level	false	boolean
			id	Rule ID	false	string
			localHost	Local host	false	
			localPort	Local ports	false	
			location	Location associated with the rule	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>type</td><td>Location type</td><td>true</td><td>enum</td></tr><tr><td>values</td><td>Location IDs (applicable for the "specific" location type only)</td><td>false</td><td><table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>id</td><td>Location ID</td><td>true</td><td>string</td></tr><tr><td>name</td><td>Location name</td><td>false</td><td>string</td></tr><tr><td>scope</td><td>Location scope</td><td>false</td><td>enum</td></tr></table></td></tr></table>
			name	The name of the firewall rule.	false	string
			order	Position in the list of rules	false	integer
			osType	[DEPRECATED] Please use os_types since multiple os types are supported.This field will	false	enum

			return the first os_type, not necessarily the only one.		
			osTypes	Os types	false	string []
			productId	Product identifier. Unique for a specific product module, per vendor ID, Interface.	false	string
			protocol	The protocol.	false	string
			remoteHost	[DEPRECATED] First remote host in the rule. Full list in remote_hosts	false	
			remoteHosts	List of remote hosts	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>type</td><td>Type of the host</td><td>false</td><td>enum</td></tr><tr><td>values</td><td>Value of the host</td><td>false</td><td>string []</td></tr></table>
			remotePort	Remote ports	false	
			ruleCategory	Network quarantine rule or standard firewall rule	false	enum
			scope	Scope of the rule	false	enum
			scopeId	The group or site id depending on the scope. null if it is global.	false	string

<table>
<tr><td></td><td></td><td></td><td>
<table>
<tr><td>status</td><td>Defines if rule is Enabled or Disabled</td><td>false</td><td>enum</td></tr>
<tr><td>tag</td><td>[DEPRECATED] Free text to describe the rule. Please use description instead.</td><td>false</td><td>string</td></tr>
<tr><td>tagIds</td><td>Tag ids</td><td>false</td><td>string []</td></tr>
<tr><td>tagNames</td><td>Tag names</td><td>false</td><td>string []</td></tr>
<tr><td>tags</td><td>Tags</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>id</td><td></td><td>false</td><td>string</td></tr>
<tr><td>name</td><td></td><td>false</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>updatedAt</td><td>Date of last update</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Create Firewall Rule

POST /web/api/v2.1/firewall-control/{firewall_rule_category}

Create a Firewall Control rule for a scope specified by ID (run "accounts", "sites", "groups", or set "tenant" to "true") and specific OS, to allow or block network traffic to matching endpoints.
You can create one clean-up rule, with the Action of Allow or Block and with no other parameters defined explicitly. Make this the default rule at the end of your rule list. Traffic that does not match other rules first will match this rule. If you do not have a clean-up rule to match all traffic, the default Firewall Control behavior is to allow traffic that is not explicitly blocked.
Firewall Control requires Control SKU.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
action	Defines if agent shall Block or Allow use of firewalls which matches the rule parameters.	false	enum
application	Application for the rule	false	
createdAt	Date of rule creation	false	string
creator	Full name of the creating user	false	string

			creatorId	Id of the creating user	false	string
			description	Description	false	string
			direction	Defines the Direction of the Firewall rule.	false	enum
			editable	True if the rule can be modified at this scope level	false	boolean
			id	Rule ID	false	string
			localHost	Local host	false	
			localPort	Local ports	false	
			location	Location associated with the rule	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>type</td><td>Location type</td><td>true</td><td>enum</td></tr><tr><td>values</td><td>Location IDs (applicable for the "specific" location type only)</td><td>false</td><td><table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>id</td><td>Location ID</td><td>true</td><td>string</td></tr><tr><td>name</td><td>Location name</td><td>false</td><td>string</td></tr><tr><td>scope</td><td>Location scope</td><td>false</td><td>enum</td></tr></table></td></tr></table>
			name	The name of the firewall rule.	false	string
			order	Position in the list of rules	false	integer
			osType	[DEPRECATED] Please use os_types since multiple os types are supported.This field will return the first os_type,	false	enum

				not necessarily the only one.		
			osTypes	Os types	false	string []
			productId	Product identifier. Unique for a specific product module, per vendor ID, Interface.	false	string
			protocol	The protocol.	false	string
			remoteHost	[DEPRECATED] First remote host in the rule. Full list in remote_hosts	false	
			remoteHosts	List of remote hosts	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>type</td><td>Type of the host</td><td>false</td><td>enum</td></tr><tr><td>values</td><td>Value of the host</td><td>false</td><td>string []</td></tr></table>
			remotePort	Remote ports	false	
			ruleCategory	Network quarantine rule or standard firewall rule	false	enum
			scope	Scope of the rule	false	enum
			scopeId	The group or site id depending on the scope. null if it is global.	false	string
			status	Defines if rule is	false	enum

<table>
<tr><td></td><td></td><td></td><td>
<table>
<tr><td></td><td>Enabled or Disabled</td><td></td><td></td></tr>
<tr><td>tag</td><td>[DEPRECATED] Free text to describe the rule. Please use description instead.</td><td>false</td><td>string</td></tr>
<tr><td>tagIds</td><td>Tag ids</td><td>false</td><td>string []</td></tr>
<tr><td>tagNames</td><td>Tag names</td><td>false</td><td>string []</td></tr>
<tr><td>tags</td><td>Tags</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>id</td><td></td><td>false</td><td>string</td></tr>
<tr><td>name</td><td></td><td>false</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>updatedAt</td><td>Date of last update</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

Name	Description	Required	Value
data	Data	true	

Name	Description	Required	Value
action	Defines if agent shall Block or Allow use of firewalls which matches the rule parameters.	true	enum
name	The name of the firewall rule.	true	string
status	Defines if rule is Enabled or Disabled	true	enum
application	Application for the rule	false	

Name	Description	Required	Value
type	Type of the application	false	enum
values	Value of the application	false	string []

Name	Description	Required	Value
description	Description	false	string
direction	Defines the Direction of the Firewall rule.	false	enum
localHost	Local host structure with a type and a set of values	false	

Name	Description	Required	Value
type	Type of the host	false	enum
values	Value of the host	false	string []

Name	Description	Required	Value
localPort	Local ports structure with a type	false	

Name	Description	Required	Value
type	Type of the	false	enum

				and a set of values		ports values: A list of port numbers (false, integer [])
			location	Location structure with a type and a set of values	false	type: Location type (true, enum) values: Location IDs (applicable for the "specific" location type only) (false) id: Location ID (true, string) name: Location name (false, string) scope: Location scope (false, enum)
			osType	[DEPRECATED] Please use os_types since multiple os types are supported.This field will return the first os_type, not necessarily the only one.	false	enum
			osTypes	Os types	false	string []
			protocol	The protocol	false	string
			remoteHost	[DEPRECATED] Please use remote_hosts .Remote host structure with a type and a set of values.	false	type: Type of the host (false, enum) values: Value of the host (false, string [])
			remoteHosts	List of remote hosts, each structured with a type and a set of	false	type: Type of the host (false, enum) values: Value of the (false, string [])

<table>
<tr><td></td><td></td><td></td><td>
<table>
<tr><td></td><td>values</td><td></td><td>
<table>
<tr><td></td><td>host</td><td></td><td></td></tr>
</table>
</td></tr>
<tr><td>remotePort</td><td>Remote ports structure with a type and a set of values</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>type</td><td>Type of the ports</td><td>false</td><td>enum</td></tr>
<tr><td>values</td><td>A list of port numbers</td><td>false</td><td>integer []</td></tr>
</table>
</td></tr>
<tr><td>tag</td><td>[DEPRECATED] Free text to describe the rule. Please use description instead.</td><td>false</td><td>string</td></tr>
<tr><td>tagIds</td><td>Tag ids</td><td>false</td><td>string []</td></tr>
</table>
</td></tr>
<tr><td>filter</td><td>Filter</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>groupIds</td><td>List of Group IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>siteIds</td><td>List of Site IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>tenant</td><td>Indicates a tenant scope request</td><td>false</td><td>boolean</td></tr>
</table>
</td></tr>
</table>

Delete Rules

DELETE /web/api/v2.1/firewall-control/{firewall_rule_category}

Delete Firewall Control rules that match the filter.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>affected</td><td>Number of entities affected by the requested operation</td><td>false</td><td>integer</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

Name	Description	Required	Value
filter	Filter	false	

Name	Description	Required	Value
accountIds	List of Account IDs to filter by	false	string []
actions	Return firewall rules with the filtered action.	false	string []
application__contains	Free-text filter by application (supports multiple values)	false	string []
applications	Return firewall rules with the filtered firewall class.	false	string []
createdAt__between	Return firewall rules created within this range (inclusive)	false	string
createdAt__gt	Return firewall rules created after this timestamp.	false	string
createdAt__gte	Return firewall rules created after or at this timestamp.	false	string
createdAt__lt	Return firewall rules	false	string

				created before this timestamp.		
			createdAt__lte	Return firewall rules created before or at this timestamp.	false	string
			directions	Return firewall rules with the filtered directions.	false	string []
			groupIds	List of Group IDs to filter by	false	string []
			ids	List of ids to filter by	false	string []
			locationIds	Filter by associated locations	false	string []
			name	Return firewall rules with the filtered name.	false	string
			name__contains	Free-text filter by the Rule name (supports multiple values)	false	string []
			osTypes	Return firewall rules with the filtered os_type.	false	string []
			protocol__contains	Free-text filter by protocol (supports multiple	false	string []

				values)		
			protocols	Return firewall rules with the filtered protocols.	false	string []
			query	Free text search on name, tag, application, protocol	false	string
			scopes	Return only firewall rules in this scope	false	string []
			service__contains	Free-text filter by service (supports multiple values)	false	string []
			siteIds	List of Site IDs to filter by	false	string []
			statuses	Return firewall rules with the filtered status.	false	string []
			tagIds	Filter by associated tags	false	string []
			tagName__contains	Free-text filter by the Tag name (supports multiple values)	false	string []
			tenant	Indicates a tenant scope request	false	boolean

Copy Rules

POST /web/api/v2.1/firewall-control/{firewall_rule_category}/copy-rules

Copy a set of rules to other scopes.
In the filter of the body, enter the properties to define the source. In the data field of the body, define the targets by ID. To get a scope ID, run 'accounts', 'sites', or 'groups'.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>affected</td><td>Number of entities affected by the requested operation</td><td>false</td><td>integer</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountId</td><td>Target account</td><td>false</td><td>string</td></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>groupId</td><td>Target group</td><td>false</td><td>string</td></tr>
<tr><td>groupIds</td><td>[DEPRECATED] Target group(s)</td><td>false</td><td>string []</td></tr>
<tr><td>siteId</td><td>Target site</td><td>false</td><td>string</td></tr>
<tr><td>siteIds</td><td>List of Site IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>tenant</td><td>Indicates a tenant scope request</td><td>false</td><td>boolean</td></tr>
</table>
</td></tr>
<tr><td>filter</td><td>Filter</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>actions</td><td>Return firewall rules with the filtered action.</td><td>false</td><td>string []</td></tr>
<tr><td>application__contains</td><td>Free-text filter by application (supports multiple values)</td><td>false</td><td>string []</td></tr>
<tr><td>applications</td><td>Return firewall rules with the filtered</td><td>false</td><td>string []</td></tr>
</table>
</td></tr>
</table>

				firewall class.		
			createdAt__between	Return firewall rules created within this range (inclusive)	false	string
			createdAt__gt	Return firewall rules created after this timestamp.	false	string
			createdAt__gte	Return firewall rules created after or at this timestamp.	false	string
			createdAt__lt	Return firewall rules created before this timestamp.	false	string
			createdAt__lte	Return firewall rules created before or at this timestamp.	false	string
			directions	Return firewall rules with the filtered directions.	false	string []
			groupIds	List of Group IDs to filter by	false	string []
			ids	List of ids to filter by	false	string []
			locationIds	Filter by associated locations	false	string []

			name	Return firewall rules with the filtered name.	false	string
			name__contains	Free-text filter by the Rule name (supports multiple values)	false	string []
			osTypes	Return firewall rules with the filtered os_type.	false	string []
			protocol__contains	Free-text filter by protocol (supports multiple values)	false	string []
			protocols	Return firewall rules with the filtered protocols.	false	string []
			query	Free text search on name, tag, application, protocol	false	string
			scopes	Return only firewall rules in this scope	false	string []
			service__contains	Free-text filter by service (supports multiple values)	false	string []
			siteIds	List of Site IDs to filter	false	string []

				by		
			statuses	Return firewall rules with the filtered status.	false	string []
			tagIds	Filter by associated tags	false	string []
			tagName__contains	Free-text filter by the Tag name (supports multiple values)	false	string []
			tenant	Indicates a tenant scope request	false	boolean

Move Rules

POST /web/api/v2.1/firewall-control/{firewall_rule_category}/move-rules

Remove Firewall Rules, defined with the ID of the rules (run 'firewall-control'), from scopes specified by ID (run 'accounts', 'sites', or 'groups') and add the rules to the scope IDs in the data field.
Firewall Control requires Control SKU.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>affected</td><td>Number of entities affected by the requested operation</td><td>false</td><td>integer</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountId</td><td>Target account</td><td>false</td><td>string</td></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>groupId</td><td>Target group</td><td>false</td><td>string</td></tr>
<tr><td>groupIds</td><td>[DEPRECATED] Target group(s)</td><td>false</td><td>string []</td></tr>
<tr><td>siteId</td><td>Target site</td><td>false</td><td>string</td></tr>
<tr><td>siteIds</td><td>List of Site IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>tenant</td><td>Indicates a tenant scope request</td><td>false</td><td>boolean</td></tr>
</table>
</td></tr>
<tr><td>filter</td><td>Filter</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>actions</td><td>Return firewall rules with the filtered action.</td><td>false</td><td>string []</td></tr>
<tr><td>application__contains</td><td>Free-text filter by application (supports multiple values)</td><td>false</td><td>string []</td></tr>
<tr><td>applications</td><td>Return firewall rules with the filtered</td><td>false</td><td>string []</td></tr>
</table>
</td></tr>
</table>

				firewall class.		
			createdAt__between	Return firewall rules created within this range (inclusive)	false	string
			createdAt__gt	Return firewall rules created after this timestamp.	false	string
			createdAt__gte	Return firewall rules created after or at this timestamp.	false	string
			createdAt__lt	Return firewall rules created before this timestamp.	false	string
			createdAt__lte	Return firewall rules created before or at this timestamp.	false	string
			directions	Return firewall rules with the filtered directions.	false	string []
			groupIds	List of Group IDs to filter by	false	string []
			ids	List of ids to filter by	false	string []
			locationIds	Filter by associated locations	false	string []

			name	Return firewall rules with the filtered name.	false	string
			name__contains	Free-text filter by the Rule name (supports multiple values)	false	string []
			osTypes	Return firewall rules with the filtered os_type.	false	string []
			protocol__contains	Free-text filter by protocol (supports multiple values)	false	string []
			protocols	Return firewall rules with the filtered protocols.	false	string []
			query	Free text search on name, tag, application, protocol	false	string
			scopes	Return only firewall rules in this scope	false	string []
			service__contains	Free-text filter by service (supports multiple values)	false	string []
			siteIds	List of Site IDs to filter	false	string []

				by		
			statuses	Return firewall rules with the filtered status.	false	string []
			tagIds	Filter by associated tags	false	string []
			tagName__contains	Free-text filter by the Tag name (supports multiple values)	false	string []
			tenant	Indicates a tenant scope request	false	boolean

Set Location

POST /web/api/v2.1/firewall-control/{firewall_rule_category}/set-location

Set location attributes for a Location Aware Firewall Control rule. These rules are applied by Agents only if the network parameters of the endpoint match the properties of the location definition. To get a Location ID, run "locations".
Firewall Control requires Control SKU.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
data	Response data	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>affected</td><td>Number of entities affected by the requested operation</td><td>false</td><td>integer</td></tr></table>
errors	Errors	false	array

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>type</td><td>Location type</td><td>true</td><td>enum</td></tr>
<tr><td>values</td><td>Location IDs (applicable for the "specific" location type only)</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>id</td><td>Location ID</td><td>true</td><td>string</td></tr>
<tr><td>name</td><td>Location name</td><td>false</td><td>string</td></tr>
<tr><td>scope</td><td>Location scope</td><td>false</td><td>enum</td></tr>
</table>
</td></tr>
</table>
</td></tr>
<tr><td>filter</td><td>Filter</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>actions</td><td>Return firewall rules with the filtered action.</td><td>false</td><td>string []</td></tr>
<tr><td>application__contains</td><td>Free-text filter by application (supports multiple values)</td><td>false</td><td>string []</td></tr>
<tr><td>applications</td><td>Return firewall rules with the filtered firewall class.</td><td>false</td><td>string []</td></tr>
<tr><td>createdAt__between</td><td>Return firewall rules created within this range (inclusive)</td><td>false</td><td>string</td></tr>
<tr><td>createdAt__g</td><td>Return</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
</table>

			t	firewall rules created after this timestamp.			
			createdAt__gte	Return firewall rules created after or at this timestamp.	false	string	
			createdAt__lt	Return firewall rules created before this timestamp.	false	string	
			createdAt__lte	Return firewall rules created before or at this timestamp.	false	string	
			directions	Return firewall rules with the filtered directions.	false	string []	
			groupIds	List of Group IDs to filter by	false	string []	
			ids	List of ids to filter by	false	string []	
			locationIds	Filter by associated locations	false	string []	
			name	Return firewall rules with the filtered name.	false	string	
			name__contains	Free-text filter by the Rule name (supports multiple	false	string []	

				values)		
			osTypes	Return firewall rules with the filtered os_type.	false	string []
			protocol__contains	Free-text filter by protocol (supports multiple values)	false	string []
			protocols	Return firewall rules with the filtered protocols.	false	string []
			query	Free text search on name, tag, application, protocol	false	string
			scopes	Return only firewall rules in this scope	false	string []
			service__contains	Free-text filter by service (supports multiple values)	false	string []
			siteIds	List of Site IDs to filter by	false	string []
			statuses	Return firewall rules with the filtered status.	false	string []
			tagIds	Filter by associated tags	false	string []

			tagName__contains	Free-text filter by the Tag name (supports multiple values)	false	string []	
			tenant	Indicates a tenant scope request	false	boolean	

Reorder Rules

PUT /web/api/v2.1/firewall-control/{firewall_rule_category}/reorder

Change the order of rules for a scope specified by ID (run "accounts", "sites", or "groups").
The Agent looks at the rules based on their order in the Firewall Control policy, from the top to the bottom. First it goes through the Group rules, then the Site rules, then the Account rules, then the Global rules. When the Agent finds a rule that matches the parameters of the traffic, that rule is applied. The Agent does not continue to the lower rules in the list. Thus, the scope and the order of the rules is important.
Firewall Control requires Control SKU.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>success</td><td>Indicates a successful operation</td><td>false</td><td>boolean</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>filter</td><td>Filter</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>groupIds</td><td>List of Group IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>osTypes</td><td>[DEPRECATED] Rules OS type (was relevant for when each OS type had its own rule order)</td><td>false</td><td>string []</td></tr>
<tr><td>siteIds</td><td>List of Site IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>tenant</td><td>Indicates a tenant scope request</td><td>false</td><td>boolean</td></tr>
</table>
</td></tr>
<tr><td>data</td><td>Data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>id</td><td>Rule ID</td><td>true</td><td>string</td></tr>
<tr><td>order</td><td>Desired position in the list of rules</td><td>true</td><td>integer</td></tr>
</table>
</td></tr>
</table>

Get Configuration

GET /web/api/v2.1/firewall-control/{firewall_rule_category}/configuration

Get the Firewall Control configuration for a given scope.
To filter the results for a scope:
* Global - Make sure "tenant" is "true" and no other scope ID is given.
* Account - Make sure "tenant" is "false" and at least one Account ID is given.
* Site - Make sure "tenant" is "false" and at least one Site ID is given.
The response shows if Firewall Control is enabled for the scope, if Location Awareness is enabled, the higher scope from which this scope inherited the configuration, and whether a lower scope inherits this configuration.
Firewall Control requires Control SKU.

Parameters

accountids	optional	List of Account IDs to filter by. Example: "225494730938493804,225494730938493915".
groupids	optional	List of Group IDs to filter by. Example: "225494730938493804,225494730938493915".
siteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".
tenant	optional	Indicates a tenant scope request

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
enabled	Firewall control enabled for	false	boolean

				the scope		
			inheritAllFirewallRules	Inherit all the rules and tags from the parent scope. Expands on 'inherits' value.	false	boolean
			inheritedFrom	If null it means it is own policy else it tells the ancestor for the policy.For groups options are null/Site/Global, for site options are null/Global.	false	string
			inherits	True if rules are decoupled from parent rules	false	boolean
			inheritSettings	Inherit firewall settings from parent scope	false	boolean
			locationAware	Firewall control supports location awareness for the scope	false	boolean
			reportBlocked	Agent should report blocked events	false	boolean
			selectedTags	Selected tags	false	string []

errors	Errors	false	array

Update Configuration

PUT /web/api/v2.1/firewall-control/{firewall_rule_category}/configuration

Change the Firewall Control configuration for a given scope.
To get the ID of a scope, run "accounts", "sites", or "groups". To change the Global configuration, leave the filters empty and set "tenant" to "true". In the Body, you can set if Firewall Control is enabled for the scope, if Location Awareness is enabled, the higher scope from which this scope inherits the configuration ("Global" or a scope ID), whether the lower scopes inherit this configuration, and whether blocked actions are reported.
Firewall Control requires Control SKU.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>enabled</td><td>Firewall control enabled for the scope</td><td>false</td><td>boolean</td></tr>
<tr><td>inheritAllFirewallRules</td><td>Inherit all the rules and tags from the parent scope. Expands on 'inherits' value.</td><td>false</td><td>boolean</td></tr>
<tr><td>inheritedFrom</td><td>If null it means it is own policy else it tells the ancestor for the policy.For</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
</table>

			groups options are null/Site/Global, for site options are null/Global.
			inherits: True if rules are decoupled from parent rules (false, boolean)
			inheritSettings: Inherit firewall settings from parent scope (false, boolean)
			locationAware: Firewall control supports location awareness for the scope (false, boolean)
			reportBlocked: Agent should report blocked events (false, boolean)
			selectedTags: Selected tags (false, string [])
errors	Errors	false	array

Body Schema

Name	Description	Required	Value
data	Data	true	

Name	Description	Required	Value
enabled	Firewall control enabled for the scope	false	boolean
inheritAllFirewallRules	Inherit all the rules and tags from the parent scope. Expands on 'inherits' value.	false	boolean
inheritedFrom	If null it means it is own policy else it tells the ancestor for the policy.For groups options are null/Site/Global, for site options are null/Global.	false	string
inherits	True if rules are decoupled from parent rules	false	boolean
inheritSettings	Inherit firewall settings from parent scope	false	boolean
locationAware	Firewall control supports location	false	boolean

filter	Filter	true	

	awareness for the scope		
reportBlocked	Agent should report blocked events	false	boolean
selectedTags	Selected tags	false	string []

Name	Description	Required	Value
accountIds	List of Account IDs to filter by	false	string []
groupIds	List of Group IDs to filter by	false	string []
siteIds	List of Site IDs to filter by	false	string []
tenant	Indicates a tenant scope request	false	boolean

Export Rules

GET /web/api/v2.1/firewall-control/{firewall_rule_category}/export

Export Firewall Control rules that match the filter to a JSON file from a scope specified by ID (run "accounts", "sites", "groups", or leave the scope empty and set "tenant" to "true") and import them to another scope (with the "import" command.
Firewall Control requires Control SKU.

Parameters

accountids	optional	List of Account IDs to filter by. Example: "225494730938493804,225494730938493915".
actions	optional	Return firewall rules with the filtered action. Example: "Allow".
application__contains	optional	Free-text filter by application (supports multiple values)
applications	optional	Return firewall rules with the filtered firewall class.
createdat__between	optional	Return firewall rules created within this range (inclusive). Example: "1514978764288-1514978999999".
createdat__gt	optional	Return firewall rules created after this timestamp. Example: "2018-02-27T04:49:26.257525Z".
createdat__gte	optional	Return firewall rules created after or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
createdat__lt	optional	Return firewall rules created before this timestamp. Example: "2018-02-27T04:49:26.257525Z".
createdat__lte	optional	Return firewall rules created before or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
directions	optional	Return firewall rules with the filtered directions. Example: "any".
groupids	optional	List of Group IDs to filter by. Example: "225494730938493804,225494730938493915".
ids	optional	List of ids to filter by. Example: "225494730938493804,225494730938493915".
locationids	optional	Filter by associated locations. Example: "225494730938493804,225494730938493915".
name	optional	Return firewall rules with the filtered name.
name__contains	optional	Free-text filter by the Rule name (supports multiple values)
ostypes	optional	Return firewall rules with the filtered os_type. Example: "macos".

protocol__contains	optional	Free-text filter by protocol (supports multiple values)
protocols	optional	Return firewall rules with the filtered protocols.
query	optional	Free text search on name, tag, application, protocol
scopes	optional	Return only firewall rules in this scope. Example: "account".
service__contains	optional	Free-text filter by service (supports multiple values)
siteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".
statuses	optional	Return firewall rules with the filtered status. Example: "Enabled".
tagids	optional	Filter by associated tags. Example: "225494730938493804,225494730938493915".
tagname__contains	optional	Free-text filter by the Tag name (supports multiple values)
tenant	optional	Indicates a tenant scope request

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Import Rules

POST /web/api/v2.1/firewall-control/{firewall_rule_category}/import

Import Firewall Control rules from an exported JSON file to scopes specified by ID (run "accounts", "sites", "groups", or leave the scope empty and set "tenant" to "true"). Firewall Control requires Control SKU, in the target and in the source.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
data	Response data	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>success</td><td>Indicates a successful operation</td><td>false</td><td>boolean</td></tr></table>
errors	Errors	false	array

Body Schema

Name	Description	Required	Value
formData		false	

Name	Description	Required	Value
file	File	true	file
accountIds	List of Account IDs to filter by. Example: "225494730938493804,225494730938493915".	false	string []
groupIds	List of Group IDs to filter by. Example: "225494730938493804,225494730938493915".	false	string []
siteIds	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".	false	string []
tenant	Indicates a tenant scope request	false	boolean

Enable/Disable Rules

PUT /web/api/v2.1/firewall-control/{firewall_rule_category}/enable

Change the status of a set of Firewall Control rules that match the filter to "Enabled" or "Disabled". In one request, you can set one status or the other.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>affected</td><td>Number of entities affected by the requested operation</td><td>false</td><td>integer</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>status</td><td>should the rules be enabled/ disabled</td><td>true</td><td>enum</td></tr>
</table>
</td></tr>
<tr><td>filter</td><td>Filter</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>actions</td><td>Return firewall rules with the filtered action.</td><td>false</td><td>string []</td></tr>
<tr><td>application__contains</td><td>Free-text filter by application (supports multiple values)</td><td>false</td><td>string []</td></tr>
<tr><td>applications</td><td>Return firewall rules with the filtered firewall class.</td><td>false</td><td>string []</td></tr>
<tr><td>createdAt__between</td><td>Return firewall rules created within this range (inclusive)</td><td>false</td><td>string</td></tr>
<tr><td>createdAt__gt</td><td>Return firewall rules created after this timestamp.</td><td>false</td><td>string</td></tr>
<tr><td>createdAt__g</td><td>Return</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
</table>

			te	firewall rules created after or at this timestamp.		
			createdAt__lt	Return firewall rules created before this timestamp.	false	string
			createdAt__lte	Return firewall rules created before or at this timestamp.	false	string
			directions	Return firewall rules with the filtered directions.	false	string []
			groupIds	List of Group IDs to filter by	false	string []
			ids	List of ids to filter by	false	string []
			locationIds	Filter by associated locations	false	string []
			name	Return firewall rules with the filtered name.	false	string
			name__contains	Free-text filter by the Rule name (supports multiple values)	false	string []
			osTypes	Return firewall rules with the filtered	false	string []

				os_type.		
			protocol__contains	Free-text filter by protocol (supports multiple values)	false	string []
			protocols	Return firewall rules with the filtered protocols.	false	string []
			query	Free text search on name, tag, application, protocol	false	string
			scopes	Return only firewall rules in this scope	false	string []
			service__contains	Free-text filter by service (supports multiple values)	false	string []
			siteIds	List of Site IDs to filter by	false	string []
			statuses	Return firewall rules with the filtered status.	false	string []
			tagIds	Filter by associated tags	false	string []
			tagName__contains	Free-text filter by the Tag name (supports multiple	false	string []

				values)		
			tenant	Indicates a tenant scope request	false	boolean

Get Protocols

GET /web/api/v2.1/firewall-control/{firewall_rule_category}/protocols

Get a list of protocols that can be used in Firewall Control rules.

Parameters

countonly	optional	If true, only total number of items will be returned, without any of the actual objects.
cursor	optional	Cursor position returned by the last request. Use to iterate over more than 1000 items. Example: "YWdlbnRfaWQ6NTgwMjkzODE=".
disablepagination	optional	If true, all rules for requested scope will be returned
limit	optional	Limit number of returned items (1-1000). Example: "10".
query	optional	Full text search on protocols
skip	optional	Skip first number of items (0-1000). To iterate over more than 1000 items, use "cursor". Example: "150".
skipcount	optional	If true, total number of items will not be calculated, which speeds up execution time.
sortby	optional	The column to sort the results by. Example: "id".
sortorder	optional	Sort direction. Example: "asc".

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
pagination	Pagination information	true	

Name	Description	Required	Value
totalItems	Total number	true	integer

<table>
<tr><td></td><td></td><td></td><td><table>
<tr><td></td><td>of items found matching your query</td><td></td><td></td></tr>
<tr><td>nextCursor</td><td>Pass this value as "cursor" on your next request, to get the next page of results (Will be "null" when last page reached)</td><td>false</td><td>string</td></tr>
</table></td></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td><table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>groupIds</td><td>List of Group IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>name</td><td>Description of the protocol</td><td>false</td><td>string</td></tr>
<tr><td>siteIds</td><td>List of Site IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>tenant</td><td>Indicates a tenant scope request</td><td>false</td><td>boolean</td></tr>
<tr><td>value</td><td>Short code identifying the protocol</td><td>false</td><td>string</td></tr>
</table></td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Add Rule Tags

POST /web/api/v2.1/firewall-control/{firewall_rule_category}/add-tags

Create a Firewall Rule tag.
Create tags to represent Firewall policies - a set of rules in a specific order. After you create the tag, add rules to it.
Notes:
* Tags apply to a scope and cannot be linked to rules from different scopes.
* Tags must be 2 to 256 characters.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>affected</td><td>Number of entities affected by the requested operation</td><td>false</td><td>integer</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>tagIds</td><td>Tag ids</td><td>false</td><td>string []</td></tr>
</table>
</td></tr>
<tr><td>filter</td><td>Filter</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>actions</td><td>Return firewall rules with the filtered action.</td><td>false</td><td>string []</td></tr>
<tr><td>application__contains</td><td>Free-text filter by application (supports multiple values)</td><td>false</td><td>string []</td></tr>
<tr><td>applications</td><td>Return firewall rules with the filtered firewall class.</td><td>false</td><td>string []</td></tr>
<tr><td>createdAt__between</td><td>Return firewall rules created within this range (inclusive)</td><td>false</td><td>string</td></tr>
<tr><td>createdAt__gt</td><td>Return firewall rules created after this timestamp.</td><td>false</td><td>string</td></tr>
<tr><td>createdAt__gte</td><td>Return firewall rules created after or at this</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
</table>

				timestamp.		
			createdAt__lt	Return firewall rules created before this timestamp.	false	string
			createdAt__lte	Return firewall rules created before or at this timestamp.	false	string
			directions	Return firewall rules with the filtered directions.	false	string []
			groupIds	List of Group IDs to filter by	false	string []
			ids	List of ids to filter by	false	string []
			locationIds	Filter by associated locations	false	string []
			name	Return firewall rules with the filtered name.	false	string
			name__contains	Free-text filter by the Rule name (supports multiple values)	false	string []
			osTypes	Return firewall rules with the filtered os_type.	false	string []
			protocol__con	Free-text	false	string []

			tains	filter by protocol (supports multiple values)		
			protocols	Return firewall rules with the filtered protocols.	false	string []
			query	Free text search on name, tag, application, protocol	false	string
			scopes	Return only firewall rules in this scope	false	string []
			service__contains	Free-text filter by service (supports multiple values)	false	string []
			siteIds	List of Site IDs to filter by	false	string []
			statuses	Return firewall rules with the filtered status.	false	string []
			tagIds	Filter by associated tags	false	string []
			tagName__contains	Free-text filter by the Tag name (supports multiple values)	false	string []
			tenant	Indicates a	false	boolean

				tenant scope request		

Remove Rule Tags

POST /web/api/v2.1/firewall-control/{firewall_rule_category}/remove-tags

Remove firewall tags from rules matching the filter.
Tags represent Firewall policies - a set of rules in a specific order. When you remove a rule with a tag, all scopes that subscribe to the tag get the change.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>affected</td><td>Number of entities affected by the requested operation</td><td>false</td><td>integer</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>tagIds</td><td>Tag ids</td><td>false</td><td>string []</td></tr>
</table>
</td></tr>
<tr><td>filter</td><td>Filter</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>actions</td><td>Return firewall rules with the filtered action.</td><td>false</td><td>string []</td></tr>
<tr><td>application__contains</td><td>Free-text filter by application (supports multiple values)</td><td>false</td><td>string []</td></tr>
<tr><td>applications</td><td>Return firewall rules with the filtered firewall class.</td><td>false</td><td>string []</td></tr>
<tr><td>createdAt__between</td><td>Return firewall rules created within this range (inclusive)</td><td>false</td><td>string</td></tr>
<tr><td>createdAt__gt</td><td>Return firewall rules created after this timestamp.</td><td>false</td><td>string</td></tr>
<tr><td>createdAt__gte</td><td>Return firewall rules created after or at this</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
</table>

				timestamp.		
			createdAt__lt	Return firewall rules created before this timestamp.	false	string
			createdAt__lte	Return firewall rules created before or at this timestamp.	false	string
			directions	Return firewall rules with the filtered directions.	false	string []
			groupIds	List of Group IDs to filter by	false	string []
			ids	List of ids to filter by	false	string []
			locationIds	Filter by associated locations	false	string []
			name	Return firewall rules with the filtered name.	false	string
			name__contains	Free-text filter by the Rule name (supports multiple values)	false	string []
			osTypes	Return firewall rules with the filtered os_type.	false	string []
			protocol__con	Free-text	false	string []

			tains	filter by protocol (supports multiple values)		
			protocols	Return firewall rules with the filtered protocols.	false	string []
			query	Free text search on name, tag, application, protocol	false	string
			scopes	Return only firewall rules in this scope	false	string []
			service__contains	Free-text filter by service (supports multiple values)	false	string []
			siteIds	List of Site IDs to filter by	false	string []
			statuses	Return firewall rules with the filtered status.	false	string []
			tagIds	Filter by associated tags	false	string []
			tagName__contains	Free-text filter by the Tag name (supports multiple values)	false	string []
			tenant	Indicates a	false	boolean

				tenant scope request		

Policies

Group Policy

GET /web/api/v2.1/groups/{group_id}/policy

Get the policy of the Group given by ID. To get the ID of a Group, run "groups". See also: Get Policy.

Response Messages

200 - Success

401 - Unauthorized access - please sign in and retry.

404 - Policy not found

Response Schema

Name	Description	Required	Value
data	Response data	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>agentLoggingOn</td><td>True if logging is enabled in the agent</td><td>false</td><td>boolean</td></tr><tr><td>agentNotification</td><td>[DEPRECATED] Show end point notification on suspicious.Replaced by 'show_suspicious' in the agent UI section</td><td>false</td><td>boolean</td></tr><tr><td>agentUi</td><td>Agent ui</td><td>false</td><td><table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr></table></td></tr></table>

						agentUiOn	Agent ui on	false	boolean	
						contactCompany	Contact company	false	string	
						contactDirectMessage	Contact direct message	false	string	
						contactEmail	Contact email	false	string	
						contactFreeText	Contact free text	false	string	
						contactOther	Contact other	false	string	
						contactPhoneNumber	Contact phone number	false	string	
						contactSupportWebsite	Contact support website	false	string	
						devicePopUpNotifications	Device pop up notifications	false	boolean	
						maxEventAgeDays	Max event age days	false	integer	
						showAgentWarnings	Show agent warnings	false	boolean	
						showDeviceTab	Show device tab	false	boolean	
						showQuarantineTab	Show quarantine tab	false	boolean	
						showSupport	Show support	false	boolean	
						showSuspicious	Show suspicious	false	boolean	
						threatPopUpNotifications	Threat pop up notifications	false	boolean	
				agentUiOn	[DEPRECATED] Show/hide Agent UI. Moved inside	false	boolean			

				the agent UI section		
			allowRemoteShell	True if Remote Shell is enabled for the scope	false	boolean
			antiTamperingOn	Anti tampering on/off	false	boolean
			autoDecommissionDays	Automatic decommission period in days	false	integer
			autoDecommissionOn	Auto decommission on	false	boolean
			autoFileUpload	Automatic file upload configuration	false	

Name	Description	Required	Value
enabled	Automatic file upload on/off	false	boolean
includeBenignFiles	Upload benign files	false	boolean
maxDailyFileUpload	Maximum size (MB) to upload daily	false	integer
maxDailyFileUploadLimit	Limit for the maximum size (MB) to upload daily	false	integer
maxFileSize	Maximum file size (MB) to upload	false	integer
maxFileSizeLimit	Limit for the maximum file size (MB) to upload	false	integer
maxLocalDiskUsage	Maximum local disk usage (MB) for uploaded	false	integer

							files		
						maxLocalDiskUsageLimit	Limit for the maximum local disk usage (MB) for uploaded files	false	integer
			autoImmuneOn	Automatic immune on/off - this value must be true since all policies are immune by default	false	boolean			
			autoMitigationAction	Default action for auto mitigation	false	string			
			cloudValidationOn	Cloud validation on	false				
			createdAt	Timestamp of policy creation	false	string			
			driverBlocking	Suspicious driver blocking engine on/off	false	boolean			
			dvAttributesPerEventType	The DV attributes	false	Name	Description	Required	Value
						autoInstallBrowserExtensions	Auto install browser extensions	false	Name: autoInstallBrowserExtensions; Description: Auto install browser extensions; Required: false; Value: boolean
						behavioralIndicators	Behavioral indicators event	false	Name: dvEventTypeBehavioralIndicators; Description: Behavioral indicators event; Required: false; Value: boolean
						commandScri	Command	false	

						pts	scripts event		Name: dvEventTypeCommandScripts Description: Command scripts event Required: false Value: boolean
						crossProcess	Cross process event	false	Name: dvEventTypeCrossProcessDuplicateProcess Description: Duplicate Process Event Type Required: false Value: boolean Name: dvEventTypeCrossProcessDuplicateThread Description: Duplicate Thread Event Type Required: false Value: boolean Name: dvEventTypeCrossProcessOpenProcess Description: Open Process Event Type Required: false Value: boolean Name: dvEventTypeCrossProcessRemoteThread Description: Remote Thread Event Type Required: false Value: boolean
						dataMasking	Data masking	false	Name: dataMasking Description: Data masking Required: false Value: boolean
						dllModuleLoad	DLL module load event	false	Name: dvEventTypeDllModuleLoad Description: DLL module load event Required: false Value: boolean
						dns	Network event - DNS	false	Name: dvEventTypeDns Description: Network event - DNS Required: false Value: boolean
						driver	Driver	false	Name: dvEventTypeDriverLoad Description: Driver Load Required: false Value: boolean
						file	File event	false	Name: dvEventTypeF Description: File Creation Required: false Value: boolean

										ileCreation	Event Type		
										dvEventTypeFileDeletion	File Deletion Event Type	false	boolean
										dvEventTypeFileModification	File Modification Event Type	false	boolean
										dvEventTypeFileRename	File Rename Event Type	false	boolean
										fullDiskScan	File Scan Event Type	false	boolean
							ip	Network event - IP	false	Name	Description	Required	Value
										dvEventTypeIpConnect	IP Connect Event Type	false	boolean
										dvEventTypeIpListen	IP Listen Event Type	false	boolean
							login	User login/ logout event	false	Name	Description	Required	Value
										dvEventTypeLoginLoggedIn	User Login Event Type	false	boolean
										dvEventTypeLoginLoggedOut	User Logout Event Type	false	boolean
							namedPipe	Named Pipe	false	Name	Description	Required	Value
										dvEventTypeNamedPipeConnection	Named Pipe Connection Event Type	false	boolean
										dvEventTypeNamedPipeCreation	Named Pipe Creation Event Type	false	boolean
							namedPipeExtended	Named Pipe Extended	false	Name	Description	Required	Value
										namedPipeExtended	Named Pipe Connection Extended Event Type	false	boolean
							process	Process event	false	Name	Description	Required	Value

										dvEventTypeProcessCreation	Process Creation Event Type	false	boolean					
										dvEventTypeProcessExit	Process Exit Event Type	false	boolean					
										dvEventTypeProcessModification	Process Termination Event Type	false	boolean					
							registry	Registry event	false	Name	Description	Required	Value					
										dvEventTypeRegistryKeyCreated	Registry Key Created Event Type	false	boolean					
										dvEventTypeRegistryKeyDelete	Registry Key Delete Event Type	false	boolean					
										dvEventTypeRegistryKeyExport	Registry Key Export Event Type	false	boolean					
										dvEventTypeRegistryKeyImport	Registry Key Import Event Type	false	boolean					
										dvEventType RegistryKey Rename	Registry Key Rename Event Type	false	boolean					
										dvEventTypeRegistryKeySecurityChanged	Registry Key Security Changed Event Type	false	boolean					
										dvEventTypeRegistryValueCreated	Registry Value Crated Event Type	false	boolean					
										dvEventTypeRegistryValueDeleted	Registry Value Deleted Event Type	false	boolean					
										dvEventTypeRegistryValueModified	Registry Value Modified	false	boolean					

										Event Type		
						scheduledTask	Scheduled task event	false				
									Name	Description	Required	Value
									dvEventTypeScheduledTaskDelete	Scheduled Task Delete Event Type	false	boolean
									dvEventTypeScheduledTaskRegister	Scheduled Task Register Event Type	false	boolean
									dvEventTypeScheduledTaskStart	Scheduled Task Start Event Type	false	boolean
									dvEventTypeScheduledTaskTrigger	Scheduled Task Trigeer Event Type	false	boolean
									dvEventTypeScheduledTaskUpdate	Scheduled Task Update Event Type	false	boolean
						smartFileMonitoring	Smart file monitoring	false				
									Name	Description	Required	Value
									smartFileMonitoring	Smart file monitoring	false	boolean
						url	URL Actions event	false				
									Name	Description	Required	Value
									dvEventTypeUrl	URL Actions event	false	boolean
						windowsEventLogs	Windows Event Log	false				
									Name	Description	Required	Value
									dvEventTypeWindowsEventLogCreation	Windows Event Log Creation Event Type	false	boolean
						windowsEventLogsExtended	Windows Event Log Extended	false				
									Name	Description	Required	Value
									windowsEventLogsExtended	Windows Event Log Extended Event Type	false	boolean
			engines	The engines	false							

				statuses		

Name	Description	Required	Value
applicationControl	application control	false	enum
dataFiles	data files	false	enum
executables	executables	false	enum
exploits	exploits	false	enum
lateralMovement	lateral movement	false	enum
penetration	penetration	false	enum
preExecution	on-write	false	enum
preExecutionSuspicious	pre execution suspicious	false	enum
pup	potentially unwanted applications (PUP)	false	enum
remoteShell	remote shell	false	enum
reputation	reputation	false	enum

forensicsAutoTriggering	Forensics auto triggering configuration	false

Name	Description	Required	Value
linuxEnabled	True if linux forensics is enabled	false	boolean
linuxProfileId	The profile id for the linux forensics	false	string
linuxProfileName	The profile name for the linux forensics	false	string
macosEnabled	True if macos forensics is enabled	false	boolean
macosProfileId	The profile id for the macos forensics	false	string
macosProfil	The profile	false	string

						eName: name for the macos forensics windowsEnabled: True if windows forensics is enabled, false, boolean windowsProfileId: The profile id for the windows forensics, false, string windowsProfileName: The profile name for the windows forensics, false, string
			fwForNetworkQuarantineEnabled	True if Firewall Control for Network Quarantine is enabled	false	boolean
			identityEndpointReporting	Endpoint reporting level	false	enum
			identityOn	Identity module on/off	false	boolean
			identityReportInterval	Identity telemetry report interval in minutes	false	integer
			identityThrottlingInterval	Identity duplicate command consolidation interval in minutes	false	integer
			identityUpdateInterval	Identity update interval in	false	integer

				minutes		
			inheritedFrom	Indicates the parent scope from which this policy is inherited, or 'null' if it is not inherited (modified specifically for the current scope).	false	enum
			ioc	True if ioc is enabled	false	boolean
			iocAttributes	The Ioc attributes	false	

Name	Description	Required	Value
autoInstallBrowserExtensions	Update auto install browser extensions	false	boolean
behavioralIndicators	Update behavioral indicators	false	boolean
commandScripts	Update command scripts	false	boolean
crossProcess	Update cross process	false	boolean
dataMasking	Update data masking	false	boolean
dllModuleLoad	Update DLL module load	false	boolean
dns	Network event - DNS	false	boolean
driver	Driver	false	boolean
fds	Full disk scan	false	boolean
file	File event	false	boolean
ip	Network event - IP	false	boolean

						login: User login/ logout event; false; boolean namedPipe: Named Pipe; false; boolean namedPipeExtended: Named Pipe Extended; false; boolean process: Process creation event; false; boolean registry: Registry event; false; boolean scheduledTask: Scheduled task event; false; boolean smartFileMonitoring: Smart file monitoring; false; boolean url: Ioc URI; false; boolean windowsEventLogs: Windows Event Log; false; boolean windowsEventLogsExtended: Windows Event Log Extended; false; boolean
			iocSupported	Ioc supported for the scope	false	boolean
			isDefault	True if this is the tenant policy	false	boolean
			isDvPolicyPerEventType	FE indication as to how to display DV policy	false	boolean
			mitigationMode	Mitigation modes	false	enum
			mitigationModeSuspicious	Mitigation mode	false	enum
			monitorOnExecute	Monitor on execute on/ off	false	boolean
			monitorOnWrite	Monitor on write	false	boolean

			networkQuarantineOn	Network quarantine on	false	boolean
			remoteOpsForensics	Remote ops forensics configuration	false	

Name	Description	Required	Value
cpuLimit	CPU resources limit for collection process	false	integer
enabled	Enabled	false	boolean
maximumDailyUpload	Maximum size to upload daily	false	integer
maximumDailyUploadLimit	Limit for the maximum size to upload daily	false	integer
maximumFileSizeUpload	Maximum size for single file	false	integer
maximumFileSizeUploadLimit	Limit for the maximum file size to upload	false	integer
parsedArtifactsDestination	Default destination of parsed artifacts	false	enum

			remoteScriptOrchestration	Remote script orchestration upload limits configuration	false	

Name	Description	Required	Value
alwaysUploadStreamToCloud	Always upload streams to cloud	false	boolean
maxDailyFileDownload	Maximum size (MB) to download daily	false	integer
maxDailyFileDownloadLimit	Limit for the maximum size (MB) to download	false	integer

							daily		
						maxDailyFileUpload	Maximum size (MB) to upload daily	false	integer
						maxDailyFileUploadLimit	Limit for the maximum size (MB) to upload daily	false	integer
						maxFileSize	Maximum size in bytes for single file	false	integer
						maxFileSizeLimit	Limit for the maximum file size (MB) to upload	false	integer
						maxLocalPackageDiskUsage	Maximum local disk usage (MB) for packages	false	integer
						maxLocalPackageDiskUsageLimit	Limit for the maximum local disk usage (MB) for packages	false	integer
			removeMacros	Determines if macros should be removed from macro threats	false	boolean			
			researchOn	Share data with SentinelOne	false	boolean			
			scanNewAgents	If True initiate full disk scan upon first registration	false	boolean			
			signedDriverBlockingOn	Suspicious signed driver blocking on/off	false	boolean			

			snapshotsOn	True if snapshots are enabled	false	boolean
			unsignedDriverBlockingOn	Suspicious unsigned driver blocking on/off	false	boolean
			updatedAt	Time of the last update to the policy	false	string
			userFullName	The user that created the policy	false	string
			userId	The user id	false	string
errors	Errors	false	array			

Update Group Policy

PUT /web/api/v2.1/groups/{group_id}/policy

Change the policy for the Group given by ID. Best practice: Get the policy of the Group before you attempt to change it. See also: Get Policy.

BEST PRACTICE

Get the policy of the Group before you attempt to change it. See also: Get Policy.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

404 - Group not found

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
agentLoggingOn	True if logging is enabled in the agent	false	boolean
agentNotification	[DEPRECATED] Show end point notification on suspicious.Replaced by 'show_suspicious' in the agent UI section	false	boolean

			agentUi	Agent ui	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>agentUiOn</td><td>Agent ui on</td><td>false</td><td>boolean</td></tr><tr><td>contactCompany</td><td>Contact company</td><td>false</td><td>string</td></tr><tr><td>contactDirectMessage</td><td>Contact direct message</td><td>false</td><td>string</td></tr><tr><td>contactEmail</td><td>Contact email</td><td>false</td><td>string</td></tr><tr><td>contactFreeText</td><td>Contact free text</td><td>false</td><td>string</td></tr><tr><td>contactOther</td><td>Contact other</td><td>false</td><td>string</td></tr><tr><td>contactPhoneNumber</td><td>Contact phone number</td><td>false</td><td>string</td></tr><tr><td>contactSupportWebsite</td><td>Contact support website</td><td>false</td><td>string</td></tr><tr><td>devicePopUpNotifications</td><td>Device pop up notifications</td><td>false</td><td>boolean</td></tr><tr><td>maxEventAgeDays</td><td>Max event age days</td><td>false</td><td>integer</td></tr><tr><td>showAgentWarnings</td><td>Show agent warnings</td><td>false</td><td>boolean</td></tr><tr><td>showDeviceTab</td><td>Show device tab</td><td>false</td><td>boolean</td></tr><tr><td>showQuarantineTab</td><td>Show quarantine tab</td><td>false</td><td>boolean</td></tr><tr><td>showSupport</td><td>Show support</td><td>false</td><td>boolean</td></tr><tr><td>showSuspicious</td><td>Show suspicious</td><td>false</td><td>boolean</td></tr><tr><td>threatPopUpNotifications</td><td>Threat pop up notifications</td><td>false</td><td>boolean</td></tr></table>
			agentUiOn	[DEPRECATED] Show/hide	false	boolean

				Agent UI. Moved inside the agent UI section		
			allowRemoteShell	True if Remote Shell is enabled for the scope	false	boolean
			antiTamperingOn	Anti tampering on/off	false	boolean
			autoDecommissionDays	Automatic decommission period in days	false	integer
			autoDecommissionOn	Auto decommission on	false	boolean
			autoFileUpload	Automatic file upload configuration	false	

Name	Description	Required	Value
enabled	Automatic file upload on/off	false	boolean
includeBenignFiles	Upload benign files	false	boolean
maxDailyFileUpload	Maximum size (MB) to upload daily	false	integer
maxDailyFileUploadLimit	Limit for the maximum size (MB) to upload daily	false	integer
maxFileSize	Maximum file size (MB) to upload	false	integer
maxFileSizeLimit	Limit for the maximum file size (MB) to upload	false	integer
maxLocalDiskUsage	Maximum local disk	false	integer

							usage (MB) for uploaded files		
						maxLocalDiskUsageLimit	Limit for the maximum local disk usage (MB) for uploaded files	false	integer
			autoImmuneOn	Automatic immune on/off - this value must be true since all policies are immune by default	false	boolean			
			autoMitigationAction	Default action for auto mitigation	false	string			
			cloudValidationOn	Cloud validation on	false				
			createdAt	Timestamp of policy creation	false	string			
			driverBlocking	Suspicious driver blocking engine on/off	false	boolean			
			dvAttributesPerEventType	The DV attributes	false	Name	Description	Required	Value
						autoInstallBrowserExtensions	Auto install browser extensions	false	Name: autoInstallBrowserExtensions; Description: Auto install browser extensions; Required: false; Value: boolean
						behavioralIndicators	Behavioral indicators event	false	Name: dvEventTypeBehavioralIndica; Description: Behavioral indicators; Required: false; Value: boolean

| | | |

										dvEventTypeFileCreation	File Creation Event Type	false	boolean		
										dvEventTypeFileDeletion	File Deletion Event Type	false	boolean		
										dvEventTypeFileModification	File Modification Event Type	false	boolean		
										dvEventTypeFileRename	File Rename Event Type	false	boolean		
										fullDiskScan	File Scan Event Type	false	boolean		
							ip	Network event - IP	false	Name	Description	Required	Value		
										dvEventTypeIpConnect	IP Connect Event Type	false	boolean		
										dvEventTypeIpListen	IP Listen Event Type	false	boolean		
							login	User login/ logout event	false	Name	Description	Required	Value		
										dvEventTypeLoginLoggedIn	User Login Event Type	false	boolean		
										dvEventTypeLoginLoggedOut	User Logout Event Type	false	boolean		
							namedPipe	Named Pipe	false	Name	Description	Required	Value		
										dvEventTypeNamedPipeConnection	Named Pipe Connection Event Type	false	boolean		
										dvEventTypeNamedPipeCreation	Named Pipe Creation Event Type	false	boolean		
							namedPipeExtended	Named Pipe Extended	false	Name	Description	Required	Value		
										namedPipeExtended	Named Pipe Connection Extended Event Type	false	boolean		
							process	Process event	false						

| | | |

									odified	Modified Event Type		
						scheduledTask	Scheduled task event	false	Name	Description	Required	Value
									dvEventTypeScheduledTaskDelete	Scheduled Task Delete Event Type	false	boolean
									dvEventTypeScheduledTaskRegister	Scheduled Task Register Event Type	false	boolean
									dvEventTypeScheduledTaskStart	Scheduled Task Start Event Type	false	boolean
									dvEventTypeScheduledTaskTrigger	Scheduled Task Trigeer Event Type	false	boolean
									dvEventTypeScheduledTaskUpdate	Scheduled Task Update Event Type	false	boolean
						smartFileMonitoring	Smart file monitoring	false	Name	Description	Required	Value
									smartFileMonitoring	Smart file monitoring	false	boolean
						url	URL Actions event	false	Name	Description	Required	Value
									dvEventTypeUrl	URL Actions event	false	boolean
						windowsEventLogs	Windows Event Log	false	Name	Description	Required	Value
									dvEventTypeWindowsEventLogCreation	Windows Event Log Creation Event Type	false	boolean
						windowsEventLogsExtended	Windows Event Log Extended	false	Name	Description	Required	Value
									windowsEventLogsExtended	Windows Event Log Extended Event Type	false	boolean

			engines	The engines statuses	false	

Name	Description	Required	Value
applicationControl	application control	false	enum
dataFiles	data files	false	enum
executables	executables	false	enum
exploits	exploits	false	enum
lateralMovement	lateral movement	false	enum
penetration	penetration	false	enum
preExecution	on-write	false	enum
preExecutionSuspicious	pre execution suspicious	false	enum
pup	potentially unwanted applications (PUP)	false	enum
remoteShell	remote shell	false	enum
reputation	reputation	false	enum

forensicsAutoTriggering	Forensics auto triggering configuration	false	

Name	Description	Required	Value
linuxEnabled	True if linux forensics is enabled	false	boolean
linuxProfileId	The profile id for the linux forensics	false	string
linuxProfileName	The profile name for the linux forensics	false	string
macosEnabled	True if macos forensics is enabled	false	boolean
macosProfileId	The profile id for the macos forensics	false	string
macosProfil	The profile	false	string

						eName: name for the macos forensics windowsEnabled: True if windows forensics is enabled, false, boolean windowsProfileId: The profile id for the windows forensics, false, string windowsProfileName: The profile name for the windows forensics, false, string
			fwForNetworkQuarantineEnabled	True if Firewall Control for Network Quarantine is enabled	false	boolean
			identityEndpointReporting	Endpoint reporting level	false	enum
			identityOn	Identity module on/off	false	boolean
			identityReportInterval	Identity telemetry report interval in minutes	false	integer
			identityThrottlingInterval	Identity duplicate command consolidation interval in minutes	false	integer
			identityUpdateInterval	Identity update interval in	false	integer

			minutes		
		inheritedFrom	Indicates the parent scope from which this policy is inherited, or 'null' if it is not inherited (modified specifically for the current scope).	false	enum
		ioc	True if ioc is enabled	false	boolean
		iocAttributes	The Ioc attributes	false	

Name	Description	Required	Value
autoInstallBrowserExtensions	Update auto install browser extensions	false	boolean
behavioralIndicators	Update behavioral indicators	false	boolean
commandScripts	Update command scripts	false	boolean
crossProcess	Update cross process	false	boolean
dataMasking	Update data masking	false	boolean
dllModuleLoad	Update DLL module load	false	boolean
dns	Network event - DNS	false	boolean
driver	Driver	false	boolean
fds	Full disk scan	false	boolean
file	File event	false	boolean
ip	Network event - IP	false	boolean

						login User login/ logout event false boolean namedPipe Named Pipe false boolean namedPipeExtended Named Pipe Extended false boolean process Process creation event false boolean registry Registry event false boolean scheduledTask Scheduled task event false boolean smartFileMonitoring Smart file monitoring false boolean url Ioc URI false boolean windowsEventLogs Windows Event Log false boolean windowsEventLogsExtended Windows Event Log Extended false boolean
			iocSupported	Ioc supported for the scope	false	boolean
			isDefault	True if this is the tenant policy	false	boolean
			isDvPolicyPerEventType	FE indication as to how to display DV policy	false	boolean
			mitigationMode	Mitigation modes	false	enum
			mitigationModeSuspicious	Mitigation mode	false	enum
			monitorOnExecute	Monitor on execute on/ off	false	boolean
			monitorOnWrite	Monitor on write	false	boolean

			networkQuarantineOn	Network quarantine on	false	boolean
			remoteOpsForensics	Remote ops forensics configuration	false	

Name	Description	Required	Value
cpuLimit	CPU resources limit for collection process	false	integer
enabled	Enabled	false	boolean
maximumDailyUpload	Maximum size to upload daily	false	integer
maximumDailyUploadLimit	Limit for the maximum size to upload daily	false	integer
maximumFileSizeUpload	Maximum size for single file	false	integer
maximumFileSizeUploadLimit	Limit for the maximum file size to upload	false	integer
parsedArtifactsDestination	Default destination of parsed artifacts	false	enum

			remoteScriptOrchestration	Remote script orchestration upload limits configuration	false	

Name	Description	Required	Value
alwaysUploadStreamToCloud	Always upload streams to cloud	false	boolean
maxDailyFileDownload	Maximum size (MB) to download daily	false	integer
maxDailyFileDownloadLimit	Limit for the maximum size (MB) to download	false	integer

							daily		
						maxDailyFileUpload	Maximum size (MB) to upload daily	false	integer
						maxDailyFileUploadLimit	Limit for the maximum size (MB) to upload daily	false	integer
						maxFileSize	Maximum size in bytes for single file	false	integer
						maxFileSizeLimit	Limit for the maximum file size (MB) to upload	false	integer
						maxLocalPackageDiskUsage	Maximum local disk usage (MB) for packages	false	integer
						maxLocalPackageDiskUsageLimit	Limit for the maximum local disk usage (MB) for packages	false	integer
			removeMacros	Determines if macros should be removed from macro threats	false	boolean			
			researchOn	Share data with SentinelOne	false	boolean			
			scanNewAgents	If True initiate full disk scan upon first registration	false	boolean			
			signedDriverBlockingOn	Suspicious signed driver blocking on/off	false	boolean			

			snapshotsOn: True if snapshots are enabled; false; boolean unsignedDriverBlockingOn: Suspicious unsigned driver blocking on/off; false; boolean updatedAt: Time of the last update to the policy; false; string userFullName: The user that created the policy; false; string userId: The user id; false; string
errors	Errors	false	array

Body Schema

Name	Description	Required	Value
data	Data	true	

Name	Description	Required	Value
agentLoggingOn	True if logging is enabled in the agent	false	boolean
agentNotification	[DEPRECATED] Show end point notification on suspicious.Replaced by 'show_suspicious' in the agent UI section	false	boolean
agentUi	Agent ui	false	

Name	Description	Required	Value
agentUiOn	Agent ui on	false	boolean
contactCompany	Contact company	false	string
contactDirectMessage	Contact direct message	false	string
contactEmail	Contact email	false	string
contactFreeText	Contact free text	false	string
contactOther	Contact other	false	string
contactPhoneNumber	Contact phone number	false	string
contactSupportWebsite	Contact support website	false	string
devicePopUpNotifications	Device pop up notifications	false	boolean

						maxEventAgeDays: Max event age days; false; integer showAgentWarnings: Show agent warnings; false; boolean showDeviceTab: Show device tab; false; boolean showQuarantineTab: Show quarantine tab; false; boolean showSupport: Show support; false; boolean showSuspicious: Show suspicious; false; boolean threatPopUpNotifications: Threat pop up notifications; false; boolean
			agentUiOn	[DEPRECATED] Show/hide Agent UI. Moved inside the agent UI section	false	boolean
			allowRemoteShell	True if Remote Shell is enabled for the scope	false	boolean
			antiTamperingOn	Anti tampering on/off	false	boolean
			autoDecommissionDays	Automatic decommission period in days	false	integer
			autoDecommissionOn	Auto decommission on	false	boolean
			autoFileUpload	Automatic file upload configuration	false	Name: enabled; Description: Automatic file upload on/off; Required: false; Value: boolean

						includeBenignFiles	Upload benign files	false	boolean
						maxDailyFileUpload	Maximum size (MB) to upload daily	false	integer
						maxDailyFileUploadLimit	Limit for the maximum size (MB) to upload daily	false	integer
						maxFileSize	Maximum file size (MB) to upload	false	integer
						maxFileSizeLimit	Limit for the maximum file size (MB) to upload	false	integer
						maxLocalDiskUsage	Maximum local disk usage (MB) for uploaded files	false	integer
						maxLocalDiskUsageLimit	Limit for the maximum local disk usage (MB) for uploaded files	false	integer
			autoImmuneOn	Automatic immune on/off - this value must be true since all policies are immune by default	false	boolean			
			autoMitigationAction	Default action for auto mitigation	false	string			
			cloudValidationOn	Cloud validation on	false				

			createdAt	Timestamp of policy creation	false	string
			driverBlocking	Suspicious driver blocking engine on/off	false	boolean
			dvAttributesPerEventType	The DV attributes	false	

Name	Description	Required	Value
autoInstallBrowserExtensions	Auto install browser extensions	false	

Name	Description	Required	Value
autoInstallBrowserExtensions	Auto install browser extensions	false	boolean

Name	Description	Required	Value
behavioralIndicators	Behavioral indicators event	false	

Name	Description	Required	Value
dvEventTypeBehavioralIndicators	Behavioral indicators event	false	boolean

Name	Description	Required	Value
commandScripts	Command scripts event	false	

Name	Description	Required	Value
dvEventTypeCommandScripts	Command scripts event	false	boolean

Name	Description	Required	Value
crossProcess	Cross process event	false	

Name	Description	Required	Value
dvEventTypeCrossProcessDuplicateProcess	Duplicate Process Event Type	false	boolean
dvEventTypeCrossProcessDuplicateThread	Duplicate Thread Event Type	false	boolean
dvEventTypeCrossProcessOpenProcess	Open Process Event Type	false	boolean
dvEventTypeCrossProcessRemoteThread	Remote Thread Event Type	false	boolean

Name	Description	Required	Value
dataMasking	Data masking	false	

Name	Description	Required	Value

| | | |

									LoginLogged Out	Event Type		
						namedPipe	Named Pipe	false	Name	Description	Required	Value
									dvEventType NamedPipeConnection	Named Pipe Connection Event Type	false	boolean
									dvEventType NamedPipeCreation	Named Pipe Creation Event Type	false	boolean
						namedPipeExtended	Named Pipe Extended	false	Name	Description	Required	Value
									namedPipeExtended	Named Pipe Connection Extended Event Type	false	boolean
						process	Process event	false	Name	Description	Required	Value
									dvEventTypeProcessCreation	Process Creation Event Type	false	boolean
									dvEventTypeProcessExit	Process Exit Event Type	false	boolean
									dvEventTypeProcessModification	Process Termination Event Type	false	boolean
						registry	Registry event	false	Name	Description	Required	Value
									dvEventTypeRegistryKeyCreated	Registry Key Created Event Type	false	boolean
									dvEventTypeRegistryKeyDelete	Registry Key Delete Event Type	false	boolean
									dvEventTypeRegistryKeyExport	Registry Key Export Event Type	false	boolean
									dvEventTypeRegistryKeyIm	Registry Key Import Event	false	boolean

| | | |

									toring	monitoring		
						url	URL Actions event	false	Name / Description / Required / Value dvEventTypeUrl / URL Actions event / false / boolean			
						windowsEventLogs	Windows Event Log	false	Name / Description / Required / Value dvEventTypeWindowsEventLogCreation / Windows Event Log Creation Event Type / false / boolean			
						windowsEventLogsExtended	Windows Event Log Extended	false	Name / Description / Required / Value windowsEventLogsExtended / Windows Event Log Extended Event Type / false / boolean			
				engines	The engines statuses	false	Name / Description / Required / Value applicationControl / application control / false / enum dataFiles / data files / false / enum executables / executables / false / enum exploits / exploits / false / enum lateralMovement / lateral movement / false / enum penetration / penetration / false / enum preExecution / on-write / false / enum preExecutionSuspicious / pre execution suspicious / false / enum pup / potentially unwanted applications (PUP) / false / enum remoteShell / remote shell / false / enum reputation / reputation / false / enum			

			forensicsAutoTriggering	Forensics auto triggering configuration	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>linuxEnabled</td><td>True if linux forensics is enabled</td><td>false</td><td>boolean</td></tr><tr><td>linuxProfileId</td><td>The profile id for the linux forensics</td><td>false</td><td>string</td></tr><tr><td>linuxProfileName</td><td>The profile name for the linux forensics</td><td>false</td><td>string</td></tr><tr><td>macosEnabled</td><td>True if macos forensics is enabled</td><td>false</td><td>boolean</td></tr><tr><td>macosProfileId</td><td>The profile id for the macos forensics</td><td>false</td><td>string</td></tr><tr><td>macosProfileName</td><td>The profile name for the macos forensics</td><td>false</td><td>string</td></tr><tr><td>windowsEnabled</td><td>True if windows forensics is enabled</td><td>false</td><td>boolean</td></tr><tr><td>windowsProfileId</td><td>The profile id for the windows forensics</td><td>false</td><td>string</td></tr><tr><td>windowsProfileName</td><td>The profile name for the windows forensics</td><td>false</td><td>string</td></tr></table>
			identityEndpointReporting	Endpoint reporting level	false	enum
			identityOn	Identity module on/off	false	boolean
			identityRepor	Identity	false	integer

			tInterval	telemetry report interval in minutes		
			identityThrottlingInterval	Identity duplicate command consolidation interval in minutes	false	integer
			identityUpdateInterval	Identity update interval in minutes	false	integer
			inheritedFrom	Indicates the parent scope from which this policy is inherited, or 'null' if it is not inherited (modified specifically for the current scope).	false	enum
			ioc	True if ioc is enabled	false	boolean
			iocAttributes	The Ioc attributes	false	

Name	Description	Required	Value
autoInstallBrowserExtensions	Update auto install browser extensions	false	boolean
behavioralIndicators	Update behavioral indicators	false	boolean
commandScripts	Update command scripts	false	boolean
crossProcess	Update cross process	false	boolean

						dataMasking	Update data masking	false	boolean
						dllModuleLoad	Update DLL module load	false	boolean
						dns	Network event - DNS	false	boolean
						driver	Driver	false	boolean
						fds	Full disk scan	false	boolean
						file	File event	false	boolean
						ip	Network event - IP	false	boolean
						login	User login/ logout event	false	boolean
						namedPipe	Named Pipe	false	boolean
						namedPipeExtended	Named Pipe Extended	false	boolean
						process	Process creation event	false	boolean
						registry	Registry event	false	boolean
						scheduledTask	Scheduled task event	false	boolean
						smartFileMonitoring	Smart file monitoring	false	boolean
						url	Ioc URI	false	boolean
						windowsEventLogs	Windows Event Log	false	boolean
						windowsEventLogsExtended	Windows Event Log Extended	false	boolean
				iocSupported	Ioc supported for the scope	false	boolean		
				isDefault	True if this is the tenant policy	false	boolean		

			isDvPolicyPerEventType	FE indication as to how to display DV policy	false	boolean
			mitigationMode	Mitigation modes	false	enum
			mitigationModeSuspicious	Mitigation mode	false	enum
			monitorOnExecute	Monitor on execute on/off	false	boolean
			monitorOnWrite	Monitor on write	false	boolean
			networkQuarantineOn	Network quarantine on	false	boolean
			remoteOpsForensics	Remote ops forensics configuration	false	

Name	Description	Required	Value
cpuLimit	CPU resources limit for collection process	false	integer
enabled	Enabled	false	boolean
maximumDailyUpload	Maximum size to upload daily	false	integer
maximumDailyUploadLimit	Limit for the maximum size to upload daily	false	integer
maximumFileSizeUpload	Maximum size for single file	false	integer
maximumFileSizeUploadLimit	Limit for the maximum file size to upload	false	integer
parsedArtifactsDestination	Default destination of parsed artifacts	false	enum

			remoteScriptOrchestration	Remote script orchestration upload limits configuration	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>alwaysUploadStreamToCloud</td><td>Always upload streams to cloud</td><td>false</td><td>boolean</td></tr><tr><td>maxDailyFileDownload</td><td>Maximum size (MB) to download daily</td><td>false</td><td>integer</td></tr><tr><td>maxDailyFileDownloadLimit</td><td>Limit for the maximum size (MB) to download daily</td><td>false</td><td>integer</td></tr><tr><td>maxDailyFileUpload</td><td>Maximum size (MB) to upload daily</td><td>false</td><td>integer</td></tr><tr><td>maxDailyFileUploadLimit</td><td>Limit for the maximum size (MB) to upload daily</td><td>false</td><td>integer</td></tr><tr><td>maxFileSize</td><td>Maximum size in bytes for single file</td><td>false</td><td>integer</td></tr><tr><td>maxFileSizeLimit</td><td>Limit for the maximum file size (MB) to upload</td><td>false</td><td>integer</td></tr><tr><td>maxLocalPackageDiskUsage</td><td>Maximum local disk usage (MB) for packages</td><td>false</td><td>integer</td></tr><tr><td>maxLocalPackageDiskUsageLimit</td><td>Limit for the maximum local disk usage (MB) for packages</td><td>false</td><td>integer</td></tr></table>
			removeMacros	Determines if macros should be removed	false	boolean

				from macro threats		
			researchOn	Share data with SentinelOne	false	boolean
			scanNewAgents	If True initiate full disk scan upon first registration	false	boolean
			signedDriverBlockingOn	Suspicious signed driver blocking on/off	false	boolean
			snapshotsOn	True if snapshots are enabled	false	boolean
			unsignedDriverBlockingOn	Suspicious unsigned driver blocking on/off	false	boolean
			updatedAt	Time of the last update to the policy	false	string
			userFullName	The user that created the policy	false	string
			userId	The user id	false	string

Site Policy

GET /web/api/v2.1/sites/{site_id}/policy

Get the policy of the Site given by ID. To get the ID of a Site, run "sites". See also: Get Policy.

Response Messages

200 - Success

401 - Unauthorized access - please sign in and retry.

404 - Policy not found

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
agentLoggingOn	True if logging is enabled in the agent	false	boolean
agentNotification	[DEPRECATED] Show end point notification on suspicious.Replaced by 'show_suspicious' in the agent UI section	false	boolean
agentUi	Agent ui	false	

Name	Description	Required	Value
agentUiOn	Agent ui on	false	boolean
contactCompany	Contact company	false	string
contactDirec	Contact	false	string

						tMessage	direct message			
						contactEmail	Contact email	false	string	
						contactFreeText	Contact free text	false	string	
						contactOther	Contact other	false	string	
						contactPhoneNumber	Contact phone number	false	string	
						contactSupportWebsite	Contact support website	false	string	
						devicePopUpNotifications	Device pop up notifications	false	boolean	
						maxEventAgeDays	Max event age days	false	integer	
						showAgentWarnings	Show agent warnings	false	boolean	
						showDeviceTab	Show device tab	false	boolean	
						showQuarantineTab	Show quarantine tab	false	boolean	
						showSupport	Show support	false	boolean	
						showSuspicious	Show suspicious	false	boolean	
						threatPopUpNotifications	Threat pop up notifications	false	boolean	
				agentUiOn	[DEPRECATED] Show/hide Agent UI. Moved inside the agent UI section	false	boolean			
				allowRemoteShell	True if Remote Shell	false	boolean			

				is enabled for the scope		
			antiTamperingOn	Anti tampering on/off	false	boolean
			autoDecommissionDays	Automatic decommission period in days	false	integer
			autoDecommissionOn	Auto decommission on	false	boolean
			autoFileUpload	Automatic file upload configuration	false	

Name	Description	Required	Value
enabled	Automatic file upload on/off	false	boolean
includeBenignFiles	Upload benign files	false	boolean
maxDailyFileUpload	Maximum size (MB) to upload daily	false	integer
maxDailyFileUploadLimit	Limit for the maximum size (MB) to upload daily	false	integer
maxFileSize	Maximum file size (MB) to upload	false	integer
maxFileSizeLimit	Limit for the maximum file size (MB) to upload	false	integer
maxLocalDiskUsage	Maximum local disk usage (MB) for uploaded files	false	integer
maxLocalDiskUsageLimit	Limit for the maximum local disk	false	integer

							usage (MB) for uploaded files			
			autoImmuneOn	Automatic immune on/off - this value must be true since all policies are immune by default	false	boolean				
			autoMitigationAction	Default action for auto mitigation	false	string				
			cloudValidationOn	Cloud validation on	false					
			createdAt	Timestamp of policy creation	false	string				
			driverBlocking	Suspicious driver blocking engine on/off	false	boolean				
			dvAttributesPerEventType	The DV attributes	false	Name	Description	Required	Value	
						autoInstallBrowserExtensions	Auto install browser extensions	false	Name	Description	Required	Value
									autoInstallBrowserExtensions	Auto install browser extensions	false	boolean
						behavioralIndicators	Behavioral indicators event	false	Name	Description	Required	Value
									dvEventTypeBehavioralIndicators	Behavioral indicators event	false	boolean
						commandScripts	Command scripts event	false	Name	Description	Required	Value
									dvEventTypeCommandScripts	Command scripts event	false	boolean

| | | |

| | | |

										dvEventTypeScheduledTaskRegister	Scheduled Task Register Event Type	false	boolean
										dvEventTypeScheduledTaskStart	Scheduled Task Start Event Type	false	boolean
										dvEventTypeScheduledTaskTrigger	Scheduled Task Trigeer Event Type	false	boolean
										dvEventTypeScheduledTaskUpdate	Scheduled Task Update Event Type	false	boolean
							smartFileMonitoring	Smart file monitoring	false	Name	Description	Required	Value
										smartFileMonitoring	Smart file monitoring	false	boolean
							url	URL Actions event	false	Name	Description	Required	Value
										dvEventTypeUrl	URL Actions event	false	boolean
							windowsEventLogs	Windows Event Log	false	Name	Description	Required	Value
										dvEventTypeWindowsEventLogCreation	Windows Event Log Creation Event Type	false	boolean
							windowsEventLogsExtended	Windows Event Log Extended	false	Name	Description	Required	Value
										windowsEventLogsExtended	Windows Event Log Extended Event Type	false	boolean
				engines	The engines statuses	false	Name	Description	Required	Value			
							applicationControl	application control	false	enum			
							dataFiles	data files	false	enum			
							executables	executables	false	enum			

						exploits	exploits	false	enum
						lateralMovement	lateral movement	false	enum
						penetration	penetration	false	enum
						preExecution	on-write	false	enum
						preExecutionSuspicious	pre execution suspicious	false	enum
						pup	potentially unwanted applications (PUP)	false	enum
						remoteShell	remote shell	false	enum
						reputation	reputation	false	enum
				forensicsAutoTriggering	Forensics auto triggering configuration	false			

Name	Description	Required	Value
linuxEnabled	True if linux forensics is enabled	false	boolean
linuxProfileId	The profile id for the linux forensics	false	string
linuxProfileName	The profile name for the linux forensics	false	string
macosEnabled	True if macos forensics is enabled	false	boolean
macosProfileId	The profile id for the macos forensics	false	string
macosProfileName	The profile name for the macos forensics	false	string
windowsEnabled	True if windows forensics is enabled	false	boolean

						windowsProfileId: The profile id for the windows forensics; false; string windowsProfileName: The profile name for the windows forensics; false; string
			fwForNetworkQuarantineEnabled	True if Firewall Control for Network Quarantine is enabled	false	boolean
			identityEndpointReporting	Endpoint reporting level	false	enum
			identityOn	Identity module on/off	false	boolean
			identityReportInterval	Identity telemetry report interval in minutes	false	integer
			identityThrottlingInterval	Identity duplicate command consolidation interval in minutes	false	integer
			identityUpdateInterval	Identity update interval in minutes	false	integer
			inheritedFrom	Indicates the parent scope from which this policy is inherited, or 'null' if it is not inherited	false	enum

				(modified specifically for the current scope).		
			ioc	True if ioc is enabled	false	boolean
			iocAttributes	The Ioc attributes	false	

Name	Description	Required	Value
autoInstallBrowserExtensions	Update auto install browser extensions	false	boolean
behavioralIndicators	Update behavioral indicators	false	boolean
commandScripts	Update command scripts	false	boolean
crossProcess	Update cross process	false	boolean
dataMasking	Update data masking	false	boolean
dllModuleLoad	Update DLL module load	false	boolean
dns	Network event - DNS	false	boolean
driver	Driver	false	boolean
fds	Full disk scan	false	boolean
file	File event	false	boolean
ip	Network event - IP	false	boolean
login	User login/ logout event	false	boolean
namedPipe	Named Pipe	false	boolean
namedPipeExtended	Named Pipe Extended	false	boolean
process	Process	false	boolean

						creation event		
						registry	Registry event	false	boolean
						scheduledTask	Scheduled task event	false	boolean
						smartFileMonitoring	Smart file monitoring	false	boolean
						url	Ioc URI	false	boolean
						windowsEventLogs	Windows Event Log	false	boolean
						windowsEventLogsExtended	Windows Event Log Extended	false	boolean
			iocSupported	Ioc supported for the scope	false	boolean
			isDefault	True if this is the tenant policy	false	boolean
			isDvPolicyPerEventType	FE indication as to how to display DV policy	false	boolean
			mitigationMode	Mitigation modes	false	enum
			mitigationModeSuspicious	Mitigation mode	false	enum
			monitorOnExecute	Monitor on execute on/off	false	boolean
			monitorOnWrite	Monitor on write	false	boolean
			networkQuarantineOn	Network quarantine on	false	boolean
			remoteOpsForensics	Remote ops forensics configuration	false	Name | Description | Required | Value cpuLimit | CPU resources | false | integer

							limit for collection process		
						enabled	Enabled	false	boolean
						maximumDailyUpload	Maximum size to upload daily	false	integer
						maximumDailyUploadLimit	Limit for the maximum size to upload daily	false	integer
						maximumFileSizeUpload	Maximum size for single file	false	integer
						maximumFileSizeUploadLimit	Limit for the maximum file size to upload	false	integer
						parsedArtifactsDestination	Default destination of parsed artifacts	false	enum
				remoteScriptOrchestration	Remote script orchestration upload limits configuration	false	Name	Description	Required	Value
							alwaysUploadStreamToCloud	Always upload streams to cloud	false	boolean
							maxDailyFileDownload	Maximum size (MB) to download daily	false	integer
							maxDailyFileDownloadLimit	Limit for the maximum size (MB) to download daily	false	integer
							maxDailyFileUpload	Maximum size (MB) to upload daily	false	integer
							maxDailyFile	Limit for the	false	integer

						UploadLimit: maximum size (MB) to upload daily maxFileSize: Maximum size in bytes for single file; false; integer maxFileSizeLimit: Limit for the maximum file size (MB) to upload; false; integer maxLocalPackageDiskUsage: Maximum local disk usage (MB) for packages; false; integer maxLocalPackageDiskUsageLimit: Limit for the maximum local disk usage (MB) for packages; false; integer
			removeMacros	Determines if macros should be removed from macro threats	false	boolean
			researchOn	Share data with SentinelOne	false	boolean
			scanNewAgents	If True initiate full disk scan upon first registration	false	boolean
			signedDriverBlockingOn	Suspicious signed driver blocking on/off	false	boolean
			snapshotsOn	True if snapshots are enabled	false	boolean
			unsignedDriverBlockingOn	Suspicious unsigned	false	boolean

				driver blocking on/off		
			updatedAt	Time of the last update to the policy	false	string
			userFullName	The user that created the policy	false	string
			userId	The user id	false	string
errors	Errors	false	array			

Update Site Policy

PUT /web/api/v2.1/sites/{site_id}/policy

Change the policy for the Site given by ID. Best practice: Get the policy of the Site before you attempt to change it. See also: Get Policy.

BEST PRACTICE

Get the policy of the Site before you attempt to change it. See also: Get Policy.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

404 - Site not found

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
agentLoggingOn	True if logging is enabled in the agent	false	boolean
agentNotification	[DEPRECATED] Show end point notification on suspicious.Replaced by 'show_suspicious' in the agent UI section	false	boolean

			agentUi	Agent ui	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>agentUiOn</td><td>Agent ui on</td><td>false</td><td>boolean</td></tr><tr><td>contactCompany</td><td>Contact company</td><td>false</td><td>string</td></tr><tr><td>contactDirectMessage</td><td>Contact direct message</td><td>false</td><td>string</td></tr><tr><td>contactEmail</td><td>Contact email</td><td>false</td><td>string</td></tr><tr><td>contactFreeText</td><td>Contact free text</td><td>false</td><td>string</td></tr><tr><td>contactOther</td><td>Contact other</td><td>false</td><td>string</td></tr><tr><td>contactPhoneNumber</td><td>Contact phone number</td><td>false</td><td>string</td></tr><tr><td>contactSupportWebsite</td><td>Contact support website</td><td>false</td><td>string</td></tr><tr><td>devicePopUpNotifications</td><td>Device pop up notifications</td><td>false</td><td>boolean</td></tr><tr><td>maxEventAgeDays</td><td>Max event age days</td><td>false</td><td>integer</td></tr><tr><td>showAgentWarnings</td><td>Show agent warnings</td><td>false</td><td>boolean</td></tr><tr><td>showDeviceTab</td><td>Show device tab</td><td>false</td><td>boolean</td></tr><tr><td>showQuarantineTab</td><td>Show quarantine tab</td><td>false</td><td>boolean</td></tr><tr><td>showSupport</td><td>Show support</td><td>false</td><td>boolean</td></tr><tr><td>showSuspicious</td><td>Show suspicious</td><td>false</td><td>boolean</td></tr><tr><td>threatPopUpNotifications</td><td>Threat pop up notifications</td><td>false</td><td>boolean</td></tr></table>
			agentUiOn	[DEPRECATED] Show/hide	false	boolean

				Agent UI. Moved inside the agent UI section		
			allowRemoteShell	True if Remote Shell is enabled for the scope	false	boolean
			antiTamperingOn	Anti tampering on/off	false	boolean
			autoDecommissionDays	Automatic decommission period in days	false	integer
			autoDecommissionOn	Auto decommission on	false	boolean
			autoFileUpload	Automatic file upload configuration	false	

Name	Description	Required	Value
enabled	Automatic file upload on/off	false	boolean
includeBenignFiles	Upload benign files	false	boolean
maxDailyFileUpload	Maximum size (MB) to upload daily	false	integer
maxDailyFileUploadLimit	Limit for the maximum size (MB) to upload daily	false	integer
maxFileSize	Maximum file size (MB) to upload	false	integer
maxFileSizeLimit	Limit for the maximum file size (MB) to upload	false	integer
maxLocalDiskUsage	Maximum local disk	false	integer

						usage (MB) for uploaded files			
						maxLocalDiskUsageLimit	Limit for the maximum local disk usage (MB) for uploaded files	false	integer
			autoImmuneOn	Automatic immune on/off - this value must be true since all policies are immune by default	false	boolean			
			autoMitigationAction	Default action for auto mitigation	false	string			
			cloudValidationOn	Cloud validation on	false				
			createdAt	Timestamp of policy creation	false	string			
			driverBlocking	Suspicious driver blocking engine on/off	false	boolean			
			dvAttributesPerEventType	The DV attributes	false	Name	Description	Required	Value
						autoInstallBrowserExtensions	Auto install browser extensions	false	Name: autoInstallBrowserExtensions; Description: Auto install browser extensions; Required: false; Value: boolean
						behavioralIndicators	Behavioral indicators event	false	Name: dvEventTypeBehavioralIndica; Description: Behavioral indicators; Required: false; Value: boolean

| | | |

										dvEventTypeFileCreation	File Creation Event Type	false	boolean		
										dvEventTypeFileDeletion	File Deletion Event Type	false	boolean		
										dvEventTypeFileModification	File Modification Event Type	false	boolean		
										dvEventTypeFileRename	File Rename Event Type	false	boolean		
										fullDiskScan	File Scan Event Type	false	boolean		
								ip	Network event - IP	false	Name	Description	Required	Value	
											dvEventTypeIpConnect	IP Connect Event Type	false	boolean	
											dvEventTypeIpListen	IP Listen Event Type	false	boolean	
								login	User login/ logout event	false	Name	Description	Required	Value	
											dvEventTypeLoginLoggedIn	User Login Event Type	false	boolean	
											dvEventTypeLoginLoggedOut	User Logout Event Type	false	boolean	
								namedPipe	Named Pipe	false	Name	Description	Required	Value	
											dvEventTypeNamedPipeConnection	Named Pipe Connection Event Type	false	boolean	
											dvEventTypeNamedPipeCreation	Named Pipe Creation Event Type	false	boolean	
								namedPipeExtended	Named Pipe Extended	false	Name	Description	Required	Value	
											namedPipeExtended	Named Pipe Connection Extended Event Type	false	boolean	
								process	Process event	false					

									Name	Description	Required	Value
									dvEventTypeProcessCreation	Process Creation Event Type	false	boolean
									dvEventTypeProcessExit	Process Exit Event Type	false	boolean
									dvEventTypeProcessModification	Process Termination Event Type	false	boolean
							registry	Registry event	false			
									Name	Description	Required	Value
									dvEventTypeRegistryKeyCreated	Registry Key Created Event Type	false	boolean
									dvEventTypeRegistryKeyDelete	Registry Key Delete Event Type	false	boolean
									dvEventTypeRegistryKeyExport	Registry Key Export Event Type	false	boolean
									dvEventTypeRegistryKeyImport	Registry Key Import Event Type	false	boolean
									dvEventType RegistryKey Rename	Registry Key Rename Event Type	false	boolean
									dvEventTypeRegistryKeySecurityChanged	Registry Key Security Changed Event Type	false	boolean
									dvEventTypeRegistryValueCreated	Registry Value Crated Event Type	false	boolean
									dvEventTypeRegistryValueDeleted	Registry Value Deleted Event Type	false	boolean
									dvEventTypeRegistryValueM	Registry Value	false	boolean

									odified	Modified Event Type		
						scheduledTask	Scheduled task event	false				
									Name	Description	Required	Value
									dvEventTypeScheduledTaskDelete	Scheduled Task Delete Event Type	false	boolean
									dvEventTypeScheduledTaskRegister	Scheduled Task Register Event Type	false	boolean
									dvEventTypeScheduledTaskStart	Scheduled Task Start Event Type	false	boolean
									dvEventTypeScheduledTaskTrigger	Scheduled Task Trigeer Event Type	false	boolean
									dvEventTypeScheduledTaskUpdate	Scheduled Task Update Event Type	false	boolean
						smartFileMonitoring	Smart file monitoring	false				
									Name	Description	Required	Value
									smartFileMonitoring	Smart file monitoring	false	boolean
						url	URL Actions event	false				
									Name	Description	Required	Value
									dvEventTypeUrl	URL Actions event	false	boolean
						windowsEventLogs	Windows Event Log	false				
									Name	Description	Required	Value
									dvEventTypeWindowsEventLogCreation	Windows Event Log Creation Event Type	false	boolean
						windowsEventLogsExtended	Windows Event Log Extended	false				
									Name	Description	Required	Value
									windowsEventLogsExtended	Windows Event Log Extended Event Type	false	boolean

			engines	The engines statuses	false

Name	Description	Required	Value
applicationControl	application control	false	enum
dataFiles	data files	false	enum
executables	executables	false	enum
exploits	exploits	false	enum
lateralMovement	lateral movement	false	enum
penetration	penetration	false	enum
preExecution	on-write	false	enum
preExecutionSuspicious	pre execution suspicious	false	enum
pup	potentially unwanted applications (PUP)	false	enum
remoteShell	remote shell	false	enum
reputation	reputation	false	enum

forensicsAutoTriggering	Forensics auto triggering configuration	false	

Name	Description	Required	Value
linuxEnabled	True if linux forensics is enabled	false	boolean
linuxProfileId	The profile id for the linux forensics	false	string
linuxProfileName	The profile name for the linux forensics	false	string
macosEnabled	True if macos forensics is enabled	false	boolean
macosProfileId	The profile id for the macos forensics	false	string
macosProfil	The profile	false	string

						eName: name for the macos forensics windowsEnabled: True if windows forensics is enabled, false, boolean windowsProfileId: The profile id for the windows forensics, false, string windowsProfileName: The profile name for the windows forensics, false, string
			fwForNetworkQuarantineEnabled	True if Firewall Control for Network Quarantine is enabled	false	boolean
			identityEndpointReporting	Endpoint reporting level	false	enum
			identityOn	Identity module on/off	false	boolean
			identityReportInterval	Identity telemetry report interval in minutes	false	integer
			identityThrottlingInterval	Identity duplicate command consolidation interval in minutes	false	integer
			identityUpdateInterval	Identity update interval in	false	integer

			minutes		
		inheritedFrom	Indicates the parent scope from which this policy is inherited, or 'null' if it is not inherited (modified specifically for the current scope).	false	enum
		ioc	True if ioc is enabled	false	boolean
		iocAttributes	The Ioc attributes	false	

Name	Description	Required	Value
autoInstallBrowserExtensions	Update auto install browser extensions	false	boolean
behavioralIndicators	Update behavioral indicators	false	boolean
commandScripts	Update command scripts	false	boolean
crossProcess	Update cross process	false	boolean
dataMasking	Update data masking	false	boolean
dllModuleLoad	Update DLL module load	false	boolean
dns	Network event - DNS	false	boolean
driver	Driver	false	boolean
fds	Full disk scan	false	boolean
file	File event	false	boolean
ip	Network event - IP	false	boolean

						login: User login/ logout event; false; boolean namedPipe: Named Pipe; false; boolean namedPipeExtended: Named Pipe Extended; false; boolean process: Process creation event; false; boolean registry: Registry event; false; boolean scheduledTask: Scheduled task event; false; boolean smartFileMonitoring: Smart file monitoring; false; boolean url: Ioc URI; false; boolean windowsEventLogs: Windows Event Log; false; boolean windowsEventLogsExtended: Windows Event Log Extended; false; boolean
			iocSupported	Ioc supported for the scope	false	boolean
			isDefault	True if this is the tenant policy	false	boolean
			isDvPolicyPerEventType	FE indication as to how to display DV policy	false	boolean
			mitigationMode	Mitigation modes	false	enum
			mitigationModeSuspicious	Mitigation mode	false	enum
			monitorOnExecute	Monitor on execute on/ off	false	boolean
			monitorOnWrite	Monitor on write	false	boolean

			networkQuarantineOn	Network quarantine on	false	boolean
			remoteOpsForensics	Remote ops forensics configuration	false	

Name	Description	Required	Value
cpuLimit	CPU resources limit for collection process	false	integer
enabled	Enabled	false	boolean
maximumDailyUpload	Maximum size to upload daily	false	integer
maximumDailyUploadLimit	Limit for the maximum size to upload daily	false	integer
maximumFileSizeUpload	Maximum size for single file	false	integer
maximumFileSizeUploadLimit	Limit for the maximum file size to upload	false	integer
parsedArtifactsDestination	Default destination of parsed artifacts	false	enum

			remoteScriptOrchestration	Remote script orchestration upload limits configuration	false	

Name	Description	Required	Value
alwaysUploadStreamToCloud	Always upload streams to cloud	false	boolean
maxDailyFileDownload	Maximum size (MB) to download daily	false	integer
maxDailyFileDownloadLimit	Limit for the maximum size (MB) to download	false	integer

						daily
						maxDailyFileUpload: Maximum size (MB) to upload daily; false; integer
						maxDailyFileUploadLimit: Limit for the maximum size (MB) to upload daily; false; integer
						maxFileSize: Maximum size in bytes for single file; false; integer
						maxFileSizeLimit: Limit for the maximum file size (MB) to upload; false; integer
						maxLocalPackageDiskUsage: Maximum local disk usage (MB) for packages; false; integer
						maxLocalPackageDiskUsageLimit: Limit for the maximum local disk usage (MB) for packages; false; integer
			removeMacros	Determines if macros should be removed from macro threats	false	boolean
			researchOn	Share data with SentinelOne	false	boolean
			scanNewAgents	If True initiate full disk scan upon first registration	false	boolean
			signedDriverBlockingOn	Suspicious signed driver blocking on/off	false	boolean

			snapshotsOn: True if snapshots are enabled; false; boolean unsignedDriverBlockingOn: Suspicious unsigned driver blocking on/off; false; boolean updatedAt: Time of the last update to the policy; false; string userFullName: The user that created the policy; false; string userId: The user id; false; string
errors	Errors	false	array

Body Schema

Name	Description	Required	Value
data	Data	true	

Name	Description	Required	Value
agentLoggingOn	True if logging is enabled in the agent	false	boolean
agentNotification	[DEPRECATED] Show end point notification on suspicious.Replaced by 'show_suspicious' in the agent UI section	false	boolean
agentUi	Agent ui	false	

Name	Description	Required	Value
agentUiOn	Agent ui on	false	boolean
contactCompany	Contact company	false	string
contactDirectMessage	Contact direct message	false	string
contactEmail	Contact email	false	string
contactFreeText	Contact free text	false	string
contactOther	Contact other	false	string
contactPhoneNumber	Contact phone number	false	string
contactSupportWebsite	Contact support website	false	string
devicePopUpNotifications	Device pop up notifications	false	boolean

						maxEventAgeDays: Max event age days; false; integer showAgentWarnings: Show agent warnings; false; boolean showDeviceTab: Show device tab; false; boolean showQuarantineTab: Show quarantine tab; false; boolean showSupport: Show support; false; boolean showSuspicious: Show suspicious; false; boolean threatPopUpNotifications: Threat pop up notifications; false; boolean
			agentUiOn	[DEPRECATED] Show/hide Agent UI. Moved inside the agent UI section	false	boolean
			allowRemoteShell	True if Remote Shell is enabled for the scope	false	boolean
			antiTamperingOn	Anti tampering on/off	false	boolean
			autoDecommissionDays	Automatic decommission period in days	false	integer
			autoDecommissionOn	Auto decommission on	false	boolean
			autoFileUpload	Automatic file upload configuration	false	Name: enabled; Description: Automatic file upload on/off; Required: false; Value: boolean

						includeBenignFiles	Upload benign files	false	boolean
						maxDailyFileUpload	Maximum size (MB) to upload daily	false	integer
						maxDailyFileUploadLimit	Limit for the maximum size (MB) to upload daily	false	integer
						maxFileSize	Maximum file size (MB) to upload	false	integer
						maxFileSizeLimit	Limit for the maximum file size (MB) to upload	false	integer
						maxLocalDiskUsage	Maximum local disk usage (MB) for uploaded files	false	integer
						maxLocalDiskUsageLimit	Limit for the maximum local disk usage (MB) for uploaded files	false	integer
			autoImmuneOn	Automatic immune on/off - this value must be true since all policies are immune by default	false	boolean			
			autoMitigationAction	Default action for auto mitigation	false	string			
			cloudValidationOn	Cloud validation on	false				

			createdAt	Timestamp of policy creation	false	string
			driverBlocking	Suspicious driver blocking engine on/off	false	boolean
			dvAttributesPerEventType	The DV attributes	false	

Name	Description	Required	Value
autoInstallBrowserExtensions	Auto install browser extensions	false	

Name	Description	Required	Value
autoInstallBrowserExtensions	Auto install browser extensions	false	boolean

Name	Description	Required	Value
behavioralIndicators	Behavioral indicators event	false	

Name	Description	Required	Value
dvEventTypeBehavioralIndicators	Behavioral indicators event	false	boolean

Name	Description	Required	Value
commandScripts	Command scripts event	false	

Name	Description	Required	Value
dvEventTypeCommandScripts	Command scripts event	false	boolean

Name	Description	Required	Value
crossProcess	Cross process event	false	

Name	Description	Required	Value
dvEventTypeCrossProcessDuplicateProcess	Duplicate Process Event Type	false	boolean
dvEventTypeCrossProcessDuplicateThread	Duplicate Thread Event Type	false	boolean
dvEventTypeCrossProcessOpenProcess	Open Process Event Type	false	boolean
dvEventTypeCrossProcessRemoteThread	Remote Thread Event Type	false	boolean

Name	Description	Required	Value
dataMasking	Data masking	false	

Name	Description	Required	Value

| | | |

| | | |

| | | |

									toring	monitoring		
						url	URL Actions event	false	Name: dvEventTypeUrl Description: URL Actions event Required: false Value: boolean			
						windowsEventLogs	Windows Event Log	false	Name: dvEventTypeWindowsEventLogCreation Description: Windows Event Log Creation Event Type Required: false Value: boolean			
						windowsEventLogsExtended	Windows Event Log Extended	false	Name: windowsEventLogsExtended Description: Windows Event Log Extended Event Type Required: false Value: boolean			
				engines	The engines statuses	false	Name: applicationControl Description: application control Required: false Value: enum Name: dataFiles Description: data files Required: false Value: enum Name: executables Description: executables Required: false Value: enum Name: exploits Description: exploits Required: false Value: enum Name: lateralMovement Description: lateral movement Required: false Value: enum Name: penetration Description: penetration Required: false Value: enum Name: preExecution Description: on-write Required: false Value: enum Name: preExecutionSuspicious Description: pre execution suspicious Required: false Value: enum Name: pup Description: potentially unwanted applications (PUP) Required: false Value: enum Name: remoteShell Description: remote shell Required: false Value: enum Name: reputation Description: reputation Required: false Value: enum			

			forensicsAutoTriggering	Forensics auto triggering configuration	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>linuxEnabled</td><td>True if linux forensics is enabled</td><td>false</td><td>boolean</td></tr><tr><td>linuxProfileId</td><td>The profile id for the linux forensics</td><td>false</td><td>string</td></tr><tr><td>linuxProfileName</td><td>The profile name for the linux forensics</td><td>false</td><td>string</td></tr><tr><td>macosEnabled</td><td>True if macos forensics is enabled</td><td>false</td><td>boolean</td></tr><tr><td>macosProfileId</td><td>The profile id for the macos forensics</td><td>false</td><td>string</td></tr><tr><td>macosProfileName</td><td>The profile name for the macos forensics</td><td>false</td><td>string</td></tr><tr><td>windowsEnabled</td><td>True if windows forensics is enabled</td><td>false</td><td>boolean</td></tr><tr><td>windowsProfileId</td><td>The profile id for the windows forensics</td><td>false</td><td>string</td></tr><tr><td>windowsProfileName</td><td>The profile name for the windows forensics</td><td>false</td><td>string</td></tr></table>
			identityEndpointReporting	Endpoint reporting level	false	enum
			identityOn	Identity module on/off	false	boolean
			identityRepor	Identity	false	integer

			tInterval	telemetry report interval in minutes		
			identityThrottlingInterval	Identity duplicate command consolidation interval in minutes	false	integer
			identityUpdateInterval	Identity update interval in minutes	false	integer
			inheritedFrom	Indicates the parent scope from which this policy is inherited, or 'null' if it is not inherited (modified specifically for the current scope).	false	enum
			ioc	True if ioc is enabled	false	boolean
			iocAttributes	The Ioc attributes	false	

Name	Description	Required	Value
autoInstallBrowserExtensions	Update auto install browser extensions	false	boolean
behavioralIndicators	Update behavioral indicators	false	boolean
commandScripts	Update command scripts	false	boolean
crossProcess	Update cross process	false	boolean

						dataMasking	Update data masking	false	boolean
						dllModuleLoad	Update DLL module load	false	boolean
						dns	Network event - DNS	false	boolean
						driver	Driver	false	boolean
						fds	Full disk scan	false	boolean
						file	File event	false	boolean
						ip	Network event - IP	false	boolean
						login	User login/ logout event	false	boolean
						namedPipe	Named Pipe	false	boolean
						namedPipeExtended	Named Pipe Extended	false	boolean
						process	Process creation event	false	boolean
						registry	Registry event	false	boolean
						scheduledTask	Scheduled task event	false	boolean
						smartFileMonitoring	Smart file monitoring	false	boolean
						url	Ioc URI	false	boolean
						windowsEventLogs	Windows Event Log	false	boolean
						windowsEventLogsExtended	Windows Event Log Extended	false	boolean
				iocSupported	Ioc supported for the scope	false	boolean		
				isDefault	True if this is the tenant policy	false	boolean		

			isDvPolicyPerEventType	FE indication as to how to display DV policy	false	boolean
			mitigationMode	Mitigation modes	false	enum
			mitigationModeSuspicious	Mitigation mode	false	enum
			monitorOnExecute	Monitor on execute on/off	false	boolean
			monitorOnWrite	Monitor on write	false	boolean
			networkQuarantineOn	Network quarantine on	false	boolean
			remoteOpsForensics	Remote ops forensics configuration	false	

Name	Description	Required	Value
cpuLimit	CPU resources limit for collection process	false	integer
enabled	Enabled	false	boolean
maximumDailyUpload	Maximum size to upload daily	false	integer
maximumDailyUploadLimit	Limit for the maximum size to upload daily	false	integer
maximumFileSizeUpload	Maximum size for single file	false	integer
maximumFileSizeUploadLimit	Limit for the maximum file size to upload	false	integer
parsedArtifactsDestination	Default destination of parsed artifacts	false	enum

			remoteScriptOrchestration	Remote script orchestration upload limits configuration	false
			removeMacros	Determines if macros should be removed	false

Name	Description	Required	Value
alwaysUploadStreamToCloud	Always upload streams to cloud	false	boolean
maxDailyFileDownload	Maximum size (MB) to download daily	false	integer
maxDailyFileDownloadLimit	Limit for the maximum size (MB) to download daily	false	integer
maxDailyFileUpload	Maximum size (MB) to upload daily	false	integer
maxDailyFileUploadLimit	Limit for the maximum size (MB) to upload daily	false	integer
maxFileSize	Maximum size in bytes for single file	false	integer
maxFileSizeLimit	Limit for the maximum file size (MB) to upload	false	integer
maxLocalPackageDiskUsage	Maximum local disk usage (MB) for packages	false	integer
maxLocalPackageDiskUsageLimit	Limit for the maximum local disk usage (MB) for packages	false	integer

boolean

				from macro threats		
			researchOn	Share data with SentinelOne	false	boolean
			scanNewAgents	If True initiate full disk scan upon first registration	false	boolean
			signedDriverBlockingOn	Suspicious signed driver blocking on/off	false	boolean
			snapshotsOn	True if snapshots are enabled	false	boolean
			unsignedDriverBlockingOn	Suspicious unsigned driver blocking on/off	false	boolean
			updatedAt	Time of the last update to the policy	false	string
			userFullName	The user that created the policy	false	string
			userId	The user id	false	string

Account Policy

GET /web/api/v2.1/accounts/{account_id}/policy

Get the policy for the Account given by ID. To get the ID of an Account, run "accounts". See also: Get Policy.

Response Messages

200 - Success

401 - Unauthorized access - please sign in and retry.

404 - Policy not found

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
agentLoggingOn	True if logging is enabled in the agent	false	boolean
agentNotification	[DEPRECATED] Show end point notification on suspicious.Replaced by 'show_suspicious' in the agent UI section	false	boolean
agentUi	Agent ui	false	

Name	Description	Required	Value
agentUiOn	Agent ui on	false	boolean
contactCompany	Contact company	false	string
contactDirec	Contact	false	string

						tMessage	direct message			
						contactEmail	Contact email	false	string	
						contactFreeText	Contact free text	false	string	
						contactOther	Contact other	false	string	
						contactPhoneNumber	Contact phone number	false	string	
						contactSupportWebsite	Contact support website	false	string	
						devicePopUpNotifications	Device pop up notifications	false	boolean	
						maxEventAgeDays	Max event age days	false	integer	
						showAgentWarnings	Show agent warnings	false	boolean	
						showDeviceTab	Show device tab	false	boolean	
						showQuarantineTab	Show quarantine tab	false	boolean	
						showSupport	Show support	false	boolean	
						showSuspicious	Show suspicious	false	boolean	
						threatPopUpNotifications	Threat pop up notifications	false	boolean	
				agentUiOn	[DEPRECATED] Show/hide Agent UI. Moved inside the agent UI section	false	boolean			
				allowRemoteShell	True if Remote Shell	false	boolean			

				is enabled for the scope		
			antiTamperingOn	Anti tampering on/off	false	boolean
			autoDecommissionDays	Automatic decommission period in days	false	integer
			autoDecommissionOn	Auto decommission on	false	boolean
			autoFileUpload	Automatic file upload configuration	false	

Name	Description	Required	Value
enabled	Automatic file upload on/off	false	boolean
includeBenignFiles	Upload benign files	false	boolean
maxDailyFileUpload	Maximum size (MB) to upload daily	false	integer
maxDailyFileUploadLimit	Limit for the maximum size (MB) to upload daily	false	integer
maxFileSize	Maximum file size (MB) to upload	false	integer
maxFileSizeLimit	Limit for the maximum file size (MB) to upload	false	integer
maxLocalDiskUsage	Maximum local disk usage (MB) for uploaded files	false	integer
maxLocalDiskUsageLimit	Limit for the maximum local disk	false	integer

						usage (MB) for uploaded files			
			autoImmuneOn	Automatic immune on/off - this value must be true since all policies are immune by default	false	boolean			
			autoMitigationAction	Default action for auto mitigation	false	string			
			cloudValidationOn	Cloud validation on	false				
			createdAt	Timestamp of policy creation	false	string			
			driverBlocking	Suspicious driver blocking engine on/off	false	boolean			
			dvAttributesPerEventType	The DV attributes	false	Name	Description	Required	Value
						autoInstallBrowserExtensions	Auto install browser extensions	false	Name: autoInstallBrowserExtensions; Description: Auto install browser extensions; Required: false; Value: boolean
						behavioralIndicators	Behavioral indicators event	false	Name: dvEventTypeBehavioralIndicators; Description: Behavioral indicators event; Required: false; Value: boolean
						commandScripts	Command scripts event	false	Name: dvEventTypeCommandScripts; Description: Command scripts event; Required: false; Value: boolean

| | | |

										n	Event Type			
										dvEventTypeFileRename	File Rename Event Type	false	boolean	
										fullDiskScan	File Scan Event Type	false	boolean	
							ip	Network event - IP	false	Name	Description	Required	Value	
										dvEventTypeIpConnect	IP Connect Event Type	false	boolean	
										dvEventTypeIpListen	IP Listen Event Type	false	boolean	
							login	User login/ logout event	false	Name	Description	Required	Value	
										dvEventTypeLoginLoggedIn	User Login Event Type	false	boolean	
										dvEventTypeLoginLoggedOut	User Logout Event Type	false	boolean	
							namedPipe	Named Pipe	false	Name	Description	Required	Value	
										dvEventTypeNamedPipeConnection	Named Pipe Connection Event Type	false	boolean	
										dvEventTypeNamedPipeCreation	Named Pipe Creation Event Type	false	boolean	
							namedPipeExtended	Named Pipe Extended	false	Name	Description	Required	Value	
										namedPipeExtended	Named Pipe Connection Extended Event Type	false	boolean	
							process	Process event	false	Name	Description	Required	Value	
										dvEventTypeProcessCreation	Process Creation Event Type	false	boolean	
										dvEventTypeProcessExit	Process Exit Event Type	false	boolean	

| | | |

										dvEventTypeScheduledTaskRegister	Scheduled Task Register Event Type	false	boolean
										dvEventTypeScheduledTaskStart	Scheduled Task Start Event Type	false	boolean
										dvEventTypeScheduledTaskTrigger	Scheduled Task Trigeer Event Type	false	boolean
										dvEventTypeScheduledTaskUpdate	Scheduled Task Update Event Type	false	boolean
							smartFileMonitoring	Smart file monitoring	false	Name	Description	Required	Value
										smartFileMonitoring	Smart file monitoring	false	boolean
							url	URL Actions event	false	Name	Description	Required	Value
										dvEventTypeUrl	URL Actions event	false	boolean
							windowsEventLogs	Windows Event Log	false	Name	Description	Required	Value
										dvEventTypeWindowsEventLogCreation	Windows Event Log Creation Event Type	false	boolean
							windowsEventLogsExtended	Windows Event Log Extended	false	Name	Description	Required	Value
										windowsEventLogsExtended	Windows Event Log Extended Event Type	false	boolean
				engines	The engines statuses	false	Name	Description	Required	Value			
							applicationControl	application control	false	enum			
							dataFiles	data files	false	enum			
							executables	executables	false	enum			

						exploits	exploits	false	enum
						lateralMovement	lateral movement	false	enum
						penetration	penetration	false	enum
						preExecution	on-write	false	enum
						preExecutionSuspicious	pre execution suspicious	false	enum
						pup	potentially unwanted applications (PUP)	false	enum
						remoteShell	remote shell	false	enum
						reputation	reputation	false	enum
				forensicsAutoTriggering	Forensics auto triggering configuration	false			

Name	Description	Required	Value
linuxEnabled	True if linux forensics is enabled	false	boolean
linuxProfileId	The profile id for the linux forensics	false	string
linuxProfileName	The profile name for the linux forensics	false	string
macosEnabled	True if macos forensics is enabled	false	boolean
macosProfileId	The profile id for the macos forensics	false	string
macosProfileName	The profile name for the macos forensics	false	string
windowsEnabled	True if windows forensics is enabled	false	boolean

						windowsProfileId: The profile id for the windows forensics; false; string windowsProfileName: The profile name for the windows forensics; false; string
			fwForNetworkQuarantineEnabled	True if Firewall Control for Network Quarantine is enabled	false	boolean
			identityEndpointReporting	Endpoint reporting level	false	enum
			identityOn	Identity module on/off	false	boolean
			identityReportInterval	Identity telemetry report interval in minutes	false	integer
			identityThrottlingInterval	Identity duplicate command consolidation interval in minutes	false	integer
			identityUpdateInterval	Identity update interval in minutes	false	integer
			inheritedFrom	Indicates the parent scope from which this policy is inherited, or 'null' if it is not inherited	false	enum

			(modified specifically for the current scope).		
			ioc	True if ioc is enabled	false	boolean
			iocAttributes	The Ioc attributes	false

Name	Description	Required	Value
autoInstallBrowserExtensions	Update auto install browser extensions	false	boolean
behavioralIndicators	Update behavioral indicators	false	boolean
commandScripts	Update command scripts	false	boolean
crossProcess	Update cross process	false	boolean
dataMasking	Update data masking	false	boolean
dllModuleLoad	Update DLL module load	false	boolean
dns	Network event - DNS	false	boolean
driver	Driver	false	boolean
fds	Full disk scan	false	boolean
file	File event	false	boolean
ip	Network event - IP	false	boolean
login	User login/ logout event	false	boolean
namedPipe	Named Pipe	false	boolean
namedPipeExtended	Named Pipe Extended	false	boolean
process	Process	false	boolean

						creation event		
						registry	Registry event	false	boolean
						scheduledTask	Scheduled task event	false	boolean
						smartFileMonitoring	Smart file monitoring	false	boolean
						url	Ioc URI	false	boolean
						windowsEventLogs	Windows Event Log	false	boolean
						windowsEventLogsExtended	Windows Event Log Extended	false	boolean
			iocSupported	Ioc supported for the scope	false	boolean
			isDefault	True if this is the tenant policy	false	boolean
			isDvPolicyPerEventType	FE indication as to how to display DV policy	false	boolean
			mitigationMode	Mitigation modes	false	enum
			mitigationModeSuspicious	Mitigation mode	false	enum
			monitorOnExecute	Monitor on execute on/off	false	boolean
			monitorOnWrite	Monitor on write	false	boolean
			networkQuarantineOn	Network quarantine on	false	boolean
			remoteOpsForensics	Remote ops forensics configuration	false	Name / Description / Required / Value
						cpuLimit	CPU resources	false	integer

							limit for collection process		
						enabled	Enabled	false	boolean
						maximumDailyUpload	Maximum size to upload daily	false	integer
						maximumDailyUploadLimit	Limit for the maximum size to upload daily	false	integer
						maximumFileSizeUpload	Maximum size for single file	false	integer
						maximumFileSizeUploadLimit	Limit for the maximum file size to upload	false	integer
						parsedArtifactsDestination	Default destination of parsed artifacts	false	enum
				remoteScriptOrchestration	Remote script orchestration upload limits configuration	false	Name	Description	Required	Value
							alwaysUploadStreamToCloud	Always upload streams to cloud	false	boolean
							maxDailyFileDownload	Maximum size (MB) to download daily	false	integer
							maxDailyFileDownloadLimit	Limit for the maximum size (MB) to download daily	false	integer
							maxDailyFileUpload	Maximum size (MB) to upload daily	false	integer
							maxDailyFile	Limit for the	false	integer

						UploadLimit: maximum size (MB) to upload daily maxFileSize: Maximum size in bytes for single file; false; integer maxFileSizeLimit: Limit for the maximum file size (MB) to upload; false; integer maxLocalPackageDiskUsage: Maximum local disk usage (MB) for packages; false; integer maxLocalPackageDiskUsageLimit: Limit for the maximum local disk usage (MB) for packages; false; integer
			removeMacros	Determines if macros should be removed from macro threats	false	boolean
			researchOn	Share data with SentinelOne	false	boolean
			scanNewAgents	If True initiate full disk scan upon first registration	false	boolean
			signedDriverBlockingOn	Suspicious signed driver blocking on/off	false	boolean
			snapshotsOn	True if snapshots are enabled	false	boolean
			unsignedDriverBlockingOn	Suspicious unsigned	false	boolean

				driver blocking on/ off		
			updatedAt	Time of the last update to the policy	false	string
			userFullName	The user that created the policy	false	string
			userId	The user id	false	string
errors	Errors	false	array			

Update Account Policy

PUT /web/api/v2.1/accounts/{account_id}/policy

Change the policy for the Account given by ID. Best practice: Get the policy of the Account before you attempt to change it. See also: Get Policy.

BEST PRACTICE

Get the policy of the Account before you attempt to change it. See also: Get Policy.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

404 - Account not found

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
agentLoggingOn	True if logging is enabled in the agent	false	boolean
agentNotification	[DEPRECATED] Show end point notification on suspicious.Replaced by 'show_suspicious' in the agent UI section	false	boolean

			agentUi	Agent ui	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>agentUiOn</td><td>Agent ui on</td><td>false</td><td>boolean</td></tr><tr><td>contactCompany</td><td>Contact company</td><td>false</td><td>string</td></tr><tr><td>contactDirectMessage</td><td>Contact direct message</td><td>false</td><td>string</td></tr><tr><td>contactEmail</td><td>Contact email</td><td>false</td><td>string</td></tr><tr><td>contactFreeText</td><td>Contact free text</td><td>false</td><td>string</td></tr><tr><td>contactOther</td><td>Contact other</td><td>false</td><td>string</td></tr><tr><td>contactPhoneNumber</td><td>Contact phone number</td><td>false</td><td>string</td></tr><tr><td>contactSupportWebsite</td><td>Contact support website</td><td>false</td><td>string</td></tr><tr><td>devicePopUpNotifications</td><td>Device pop up notifications</td><td>false</td><td>boolean</td></tr><tr><td>maxEventAgeDays</td><td>Max event age days</td><td>false</td><td>integer</td></tr><tr><td>showAgentWarnings</td><td>Show agent warnings</td><td>false</td><td>boolean</td></tr><tr><td>showDeviceTab</td><td>Show device tab</td><td>false</td><td>boolean</td></tr><tr><td>showQuarantineTab</td><td>Show quarantine tab</td><td>false</td><td>boolean</td></tr><tr><td>showSupport</td><td>Show support</td><td>false</td><td>boolean</td></tr><tr><td>showSuspicious</td><td>Show suspicious</td><td>false</td><td>boolean</td></tr><tr><td>threatPopUpNotifications</td><td>Threat pop up notifications</td><td>false</td><td>boolean</td></tr></table>
			agentUiOn	[DEPRECATED] Show/hide	false	boolean

				Agent UI. Moved inside the agent UI section		
			allowRemoteShell	True if Remote Shell is enabled for the scope	false	boolean
			antiTamperingOn	Anti tampering on/off	false	boolean
			autoDecommissionDays	Automatic decommission period in days	false	integer
			autoDecommissionOn	Auto decommission on	false	boolean
			autoFileUpload	Automatic file upload configuration	false	

Name	Description	Required	Value
enabled	Automatic file upload on/off	false	boolean
includeBenignFiles	Upload benign files	false	boolean
maxDailyFileUpload	Maximum size (MB) to upload daily	false	integer
maxDailyFileUploadLimit	Limit for the maximum size (MB) to upload daily	false	integer
maxFileSize	Maximum file size (MB) to upload	false	integer
maxFileSizeLimit	Limit for the maximum file size (MB) to upload	false	integer
maxLocalDiskUsage	Maximum local disk	false	integer

							usage (MB) for uploaded files		
						maxLocalDiskUsageLimit	Limit for the maximum local disk usage (MB) for uploaded files	false	integer
			autoImmuneOn	Automatic immune on/off - this value must be true since all policies are immune by default	false	boolean			
			autoMitigationAction	Default action for auto mitigation	false	string			
			cloudValidationOn	Cloud validation on	false				
			createdAt	Timestamp of policy creation	false	string			
			driverBlocking	Suspicious driver blocking engine on/off	false	boolean			
			dvAttributesPerEventType	The DV attributes	false	Name	Description	Required	Value
						autoInstallBrowserExtensions	Auto install browser extensions	false	Name: autoInstallBrowserExtensions; Description: Auto install browser extensions; Required: false; Value: boolean
						behavioralIndicators	Behavioral indicators event	false	Name: dvEventTypeBehavioralIndica; Description: Behavioral indicators; Required: false; Value: boolean

								tors	event
						commandScripts	Command scripts event	false	

Name	Description	Required	Value
dvEventTypeCommandScripts	Command scripts event	false	boolean

crossProcess	Cross process event	false	

Name	Description	Required	Value
dvEventTypeCrossProcessDuplicateProcess	Duplicate Process Event Type	false	boolean
dvEventTypeCrossProcessDuplicateThread	Duplicate Thread Event Type	false	boolean
dvEventTypeCrossProcessOpenProcess	Open Process Event Type	false	boolean
dvEventTypeCrossProcessRemoteThread	Remote Thread Event Type	false	boolean

dataMasking	Data masking	false	

Name	Description	Required	Value
dataMasking	Data masking	false	boolean

dllModuleLoad	DLL module load event	false	

Name	Description	Required	Value
dvEventTypeDllModuleLoad	DLL module load event	false	boolean

dns	Network event - DNS	false	

Name	Description	Required	Value
dvEventTypeDns	Network event - DNS	false	boolean

driver	Driver	false	

Name	Description	Required	Value
dvEventTypeDriverLoad	Driver Load	false	boolean

file	File event	false	

Name	Description	Required	Value

									dvEventTypeFileCreation	File Creation Event Type	false	boolean
									dvEventTypeFileDeletion	File Deletion Event Type	false	boolean
									dvEventTypeFileModification	File Modification Event Type	false	boolean
									dvEventTypeFileRename	File Rename Event Type	false	boolean
									fullDiskScan	File Scan Event Type	false	boolean
							ip	Network event - IP	false	Name	Description	Required	Value
										dvEventTypeIpConnect	IP Connect Event Type	false	boolean
										dvEventTypeIpListen	IP Listen Event Type	false	boolean
							login	User login/ logout event	false	Name	Description	Required	Value
										dvEventTypeLoginLoggedIn	User Login Event Type	false	boolean
										dvEventTypeLoginLoggedOut	User Logout Event Type	false	boolean
							namedPipe	Named Pipe	false	Name	Description	Required	Value
										dvEventTypeNamedPipeConnection	Named Pipe Connection Event Type	false	boolean
										dvEventTypeNamedPipeCreation	Named Pipe Creation Event Type	false	boolean
							namedPipeExtended	Named Pipe Extended	false	Name	Description	Required	Value
										namedPipeExtended	Named Pipe Connection Extended Event Type	false	boolean
							process	Process event	false				

									Name	Description	Required	Value	
									dvEventTypeProcessCreation	Process Creation Event Type	false	boolean	
									dvEventTypeProcessExit	Process Exit Event Type	false	boolean	
									dvEventTypeProcessModification	Process Termination Event Type	false	boolean	
							registry	Registry event	false				
									Name	Description	Required	Value	
									dvEventTypeRegistryKeyCreated	Registry Key Created Event Type	false	boolean	
									dvEventTypeRegistryKeyDelete	Registry Key Delete Event Type	false	boolean	
									dvEventTypeRegistryKeyExport	Registry Key Export Event Type	false	boolean	
									dvEventTypeRegistryKeyImport	Registry Key Import Event Type	false	boolean	
									dvEventType RegistryKey Rename	Registry Key Rename Event Type	false	boolean	
									dvEventTypeRegistryKeySecurityChanged	Registry Key Security Changed Event Type	false	boolean	
									dvEventTypeRegistryValueCreated	Registry Value Crated Event Type	false	boolean	
									dvEventTypeRegistryValueDeleted	Registry Value Deleted Event Type	false	boolean	
									dvEventTypeRegistryValueM	Registry Value	false	boolean	

									odified	Modified Event Type		
						scheduledTask	Scheduled task event	false	Name	Description	Required	Value
									dvEventTypeScheduledTaskDelete	Scheduled Task Delete Event Type	false	boolean
									dvEventTypeScheduledTaskRegister	Scheduled Task Register Event Type	false	boolean
									dvEventTypeScheduledTaskStart	Scheduled Task Start Event Type	false	boolean
									dvEventTypeScheduledTaskTrigger	Scheduled Task Trigeer Event Type	false	boolean
									dvEventTypeScheduledTaskUpdate	Scheduled Task Update Event Type	false	boolean
						smartFileMonitoring	Smart file monitoring	false	Name	Description	Required	Value
									smartFileMonitoring	Smart file monitoring	false	boolean
						url	URL Actions event	false	Name	Description	Required	Value
									dvEventTypeUrl	URL Actions event	false	boolean
						windowsEventLogs	Windows Event Log	false	Name	Description	Required	Value
									dvEventTypeWindowsEventLogCreation	Windows Event Log Creation Event Type	false	boolean
						windowsEventLogsExtended	Windows Event Log Extended	false	Name	Description	Required	Value
									windowsEventLogsExtended	Windows Event Log Extended Event Type	false	boolean

			engines	The engines statuses	false

Name	Description	Required	Value
applicationControl	application control	false	enum
dataFiles	data files	false	enum
executables	executables	false	enum
exploits	exploits	false	enum
lateralMovement	lateral movement	false	enum
penetration	penetration	false	enum
preExecution	on-write	false	enum
preExecutionSuspicious	pre execution suspicious	false	enum
pup	potentially unwanted applications (PUP)	false	enum
remoteShell	remote shell	false	enum
reputation	reputation	false	enum

forensicsAutoTriggering	Forensics auto triggering configuration	false	

Name	Description	Required	Value
linuxEnabled	True if linux forensics is enabled	false	boolean
linuxProfileId	The profile id for the linux forensics	false	string
linuxProfileName	The profile name for the linux forensics	false	string
macosEnabled	True if macos forensics is enabled	false	boolean
macosProfileId	The profile id for the macos forensics	false	string
macosProfil	The profile	false	string

						eName: name for the macos forensics windowsEnabled: True if windows forensics is enabled, false, boolean windowsProfileId: The profile id for the windows forensics, false, string windowsProfileName: The profile name for the windows forensics, false, string
			fwForNetworkQuarantineEnabled	True if Firewall Control for Network Quarantine is enabled	false	boolean
			identityEndpointReporting	Endpoint reporting level	false	enum
			identityOn	Identity module on/off	false	boolean
			identityReportInterval	Identity telemetry report interval in minutes	false	integer
			identityThrottlingInterval	Identity duplicate command consolidation interval in minutes	false	integer
			identityUpdateInterval	Identity update interval in	false	integer

				minutes		
			inheritedFrom	Indicates the parent scope from which this policy is inherited, or 'null' if it is not inherited (modified specifically for the current scope).	false	enum
			ioc	True if ioc is enabled	false	boolean
			iocAttributes	The Ioc attributes	false	

Name	Description	Required	Value
autoInstallBrowserExtensions	Update auto install browser extensions	false	boolean
behavioralIndicators	Update behavioral indicators	false	boolean
commandScripts	Update command scripts	false	boolean
crossProcess	Update cross process	false	boolean
dataMasking	Update data masking	false	boolean
dllModuleLoad	Update DLL module load	false	boolean
dns	Network event - DNS	false	boolean
driver	Driver	false	boolean
fds	Full disk scan	false	boolean
file	File event	false	boolean
ip	Network event - IP	false	boolean

						login: User login/ logout event; false; boolean namedPipe: Named Pipe; false; boolean namedPipeExtended: Named Pipe Extended; false; boolean process: Process creation event; false; boolean registry: Registry event; false; boolean scheduledTask: Scheduled task event; false; boolean smartFileMonitoring: Smart file monitoring; false; boolean url: Ioc URI; false; boolean windowsEventLogs: Windows Event Log; false; boolean windowsEventLogsExtended: Windows Event Log Extended; false; boolean
			iocSupported	Ioc supported for the scope	false	boolean
			isDefault	True if this is the tenant policy	false	boolean
			isDvPolicyPerEventType	FE indication as to how to display DV policy	false	boolean
			mitigationMode	Mitigation modes	false	enum
			mitigationModeSuspicious	Mitigation mode	false	enum
			monitorOnExecute	Monitor on execute on/ off	false	boolean
			monitorOnWrite	Monitor on write	false	boolean

			networkQuarantineOn	Network quarantine on	false	boolean
			remoteOpsForensics	Remote ops forensics configuration	false	

Name	Description	Required	Value
cpuLimit	CPU resources limit for collection process	false	integer
enabled	Enabled	false	boolean
maximumDailyUpload	Maximum size to upload daily	false	integer
maximumDailyUploadLimit	Limit for the maximum size to upload daily	false	integer
maximumFileSizeUpload	Maximum size for single file	false	integer
maximumFileSizeUploadLimit	Limit for the maximum file size to upload	false	integer
parsedArtifactsDestination	Default destination of parsed artifacts	false	enum

remoteScriptOrchestration	Remote script orchestration upload limits configuration	false	

Name	Description	Required	Value
alwaysUploadStreamToCloud	Always upload streams to cloud	false	boolean
maxDailyFileDownload	Maximum size (MB) to download daily	false	integer
maxDailyFileDownloadLimit	Limit for the maximum size (MB) to download	false	integer

						daily
						maxDailyFileUpload: Maximum size (MB) to upload daily; false; integer
						maxDailyFileUploadLimit: Limit for the maximum size (MB) to upload daily; false; integer
						maxFileSize: Maximum size in bytes for single file; false; integer
						maxFileSizeLimit: Limit for the maximum file size (MB) to upload; false; integer
						maxLocalPackageDiskUsage: Maximum local disk usage (MB) for packages; false; integer
						maxLocalPackageDiskUsageLimit: Limit for the maximum local disk usage (MB) for packages; false; integer
			removeMacros	Determines if macros should be removed from macro threats	false	boolean
			researchOn	Share data with SentinelOne	false	boolean
			scanNewAgents	If True initiate full disk scan upon first registration	false	boolean
			signedDriverBlockingOn	Suspicious signed driver blocking on/off	false	boolean

			snapshotsOn: True if snapshots are enabled — false — boolean unsignedDriverBlockingOn: Suspicious unsigned driver blocking on/off — false — boolean updatedAt: Time of the last update to the policy — false — string userFullName: The user that created the policy — false — string userId: The user id — false — string
errors	Errors	false	array

Body Schema

Name	Description	Required	Value
data	Data	true	

Name	Description	Required	Value
agentLoggingOn	True if logging is enabled in the agent	false	boolean
agentNotification	[DEPRECATED] Show end point notification on suspicious.Replaced by 'show_suspicious' in the agent UI section	false	boolean
agentUi	Agent ui	false	

Name	Description	Required	Value
agentUiOn	Agent ui on	false	boolean
contactCompany	Contact company	false	string
contactDirectMessage	Contact direct message	false	string
contactEmail	Contact email	false	string
contactFreeText	Contact free text	false	string
contactOther	Contact other	false	string
contactPhoneNumber	Contact phone number	false	string
contactSupportWebsite	Contact support website	false	string
devicePopUpNotifications	Device pop up notifications	false	boolean

						maxEventAgeDays: Max event age days; false; integer showAgentWarnings: Show agent warnings; false; boolean showDeviceTab: Show device tab; false; boolean showQuarantineTab: Show quarantine tab; false; boolean showSupport: Show support; false; boolean showSuspicious: Show suspicious; false; boolean threatPopUpNotifications: Threat pop up notifications; false; boolean
			agentUiOn	[DEPRECATED] Show/hide Agent UI. Moved inside the agent UI section	false	boolean
			allowRemoteShell	True if Remote Shell is enabled for the scope	false	boolean
			antiTamperingOn	Anti tampering on/off	false	boolean
			autoDecommissionDays	Automatic decommission period in days	false	integer
			autoDecommissionOn	Auto decommission on	false	boolean
			autoFileUpload	Automatic file upload configuration	false	Name: enabled; Description: Automatic file upload on/off; Required: false; Value: boolean

						includeBenignFiles	Upload benign files	false	boolean
						maxDailyFileUpload	Maximum size (MB) to upload daily	false	integer
						maxDailyFileUploadLimit	Limit for the maximum size (MB) to upload daily	false	integer
						maxFileSize	Maximum file size (MB) to upload	false	integer
						maxFileSizeLimit	Limit for the maximum file size (MB) to upload	false	integer
						maxLocalDiskUsage	Maximum local disk usage (MB) for uploaded files	false	integer
						maxLocalDiskUsageLimit	Limit for the maximum local disk usage (MB) for uploaded files	false	integer
			autoImmuneOn	Automatic immune on/off - this value must be true since all policies are immune by default	false	boolean			
			autoMitigationAction	Default action for auto mitigation	false	string			
			cloudValidationOn	Cloud validation on	false				

			createdAt	Timestamp of policy creation	false	string
			driverBlocking	Suspicious driver blocking engine on/off	false	boolean
			dvAttributesPerEventType	The DV attributes	false	

Name	Description	Required	Value
autoInstallBrowserExtensions	Auto install browser extensions	false	

Name	Description	Required	Value
autoInstallBrowserExtensions	Auto install browser extensions	false	boolean

Name	Description	Required	Value
behavioralIndicators	Behavioral indicators event	false	

Name	Description	Required	Value
dvEventTypeBehavioralIndicators	Behavioral indicators event	false	boolean

Name	Description	Required	Value
commandScripts	Command scripts event	false	

Name	Description	Required	Value
dvEventTypeCommandScripts	Command scripts event	false	boolean

Name	Description	Required	Value
crossProcess	Cross process event	false	

Name	Description	Required	Value
dvEventTypeCrossProcessDuplicateProcess	Duplicate Process Event Type	false	boolean
dvEventTypeCrossProcessDuplicateThread	Duplicate Thread Event Type	false	boolean
dvEventTypeCrossProcessOpenProcess	Open Process Event Type	false	boolean
dvEventTypeCrossProcessRemoteThread	Remote Thread Event Type	false	boolean

Name	Description	Required	Value
dataMasking	Data masking	false	

Name	Description	Required	Value

| | | |

									LoginLogged Out	Event Type		
						namedPipe	Named Pipe	false	Name	Description	Required	Value
									dvEventType NamedPipeConnection	Named Pipe Connection Event Type	false	boolean
									dvEventType NamedPipeCreation	Named Pipe Creation Event Type	false	boolean
						namedPipeExtended	Named Pipe Extended	false	Name	Description	Required	Value
									namedPipeExtended	Named Pipe Connection Extended Event Type	false	boolean
						process	Process event	false	Name	Description	Required	Value
									dvEventTypeProcessCreation	Process Creation Event Type	false	boolean
									dvEventTypeProcessExit	Process Exit Event Type	false	boolean
									dvEventTypeProcessModification	Process Termination Event Type	false	boolean
						registry	Registry event	false	Name	Description	Required	Value
									dvEventTypeRegistryKeyCreated	Registry Key Created Event Type	false	boolean
									dvEventTypeRegistryKeyDelete	Registry Key Delete Event Type	false	boolean
									dvEventTypeRegistryKeyExport	Registry Key Export Event Type	false	boolean
									dvEventTypeRegistryKeyIm	Registry Key Import Event	false	boolean

| | | |

									toring	monitoring		
						url	URL Actions event	false	Name / Description / Required / Value dvEventTypeUrl / URL Actions event / false / boolean			
						windowsEventLogs	Windows Event Log	false	Name / Description / Required / Value dvEventTypeWindowsEventLogCreation / Windows Event Log Creation Event Type / false / boolean			
						windowsEventLogsExtended	Windows Event Log Extended	false	Name / Description / Required / Value windowsEventLogsExtended / Windows Event Log Extended Event Type / false / boolean			
				engines	The engines statuses	false	Name / Description / Required / Value applicationControl / application control / false / enum dataFiles / data files / false / enum executables / executables / false / enum exploits / exploits / false / enum lateralMovement / lateral movement / false / enum penetration / penetration / false / enum preExecution / on-write / false / enum preExecutionSuspicious / pre execution suspicious / false / enum pup / potentially unwanted applications (PUP) / false / enum remoteShell / remote shell / false / enum reputation / reputation / false / enum			

			forensicsAutoTriggering	Forensics auto triggering configuration	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>linuxEnabled</td><td>True if linux forensics is enabled</td><td>false</td><td>boolean</td></tr><tr><td>linuxProfileId</td><td>The profile id for the linux forensics</td><td>false</td><td>string</td></tr><tr><td>linuxProfileName</td><td>The profile name for the linux forensics</td><td>false</td><td>string</td></tr><tr><td>macosEnabled</td><td>True if macos forensics is enabled</td><td>false</td><td>boolean</td></tr><tr><td>macosProfileId</td><td>The profile id for the macos forensics</td><td>false</td><td>string</td></tr><tr><td>macosProfileName</td><td>The profile name for the macos forensics</td><td>false</td><td>string</td></tr><tr><td>windowsEnabled</td><td>True if windows forensics is enabled</td><td>false</td><td>boolean</td></tr><tr><td>windowsProfileId</td><td>The profile id for the windows forensics</td><td>false</td><td>string</td></tr><tr><td>windowsProfileName</td><td>The profile name for the windows forensics</td><td>false</td><td>string</td></tr></table>
			identityEndpointReporting	Endpoint reporting level	false	enum
			identityOn	Identity module on/off	false	boolean
			identityRepor	Identity	false	integer

			tInterval	telemetry report interval in minutes		
			identityThrottlingInterval	Identity duplicate command consolidation interval in minutes	false	integer
			identityUpdateInterval	Identity update interval in minutes	false	integer
			inheritedFrom	Indicates the parent scope from which this policy is inherited, or 'null' if it is not inherited (modified specifically for the current scope).	false	enum
			ioc	True if ioc is enabled	false	boolean
			iocAttributes	The Ioc attributes	false	

Name	Description	Required	Value
autoInstallBrowserExtensions	Update auto install browser extensions	false	boolean
behavioralIndicators	Update behavioral indicators	false	boolean
commandScripts	Update command scripts	false	boolean
crossProcess	Update cross process	false	boolean

						dataMasking	Update data masking	false	boolean
						dllModuleLoad	Update DLL module load	false	boolean
						dns	Network event - DNS	false	boolean
						driver	Driver	false	boolean
						fds	Full disk scan	false	boolean
						file	File event	false	boolean
						ip	Network event - IP	false	boolean
						login	User login/ logout event	false	boolean
						namedPipe	Named Pipe	false	boolean
						namedPipeExtended	Named Pipe Extended	false	boolean
						process	Process creation event	false	boolean
						registry	Registry event	false	boolean
						scheduledTask	Scheduled task event	false	boolean
						smartFileMonitoring	Smart file monitoring	false	boolean
						url	Ioc URI	false	boolean
						windowsEventLogs	Windows Event Log	false	boolean
						windowsEventLogsExtended	Windows Event Log Extended	false	boolean
				iocSupported	Ioc supported for the scope	false	boolean		
				isDefault	True if this is the tenant policy	false	boolean		

			isDvPolicyPerEventType	FE indication as to how to display DV policy	false	boolean
			mitigationMode	Mitigation modes	false	enum
			mitigationModeSuspicious	Mitigation mode	false	enum
			monitorOnExecute	Monitor on execute on/off	false	boolean
			monitorOnWrite	Monitor on write	false	boolean
			networkQuarantineOn	Network quarantine on	false	boolean
			remoteOpsForensics	Remote ops forensics configuration	false	

Name	Description	Required	Value
cpuLimit	CPU resources limit for collection process	false	integer
enabled	Enabled	false	boolean
maximumDailyUpload	Maximum size to upload daily	false	integer
maximumDailyUploadLimit	Limit for the maximum size to upload daily	false	integer
maximumFileSizeUpload	Maximum size for single file	false	integer
maximumFileSizeUploadLimit	Limit for the maximum file size to upload	false	integer
parsedArtifactsDestination	Default destination of parsed artifacts	false	enum

			remoteScriptOrchestration	Remote script orchestration upload limits configuration	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>alwaysUploadStreamToCloud</td><td>Always upload streams to cloud</td><td>false</td><td>boolean</td></tr><tr><td>maxDailyFileDownload</td><td>Maximum size (MB) to download daily</td><td>false</td><td>integer</td></tr><tr><td>maxDailyFileDownloadLimit</td><td>Limit for the maximum size (MB) to download daily</td><td>false</td><td>integer</td></tr><tr><td>maxDailyFileUpload</td><td>Maximum size (MB) to upload daily</td><td>false</td><td>integer</td></tr><tr><td>maxDailyFileUploadLimit</td><td>Limit for the maximum size (MB) to upload daily</td><td>false</td><td>integer</td></tr><tr><td>maxFileSize</td><td>Maximum size in bytes for single file</td><td>false</td><td>integer</td></tr><tr><td>maxFileSizeLimit</td><td>Limit for the maximum file size (MB) to upload</td><td>false</td><td>integer</td></tr><tr><td>maxLocalPackageDiskUsage</td><td>Maximum local disk usage (MB) for packages</td><td>false</td><td>integer</td></tr><tr><td>maxLocalPackageDiskUsageLimit</td><td>Limit for the maximum local disk usage (MB) for packages</td><td>false</td><td>integer</td></tr></table>
			removeMacros	Determines if macros should be removed	false	boolean

				from macro threats		
			researchOn	Share data with SentinelOne	false	boolean
			scanNewAgents	If True initiate full disk scan upon first registration	false	boolean
			signedDriverBlockingOn	Suspicious signed driver blocking on/off	false	boolean
			snapshotsOn	True if snapshots are enabled	false	boolean
			unsignedDriverBlockingOn	Suspicious unsigned driver blocking on/off	false	boolean
			updatedAt	Time of the last update to the policy	false	string
			userFullName	The user that created the policy	false	string
			userId	The user id	false	string

Global Policy

GET /web/api/v2.1/tenant/policy

Get the Global policy. This is the default policy for your deployment. See also: Get Policy.

Response Messages

200 - Success

401 - Unauthorized access - please sign in and retry.

404 - Policy not found

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
agentLoggingOn	True if logging is enabled in the agent	false	boolean
agentNotification	[DEPRECATED] Show end point notification on suspicious.Replaced by 'show_suspicious' in the agent UI section	false	boolean
agentUi	Agent ui	false	

Name	Description	Required	Value
agentUiOn	Agent ui on	false	boolean
contactCompany	Contact company	false	string
contactDirec	Contact	false	string

						tMessage	direct message			
						contactEmail	Contact email	false	string	
						contactFreeText	Contact free text	false	string	
						contactOther	Contact other	false	string	
						contactPhoneNumber	Contact phone number	false	string	
						contactSupportWebsite	Contact support website	false	string	
						devicePopUpNotifications	Device pop up notifications	false	boolean	
						maxEventAgeDays	Max event age days	false	integer	
						showAgentWarnings	Show agent warnings	false	boolean	
						showDeviceTab	Show device tab	false	boolean	
						showQuarantineTab	Show quarantine tab	false	boolean	
						showSupport	Show support	false	boolean	
						showSuspicious	Show suspicious	false	boolean	
						threatPopUpNotifications	Threat pop up notifications	false	boolean	
				agentUiOn	[DEPRECATED] Show/hide Agent UI. Moved inside the agent UI section	false	boolean			
				allowRemoteShell	True if Remote Shell	false	boolean			

				is enabled for the scope		
			antiTamperingOn	Anti tampering on/off	false	boolean
			autoDecommissionDays	Automatic decommission period in days	false	integer
			autoDecommissionOn	Auto decommission on	false	boolean
			autoFileUpload	Automatic file upload configuration	false	

Name	Description	Required	Value
enabled	Automatic file upload on/off	false	boolean
includeBenignFiles	Upload benign files	false	boolean
maxDailyFileUpload	Maximum size (MB) to upload daily	false	integer
maxDailyFileUploadLimit	Limit for the maximum size (MB) to upload daily	false	integer
maxFileSize	Maximum file size (MB) to upload	false	integer
maxFileSizeLimit	Limit for the maximum file size (MB) to upload	false	integer
maxLocalDiskUsage	Maximum local disk usage (MB) for uploaded files	false	integer
maxLocalDiskUsageLimit	Limit for the maximum local disk	false	integer

						usage (MB) for uploaded files
			autoImmuneOn	Automatic immune on/off - this value must be true since all policies are immune by default	false	boolean
			autoMitigationAction	Default action for auto mitigation	false	string
			cloudValidationOn	Cloud validation on	false	
			createdAt	Timestamp of policy creation	false	string
			driverBlocking	Suspicious driver blocking engine on/off	false	boolean
			dvAttributesPerEventType	The DV attributes	false	

Name	Description	Required	Value
autoInstallBrowserExtensions	Auto install browser extensions	false	
behavioralIndicators	Behavioral indicators event	false	
commandScripts	Command scripts event	false	

Name	Description	Required	Value
autoInstallBrowserExtensions	Auto install browser extensions	false	boolean

Name	Description	Required	Value
dvEventTypeBehavioralIndicators	Behavioral indicators event	false	boolean

Name	Description	Required	Value
dvEventTypeCommandScripts	Command scripts event	false	boolean

| | | |

| | | |

										dvEventTypeScheduledTaskRegister	Scheduled Task Register Event Type	false	boolean
										dvEventTypeScheduledTaskStart	Scheduled Task Start Event Type	false	boolean
										dvEventTypeScheduledTaskTrigger	Scheduled Task Trigeer Event Type	false	boolean
										dvEventTypeScheduledTaskUpdate	Scheduled Task Update Event Type	false	boolean
							smartFileMonitoring	Smart file monitoring	false	Name	Description	Required	Value
										smartFileMonitoring	Smart file monitoring	false	boolean
							url	URL Actions event	false	Name	Description	Required	Value
										dvEventTypeUrl	URL Actions event	false	boolean
							windowsEventLogs	Windows Event Log	false	Name	Description	Required	Value
										dvEventTypeWindowsEventLogCreation	Windows Event Log Creation Event Type	false	boolean
							windowsEventLogsExtended	Windows Event Log Extended	false	Name	Description	Required	Value
										windowsEventLogsExtended	Windows Event Log Extended Event Type	false	boolean
				engines	The engines statuses	false	Name	Description	Required	Value			
							applicationControl	application control	false	enum			
							dataFiles	data files	false	enum			
							executables	executables	false	enum			

						exploits	exploits	false	enum
						lateralMovement	lateral movement	false	enum
						penetration	penetration	false	enum
						preExecution	on-write	false	enum
						preExecutionSuspicious	pre execution suspicious	false	enum
						pup	potentially unwanted applications (PUP)	false	enum
						remoteShell	remote shell	false	enum
						reputation	reputation	false	enum
				forensicsAutoTriggering	Forensics auto triggering configuration	false			

Name	Description	Required	Value
linuxEnabled	True if linux forensics is enabled	false	boolean
linuxProfileId	The profile id for the linux forensics	false	string
linuxProfileName	The profile name for the linux forensics	false	string
macosEnabled	True if macos forensics is enabled	false	boolean
macosProfileId	The profile id for the macos forensics	false	string
macosProfileName	The profile name for the macos forensics	false	string
windowsEnabled	True if windows forensics is enabled	false	boolean

						windowsProfileId: The profile id for the windows forensics; false; string windowsProfileName: The profile name for the windows forensics; false; string
			fwForNetworkQuarantineEnabled	True if Firewall Control for Network Quarantine is enabled	false	boolean
			identityEndpointReporting	Endpoint reporting level	false	enum
			identityOn	Identity module on/off	false	boolean
			identityReportInterval	Identity telemetry report interval in minutes	false	integer
			identityThrottlingInterval	Identity duplicate command consolidation interval in minutes	false	integer
			identityUpdateInterval	Identity update interval in minutes	false	integer
			inheritedFrom	Indicates the parent scope from which this policy is inherited, or 'null' if it is not inherited	false	enum

			(modified specifically for the current scope).		
			ioc	True if ioc is enabled	false	boolean
			iocAttributes	The Ioc attributes	false

Name	Description	Required	Value
autoInstallBrowserExtensions	Update auto install browser extensions	false	boolean
behavioralIndicators	Update behavioral indicators	false	boolean
commandScripts	Update command scripts	false	boolean
crossProcess	Update cross process	false	boolean
dataMasking	Update data masking	false	boolean
dllModuleLoad	Update DLL module load	false	boolean
dns	Network event - DNS	false	boolean
driver	Driver	false	boolean
fds	Full disk scan	false	boolean
file	File event	false	boolean
ip	Network event - IP	false	boolean
login	User login/ logout event	false	boolean
namedPipe	Named Pipe	false	boolean
namedPipeExtended	Named Pipe Extended	false	boolean
process	Process	false	boolean

						creation event		
						registry	Registry event	false	boolean
						scheduledTask	Scheduled task event	false	boolean
						smartFileMonitoring	Smart file monitoring	false	boolean
						url	Ioc URI	false	boolean
						windowsEventLogs	Windows Event Log	false	boolean
						windowsEventLogsExtended	Windows Event Log Extended	false	boolean
			iocSupported	Ioc supported for the scope	false	boolean
			isDefault	True if this is the tenant policy	false	boolean
			isDvPolicyPerEventType	FE indication as to how to display DV policy	false	boolean
			mitigationMode	Mitigation modes	false	enum
			mitigationModeSuspicious	Mitigation mode	false	enum
			monitorOnExecute	Monitor on execute on/off	false	boolean
			monitorOnWrite	Monitor on write	false	boolean
			networkQuarantineOn	Network quarantine on	false	boolean
			remoteOpsForensics	Remote ops forensics configuration	false	Name | Description | Required | Value cpuLimit | CPU resources | false | integer

							limit for collection process		
						enabled	Enabled	false	boolean
						maximumDailyUpload	Maximum size to upload daily	false	integer
						maximumDailyUploadLimit	Limit for the maximum size to upload daily	false	integer
						maximumFileSizeUpload	Maximum size for single file	false	integer
						maximumFileSizeUploadLimit	Limit for the maximum file size to upload	false	integer
						parsedArtifactsDestination	Default destination of parsed artifacts	false	enum
				remoteScriptOrchestration	Remote script orchestration upload limits configuration	false			
						Name	Description	Required	Value
						alwaysUploadStreamToCloud	Always upload streams to cloud	false	boolean
						maxDailyFileDownload	Maximum size (MB) to download daily	false	integer
						maxDailyFileDownloadLimit	Limit for the maximum size (MB) to download daily	false	integer
						maxDailyFileUpload	Maximum size (MB) to upload daily	false	integer
						maxDailyFile	Limit for the	false	integer

						UploadLimit: maximum size (MB) to upload daily maxFileSize: Maximum size in bytes for single file; false; integer maxFileSizeLimit: Limit for the maximum file size (MB) to upload; false; integer maxLocalPackageDiskUsage: Maximum local disk usage (MB) for packages; false; integer maxLocalPackageDiskUsageLimit: Limit for the maximum local disk usage (MB) for packages; false; integer
			removeMacros	Determines if macros should be removed from macro threats	false	boolean
			researchOn	Share data with SentinelOne	false	boolean
			scanNewAgents	If True initiate full disk scan upon first registration	false	boolean
			signedDriverBlockingOn	Suspicious signed driver blocking on/off	false	boolean
			snapshotsOn	True if snapshots are enabled	false	boolean
			unsignedDriverBlockingOn	Suspicious unsigned	false	boolean

				driver blocking on/ off		
			updatedAt	Time of the last update to the policy	false	string
			userFullName	The user that created the policy	false	string
			userId	The user id	false	string
errors	Errors	false	array			

Update Global Policy

PUT /web/api/v2.1/tenant/policy

Change the policy of your deployment. Best practice: Get the Global policy before you attempt to change it. See also: Get Policy.
You must be a Global Admin user to change the Global Policy.

BEST PRACTICE

Get the Global policy before you attempt to change it. See also: Get Policy.
You must be a Global Admin user to change the Global Policy.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

404 - Policy not found

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
agentLoggingOn	True if logging is enabled in the agent	false	boolean
agentNotification	[DEPRECATED] Show end point notification on suspicious.Replaced by 'show_suspicious' in the	false	boolean

				agent UI section		
			agentUi	Agent ui	false	

Name	Description	Required	Value
agentUiOn	Agent ui on	false	boolean
contactCompany	Contact company	false	string
contactDirectMessage	Contact direct message	false	string
contactEmail	Contact email	false	string
contactFreeText	Contact free text	false	string
contactOther	Contact other	false	string
contactPhoneNumber	Contact phone number	false	string
contactSupportWebsite	Contact support website	false	string
devicePopUpNotifications	Device pop up notifications	false	boolean
maxEventAgeDays	Max event age days	false	integer
showAgentWarnings	Show agent warnings	false	boolean
showDeviceTab	Show device tab	false	boolean
showQuarantineTab	Show quarantine tab	false	boolean
showSupport	Show support	false	boolean
showSuspicious	Show suspicious	false	boolean
threatPopUpNotifications	Threat pop up notifications	false	boolean

			agentUiOn	[DEPRECATED] Show/hide Agent UI. Moved inside the agent UI section	false	boolean
			allowRemoteShell	True if Remote Shell is enabled for the scope	false	boolean
			antiTamperingOn	Anti tampering on/off	false	boolean
			autoDecommissionDays	Automatic decommission period in days	false	integer
			autoDecommissionOn	Auto decommission on	false	boolean
			autoFileUpload	Automatic file upload configuration	false	

Name	Description	Required	Value
enabled	Automatic file upload on/off	false	boolean
includeBenignFiles	Upload benign files	false	boolean
maxDailyFileUpload	Maximum size (MB) to upload daily	false	integer
maxDailyFileUploadLimit	Limit for the maximum size (MB) to upload daily	false	integer
maxFileSize	Maximum file size (MB) to upload	false	integer
maxFileSizeLimit	Limit for the maximum file size (MB) to upload	false	integer

						maxLocalDiskUsage: Maximum local disk usage (MB) for uploaded files; false; integer maxLocalDiskUsageLimit: Limit for the maximum local disk usage (MB) for uploaded files; false; integer
			autoImmuneOn	Automatic immune on/off - this value must be true since all policies are immune by default	false	boolean
			autoMitigationAction	Default action for auto mitigation	false	string
			cloudValidationOn	Cloud validation on	false	
			createdAt	Timestamp of policy creation	false	string
			driverBlocking	Suspicious driver blocking engine on/off	false	boolean
			dvAttributesPerEventType	The DV attributes	false	Name: autoInstallBrowserExtensions; Description: Auto install browser extensions; Required: false; Value: Name: autoInstallBrowserExtensions; Description: Auto install browser extensions; Required: false; Value: boolean behavioralIndicators; Behavioral indicators; false; Name; Description; Required; Value

| | | |

						file	File event	false

Name	Description	Required	Value
dvEventTypeFileCreation	File Creation Event Type	false	boolean
dvEventTypeFileDeletion	File Deletion Event Type	false	boolean
dvEventTypeFileModification	File Modification Event Type	false	boolean
dvEventTypeFileRename	File Rename Event Type	false	boolean
fullDiskScan	File Scan Event Type	false	boolean

ip	Network event - IP	false

Name	Description	Required	Value
dvEventTypeIpConnect	IP Connect Event Type	false	boolean
dvEventTypeIpListen	IP Listen Event Type	false	boolean

login	User login/ logout event	false

Name	Description	Required	Value
dvEventTypeLoginLoggedIn	User Login Event Type	false	boolean
dvEventTypeLoginLoggedOut	User Logout Event Type	false	boolean

namedPipe	Named Pipe	false

Name	Description	Required	Value
dvEventTypeNamedPipeConnection	Named Pipe Connection Event Type	false	boolean
dvEventTypeNamedPipeCreation	Named Pipe Creation Event Type	false	boolean

namedPipeExtended	Named Pipe Extended	false

Name	Description	Required	Value
namedPipeExtended	Named Pipe Connection Extended Event Type	false	boolean

| | | |

									odified	Modified Event Type		
						scheduledTask	Scheduled task event	false	Name	Description	Required	Value
									dvEventTypeScheduledTaskDelete	Scheduled Task Delete Event Type	false	boolean
									dvEventTypeScheduledTaskRegister	Scheduled Task Register Event Type	false	boolean
									dvEventTypeScheduledTaskStart	Scheduled Task Start Event Type	false	boolean
									dvEventTypeScheduledTaskTrigger	Scheduled Task Trigeer Event Type	false	boolean
									dvEventTypeScheduledTaskUpdate	Scheduled Task Update Event Type	false	boolean
						smartFileMonitoring	Smart file monitoring	false	Name	Description	Required	Value
									smartFileMonitoring	Smart file monitoring	false	boolean
						url	URL Actions event	false	Name	Description	Required	Value
									dvEventTypeUrl	URL Actions event	false	boolean
						windowsEventLogs	Windows Event Log	false	Name	Description	Required	Value
									dvEventTypeWindowsEventLogCreation	Windows Event Log Creation Event Type	false	boolean
						windowsEventLogsExtended	Windows Event Log Extended	false	Name	Description	Required	Value
									windowsEventLogsExtended	Windows Event Log Extended Event Type	false	boolean

			engines	The engines statuses	false

Name	Description	Required	Value
applicationControl	application control	false	enum
dataFiles	data files	false	enum
executables	executables	false	enum
exploits	exploits	false	enum
lateralMovement	lateral movement	false	enum
penetration	penetration	false	enum
preExecution	on-write	false	enum
preExecutionSuspicious	pre execution suspicious	false	enum
pup	potentially unwanted applications (PUP)	false	enum
remoteShell	remote shell	false	enum
reputation	reputation	false	enum

forensicsAutoTriggering	Forensics auto triggering configuration	false	

Name	Description	Required	Value
linuxEnabled	True if linux forensics is enabled	false	boolean
linuxProfileId	The profile id for the linux forensics	false	string
linuxProfileName	The profile name for the linux forensics	false	string
macosEnabled	True if macos forensics is enabled	false	boolean
macosProfileId	The profile id for the macos forensics	false	string
macosProfil	The profile	false	string

						eName: name for the macos forensics windowsEnabled: True if windows forensics is enabled, false, boolean windowsProfileId: The profile id for the windows forensics, false, string windowsProfileName: The profile name for the windows forensics, false, string
			fwForNetworkQuarantineEnabled	True if Firewall Control for Network Quarantine is enabled	false	boolean
			identityEndpointReporting	Endpoint reporting level	false	enum
			identityOn	Identity module on/off	false	boolean
			identityReportInterval	Identity telemetry report interval in minutes	false	integer
			identityThrottlingInterval	Identity duplicate command consolidation interval in minutes	false	integer
			identityUpdateInterval	Identity update interval in	false	integer

				minutes		
			inheritedFrom	Indicates the parent scope from which this policy is inherited, or 'null' if it is not inherited (modified specifically for the current scope).	false	enum
			ioc	True if ioc is enabled	false	boolean
			iocAttributes	The Ioc attributes	false	

Name	Description	Required	Value
autoInstallBrowserExtensions	Update auto install browser extensions	false	boolean
behavioralIndicators	Update behavioral indicators	false	boolean
commandScripts	Update command scripts	false	boolean
crossProcess	Update cross process	false	boolean
dataMasking	Update data masking	false	boolean
dllModuleLoad	Update DLL module load	false	boolean
dns	Network event - DNS	false	boolean
driver	Driver	false	boolean
fds	Full disk scan	false	boolean
file	File event	false	boolean
ip	Network event - IP	false	boolean

						login: User login/ logout event; false; boolean namedPipe: Named Pipe; false; boolean namedPipeExtended: Named Pipe Extended; false; boolean process: Process creation event; false; boolean registry: Registry event; false; boolean scheduledTask: Scheduled task event; false; boolean smartFileMonitoring: Smart file monitoring; false; boolean url: Ioc URI; false; boolean windowsEventLogs: Windows Event Log; false; boolean windowsEventLogsExtended: Windows Event Log Extended; false; boolean
			iocSupported	Ioc supported for the scope	false	boolean
			isDefault	True if this is the tenant policy	false	boolean
			isDvPolicyPerEventType	FE indication as to how to display DV policy	false	boolean
			mitigationMode	Mitigation modes	false	enum
			mitigationModeSuspicious	Mitigation mode	false	enum
			monitorOnExecute	Monitor on execute on/ off	false	boolean
			monitorOnWrite	Monitor on write	false	boolean

			networkQuarantineOn	Network quarantine on	false	boolean
			remoteOpsForensics	Remote ops forensics configuration	false	

Name	Description	Required	Value
cpuLimit	CPU resources limit for collection process	false	integer
enabled	Enabled	false	boolean
maximumDailyUpload	Maximum size to upload daily	false	integer
maximumDailyUploadLimit	Limit for the maximum size to upload daily	false	integer
maximumFileSizeUpload	Maximum size for single file	false	integer
maximumFileSizeUploadLimit	Limit for the maximum file size to upload	false	integer
parsedArtifactsDestination	Default destination of parsed artifacts	false	enum

remoteScriptOrchestration	Remote script orchestration upload limits configuration	false	

Name	Description	Required	Value
alwaysUploadStreamToCloud	Always upload streams to cloud	false	boolean
maxDailyFileDownload	Maximum size (MB) to download daily	false	integer
maxDailyFileDownloadLimit	Limit for the maximum size (MB) to download	false	integer

							daily		
						maxDailyFileUpload	Maximum size (MB) to upload daily	false	integer
						maxDailyFileUploadLimit	Limit for the maximum size (MB) to upload daily	false	integer
						maxFileSize	Maximum size in bytes for single file	false	integer
						maxFileSizeLimit	Limit for the maximum file size (MB) to upload	false	integer
						maxLocalPackageDiskUsage	Maximum local disk usage (MB) for packages	false	integer
						maxLocalPackageDiskUsageLimit	Limit for the maximum local disk usage (MB) for packages	false	integer
			removeMacros	Determines if macros should be removed from macro threats	false	boolean			
			researchOn	Share data with SentinelOne	false	boolean			
			scanNewAgents	If True initiate full disk scan upon first registration	false	boolean			
			signedDriverBlockingOn	Suspicious signed driver blocking on/off	false	boolean			

			snapshotsOn	True if snapshots are enabled	false	boolean
			unsignedDriverBlockingOn	Suspicious unsigned driver blocking on/off	false	boolean
			updatedAt	Time of the last update to the policy	false	string
			userFullName	The user that created the policy	false	string
			userId	The user id	false	string
errors	Errors	false	array			

Body Schema

Name	Description	Required	Value
data	Data	true	

Name	Description	Required	Value
agentLoggingOn	True if logging is enabled in the agent	false	boolean
agentNotification	[DEPRECATED] Show end point notification on suspicious.Replaced by 'show_suspicious' in the agent UI section	false	boolean
agentUi	Agent ui	false	

Name	Description	Required	Value
agentUiOn	Agent ui on	false	boolean
contactCompany	Contact company	false	string
contactDirectMessage	Contact direct message	false	string
contactEmail	Contact email	false	string
contactFreeText	Contact free text	false	string
contactOther	Contact other	false	string
contactPhoneNumber	Contact phone number	false	string
contactSupportWebsite	Contact support website	false	string
devicePopUpNotifications	Device pop up notifications	false	boolean

						maxEventAgeDays: Max event age days; false; integer showAgentWarnings: Show agent warnings; false; boolean showDeviceTab: Show device tab; false; boolean showQuarantineTab: Show quarantine tab; false; boolean showSupport: Show support; false; boolean showSuspicious: Show suspicious; false; boolean threatPopUpNotifications: Threat pop up notifications; false; boolean
			agentUiOn	[DEPRECATED] Show/hide Agent UI. Moved inside the agent UI section	false	boolean
			allowRemoteShell	True if Remote Shell is enabled for the scope	false	boolean
			antiTamperingOn	Anti tampering on/off	false	boolean
			autoDecommissionDays	Automatic decommission period in days	false	integer
			autoDecommissionOn	Auto decommission on	false	boolean
			autoFileUpload	Automatic file upload configuration	false	Name: enabled; Description: Automatic file upload on/off; Required: false; Value: boolean

						includeBenignFiles	Upload benign files	false	boolean
						maxDailyFileUpload	Maximum size (MB) to upload daily	false	integer
						maxDailyFileUploadLimit	Limit for the maximum size (MB) to upload daily	false	integer
						maxFileSize	Maximum file size (MB) to upload	false	integer
						maxFileSizeLimit	Limit for the maximum file size (MB) to upload	false	integer
						maxLocalDiskUsage	Maximum local disk usage (MB) for uploaded files	false	integer
						maxLocalDiskUsageLimit	Limit for the maximum local disk usage (MB) for uploaded files	false	integer
			autoImmuneOn	Automatic immune on/off - this value must be true since all policies are immune by default	false	boolean			
			autoMitigationAction	Default action for auto mitigation	false	string			
			cloudValidationOn	Cloud validation on	false				

			createdAt	Timestamp of policy creation	false	string
			driverBlocking	Suspicious driver blocking engine on/off	false	boolean
			dvAttributesPerEventType	The DV attributes	false	

Name	Description	Required	Value
autoInstallBrowserExtensions	Auto install browser extensions	false	

Name	Description	Required	Value
autoInstallBrowserExtensions	Auto install browser extensions	false	boolean

Name	Description	Required	Value
behavioralIndicators	Behavioral indicators event	false	

Name	Description	Required	Value
dvEventTypeBehavioralIndicators	Behavioral indicators event	false	boolean

Name	Description	Required	Value
commandScripts	Command scripts event	false	

Name	Description	Required	Value
dvEventTypeCommandScripts	Command scripts event	false	boolean

Name	Description	Required	Value
crossProcess	Cross process event	false	

Name	Description	Required	Value
dvEventTypeCrossProcessDuplicateProcess	Duplicate Process Event Type	false	boolean
dvEventTypeCrossProcessDuplicateThread	Duplicate Thread Event Type	false	boolean
dvEventTypeCrossProcessOpenProcess	Open Process Event Type	false	boolean
dvEventTypeCrossProcessRemoteThread	Remote Thread Event Type	false	boolean

Name	Description	Required	Value
dataMasking	Data masking	false	

Name	Description	Required	Value

| | | |

									LoginLogged Out	Event Type		
						namedPipe	Named Pipe	false	Name	Description	Required	Value
									dvEventType NamedPipeConnection	Named Pipe Connection Event Type	false	boolean
									dvEventType NamedPipeCreation	Named Pipe Creation Event Type	false	boolean
						namedPipeExtended	Named Pipe Extended	false	Name	Description	Required	Value
									namedPipeExtended	Named Pipe Connection Extended Event Type	false	boolean
						process	Process event	false	Name	Description	Required	Value
									dvEventTypeProcessCreation	Process Creation Event Type	false	boolean
									dvEventTypeProcessExit	Process Exit Event Type	false	boolean
									dvEventTypeProcessModification	Process Termination Event Type	false	boolean
						registry	Registry event	false	Name	Description	Required	Value
									dvEventTypeRegistryKeyCreated	Registry Key Created Event Type	false	boolean
									dvEventTypeRegistryKeyDelete	Registry Key Delete Event Type	false	boolean
									dvEventTypeRegistryKeyExport	Registry Key Export Event Type	false	boolean
									dvEventTypeRegistryKeyIm	Registry Key Import Event	false	boolean

										port	Type							
										dvEventTypeRegistryKeyRename	Registry Key Rename Event Type	false	boolean					
										dvEventTypeRegistryKeySecurityChanged	Registry Key Security Changed Event Type	false	boolean					
										dvEventTypeRegistryValueCreated	Registry Value Crated Event Type	false	boolean					
										dvEventTypeRegistryValueDeleted	Registry Value Deleted Event Type	false	boolean					
										dvEventTypeRegistryValueModified	Registry Value Modified Event Type	false	boolean					
								scheduledTask	Scheduled task event	false	Name	Description	Required	Value				
											dvEventTypeScheduledTaskDelete	Scheduled Task Delete Event Type	false	boolean				
											dvEventTypeScheduledTaskRegister	Scheduled Task Register Event Type	false	boolean				
											dvEventTypeScheduledTaskStart	Scheduled Task Start Event Type	false	boolean				
											dvEventTypeScheduledTaskTrigger	Scheduled Task Trigeer Event Type	false	boolean				
											dvEventTypeScheduledTaskUpdate	Scheduled Task Update Event Type	false	boolean				
								smartFileMonitoring	Smart file monitoring	false	Name	Description	Required	Value				
											smartFileMoni	Smart file	false	boolean				

									toring	monitoring		
						url	URL Actions event	false	Name: dvEventTypeUrl Description: URL Actions event Required: false Value: boolean			
						windowsEventLogs	Windows Event Log	false	Name: dvEventTypeWindowsEventLogCreation Description: Windows Event Log Creation Event Type Required: false Value: boolean			
						windowsEventLogsExtended	Windows Event Log Extended	false	Name: windowsEventLogsExtended Description: Windows Event Log Extended Event Type Required: false Value: boolean			
				engines	The engines statuses	false	Name: applicationControl Description: application control Required: false Value: enum Name: dataFiles Description: data files Required: false Value: enum Name: executables Description: executables Required: false Value: enum Name: exploits Description: exploits Required: false Value: enum Name: lateralMovement Description: lateral movement Required: false Value: enum Name: penetration Description: penetration Required: false Value: enum Name: preExecution Description: on-write Required: false Value: enum Name: preExecutionSuspicious Description: pre execution suspicious Required: false Value: enum Name: pup Description: potentially unwanted applications (PUP) Required: false Value: enum Name: remoteShell Description: remote shell Required: false Value: enum Name: reputation Description: reputation Required: false Value: enum			

			forensicsAutoTriggering	Forensics auto triggering configuration	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>linuxEnabled</td><td>True if linux forensics is enabled</td><td>false</td><td>boolean</td></tr><tr><td>linuxProfileId</td><td>The profile id for the linux forensics</td><td>false</td><td>string</td></tr><tr><td>linuxProfileName</td><td>The profile name for the linux forensics</td><td>false</td><td>string</td></tr><tr><td>macosEnabled</td><td>True if macos forensics is enabled</td><td>false</td><td>boolean</td></tr><tr><td>macosProfileId</td><td>The profile id for the macos forensics</td><td>false</td><td>string</td></tr><tr><td>macosProfileName</td><td>The profile name for the macos forensics</td><td>false</td><td>string</td></tr><tr><td>windowsEnabled</td><td>True if windows forensics is enabled</td><td>false</td><td>boolean</td></tr><tr><td>windowsProfileId</td><td>The profile id for the windows forensics</td><td>false</td><td>string</td></tr><tr><td>windowsProfileName</td><td>The profile name for the windows forensics</td><td>false</td><td>string</td></tr></table>
			identityEndpointReporting	Endpoint reporting level	false	enum
			identityOn	Identity module on/off	false	boolean
			identityRepor	Identity	false	integer

			tInterval	telemetry report interval in minutes		
			identityThrottlingInterval	Identity duplicate command consolidation interval in minutes	false	integer
			identityUpdateInterval	Identity update interval in minutes	false	integer
			inheritedFrom	Indicates the parent scope from which this policy is inherited, or 'null' if it is not inherited (modified specifically for the current scope).	false	enum
			ioc	True if ioc is enabled	false	boolean
			iocAttributes	The Ioc attributes	false	

Name	Description	Required	Value
autoInstallBrowserExtensions	Update auto install browser extensions	false	boolean
behavioralIndicators	Update behavioral indicators	false	boolean
commandScripts	Update command scripts	false	boolean
crossProcess	Update cross process	false	boolean

						dataMasking	Update data masking	false	boolean
						dllModuleLoad	Update DLL module load	false	boolean
						dns	Network event - DNS	false	boolean
						driver	Driver	false	boolean
						fds	Full disk scan	false	boolean
						file	File event	false	boolean
						ip	Network event - IP	false	boolean
						login	User login/ logout event	false	boolean
						namedPipe	Named Pipe	false	boolean
						namedPipeExtended	Named Pipe Extended	false	boolean
						process	Process creation event	false	boolean
						registry	Registry event	false	boolean
						scheduledTask	Scheduled task event	false	boolean
						smartFileMonitoring	Smart file monitoring	false	boolean
						url	Ioc URI	false	boolean
						windowsEventLogs	Windows Event Log	false	boolean
						windowsEventLogsExtended	Windows Event Log Extended	false	boolean
				iocSupported	Ioc supported for the scope	false	boolean		
				isDefault	True if this is the tenant policy	false	boolean		

			isDvPolicyPerEventType	FE indication as to how to display DV policy	false	boolean
			mitigationMode	Mitigation modes	false	enum
			mitigationModeSuspicious	Mitigation mode	false	enum
			monitorOnExecute	Monitor on execute on/off	false	boolean
			monitorOnWrite	Monitor on write	false	boolean
			networkQuarantineOn	Network quarantine on	false	boolean
			remoteOpsForensics	Remote ops forensics configuration	false	

Name	Description	Required	Value
cpuLimit	CPU resources limit for collection process	false	integer
enabled	Enabled	false	boolean
maximumDailyUpload	Maximum size to upload daily	false	integer
maximumDailyUploadLimit	Limit for the maximum size to upload daily	false	integer
maximumFileSizeUpload	Maximum size for single file	false	integer
maximumFileSizeUploadLimit	Limit for the maximum file size to upload	false	integer
parsedArtifactsDestination	Default destination of parsed artifacts	false	enum

			remoteScriptOrchestration	Remote script orchestration upload limits configuration	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>alwaysUploadStreamToCloud</td><td>Always upload streams to cloud</td><td>false</td><td>boolean</td></tr><tr><td>maxDailyFileDownload</td><td>Maximum size (MB) to download daily</td><td>false</td><td>integer</td></tr><tr><td>maxDailyFileDownloadLimit</td><td>Limit for the maximum size (MB) to download daily</td><td>false</td><td>integer</td></tr><tr><td>maxDailyFileUpload</td><td>Maximum size (MB) to upload daily</td><td>false</td><td>integer</td></tr><tr><td>maxDailyFileUploadLimit</td><td>Limit for the maximum size (MB) to upload daily</td><td>false</td><td>integer</td></tr><tr><td>maxFileSize</td><td>Maximum size in bytes for single file</td><td>false</td><td>integer</td></tr><tr><td>maxFileSizeLimit</td><td>Limit for the maximum file size (MB) to upload</td><td>false</td><td>integer</td></tr><tr><td>maxLocalPackageDiskUsage</td><td>Maximum local disk usage (MB) for packages</td><td>false</td><td>integer</td></tr><tr><td>maxLocalPackageDiskUsageLimit</td><td>Limit for the maximum local disk usage (MB) for packages</td><td>false</td><td>integer</td></tr></table>
			removeMacros	Determines if macros should be removed	false	boolean

				from macro threats		
			researchOn	Share data with SentinelOne	false	boolean
			scanNewAgents	If True initiate full disk scan upon first registration	false	boolean
			signedDriverBlockingOn	Suspicious signed driver blocking on/off	false	boolean
			snapshotsOn	True if snapshots are enabled	false	boolean
			unsignedDriverBlockingOn	Suspicious unsigned driver blocking on/off	false	boolean
			updatedAt	Time of the last update to the policy	false	string
			userFullName	The user that created the policy	false	string
			userId	The user id	false	string

Ranger

Get Ranger Table

GET /web/api/v2.1/ranger/table-view

Get the data for each row in the Ranger Device Inventory Table. Best practice: Set filters. Each row is a set of parameters that quickly fills the pagination limits.

BEST PRACTICE

Set filters. Each row is a set of parameters that quickly fills the pagination limits.

Parameters

accountids	optional	Single Account ID to filter by. Example: "225494730938493804".
agentids	optional	List of agent ids. Example: "225494730938493804,225494730938493915".
countonly	optional	If true, only total number of items will be returned, without any of the actual objects.
cursor	optional	Cursor position returned by the last request. Use to iterate over more than 1000 items. Example: "YWdlbnRfaWQ6NTgwMjkzODE=".
devicefunction__contains	optional	Free-text filter by device function (supports multiple values). Example: "security,mobile".
devicereviews	optional	The device review state
devicetype	optional	Device type. Example: "Server/Workstation/...".
devicetypes	optional	Device types
discoverymethods	optional	Discovery methods
domains	optional	Included network domains. Example: "mybusiness,workgroup".
externalip	optional	Search using external IP
externalip__contains	optional	Free-text filter by visible IP (supports multiple values). Example: "192.168.0.1/24,10.1".
firstseen__between	optional	Date range refor first seen(format: <from_timestamp>-

		<to_timestamp>, inclusive). Example: "1514978890136-1514978650130".
firstseen__gt	optional	Devices first seen after this timestamp. Example: "2018-02-27T04:49:26.257525Z".
firstseen__gte	optional	Devices first seen after or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
firstseen__lt	optional	Devices first seen before this timestamp. Example: "2018-02-27T04:49:26.257525Z".
firstseen__lte	optional	Devices first seen before or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
gatewaymacaddress	optional	A gateway mac address to search for
gatewaymacaddress__contains	optional	Free-text filter by gateway mac address (supports multiple values). Example: "aa:ee:b1".
hostnames	optional	Hostnames
hostnames__contains	optional	Free-text filter by hostname (supports multiple values). Example: "s1_host,SomeHost".
ids	optional	List of device ids. Example: "225494730938493804,225494730938493915".
knownfingerprintingdata	optional	Known fingerprinting data. Example: "Manufacturer".
lastseen__between	optional	Date range for last seen(format: <from_timestamp>-<to_timestamp>, inclusive). Example: "1514978890136-1514978650130".
lastseen__gt	optional	Devices last seen after this timestamp. Example: "2018-02-27T04:49:26.257525Z".
lastseen__gte	optional	Devices last seen after or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
lastseen__lt	optional	Devices last seen before this timestamp. Example: "2018-02-27T04:49:26.257525Z".
lastseen__lte	optional	Devices last seen before or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
limit	optional	Limit number of returned items (1-1000). Example: "10".
localip	optional	Search using local IP
localip__contains	optional	Free-text filter by IP Address (supports multiple values). Example:

		"192.168.0.1/24,10.1".
macaddress	optional	A mac address to search for
macaddress__contains	optional	Free-text filter by mac address (supports multiple values). Example: "aa:ee:b1".
managedstate	optional	Is the device managed
managedstates	optional	Is the device managed
manufacturer	optional	Manufacturer of the device or network interface
manufacturer__contains	optional	Free-text filter by manufacturer (supports multiple values). Example: "Company".
networkname	optional	Search using network name
networkname__contains	optional	Free-text filter by network name (supports multiple values). Example: "Office".
osname	optional	Os name
ostype	optional	OS type
ostypes	optional	Included OS types
osversion	optional	Os version
osversion__contains	optional	Free-text filter by OS full name and version (supports multiple values). Example: "Service Pack 1".
period	optional	Period. Example: "latest".
query	optional	Query
siteids	optional	Single Site ID to filter by. Example: "225494730938493804".
sitenames	optional	Included site names. Example: "Office,Test".
skip	optional	Skip first number of items (0-1000). To iterate over more than 1000 items, use "cursor". Example: "150".
skipcount	optional	If true, total number of items will not be calculated, which speeds up execution time.
sortby	optional	The column to sort the results by. Example: "id".
sortorder	optional	Sort direction. Example: "asc".
subnetaddress__contains	optional	Free-text filter by Subnet Address (supports multiple values). Example: "192.168.0.1/24,10.1".
tagname__contains	optional	Free-text filter by tag name (supports multiple values). Example: "iot".

tcpports__contains	optional	Free-text filter by tcp port (supports multiple values). Example: "80,24".
udpports__contains	optional	Free-text filter by udp port (supports multiple values). Example: "137,2002".

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - Insufficient permissions

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>pagination</td><td>Pagination information</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>totalItems</td><td>Total number of items found matching your query</td><td>true</td><td>integer</td></tr>
<tr><td>nextCursor</td><td>Pass this value as "cursor" on your next request, to get the next page of results (Will be "null" when last page reached)</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>agentId</td><td>The agent id if this is a known</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
</table>

				managed device		
			deviceFunction	Function of the device	false	string
			deviceReview	The device review state	false	string
			deviceReviewLog	Log of actions for this device	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>current</td><td></td><td>false</td><td>string</td></tr><tr><td>previous</td><td></td><td>false</td><td>string</td></tr><tr><td>reason</td><td></td><td>false</td><td>string</td></tr><tr><td>reasonDetails</td><td></td><td>false</td><td>string</td></tr><tr><td>updatedAt</td><td></td><td>false</td><td>string</td></tr><tr><td>username</td><td></td><td>false</td><td>string</td></tr></table>
			deviceType	Role of the device	false	string
			discoveryMethods	Methods used to discover the device	false	string []
			domain	The domain of the device	false	string
			externalIp	Main Gateway Visible IP	false	string
			fingerPrintScore	The confidence for this fingerprinting result	false	integer
			firstSeen	Time the device was first seen	false	string
			gatewayIpAddress	Main gateway IP address	false	string
			gatewayMacAddress	Main gateway	false	string

				MAC address		
			hasIdentity	Would we be able to identify this device over time	false	boolean
			hasUserLabel	True if it has a user label	false	boolean
			hostnames	Array of host names	false	string []
			id	Id of the device	false	string
			ipAddresses	A list of ip addresses. When it is not combined it is always one element	false	string []
			labelUpdatedAt	The date of the last label update	false	string
			labelUserName	The user that changed the label	false	string
			lastSeen	Time the device was last seen	false	string
			localIp	Local ip of the device	false	string
			macAddress	Mac address of the device	false	string
			managedState	Protection state of the device	false	string
			manufacturer	Manufacturer of the device or network interface	false	string
			networkName	The network name	false	string

			networks	A list of all the networks associated to the device. When it is not combined it is always one element	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>externalIp</td><td>Main Gateway Visible IP</td><td>false</td><td>string</td></tr><tr><td>gatewayIpAddress</td><td>Main gateway IP address</td><td>false</td><td>string</td></tr><tr><td>gatewayMacAddress</td><td>Main gateway MAC address</td><td>false</td><td>string</td></tr><tr><td>ip</td><td>The IP of the device in the network</td><td>false</td><td>string</td></tr><tr><td>networkName</td><td>The network name</td><td>false</td><td>string</td></tr><tr><td>subnetAddress</td><td>Main subnet address</td><td>false</td><td>string</td></tr></table>
			osName	OS Name/ Version of the device	false	string
			osType	Os Type of the device	false	string
			osVersion	OS Version of the device	false	string
			previousDeviceFunction	Previous Function of the device if manually changed	false	string
			previousOsType	Previous Os Type of the device if manually changed	false	string
			previousOsVersion	Previous OS Version of the device if manually changed	false	string

<table>
<tr><td></td><td></td><td></td><td>
<table>
<tr><td>siteName</td><td>Site name</td><td>false</td><td>string</td></tr>
<tr><td>subnetAddress</td><td>Main subnet address</td><td>false</td><td>string</td></tr>
<tr><td>tags</td><td>The tags</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>id</td><td>The tag id</td><td>true</td><td>string</td></tr>
<tr><td>description</td><td>The tag description</td><td>false</td><td>string</td></tr>
<tr><td>kind</td><td>Kind of tag if relevant</td><td>false</td><td>string</td></tr>
<tr><td>name</td><td>The tag name</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>tcpPorts</td><td>TCP Ports</td><td>false</td><td>integer []</td></tr>
<tr><td>udpPorts</td><td>UDP Ports</td><td>false</td><td>integer []</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Export Ranger Data

GET /web/api/v2.1/ranger/report/csv

Export Ranger data to csv. You can set filters to get only relevant data. The response sends the csv data as text.

Parameters

accountids	optional	Single Account ID to filter by. Example: "225494730938493804".
agentids	optional	List of agent ids. Example: "225494730938493804,225494730938493915".
devicefunction__contains	optional	Free-text filter by device function (supports multiple values). Example: "security,mobile".
devicereviews	optional	The device review state
devicetype	optional	Device type. Example: "Server/Workstation/...".
devicetypes	optional	Device types
discoverymethods	optional	Discovery methods
domains	optional	Included network domains. Example: "mybusiness,workgroup".
externalip	optional	Search using external IP
externalip__contains	optional	Free-text filter by visible IP (supports multiple values). Example: "192.168.0.1/24,10.1".
firstseen__between	optional	Date range refor first seen(format: <from_timestamp>-<to_timestamp>, inclusive). Example: "1514978890136-1514978650130".
firstseen__gt	optional	Devices first seen after this timestamp. Example: "2018-02-27T04:49:26.257525Z".
firstseen__gte	optional	Devices first seen after or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
firstseen__lt	optional	Devices first seen before this timestamp. Example: "2018-02-27T04:49:26.257525Z".
firstseen__lte	optional	Devices first seen before or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
gatewaymacaddress	optional	A gateway mac address to search for
gatewaymacaddress__c	optional	Free-text filter by gateway mac address (supports multiple values).

ontains		Example: "aa:ee:b1".
hostnames	optional	Hostnames
hostnames__contains	optional	Free-text filter by hostname (supports multiple values). Example: "s1_host,SomeHost".
ids	optional	List of device ids. Example: "225494730938493804,225494730938493915".
knownfingerprintingdata	optional	Known fingerprinting data. Example: "Manufacturer".
lastseen__between	optional	Date range for last seen(format: <from_timestamp>-<to_timestamp>, inclusive). Example: "1514978890136-1514978650130".
lastseen__gt	optional	Devices last seen after this timestamp. Example: "2018-02-27T04:49:26.257525Z".
lastseen__gte	optional	Devices last seen after or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
lastseen__lt	optional	Devices last seen before this timestamp. Example: "2018-02-27T04:49:26.257525Z".
lastseen__lte	optional	Devices last seen before or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
localip	optional	Search using local IP
localip__contains	optional	Free-text filter by IP Address (supports multiple values). Example: "192.168.0.1/24,10.1".
macaddress	optional	A mac address to search for
macaddress__contains	optional	Free-text filter by mac address (supports multiple values). Example: "aa:ee:b1".
managedstate	optional	Is the device managed
managedstates	optional	Is the device managed
manufacturer	optional	Manufacturer of the device or network interface
manufacturer__contains	optional	Free-text filter by manufacturer (supports multiple values). Example: "Company".
networkname	optional	Search using network name
networkname__contains	optional	Free-text filter by network name (supports multiple values). Example: "Office".

osname	optional	Os name
ostype	optional	OS type
ostypes	optional	Included OS types
osversion	optional	Os version
osversion__contains	optional	Free-text filter by OS full name and version (supports multiple values). Example: "Service Pack 1".
period	optional	Period. Example: "latest".
query	optional	Query
siteids	optional	Single Site ID to filter by. Example: "225494730938493804".
sitenames	optional	Included site names. Example: "Office,Test".
subnetaddress__contains	optional	Free-text filter by Subnet Address (supports multiple values). Example: "192.168.0.1/24,10.1".
tagname__contains	optional	Free-text filter by tag name (supports multiple values). Example: "iot".
tcpports__contains	optional	Free-text filter by tcp port (supports multiple values). Example: "80,24".
udpports__contains	optional	Free-text filter by udp port (supports multiple values). Example: "137,2002".

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

JSON Raw Data

GET /web/api/v2.1/ranger/{inventory_id}/json

Get a json string with the Ranger data for one device, by ID in the Device Inventory Data.

Response Messages

200 - Success

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
data	Response data	false	
errors	Errors	false	array

Export JSON Raw Data

GET /web/api/v2.1/ranger/{inventory_id}/json/export

Export the raw data for one device, by its ID in the Device Inventory Data. To get the ID, run ranger/table-view (see Get Ranger Table). Use this command to get data for Support.

Response Messages

200 - Success

401 - Unauthorized access - please sign in and retry.

404 - Not found

Get Ranger Settings

GET /web/api/v2.1/ranger/settings

Ranger gives full visibility of all devices connected to your network. Ranger scans your corporate environment to identify and manage connected devices, even those not protected by or supported by SentinelOne. Ranger identifies devices as:
* Secured - End-user computer or laptop, or server, with a SentinelOne Agent.
* Unsecured - Endpoint of supported hardware and OS, without an Agent.
* Unsupported - Hardware or software that are not compatible with the SentinelOne Agent.
* Unknown - Ranger cannot determine if the device is Unsecured or Unsupported.
When you install Windows Agents with Ranger, the Agents can become scanners. Selected scanners from networks that you enable for scanning find connected devices with passive and active scan techniques. The scanners send the collected data to Ranger on the Management. Ranger then runs fingerprinting to identify and classify unique devices and to update the Device Inventory Table in the Management Console. With port scanning, it is important that you understand the legal and ethical considerations and that you document a Ranger plan and implementation. See https://support.sentinelone.com/hc/en-us/articles/360041484913 > Legal Considerations and Proper Implementation.
Requirements: Ranger license, Cloud-based Management (not supported for On-Prem), Global user or Account user with scope access to the Account with a Ranger license.
Use this command to get the Ranger Settings for the Account of the given ID (run "accounts" to get an Account ID). The Response shows if Ranger is enabled on the Account, the protocols and ports of the scans, and more:
* minAgentsInNetworkToScan - To help you determine which networks are corporate, Ranger looks at the number of secured endpoints (Agents) in a network. If there are not enough Agents in a network - set by this parameter value - Ranger considers the network to be non-corporate and will not scan it.
* scanOnlyLocalSubnets - If false, Ranger scans remote subnets that do not have online Ranger scanners. This will create network traffic through the corporate firewall (and between different corporate locations), which can impact network performance.
* usePeriodicSnapshots - A complete scan includes scanner port scanning and Ranger AI analysis of the scanner data to update the Device Inventory Snapshot. If this setting is true, Ranger runs a new scan on an interval. If snapshotPeriod is shorter, the data is more accurate. If longer, there is better performance.

Parameters

accountids	optional	List of Account IDs to filter by. Example: "225494730938493804,225494730938493915".
siteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - Insufficient permissions

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
accountId	Account id	false	string
autoEnableNetworks	All networks that match the min agents configuration will be enabled automatically	false	boolean
combineDevices	Combine devices as one among multiple networks	false	boolean
enabled	Is the ranger collection enabled for the account	false	boolean
icmpScan	ICMP scan enabled	false	boolean
mdnsScan	MDNS scan	false	boolean

				enabled		
			minAgentsInNetworkToScan	Minimum agents required in a network to be listed as selectable for scan	false	integer
			multiScanSsdp	SSDP Multicast scan enabled	false	boolean
			networkDecommissionValue	The number of days to archive a network which was not enabled for scan	false	integer
			newNetworkInHours	Networks are going to be marked as new for this period	false	integer
			rdnsScan	RDNS scan enabled	false	boolean
			restrictions	A set of IP addresses that should not be scanned in the specific network	false	Name / Description / Required / Value annotation / An optional note with the reason for the restriction / false / string type / / false / enum values / It will be one IP or one CIDR or two values for a Range / false / string []
			scanOnlyLocalSubnets	Scan only local subnets	false	boolean
			scopeId	Scope id	false	string

<table>
<tr><td></td><td></td><td></td><td>
<table>
<tr><td>smbScan</td><td>SMB scan enabled</td><td>false</td><td>boolean</td></tr>
<tr><td>snapshotPeriod</td><td>Period in minutes for each snapshot</td><td>false</td><td>integer</td></tr>
<tr><td>snmpScan</td><td>SNMP scan enabled</td><td>false</td><td>boolean</td></tr>
<tr><td>specificPorts</td><td>[FUTURE] A set of specific ports allowed to be used as source ports for an active scan</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>type</td><td></td><td>false</td><td>enum</td></tr>
<tr><td>values</td><td>It can be a single port or two ports [start, end] for a Range</td><td>false</td><td>integer []</td></tr>
</table>
</td></tr>
<tr><td>tcpPorts</td><td>TCP Ports</td><td>false</td><td>integer []</td></tr>
<tr><td>tcpPortScan</td><td>TCP Port scan enabled</td><td>false</td><td>boolean</td></tr>
<tr><td>udpPorts</td><td>UDP Ports</td><td>false</td><td>integer []</td></tr>
<tr><td>udpPortScan</td><td>UDP Port scan enabled</td><td>false</td><td>boolean</td></tr>
<tr><td>useFullDnsScan</td><td>DNS Full scan enabled</td><td>false</td><td>boolean</td></tr>
<tr><td>usePeriodicSnapshots</td><td>Ranger views are generated periodically by the snapshot period</td><td>false</td><td>boolean</td></tr>
<tr><td>useSpecificPorts</td><td>[FUTURE] Use only specific ports defined in specific ports as source ports of active scans</td><td>false</td><td>boolean</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Update Ranger Settings

PUT /web/api/v2.1/ranger/settings

Change the Ranger Settings. Best Practice: Get the current settings before you change them. See: Get Ranger Settings.

> **BEST PRACTICE**
> Get the current settings before you change them. See: Get Ranger Settings.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - Insufficient permissions

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
accountId	Account id	false	string
autoEnableNetworks	All networks that match the min agents configuration will be enabled automatically	false	boolean
combineDevices	Combine devices as one among multiple networks	false	boolean
enabled	Is the ranger	false	boolean

				collection enabled for the account		
			icmpScan	ICMP scan enabled	false	boolean
			mdnsScan	MDNS scan enabled	false	boolean
			minAgentsInNetworkToScan	Minimum agents required in a network to be listed as selectable for scan	false	integer
			multiScanSsdp	SSDP Multicast scan enabled	false	boolean
			networkDecommissionValue	The number of days to archive a network which was not enabled for scan	false	integer
			newNetworkInHours	Networks are going to be marked as new for this period	false	integer
			rdnsScan	RDNS scan enabled	false	boolean
			restrictions	A set of IP addresses that should not be scanned in the specific network	false	

Name	Description	Required	Value
annotation	An optional note with the reason for the restriction	false	string
type		false	enum
values	It will be one IP or one	false	string []

						CIDR or two values for a Range
			scanOnlyLocalSubnets	Scan only local subnets	false	boolean
			scopeId	Scope id	false	string
			smbScan	SMB scan enabled	false	boolean
			snapshotPeriod	Period in minutes for each snapshot	false	integer
			snmpScan	SNMP scan enabled	false	boolean
			specificPorts	[FUTURE] A set of specific ports allowed to be used as source ports for an active scan	false	Name: type; Description: ; Required: false; Value: enum Name: values; Description: It can be a single port or two ports [start, end] for a Range; Required: false; Value: integer []
			tcpPorts	TCP Ports	false	integer []
			tcpPortScan	TCP Port scan enabled	false	boolean
			udpPorts	UDP Ports	false	integer []
			udpPortScan	UDP Port scan enabled	false	boolean
			useFullDnsScan	DNS Full scan enabled	false	boolean
			usePeriodicSnapshots	Ranger views are generated periodically by the snapshot period	false	boolean
			useSpecificPorts	[FUTURE] Use only specific ports	false	boolean

				defined in specific ports as source ports of active scans		
errors	Errors	false	array			

Body Schema

Name	Description	Required	Value
data	Data	true	

Name	Description	Required	Value
accountId	Account id	false	string
autoEnableNetworks	All networks that match the min agents configuration will be enabled automatically	false	boolean
combineDevices	Combine devices as one among multiple networks	false	boolean
enabled	Is the ranger collection enabled for the account	false	boolean
icmpScan	ICMP scan enabled	false	boolean
mdnsScan	MDNS scan enabled	false	boolean
minAgentsInNetworkToScan	Minimum agents required in a network to be listed as selectable for scan	false	integer
multiScanSsdp	SSDP Multicast scan enabled	false	boolean
networkDecommissionValue	The number of days to archive a network which was	false	integer

				not enabled for scan		
			newNetworkInHours	Networks are going to be marked as new for this period	false	integer
			rdnsScan	RDNS scan enabled	false	boolean
			restrictions	A set of IP addresses that should not be scanned in the specific network	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>annotation</td><td>An optional note with the reason for the restriction</td><td>false</td><td>string</td></tr><tr><td>type</td><td></td><td>false</td><td>enum</td></tr><tr><td>values</td><td>It will be one IP or one CIDR or two values for a Range</td><td>false</td><td>string []</td></tr></table>
			scanOnlyLocalSubnets	Scan only local subnets	false	boolean
			scopeId	Scope id	false	string
			smbScan	SMB scan enabled	false	boolean
			snapshotPeriod	Period in minutes for each snapshot	false	integer
			snmpScan	SNMP scan enabled	false	boolean
			specificPorts	[FUTURE] A set of specific ports allowed to be used as source ports for an active scan	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>type</td><td></td><td>false</td><td>enum</td></tr><tr><td>values</td><td>It can be a single port or two ports [start, end]</td><td>false</td><td>integer []</td></tr></table>

						for a Range
			tcpPorts	TCP Ports	false	integer []
			tcpPortScan	TCP Port scan enabled	false	boolean
			udpPorts	UDP Ports	false	integer []
			udpPortScan	UDP Port scan enabled	false	boolean
			useFullDnsScan	DNS Full scan enabled	false	boolean
			usePeriodicSnapshots	Ranger views are generated periodically by the snapshot period	false	boolean
			useSpecificPorts	[FUTURE] Use only specific ports defined in specific ports as source ports of active scans	false	boolean
filter	Filter	true	Name	Description	Required	Value
			accountIds	List of Account IDs to filter by	false	string []
			siteIds	List of Site IDs to filter by	false	string []

Change Device Review in Bulk

POST /web/api/v2.1/ranger/device-review

Change the review state of more than one device.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
data	Response data	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>affected</td><td>Number of entities affected by the requested operation</td><td>false</td><td>integer</td></tr></table>
errors	Errors	false	array

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>deviceReview</td><td>The device review state</td><td>true</td><td>enum</td></tr>
<tr><td>reason</td><td>Reason for the change</td><td>false</td><td>string</td></tr>
<tr><td>reasonDetails</td><td>Reason details for the change</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>filter</td><td>Filter</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>Single Account ID to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>agentIds</td><td>List of agent ids</td><td>false</td><td>string []</td></tr>
<tr><td>deviceFunction__contains</td><td>Free-text filter by device function (supports multiple values)</td><td>false</td><td>string []</td></tr>
<tr><td>deviceReviews</td><td>The device review state</td><td>false</td><td>string []</td></tr>
<tr><td>deviceType</td><td>Device type</td><td>false</td><td>string</td></tr>
<tr><td>deviceTypes</td><td>Device types</td><td>false</td><td>string []</td></tr>
<tr><td>discoveryMethods</td><td>Discovery methods</td><td>false</td><td>string []</td></tr>
<tr><td>domains</td><td>Included network domains</td><td>false</td><td>string []</td></tr>
<tr><td>externalIp</td><td>Search using external IP</td><td>false</td><td>string</td></tr>
<tr><td>externalIp__contains</td><td>Free-text filter by visible IP</td><td>false</td><td>string []</td></tr>
</table>
</td></tr>
</table>

				(supports multiple values)		
			firstSeen__between	Date range refor first seen(format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			firstSeen__gt	Devices first seen after this timestamp	false	string
			firstSeen__gte	Devices first seen after or at this timestamp	false	string
			firstSeen__lt	Devices first seen before this timestamp	false	string
			firstSeen__lte	Devices first seen before or at this timestamp	false	string
			gatewayMacAddress	A gateway mac address to search for	false	string
			gatewayMacAddress__contains	Free-text filter by gateway mac address (supports multiple values)	false	string []
			hasUserLabel		false	boolean
			hostnames	Hostnames	false	string []
			hostnames__contains	Free-text filter by hostname	false	string []

				(supports multiple values)		
			ids	List of device ids	false	string []
			knownFingerprintingData	Known fingerprinting data	false	string []
			lastSeen__between	Date range for last seen(format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			lastSeen__gt	Devices last seen after this timestamp	false	string
			lastSeen__gte	Devices last seen after or at this timestamp	false	string
			lastSeen__lt	Devices last seen before this timestamp	false	string
			lastSeen__lte	Devices last seen before or at this timestamp	false	string
			localIp	Search using local IP	false	string
			localIp__contains	Free-text filter by IP Address (supports multiple values)	false	string []
			macAddress	A mac address to	false	string

				search for		
			macAddress__contains	Free-text filter by mac address (supports multiple values)	false	string []
			managedState	Is the device managed	false	string
			managedStates	Is the device managed	false	string []
			manufacturer	Manufacturer of the device or network interface	false	string
			manufacturer__contains	Free-text filter by manufacturer (supports multiple values)	false	string []
			networkName	Search using network name	false	string
			networkName__contains	Free-text filter by network name (supports multiple values)	false	string []
			osName	Os name	false	string
			osType	OS type	false	string
			osTypes	Included OS types	false	string []
			osVersion	Os version	false	string
			osVersion__contains	Free-text filter by OS full name and version	false	string []

				(supports multiple values)		
			period	Period	false	enum
			query	Query	false	string
			siteIds	Single Site ID to filter by	false	string []
			siteNames	Included site names	false	string []
			subnetAddress__contains	Free-text filter by Subnet Address (supports multiple values)	false	string []
			tagName__contains	Free-text filter by tag name (supports multiple values)	false	string []
			tcpPorts__contains	Free-text filter by tcp port (supports multiple values)	false	integer []
			udpPorts__contains	Free-text filter by udp port (supports multiple values)	false	integer []

Change Device Review

PUT /web/api/v2.1/ranger/device-review/{inventory_id}

Change the review state of one device.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
agentId	The agent id if this is a known managed device	false	string
deviceFunction	Function of the device	false	string
deviceReview	The device review state	false	string
deviceReviewLog	Log of actions for this device	false	

Name	Description	Required	Value
current		false	string
previous		false	string
reason		false	string
reasonDetails		false	string
updatedAt		false	string
username		false	string

Name	Description	Required	Value
deviceType	Role of the device	false	string

			discoveryMethods	Methods used to discover the device	false	string []
			domain	The domain of the device	false	string
			externalIp	Main Gateway Visible IP	false	string
			fingerPrintScore	The confidence for this fingerprinting result	false	integer
			firstSeen	Time the device was first seen	false	string
			gatewayIpAddress	Main gateway IP address	false	string
			gatewayMacAddress	Main gateway MAC address	false	string
			hasIdentity	Would we be able to identify this device over time	false	boolean
			hasUserLabel	True if it has a user label	false	boolean
			hostnames	Array of host names	false	string []
			id	Id of the device	false	string
			ipAddresses	A list of ip addresses. When it is not combined it is always one element	false	string []

			labelUpdatedAt	The date of the last label update	false	string
			labelUserName	The user that changed the label	false	string
			lastSeen	Time the device was last seen	false	string
			localIp	Local ip of the device	false	string
			macAddress	Mac address of the device	false	string
			managedState	Protection state of the device	false	string
			manufacturer	Manufacturer of the device or network interface	false	string
			networkName	The network name	false	string
			networks	A list of all the networks associated to the device. When it is not combined it is always one element	false	

Name	Description	Required	Value
externalIp	Main Gateway Visible IP	false	string
gatewayIpAddress	Main gateway IP address	false	string
gatewayMacAddress	Main gateway MAC address	false	string
ip	The IP of the device in the network	false	string
networkName	The network name	false	string
subnetAddress	Main subnet address	false	string

<table>
<tr><td></td><td></td><td></td><td>
<table>
<tr><td>osName</td><td>OS Name/ Version of the device</td><td>false</td><td>string</td></tr>
<tr><td>osType</td><td>Os Type of the device</td><td>false</td><td>string</td></tr>
<tr><td>osVersion</td><td>OS Version of the device</td><td>false</td><td>string</td></tr>
<tr><td>previousDeviceFunction</td><td>Previous Function of the device if manually changed</td><td>false</td><td>string</td></tr>
<tr><td>previousOsType</td><td>Previous Os Type of the device if manually changed</td><td>false</td><td>string</td></tr>
<tr><td>previousOsVersion</td><td>Previous OS Version of the device if manually changed</td><td>false</td><td>string</td></tr>
<tr><td>siteName</td><td>Site name</td><td>false</td><td>string</td></tr>
<tr><td>subnetAddress</td><td>Main subnet address</td><td>false</td><td>string</td></tr>
<tr><td>tags</td><td>The tags</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>id</td><td>The tag id</td><td>true</td><td>string</td></tr>
<tr><td>description</td><td>The tag description</td><td>false</td><td>string</td></tr>
<tr><td>kind</td><td>Kind of tag if relevant</td><td>false</td><td>string</td></tr>
<tr><td>name</td><td>The tag name</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>tcpPorts</td><td>TCP Ports</td><td>false</td><td>integer []</td></tr>
<tr><td>udpPorts</td><td>UDP Ports</td><td>false</td><td>integer []</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>deviceReview</td><td>The device review state</td><td>true</td><td>enum</td></tr>
<tr><td>reason</td><td>Reason for the change</td><td>false</td><td>string</td></tr>
<tr><td>reasonDetails</td><td>Reason details for the change</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
</table>

Change Device Tags

POST /web/api/v2.1/ranger/tags

Change the device tags.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
data	Response data	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>affected</td><td>Number of entities affected by the requested operation</td><td>false</td><td>integer</td></tr></table>
errors	Errors	false	array

Body Schema

Name	Description	Required	Value
filter	Filter	true	

Name	Description	Required	Value
accountIds	Single Account ID to filter by	false	string []
agentIds	List of agent ids	false	string []
deviceFunction__contains	Free-text filter by device function (supports multiple values)	false	string []
deviceReviews	The device review state	false	string []
deviceType	Device type	false	string
deviceTypes	Device types	false	string []
discoveryMethods	Discovery methods	false	string []
domains	Included network domains	false	string []
externalIp	Search using external IP	false	string
externalIp__contains	Free-text filter by visible IP (supports multiple values)	false	string []
firstSeen__between	Date range refor first seen(format: <from_timestamp>-<to_timestamp>, inclusive)	false	string

			firstSeen__gt	Devices first seen after this timestamp	false	string
			firstSeen__gte	Devices first seen after or at this timestamp	false	string
			firstSeen__lt	Devices first seen before this timestamp	false	string
			firstSeen__lte	Devices first seen before or at this timestamp	false	string
			gatewayMacAddress	A gateway mac address to search for	false	string
			gatewayMacAddress__contains	Free-text filter by gateway mac address (supports multiple values)	false	string []
			hasUserLabel		false	boolean
			hostnames	Hostnames	false	string []
			hostnames__contains	Free-text filter by hostname (supports multiple values)	false	string []
			ids	List of device ids	false	string []
			knownFingerprintingData	Known fingerprinting data	false	string []
			lastSeen__between	Date range for last	false	string

				seen(format: <from_timestamp>-<to_timestamp>, inclusive)		
			lastSeen__gt	Devices last seen after this timestamp	false	string
			lastSeen__gte	Devices last seen after or at this timestamp	false	string
			lastSeen__lt	Devices last seen before this timestamp	false	string
			lastSeen__lte	Devices last seen before or at this timestamp	false	string
			localIp	Search using local IP	false	string
			localIp__contains	Free-text filter by IP Address (supports multiple values)	false	string []
			macAddress	A mac address to search for	false	string
			macAddress__contains	Free-text filter by mac address (supports multiple values)	false	string []
			managedState	Is the device managed	false	string
			managedStat	Is the device	false	string []

			es	managed		
			manufacturer	Manufacturer of the device or network interface	false	string
			manufacturer__contains	Free-text filter by manufacturer (supports multiple values)	false	string []
			networkName	Search using network name	false	string
			networkName__contains	Free-text filter by network name (supports multiple values)	false	string []
			osName	Os name	false	string
			osType	OS type	false	string
			osTypes	Included OS types	false	string []
			osVersion	Os version	false	string
			osVersion__contains	Free-text filter by OS full name and version (supports multiple values)	false	string []
			period	Period	false	enum
			query	Query	false	string
			siteIds	Single Site ID to filter by	false	string []
			siteNames	Included site names	false	string []

<table>
<tr><td></td><td></td><td></td><td>
<table>
<tr><td>subnetAddress__contains</td><td>Free-text filter by Subnet Address (supports multiple values)</td><td>false</td><td>string []</td></tr>
<tr><td>tagName__contains</td><td>Free-text filter by tag name (supports multiple values)</td><td>false</td><td>string []</td></tr>
<tr><td>tcpPorts__contains</td><td>Free-text filter by tcp port (supports multiple values)</td><td>false</td><td>integer []</td></tr>
<tr><td>udpPorts__contains</td><td>Free-text filter by udp port (supports multiple values)</td><td>false</td><td>integer []</td></tr>
</table>
</td></tr>
<tr><td>data</td><td>Data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>id</td><td>The tag id</td><td>true</td><td>string</td></tr>
<tr><td>description</td><td>The tag description</td><td>false</td><td>string</td></tr>
<tr><td>kind</td><td>Kind of tag if relevant</td><td>false</td><td>string</td></tr>
<tr><td>name</td><td>The tag name</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
</table>

Ranger Deploy

Create Cred Group

POST /web/api/v2.1/ranger/cred-groups

Create a new Cred Group.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
groupName	The cred group name	true	string
groupPassphrase	Encrypted passphrase with key unknown by the management	true	string
scopeId	Scope id	true	string
domain	The domain associated to this cred group	false	string
id	The cred group id	false	string
targetOs	The os type	false	enum

				for this cred group		
			totalDetails	The number of cred details in the group	false	integer
errors	Errors	false	array			

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>groupName</td><td>The cred group name</td><td>true</td><td>string</td></tr>
<tr><td>groupPassphrase</td><td>Encrypted passphrase with key unknown by the management</td><td>true</td><td>string</td></tr>
<tr><td>scopeId</td><td>Scope id</td><td>true</td><td>string</td></tr>
<tr><td>domain</td><td>The domain associated to this cred group</td><td>false</td><td>string</td></tr>
<tr><td>targetOs</td><td>The os type for this cred group</td><td>false</td><td>enum</td></tr>
</table>
</td></tr>
</table>

Get Cred groups

GET /web/api/v2.1/ranger/cred-groups

Get the data for each row in the Cred Groups table.

Parameters

accountids	optional	Single Account ID to filter by. Example: "225494730938493804".
countonly	optional	If true, only total number of items will be returned, without any of the actual objects.
cursor	optional	Cursor position returned by the last request. Use to iterate over more than 1000 items. Example: "YWdlbnRfaWQ6NTgwMjkzODE=".
groupname	optional	Group name being searched
groupnamelike	optional	Group name being searched
ids	optional	A list of ids to get
limit	optional	Limit number of returned items (1-1000). Example: "10".
siteids	optional	Single Site ID to filter by. Example: "225494730938493804".
skip	optional	Skip first number of items (0-1000). To iterate over more than 1000 items, use "cursor". Example: "150".
skipcount	optional	If true, total number of items will not be calculated, which speeds up execution time.
sortby	optional	The column to sort the results by. Example: "id".
sortorder	optional	Sort direction. Example: "asc".
targetos	optional	The os type for this cred group. Example: "windows".
totaldetails__gt	optional	Get creds with total details greater than the supplied number

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - Insufficient permissions

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>pagination</td><td>Pagination information</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>totalItems</td><td>Total number of items found matching your query</td><td>true</td><td>integer</td></tr>
<tr><td>nextCursor</td><td>Pass this value as "cursor" on your next request, to get the next page of results (Will be "null" when last page reached)</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>groupName</td><td>The cred group name</td><td>true</td><td>string</td></tr>
<tr><td>groupPassphrase</td><td>Encrypted passphrase with key unknown by the management</td><td>true</td><td>string</td></tr>
<tr><td>scopeId</td><td>Scope id</td><td>true</td><td>string</td></tr>
<tr><td>domain</td><td>The domain associated to this cred group</td><td>false</td><td>string</td></tr>
<tr><td>id</td><td>The cred group id</td><td>false</td><td>string</td></tr>
<tr><td>targetOs</td><td>The os type</td><td>false</td><td>enum</td></tr>
</table>
</td></tr>
</table>

				for this cred group		
			totalDetails	The number of cred details in the group	false	integer
errors	Errors	false	array			

Delete Cred Group

DELETE /web/api/v2.1/ranger/cred-groups/{cred_group_id}

Delete cred group value.

Response Messages

200 - Success

401 - Unauthorized access - please sign in and retry.

404 - Cred group not found.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td><table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>success</td><td>Indicates a successful operation</td><td>false</td><td>boolean</td></tr></table></td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Add cred details

POST /web/api/v2.1/ranger/cred-groups/details

Add cred details to a cred group.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

404 - Cred group not found.

Response Schema

Name	Description	Required	Value
data	Response data	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>success</td><td>Indicates a successful operation</td><td>false</td><td>boolean</td></tr></table>
errors	Errors	false	array

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>credGroupId</td><td>Cred group id</td><td>true</td><td>string</td></tr>
<tr><td>details</td><td>The cred group details</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>credType</td><td>The type of the cred</td><td>true</td><td>string</td></tr>
<tr><td>encryptedCred</td><td>The encrypted creds</td><td>true</td><td>string</td></tr>
<tr><td>encryptedKey</td><td>A encrypted key for the creds</td><td>true</td><td>string</td></tr>
<tr><td>title</td><td>The title for the cred</td><td>true</td><td>string</td></tr>
</table>
</td></tr>
</table>
</td></tr>
</table>

Get Cred group details

GET /web/api/v2.1/ranger/cred-groups/details

Get the data for each row in the Cred Groups details table.

Parameters

accountids	optional	Single Account ID to filter by. Example: "225494730938493804".
countonly	optional	If true, only total number of items will be returned, without any of the actual objects.
credgroupids	optional	A list of ids to get
credtypelike	optional	The type of the cred group
cursor	optional	Cursor position returned by the last request. Use to iterate over more than 1000 items. Example: "YWdlbnRfaWQ6NTgwMjkzODE=".
ids	optional	A list of ids to get
limit	optional	Limit number of returned items (1-1000). Example: "10".
siteids	optional	Single Site ID to filter by. Example: "225494730938493804".
skip	optional	Skip first number of items (0-1000). To iterate over more than 1000 items, use "cursor". Example: "150".
skipcount	optional	If true, total number of items will not be calculated, which speeds up execution time.
sortby	optional	The column to sort the results by. Example: "id".
sortorder	optional	Sort direction. Example: "asc".
title	optional	Exact filter by title
titlelike	optional	Like filter by title

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - Insufficient permissions

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>pagination</td><td>Pagination information</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>totalItems</td><td>Total number of items found matching your query</td><td>true</td><td>integer</td></tr>
<tr><td>nextCursor</td><td>Pass this value as "cursor" on your next request, to get the next page of results (Will be "null" when last page reached)</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>credType</td><td>The type of the cred group</td><td>true</td><td>string</td></tr>
<tr><td>title</td><td>The title for the cred</td><td>true</td><td>string</td></tr>
<tr><td>createdAt</td><td>The creation time</td><td>false</td><td>string</td></tr>
<tr><td>createdBy</td><td>The user that created the details</td><td>false</td><td>string</td></tr>
<tr><td>credGroupId</td><td>The cred group id</td><td>false</td><td>string</td></tr>
<tr><td>id</td><td>The detail id</td><td>false</td><td>string</td></tr>
<tr><td>updatedAt</td><td>The last update time</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
</table>

			updatedBy | The user that updated the details | false | string
errors	Errors	false	array

Delete Cred Group Detail

DELETE /web/api/v2.1/ranger/cred-groups/details/{detail_id}

Delete cred group detail value.

Response Messages

200 - Success

401 - Unauthorized access - please sign in and retry.

404 - Cred group not found.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td><table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>success</td><td>Indicates a successful operation</td><td>false</td><td>boolean</td></tr></table></td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Update Cred Group Details

PUT /web/api/v2.1/ranger/cred-groups/details/{detail_id}

Update cred group values.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

404 - Cred group not found.

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
credType	The type of the cred group	true	string
title	The title for the cred	true	string
createdAt	The creation time	false	string
createdBy	The user that created the details	false	string
credGroupId	The cred group id	false	string
id	The detail id	false	string
updatedAt	The last update time	false	string
updatedBy	The user that updated the details	false	string

errors	Errors	false	array

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>credType</td><td>The type of the cred</td><td>true</td><td>string</td></tr>
<tr><td>encryptedCred</td><td>The encrypted creds</td><td>true</td><td>string</td></tr>
<tr><td>encryptedKey</td><td>A encrypted key for the creds</td><td>true</td><td>string</td></tr>
<tr><td>title</td><td>The title for the cred</td><td>true</td><td>string</td></tr>
</table>
</td></tr>
</table>

Ranger Self Enablement

Get Self Enablement

GET /web/api/v2.1/ranger/enablement

[DEPRECATED] Use the Update Account, Get Account, Get Sites, or the Update Site Add-ons APIs instead.

Parameters

accountids	optional	List of Account IDs to filter by. Example: "225494730938493804,225494730938493915".
activeagents	optional	The number of non-decommissioned agents in the site
activeagents__between	optional	Agent count (between). Example: "2-8".
activeagents__gt	optional	Agent count (more than)
activeagents__gte	optional	Agent count (more than or equal)
activeagents__lt	optional	Agent count (less than)
activeagents__lte	optional	Agent count (less than or equal)
countonly	optional	If true, only total number of items will be returned, without any of the actual objects.
cursor	optional	Cursor position returned by the last request. Use to iterate over more than 1000 items. Example: "YWdlbnRfaWQ6NTgwMjkzODE=".
groupids	optional	List of Group IDs to filter by. Example: "225494730938493804,225494730938493915".
id	optional	The enablement id. Example: "225494730938493804".
ids	optional	A list of ids to get. Example: "225494730938493804,225494730938493915".
limit	optional	Limit number of returned items (1-1000). Example: "10".
rangerenabled	optional	Ranger Enabled true/false
rangerproenabled	optional	[DEPRECATED]. Use rangerEnabled instead. Ranger Pro Enabled true/false

roguesenabled	optional	Rogues Enabled true/false
siteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".
sitename	optional	The site name
sitename__contains	optional	Free-text filter by site name (supports multiple values)
skip	optional	Skip first number of items (0-1000). To iterate over more than 1000 items, use "cursor". Example: "150".
skipcount	optional	If true, total number of items will not be calculated, which speeds up execution time.
sortby	optional	The column to sort the results by. Example: "id".
sortorder	optional	Sort direction. Example: "asc".
tenant	optional	Indicates a tenant scope request

Response Messages

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

404 -

Change Ranger or Rogues Features

POST /web/api/v2.1/ranger/enablement

[DEPRECATED] Use the Update Account, Get Account, Get Sites, or the Update Site Add-ons APIs instead.

Response Messages

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

404 -

Body Schema

Name	Description	Required	Value
data	Data	true	

Name	Description	Required	Value
rangerEnabled	Ranger Enabled true/false	false	boolean
rangerProEnabled	[DEPRECATED] Use rangerEnabled parameter instead. Ranger Pro Enabled true/false	false	boolean
roguesEnabled	Rogues Enabled true/false	false	boolean

Name	Description	Required	Value
filter	Filter	true	

Name	Description	Required	Value
accountIds	List of Account IDs to filter by	false	string []
activeAgents	The number of non-decommissioned agents in the site	false	integer
activeAgents__between	Agent count (between)	false	string
activeAgents__gt	Agent count (more than)	false	integer
activeAgents__gte	Agent count (more than or equal)	false	integer
activeAgents__lt	Agent count (less than)	false	integer
activeAgents__lte	Agent count (less than or equal)	false	integer
groupIds	List of Group IDs to filter	false	string []

				by		
			id	The enablement id	false	string
			ids	A list of ids to get	false	string []
			rangerEnabled	Ranger Enabled true/false	false	boolean
			rangerProEnabled	[DEPRECATED]. Use rangerEnabled instead. Ranger Pro Enabled true/false	false	boolean
			roguesEnabled	Rogues Enabled true/false	false	boolean
			siteIds	List of Site IDs to filter by	false	string []
			siteName	The site name	false	string
			siteName__contains	Free-text filter by site name (supports multiple values)	false	string []
			tenant	Indicates a tenant scope request	false	boolean

Change the Self-Enablement for Accounts

POST /web/api/v2.1/ranger/enable-self-management

[DEPRECATED] Use the Update Account, Get Account, Get Sites, or the Update Site Add-ons APIs instead.

Response Messages

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

404 -

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>enable</td><td>enable: true/ false</td><td>false</td><td>boolean</td></tr>
</table>
</td></tr>
<tr><td>filter</td><td>Filter</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
</table>
</td></tr>
</table>

Features Configuration for New Sites

GET /web/api/v2.1/ranger/enablement/defaults

[DEPRECATED] Use the Update Account, Get Account, Get Sites, or the Update Site Add-ons APIs instead..

Parameters

accountids	optional	List of Account IDs to filter by. Example: "225494730938493804,225494730938493915".

Response Messages

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

404 -

Change Feature Defaults for New Sites

POST /web/api/v2.1/ranger/enablement/defaults

[DEPRECATED] Use the Update Account, Get Account, Get Sites, or the Update Site Add-ons APIs instead.

Response Messages

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

404 -

Body Schema

Name	Description	Required	Value
data	Data	true	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr></table>

			rangerEnabled	Ranger Enabled true/false	false	boolean
			rangerProEnabled	[DEPRECATED] Use rangerEnabled parameter instead. Ranger Pro Enabled true/false	false	boolean
			roguesEnabled	Rogues Enabled true/false	false	boolean
filter	Filter	true	Name	Description	Required	Value
			accountIds	List of Account IDs to filter by	false	string []
			activeAgents	The number of non-decommissioned agents in the site	false	integer
			activeAgents__between	Agent count (between)	false	string
			activeAgents__gt	Agent count (more than)	false	integer
			activeAgents__gte	Agent count (more than or equal)	false	integer
			activeAgents__lt	Agent count (less than)	false	integer
			activeAgents__lte	Agent count (less than or equal)	false	integer
			groupIds	List of Group IDs to filter by	false	string []
			id	The enablement	false	string

				id		
			ids	A list of ids to get	false	string []
			rangerEnabled	Ranger Enabled true/false	false	boolean
			rangerProEnabled	[DEPRECATED]. Use rangerEnabled instead. Ranger Pro Enabled true/false	false	boolean
			roguesEnabled	Rogues Enabled true/false	false	boolean
			siteIds	List of Site IDs to filter by	false	string []
			siteName	The site name	false	string
			siteName__contains	Free-text filter by site name (supports multiple values)	false	string []
			tenant	Indicates a tenant scope request	false	boolean

RBAC

Get All Roles

GET /web/api/v2.1/rbac/roles

See roles assigned to users that match the filter, a basic description of the roles, and the number of users for each role.
Role-Based Access Control (RBAC) has predefined roles. (Currently, customized roles are not supported.), This command gives the ID of the role, which you can use in other commands.

Parameters

accountids	optional	List of Account IDs to filter by. Example: "225494730938493804,225494730938493915".
accountname	optional	Name of the account that contains the role
countonly	optional	If true, only total number of items will be returned, without any of the actual objects.
createdat	optional	Created at. Example: "2018-02-27T04:49:26.257525Z".
createdat__between	optional	Return RBAC roles created within this range (inclusive). Example: "1514978764288-1514978999999".
createdat__gt	optional	Return RBAC roles created after this timestamp. Example: "2018-02-27T04:49:26.257525Z".
createdat__gte	optional	Return RBAC roles created after or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
createdat__lt	optional	Return RBAC roles created before this timestamp. Example: "2018-02-27T04:49:26.257525Z".
createdat__lte	optional	Return RBAC roles created before or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
creator	optional	Email of the creating user
creatorid	optional	Id of the creating user. Example: "225494730938493804".
cursor	optional	Cursor position returned by the last request. Use to iterate over more than 1000 items. Example: "YWdlbnRfaWQ6NTgwMjkzODE=".

description	optional	Description
groupids	optional	List of Group IDs to filter by. Example: "225494730938493804,225494730938493915".
ids	optional	List of ids to filter by. Example: "225494730938493804,225494730938493915".
includechildren	optional	Include child scopes roles
includeparents	optional	Include parent scopes roles
limit	optional	Limit number of returned items (1-1000). Example: "10".
name	optional	Return RBAC role matching the name
query	optional	Free text search on role name, and description
siteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".
sitename	optional	Name of the site that contains the role
skip	optional	Skip first number of items (0-1000). To iterate over more than 1000 items, use "cursor". Example: "150".
skipcount	optional	If true, total number of items will not be calculated, which speeds up execution time.
sortby	optional	The column to sort the results by. Example: "id".
sortorder	optional	Sort direction. Example: "asc".
tenancyids	optional	List of Tenancies IDs to filter by. Example: "225494730938493804,225494730938493915".
tenant	optional	Indicates a tenant scope request
updatedat	optional	Updated at. Example: "2018-02-27T04:49:26.257525Z".
updatedat__between	optional	Return RBAC roles updated within this range (inclusive). Example: "1514978764288-1514978999999".
updatedat__gt	optional	Return RBAC roles updated after this timestamp. Example: "2018-02-27T04:49:26.257525Z".
updatedat__gte	optional	Return RBAC roles updated after or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
updatedat__lt	optional	Return RBAC roles updated before this timestamp. Example: "2018-02-27T04:49:26.257525Z".
updatedat__lte	optional	Return RBAC roles updated before or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".

updatedby	optional	Email of the updating user
updatedbyid	optional	Id of the updating user. Example: "225494730938493804".
usersinroles	optional	How many users use this role

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
pagination	Pagination information	true	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>totalItems</td><td>Total number of items found matching your query</td><td>true</td><td>integer</td></tr><tr><td>nextCursor</td><td>Pass this value as "cursor" on your next request, to get the next page of results (Will be "null" when last page reached)</td><td>false</td><td>string</td></tr></table>
data	Response data	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>accountName</td><td>Account name</td><td>false</td><td>string</td></tr><tr><td>createdAt</td><td>Created at</td><td>false</td><td>string</td></tr><tr><td>creator</td><td>Email of the creating user</td><td>false</td><td>string</td></tr></table>

			<table><tr><td>creatorId</td><td>Id of the creating user</td><td>false</td><td>string</td></tr><tr><td>description</td><td>Description</td><td>false</td><td>string</td></tr><tr><td>id</td><td>Id</td><td>false</td><td>string</td></tr><tr><td>name</td><td>Name</td><td>false</td><td>string</td></tr><tr><td>predefinedRole</td><td>Whether this role is a system role</td><td>false</td><td>boolean</td></tr><tr><td>scope</td><td>Scope of the role (Group/Site/Account/Tenant)</td><td>false</td><td>string</td></tr><tr><td>scopeId</td><td>Id of the containing scope</td><td>false</td><td>string</td></tr><tr><td>siteName</td><td>Site name</td><td>false</td><td>string</td></tr><tr><td>updatedAt</td><td>Updated at</td><td>false</td><td>string</td></tr><tr><td>updatedBy</td><td>Email of the updating user</td><td>false</td><td>string</td></tr><tr><td>updatedById</td><td>Id of the creating user</td><td>false</td><td>string</td></tr><tr><td>usersInRoles</td><td>How many users use this role</td><td>false</td><td>integer</td></tr></table>
errors	Errors	false	array

Get Specific Role Definition

GET /web/api/v2.1/rbac/role/{role_id}

With the ID of a role (see Get All Roles) you can see the permissions of that role.
The definition of a role can change in different scopes and SKUs. For example, an Admin role with the scope access of a Site does not have Ranger permissions, but an IT role with the scope access of an Account with a Ranger license does have permissions on Ranger.
The Response shows role permissions to see views in the WebUI and to use Console features.

Parameters

accountids	optional	List of Account IDs to filter by. Example: "225494730938493804,225494730938493915".
createdat__between	optional	Return RBAC roles created within this range (inclusive). Example: "1514978764288-1514978999999".
createdat__gt	optional	Return RBAC roles created after this timestamp. Example: "2018-02-27T04:49:26.257525Z".
createdat__gte	optional	Return RBAC roles created after or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
createdat__lt	optional	Return RBAC roles created before this timestamp. Example: "2018-02-27T04:49:26.257525Z".
createdat__lte	optional	Return RBAC roles created before or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
groupids	optional	List of Group IDs to filter by. Example: "225494730938493804,225494730938493915".
name	optional	Return RBAC role matching the name
query	optional	Free text search on role name, and description
siteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".
tenant	optional	Indicates a tenant scope request
updatedat__between	optional	Return RBAC roles updated within this range (inclusive). Example: "1514978764288-1514978999999".
updatedat__gt	optional	Return RBAC roles updated after this timestamp. Example: "2018-02-27T04:49:26.257525Z".
updatedat__gte	optional	Return RBAC roles updated after or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".

updatedat__lt	optional	Return RBAC roles updated before this timestamp. Example: "2018-02-27T04:49:26.257525Z".
updatedat__lte	optional	Return RBAC roles updated before or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
accountName	Account name	false	string
createdAt	Created at	false	string
creator	Email of the creating user	false	string
creatorId	Id of the creating user	false	string
description	Description	false	string
id	Id	false	string
name	Name	false	string
pages	Pages	false	

Name	Description	Required	Value
identifier	Identifier	false	string
name	Name	false	string
permissions	Permissions	false	

Name	Description	Required	Value
additionalDescription	Additional description	false	string
dependsOn	Depends on	false	string []
description	Description	false	string

									disabledReason	Disabled reason	false	string
									disabledReasonCode	Disabled reason code	false	string
									groupName	Group name	false	string
									identifier	Identifier	false	string
									title	Title	false	string
									type	Type	false	string
									value	Value	false	boolean
			predefinedRole	Whether this role is a system role	false	boolean						
			scope	Scope of the role (Group/ Site/ Account/ Tenant)	false	string						
			scopeId	Id of the containing scope	false	string						
			siteName	Site name	false	string						
			updatedAt	Updated at	false	string						
			updatedBy	Email of the updating user	false	string						
			updatedById	Id of the creating user	false	string						
			usersInRoles	How many users use this role	false	integer						
errors	Errors	false	array									

Update role

PUT /web/api/v2.1/rbac/role/{role_id}

With the ID of a role (see Get All Roles), you can update the permissions of users with this role.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
accountName	Account name	false	string
createdAt	Created at	false	string
creator	Email of the creating user	false	string
creatorId	Id of the creating user	false	string
description	Description	false	string
id	Id	false	string
name	Name	false	string
pages	Pages	false	

Name	Description	Required	Value
identifier	Identifier	false	string
name	Name	false	string
permissions	Permissions	false	

Name	Description	Required	Value
additionalDescription	Additional description	false	string

									dependsOn	Depends on	false	string []
									description	Description	false	string
									disabledReason	Disabled reason	false	string
									disabledReasonCode	Disabled reason code	false	string
									groupName	Group name	false	string
									identifier	Identifier	false	string
									title	Title	false	string
									type	Type	false	string
									value	Value	false	boolean
			predefinedRole	Whether this role is a system role	false	boolean						
			scope	Scope of the role (Group/ Site/ Account/ Tenant)	false	string						
			scopeId	Id of the containing scope	false	string						
			siteName	Site name	false	string						
			updatedAt	Updated at	false	string						
			updatedBy	Email of the updating user	false	string						
			updatedById	Id of the creating user	false	string						
			usersInRoles	How many users use this role	false	integer						
errors	Errors	false	array									

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>description</td><td>Description</td><td>true</td><td>string</td></tr>
<tr><td>name</td><td>Recommendation: Use a prefix or suffix for each role that identifies it as related to a specific Account or Site.</td><td>true</td><td>string</td></tr>
<tr><td>permissionIds</td><td>Permission ids</td><td>false</td><td>string []</td></tr>
</table>
</td></tr>
<tr><td>filter</td><td>Filter</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>groupIds</td><td>List of Group IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>siteIds</td><td>List of Site IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>tenant</td><td>Indicates a tenant scope request</td><td>false</td><td>boolean</td></tr>
</table>
</td></tr>
</table>

Delete role

DELETE /web/api/v2.1/rbac/role/{role_id}

With the ID of a role (see Get All Roles), you can delete a role. If there are users assigned to the role, specify the ID of their new role.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>success</td><td>Indicates a successful operation</td><td>false</td><td>boolean</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>targetId</td><td>Role ID of new role to assign to users with the role</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
</table>

Create new role

POST /web/api/v2.1/rbac/role

Create a new role for Role-Based Access Control (RBAC).

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
accountName	Account name	false	string
createdAt	Created at	false	string
creator	Email of the creating user	false	string
creatorId	Id of the creating user	false	string
description	Description	false	string
id	Id	false	string
name	Name	false	string
pages	Pages	false	

Name	Description	Required	Value
identifier	Identifier	false	string
name	Name	false	string
permissions	Permissions	false	

Name	Description	Required	Value
additionalDescription	Additional description	false	string

									dependsOn	Depends on	false	string []
									description	Description	false	string
									disabledReason	Disabled reason	false	string
									disabledReasonCode	Disabled reason code	false	string
									groupName	Group name	false	string
									identifier	Identifier	false	string
									title	Title	false	string
									type	Type	false	string
									value	Value	false	boolean
			predefinedRole	Whether this role is a system role	false	boolean						
			scope	Scope of the role (Group/ Site/ Account/ Tenant)	false	string						
			scopeId	Id of the containing scope	false	string						
			siteName	Site name	false	string						
			updatedAt	Updated at	false	string						
			updatedBy	Email of the updating user	false	string						
			updatedById	Id of the creating user	false	string						
			usersInRoles	How many users use this role	false	integer						
errors	Errors	false	array									

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>description</td><td>Description</td><td>true</td><td>string</td></tr>
<tr><td>name</td><td>Recommendation: Use a prefix or suffix for each role that identifies it as related to a specific Account or Site.</td><td>true</td><td>string</td></tr>
<tr><td>permissionIds</td><td>Permission ids</td><td>false</td><td>string []</td></tr>
</table>
</td></tr>
<tr><td>filter</td><td>Filter</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>groupIds</td><td>List of Group IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>siteIds</td><td>List of Site IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>tenant</td><td>Indicates a tenant scope request</td><td>false</td><td>boolean</td></tr>
</table>
</td></tr>
</table>

Get template for new role

GET /web/api/v2.1/rbac/role

Get the template for a new role.

Parameters

accountids	optional	List of Account IDs to filter by. Example: "225494730938493804,225494730938493915".
groupids	optional	List of Group IDs to filter by. Example: "225494730938493804,225494730938493915".
siteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".
tenant	optional	Indicates a tenant scope request

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
description	Description	true	string
pages	Pages	false	

Name	Description	Required	Value
identifier	Identifier	false	string
name	Name	false	string
permissions	Permissions	false	

Name	Description	Required	Value
additionalDescription	Additional description	false	string

									dependsOn	Depends on	false	string []
									description	Description	false	string
									disabledReason	Disabled reason	false	string
									disabledReasonCode	Disabled reason code	false	string
									groupName	Group name	false	string
									identifier	Identifier	false	string
									title	Title	false	string
									type	Type	false	string
									value	Value	false	boolean
errors	Errors	false	array									

Remote Ops MMS

Create new Destination profile.

POST /web/api/v2.1/remote-ops/data-exporter/destination-profiles

Create Destination profile inside specified scope. If the created profile is requested to be default, the default profile of the specified scope is overriden.

Response Messages

200 - Successes

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td><table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>profileId</td><td>Profile ID</td><td>true</td><td>string</td></tr></table></td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

Name	Description	Required	Value
apiKey	Write key of api account to upload data	true	string
apiUrl	URL of api instance to upload the events	true	string
destination	Destination profile type	true	enum
name	Destination profile name	true	string
scopeId	Scope ID to store the Destination profile	true	string
scopeLevel	Scope level to store the Destination profile	true	enum
isDefault	Flag if the profile should be marked as default in it's scope	false	boolean

Get available Destination profiles

GET /web/api/v2.1/remote-ops/data-exporter/destination-profiles

Get Destination profiles available for the specified scope. The profiles are inherited downwards, e.g. the profiles from parent Account and Tenant scopes are available for a Site. At most one of returned destination profiles will be marked as default for the scope. If the scope does not have default profile defined, it's inherited from the higher scope, unless inheritance was broken

Parameters

scopeid	optional	Scope ID to get Destination profiles configuration. Example: "225494730938493804".
scopelevel	optional	Scope level to get Destination profile configuration. Example: "tenant".

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - User has insufficient permission to perform such action

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
apiKey	Write key of destination account to upload data	true	string
apiUrl	URL of destination instance to upload data	true	string
creator	Email of user who created	true	string

			the Destination profile		
			creatorId	ID of user who created the Destination profile	true	string
			destination	Destination type where the results will be uploaded	true	string
			id	Destination profile ID	true	string
			isDefault	Flag if the Destination profile is default for the scope	true	boolean
			name	Destination profile name	true	string
			scopePath	Path of scope where the Destination profile is stored	true	string
			updater	Email of user who updated the Destination profile	true	string
			updaterId	ID of user who updated the Destination profile	true	string
errors	Errors	false	array

Delete multiple Destination profiles by ID

DELETE /web/api/v2.1/remote-ops/data-exporter/destination-profiles

Delete multiple Destination profiles. The profiles that are not possible to delete (e.g.non-existing or user does not have proper permissions) are skipped. IDs of successfully deleted profiles are returned in response.

Response Messages

200 - Delete was completed or partially completed.

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>affected</td><td>Deleted Destination profile IDs</td><td>false</td><td>string []</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

Name	Description	Required	Value
data	Data	false	
filter	Filter	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>ids</td><td>List of Destination profile IDs to delete</td><td>false</td><td>string []</td></tr></table>

Delete Destination profile by ID

DELETE /web/api/v2.1/remote-ops/data-exporter/destination-profiles/{profile_id}

Delete Destination profile with specified ID. If the profile was used as default for a scope, the last created profile will be marked as default for that scope.

Response Messages

200 - Destination profile is deleted

401 - Unauthorized access - please sign in and retry.

403 - User has insufficient permission to perform such action

404 - Destination profile is not found

Update existing Destination profile

PUT /web/api/v2.1/remote-ops/data-exporter/destination-profiles/{profile_id}

Update contents of existing Destination profile with specified ID. All the profile data should be specified, even if the values are not changed. If the updated profile is requested to be default, the default profile of its scope is modified.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - User has insufficient permission to perform such action

404 - Destination profile is not found

Response Schema

Name	Description	Required	Value

data	Response data	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>profileId</td><td>Profile ID</td><td>true</td><td>string</td></tr></table>
errors	Errors	false	array

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>apiKey</td><td>Write key of api account to upload data</td><td>true</td><td>string</td></tr>
<tr><td>apiUrl</td><td>URL of api instance to upload the events</td><td>true</td><td>string</td></tr>
<tr><td>name</td><td>Destination profile name</td><td>true</td><td>string</td></tr>
<tr><td>isDefault</td><td>Flag if the profile should be marked as default in it's scope</td><td>false</td><td>boolean</td></tr>
</table>
</td></tr>
</table>

Get Destination profile by ID

GET /web/api/v2.1/remote-ops/data-exporter/destination-profiles/{profile_id}

Get Destination profile with specified ID

Parameters

scopeid	optional	Scope ID to get Destination profiles configuration. Example: "225494730938493804".
scopelevel	optional	Scope level to get Destination profile configuration. Example: "tenant".

Response Messages

200 - Get Destination profile

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - User has insufficient permission to perform such action

404 - Destination profile is not found

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
apiKey	Write key of destination account to upload data	true	string
apiUrl	URL of destination instance to upload data	true	string
creator	Email of user who created	true	string

			the Destination profile
			creatorId: ID of user who created the Destination profile; true; string
			destination: Destination type where the results will be uploaded; true; string
			id: Destination profile ID; true; string
			isDefault: Flag if the Destination profile is default for the scope; true; boolean
			name: Destination profile name; true; string
			scopePath: Path of scope where the Destination profile is stored; true; string
			updater: Email of user who updated the Destination profile; true; string
			updaterId: ID of user who updated the Destination profile; true; string
errors	Errors	false	array

Set profile as default profile of the scope

POST /web/api/v2.1/remote-ops/data-exporter/destination-profiles/set-default

Set profile as default profile of the scope

Response Messages

200 - Get Destination profile

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - User has insufficient permission to perform such action

Body Schema

Name	Description	Required	Value
data	Data	true	

Name	Description	Required	Value
profileId	Profile Id to set as default profile	true	string
scopeLevel	Scope level to get Destination profile configuration	true	enum
scopeId	Scope ID to get Destination profiles configuration	false	string

Get results sent to data exporter

GET /web/api/v2.1/remote-ops/data-exporter/results

Get results sent to data exporter

Parameters

agentid	required	Id of the agent the data came from
maliciousgroupid	optional	Threat malicious group id
taskid	optional	Task id

Response Messages

200 - Get Destination profile results

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - User has insufficient permission to perform such action

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
agentResults	Agent results	false	

Name	Description	Required	Value
hasFailures	Indicates if not failures has occurred during upload returned	true	boolean
isEmpty	Indicates if not results returned	true	boolean
url	Url to relevant data source	true	string

<table>
<tr><td></td><td></td><td></td><td>
<table>
<tr><td></td><td></td><td></td><td>
<table>
<tr><td>errorMessage</td><td>Last error message</td><td>false</td><td>string</td></tr>
</table></td></tr>
<tr><td>taskResults</td><td>Task results</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>hasFailures</td><td>Indicates if not failures has occurred during upload returned</td><td>true</td><td>boolean</td></tr>
<tr><td>isEmpty</td><td>Indicates if not results returned</td><td>true</td><td>boolean</td></tr>
<tr><td>url</td><td>Url to relevant data source</td><td>true</td><td>string</td></tr>
<tr><td>errorMessage</td><td>Last error message</td><td>false</td><td>string</td></tr>
</table></td></tr>
<tr><td>threatResults</td><td>Threat results</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>hasFailures</td><td>Indicates if not failures has occurred during upload returned</td><td>true</td><td>boolean</td></tr>
<tr><td>isEmpty</td><td>Indicates if not results returned</td><td>true</td><td>boolean</td></tr>
<tr><td>url</td><td>Url to relevant data source</td><td>true</td><td>string</td></tr>
<tr><td>errorMessage</td><td>Last error message</td><td>false</td><td>string</td></tr>
</table></td></tr>
</table></td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

RemoteOps Forensics

Start collection of Forensics artifacts according to specified profile

POST /web/api/v2.1/remote-ops/forensics/start-collection

Start collection of Forensics artifacts according to specified profile

Response Messages

202 - Forensics collection has been started

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Body Schema

Name	Description	Required	Value
data	Data	true	

Name	Description	Required	Value
destination	Destination	true	

Name	Description	Required	Value
password	Password for encrypting uploaded binary artifacts	false	string
passwordFromScope	Used to specify execution where a generic password is used	false	

Name	Description	Required	Value
scopeLevel	User scope	true	enum
scopeId	string repr. of scope id	false	string

Name	Description	Required	Value
profileId	ID of profile for destination of	false	string

						exported collection date
			collectionProfileId	ID of the Collection Profile that will be used	false	string
			description	Description of the collection	false	string
			tag	Tag identifier of the collection	false	string
filter	Filter specification of targeted agents	true	accountIds	List of Account IDs to filter by	false	string []
			activeThreats	Include Agents with this amount of active threats	false	integer
			activeThreats__gt	Include Agents with at least this amount of active threats	false	integer
			adComputerMember__contains	Free-text filter by Active Directory computer groups string (supports multiple values)	false	string []
			adComputerName__contains	Free-text filter by Active Directory	false	string []

				computer name string (supports multiple values)		
			adComputerQuery__contains	Free-text filter by Active Directory computer name or its groups (supports multiple values)	false	string []
			adQuery	An Active Directory query string	false	string
			adQuery__contains	Free-text filter by Active Directory string (supports multiple values)	false	string []
			adUserMember__contains	Free-text filter by Active Directory user groups string (supports multiple values)	false	string []
			adUserName__contains	Free-text filter by Active Directory username string (supports multiple values)	false	string []

			adUserQuery__contains	Free-text filter by Active Directory computer name or its groups (supports multiple values)	false	string []
			agentNamespace__contains	Free-text filter by agent namespace (supports multiple values)	false	string []
			agentPodName__contains	Free-text filter by agent pod name (supports multiple values)	false	string []
			agentVersion__between	Version range for agent version (format: <from_version>-<to_version>, inclusive)	false	string
			agentVersion__gt	Agents versions greater than given version	false	string
			agentVersion__gte	Agents versions greater than or equal to given version	false	string
			agentVersion__lt	Agents versions less than given version	false	string

			agentVersion__lte	Agents versions less than or equal to given version	false	string
			agentVersions	Agent versions to include	false	string []
			agentVersionsNin	Agent versions not to include	false	string []
			appsVulnerabilityStatuses	Apps vulnerability status in	false	string []
			appsVulnerabilityStatusesNin	Apps vulnerability status nin	false	string []
			awsRole__contains	Free-text filter by aws role(supports multiple values)	false	string []
			awsSecurityGroups__contains	Free-text filter by aws securityGroups(supports multiple values)	false	string []
			awsSubnetIds__contains	Free-text filter by aws subnet ids (supports multiple values)	false	string []
			azureResourceGroup__contains	Free-text filter by azure resource group(supports multiple values)	false	string []
			cloudAccount__contains	Free-text filter by cloud	false	string []

				account (supports multiple values)			
			cloudImage__contains	Free-text filter by cloud image (supports multiple values)	false	string []	
			cloudInstanceId__contains	Free-text filter by cloud instance id(supports multiple values)	false	string []	
			cloudInstanceSize__contains	Free-text filter by cloud instance size(supports multiple values)	false	string []	
			cloudLocation__contains	Free-text filter by cloud location (supports multiple values)	false	string []	
			cloudNetwork__contains	Free-text filter by cloud network (supports multiple values)	false	string []	
			cloudProvider	Agents from which cloud provider	false	string []	
			cloudProviderNin	Exclude Agents from these cloud provider	false	string []	
			cloudTags__co	Free-text	false	string []	

			ntains	filter by cloud tags (supports multiple values)		
			clusterName__contains	Free-text filter by cluster name (supports multiple values)	false	string []
			computerName	Computer name	false	string
			computerName__contains	Free-text filter by computer name (supports multiple values)	false	string []
			computerName__like	Match computer name partially (substring)	false	string
			consoleMigrationStatuses	Migration status in	false	string []
			consoleMigrationStatusesNin	Migration status nin	false	string []
			coreCount__between	Possible number of CPU cores (inclusive)	false	string
			coreCount__gt	CPU cores (more than)	false	integer
			coreCount__gte	CPU cores (more than or equal)	false	integer
			coreCount__lt	CPU cores (less than)	false	integer

			coreCount__lte	CPU cores (less than or equal)	false	integer
			cpuCount__between	Possible number of CPU cores (inclusive)	false	string
			cpuCount__gt	Number of CPUs (more than)	false	integer
			cpuCount__gte	Number of CPUs (more than or equal)	false	integer
			cpuCount__lt	Number of CPUs (less than)	false	integer
			cpuCount__lte	Number of CPUs (less than or equal)	false	integer
			cpuId__contains	Free-text filter by CPU name (supports multiple values)	false	string []
			createdAt__between	Date range for creation time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			createdAt__gt	Agents created after this timestamp	false	string
			createdAt__gte	Agents created after or at this timestamp	false	string
			createdAt__lt	Agents	false	string

				created before this timestamp		
			createdAt__lte	Agents created before or at this timestamp	false	string
			csvFilterId	The ID of the CSV file to filter by	false	string
			decommissionedAt__between	Date range for decommission time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			decommissionedAt__gt	Agents decommissioned after this timestamp	false	string
			decommissionedAt__gte	Agents decommissioned after or at this timestamp	false	string
			decommissionedAt__lt	Agents decommissioned before this timestamp	false	string
			decommissionedAt__lte	Agents decommissioned before this timestamp	false	string
			domains	Included network domains	false	string []
			domainsNin	Not included network domains	false	string []

			encryptedApplications	Disk encryption status	false	boolean
			externalId__contains	Free-text filter by external ID (Customer ID)	false	string []
			externalIp__contains	Free-text filter by visible IP (supports multiple values)	false	string []
			filteredGroupIds	List of Group IDs to filter by	false	string []
			filteredSiteIds	List of Site IDs to filter by	false	string []
			filterId	Include all Agents matching this saved filter	false	string
			firewallEnabled	The agents supports Firewall Control and it is enabled for the agent's group	false	boolean []
			gatewayIp	Gateway ip	false	string
			gcpServiceAccount__contains	Free-text filter by gcp service account (supports multiple values)	false	string []
			groupIds	List of Group IDs to filter by	false	string []

			hasContainerizedWorkload	Include only Agents protecting containerized workloads	false	boolean	
			hasLocalConfiguration	Agent has a local configuration set	false	boolean	
			hasTags	Include only Agents that have any tags assigned if True, or none if False	false	boolean	
			ids	A list of Agent IDs	false	string []	
			infected	Include only Agents with at least one active threat	false	boolean	
			installerTypes	Include only Agents installed with these package types	false	string []	
			installerTypesNin	Exclude Agents installed with these package types	false	string []	
			isActive	Include only active Agents	false	boolean	
			isDecommissioned	Include active, decommissioned or both	false	boolean []	
			isPendingUninstall	Include only Agents with pending	false	boolean	

				uninstall requests			
			isUninstalled	Include installed, uninstalled or both	false	boolean []	
			isUpToDate	Include only Agents with updated software	false	boolean	
			k8sNodeLabels__contains	Free-text filter by K8s node labels (supports multiple values)	false	string []	
			k8sNodeName__contains	Free-text filter by K8s node name (supports multiple values)	false	string []	
			k8sType__contains	Free-text filter by K8s type(supports multiple values)	false	string []	
			k8sVersion__contains	Free-text filter by K8s version (supports multiple values)	false	string []	
			lastActiveDate__between	Date range for last active date(format: <from_timestamp>-<to_timestamp>, inclusive)	false	string	
			lastActiveDate__gt	Agents last active after	false	string	

				this time		
			lastActiveDate__gte	Agents last active after or at this time	false	string
			lastActiveDate__lt	Agents last active before this time	false	string
			lastActiveDate__lte	Agents last active before or at this time	false	string
			lastLoggedInUserName__contains	Free-text filter by username (supports multiple values)	false	string []
			lastSuccessfulScanDate__between	Date range for last successful full disk scan(format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			lastSuccessfulScanDate__gt	Agents last successful full disk scan after this time	false	string
			lastSuccessfulScanDate__gte	Agents last successful full disk scan after or at this time	false	string
			lastSuccessfulScanDate__lt	Agents last successful full disk scan before this time	false	string
			lastSuccessfulScanDate__lt	Agents last successful full	false	string

			e	disk scan before or at this time		
			liveUpdateId__contains	Free-text filter by live update ID (supports multiple values)	false	string []
			locationEnabled	The agents supports Location Awareness and it is enabled for the agent's group	false	boolean []
			locationIds	Include only Agents reporting these locations	false	string []
			locationIdsNin	Do not include only Agents reporting these locations	false	string []
			machineTypes	Included machine types	false	string []
			machineTypesNin	Not included machine types	false	string []
			migrationStatus	Migration status	false	enum
			missingPermissions	Included missing permissions	false	string []
			missingPermissionsNin	Excluded missing permissions	false	string []

			mitigationMode	Agent mitigation mode policy	false	enum
			mitigationModeSuspicious	Mitigation mode policy for suspicious activity	false	enum
			networkInterfaceGatewayMacAddress__contains	Free-text filter by Gateway MAC address (supports multiple values)	false	string []
			networkInterfaceInet__contains	Free-text filter by local IP (supports multiple values)	false	string []
			networkInterfacePhysical__contains	Free-text filter by MAC address (supports multiple values)	false	string []
			networkQuarantineEnabled	The agents supports Network Quarantine Control and its enabled for the agent's group	false	boolean []
			networkStatuses	Included network statuses	false	string []
			networkStatusesNin	Included network statuses	false	string []
			operationalStates	Agent operational state	false	string []

			operationalStatesNin	Do not include these Agent operational states	false	string []
			osArch	OS architecture	false	enum
			osTypes	Included OS types	false	string []
			osTypesNin	Not included OS types	false	string []
			osVersion__contains	Free-text filter by OS full name and version (supports multiple values)	false	string []
			query	A free-text search term, will match applicable attributes (sub-string match). Note: Device's physical addresses will be matched if they start with the search term only (no match if they contain the term).	false	string
			rangerStatus	[DEPRECATED] Use rangerStatuses.	false	enum
			rangerStatuses	Status of Ranger	false	string []

			rangerStatusesNin	Do not include these Ranger Statuses	false	string []	
			rangerVersions	Ranger versions to include	false	string []	
			rangerVersionsNin	Ranger versions not to include	false	string []	
			registeredAt__between	Date range for first registration time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string	
			registeredAt__gt	Agents registered after this time	false	string	
			registeredAt__gte	Agents registered after or at this time	false	string	
			registeredAt__lt	Agents registered before this time	false	string	
			registeredAt__lte	Agents registered before or at this time	false	string	
			remoteOpsForensicsSupported	Include only agents that has Remote Ops Forensicsfeature supported	false	boolean	
			remoteProfili	Agent remote	false	string []	

			ngStates	profiling state			
			remoteProfilingStatesNin	Do not include these Agent remote profiling states	false	string []	
			rsoLevel	Supported Remote Script Orchestration level	false	enum	
			scanStatus	Scan status	false	enum	
			scanStatuses	Included scan statuses	false	string []	
			scanStatuses Nin	Not included scan statuses	false	string []	
			serialNumber __contains	Free-text filter by Serial Number (supports multiple values)	false	string []	
			siteIds	List of Site IDs to filter by	false	string []	
			tagsData	Filter agents by their assigned tags. Given in form of a JSON where each key represents a tag key, and each value represents a list of string values to filter by. To filter by unassigned tag values,	false	string	

				use __nin suffix in the tag key.		
			threatContentHash	Include only Agents that have at least one threat with this content hash	false	string
			threatCreatedAt__between	Agents with threats reported in a date range (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			threatCreatedAt__gt	Agents with threats reported after this time	false	string
			threatCreatedAt__gte	Agents with threats reported after or at this time	false	string
			threatCreatedAt__lt	Agents with threats reported before this time	false	string
			threatCreatedAt__lte	Agents with threats reported before or at this time	false	string
			threatHidden	Include only Agents with at least one hidden threat	false	boolean

			threatMitigationStatus	Include only Agents that have threats with this mitigation status	false	enum
			threatRebootRequired	Has at least one threat with at least one mitigation action pending reboot to succeed	false	boolean []
			threatResolved	Include only Agents with at least one resolved threat	false	boolean
			totalMemory__between	Total memory range (GB, inclusive)	false	string
			totalMemory__gt	Memory size (MB, more than)	false	integer
			totalMemory__gte	Memory size (MB, more than or equal)	false	integer
			totalMemory__lt	Memory size (MB, less than)	false	integer
			totalMemory__lte	Memory size (MB, less than or equal)	false	integer
			updatedAt__between	Date range for update time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string

	updatedAt__gt	Agents updated after this timestamp	false	string		
	updatedAt__gte	Agents updated after or at this timestamp	false	string		
	updatedAt__lt	Agents updated before this timestamp	false	string		
	updatedAt__lte	Agents updated before or at this timestamp	false	string		
	userActionsNeeded	Included pending user actions	false	string []		
	userActionsNeededNin	Excluded pending user actions	false	string []		
	uuid	Agent's universally unique identifier	false	string		
	uuid__contains	Free-text filter by Agent UUID (supports multiple values)	false	string []		
	uuids	A list of included UUIDs	false	string []		

Return result of collection task

GET /web/api/v2.1/remote-ops/forensics/task-result

Return result of collection task

Parameters

taskid	required	Task id. Example: "225494730938493804".

Response Messages

200 - Task is found and result is returned

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
collection	Details of the collection	false	

Name	Description	Required	Value
tag	Tag of the collection	true	string
artifacts	Artifacts included in the collection	false	

Name	Description	Required	Value
artifactType	Type of the artifact	true	string
detailedStatus	Detailed status of the artifact collection	true	string
osType	Target Os	true	string
status	Status of the artifact collection	true	string

									parameters	Parameters passed to the artifact collector	false	object
						description	Description of the collection	false	string			
			collectionFile	Details of the collection file, if exists	false	Name	Description	Required	Value			
						agentId	Agent id	true	string			
						signature	File Signature	true	string			
						siteId	Site id	true	string			
						uploadedTimestamp	Uploaded timestamp	true	string			
						signatureType	Signature type	false	string			
			collectionProfile	Details of the collection profile used for collection	false	Name	Description	Required	Value			
						id	ID of used collection profile	true	string			
						name	Name of used collection profile	true	string			
			destination	Details of the destination	false	Name	Description	Required	Value			
						profileId	ID of destination profile used for collection	false	string			
			skylightParentTaskResultsUrl	Link to Skylight view with results for parent task	false	string						
			skylightResultsStatus	Status of Skylight results	false	Name	Description	Required	Value			
						hasFailures	Indicates if there were	true	boolean			

							failures during uploading data to Skylight		
						isEmpty	Indicates if the collection contains no data store in Skylight	true	boolean
						errorMessage	Last error message if there were failures during upload	false	string
			skylightResultsUrl	Link to Skylight view with results for the single task	false	string			
errors	Errors	false	array						

Returns collection file download pre-signed url

GET /web/api/v2.1/remote-ops/forensics/collection-file-url

Returns collection file download pre-signed url

Parameters

agentid	required	Agent id. Example: "225494730938493804".
signature	required	Signature
signaturetype	required	Signature type
siteid	required	Site id. Example: "225494730938493804".
uploadedtimestamp	required	Uploaded timestamp

Response Messages

200 - Remote Ops Forensics Collection File Found

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
data	Response data	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>downloadUrl</td><td>download link for the file</td><td>false</td><td>string</td></tr><tr><td>fileName</td><td>the name of the file</td><td>false</td><td>string</td></tr></table>
errors	Errors	false	array

Check if collection file exists for given storyline

GET /web/api/v2.1/remote-ops/forensics/is-collection-file

Check if collection file exists for given storyline

Parameters

agentid	required	Agent's ID. Example: "225494730938493804".
storyline	required	Storyline ID

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

404 - Collection file not found

Response Schema

Name	Description	Required	Value
data	Response data	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>agentId</td><td>Agent's ID</td><td>true</td><td>string</td></tr><tr><td>signature</td><td>File's Signature</td><td>true</td><td>string</td></tr><tr><td>siteId</td><td>Site's ID</td><td>true</td><td>string</td></tr><tr><td>signatureType</td><td>Signature type</td><td>false</td><td>string</td></tr><tr><td>uploadedTimestamp</td><td>Collection file uploaded DateTime iso-formatted</td><td>false</td><td>string</td></tr></table>
errors	Errors	false	array

Get list of supported artifact types

GET /web/api/v2.1/remote-ops/forensics/artifact-types

Return a complete list of supported artifact types

Response Messages

200 - Successes

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
artifactType	Artifact type code name, used as identifier of the artifact	true	string
category	Category of the artifact type	true	string
name	User-readable name of the artifact	true	string
osTypes	Os types	false	string []
parameters	Parameters	false	

Name	Description	Required	Value
default	Default value of artifact parameter, null if the parameter does not allow default	true	string
key	Unique key of	true	string

							artifact parameter		
						type	Type of artifact parameter	true	enum
						description	Artifact parameter description	false	string
						example	Example of the parameter value	false	string
			version	Internal version of the artifact type	false	integer			
errors	Errors	false	array						

Get Collection profile by ID

GET /web/api/v2.1/remote-ops/forensics/collection-profiles/{profile_id}

Get contents of an existing Forensics Collection profile, including specification of artifacts to be collected and profile metadata.

Response Messages

200 - Collection profile content in returned

401 - Unauthorized access - please sign in and retry.

403 - User has insufficient permission to perform such action

404 - Collection profile was not found

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
createdAt	Timestamp when the profile was created	true	string
creator	Email of user who created the profile	true	string
description	Collection profile description	true	string
id	Collection profile ID	true	string
isBundled	Flag indicating if the Collection profile is bundled (provided by	true	boolean

				S1)		
			name	name of collection profile in db	true	string
			scopeId	Scope ID where the Collection profile is stored	true	string
			scopeLevel	Scope level where the Collection profile is stored	true	enum
			scopeName	Scope name where the Collection profile is stored	true	string
			scopePath	Full path of Scope where the Collection profile is stored	true	string
			type	Type of RemoteOps Action (forensicsProfile)	true	enum
			updater	Email of user who update the profile	true	string
			version	Collection profile version	true	string
			artifacts	Artifacts	false	

Name	Description	Required	Value
artifactType	Type of artifact to collect	true	string

						osType	OS type where the artifact will be collected	true	enum
						parameters	Input parameters for the artifact	false	object
			osTypes	Os types	false	string []			
			updatedAt	Timestamp when the profile was updated	false	string			
errors	Errors	false	array						

Update Collection profile by ID

PUT /web/api/v2.1/remote-ops/forensics/collection-profiles/{profile_id}

Update contents of an existing Forensics Collection profile. All the profile data should be specified, even if the values are not changed. It's not allowed to change scope of profile. The namemust be unique inside the scope, if different profile with specified name already exists, Bad requesterror is returned and no profile data is changed.

Response Messages

200 - Collection profile is updated

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - User has insufficient permission to perform such action

404 - Collection profile was not found

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
createdAt	Timestamp when the profile was created	true	string
creator	Email of user who created the profile	true	string
description	Collection profile description	true	string
id	Collection profile ID	true	string
isBundled	Flag indicating if the Collection	true	boolean

				profile is bundled (provided by S1)		
			name	name of collection profile in db	true	string
			scopeId	Scope ID where the Collection profile is stored	true	string
			scopeLevel	Scope level where the Collection profile is stored	true	enum
			scopeName	Scope name where the Collection profile is stored	true	string
			scopePath	Full path of Scope where the Collection profile is stored	true	string
			type	Type of RemoteOps Action (forensicsProfile)	true	enum
			updater	Email of user who update the profile	true	string
			version	Collection profile version	true	string
			artifacts	Artifacts	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>artifactType</td><td>Type of</td><td>true</td><td>string</td></tr></table>

							artifact to collect		
						osType	OS type where the artifact will be collected	true	enum
						parameters	Input parameters for the artifact	false	object
			osTypes	Os types	false	string []			
			updatedAt	Timestamp when the profile was updated	false	string			
errors	Errors	false	array						

Body Schema

Name	Description	Required	Value
data	Data	true	

Name	Description	Required	Value
name	Collection profile name	true	string
artifacts	Artifacts	false	
description	Collection profile description	false	string

Name	Description	Required	Value
artifactType	Type of artifact to collect	true	string
osType	OS type where the artifact will be collected	true	enum
parameters	Input parameters for the artifact	false	object

Delete Collection profiles

DELETE /web/api/v2.1/remote-ops/forensics/collection-profiles

Delete multiple Forensics Collection profiles. The profiles that are not possible to delete (e.g. bundled profiles by S1, non-existing or user does not have proper permissions) are skipped. Contents of successfully deleted profiles are returned in response.

Response Messages

200 - Delete was completed or partially completed.

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>createdAt</td><td>Timestamp when the profile was created</td><td>true</td><td>string</td></tr>
<tr><td>creator</td><td>Email of user who created the profile</td><td>true</td><td>string</td></tr>
<tr><td>description</td><td>Collection profile description</td><td>true</td><td>string</td></tr>
<tr><td>id</td><td>Collection profile ID</td><td>true</td><td>string</td></tr>
<tr><td>isBundled</td><td>Flag indicating if the Collection profile is bundled (provided by S1)</td><td>true</td><td>boolean</td></tr>
</table>
</td></tr>
</table>

			name	name of collection profile in db	true	string
			scopeId	Scope ID where the Collection profile is stored	true	string
			scopeLevel	Scope level where the Collection profile is stored	true	enum
			scopeName	Scope name where the Collection profile is stored	true	string
			scopePath	Full path of Scope where the Collection profile is stored	true	string
			type	Type of RemoteOps Action (forensicsProfile)	true	enum
			updater	Email of user who update the profile	true	string
			version	Collection profile version	true	string
			artifacts	Artifacts	false	

Name	Description	Required	Value
artifactType	Type of artifact to collect	true	string
osType	OS type where the	true	enum

							artifact will be collected		
						parameters	Input parameters for the artifact	false	object
			osTypes	Os types	false	string []			
			updatedAt	Timestamp when the profile was updated	false	string			
errors	Errors	false	array						

Body Schema

Name	Description	Required	Value
data	Data	false	
filter	Filter	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr><tr><td>ids</td><td>List of Collection profile IDs to delete</td><td>false</td><td>string []</td></tr><tr><td>siteIds</td><td>List of Site IDs to filter by</td><td>false</td><td>string []</td></tr></table>

Create new Collection profile

POST /web/api/v2.1/remote-ops/forensics/collection-profiles

Create a Forensics Collection profile with provided artifacts on the specified scope. The profile name must be unique inside the scope, if the name already exists, Bad request error is returned.

Response Messages

200 - Collection profile is created

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>createdAt</td><td>Timestamp when the profile was created</td><td>true</td><td>string</td></tr>
<tr><td>creator</td><td>Email of user who created the profile</td><td>true</td><td>string</td></tr>
<tr><td>description</td><td>Collection profile description</td><td>true</td><td>string</td></tr>
<tr><td>id</td><td>Collection profile ID</td><td>true</td><td>string</td></tr>
<tr><td>isBundled</td><td>Flag indicating if the Collection profile is bundled (provided by S1)</td><td>true</td><td>boolean</td></tr>
</table>
</td></tr>
</table>

			name	name of collection profile in db	true	string
			scopeId	Scope ID where the Collection profile is stored	true	string
			scopeLevel	Scope level where the Collection profile is stored	true	enum
			scopeName	Scope name where the Collection profile is stored	true	string
			scopePath	Full path of Scope where the Collection profile is stored	true	string
			type	Type of RemoteOps Action (forensicsProfile)	true	enum
			updater	Email of user who update the profile	true	string
			version	Collection profile version	true	string
			artifacts	Artifacts	false	

Name	Description	Required	Value
artifactType	Type of artifact to collect	true	string
osType	OS type where the	true	enum

							artifact will be collected		
						parameters	Input parameters for the artifact	false	object
			osTypes	Os types	false	string []			
			updatedAt	Timestamp when the profile was updated	false	string			
errors	Errors	false	array						

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>name</td><td>Collection profile name</td><td>true</td><td>string</td></tr>
<tr><td>scopeLevel</td><td>Scope level of the collection profile</td><td>true</td><td>enum</td></tr>
<tr><td>artifacts</td><td>Artifacts</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>artifactType</td><td>Type of artifact to collect</td><td>true</td><td>string</td></tr>
<tr><td>osType</td><td>OS type where the artifact will be collected</td><td>true</td><td>enum</td></tr>
<tr><td>parameters</td><td>Input parameters for the artifact</td><td>false</td><td>object</td></tr>
</table>
</td></tr>
<tr><td>description</td><td>Collection profile description</td><td>false</td><td>string</td></tr>
<tr><td>scopeId</td><td>Scope ID of the collection profile</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
</table>

Get list of available Collection profiles

GET /web/api/v2.1/remote-ops/forensics/collection-profiles

Get list of available Forensics collection profiles. The list may be narrowed by specifying filter parameter. Profiles are inherited between scopes in both upward and downward directions, e.g. profiles on parent Account and Tenant scopes are returned when querying for a Site scope, and profiles on a Site scopes are returned when querying its parent Account. Bundled profiles are available regardless of requested scqpe. If scope is not specified in filter, the scopes of the requesting user are considered.

Parameters

accountids	optional	List of Account IDs to filter by. Example: "225494730938493804,225494730938493915".
countonly	optional	If true, only total number of items will be returned, without any of the actual objects.
cursor	optional	Cursor position returned by the last request. Use to iterate over more than 1000 items. Example: "YWdlbnRfaWQ6NTgwMjkzODE=".
ids	optional	A list of collection profiles IDs. Example: "225494730938493804,225494730938493915".
limit	optional	Limit number of returned items (1-1000). Example: "10".
ostypes	optional	Os types. Example: "linux".
query	optional	Keyword to search in Collection profile name / description
siteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".
skip	optional	Skip first number of items (0-1000). To iterate over more than 1000 items, use "cursor". Example: "150".
skipcount	optional	If true, total number of items will not be calculated, which speeds up execution time.
sortby	optional	The column to sort the results by. Example: "id".
sortorder	optional	Sort direction. Example: "asc".

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>pagination</td><td>Pagination information</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>totalItems</td><td>Total number of items found matching your query</td><td>true</td><td>integer</td></tr>
<tr><td>nextCursor</td><td>Pass this value as "cursor" on your next request, to get the next page of results (Will be "null" when last page reached)</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>createdAt</td><td>Timestamp when the profile was created</td><td>true</td><td>string</td></tr>
<tr><td>creator</td><td>Email of user who created the profile</td><td>true</td><td>string</td></tr>
<tr><td>creatorId</td><td>ID of user who created the profile</td><td>true</td><td>string</td></tr>
<tr><td>description</td><td>Collection profile description</td><td>true</td><td>string</td></tr>
<tr><td>id</td><td>Collection profile ID</td><td>true</td><td>string</td></tr>
<tr><td>isBundled</td><td>Flag</td><td>true</td><td>boolean</td></tr>
</table>
</td></tr>
</table>

				indicating if the Collection profile is bundled (provided by S1)		
			name	name of collection profile in db	true	string
			scopeId	Scope ID where the Collection profile is stored	true	string
			scopeLevel	Scope level where the Collection profile is stored	true	enum
			scopeName	Scope name where the Collection profile is stored	true	string
			scopePath	Full path of Scope where the Collection profile is stored	true	string
			type	Type of RemoteOps Action (forensicsProfile)	true	enum
			updater	Email of user who update the profile	true	string
			updaterId	ID of user who updated the profile	true	string

			version Collection profile version true string osTypes Os types false string [] updatedAt Timestamp when the profile was updated false string
errors	Errors	false	array

RemoteOps Scripts

Run Remote Script

POST /web/api/v2.1/remote-scripts/execute

Run a remote script that was uploaded to the SentinelOne Script Library.

Response Messages

200 - Run remote script request was successful

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
affected	Number of entities affected by the requested operation	false	integer
parentTaskId	The parent task id of the script execution task, null in case of pending execution	false	string
pending	Flag indicating if requested script	false	boolean

				execution requires approval and is created as pending execution		
			pendingExecutionId	ID of created pending execution, present only if pending flag is true	false	string
errors	Errors	false	array			

Body Schema

Name	Description	Required	Value
filter	Applied filter	true	

Name	Description	Required	Value
accountIds	List of Account IDs to filter by	false	string []
activeThreats	Include Agents with this amount of active threats	false	integer
activeThreats__gt	Include Agents with at least this amount of active threats	false	integer
adComputerMember__contains	Free-text filter by Active Directory computer groups string (supports multiple values)	false	string []
adComputerName__contains	Free-text filter by Active Directory computer name string (supports multiple values)	false	string []
adComputerQuery__contains	Free-text filter by Active Directory computer name or its groups	false	string []

				(supports multiple values)			
			adQuery	An Active Directory query string	false	string	
			adQuery__contains	Free-text filter by Active Directory string (supports multiple values)	false	string []	
			adUserMember__contains	Free-text filter by Active Directory user groups string (supports multiple values)	false	string []	
			adUserName__contains	Free-text filter by Active Directory username string (supports multiple values)	false	string []	
			adUserQuery__contains	Free-text filter by Active Directory computer name or its groups (supports multiple values)	false	string []	
			agentNamespa	Free-text	false	string []	

			ce__contains	filter by agent namespace (supports multiple values)			
			agentPodName__contains	Free-text filter by agent pod name (supports multiple values)	false	string []	
			agentVersion__between	Version range for agent version (format: <from_version>-<to_version>, inclusive)	false	string	
			agentVersion__gt	Agents versions greater than given version	false	string	
			agentVersion__gte	Agents versions greater than or equal to given version	false	string	
			agentVersion__lt	Agents versions less than given version	false	string	
			agentVersion__lte	Agents versions less than or equal to given version	false	string	
			agentVersions	Agent versions to include	false	string []	
			agentVersionsNin	Agent versions not	false	string []	

				to include		
			appsVulnerabilityStatuses	Apps vulnerability status in	false	string []
			appsVulnerabilityStatusesNin	Apps vulnerability status nin	false	string []
			awsRole__contains	Free-text filter by aws role(supports multiple values)	false	string []
			awsSecurityGroups__contains	Free-text filter by aws securityGroups(supports multiple values)	false	string []
			awsSubnetIds__contains	Free-text filter by aws subnet ids (supports multiple values)	false	string []
			azureResourceGroup__contains	Free-text filter by azure resource group(supports multiple values)	false	string []
			cloudAccount__contains	Free-text filter by cloud account (supports multiple values)	false	string []
			cloudImage__contains	Free-text filter by cloud image (supports multiple values)	false	string []

			cloudInstanceId__contains	Free-text filter by cloud instance id(supports multiple values)	false	string []	
			cloudInstanceSize__contains	Free-text filter by cloud instance size(supports multiple values)	false	string []	
			cloudLocation__contains	Free-text filter by cloud location (supports multiple values)	false	string []	
			cloudNetwork__contains	Free-text filter by cloud network (supports multiple values)	false	string []	
			cloudProvider	Agents from which cloud provider	false	string []	
			cloudProviderNin	Exclude Agents from these cloud provider	false	string []	
			cloudTags__contains	Free-text filter by cloud tags (supports multiple values)	false	string []	
			clusterName__contains	Free-text filter by cluster name (supports multiple values)	false	string []	

			computerName	Computer name	false	string
			computerName__contains	Free-text filter by computer name (supports multiple values)	false	string []
			computerName__like	Match computer name partially (substring)	false	string
			consoleMigrationStatuses	Migration status in	false	string []
			consoleMigrationStatusesNin	Migration status nin	false	string []
			coreCount__between	Possible number of CPU cores (inclusive)	false	string
			coreCount__gt	CPU cores (more than)	false	integer
			coreCount__gte	CPU cores (more than or equal)	false	integer
			coreCount__lt	CPU cores (less than)	false	integer
			coreCount__lte	CPU cores (less than or equal)	false	integer
			cpuCount__between	Possible number of CPU cores (inclusive)	false	string
			cpuCount__gt	Number of CPUs (more than)	false	integer

			cpuCount__gte	Number of CPUs (more than or equal)	false	integer
			cpuCount__lt	Number of CPUs (less than)	false	integer
			cpuCount__lte	Number of CPUs (less than or equal)	false	integer
			cpuId__contains	Free-text filter by CPU name (supports multiple values)	false	string []
			createdAt__between	Date range for creation time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			createdAt__gt	Agents created after this timestamp	false	string
			createdAt__gte	Agents created after or at this timestamp	false	string
			createdAt__lt	Agents created before this timestamp	false	string
			createdAt__lte	Agents created before or at this timestamp	false	string
			csvFilterId	The ID of the CSV file to filter by	false	string

			decommissionedAt__between	Date range for decommission time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string	
			decommissionedAt__gt	Agents decommissioned after this timestamp	false	string	
			decommissionedAt__gte	Agents decommissioned after or at this timestamp	false	string	
			decommissionedAt__lt	Agents decommissioned before this timestamp	false	string	
			decommissionedAt__lte	Agents decommissioned before this timestamp	false	string	
			domains	Included network domains	false	string []	
			domainsNin	Not included network domains	false	string []	
			encryptedApplications	Disk encryption status	false	boolean	
			externalId__contains	Free-text filter by external ID (Customer ID)	false	string []	
			externalIp__contains	Free-text filter by visible IP (supports	false	string []	

				multiple values)			
			filteredGroupIds	List of Group IDs to filter by	false	string []	
			filteredSiteIds	List of Site IDs to filter by	false	string []	
			filterId	Include all Agents matching this saved filter	false	string	
			firewallEnabled	The agents supports Firewall Control and it is enabled for the agent's group	false	boolean []	
			gatewayIp	Gateway ip	false	string	
			gcpServiceAccount__contains	Free-text filter by gcp service account (supports multiple values)	false	string []	
			groupIds	List of Group IDs to filter by	false	string []	
			hasContainerizedWorkload	Include only Agents protecting containerized workloads	false	boolean	
			hasLocalConfiguration	Agent has a local configuration set	false	boolean	
			hasTags	Include only Agents that	false	boolean	

				have any tags assigned if True, or none if False		
			ids	A list of Agent IDs	false	string []
			infected	Include only Agents with at least one active threat	false	boolean
			installerTypes	Include only Agents installed with these package types	false	string []
			installerTypesNin	Exclude Agents installed with these package types	false	string []
			isActive	Include only active Agents	false	boolean
			isDecommissioned	Include active, decommissioned or both	false	boolean []
			isPendingUninstall	Include only Agents with pending uninstall requests	false	boolean
			isUninstalled	Include installed, uninstalled or both	false	boolean []
			isUpToDate	Include only Agents with updated software	false	boolean

			k8sNodeLabels__contains	Free-text filter by K8s node labels (supports multiple values)	false	string []
			k8sNodeName__contains	Free-text filter by K8s node name (supports multiple values)	false	string []
			k8sType__contains	Free-text filter by K8s type(supports multiple values)	false	string []
			k8sVersion__contains	Free-text filter by K8s version (supports multiple values)	false	string []
			lastActiveDate__between	Date range for last active date(format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			lastActiveDate__gt	Agents last active after this time	false	string
			lastActiveDate__gte	Agents last active after or at this time	false	string
			lastActiveDate__lt	Agents last active before this time	false	string
			lastActiveDate__lte	Agents last active before or at this time	false	string

			lastLoggedInUserName__contains	Free-text filter by username (supports multiple values)	false	string []	
			lastSuccessfulScanDate__between	Date range for last successful full disk scan(format: <from_timestamp>-<to_timestamp>, inclusive)	false	string	
			lastSuccessfulScanDate__gt	Agents last successful full disk scan after this time	false	string	
			lastSuccessfulScanDate__gte	Agents last successful full disk scan after or at this time	false	string	
			lastSuccessfulScanDate__lt	Agents last successful full disk scan before this time	false	string	
			lastSuccessfulScanDate__lte	Agents last successful full disk scan before or at this time	false	string	
			liveUpdateId__contains	Free-text filter by live update ID (supports multiple values)	false	string []	
			locationEnabled	The agents supports	false	boolean []	

				Location Awareness and it is enabled for the agent's group			
			locationIds	Include only Agents reporting these locations	false	string []	
			locationIdsNin	Do not include only Agents reporting these locations	false	string []	
			machineTypes	Included machine types	false	string []	
			machineTypesNin	Not included machine types	false	string []	
			migrationStatus	Migration status	false	enum	
			missingPermissions	Included missing permissions	false	string []	
			missingPermissionsNin	Excluded missing permissions	false	string []	
			mitigationMode	Agent mitigation mode policy	false	enum	
			mitigationModeSuspicious	Mitigation mode policy for suspicious activity	false	enum	
			networkInterfaceGatewayMacAddress__c	Free-text filter by Gateway	false	string []	

			ontains	MAC address (supports multiple values)			
			networkInterfaceInet__contains	Free-text filter by local IP (supports multiple values)	false	string []	
			networkInterfacePhysical__contains	Free-text filter by MAC address (supports multiple values)	false	string []	
			networkQuarantineEnabled	The agents supports Network Quarantine Control and its enabled for the agent's group	false	boolean []	
			networkStatuses	Included network statuses	false	string []	
			networkStatusesNin	Included network statuses	false	string []	
			operationalStates	Agent operational state	false	string []	
			operationalStatesNin	Do not include these Agent operational states	false	string []	
			osArch	OS architecture	false	enum	
			osTypes	Included OS types	false	string []	

	osTypesNin	Not included OS types	false	string []		
	osVersion__contains	Free-text filter by OS full name and version (supports multiple values)	false	string []		
	query	A free-text search term, will match applicable attributes (sub-string match). Note: Device's physical addresses will be matched if they start with the search term only (no match if they contain the term).	false	string		
	rangerStatus	[DEPRECATED] Use rangerStatuses.	false	enum		
	rangerStatuses	Status of Ranger	false	string []		
	rangerStatusesNin	Do not include these Ranger Statuses	false	string []		
	rangerVersions	Ranger versions to include	false	string []		
	rangerVersionsNin	Ranger versions not to include	false	string []		

			registeredAt__between	Date range for first registration time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string	
			registeredAt__gt	Agents registered after this time	false	string	
			registeredAt__gte	Agents registered after or at this time	false	string	
			registeredAt__lt	Agents registered before this time	false	string	
			registeredAt__lte	Agents registered before or at this time	false	string	
			remoteOpsForensicsSupported	Include only agents that has Remote Ops Forensicsfeature supported	false	boolean	
			remoteProfilingStates	Agent remote profiling state	false	string []	
			remoteProfilingStatesNin	Do not include these Agent remote profiling states	false	string []	
			rsoLevel	Supported Remote Script Orchestration	false	enum	

				level			
			scanStatus	Scan status	false	enum	
			scanStatuses	Included scan statuses	false	string []	
			scanStatuses Nin	Not included scan statuses	false	string []	
			serialNumber __contains	Free-text filter by Serial Number (supports multiple values)	false	string []	
			siteIds	List of Site IDs to filter by	false	string []	
			tagsData	Filter agents by their assigned tags. Given in form of a JSON where each key represents a tag key, and each value represents a list of string values to filter by. To filter by unassigned tag values, use __nin suffix in the tag key.	false	string	
			tenant	Indicates a tenant scope request	false	boolean	
			threatConten tHash	Include only Agents that have at least one threat	false	string	

				with this content hash			
			threatCreatedAt__between	Agents with threats reported in a date range (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string	
			threatCreatedAt__gt	Agents with threats reported after this time	false	string	
			threatCreatedAt__gte	Agents with threats reported after or at this time	false	string	
			threatCreatedAt__lt	Agents with threats reported before this time	false	string	
			threatCreatedAt__lte	Agents with threats reported before or at this time	false	string	
			threatHidden	Include only Agents with at least one hidden threat	false	boolean	
			threatMitigationStatus	Include only Agents that have threats with this mitigation status	false	enum	
			threatReboot	Has at least	false	boolean []	

			Required	one threat with at least one mitigation action pending reboot to succeed			
			threatResolved	Include only Agents with at least one resolved threat	false	boolean	
			totalMemory__between	Total memory range (GB, inclusive)	false	string	
			totalMemory__gt	Memory size (MB, more than)	false	integer	
			totalMemory__gte	Memory size (MB, more than or equal)	false	integer	
			totalMemory__lt	Memory size (MB, less than)	false	integer	
			totalMemory__lte	Memory size (MB, less than or equal)	false	integer	
			updatedAt__between	Date range for update time (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string	
			updatedAt__gt	Agents updated after this timestamp	false	string	
			updatedAt__gte	Agents updated after or at this	false	string	

			timestamp		
	updatedAt__lt	Agents updated before this timestamp	false	string
	updatedAt__lte	Agents updated before or at this timestamp	false	string
	userActionsNeeded	Included pending user actions	false	string []
	userActionsNeededNin	Excluded pending user actions	false	string []
	uuid	Agent's universally unique identifier	false	string
	uuid__contains	Free-text filter by Agent UUID (supports multiple values)	false	string []
	uuids	A list of included UUIDs	false	string []

data	Data	false	Name	Description	Required	Value
			outputDestination	Output destination	true	enum
			scriptId	Script id	true	string
			taskDescription	Task description	true	string
			apiKey	Api key	false	string

			destinationProfileId	Id of destination profile to use	false	string
			destinationProfileKeyword	Destination profile keyword	false	string
			inputParams	Input params	false	string
			outputDirectory	Output directory	false	string
			outputFilePaths	Output file paths	false	string []
			password	Password	false	string
			passwordFromScope	Used to specify execution where a generic password is used	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>scopeLevel</td><td>User scope</td><td>true</td><td>enum</td></tr><tr><td>scopeId</td><td>string repr. of scope id</td><td>false</td><td>string</td></tr></table>
			requiresApproval	If set to true, execution will require approval	false	boolean
			scriptRuntimeTimeoutSeconds	Script runtime timout in seconds for current execution	false	integer
			singularityxdrKeyword	Singularityxdr keyword	false	string
			singularityxdrUrl	Singularityxdr url	false	string

Get Remote Scripts Tasks Status

GET /web/api/v2.1/remote-scripts/status

Get remote scripts tasks using a variety of filters. Accessible via API only
parent_task_id or parent_task_id__in query parameter is mandatory

Parameters

accountids	optional	List of Account IDs to filter by. Example: "225494730938493804,225494730938493915".
computername__contains	optional	Free-text filter by agent computer name (supports multiple values)
countonly	optional	If true, only total number of items will be returned, without any of the actual objects.
createdat__gt	optional	Created at greater than. Example: "2018-02-27T04:49:26.257525Z".
createdat__gte	optional	Created at greater or equal than. Example: "2018-02-27T04:49:26.257525Z".
createdat__lt	optional	Created at lesser than. Example: "2018-02-27T04:49:26.257525Z".
createdat__lte	optional	Created at lesser or equal than. Example: "2018-02-27T04:49:26.257525Z".
cursor	optional	Cursor position returned by the last request. Use to iterate over more than 1000 items. Example: "YWdlbnRfaWQ6NTgwMjkzODE=".
description__contains	optional	Only include tasks with specific description
detailedstatus__contains	optional	Only include tasks with specific detailed status
groupids	optional	List of Group IDs to filter by. Example: "225494730938493804,225494730938493915".
ids	optional	List of IDs to filter by. Example: "225494730938493804,225494730938493915".
initiatedby__contains	optional	Only include tasks from specific initiating user
limit	optional	Limit number of returned items (1-1000). Example: "10".
parenttaskid	optional	parent task id to fetch the status by. Example:

		"225494730938493804".
parenttaskid__in	optional	List of IDs to filter by
query	optional	Query
siteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".
skip	optional	Skip first number of items (0-1000). To iterate over more than 1000 items, use "cursor". Example: "150".
skipcount	optional	If true, total number of items will not be calculated, which speeds up execution time.
sortby	optional	The column to sort the results by. Example: "id".
sortorder	optional	Sort direction. Example: "asc".
status	optional	Status in. Example: "created".
tenant	optional	Indicates a tenant scope request
type	optional	Type
types	optional	Type in
updatedat__gt	optional	Updated at greater than. Example: "2018-02-27T04:49:26.257525Z".
updatedat__gte	optional	Updated at greater or equal than. Example: "2018-02-27T04:49:26.257525Z".
updatedat__lt	optional	Updated at lesser than. Example: "2018-02-27T04:49:26.257525Z".
updatedat__lte	optional	Updated at lesser or equal than. Example: "2018-02-27T04:49:26.257525Z".
uuid__contains	optional	Free-text filter by agent UUID (supports multiple values)

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value

pagination	Pagination information	true	

Name	Description	Required	Value
totalItems	Total number of items found matching your query	true	integer
nextCursor	Pass this value as "cursor" on your next request, to get the next page of results (Will be "null" when last page reached)	false	string

data	Response data	false	

Name	Description	Required	Value
accountId	Account id	false	string
accountName	Account name	false	string
agentComputerName	Agent computer name	false	string
agentId	Agent id	false	string
agentIsActive	Agent is active	false	boolean
agentIsDecommissioned	Agent is decommissioned	false	boolean
agentMachineType	Agent machine type	false	string
agentOsType	OS type	false	enum
agentUuid	Agent uuid	false	string
createdAt	Timestamp of date creation	false	string
description	Description	false	string

			detailedStatus | Detailed status | false | string groupId | Group id | false | string groupName | Group name | false | string id | Task id | false | string initiatedBy | Initiated by | false | string initiatedById | Initiated by id | false | string parentTaskId | Parent task id | false | string scriptResultsBucket | Script results bucket | false | string scriptResultsPath | Script results path | false | string scriptResultsSignature | Script results signature | false | string siteId | Site id | false | string siteName | Site name | false | string status | Status | false | enum statusCode | Status code | false | integer statusDescription | Status description | false | type | Type | false | string updatedAt | Timestamp of last update | false | string
errors	Errors	false	array

Get Script Results

POST /web/api/v2.1/remote-scripts/fetch-files

Get scripts results URLs. Accessible via API only

Response Messages

200 - Get remote script results was successful

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
data	Data	false	

Name	Description	Required	Value
downloadLinks	List of download links	false	

Name	Description	Required	Value
downloadUrl	download link for the file	false	string
fileName	the name of the file	false	string
taskId	the task id related to the download link	false	string

Name	Description	Required	Value
errors	Task id's and detailed errors for tasks which a download link couldn't be fetched	false	array

Name	Description	Required	Value
errors	Errors	false	array

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>computerNames</td><td>A list of partial or whole computer names, which ran scripts, to get a download link for</td><td>false</td><td>string []</td></tr>
<tr><td>taskIds</td><td>A list of task ids to get a download link for</td><td>false</td><td>string []</td></tr>
</table>
</td></tr>
</table>

Get script content

GET /web/api/v2.1/remote-scripts/script-content

Get Script content by script id

Parameters

scriptid	optional	Script ID. Example: "225494730938493804".

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

404 - Script not found

Response Schema

Name	Description	Required	Value
data	Response data	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>scriptContent</td><td>Script content</td><td>true</td><td>string</td></tr></table>
errors	Errors	false	array

Get Scripts

GET /web/api/v2.1/remote-scripts

Get data of the scripts in the SentinelOne Script Library.
The SentinelOne Script Library, used for the Remote Script Orchestration feature, gives you a wide range of scripts to collect various forensic artifacts, parse them, and show them in formats that are easy to analyze. Use the scripts to collect information such as hardware and software inventory and configuration, running applications and processes, files and directories, network connections, and more.

Parameters

accountids	optional	List of Account IDs to filter by. Example: "225494730938493804,225494730938493915".
countonly	optional	If true, only total number of items will be returned, without any of the actual objects.
cursor	optional	Cursor position returned by the last request. Use to iterate over more than 1000 items. Example: "YWdlbnRfaWQ6NTgwMjkzODE=".
groupids	optional	List of group IDs to filter by. Example: "225494730938493804,225494730938493915".
ids	optional	A list of script IDs. Example: "225494730938493804,225494730938493915".
isavailableforars	optional	Is the script runnable in Advanced Response Scripts
limit	optional	Limit number of returned items (1-1000). Example: "10".
ostypes	optional	List of the script OS types. Example: "linux".
query	optional	Query
scripttype	optional	List of the script types. Example: "artifactCollection".
siteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".
skip	optional	Skip first number of items (0-1000). To iterate over more than 1000 items, use "cursor". Example: "150".
skipcount	optional	If true, total number of items will not be calculated, which speeds up execution time.
sortby	optional	The column to sort the results by. Example: "id".
sortorder	optional	Sort direction. Example: "asc".

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>pagination</td><td>Pagination information</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>totalItems</td><td>Total number of items found matching your query</td><td>true</td><td>integer</td></tr>
<tr><td>nextCursor</td><td>Pass this value as "cursor" on your next request, to get the next page of results (Will be "null" when last page reached)</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>createdByUserId</td><td>Created by user id</td><td>true</td><td>string</td></tr>
<tr><td>inputExample</td><td>Input example</td><td>true</td><td>string</td></tr>
<tr><td>inputInstructions</td><td>Input instructions</td><td>true</td><td>string</td></tr>
<tr><td>inputRequired</td><td>Is input required</td><td>true</td><td>boolean</td></tr>
<tr><td>scriptName</td><td>Script name</td><td>true</td><td>string</td></tr>
<tr><td>scriptType</td><td>Script type</td><td>true</td><td>string</td></tr>
</table>
</td></tr>
</table>

			version	Version	true	string
			bucketName	Bucket name	false	string
			createdAt	Created at	false	string
			createdByUser	Created by user	false	string
			creator	Name of the creating user	false	string
			creatorId	Id of the creating user	false	string
			fileName	File name with full path	false	string
			fileSize	File size	false	integer
			id	Script ID	false	string
			isAvailableForArs	Is the script runnable in Advanced Response Scripts	false	boolean
			isAvailableForLite	Is the script runnable in Lite version	false	boolean
			mgmtId	Mgmt id	false	integer
			osTypes	OS types	false	string []
			outputFilePaths	Output file paths	false	string []
			package	Package	false	

Name	Description	Required	Value
bucketName	Bucket name	false	string
endpointExpiration	Package expiration option on endpoint	false	string
endpointExpirationSeconds	Package expiration time on endpoint	false	integer
fileName	File name with full path	false	string

						fileSize | File size | false | integer id | Package ID | false | string signature | Signature | false | string signatureType | Signature type | false | string
			scopeId	Scope ID	false	string
			scopeLevel	Scope level	false	enum
			scopeName	The scripts scope name	false	string
			scopePath	The path of the scripts scope	false	string
			scriptDescription	Script description	false	string
			scriptRuntimeTimeoutSeconds	Script runtime timeout in seconds	false	integer
			shortFileName	File name	false	string
			signature	Signature	false	string
			signatureType	Signature type	false	string
			supportedDestinations	Supported destinations	false	string []
			updatedAt	Updated at	false	string
			updater	Name of the updating user	false	string
			updaterId	Id of the updating user	false	string
errors	Errors	false	array			

Upload New Script

POST /web/api/v2.1/remote-scripts

Upload a new script file. The file and various properties are required. To see the mandatory and optional parameters and their valid values, see the Body Schema or click Run On Console.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
createdByUserId	Created by user id	true	string
inputExample	Input example	true	string
inputInstructions	Input instructions	true	string
inputRequired	Is input required	true	boolean
scriptName	Script name	true	string
scriptType	Script type	true	string
version	Version	true	string
bucketName	Bucket name	false	string
createdAt	Created at	false	string
createdByUser	Created by user	false	string
creator	Name of the creating user	false	string

			creatorId	Id of the creating user	false	string
			fileName	File name with full path	false	string
			fileSize	File size	false	integer
			id	Script ID	false	string
			isAvailableForArs	Is the script runnable in Advanced Response Scripts	false	boolean
			isAvailableForLite	Is the script runnable in Lite version	false	boolean
			mgmtId	Mgmt id	false	integer
			osTypes	OS types	false	string []
			outputFilePaths	Output file paths	false	string []
			package	Package	false	

Name	Description	Required	Value
bucketName	Bucket name	false	string
endpointExpiration	Package expiration option on endpoint	false	string
endpointExpirationSeconds	Package expiration time on endpoint	false	integer
fileName	File name with full path	false	string
fileSize	File size	false	integer
id	Package ID	false	string
signature	Signature	false	string
signatureType	Signature type	false	string

			scopeId	Scope ID	false	string
			scopeLevel	Scope level	false	enum

			scopeName: The scripts scope name; false; string scopePath: The path of the scripts scope; false; string scriptDescription: Script description; false; string scriptRuntimeTimeoutSeconds: Script runtime timeout in seconds; false; integer shortFileName: File name; false; string signature: Signature; false; string signatureType: Signature type; false; string supportedDestinations: Supported destinations; false; string [] updatedAt: Updated at; false; string updater: Name of the updating user; false; string updaterId: Id of the updating user; false; string
errors	Errors	false	array

Body Schema

Name	Description	Required	Value
formData		false	

Name	Description	Required	Value
inputRequired	Is input required	true	boolean
scopeLevel	Scope level. Example: "site".	true	enum
scriptName	Script name	true	string
scriptType	Script type. Example: "artifactCollection".	true	enum
consoleData	Console data	false	string
file	File	false	file
inputExample	Input example	false	string
inputInstructions	Input instructions	false	string
isDuplication	True if script/package files should be taken from an existing script specified in original_script_id	false	boolean
isScriptContentEncoded	True if script content is encoded	false	boolean
originalScriptId	ID of script, from which the script/package files will becopied, applicable ony if is_duplication is true.	false	string

				Example: "225494730938493804".		
			osTypes	Os types. Example: "m,a,c,o,s,,,l,i,n,u,x".	false	string []
			packageEndpointExpiration	Package expiration option on endpoint. Example: "None".	false	enum
			packageEndpointExpirationSeconds	Package expiration time on endpoint	false	integer
			packageFile	Package file	false	file
			packageMaxSize	Package max size	false	string
			packageRemoved	True if package should file should not be copied, applicable only if is_duplication is true	false	boolean
			scopeId	Scope ID. Example: "225494730938493804".	false	string
			scriptContent	Content of the script file, applicable only if is_duplication is true	false	string
			scriptDescription	Script description	false	string

			scriptRuntimeTimeoutSeconds	Script runtime timeout in seconds	false	integer
			sendActivity	Send activity	false	boolean

Delete Scripts

DELETE /web/api/v2.1/remote-scripts

Deletes scripts that match a filter.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>pagination</td><td>Pagination information</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>totalItems</td><td>Total number of items found matching your query</td><td>true</td><td>integer</td></tr>
<tr><td>nextCursor</td><td>Pass this value as "cursor" on your next request, to get the next page of results (Will be "null" when last page reached)</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>createdByUserId</td><td>Created by user id</td><td>true</td><td>string</td></tr>
</table>
</td></tr>
</table>

			inputExample	Input example	true	string
			inputInstructions	Input instructions	true	string
			inputRequired	Is input required	true	boolean
			scriptName	Script name	true	string
			scriptType	Script type	true	string
			version	Version	true	string
			bucketName	Bucket name	false	string
			createdAt	Created at	false	string
			createdByUser	Created by user	false	string
			creator	Name of the creating user	false	string
			creatorId	Id of the creating user	false	string
			fileName	File name with full path	false	string
			fileSize	File size	false	integer
			id	Script ID	false	string
			isAvailableForArs	Is the script runnable in Advanced Response Scripts	false	boolean
			isAvailableForLite	Is the script runnable in Lite version	false	boolean
			mgmtId	Mgmt id	false	integer
			osTypes	OS types	false	string []
			outputFilePaths	Output file paths	false	string []
			package	Package	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>bucketName</td><td>Bucket name</td><td>false</td><td>string</td></tr><tr><td>endpointExpir</td><td>Package</td><td>false</td><td>string</td></tr></table>

			updaterId | Id of the updating user | false | string
errors	Errors	false	array

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>filter</td><td>Filter</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>groupIds</td><td>List of group IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>ids</td><td>A list of Scripts IDs</td><td>false</td><td>string []</td></tr>
<tr><td>osTypes</td><td>List of the script OS types.</td><td>false</td><td>string []</td></tr>
<tr><td>query</td><td>Query</td><td>false</td><td>string</td></tr>
<tr><td>scriptType</td><td>List of the script types</td><td>false</td><td>string []</td></tr>
<tr><td>siteIds</td><td>List of Site IDs to filter by</td><td>false</td><td>string []</td></tr>
</table>
</td></tr>
<tr><td>consoleData</td><td>Console data</td><td>false</td><td>string</td></tr>
<tr><td>sendActivity</td><td>Send activity</td><td>false</td><td>boolean</td></tr>
</table>

Update a Script

PUT /web/api/v2.1/remote-scripts/edit/{script_id}

Change the properties of a given script: runtime timeout, name, and whether input is required (if true, input example and instructions are requried),or script content itselt. This command requires the script ID, which you can get from the Get Scripts API.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

404 - Script not found

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
createdByUserId	Created by user id	true	string
inputExample	Input example	true	string
inputInstructions	Input instructions	true	string
inputRequired	Is input required	true	boolean
scriptName	Script name	true	string
scriptType	Script type	true	string
version	Version	true	string
bucketName	Bucket name	false	string
createdAt	Created at	false	string
createdByUser	Created by user	false	string

			creator	Name of the creating user	false	string
			creatorId	Id of the creating user	false	string
			fileName	File name with full path	false	string
			fileSize	File size	false	integer
			id	Script ID	false	string
			isAvailableForArs	Is the script runnable in Advanced Response Scripts	false	boolean
			isAvailableForLite	Is the script runnable in Lite version	false	boolean
			mgmtId	Mgmt id	false	integer
			osTypes	OS types	false	string []
			outputFilePaths	Output file paths	false	string []
			package	Package	false	

Name	Description	Required	Value
bucketName	Bucket name	false	string
endpointExpiration	Package expiration option on endpoint	false	string
endpointExpirationSeconds	Package expiration time on endpoint	false	integer
fileName	File name with full path	false	string
fileSize	File size	false	integer
id	Package ID	false	string
signature	Signature	false	string
signatureType	Signature type	false	string

			scopeId | Scope ID | false | string scopeLevel | Scope level | false | enum scopeName | The scripts scope name | false | string scopePath | The path of the scripts scope | false | string scriptDescription | Script description | false | string scriptRuntimeTimeoutSeconds | Script runtime timeout in seconds | false | integer shortFileName | File name | false | string signature | Signature | false | string signatureType | Signature type | false | string supportedDestinations | Supported destinations | false | string [] updatedAt | Updated at | false | string updater | Name of the updating user | false | string updaterId | Id of the updating user | false | string
errors	Errors	false	array

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>formData</td><td></td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>inputExample</td><td>Input example</td><td>true</td><td>string</td></tr>
<tr><td>inputInstructions</td><td>Input instructions</td><td>true</td><td>string</td></tr>
<tr><td>inputRequired</td><td>Is input required</td><td>true</td><td>boolean</td></tr>
<tr><td>scriptName</td><td>Script name</td><td>true</td><td>string</td></tr>
<tr><td>scriptRuntimeTimeoutSeconds</td><td>Script runtime timeout in seconds</td><td>true</td><td>integer</td></tr>
<tr><td>scriptType</td><td>Script type. Example: "artifactCollection".</td><td>true</td><td>enum</td></tr>
<tr><td>consoleData</td><td>Console data</td><td>false</td><td>string</td></tr>
<tr><td>isScriptContentEncoded</td><td>Is the script content base64 encoded?</td><td>false</td><td>boolean</td></tr>
<tr><td>osTypes</td><td>Os types. Example: "m,a,c,o,s,,,l,i,n,u,x".</td><td>false</td><td>string []</td></tr>
<tr><td>packageEndpointExpiration</td><td>Package expiration option on endpoint. Example: "None".</td><td>false</td><td>enum</td></tr>
<tr><td>packageEndpointExpirationSeconds</td><td>Package expiration time on endpoint</td><td>false</td><td>integer</td></tr>
<tr><td>packageFile</td><td>Package file</td><td>false</td><td>file</td></tr>
</table>
</td></tr>
</table>

			packageMaxSize	Package max size	false	string
			packageRemoved	Was package removed during edit of the script?	false	boolean
			scriptContent	Filled out with a new content of a script if the script content was changedon an already previously uploaded script	false	string
			scriptDescription	Script description	false	string
			scriptFile	Script file	false	file
			sendActivity	Send activity	false	boolean

Get paginated pending executions

GET /web/api/v2.1/remote-scripts/pending-executions

Get paginated pending executions

Parameters

accountids	optional	List of Account IDs to filter by. Example: "225494730938493804,225494730938493915".
countonly	optional	If true, only total number of items will be returned, without any of the actual objects.
cursor	optional	Cursor position returned by the last request. Use to iterate over more than 1000 items. Example: "YWdlbnRfaWQ6NTgwMjkzODE=".
groupids	optional	List of group IDs to filter by. Example: "225494730938493804,225494730938493915".
limit	optional	Limit number of returned items (1-1000). Example: "10".
siteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".
skip	optional	Skip first number of items (0-1000). To iterate over more than 1000 items, use "cursor". Example: "150".
skipcount	optional	If true, total number of items will not be calculated, which speeds up execution time.
sortby	optional	The column to sort the results by. Example: "id".
sortorder	optional	Sort direction. Example: "asc".

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
pagination	Pagination information	true	

Name	Description	Required	Value
totalItems	Total number of items found matching your query	true	integer
nextCursor	Pass this value as "cursor" on your next request, to get the next page of results (Will be "null" when last page reached)	false	string

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
canApproveOrDecline	Can approve or decline	true	boolean
creator	Creator	true	string
creatorId	Creator id	true	string
executionData	Execution data	true	

Name	Description	Required	Value
outputDestination	Output destination	true	enum
scriptId	Script id	true	string
taskDescription	Task description	true	string
apiKey	Api key	false	string
destinationProfileId	Id of destination profile to use	false	string
destinationProfileKeyword	Destination profile keyword	false	string
inputParams	Input params	false	string

						outputDirectory	Output directory	false	string
						outputFilePaths	Output file paths	false	string []
						password	Password	false	string
						passwordFromScope	Used to specify execution where a generic password is used	false	Name / Description / Required / Value scopeLevel / User scope / true / enum scopeId / string repr. of scope id / false / string
						requiresApproval	If set to true, execution will require approval	false	boolean
						scriptRuntimeTimeoutSeconds	Script runtime timout in seconds for current execution	false	integer
						singularityxdrKeyword	Singularityxdr keyword	false	string
						singularityxdrUrl	Singularityxdr url	false	string
				pendingExecutionId	Pending execution id	true	string		
				reviewer	Reviewer	true	string		
				reviewerId	Reviewer id	true	string		
				scriptData	Script data	true	Name / Description / Required / Value createdByUserId / Created by user id / true / string inputExample / Input example / true / string inputInstructions / Input instructions / true / string inputRequire / Is input / true / boolean		

						d	required		
						scriptName	Script name	true	string
						scriptType	Script type	true	string
						version	Version	true	string
						bucketName	Bucket name	false	string
						createdAt	Created at	false	string
						createdByUser	Created by user	false	string
						creator	Name of the creating user	false	string
						creatorId	Id of the creating user	false	string
						fileName	File name with full path	false	string
						fileSize	File size	false	integer
						id	Script ID	false	string
						isAvailableForArs	Is the script runnable in Advanced Response Scripts	false	boolean
						isAvailableForLite	Is the script runnable in Lite version	false	boolean
						mgmtId	Mgmt id	false	integer
						osTypes	OS types	false	string []
						outputFilePaths	Output file paths	false	string []
						package	Package	false	

Name	Description	Required	Value
bucketName	Bucket name	false	string
endpointExpiration	Package expiration option on endpoint	false	string
endpointExpi	Package	false	integer

									rationSeconds	expiration time on endpoint		
									fileName	File name with full path	false	string
									fileSize	File size	false	integer
									id	Package ID	false	string
									signature	Signature	false	string
									signatureType	Signature type	false	string
						scopeId	Scope ID	false	string			
						scopeLevel	Scope level	false	enum			
						scopeName	The scripts scope name	false	string			
						scopePath	The path of the scripts scope	false	string			
						scriptDescription	Script description	false	string			
						scriptRuntimeTimeoutSeconds	Script runtime timeout in seconds	false	integer			
						shortFileName	File name	false	string			
						signature	Signature	false	string			
						signatureType	Signature type	false	string			
						supportedDestinations	Supported destinations	false	string []			
						updatedAt	Updated at	false	string			
						updater	Name of the updating user	false	string			
						updaterId	Id of the updating user	false	string			

<table>
<tr><td></td><td></td><td></td><td>
<table>
<tr><td>state</td><td>State</td><td>true</td><td>enum</td></tr>
<tr><td>totalEndpoints</td><td>Total endpoints</td><td>true</td><td>integer</td></tr>
<tr><td>createdAt</td><td>Created at</td><td>false</td><td>string</td></tr>
<tr><td>endpointsBy Scope</td><td>Endpoints by scope</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>scopeName</td><td></td><td>true</td><td>string</td></tr>
<tr><td>totalEndpoints</td><td></td><td>true</td><td>integer</td></tr>
</table>
</td></tr>
<tr><td>scheduledTaskId</td><td>Scheduled task id</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Approve/decline pending execution

PUT /web/api/v2.1/remote-scripts/pending-executions/{pending_execution_id}

Approve/decline pending execution

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

404 - Pending execution not found

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td><table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>success</td><td>Operation result</td><td>false</td><td>boolean</td></tr></table></td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

Name	Description	Required	Value
data	Data	true	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>action</td><td>Action</td><td>true</td><td>enum</td></tr></table>

Gets a guardrails configuration for a given scope

GET /web/api/v2.1/remote-scripts/guardrails/configuration

Gets a guardrails configuration for a given scope

Parameters

scopeid	required	Scope ID. Example: "225494730938493804".
scopelevel	required	Scope level. Example: "account".

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
data	Response data	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>enabled</td><td>Whether guardrail is active</td><td>true</td><td>boolean</td></tr><tr><td>endpointsQuantity</td><td>Threshold for number of endpoints</td><td>true</td><td>integer</td></tr><tr><td>inherited</td><td>Whether guardrail is inherited</td><td>true</td><td>boolean</td></tr><tr><td>scriptTypes</td><td>List of script types that the guardrail relates to</td><td>false</td><td>string []</td></tr></table>
errors	Errors	false	array

Updates or inserts (if record does not exist) a guardrails configuration

POST /web/api/v2.1/remote-scripts/guardrails/configuration

Updates or inserts (if record does not exist) a guardrails configuration

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td><table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>success</td><td>Operation result</td><td>false</td><td>boolean</td></tr></table></td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

Name	Description	Required	Value
data	Data	true	

Name	Description	Required	Value
enabled	Whether guardrail is active	true	boolean
endpointsQuantity	Threshold for number of endpoints	true	integer
scopeId	Scope ID	true	string
scopeLevel	Scope level	true	enum
scriptTypes	List of script types that the guardrail relates to	false	string []

Deletes a specific guardrails configuration

DELETE /web/api/v2.1/remote-scripts/guardrails/configuration

Deletes a specific guardrails configuration

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td><table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>success</td><td>Operation result</td><td>false</td><td>boolean</td></tr></table></td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>scopeId</td><td>Scope ID</td><td>true</td><td>string</td></tr>
<tr><td>scopeLevel</td><td>Scope level</td><td>true</td><td>enum</td></tr>
</table>
</td></tr>
</table>

Check whether guardrail applies to an execution

POST /web/api/v2.1/remote-scripts/guardrails/check

Check whether guardrail applies to an execution

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>requiresApproval</td><td>Whether the guardrail check requires approval</td><td>false</td><td>boolean</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>scriptId</td><td>Script id</td><td>true</td><td>string</td></tr>
<tr><td>agentIds</td><td>Agent ids</td><td>false</td><td>string []</td></tr>
</table>
</td></tr>
</table>

Rogues

Get Rogues Table

GET /web/api/v2.1/rogues/table-view

Get the data for each row in the Rogues Device Inventory Table.
Best practice: Set filters. Each row is a set of parameters that quickly fills the pagination limits.

BEST PRACTICE

Set filters. Each row is a set of parameters that quickly fills the pagination limits.

Parameters

accountids	optional	List of Account IDs to filter by. Example: "225494730938493804,225494730938493915".
countonly	optional	If true, only total number of items will be returned, without any of the actual objects.
cursor	optional	Cursor position returned by the last request. Use to iterate over more than 1000 items. Example: "YWdlbnRfaWQ6NTgwMjkzODE=".
devicetype	optional	Device type. Example: "Server/Workstation/...".
devicetypes	optional	Device types
externalip	optional	Search using external IP
externalip__contains	optional	Free-text filter by visible IP (supports multiple values). Example: "192.168.0.1/24,10.1".
firstseen__between	optional	Date range refor first seen(format: <from_timestamp>-<to_timestamp>, inclusive). Example: "1514978890136-1514978650130".
firstseen__gt	optional	Devices first seen after this timestamp. Example: "2018-02-27T04:49:26.257525Z".
firstseen__gte	optional	Devices first seen after or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".

firstseen__lt	optional	Devices first seen before this timestamp. Example: "2018-02-27T04:49:26.257525Z".
firstseen__lte	optional	Devices first seen before or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
groupids	optional	List of Group IDs to filter by. Example: "225494730938493804,225494730938493915".
hostnames	optional	Hostnames
hostnames__contains	optional	Free-text filter by hostanem (supports multiple values). Example: "s1_host,SomeHost".
ids	optional	List of device ids. Example: "225494730938493804,225494730938493915".
lastseen__between	optional	Date range for last seen(format: <from_timestamp>-<to_timestamp>, inclusive). Example: "1514978890136-1514978650130".
lastseen__gt	optional	Devices last seen after this timestamp. Example: "2018-02-27T04:49:26.257525Z".
lastseen__gte	optional	Devices last seen after or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
lastseen__lt	optional	Devices last seen before this timestamp. Example: "2018-02-27T04:49:26.257525Z".
lastseen__lte	optional	Devices last seen before or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
limit	optional	Limit number of returned items (1-1000). Example: "10".
localip	optional	Search using local IP
localip__contains	optional	Free-text filter by IP Address (supports multiple values). Example: "192.168.0.1/24,10.1".
macaddress	optional	A mac address to search for
macaddress__contains	optional	Free-text filter by mac address (supports multiple values). Example: "aa:ee:b1".
manufacturer	optional	Manufacturer of the device or network interface
manufacturer__contains	optional	Free-text filter by manufacturer (supports multiple values). Example: "Company".
osname	optional	Os name
ostype	optional	OS type

ostypes	optional	Included OS types
osversion	optional	Os version
osversion__contains	optional	Free-text filter by OS full name and version (supports multiple values). Example: "Service Pack 1".
query	optional	Query
siteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".
skip	optional	Skip first number of items (0-1000). To iterate over more than 1000 items, use "cursor". Example: "150".
skipcount	optional	If true, total number of items will not be calculated, which speeds up execution time.
sortby	optional	The column to sort the results by. Example: "id".
sortorder	optional	Sort direction. Example: "asc".
tenant	optional	Indicates a tenant scope request

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - Insufficient permissions

Response Schema

Name	Description	Required	Value
pagination	Pagination information	true	

Name	Description	Required	Value
totalItems	Total number of items found matching your query	true	integer
nextCursor	Pass this value as "cursor" on	false	string

			your next request, to get the next page of results (Will be "null" when last page reached)		
data	Response data	false	

Name	Description	Required	Value
deviceFunction	Function of the device	false	string
deviceType	Role of the device	false	string
externalIp	Main Gateway Visible IP	false	string
firstSeen	Time the device was first seen	false	string
hostnames	Array of host names	false	string []
id	Id of the device	false	string
lastSeen	Time the device was last seen	false	string
localIp	Local ip of the device	false	string
macAddress	Mac address of the device	false	string
manufacturer	Manufacturer of the device or network interface	false	string
osName	OS Name/ Version of the device	false	string
osType	Os Type of	false	string

			the device		
			osVersion	OS Version of the device	false	string
errors	Errors	false	array

Export Rogues Data

GET /web/api/v2.1/rogues/report/csv

Export Rogues data to CSV. You can set filters to get only relevant data. The response sends the CSV data as text.

Parameters

accountids	optional	List of Account IDs to filter by. Example: "225494730938493804,225494730938493915".
devicetype	optional	Device type. Example: "Server/Workstation/...".
devicetypes	optional	Device types
externalip	optional	Search using external IP
externalip__contains	optional	Free-text filter by visible IP (supports multiple values). Example: "192.168.0.1/24,10.1".
firstseen__between	optional	Date range refor first seen(format: <from_timestamp>-<to_timestamp>, inclusive). Example: "1514978890136-1514978650130".
firstseen__gt	optional	Devices first seen after this timestamp. Example: "2018-02-27T04:49:26.257525Z".
firstseen__gte	optional	Devices first seen after or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
firstseen__lt	optional	Devices first seen before this timestamp. Example: "2018-02-27T04:49:26.257525Z".
firstseen__lte	optional	Devices first seen before or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
groupids	optional	List of Group IDs to filter by. Example: "225494730938493804,225494730938493915".
hostnames	optional	Hostnames
hostnames__contains	optional	Free-text filter by hostanem (supports multiple values). Example: "s1_host,SomeHost".
ids	optional	List of device ids. Example: "225494730938493804,225494730938493915".
lastseen__between	optional	Date range for last seen(format: <from_timestamp>-<to_timestamp>, inclusive). Example:

		"1514978890136-1514978650130".
lastseen__gt	optional	Devices last seen after this timestamp. Example: "2018-02-27T04:49:26.257525Z".
lastseen__gte	optional	Devices last seen after or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
lastseen__lt	optional	Devices last seen before this timestamp. Example: "2018-02-27T04:49:26.257525Z".
lastseen__lte	optional	Devices last seen before or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
localip	optional	Search using local IP
localip__contains	optional	Free-text filter by IP Address (supports multiple values). Example: "192.168.0.1/24,10.1".
macaddress	optional	A mac address to search for
macaddress__contains	optional	Free-text filter by mac address (supports multiple values). Example: "aa:ee:b1".
manufacturer	optional	Manufacturer of the device or network interface
manufacturer__contains	optional	Free-text filter by manufacturer (supports multiple values). Example: "Company".
osname	optional	Os name
ostype	optional	OS type
ostypes	optional	Included OS types
osversion	optional	Os version
osversion__contains	optional	Free-text filter by OS full name and version (supports multiple values). Example: "Service Pack 1".
query	optional	Query
siteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".
tenant	optional	Indicates a tenant scope request

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Get Rogues Settings

GET /web/api/v2.1/rogues/settings

Rogues gives full visibility of all unsecured devices connected to your network. Rogues scans your corporate environment to identify and manage connected devices, even those not protected by or supported by SentinelOne. Rogues identifies devices as:
* UnSecured - End-user computer or laptop, or server, without a SentinelOne Agent.
When you install Windows Agents with Rogues, the Agents can become scanners. Selected scanners from networks that you enable for scanning find connected devices with passive and active scan techniques. The scanners send the collected data to Rogues on the Management. Rogues then runs fingerprinting to identify and classify unique devices and to update the Device Inventory Table in the Management Console. With port scanning, it is important that you understand the legal and ethical considerations and that you document a Rogues plan and implementation. See Legal Considerations and Proper Implementation in the Console Help.
* minAgentsInNetworkToScan - To help you determine which networks are corporate, Rogues looks at the number of secured endpoints (Agents) in a network. If there are not enough Agents in a network - set by this parameter value - Rogues considers the network to be non-corporate and will not scan it.

Parameters

accountids	optional	List of Account IDs to filter by. Example: "225494730938493804,225494730938493915".
siteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - Insufficient permissions

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
accountId	Account id	false	string
enabled	Is the ranger	false	boolean

				collection enabled for the account		
			minAgentsInNetworkToScan	Minimum agents required in a network to be listed as selectable for scan.Valid values are 2, 10 and 100 if rogues is enabled	false	integer
			restrictions	A set of IP addresses that should not be scanned in the specific network	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>annotation</td><td>An optional note with the reason for the restriction</td><td>false</td><td>string</td></tr><tr><td>type</td><td></td><td>false</td><td>enum</td></tr><tr><td>values</td><td>It will be one IP or one CIDR or two values for a Range</td><td>false</td><td>string []</td></tr></table>
			specificPorts	[FUTURE] A set of specific ports allowed to be used as source ports for an active scan	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>type</td><td></td><td>false</td><td>enum</td></tr><tr><td>values</td><td>It can be a single port or two ports [start, end] for a Range</td><td>false</td><td>integer []</td></tr></table>
			useSpecificPorts	[FUTURE] Use only specific ports defined in specific ports as source ports of	false	boolean

			active scans
errors	Errors	false	array

Update Rogues Settings

PUT /web/api/v2.1/rogues/settings

Change the Rogues Settings. Best Practice: Get the current settings before you change them. See: Get Rogues Settings.

> **BEST PRACTICE**
> Get the current settings before you change them. See: Get Rogues Settings.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - Insufficient permissions

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
accountId	Account id	false	string
enabled	Is the ranger collection enabled for the account	false	boolean
minAgentsInNetworkToScan	Minimum agents required in a network to be listed as selectable for scan.Valid values are 2, 10 and 100 if rogues is	false	integer

<table>
<tr><td></td><td></td><td></td><td>
<table>
<tr><td></td><td>enabled</td><td></td><td></td></tr>
<tr><td>restrictions</td><td>A set of IP addresses that should not be scanned in the specific network</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>annotation</td><td>An optional note with the reason for the restriction</td><td>false</td><td>string</td></tr>
<tr><td>type</td><td></td><td>false</td><td>enum</td></tr>
<tr><td>values</td><td>It will be one IP or one CIDR or two values for a Range</td><td>false</td><td>string []</td></tr>
</table>
</td></tr>
<tr><td>specificPorts</td><td>[FUTURE] A set of specific ports allowed to be used as source ports for an active scan</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>type</td><td></td><td>false</td><td>enum</td></tr>
<tr><td>values</td><td>It can be a single port or two ports [start, end] for a Range</td><td>false</td><td>integer []</td></tr>
</table>
</td></tr>
<tr><td>useSpecificPorts</td><td>[FUTURE] Use only specific ports defined in specific ports as source ports of active scans</td><td>false</td><td>boolean</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

Name	Description	Required	Value
data	Data	true	

Name	Description	Required	Value
accountId	Account id	false	string
enabled	Is the ranger collection enabled for the account	false	boolean
minAgentsInNetworkToScan	Minimum agents required in a network to be listed as selectable for scan.Valid values are 2, 10 and 100 if rogues is enabled	false	integer
restrictions	A set of IP addresses that should not be scanned in the specific network	false	
specificPorts	[FUTURE] A set of specific ports allowed to be used as source ports for an active scan	false	

Name	Description	Required	Value
annotation	An optional note with the reason for the restriction	false	string
type		false	enum
values	It will be one IP or one CIDR or two values for a Range	false	string []

Name	Description	Required	Value
type		false	enum
values	It can be a single port or two ports [start, end] for a Range	false	integer []

<table>
<tr><td></td><td></td><td></td><td><table><tr><td>useSpecificPorts</td><td>[FUTURE] Use only specific ports defined in specific ports as source ports of active scans</td><td>false</td><td>boolean</td></tr></table></td></tr>
<tr><td>filter</td><td>Filter</td><td>true</td><td><table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr><tr><td>siteIds</td><td>List of Site IDs to filter by</td><td>false</td><td>string []</td></tr></table></td></tr>
</table>

Service Users

Get Service Users

GET /web/api/v2.1/service-users

Get a list of service users.

Parameters

accountids	optional	List of Account IDs to filter by. Example: "225494730938493804,225494730938493915".
countonly	optional	If true, only total number of items will be returned, without any of the actual objects.
cursor	optional	Cursor position returned by the last request. Use to iterate over more than 1000 items. Example: "YWdlbnRfaWQ6NTgwMjkzODE=".
ids	optional	List of service user IDs to filter by. Example: "225494730938493804,225494730938493915".
limit	optional	Limit number of returned items (1-1000). Example: "10".
query	optional	Full text search for fields: full_name, email, description
roleids	optional	List of rbac roles to filter by. Example: "225494730938493804,225494730938493915".
siteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".
skip	optional	Skip first number of items (0-1000). To iterate over more than 1000 items, use "cursor". Example: "150".
skipcount	optional	If true, total number of items will not be calculated, which speeds up execution time.
sortby	optional	The column to sort the results by. Example: "id".
sortorder	optional	Sort direction. Example: "asc".

Response Messages

200 - List of service users retrieved successfully.

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
pagination	Pagination information	true	

Name	Description	Required	Value
totalItems	Total number of items found matching your query	true	integer
nextCursor	Pass this value as "cursor" on your next request, to get the next page of results (Will be "null" when last page reached)	false	string

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
scope	User Scope	true	enum
apiToken	Api token	false	
createdAt	Created at	false	string
createdBy	Created by	false	
description	Description	false	string

Name	Description	Required	Value
createdAt	Created at	false	string
expiresAt	Expires at	false	string

Name	Description	Required	Value
id	Id	false	string
name	Name	false	string

<table>
<tr><td></td><td></td><td></td><td>
<table>
<tr><td>id</td><td>Id</td><td>false</td><td>string</td></tr>
<tr><td>lastActivation</td><td>Last activation</td><td>false</td><td>string</td></tr>
<tr><td>name</td><td>Name</td><td>false</td><td>string</td></tr>
<tr><td>scopeRoles</td><td>Roles of the scope user</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountName</td><td>Scope name</td><td>true</td><td>string</td></tr>
<tr><td>name</td><td>Scope name</td><td>true</td><td>string</td></tr>
<tr><td>id</td><td>Scope ID</td><td>false</td><td>string</td></tr>
<tr><td>roleId</td><td>ID of the wanted role</td><td>false</td><td>string</td></tr>
<tr><td>roleName</td><td>[DEPRECATED] Name of the role, will work only for predefined roles</td><td>false</td><td>string</td></tr>
<tr><td>roles</td><td>[DEPRECATED] List containing the desired role name in this scope. Use role_id or role_name instead.</td><td>false</td><td>string []</td></tr>
</table>
</td></tr>
<tr><td>updatedAt</td><td>Updated at</td><td>false</td><td>string</td></tr>
<tr><td>updatedBy</td><td>Updated by</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>id</td><td>Id</td><td>false</td><td>string</td></tr>
<tr><td>name</td><td>Name</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Create Service User

POST /web/api/v2.1/service-users

Create a new service user.

Response Messages

200 - Service User created successfully.

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - Not enough permissions to create service user.

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
scope	User Scope	true	enum
apiToken	Api token	false	
createdAt	Created at	false	string
createdBy	Created by	false	
description	Description	false	string
id	Id	false	string
lastActivation	Last activation	false	string
name	Name	false	string

Name	Description	Required	Value
createdAt	Created at	false	string
expiresAt	Expires at	false	string
value	Value	false	string

Name	Description	Required	Value
id	Id	false	string
name	Name	false	string

<table>
<tr><td></td><td></td><td></td><td>scopeRoles</td><td>Roles of the scope user</td><td>false</td><td><table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>accountName</td><td>Scope name</td><td>true</td><td>string</td></tr><tr><td>name</td><td>Scope name</td><td>true</td><td>string</td></tr><tr><td>id</td><td>Scope ID</td><td>false</td><td>string</td></tr><tr><td>roleId</td><td>ID of the wanted role</td><td>false</td><td>string</td></tr><tr><td>roleName</td><td>[DEPRECATED] Name of the role, will work only for predefined roles</td><td>false</td><td>string</td></tr><tr><td>roles</td><td>[DEPRECATED] List containing the desired role name in this scope. Use role_id or role_name instead.</td><td>false</td><td>string []</td></tr></table></td></tr>
<tr><td></td><td></td><td></td><td>updatedAt</td><td>Updated at</td><td>false</td><td>string</td></tr>
<tr><td></td><td></td><td></td><td>updatedBy</td><td>Updated by</td><td>false</td><td><table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>id</td><td>Id</td><td>false</td><td>string</td></tr><tr><td>name</td><td>Name</td><td>false</td><td>string</td></tr></table></td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td colspan="4">array</td></tr>
</table>

Body Schema

Name	Description	Required	Value
data	Data	true	

Name	Description	Required	Value
expirationDate	Date when the generated token expires	true	string
name	Name of the service user	true	string
scope	User scope	true	enum
description	Description	false	string
forceLegacy	Temporary attribute for WA: If the flag is set to True the legacy token will be generated even if the auth_tokens global switch is turned on	false	boolean
scopeRoles	List of id and role id, id is mandatory for user in scope account/site. User in tenant (global) role does not need to provide an id.	false	

Name	Description	Required	Value
id	Scope ID	false	string
roleId	ID of the wanted role	false	string
roleName	[DEPRECATED] Name of the role, will work only for predefined roles	false	string
roles	[DEPRECATED] List containing the desired role name in	false	string []

							this scope. Use role_id or role_name instead.		

Export Service Users

GET /web/api/v2.1/export/service-users

Export Service User data to a CSV, for Service Users that match the filter.

Parameters

accountids	optional	List of Account IDs to filter by. Example: "225494730938493804,225494730938493915".
ids	optional	List of service user IDs to filter by. Example: "225494730938493804,225494730938493915".
query	optional	Full text search for fields: full_name, email, description
roleids	optional	List of rbac roles to filter by. Example: "225494730938493804,225494730938493915".
siteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Update Service User

PUT /web/api/v2.1/service-users/{service_user_id}

Change properties of the service user with the given ID.

Response Messages

200 - Service User updated successfully.

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - Forbidden.

404 - Service User not found.

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
scope	User Scope	true	enum
apiToken	Api token	false	
createdAt	Created at	false	string
createdBy	Created by	false	
description	Description	false	string
id	Id	false	string
lastActivation	Last activation	false	string
name	Name	false	string
scopeRoles	Roles of the scope user	false	

Name	Description	Required	Value
createdAt	Created at	false	string
expiresAt	Expires at	false	string

Name	Description	Required	Value
id	Id	false	string
name	Name	false	string

Name	Description	Required	Value
accountName	Scope name	true	string
name	Scope name	true	string
id	Scope ID	false	string
roleId	ID of the wanted role	false	string
roleName	[DEPRECATED] Name of the role, will work only for predefined	false	string

<table>
<tr><td></td><td></td><td></td><td>
<table>
<tr><td></td><td></td><td></td><td>
<table>
<tr><td></td><td>roles</td><td></td><td></td></tr>
<tr><td>roles</td><td>[DEPRECATED] List containing the desired role name in this scope. Use role_id or role_name instead.</td><td>false</td><td>string []</td></tr>
</table>
</td></tr>
<tr><td>updatedAt</td><td>Updated at</td><td>false</td><td>string</td></tr>
<tr><td>updatedBy</td><td>Updated by</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>id</td><td>Id</td><td>false</td><td>string</td></tr>
<tr><td>name</td><td>Name</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

Name	Description	Required	Value
data	Data	true	

Name	Description	Required	Value
description	Description	false	string
scope	User scope	false	enum
scopeRoles	List of id and role id, id is mandatory for user in scope account/site. User in tenant (global) role does not need to provide an id.	false	

Name	Description	Required	Value
id	Scope ID	false	string
roleId	ID of the wanted role	false	string
roleName	[DEPRECATED] Name of the role, will work only for predefined roles	false	string
roles	[DEPRECATED] List containing the desired role name in this scope. Use role_id or role_name instead.	false	string []

Delete Service User

DELETE /web/api/v2.1/service-users/{service_user_id}

Delete a service user by ID.

Response Messages

200 - Service User deleted successfully.

401 - Unauthorized access - please sign in and retry.

403 - Insufficient permissions.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td><table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>success</td><td>Indicates a successful operation</td><td>false</td><td>boolean</td></tr></table></td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Bulk Delete Service Users

POST /web/api/v2.1/service-users/delete-service-users

Delete all service users that match the filter.

Response Messages

200 - Service Users deleted successfully.

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - Insufficient permissions.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>affected</td><td>Number of entities affected by the requested operation</td><td>false</td><td>integer</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>filter</td><td>Filter</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>ids</td><td>List of service user IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>query</td><td>Full text search for fields: full_name, email, description</td><td>false</td><td>string</td></tr>
<tr><td>roleIds</td><td>List of rbac roles to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>siteIds</td><td>List of Site IDs to filter by</td><td>false</td><td>string []</td></tr>
</table>
</td></tr>
<tr><td>data</td><td>Data</td><td>false</td><td></td></tr>
</table>

Settings

Get SSO Settings

GET /web/api/v2.1/settings/sso

Get the Single Sign-On configuration for the given Sites (to get the IDs, run "sites") or Accounts ("accounts").

Parameters

accountids	optional	List of Account IDs to filter by. Example: "225494730938493804,225494730938493915".
siteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
autoProvisioning	True if the user should be auto provisioned	false	boolean
defaultUserRole	The role name of the default role for a new user logging in via SSO for	false	string

				the first time		
			defaultUserRoleId	The role name of the default role for a new user logging in via SSO for the first time	false	string
			domains	A list of domain names associated with the scope	false	string []
			enabled	Indicates if SSO is enabled	false	boolean
			idpCertName	Identity provider's certificate file name (If not provided, cert name and content will stay untouched in the DB)	false	string
			idpEntityId	Identity provider's Entity ID (a.k.a. Issuer)	false	string
			idpSsoUrl	The SSO URL of the Identity Provider (Login URL)	false	string
			signRequest	Indicates if SAML Request Signing is enabled	false	boolean
			spAcsUrl	Management	false	string

				console Assertion Consumer Service (ACS) URL. This is were IDP should send the authenticatio n request		
			spEntityId	Identifier the Management console creates to dialogue with the SSO provider.	false	string
			ssoElevatedS essionReauth Type	Type of re-authenticatio n used for session elevation.	false	enum
			ssoElevatedS essionReauth TypeEnabled	Marks whether re-auth type choice should be available in SSO settings	false	boolean
			ssoInheritab leDomains	A dictionary of inheritable domains	false	object
			ssoInheritDo mainsFrom	Scope(s) to inherit domains from	false	string []
			ssoPropagate DomainsToChi ldren	True if the domains should be propagated to children scopes	false	boolean
errors	Errors	false	array			

Set SSO Settings

PUT /web/api/v2.1/settings/sso

Change the Single Sign-On configuration for the given Sites (to get the IDs, run "sites") or Accounts ("accounts").
The Management supports SAML 2.0 and will integrate with SAML 2.0 compliant SSO providers.
SentinelOne Technical Support can help you with issues related to the provider we tested: Okta. To use a different ID provider, see the provider documentation and support.
For requirements and best practices of Okta integration, see https://support.sentinelone.com/hc/en-us/articles/360004195714.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>autoProvisioning</td><td>True if the user should be auto provisioned</td><td>false</td><td>boolean</td></tr>
<tr><td>defaultUserRole</td><td>The role name of the default role for a new user logging in via SSO for the first time</td><td>false</td><td>string</td></tr>
<tr><td>defaultUserRoleId</td><td>The role name of the default role for a new user logging in via SSO for the first time</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
</table>

			domains	A list of domain names associated with the scope	false	string []
			enabled	Indicates if SSO is enabled	false	boolean
			idpCertName	Identity provider's certificate file name (If not provided, cert name and content will stay untouched in the DB)	false	string
			idpEntityId	Identity provider's Entity ID (a.k.a. Issuer)	false	string
			idpSsoUrl	The SSO URL of the Identity Provider (Login URL)	false	string
			signRequest	Indicates if SAML Request Signing is enabled	false	boolean
			spAcsUrl	Management console Assertion Consumer Service (ACS) URL. This is were IDP should send the authenticatio	false	string

			n request		
			spEntityId	Identifier the Management console creates to dialogue with the SSO provider.	false	string
			ssoElevatedSessionReauthType	Type of re-authentication used for session elevation.	false	enum
			ssoElevatedSessionReauthTypeEnabled	Marks whether re-auth type choice should be available in SSO settings	false	boolean
			ssoInheritableDomains	A dictionary of inheritable domains	false	object
			ssoInheritDomainsFrom	Scope(s) to inherit domains from	false	string []
			ssoPropagateDomainsToChildren	True if the domains should be propagated to children scopes	false	boolean
errors	Errors	false	array			

Body Schema

Name	Description	Required	Value
data	Data	true	

Name	Description	Required	Value
enabled	If True, other arguments must also be supplied, if False, other arguments stay untouched in the DB	true	boolean
autoProvisioning	True if the user should be auto provisioned	false	boolean
defaultUserRole	The name of the default role for a new user who logs in with SSO. Sending it without default_user_role_id will search only in global scope	false	string
defaultUserRoleId	The role name of the default role for a new user logging in via SSO for the first time	false	string
domains	A list of domain names associated with the scope	false	string []
idpCertConte	Identity	false	string

			nt	provider's certificate file content (Base64 encoded string)		
			idpCertName	Identity provider's certificate file name (If not provided, cert name and content will stay untouched in the DB)	false	string
			idpEntityId	Identity provider's Entity ID (a.k.a. Issuer)	false	string
			idpSsoUrl	The SSO URL of the Identity Provider (Login URL)	false	string
			signRequest	Indicates if SAML Request Signing is enabled	false	boolean
			ssoElevatedSessionReauthType	Type of re-authentication used for session elevation.	false	enum
			ssoInheritDomainsFrom	Scope(s) to inherit domains from	false	string []
			ssoPropagateDomainsToChildren	True if the domains should be propagated to children	false	boolean

			scopes
filter	Filter	true	Name | Description | Required | Value accountIds | List of Account IDs to filter by | false | string [] siteIds | List of Site IDs to filter by | false | string []

Get SSO Service Provider Certificate

GET /web/api/v2.1/settings/sso/sp-cert

Get the Service Provider Certificate for the Single Sign-On configuration for the given scope.

Parameters

accountids	optional	List of Account IDs to filter by. Example: "225494730938493804,225494730938493915".
siteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
expiresAt	Certificate expires at	false	string
fileName	File name of the signing certificate used by the service provider to sign SAML requests	false	string
issuedAt	Certificate issued at	false	string
pem	Certificate in PEM format	false	string

errors	Errors	false	array

Download SSO Service Provider Certificate

GET /web/api/v2.1/settings/sso/sp-cert/download

Download the Service Provider Certificate for the Single Sign-On configuration for the given scope.

Parameters

accountids	optional	List of Account IDs to filter by. Example: "225494730938493804,225494730938493915".
siteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Test SSO Settings

POST /web/api/v2.1/settings/sso/test

Test Single Sign-On settings.

Response Messages

200 - The url to redirect too.

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value

<table>
<tr><td>data</td><td>Response data</td><td>false</td><td><table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>redirectUrl</td><td>The url to redirect for test.</td><td>false</td><td>string</td></tr></table></td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

Name	Description	Required	Value
data	Data	true	

Name	Description	Required	Value
enabled	If True, other arguments must also be supplied, if False, other arguments stay untouched in the DB	true	boolean
autoProvisioning	True if the user should be auto provisioned	false	boolean
defaultUserRole	The name of the default role for a new user who logs in with SSO. Sending it without default_user_role_id will search only in global scope	false	string
defaultUserRoleId	The role name of the default role for a new user logging in via SSO for the first time	false	string
domains	A list of domain names associated with the scope	false	string []
idpCertConte	Identity	false	string

			nt	provider's certificate file content (Base64 encoded string)		
			idpCertName	Identity provider's certificate file name (If not provided, cert name and content will stay untouched in the DB)	false	string
			idpEntityId	Identity provider's Entity ID (a.k.a. Issuer)	false	string
			idpSsoUrl	The SSO URL of the Identity Provider (Login URL)	false	string
			signRequest	Indicates if SAML Request Signing is enabled	false	boolean
			ssoElevatedSessionReauthType	Type of re-authentication used for session elevation.	false	enum
			ssoInheritDomainsFrom	Scope(s) to inherit domains from	false	string []
			ssoPropagateDomainsToChildren	True if the domains should be propagated to children	false	boolean

			scopes
filter	Filter	true	Name: accountIds Description: List of Account IDs to filter by Required: false Value: string [] Name: siteIds Description: List of Site IDs to filter by Required: false Value: string []

Get Notification Settings

GET /web/api/v2.1/settings/notifications

Get the notification settings for the given Sites (to get the IDs, run "settings") or Accounts ("accounts").
The response shows every possible notification and whether it is active and if so, for email or syslog or both. It also shows the ID string for each notification, which can be used in other commands.
Note: Each notification also shows "sms" which is deprecated.

Parameters

accountids	optional	List of Account IDs to filter by. Example: "225494730938493804,225494730938493915".
siteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".

Response Messages

200 - Data retrieved successfully

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - User is not allowed in this scope

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
configurations	Configurations	false	

Name	Description	Required	Value
email	If not empty, email configuration is missing	false	string
sms	If not empty, sms configuration	false	string

							is missing		
						syslog	If not empty, syslog configuration is missing	false	string
			lastModified	Notifications last modified	false				
						Name	Description	Required	Value
						updatedAt	Last Modified details level data	false	string
						updatedBy	Last Modified details level data	false	string
			notifications	Notifications categories	false				
						Name	Description	Required	Value
						activedirectory	Category Items	false	object
						administrative	Category Items	false	object
						customrules	Category Items	false	object
						devicecontrol	Category Items	false	object
						endpointtagging	Category Items	false	object
						firewallcontrol	Category Items	false	object
						locations	Category Items	false	object
						malware	Category Items	false	object
						mitigation	Category Items	false	object
						operations	Category Items	false	object
						ranger	Category Items	false	object
						remoteshell	Category	false	object

							Items		
						threatmanagement	Category Items	false	object
						whitelistblacklist	Category Items	false	object
errors	Errors	false	array						

Set Notification Settings

PUT /web/api/v2.1/settings/notifications

Change the notifications for the given Sites (to get the IDs, run "settings") or Accounts ("accounts"). Best practice: Get the current settings (see Get Notification Settings) before you run this command.

> **BEST PRACTICE**
> Get the current settings (see Get Notification Settings) before you run this command.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - User is not allowed in this scope

404 - Scope does not exist

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
configurations	Configurations	false	

Name	Description	Required	Value
email	If not empty, email configuration is missing	false	string
sms	If not empty, sms configuration is missing	false	string
syslog	If not empty, syslog	false	string

							configuration is missing		
			lastModified	Notifications last modified	false	Name	Description	Required	Value
						updatedAt	Last Modified details level data	false	string
						updatedBy	Last Modified details level data	false	string
			notifications	Notifications categories	false	Name	Description	Required	Value
						activedirectory	Category Items	false	object
						administrative	Category Items	false	object
						customrules	Category Items	false	object
						devicecontrol	Category Items	false	object
						endpointtagging	Category Items	false	object
						firewallcontrol	Category Items	false	object
						locations	Category Items	false	object
						malware	Category Items	false	object
						mitigation	Category Items	false	object
						operations	Category Items	false	object
						ranger	Category Items	false	object
						remoteshell	Category Items	false	object
						threatmanagement	Category Items	false	object

						whitelistblacklist	Category Items	false	object
errors	Errors	false	array						

Body Schema

Name	Description	Required	Value
data	Data	true	

Name	Description	Required	Value
configurations	Configurations	false	

Name	Description	Required	Value
email	If not empty, email configuration is missing	false	string
sms	If not empty, sms configuration is missing	false	string
syslog	If not empty, syslog configuration is missing	false	string

Name	Description	Required	Value
lastModified	Notifications last modified	false	

Name	Description	Required	Value
updatedAt	Last Modified details level data	false	string
updatedBy	Last Modified details level data	false	string

Name	Description	Required	Value
notifications	Notifications categories	false	

Name	Description	Required	Value
activedirectory	Category Items	false	object
administrative	Category Items	false	object
customrules	Category Items	false	object
devicecontrol	Category Items	false	object
endpointtagging	Category Items	false	object
firewallcontro	Category	false	object

						l	Items		
						locations	Category Items	false	object
						malware	Category Items	false	object
						mitigation	Category Items	false	object
						operations	Category Items	false	object
						ranger	Category Items	false	object
						remoteshell	Category Items	false	object
						threatmanagement	Category Items	false	object
						whitelistblacklist	Category Items	false	object
filter	Filter	true	Name	Description	Required	Value			
			accountIds	List of Account IDs to filter by	false	string []			
			siteIds	List of Site IDs to filter by	false	string []			

Clear Pending Emails

POST /web/api/v2.1/settings/notifications/cancel-pending-emails

Clear (discard without sending) pending email notifications for the given Sites (to get the IDs, run "sites") or Accounts ("accounts").
When you set email recipients to get notifications for activities in the system, you can set too many, or in other ways cause issues that demand that the queue be cleared.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - User is not allowed in this scope

404 - Scope does not exist

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td><table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>canceled</td><td>Canceled</td><td>true</td><td>integer</td></tr></table></td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>filter</td><td>Filter</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>siteIds</td><td>List of Site IDs to filter by</td><td>false</td><td>string []</td></tr>
</table>
</td></tr>
</table>

Get SMTP Settings

GET /web/api/v2.1/settings/smtp

Get the SMTP server configuration of the given Sites (to get the IDs, run "sites") or Accounts ("accounts"). The SMTP integration is required to send notifications by email.

Parameters

accountids	optional	List of Account IDs to filter by. Example: "225494730938493804,225494730938493915".
siteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".

Response Messages

200 - Data retrieved successfully

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - User is not allowed in this scope

404 - Scope does not exist

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
enabled	SMTP service is enabled	false	boolean
encryption	SMTP service encryption type	false	enum
host	SMTP service host	false	string
inherits	True if site inherits SMTP	false	boolean

			settings from global scope, False if using custom settings.		
			noReplyEmail	SMTP service no-reply-email	false	string
			password	SMTP service password. Required when creating new SMTP settings or updating host and/or port of the existing one.	false	string
			port	SMTP service port	false	integer
			username	SMTP service username	false	string
errors	Errors	false	array			

Set SMTP Settings

PUT /web/api/v2.1/settings/smtp

Change the SMTP server configuration for the given Sites or Accounts. Use this command to integrate a different SMTP server, which is required to send notifications by email.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - User is not allowed in this scope

404 - Scope does not exist

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
enabled	SMTP service is enabled	false	boolean
encryption	SMTP service encryption type	false	enum
host	SMTP service host	false	string
inherits	True if site inherits SMTP settings from global scope, False if using custom settings.	false	boolean
noReplyEmail	SMTP service	false	string

Body Schema

Name	Description	Required	Value
data	Data	true	

Name	Description	Required	Value
enabled	SMTP service is enabled	false	boolean
encryption	SMTP service encryption type	false	enum
host	SMTP service host	false	string
inherits	True if site inherits SMTP settings from global scope, False if using custom settings.	false	boolean
noReplyEmail	SMTP service no-reply-email	false	string
password	SMTP service password. Required when creating new SMTP settings or updating host and/or port of the existing one.	false	string
port	SMTP service port	false	integer
username	SMTP service username	false	string

Name	Description	Required	Value
filter	Filter	true	

Name	Description	Required	Value
accountIds	List of	false	string []

				Account IDs to filter by		
			siteIds	List of Site IDs to filter by	false	string []

Test SMTP Settings

POST /web/api/v2.1/settings/smtp/test

Test SMTP settings between the Management and the SMTP server. This integration is required if you use email notifications.

Response Messages

200 - Data retrieved successfully

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

404 - Scope does not exist

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td><table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>status</td><td>Status</td><td>true</td><td>boolean</td></tr></table></td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>enabled</td><td>SMTP service is enabled</td><td>false</td><td>boolean</td></tr>
<tr><td>encryption</td><td>SMTP service encryption type</td><td>false</td><td>enum</td></tr>
<tr><td>host</td><td>SMTP service host</td><td>false</td><td>string</td></tr>
<tr><td>inherits</td><td>True if site inherits SMTP settings from global scope, False if using custom settings.</td><td>false</td><td>boolean</td></tr>
<tr><td>noReplyEmail</td><td>SMTP service no-reply-email</td><td>false</td><td>string</td></tr>
<tr><td>password</td><td>SMTP service password. Required when testing new SMTP settings or testing update of host and/or port of the existing one.</td><td>false</td><td>string</td></tr>
<tr><td>port</td><td>SMTP service port</td><td>false</td><td>integer</td></tr>
<tr><td>username</td><td>SMTP service username</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>filter</td><td>Filter</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of</td><td>false</td><td>string []</td></tr>
</table>
</td></tr>
</table>

				Account IDs to filter by		
			siteIds	List of Site IDs to filter by	false	string []

Get Syslog Settings

GET /web/api/v2.1/settings/syslog

Get the configuration of the syslog server integrated with the given Sites (to get the IDs, run "sites") or Accounts ("accounts").

Parameters

accountids	optional	List of Account IDs to filter by. Example: "225494730938493804,225494730938493915".
siteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".

Response Messages

200 - Data retrieved successfully

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - User is not allowed in this scope

404 - Scope does not exist

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
clientCertContent	SysLog service client certificate content in Base64	false	string
clientCertName	SysLog service client certificate name	false	string
clientKeyCon	SysLog	false	string

			tent: service client key content in Base64 clientKeyName: SysLog service client key name (false, string) enabled: SysLog service is enabled (false, boolean) format: SysLog service format (false, enum) host: SysLog service host (false, string) port: SysLog service port (false, integer) serverCertContent: SysLog service server certificate content in Base64 (false, string) serverCertName: SysLog service server certificate name (false, string) ssl: SysLog service uses ssl (false, boolean) token: SysLog server token (false, string)
errors	Errors	false	array

Set Syslog Settings

PUT /web/api/v2.1/settings/syslog

Change the configuration of the syslog server of the given Sites (to get the IDs, run "sites") or Accounts ("accounts"). Use this command to send notifications to a different syslog server. Best Practice: Get Syslog Settings before you run this command.

BEST PRACTICE

Get Syslog Settings before you run this command.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - User is not allowed in this scope

404 - Scope does not exist

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
clientCertContent	SysLog service client certificate content in Base64	false	string
clientCertName	SysLog service client certificate name	false	string
clientKeyContent	SysLog service client key content	false	string

			in Base64		
			clientKeyName	SysLog service client key name	false	string
			enabled	SysLog service is enabled	false	boolean
			format	SysLog service format	false	enum
			host	SysLog service host	false	string
			port	SysLog service port	false	integer
			serverCertContent	SysLog service server certificate content in Base64	false	string
			serverCertName	SysLog service server certificate name	false	string
			ssl	SysLog service uses ssl	false	boolean
			token	SysLog server token	false	string
errors	Errors	false	array			

Body Schema

Name	Description	Required	Value
data	Data	true	

Name	Description	Required	Value
clientCertContent	SysLog service client certificate content in Base64	false	string
clientCertName	SysLog service client certificate name	false	string
clientKeyContent	SysLog service client key content in Base64	false	string
clientKeyName	SysLog service client key name	false	string
enabled	SysLog service is enabled	false	boolean
format	SysLog service format	false	enum
host	SysLog service host	false	string
port	SysLog service port	false	integer
serverCertContent	SysLog service server certificate content in Base64	false	string
serverCertName	SysLog service server certificate name	false	string
ssl	SysLog	false	boolean

			service uses ssl		
			token	SysLog server token	false	string
filter	Filter	true	Name	Description	Required	Value
			accountIds	List of Account IDs to filter by	false	string []
			siteIds	List of Site IDs to filter by	false	string []

Test Syslog Settings

POST /web/api/v2.1/settings/syslog/test

Test Syslog settings. The Management tests the connection to the Syslog server.

Response Messages

200 - Data retrieved successfully

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

404 - Scope does not exist

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>status</td><td>Status</td><td>true</td><td>boolean</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>clientCertContent</td><td>SysLog service client certificate content in Base64</td><td>false</td><td>string</td></tr>
<tr><td>clientCertName</td><td>SysLog service client certificate name</td><td>false</td><td>string</td></tr>
<tr><td>clientKeyContent</td><td>SysLog service client key content in Base64</td><td>false</td><td>string</td></tr>
<tr><td>clientKeyName</td><td>SysLog service client key name</td><td>false</td><td>string</td></tr>
<tr><td>enabled</td><td>SysLog service is enabled</td><td>false</td><td>boolean</td></tr>
<tr><td>format</td><td>SysLog service format</td><td>false</td><td>enum</td></tr>
<tr><td>host</td><td>SysLog service host</td><td>false</td><td>string</td></tr>
<tr><td>port</td><td>SysLog service port</td><td>false</td><td>integer</td></tr>
<tr><td>serverCertContent</td><td>SysLog service server certificate content in Base64</td><td>false</td><td>string</td></tr>
<tr><td>serverCertName</td><td>SysLog service server certificate name</td><td>false</td><td>string</td></tr>
<tr><td>ssl</td><td>SysLog</td><td>false</td><td>boolean</td></tr>
</table>
</td></tr>
</table>

			service uses ssl		
			token	SysLog server token	false	string
filter	Filter	true	Name	Description	Required	Value
			accountIds	List of Account IDs to filter by	false	string []
			siteIds	List of Site IDs to filter by	false	string []

Get SMS Settings

GET /web/api/v2.1/settings/sms

[DEPRECATED] Gets the site's SMS settings.

Parameters

accountids	optional	List of Account IDs to filter by. Example: "225494730938493804,225494730938493915".
siteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".

Response Messages

200 - Data retrieved successfully

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - User is not allowed in this scope

404 - Scope does not exist

Response Schema

Name	Description	Required	Value
data	Response data	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>enabled</td><td>SMS service is enabled</td><td>false</td><td>boolean</td></tr></table>
errors	Errors	false	array

Set SMS Settings

PUT /web/api/v2.1/settings/sms

[DEPRECATED] Set SMS settings.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - User is not allowed in this scope

404 - Scope does not exist

Response Schema

Name	Description	Required	Value
data	Response data	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>enabled</td><td>SMS service is enabled</td><td>false</td><td>boolean</td></tr></table>
errors	Errors	false	array

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>enabled</td><td>SMS service is enabled</td><td>false</td><td>boolean</td></tr>
</table>
</td></tr>
<tr><td>filter</td><td>Filter</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>siteIds</td><td>List of Site IDs to filter by</td><td>false</td><td>string []</td></tr>
</table>
</td></tr>
</table>

Get Notification Recipients

GET /web/api/v2.1/settings/recipients

Get the emails that are configured to receive notifications.

Parameters

accountids	optional	List of Account IDs to filter by. Example: "225494730938493804,225494730938493915".
email	optional	Email
name	optional	Name
query	optional	Full text search for fields: name, email, sms
siteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".
sms	optional	Sms

Response Messages

200 - Data retrieved successfully

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - User is not allowed in this scope

404 - Scope does not exist

Response Schema

Name	Description	Required	Value
data	Response data	false	Name | Description | Required | Value recipients | Notification Recipients | false | Name | Description | Required | Value email | Notification Recipients Email | false | string

						id	Notification Recipients Id	false	string
						name	Notification Recipients Email	false	string
						sms	Notification Recipients SMS	false	string
errors	Errors	false	array						

Set Notification Recipients

PUT /web/api/v2.1/settings/recipients

Set the emails of recipients to get notifications.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - User is not allowed in this scope

404 - Scope does not exist

Response Schema

Name	Description	Required	Value
data	Response data	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>email</td><td>Notification Recipients Email</td><td>false</td><td>string</td></tr><tr><td>id</td><td>Notification Recipients Id</td><td>false</td><td>string</td></tr><tr><td>name</td><td>Notification Recipients Email</td><td>false</td><td>string</td></tr><tr><td>sms</td><td>Notification Recipients SMS</td><td>false</td><td>string</td></tr></table>
errors	Errors	false	array

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>email</td><td>Notification Recipients Email</td><td>false</td><td>string</td></tr>
<tr><td>id</td><td>Notification Recipients Id</td><td>false</td><td>string</td></tr>
<tr><td>name</td><td>Notification Recipients Email</td><td>false</td><td>string</td></tr>
<tr><td>sms</td><td>Notification Recipients SMS</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>filter</td><td>Filter</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>siteIds</td><td>List of Site IDs to filter by</td><td>false</td><td>string []</td></tr>
</table>
</td></tr>
</table>

Delete Notification Recipient

DELETE /web/api/v2.1/settings/recipients/{recipient_id}

Delete a notification recipient by ID. To get the IDs of recipients, run "recipients" (see Get Notification Recipients).

Response Messages

200 - Recipient deleted successfully.

401 - Unauthorized access - please sign in and retry.

403 - Insufficient permissions.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>success</td><td>Indicates a successful operation</td><td>false</td><td>boolean</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Get AD Settings

GET /web/api/v2.1/settings/active-directory

Get the Global Active Directory settings.

Parameters

accountids	optional	List of Account IDs to filter by. Example: "225494730938493804,225494730938493915".
siteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".

Response Messages

200 - Data retrieved successfully

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - User is not allowed in this scope

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
enabled	Is AD service enabled?	false	boolean
host	Active Directory server address	false	string
port	Active Directory server port	false	integer
rootDn	Root Domain Name of Active	false	string

			Directory		
			ssl	Should we speak to the Active Directory server using SSL?	false	boolean
			username	Username used to log in to active directory	false	string
errors	Errors	false	array

Set AD Settings

PUT /web/api/v2.1/settings/active-directory

Update the Global Active Directory settings.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
enabled	Is AD service enabled?	false	boolean
host	Active Directory server address	false	string
port	Active Directory server port	false	integer
rootDn	Root Domain Name of Active Directory	false	string
ssl	Should we speak to the Active Directory server using SSL?	false	boolean
username	Username used to log in	false	string

				to active directory		
errors	Errors	false	array			

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>enabled</td><td>Is AD service enabled?</td><td>false</td><td>boolean</td></tr>
<tr><td>host</td><td>Active Directory server address</td><td>false</td><td>string</td></tr>
<tr><td>password</td><td>Password used to log in to active directory</td><td>false</td><td>string</td></tr>
<tr><td>port</td><td>Active Directory server port</td><td>false</td><td>integer</td></tr>
<tr><td>rootDn</td><td>Root Domain Name of Active Directory</td><td>false</td><td>string</td></tr>
<tr><td>ssl</td><td>Should we speak to the Active Directory server using SSL?</td><td>false</td><td>boolean</td></tr>
<tr><td>username</td><td>Username used to log in to active directory</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
</table>

Test AD Settings

POST /web/api/v2.1/settings/active-directory/test

Test Active Directory settings.

Response Messages

200 - Data retrieved successfully

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

404 - Scope does not exist

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td><table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>status</td><td>Status</td><td>true</td><td>boolean</td></tr></table></td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>enabled</td><td>Is AD service enabled?</td><td>false</td><td>boolean</td></tr>
<tr><td>host</td><td>Active Directory server address</td><td>false</td><td>string</td></tr>
<tr><td>password</td><td>Password used to log in to active directory</td><td>false</td><td>string</td></tr>
<tr><td>port</td><td>Active Directory server port</td><td>false</td><td>integer</td></tr>
<tr><td>rootDn</td><td>Root Domain Name of Active Directory</td><td>false</td><td>string</td></tr>
<tr><td>ssl</td><td>Should we speak to the Active Directory server using SSL?</td><td>false</td><td>boolean</td></tr>
<tr><td>username</td><td>Username used to log in to active directory</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
</table>

Get AD FQDNs

GET /web/api/v2.1/settings/active-directory/scope-mapping

Get the map of Active Directory FQDNs to user roles of the given Sites (use "sites" to get IDs) or Accounts ("accounts").

Parameters

accountids	optional	List of Account IDs to filter by. Example: "225494730938493804,225494730938493915".
siteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".

Response Messages

200 - Data retrieved successfully

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - User is not allowed in this scope

Response Schema

Name	Description	Required	Value
data	Response data	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>admin</td><td>Admin</td><td>false</td><td>string []</td></tr><tr><td>viewer</td><td>Viewer</td><td>false</td><td>string []</td></tr></table>
errors	Errors	false	array

Set AD FQDNs

PUT /web/api/v2.1/settings/active-directory/scope-mapping

Update the Active Directory FQDNs of a Site or Account.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - User is not allowed in this scope

404 - Scope does not exist

Response Schema

Name	Description	Required	Value
data	Response data	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>admin</td><td>Admin</td><td>false</td><td>string []</td></tr><tr><td>viewer</td><td>Viewer</td><td>false</td><td>string []</td></tr></table>
errors	Errors	false	array

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>admin</td><td>Admin</td><td>false</td><td>string []</td></tr>
<tr><td>viewer</td><td>Viewer</td><td>false</td><td>string []</td></tr>
</table>
</td></tr>
<tr><td>filter</td><td>Filter</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>siteIds</td><td>List of Site IDs to filter by</td><td>false</td><td>string []</td></tr>
</table>
</td></tr>
</table>

Get Microsoft Settings

GET /web/api/v2.1/settings/microsoft

[DEPRECATED] Gets the Microsoft settings of the Sites or Accounts.

Parameters

accountids	optional	List of Account IDs to filter by. Example: "225494730938493804,225494730938493915".
siteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".

Response Messages

200 - Data retrieved successfully

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - User is not allowed in this scope

404 - Scope does not exist

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
enabled	Microsoft service is enabled	false	boolean
expiryDate	The expiry time of the given url	false	string
inherits	True if site inherits SMTP settings from	false	boolean

				global scope, False if using custom settings.		
			url	URL used to authenticate with microsoft	false	string
errors	Errors	false	array			

Set Microsoft Settings

PUT /web/api/v2.1/settings/microsoft

[DEPRECATED] Update Microsoft settings for the given Sites or Accounts.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - User is not allowed in this scope

404 - Scope does not exist

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
enabled	Microsoft service is enabled	false	boolean
expiryDate	The expiry time of the given url	false	string
inherits	True if site inherits SMTP settings from global scope, False if using custom settings.	false	boolean
url	URL used to authenticate with	false	string

				microsoft		
errors	Errors	false	array			

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>enabled</td><td>Microsoft service is enabled</td><td>false</td><td>boolean</td></tr>
<tr><td>expiryDate</td><td>The expiry time of the given url</td><td>false</td><td>string</td></tr>
<tr><td>inherits</td><td>True if site inherits SMTP settings from global scope, False if using custom settings.</td><td>false</td><td>boolean</td></tr>
<tr><td>url</td><td>URL used to authenticate with microsoft</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>filter</td><td>Filter</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>siteIds</td><td>List of Site IDs to filter by</td><td>false</td><td>string []</td></tr>
</table>
</td></tr>
</table>

Test Microsoft Settings

POST /web/api/v2.1/settings/microsoft/test

[DEPRECATED] Test Microsoft settings.

Response Messages

200 - Data retrieved successfully

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

404 - Scope does not exist

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>reason</td><td>Reason for unsuccessful call</td><td>false</td><td>string</td></tr>
<tr><td>success</td><td>True if succeeded</td><td>false</td><td>boolean</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>enabled</td><td>Microsoft service is enabled</td><td>false</td><td>boolean</td></tr>
<tr><td>expiryDate</td><td>The expiry time of the given url</td><td>false</td><td>string</td></tr>
<tr><td>inherits</td><td>True if site inherits SMTP settings from global scope, False if using custom settings.</td><td>false</td><td>boolean</td></tr>
<tr><td>url</td><td>URL used to authenticate with microsoft</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>filter</td><td>Filter</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>siteIds</td><td>List of Site IDs to filter by</td><td>false</td><td>string []</td></tr>
</table>
</td></tr>
</table>

Sites

Get Sites

GET /web/api/v2.1/sites

Get the Sites that match the filters.
The response includes the IDs of Sites, which you can use in other commands.

Parameters

accountid	optional	Account id. Example: "225494730938493804".
accountids	optional	List of Account IDs to filter by. Example: "225494730938493804,225494730938493915".
accountname__contains	optional	Free-text filter by account name (supports multiple values)
activelicenses	optional	Active licenses
adminonly	optional	Show sites the user has Admin privileges to
availablemovesites	optional	Only return sites the user can move agents to
countonly	optional	If true, only total number of items will be returned, without any of the actual objects.
createdat	optional	Timestamp of site creation. Example: "2018-02-27T04:49:26.257525Z".
cursor	optional	Cursor position returned by the last request. Use to iterate over more than 1000 items. Example: "YWdlbnRfaWQ6NTgwMjkzODE=".
description	optional	The description for the Site
description__contains	optional	Free-text filter by site description (supports multiple values)
expiration	optional	Expiration. Example: "2018-02-27T04:49:26.257525Z".
externalid	optional	Id in a CRM external system
features	optional	If sent return only sites that support this features. Example: "firewall-control".
healthstatus	optional	Health status

isdefault	optional	Is default
limit	optional	Limit number of returned items (1-1000). Example: "10".
module	optional	Module. Example: "star,rso".
name	optional	Name. Example: "My Site".
name__contains	optional	Free-text filter by site name (supports multiple values)
query	optional	Full text search for fields: name, account_name, description. (Note: on single-account consoles account name will not be matched)
registrationtoken	optional	Registration token. Example: "eyJ1cmwiOiAiaHR0cHM6Ly9jb25zb2xlLnNlbnRpbmVsb25lLm5ldCIs ICJzaXRlX2tleSI6ICIwNzhkYjliMWUyOTA1Y2NhIn0=".
siteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".
sitetype	optional	Site type. Example: "Trial".
skip	optional	Skip first number of items (0-1000). To iterate over more than 1000 items, use "cursor". Example: "150".
skipcount	optional	If true, total number of items will not be calculated, which speeds up execution time.
sku	optional	Sku. Example: "core".
sortby	optional	The column to sort the results by. Example: "id".
sortorder	optional	Sort direction. Example: "asc".
state	optional	Site state. Example: "active".
states	optional	List of states to filter
suite	optional	[DEPRECATED] Use sku instead. Example: "Core".
totallicenses	optional	Total licenses
updatedat	optional	Timestamp of last update. Example: "2018-02-27T04:49:26.257525Z".

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
pagination	Pagination information	true	

Name	Description	Required	Value
totalItems	Total number of items found matching your query	true	integer
nextCursor	Pass this value as "cursor" on your next request, to get the next page of results (Will be "null" when last page reached)	false	string

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
allSites	All sites	false	

Name	Description	Required	Value
activeLicenses	Active licenses	false	integer
totalLicenses	Total licenses	false	integer

Name	Description	Required	Value
sites	Sites	false	

Name	Description	Required	Value
accountId	Account id	false	string
accountName	Account name	false	string
activeLicenses	Number of active licenses for the site	false	integer
createdAt	Timestamp of site creation	false	string
creator	Full name of the creating	false	string

							user		
						creatorId	Id of the creating user	false	string
						description	The user-defined description for the Site	false	string
						expiration	Expiration	false	string
						externalId	Id of CRM external system	false	string
						healthStatus	Obsolete. Always true	false	boolean
						id	Site ID	false	string
						isDefault	Is default	false	boolean
						licenses	The site licenses	false	

Name	Description	Required	Value
bundles	The licenses Bundles	false	

Name	D
displayName	Th di
majorVersion	Th ma
minorVersion	Th mi
name	Th int na
surfaces	Th in
totalSurfaces	Th

													nu Su th -1 ur co
									modules	The licenses Add-ons	false	Name displayName majorVersion name	D Th di Th ma Th int na
									settings	The licenses Settings	false	Name displayName groupName setting settingGroup settingGroup DisplayName	D [D D] Se di Th gr Th di [D D] Se na Th gr na
							name	Name	false	string			
							registrationToken	[DEPRECATED] token generation in dedicated endpoint - /sites/	false				

							<site_id>/ token		
						siteType	Site type	false	string
						sku	[DEPRECATED] The sku of product features active for this site	false	enum
						state	Site state	false	enum
						suite	[DEPRECATED] Use sku instead	false	enum
						totalLicenses	Total licenses	false	integer
						unlimitedExpiration	The site does not expire	false	boolean
						unlimitedLicenses	Site licenses unlimited	false	boolean
						updatedAt	Timestamp of last update	false	string
						usageType	Usage type	false	string
errors	Errors	false	array						

Create Site

POST /web/api/v2.1/sites

Create a Site. This requires an Admin role with a Global scope or Account scope that has permissions over the Account to which the Site will belong.
You must have a license for a new Site.
In the body of this request, include the policy.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
accountId	Account id	false	string
accountName	Account name	false	string
activeLicenses	Number of active licenses for the site	false	integer
createdAt	Timestamp of site creation	false	string
creator	Full name of the creating user	false	string
creatorId	Id of the creating user	false	string
description	The user-defined description for the Site	false	string

			expiration	Expiration	false	string
			externalId	Id of CRM external system	false	string
			healthStatus	Obsolete. Always true	false	boolean
			id	Site ID	false	string
			isDefault	Is default	false	boolean
			licenses	The site licenses	false	

Name	Description	Required	Value
bundles	The licenses Bundles	false	

Name	Description	Required	Value
displayName	The Bundle display name	false	string
majorVersion	The Bundle major version	false	integer
minorVersion	The Bundle minor version	false	integer
name	The Bundle internal api name	false	string
surfaces	The Surfaces in the Bundle	false	

Name	D
count	Th co in ur co
name	Th na

Name	Description	Required	Value
totalSurfaces	The total number of Surfaces in this Bundle. -1 indicates unlimited count.	false	integer

Name	Description	Required	Value
modules	The licenses Add-ons	false	

Name	Description	Required	Value
displayName	The Add-on	false	string

										display name			
									majorVersion	The Add-on major version	false	integer	
									name	The Add-on internal api name	false	string	
						settings	The licenses Settings	false					
									Name	Description	Required	Value	
									displayName	[DEPRECATED] The Setting display name	false	string	
									groupName	The Setting group name	false		
									setting	The Setting display name	false		
									settingGroup	[DEPRECATED] The Setting group name	false	string	
									settingGroupDisplayName	The Setting group display name	false	string	
			name	Name	false	string							
			registrationToken	[DEPRECATED] token generation in dedicated endpoint - /sites/<site_id>/token	false								
			siteType	Site type	false	string							
			sku	[DEPRECATED] The sku of product features active for this site	false	enum							

			state	Site state	false	enum
			suite	[DEPRECATED] Use sku instead	false	enum
			totalLicenses	Total licenses	false	integer
			unlimitedExpiration	True if the Site has no expiration date	false	
			unlimitedLicenses	True if the Site has unlimited licenses	false	boolean
			updatedAt	Timestamp of last update	false	string
			usageType	Usage type	false	string
errors	Errors	false	array			

Body Schema

Name	Description	Required	Value
data	Data	true	

Name	Description	Required	Value
name	Name	true	string
accountId	Associated account. Leave empty in single-account management consoles.	false	string
accountSfId		false	string
description	The user-defined description for the Site	false	string
expiration	Expiration	false	string
externalId	Id of CRM external system	false	string
inherits	True if the policy is inherited from Tenant, False if the site has its own edited policy	false	boolean
licenses	The license configuration for the Site	false	

Name	Description	Required	Value
bundles	The list of Bundles selected	false	

Name	Description	Required	Value
name		true	string
majorVersion		false	integer
surfaces		false	

Name	D
name	
count	Th

																	of pe -1 ur co
						modules	The list of Add-ons selected	false	Name	Description	Required	Value					
									name		true	string					
			policy	Policy is mandatory if inherits is false, else it will be ignored.	false	Name	Description	Required	Value								
						agentLoggingOn	True if logging is enabled in the agent	false	boolean								
						agentNotification	[DEPRECATED] Show end point notification on suspicious.Replaced by 'show_suspicious' in the agent UI section	false	boolean								
						agentUi	Agent ui	false	Name	Description	Required	Value					
									agentUiOn	Agent ui on	false	boolean					
									contactCompany	Contact company	false	string					
									contactDirectMessage	Contact direct message	false	string					
									contactEmail	Contact email	false	string					
									contactFreeText	Contact free text	false	string					
									contactOther	Contact other	false	string					
									contactPhoneNumber	Contact phone	false	string					

											number				
										contactSupportWebsite	Contact support website	false	string		
										devicePopUpNotifications	Device pop up notifications	false	boolean		
										maxEventAgeDays	Max event age days	false	integer		
										showAgentWarnings	Show agent warnings	false	boolean		
										showDeviceTab	Show device tab	false	boolean		
										showQuarantineTab	Show quarantine tab	false	boolean		
										showSupport	Show support	false	boolean		
										showSuspicious	Show suspicious	false	boolean		
										threatPopUpNotifications	Threat pop up notifications	false	boolean		
							agentUiOn	[DEPRECATED] Show/hide Agent UI. Moved inside the agent UI section	false	boolean					
							allowRemoteShell	True if Remote Shell is enabled for the scope	false	boolean					
							antiTamperingOn	Anti tampering on/off	false	boolean					
							autoDecommissionDays	Automatic decommission period in days	false	integer					

					autoDecommissionOn	Auto decommission on	false	boolean
					autoFileUpload	Automatic file upload configuration	false	

Name	Description	Required	Value
enabled	Automatic file upload on/off	false	boolean
includeBenignFiles	Upload benign files	false	boolean
maxDailyFileUpload	Maximum size (MB) to upload daily	false	integer
maxDailyFileUploadLimit	Limit for the maximum size (MB) to upload daily	false	integer
maxFileSize	Maximum file size (MB) to upload	false	integer
maxFileSizeLimit	Limit for the maximum file size (MB) to upload	false	integer
maxLocalDiskUsage	Maximum local disk usage (MB) for uploaded files	false	integer
maxLocalDiskUsageLimit	Limit for the maximum local disk usage (MB) for uploaded files	false	integer

					autoImmuneOn	Automatic immune on/off - this value must be true since all policies are	false	boolean

							immune by default	
						autoMitigationAction	Default action for auto mitigation	false
						cloudValidationOn	Cloud validation on	false
						createdAt	Timestamp of policy creation	false
						driverBlocking	Suspicious driver blocking engine on/off	false
						dvAttributesPerEventType	The DV attributes	false

Name	Description	Required	Value
autoInstallBrowserExtensions	Auto install browser extensions	false	
behavioralIndicators	Behavioral indicators event	false	
commandScripts	Command scripts event	false	
crossProcess	Cross process event	false

													d	
													dvEventTypeCrossProcessOpenProcess	Op Ev
													dvEventTypeCrossProcessRemoteThread	Re Th Ty
										dataMasking	Data masking	false	Name	De
													dataMasking	Da
										dllModuleLoad	DLL module load event	false	Name	De
													dvEventTypeDllModuleLoad	Dl loa
										dns	Network event - DNS	false	Name	De
													dvEventTypeDns	Ne ev
										driver	Driver	false	Name	De
													dvEventTypeDriverLoad	Dr
										file	File event	false	Name	De
													dvEventTypeFileCreation	Fil Ev
													dvEventTypeFileDeletion	Fil Ev
													dvEventTypeFileModification	Fil M Ev
													dvEventTypeFileRename	Fil Ev
													fullDiskScan	Fil Ev
										ip	Network event - IP	false	Name	De

												dvEventTypeIpConnect dvEventTypeIpListen
									login	User login/ logout event	false	Name dvEventTypeLoginLoggedIn dvEventTypeLoginLoggedOut
									namedPipe	Named Pipe	false	Name dvEventTypeNamedPipeConnection dvEventTypeNamedPipeCreation
									namedPipeExtended	Named Pipe Extended	false	Name namedPipeExtended
									process	Process event	false	Name dvEventTypeProcessCreation dvEventTypeProcessExit dvEventTypeProcessModification
									registry	Registry event	false	Name dvEventTypeRegistryKeyCr

														eated	Ev
														dvEventTypeRegistryKeyDelete	Re De Ty
														dvEventTypeRegistryKeyExport	Re Ex Ty
														dvEventTypeRegistryKeyImport	Re Im Ty
														dvEventTypeRegistryKeyRename	Re Re Ev
														dvEventTypeRegistryKeySecurityChanged	Re Se Ch Ev
														dvEventTypeRegistryValueCreated	Re Va Ev
														dvEventTypeRegistryValueDeleted	Re Va De Ev
														dvEventTypeRegistryValueModified	Re Va M Ev
										scheduledTask	Scheduled task event	false		Name	D
														dvEventTypeScheduledTaskDelete	Sc Ta Ev
														dvEventTypeScheduledTaskRegister	Sc Ta Ev
														dvEventTypeScheduledTaskStart	Sc Ta Ev

												dvEventTypeScheduledTaskTrigger	Sc Ta Ev
												dvEventTypeScheduledTaskUpdate	Sc Ta Ev
									smartFileMonitoring	Smart file monitoring	false	Name	De
												smartFileMonitoring	Sn mo
									url	URL Actions event	false	Name	De
												dvEventTypeUrl	UR ev
									windowsEventLogs	Windows Event Log	false	Name	De
												dvEventTypeWindowsEventLogCreation	W Ev Cr Ev
									windowsEventLogsExtended	Windows Event Log Extended	false	Name	De
												windowsEventLogsExtended	W Ev Ex Ev
							engines	The engines statuses	false	Name	Description	Required	Value
										applicationControl	application control	false	enum
										dataFiles	data files	false	enum
										executables	executables	false	enum
										exploits	exploits	false	enum
										lateralMovement	lateral movement	false	enum
										penetration	penetration	false	enum
										preExecution	on-write	false	enum

									preExecution Suspicious	pre execution suspicious	false	enum
									pup	potentially unwanted applications (PUP)	false	enum
									remoteShell	remote shell	false	enum
									reputation	reputation	false	enum
							forensicsAuto Triggering	Forensics auto triggering configuration	false	Name	Description	Required	Value
										linuxEnabled	True if linux forensics is enabled	false	boolean
										linuxProfileId	The profile id for the linux forensics	false	string
										linuxProfileName	The profile name for the linux forensics	false	string
										macosEnabled	True if macos forensics is enabled	false	boolean
										macosProfileId	The profile id for the macos forensics	false	string
										macosProfileName	The profile name for the macos forensics	false	string
										windowsEnabled	True if windows forensics is enabled	false	boolean
										windowsProfileId	The profile id for the windows forensics	false	string
										windowsProf	The profile	false	string

								ileName	name for the windows forensics
						identityEndpointReporting	Endpoint reporting level	false	enum
						identityOn	Identity module on/off	false	boolean
						identityReportInterval	Identity telemetry report interval in minutes	false	integer
						identityThrottlingInterval	Identity duplicate command consolidation interval in minutes	false	integer
						identityUpdateInterval	Identity update interval in minutes	false	integer
						inheritedFrom	Indicates the parent scope from which this policy is inherited, or 'null' if it is not inherited (modified specifically for the current scope).	false	enum
						ioc	True if ioc is enabled	false	boolean
						iocAttributes	The Ioc attributes	false	Name: autoInstallBr; Description: Update auto; Required: false; Value: boolean

| | | |

									yUploadLimit	maximum size to upload daily		
									maximumFileSizeUpload	Maximum size for single file	false	integer
									maximumFileSizeUploadLimit	Limit for the maximum file size to upload	false	integer
									parsedArtifactsDestination	Default destination of parsed artifacts	false	enum
							remoteScriptOrchestration	Remote script orchestration upload limits configuration	false	Name	Description	Required	Value
										alwaysUploadStreamToCloud	Always upload streams to cloud	false	boolean
										maxDailyFileDownload	Maximum size (MB) to download daily	false	integer
										maxDailyFileDownloadLimit	Limit for the maximum size (MB) to download daily	false	integer
										maxDailyFileUpload	Maximum size (MB) to upload daily	false	integer
										maxDailyFileUploadLimit	Limit for the maximum size (MB) to upload daily	false	integer
										maxFileSize	Maximum size in bytes for single file	false	integer
										maxFileSizeLimit	Limit for the maximum file	false	integer

											size (MB) to upload			
										maxLocalPackageDiskUsage	Maximum local disk usage (MB) for packages	false	integer	
										maxLocalPackageDiskUsageLimit	Limit for the maximum local disk usage (MB) for packages	false	integer	
							removeMacros	Determines if macros should be removed from macro threats	false	boolean				
							researchOn	Share data with SentinelOne	false	boolean				
							scanNewAgents	If True initiate full disk scan upon first registration	false	boolean				
							signedDriverBlockingOn	Suspicious signed driver blocking on/off	false	boolean				
							snapshotsOn	True if snapshots are enabled	false	boolean				
							unsignedDriverBlockingOn	Suspicious unsigned driver blocking on/off	false	boolean				
							updatedAt	Time of the last update to the policy	false	string				
							userFullName	The user that	false	string				

							created the policy		
						userId	The user id	false	string
			siteType	Site types	false	enum			
			sku	[DEPRECATED] Use licenses instead	false	enum			
			suite	[DEPRECATED] Use licenses instead	false	enum			
			totalLicenses	Total licenses	false	integer			
			unlimitedExpiration	Is expiration unlimited, if not expiration should be supplied	false	boolean			
			unlimitedLicenses	Is the site unlimited, if not then total_licenses must be supplied	false	boolean			

Export Sites

GET /web/api/v2.1/export/sites

Export Sites data to a CSV, for Sites that match the filter.

Parameters

accountid	optional	Account id. Example: "225494730938493804".
accountids	optional	List of Account IDs to filter by. Example: "225494730938493804,225494730938493915".
accountname__contains	optional	Free-text filter by account name (supports multiple values)
activelicenses	optional	Active licenses
adminonly	optional	Show sites the user has Admin privileges to
availablemovesites	optional	Only return sites the user can move agents to
createdat	optional	Timestamp of site creation. Example: "2018-02-27T04:49:26.257525Z".
description	optional	The description for the Site
description__contains	optional	Free-text filter by site description (supports multiple values)
expiration	optional	Expiration. Example: "2018-02-27T04:49:26.257525Z".
externalid	optional	Id in a CRM external system
features	optional	If sent return only sites that support this features. Example: "firewall-control".
healthstatus	optional	Health status
isdefault	optional	Is default
module	optional	Module. Example: "star,rso".
name	optional	Name. Example: "My Site".
name__contains	optional	Free-text filter by site name (supports multiple values)
query	optional	Full text search for fields: name, account_name, description. (Note: on single-account consoles account name will not be matched)
registrationtoken	optional	Registration token. Example: "eyJ1cmwiOiAiaHR0cHM6Ly9jb25zb2xlLnNlbnRpbmVsb25lLm5ldCIs

		ICJzaXRlX2tleSI6ICIwNzhkYjliMWUyOTA1Y2NhIn0=".
siteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".
sitetype	optional	Site type. Example: "Trial".
sku	optional	Sku. Example: "core".
state	optional	Site state. Example: "active".
states	optional	List of states to filter
suite	optional	[DEPRECATED] Use sku instead. Example: "Core".
totallicenses	optional	Total licenses
updatedat	optional	Timestamp of last update. Example: "2018-02-27T04:49:26.257525Z".

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Get Site by ID

GET /web/api/v2.1/sites/{site_id}

Get the data of the Site of the ID. To get the ID, run "sites".
The response shows the Site expiration date, SKU, licenses (total and active), token, Account name and ID, who and when it was created and changed, and its status.

Response Messages

200 - Success

401 - Unauthorized access - please sign in and retry.

404 - Site not found

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
accountId	Account id	false	string
accountName	Account name	false	string
activeLicenses	Number of active licenses for the site	false	integer
createdAt	Timestamp of site creation	false	string
creator	Full name of the creating user	false	string
creatorId	Id of the creating user	false	string
description	The user-defined description for the Site	false	string
expiration	Expiration	false	string
externalId	Id of CRM external system	false	string
healthStatus	Obsolete. Always true	false	boolean
id	Site ID	false	string
isDefault	Is default	false	boolean
licenses	The site licenses	false	

Name	Description	Required	Value
bundles	The licenses Bundles	false	

Name	Description	Required	Value
displayName	The Bundle display name	false	string
majorVersion	The Bundle major version	false	integer
minorVersion	The Bundle minor version	false	integer

									name	The Bundle internal api name	false	string
									surfaces	The Surfaces in the Bundle	false	<table><tr><th>Name</th><th>De</th></tr><tr><td>count</td><td>Th co in ur co</td></tr><tr><td>name</td><td>Th na</td></tr></table>
									totalSurfaces	The total number of Surfaces in this Bundle. -1 indicates unlimited count.	false	integer
							modules	The licenses Add-ons	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>displayName</td><td>The Add-on display name</td><td>false</td><td>string</td></tr><tr><td>majorVersion</td><td>The Add-on major version</td><td>false</td><td>integer</td></tr><tr><td>name</td><td>The Add-on internal api name</td><td>false</td><td>string</td></tr></table>
							settings	The licenses Settings	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>displayName</td><td>[DEPRECATED] The Setting display name</td><td>false</td><td>string</td></tr><tr><td>groupName</td><td>The Setting group name</td><td>false</td><td></td></tr><tr><td>setting</td><td>The Setting display name</td><td>false</td><td></td></tr><tr><td>settingGroup</td><td>[DEPRECATED] The</td><td>false</td><td>string</td></tr></table>

										Setting group name		
									settingGroupDisplayName	The Setting group display name	false	string
			name	Name	false	string						
			registrationToken	[DEPRECATED] token generation in dedicated endpoint - /sites/<site_id>/token	false							
			siteType	Site type	false	string						
			sku	[DEPRECATED] The sku of product features active for this site	false	enum						
			state	Site state	false	enum						
			suite	[DEPRECATED] Use sku instead	false	enum						
			totalLicenses	Total licenses	false	integer						
			unlimitedExpiration	The site does not expire	false	boolean						
			unlimitedLicenses	Site licenses unlimited	false	boolean						
			updatedAt	Timestamp of last update	false	string						
			usageType	Usage type	false	string						
errors	Errors	false	array									

Update Site

PUT /web/api/v2.1/sites/{site_id}

Change the policy and properties of the Site given by ID.
To get the ID, run 'sites'.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

404 - Site not found

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
accountId	Account id	false	string
accountName	Account name	false	string
activeLicenses	Number of active licenses for the site	false	integer
createdAt	Timestamp of site creation	false	string
creator	Full name of the creating user	false	string
creatorId	Id of the creating user	false	string
description	The user-defined description	false	string

				for the Site		
			expiration	Expiration	false	string
			externalId	Id of CRM external system	false	string
			healthStatus	Obsolete. Always true	false	boolean
			id	Site ID	false	string
			isDefault	Is default	false	boolean
			licenses	The site licenses	false	

Name	Description	Required	Value
bundles	The licenses Bundles	false	

Name	Description	Required	Value
displayName	The Bundle display name	false	string
majorVersion	The Bundle major version	false	integer
minorVersion	The Bundle minor version	false	integer
name	The Bundle internal api name	false	string
surfaces	The Surfaces in the Bundle	false	

Name	De
count	Th co in ur co
name	Th na

Name	Description	Required	Value
totalSurfaces	The total number of Surfaces in this Bundle. -1 indicates unlimited count.	false	integer

Name	Description	Required	Value
modules	The licenses Add-ons	false	

Name	Description	Required	Value

										displayName	The Add-on display name	false	string		
										majorVersion	The Add-on major version	false	integer		
										name	The Add-on internal api name	false	string		
								settings	The licenses Settings	false	Name	Description	Required	Value	
											displayName	[DEPRECATED] The Setting display name	false	string	
											groupName	The Setting group name	false		
											setting	The Setting display name	false		
											settingGroup	[DEPRECATED] The Setting group name	false	string	
											settingGroupDisplayName	The Setting group display name	false	string	
				name	Name	false	string								
				registrationToken	[DEPRECATED] token generation in dedicated endpoint - /sites/<site_id>/token	false									
				siteType	Site type	false	string								
				sku	[DEPRECATED] The sku of product features active for this	false	enum								

				site		
			state	Site state	false	enum
			suite	[DEPRECATED] Use sku instead	false	enum
			totalLicenses	Total licenses	false	integer
			unlimitedExpiration	True if the Site has no expiration date	false	
			unlimitedLicenses	True if the Site has unlimited licenses	false	boolean
			updatedAt	Timestamp of last update	false	string
			usageType	Usage type	false	string
errors	Errors	false	array			

Body Schema

Name	Description	Required	Value
data	Data	true	

Name	Description	Required	Value
description	The user-defined description for the Site	false	string
expiration	Expiration	false	string
externalId	Id of CRM external system	false	string
id	Site ID	false	string
inherits	True if the policy is inherited from Tenant, False if the site has its own edited policy	false	boolean
licenses	The license configuration for the Site	false	

Name	Description	Required	Value
bundles	The list of Bundles selected	false	
modules	The list of Add-ons selected	false	

Name	Description	Required	Value
name		true	string
majorVersion		false	integer
surfaces		false	

Name	Description	Required	Value
name		true	string

Name	D
name	
count	Th of pe -1 ur co

			name	Name	false	string
			policy	Policy	false	

Name	Description	Required	Value
agentLoggingOn	True if logging is enabled in the agent	false	boolean
agentNotification	[DEPRECATED] Show end point notification on suspicious.Replaced by 'show_suspicious' in the agent UI section	false	boolean
agentUi	Agent ui	false	

Name	Description	Required	Value
agentUiOn	Agent ui on	false	boolean
contactCompany	Contact company	false	string
contactDirectMessage	Contact direct message	false	string
contactEmail	Contact email	false	string
contactFreeText	Contact free text	false	string
contactOther	Contact other	false	string
contactPhoneNumber	Contact phone number	false	string
contactSupportWebsite	Contact support website	false	string
devicePopUpNotifications	Device pop up notifications	false	boolean
maxEventAge	Max event	false	integer

									Days | age days | | | showAgentWarnings | Show agent warnings | false | boolean showDeviceTab | Show device tab | false | boolean showQuarantineTab | Show quarantine tab | false | boolean showSupport | Show support | false | boolean showSuspicious | Show suspicious | false | boolean threatPopUpNotifications | Threat pop up notifications | false | boolean
						agentUiOn	[DEPRECATED] Show/hide Agent UI. Moved inside the agent UI section	false	boolean
						allowRemoteShell	True if Remote Shell is enabled for the scope	false	boolean
						antiTamperingOn	Anti tampering on/off	false	boolean
						autoDecommissionDays	Automatic decommission period in days	false	integer
						autoDecommissionOn	Auto decommission on	false	boolean
						autoFileUpload	Automatic file upload configuration	false	Name | Description | Required | Value enabled | Automatic file upload on/off | false | boolean

										includeBenignFiles	Upload benign files	false	boolean	
										maxDailyFileUpload	Maximum size (MB) to upload daily	false	integer	
										maxDailyFileUploadLimit	Limit for the maximum size (MB) to upload daily	false	integer	
										maxFileSize	Maximum file size (MB) to upload	false	integer	
										maxFileSizeLimit	Limit for the maximum file size (MB) to upload	false	integer	
										maxLocalDiskUsage	Maximum local disk usage (MB) for uploaded files	false	integer	
										maxLocalDiskUsageLimit	Limit for the maximum local disk usage (MB) for uploaded files	false	integer	
							autoImmuneOn	Automatic immune on/off - this value must be true since all policies are immune by default	false	boolean				
							autoMitigationAction	Default action for auto mitigation	false	string				
							cloudValidationOn	Cloud validation on	false					

						createdAt	Timestamp of policy creation	false	string
						driverBlocking	Suspicious driver blocking engine on/off	false	boolean
						dvAttributesPerEventType	The DV attributes	false	

Name	Description	Required	Value
autoInstallBrowserExtensions	Auto install browser extensions	false	
behavioralIndicators	Behavioral indicators event	false	
commandScripts	Command scripts event	false	
crossProcess	Cross process event	false	
dataMasking	Data masking	false	

Name	De
autoInstallBrowserExtensions	Au br ex

Name	De
dvEventTypeBehavioralIndicators	Be in ev

Name	De
dvEventTypeCommandScripts	Co sc

Name	De
dvEventTypeCrossProcessDuplicateProcess	Du Pr Ev
dvEventTypeCrossProcessDuplicateThread	Du Th Ty
dvEventTypeCrossProcessOpenProcess	Op Ev
dvEventTypeCrossProcessRemoteThread	Re Th Ty

												Name: dataMasking De: Da
									dllModuleLoad	DLL module load event	false	Name: dvEventTypeDllModuleLoad De: DI lo
									dns	Network event - DNS	false	Name: dvEventTypeDns De: Ne ev
									driver	Driver	false	Name: dvEventTypeDriverLoad De: Dr
									file	File event	false	Name: dvEventTypeFileCreation De: Fil Ev Name: dvEventTypeFileDeletion De: Fil Ev Name: dvEventTypeFileModification De: Fil M Ev Name: dvEventTypeFileRename De: Fil Ev Name: fullDiskScan De: Fil Ev
									ip	Network event - IP	false	Name: dvEventTypeIpConnect De: IP Ev Name: dvEventTypeIpListen De: IP Ev
									login	User login/ logout event	false	Name: dvEventTypeLoginLoggedIn De: Us Ev

| | | |

													egistryKeyImport dvEventTypeRegistryKeyRename dvEventTypeRegistryKeySecurityChanged dvEventTypeRegistryValueCreated dvEventTypeRegistryValueDeleted dvEventTypeRegistryValueModified
										scheduledTask	Scheduled task event	false	Name dvEventTypeScheduledTaskDelete dvEventTypeScheduledTaskRegister dvEventTypeScheduledTaskStart dvEventTypeScheduledTaskTrigger dvEventTypeScheduledTaskUpdate
										smartFileMonitoring	Smart file monitoring	false	Name

												smartFileMonitoring
									url	URL Actions event	false	Name: dvEventTypeUrl
									windowsEventLogs	Windows Event Log	false	Name: dvEventTypeWindowsEventLogCreation
									windowsEventLogsExtended	Windows Event Log Extended	false	Name: windowsEventLogsExtended
							engines	The engines statuses	false			

Name	Description	Required	Value
applicationControl	application control	false	enum
dataFiles	data files	false	enum
executables	executables	false	enum
exploits	exploits	false	enum
lateralMovement	lateral movement	false	enum
penetration	penetration	false	enum
preExecution	on-write	false	enum
preExecutionSuspicious	pre execution suspicious	false	enum
pup	potentially unwanted applications (PUP)	false	enum
remoteShell	remote shell	false	enum

									reputation reputation false enum
						forensicsAutoTriggering	Forensics auto triggering configuration	false	Name Description Required Value linuxEnabled True if linux forensics is enabled false boolean linuxProfileId The profile id for the linux forensics false string linuxProfileName The profile name for the linux forensics false string macosEnabled True if macos forensics is enabled false boolean macosProfileId The profile id for the macos forensics false string macosProfileName The profile name for the macos forensics false string windowsEnabled True if windows forensics is enabled false boolean windowsProfileId The profile id for the windows forensics false string windowsProfileName The profile name for the windows forensics false string
						identityEndpointReporting	Endpoint reporting level	false	enum
						identityOn	Identity	false	boolean

							module on/ off		
						identityReportInterval	Identity telemetry report interval in minutes	false	integer
						identityThrottlingInterval	Identity duplicate command consolidation interval in minutes	false	integer
						identityUpdateInterval	Identity update interval in minutes	false	integer
						inheritedFrom	Indicates the parent scope from which this policy is inherited, or 'null' if it is not inherited (modified specifically for the current scope).	false	enum
						ioc	True if ioc is enabled	false	boolean
						iocAttributes	The Ioc attributes	false	

Name	Description	Required	Value
autoInstallBrowserExtensions	Update auto install browser extensions	false	boolean
behavioralIndicators	Update behavioral indicators	false	boolean
commandScripts	Update command	false	boolean

										scripts				
									crossProcess	Update cross process	false	boolean		
									dataMasking	Update data masking	false	boolean		
									dllModuleLoad	Update DLL module load	false	boolean		
									dns	Network event - DNS	false	boolean		
									driver	Driver	false	boolean		
									fds	Full disk scan	false	boolean		
									file	File event	false	boolean		
									ip	Network event - IP	false	boolean		
									login	User login/ logout event	false	boolean		
									namedPipe	Named Pipe	false	boolean		
									namedPipeExtended	Named Pipe Extended	false	boolean		
									process	Process creation event	false	boolean		
									registry	Registry event	false	boolean		
									scheduledTask	Scheduled task event	false	boolean		
									smartFileMonitoring	Smart file monitoring	false	boolean		
									url	Ioc URI	false	boolean		
									windowsEventLogs	Windows Event Log	false	boolean		
									windowsEventLogsExtended	Windows Event Log Extended	false	boolean		
							iocSupported	Ioc supported for the scope	false	boolean				

						isDefault	True if this is the tenant policy	false	boolean
						isDvPolicyPerEventType	FE indication as to how to display DV policy	false	boolean
						mitigationMode	Mitigation modes	false	enum
						mitigationModeSuspicious	Mitigation mode	false	enum
						monitorOnExecute	Monitor on execute on/off	false	boolean
						monitorOnWrite	Monitor on write	false	boolean
						networkQuarantineOn	Network quarantine on	false	boolean
						remoteOpsForensics	Remote ops forensics configuration	false	

Name	Description	Required	Value
cpuLimit	CPU resources limit for collection process	false	integer
enabled	Enabled	false	boolean
maximumDailyUpload	Maximum size to upload daily	false	integer
maximumDailyUploadLimit	Limit for the maximum size to upload daily	false	integer
maximumFileSizeUpload	Maximum size for single file	false	integer
maximumFileSizeUploadLimit	Limit for the maximum file size to upload	false	integer

									parsedArtifactsDestination	Default destination of parsed artifacts	false	enum
						remoteScriptOrchestration	Remote script orchestration upload limits configuration	false				

Name	Description	Required	Value
alwaysUploadStreamToCloud	Always upload streams to cloud	false	boolean
maxDailyFileDownload	Maximum size (MB) to download daily	false	integer
maxDailyFileDownloadLimit	Limit for the maximum size (MB) to download daily	false	integer
maxDailyFileUpload	Maximum size (MB) to upload daily	false	integer
maxDailyFileUploadLimit	Limit for the maximum size (MB) to upload daily	false	integer
maxFileSize	Maximum size in bytes for single file	false	integer
maxFileSizeLimit	Limit for the maximum file size (MB) to upload	false	integer
maxLocalPackageDiskUsage	Maximum local disk usage (MB) for packages	false	integer
maxLocalPackageDiskUsageLimit	Limit for the maximum local disk	false	integer

										usage (MB) for packages			
						removeMacros	Determines if macros should be removed from macro threats	false	boolean				
						researchOn	Share data with SentinelOne	false	boolean				
						scanNewAgents	If True initiate full disk scan upon first registration	false	boolean				
						signedDriverBlockingOn	Suspicious signed driver blocking on/off	false	boolean				
						snapshotsOn	True if snapshots are enabled	false	boolean				
						unsignedDriverBlockingOn	Suspicious unsigned driver blocking on/off	false	boolean				
						updatedAt	Time of the last update to the policy	false	string				
						userFullName	The user that created the policy	false	string				
						userId	The user id	false	string				
				siteType	Site type	false	enum						
				suite	[DEPRECATED] Use	false	enum						

				licenses instead		
			totalLicenses	Total licenses	false	integer
			unlimitedExpiration	Is expiration unlimited, if not expiration should be supplied	false	boolean
			unlimitedLicenses	[DEPRECATED] True if the Site has unlimited licenses.	false	boolean

Delete Site

DELETE /web/api/v2.1/sites/{site_id}

Delete the Site of the given ID. To get the ID, run "sites".
You must have an Admin role with scope access that includes the Site.

Response Messages

200 - Success

401 - Unauthorized access - please sign in and retry.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td><table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>success</td><td>Indicates a successful operation</td><td>false</td><td>boolean</td></tr></table></td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Get Site registration token by ID

GET /web/api/v2.1/sites/{site_id}/token

Get the registration token of the Site of the ID.

Response Messages

200 - Success

401 - Unauthorized access - please sign in and retry.

404 - Site not found

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>token</td><td>Token</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Revert Policy

PUT /web/api/v2.1/sites/{site_id}/revert-policy

When a Site is created through the Console, it gets the Global policy.
If you change the policy and later want it set to the Global policy, use this command.
The site_id is required. You can get it from "sites".

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td><table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>success</td><td>Indicates a successful operation</td><td>false</td><td>boolean</td></tr></table></td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

Name	Description	Required	Value
data	Data	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>id</td><td>Id</td><td>false</td><td>string</td></tr></table>

Create duplicate site

POST /web/api/v2.1/sites/duplicate-site

[DEPRECATED] Create duplicate site.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
accountId	Account id	false	string
accountName	Account name	false	string
activeLicenses	Number of active licenses for the site	false	integer
createdAt	Timestamp of site creation	false	string
creator	Full name of the creating user	false	string
creatorId	Id of the creating user	false	string
description	The user-defined description for the Site	false	string
expiration	Expiration	false	string

			externalId	Id of CRM external system	false	string
			healthStatus	Obsolete. Always true	false	boolean
			id	Site ID	false	string
			isDefault	Is default	false	boolean
			licenses	The site licenses	false	

Name	Description	Required	Value
bundles	The licenses Bundles	false	

Name	Description	Required	Value
displayName	The Bundle display name	false	string
majorVersion	The Bundle major version	false	integer
minorVersion	The Bundle minor version	false	integer
name	The Bundle internal api name	false	string
surfaces	The Surfaces in the Bundle	false	

Name	D
count	Th co in un co
name	Th na

Name	Description	Required	Value
totalSurfaces	The total number of Surfaces in this Bundle. -1 indicates unlimited count.	false	integer

Name	Description	Required	Value
modules	The licenses Add-ons	false	

Name	Description	Required	Value
displayName	The Add-on display name	false	string

										majorVersion	The Add-on major version	false	integer		
										name	The Add-on internal api name	false	string		
							settings	The licenses Settings	false						
										Name	Description	Required	Value		
										displayName	[DEPRECATED] The Setting display name	false	string		
										groupName	The Setting group name	false			
										setting	The Setting display name	false			
										settingGroup	[DEPRECATED] The Setting group name	false	string		
										settingGroupDisplayName	The Setting group display name	false	string		
			name	Name	false	string									
			registrationToken	[DEPRECATED] token generation in dedicated endpoint - /sites/<site_id>/token	false										
			siteType	Site type	false	string									
			sku	[DEPRECATED] The sku of product features active for this site	false	enum									
			state	Site state	false	enum									

			suite	[DEPRECATED] Use sku instead	false	enum
			totalLicenses	Total licenses	false	integer
			unlimitedExpiration	True if the Site has no expiration date	false	
			unlimitedLicenses	True if the Site has unlimited licenses	false	boolean
			updatedAt	Timestamp of last update	false	string
			usageType	Usage type	false	string
errors	Errors	false	array			

Body Schema

Name	Description	Required	Value
data	Data	true	

Name	Description	Required	Value
copyUsers	If true adds the duplicated site to all source site users	true	boolean
name	New Site Name	true	string
policySource	Source of duplicate site policy	true	enum
sourceSiteId	Site ID of origin site	true	integer
policy	Policy is mandatory if policy_source is new, else it will be ignored.	false	

Name	Description	Required	Value
agentLoggingOn	True if logging is enabled in the agent	false	boolean
agentNotification	[DEPRECATED] Show end point notification on suspicious.Replaced by 'show_suspicious' in the agent UI section	false	boolean
agentUi	Agent ui	false	

Name	Description	Required	Value
agentUiOn	Agent ui on	false	boolean
contactCompany	Contact company	false	string
contactDirec	Contact	false	string

									tMessage	direct message		
									contactEmail	Contact email	false	string
									contactFreeText	Contact free text	false	string
									contactOther	Contact other	false	string
									contactPhoneNumber	Contact phone number	false	string
									contactSupportWebsite	Contact support website	false	string
									devicePopUpNotifications	Device pop up notifications	false	boolean
									maxEventAgeDays	Max event age days	false	integer
									showAgentWarnings	Show agent warnings	false	boolean
									showDeviceTab	Show device tab	false	boolean
									showQuarantineTab	Show quarantine tab	false	boolean
									showSupport	Show support	false	boolean
									showSuspicious	Show suspicious	false	boolean
									threatPopUpNotifications	Threat pop up notifications	false	boolean
							agentUiOn	[DEPRECATED] Show/hide Agent UI. Moved inside the agent UI section	false	boolean
							allowRemoteShell	True if Remote Shell	false	boolean

							is enabled for the scope		
						antiTamperingOn	Anti tampering on/off	false	boolean
						autoDecommissionDays	Automatic decommission period in days	false	integer
						autoDecommissionOn	Auto decommission on	false	boolean
						autoFileUpload	Automatic file upload configuration	false	

Name	Description	Required	Value
enabled	Automatic file upload on/off	false	boolean
includeBenignFiles	Upload benign files	false	boolean
maxDailyFileUpload	Maximum size (MB) to upload daily	false	integer
maxDailyFileUploadLimit	Limit for the maximum size (MB) to upload daily	false	integer
maxFileSize	Maximum file size (MB) to upload	false	integer
maxFileSizeLimit	Limit for the maximum file size (MB) to upload	false	integer
maxLocalDiskUsage	Maximum local disk usage (MB) for uploaded files	false	integer
maxLocalDiskUsageLimit	Limit for the maximum	false	integer

| | | |

													CommandScripts	sc
										crossProcess	Cross process event	false	Name	De
													dvEventTypeCrossProcessDuplicateProcess	Du Pr Ev
													dvEventTypeCrossProcessDuplicateThread	Du Th Ty
													dvEventTypeCrossProcessOpenProcess	Op Ev
													dvEventTypeCrossProcessRemoteThread	Re Th Ty
										dataMasking	Data masking	false	Name	De
													dataMasking	Da
										dllModuleLoad	DLL module load event	false	Name	De
													dvEventTypeDllModuleLoad	Dl lo
										dns	Network event - DNS	false	Name	De
													dvEventTypeDns	Ne ev
										driver	Driver	false	Name	De
													dvEventTypeDriverLoad	Dr
										file	File event	false	Name	De
													dvEventTypeFileCreation	Fil Ev
													dvEventTypeF	Fil

| | | |

												rocessCreatio n	Cr Ev
												dvEventTypeP rocessExit	Pr Ev
												dvEventTypeP rocessModific ation	Pr Te Ev
									registry	Registry event	false		
												dvEventTypeR egistryKeyCr eated	Re Cr Ev
												dvEventTypeR egistryKeyDel ete	Re De Ty
												dvEventTypeR egistryKeyExp ort	Re Ex Ty
												dvEventTypeR egistryKeyIm port	Re Im Ty
												dvEventType RegistryKey Rename	Re Re Ev
												dvEventTypeR egistryKeySe curityChange d	Re Se Ch Ev
												dvEventTypeR egistryValueC reated	Re Va Ev
												dvEventTypeR egistryValueD eleted	Re Va De Ev
												dvEventTypeR egistryValueM odified	Re Va M Ev

									scheduledTask	Scheduled task event	false	Name / Description dvEventTypeScheduledTaskDelete / Scheduled Task Event dvEventTypeScheduledTaskRegister / Scheduled Task Event dvEventTypeScheduledTaskStart / Scheduled Task Event dvEventTypeScheduledTaskTrigger / Scheduled Task Event dvEventTypeScheduledTaskUpdate / Scheduled Task Event
									smartFileMonitoring	Smart file monitoring	false	Name / Description smartFileMonitoring / Smart file monitoring
									url	URL Actions event	false	Name / Description dvEventTypeUrl / URL event
									windowsEventLogs	Windows Event Log	false	Name / Description dvEventTypeWindowsEventLogCreation / Windows Event Log Creation Event
									windowsEventLogsExtended	Windows Event Log Extended	false	Name / Description windowsEventLogsExtended / Windows Event Log Extended Event
							engines	The engines statuses	false	Name / Description / Required / Value		

									applicationControl	application control	false	enum
									dataFiles	data files	false	enum
									executables	executables	false	enum
									exploits	exploits	false	enum
									lateralMovement	lateral movement	false	enum
									penetration	penetration	false	enum
									preExecution	on-write	false	enum
									preExecutionSuspicious	pre execution suspicious	false	enum
									pup	potentially unwanted applications (PUP)	false	enum
									remoteShell	remote shell	false	enum
									reputation	reputation	false	enum
							forensicsAutoTriggering	Forensics auto triggering configuration	false	Name	Description	Required	Value
										linuxEnabled	True if linux forensics is enabled	false	boolean
										linuxProfileId	The profile id for the linux forensics	false	string
										linuxProfileName	The profile name for the linux forensics	false	string
										macosEnabled	True if macos forensics is enabled	false	boolean
										macosProfileId	The profile id for the macos forensics	false	string
										macosProfileName	The profile name for the	false	string

										macos forensics			
									windowsEnabled	True if windows forensics is enabled	false	boolean	
									windowsProfileId	The profile id for the windows forensics	false	string	
									windowsProfileName	The profile name for the windows forensics	false	string	
							identityEndpointReporting	Endpoint reporting level	false	enum			
							identityOn	Identity module on/off	false	boolean			
							identityReportInterval	Identity telemetry report interval in minutes	false	integer			
							identityThrottlingInterval	Identity duplicate command consolidation interval in minutes	false	integer			
							identityUpdateInterval	Identity update interval in minutes	false	integer			
							inheritedFrom	Indicates the parent scope from which this policy is inherited, or	false	enum			

							'null' if it is not inherited (modified specifically for the current scope).	
						ioc	True if ioc is enabled	false	boolean
						iocAttributes	The Ioc attributes	false

Name	Description	Required	Value
autoInstallBrowserExtensions	Update auto install browser extensions	false	boolean
behavioralIndicators	Update behavioral indicators	false	boolean
commandScripts	Update command scripts	false	boolean
crossProcess	Update cross process	false	boolean
dataMasking	Update data masking	false	boolean
dllModuleLoad	Update DLL module load	false	boolean
dns	Network event - DNS	false	boolean
driver	Driver	false	boolean
fds	Full disk scan	false	boolean
file	File event	false	boolean
ip	Network event - IP	false	boolean
login	User login/ logout event	false	boolean
namedPipe	Named Pipe	false	boolean
namedPipeEx	Named Pipe	false	boolean

										tended	Extended				
										process	Process creation event	false	boolean		
										registry	Registry event	false	boolean		
										scheduledTask	Scheduled task event	false	boolean		
										smartFileMonitoring	Smart file monitoring	false	boolean		
										url	Ioc URI	false	boolean		
										windowsEventLogs	Windows Event Log	false	boolean		
										windowsEventLogsExtended	Windows Event Log Extended	false	boolean		
							iocSupported	Ioc supported for the scope	false	boolean					
							isDefault	True if this is the tenant policy	false	boolean					
							isDvPolicyPerEventType	FE indication as to how to display DV policy	false	boolean					
							mitigationMode	Mitigation modes	false	enum					
							mitigationModeSuspicious	Mitigation mode	false	enum					
							monitorOnExecute	Monitor on execute on/off	false	boolean					
							monitorOnWrite	Monitor on write	false	boolean					
							networkQuarantineOn	Network quarantine on	false	boolean					
							remoteOpsFor	Remote ops	false	Name	Description	Required	Value		

						ensics	forensics configuration		cpuLimit	CPU resources limit for collection process	false	integer
									enabled	Enabled	false	boolean
									maximumDailyUpload	Maximum size to upload daily	false	integer
									maximumDailyUploadLimit	Limit for the maximum size to upload daily	false	integer
									maximumFileSizeUpload	Maximum size for single file	false	integer
									maximumFileSizeUploadLimit	Limit for the maximum file size to upload	false	integer
									parsedArtifactsDestination	Default destination of parsed artifacts	false	enum
						remoteScriptOrchestration	Remote script orchestration upload limits configuration	false	Name	Description	Required	Value
									alwaysUploadStreamToCloud	Always upload streams to cloud	false	boolean
									maxDailyFileDownload	Maximum size (MB) to download daily	false	integer
									maxDailyFileDownloadLimit	Limit for the maximum size (MB) to download daily	false	integer
									maxDailyFileUpload	Maximum size (MB) to	false	integer

										upload daily			
									maxDailyFileUploadLimit	Limit for the maximum size (MB) to upload daily	false	integer	
									maxFileSize	Maximum size in bytes for single file	false	integer	
									maxFileSizeLimit	Limit for the maximum file size (MB) to upload	false	integer	
									maxLocalPackageDiskUsage	Maximum local disk usage (MB) for packages	false	integer	
									maxLocalPackageDiskUsageLimit	Limit for the maximum local disk usage (MB) for packages	false	integer	
							removeMacros	Determines if macros should be removed from macro threats	false	boolean			
							researchOn	Share data with SentinelOne	false	boolean			
							scanNewAgents	If True initiate full disk scan upon first registration	false	boolean			
							signedDriverBlockingOn	Suspicious signed driver blocking on/off	false	boolean			
							snapshotsOn	True if snapshots are	false	boolean			

							enabled		
						unsignedDriverBlockingOn	Suspicious unsigned driver blocking on/off	false	boolean
						updatedAt	Time of the last update to the policy	false	string
						userFullName	The user that created the policy	false	string
						userId	The user id	false	string
			totalLicenses	Total licenses for duplicate site, will be subtracted from freelicenses of the source site	false	integer			
			unlimitedLicenses	Is the site unlimited, if not then total_licenses must be supplied	false	boolean			

Create Site and User

POST /web/api/v2.1/site-with-admin

Create a Site and an Admin role user. This requires an Admin role with a Global scope or Account scope that has permissions over the Account to which the Site will belong.
You must have a license for a new Site.
In the body of this request, include the policy and user properties.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
accountId	Account id	false	string
accountName	Account name	false	string
activeLicenses	Number of active licenses for the site	false	integer
createdAt	Timestamp of site creation	false	string
description	The user-defined description for the Site	false	string
expiration	Expiration	false	string
externalId	Id of CRM external system	false	string

			healthStatus	Obsolete. Always true	false	boolean
			id	Site ID	false	string
			isDefault	Is default	false	boolean
			licenses	The site licenses	false	

Name	Description	Required	Value
bundles	The licenses Bundles	false	

Name	Description	Required	Value
displayName	The Bundle display name	false	string
majorVersion	The Bundle major version	false	integer
minorVersion	The Bundle minor version	false	integer
name	The Bundle internal api name	false	string
surfaces	The Surfaces in the Bundle	false	

Name	D
count	Th co in ur co
name	Th na

Name	Description	Required	Value
totalSurfaces	The total number of Surfaces in this Bundle. -1 indicates unlimited count.	false	integer

Name	Description	Required	Value
modules	The licenses Add-ons	false	

Name	Description	Required	Value
displayName	The Add-on display name	false	string
majorVersion	The Add-on major version	false	integer
name	The Add-on	false	string

										internal api name			
						settings	The licenses Settings	false					
									Name	Description	Required	Value	
									displayName	[DEPRECATED] The Setting display name	false	string	
									groupName	The Setting group name	false		
									setting	The Setting display name	false		
									settingGroup	[DEPRECATED] The Setting group name	false	string	
									settingGroupDisplayName	The Setting group display name	false	string	
			name	Name	false	string							
			registrationToken	[DEPRECATED] token generation in dedicated endpoint - /sites/<site_id>/token	false								
			siteType	Site type	false	string							
			sku	[DEPRECATED] The sku of product features active for this site	false	enum							
			state	Site state	false	enum							
			suite	[DEPRECATED] Use sku instead	false	enum							

			totalLicenses	Total licenses	false	integer
			updatedAt	Timestamp of last update	false	string
			usageType	Usage type	false	string
			user	The data of the newly created site admin	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>email</td><td>Email</td><td>true</td><td>string</td></tr><tr><td>fullName</td><td>Full name</td><td>true</td><td>string</td></tr><tr><td>id</td><td>Id</td><td>false</td><td>string</td></tr><tr><td>primaryTwoFaMethod</td><td>Primary two fa method</td><td>false</td><td>string</td></tr><tr><td>twoFaEnabled</td><td>Two fa enabled</td><td>false</td><td>boolean</td></tr></table>
errors	Errors	false	array			

Body Schema

Name	Description	Required	Value
data	Data	true	

Name	Description	Required	Value
name	Name	true	string
user	The data of the admin user been created	true	

Name	Description	Required	Value
email	Email	true	string
fullName	Full name	true	string
id	Id	false	string
password	Password	false	string
primaryTwoFaMethod	Primary two fa method	false	string
twoFaEnabled	Two fa enabled	false	boolean

Name	Description	Required	Value
accountId	Associated account. Leave empty in single-account management consoles.	false	string
accountSfId		false	string
description	The user-defined description for the Site	false	string
expiration	Expiration	false	string
externalId	Id of CRM external system	false	string
inherits	True if the policy is inherited from Tenant, False if the site has its own edited policy	false	boolean

			licenses	The license configuration for the Site	false

Name	Description	Required	Value
bundles	The list of Bundles selected	false	

Name	Description	Required	Value
name		true	string
majorVersion		false	integer
surfaces		false	

Name	D
name	
count	Th of pe -1 un co

Name	Description	Required	Value
modules	The list of Add-ons selected	false	

Name	Description	Required	Value
name		true	string

			policy	Policy is mandatory if inherits is false, else it will be ignored.	false

Name	Description	Required	Value
agentLoggingOn	True if logging is enabled in the agent	false	boolean
agentNotification	[DEPRECATED] Show end point notification on suspicious.Replaced by 'show_suspicious' in the agent UI section	false	boolean
agentUi	Agent ui	false	

Name	Description	Required	Value
agentUiOn	Agent ui on	false	boolean
contactCompany	Contact company	false	string
contactDirec	Contact	false	string

									tMessage	direct message		
									contactEmail	Contact email	false	string
									contactFreeText	Contact free text	false	string
									contactOther	Contact other	false	string
									contactPhoneNumber	Contact phone number	false	string
									contactSupportWebsite	Contact support website	false	string
									devicePopUpNotifications	Device pop up notifications	false	boolean
									maxEventAgeDays	Max event age days	false	integer
									showAgentWarnings	Show agent warnings	false	boolean
									showDeviceTab	Show device tab	false	boolean
									showQuarantineTab	Show quarantine tab	false	boolean
									showSupport	Show support	false	boolean
									showSuspicious	Show suspicious	false	boolean
									threatPopUpNotifications	Threat pop up notifications	false	boolean
							agentUiOn	[DEPRECATED] Show/hide Agent UI. Moved inside the agent UI section	false	boolean
							allowRemoteShell	True if Remote Shell	false	boolean

							is enabled for the scope		
						antiTamperingOn	Anti tampering on/off	false	boolean
						autoDecommissionDays	Automatic decommission period in days	false	integer
						autoDecommissionOn	Auto decommission on	false	boolean
						autoFileUpload	Automatic file upload configuration	false	

Name	Description	Required	Value
enabled	Automatic file upload on/off	false	boolean
includeBenignFiles	Upload benign files	false	boolean
maxDailyFileUpload	Maximum size (MB) to upload daily	false	integer
maxDailyFileUploadLimit	Limit for the maximum size (MB) to upload daily	false	integer
maxFileSize	Maximum file size (MB) to upload	false	integer
maxFileSizeLimit	Limit for the maximum file size (MB) to upload	false	integer
maxLocalDiskUsage	Maximum local disk usage (MB) for uploaded files	false	integer
maxLocalDiskUsageLimit	Limit for the maximum	false	integer

											local disk usage (MB) for uploaded files				
							autoImmuneOn	Automatic immune on/off - this value must be true since all policies are immune by default	false	boolean					
							autoMitigationAction	Default action for auto mitigation	false	string					
							cloudValidationOn	Cloud validation on	false						
							createdAt	Timestamp of policy creation	false	string					
							driverBlocking	Suspicious driver blocking engine on/off	false	boolean					
							dvAttributesPerEventType	The DV attributes	false	Name	Description	Required	Value		
										autoInstallBrowserExtensions	Auto install browser extensions	false	Name	D	
													autoInstallBrowserExtensions	Au br ex	
										behavioralIndicators	Behavioral indicators event	false	Name	D	
													dvEventTypeBehavioralIndicators	Be in ev	
										commandScripts	Command scripts event	false	Name	D	
													dvEventType	Co	

| | | |

													ileDeletion	Ev
													dvEventTypeFileModification	Fil M Ev
													dvEventTypeFileRename	Fil Ev
													fullDiskScan	Fil Ev
										ip	Network event - IP	false	Name	De
													dvEventTypeIpConnect	IP Ev
													dvEventTypeIpListen	IP Ev
										login	User login/ logout event	false	Name	De
													dvEventTypeLoginLoggedIn	Us Ev
													dvEventTypeLoginLoggedOut	Us Ev
										namedPipe	Named Pipe	false	Name	De
													dvEventTypeNamedPipeConnection	Na Co Ev
													dvEventTypeNamedPipeCreation	Na Cr Ev
										namedPipeExtended	Named Pipe Extended	false	Name	De
													namedPipeExtended	Na Co Ex Ev
										process	Process event	false	Name	De
													dvEventTypeP	Pr

												rocessCreatio n dvEventTypeP rocessExit dvEventTypeP rocessModific ation
									registry	Registry event	false	Name dvEventTypeR egistryKeyCr eated dvEventTypeR egistryKeyDel ete dvEventTypeR egistryKeyExp ort dvEventTypeR egistryKeyIm port dvEventType RegistryKey Rename dvEventTypeR egistryKeySe curityChange d dvEventTypeR egistryValueC reated dvEventTypeR egistryValueD eleted dvEventTypeR egistryValueM odified

| | | |

									applicationControl	application control	false	enum
									dataFiles	data files	false	enum
									executables	executables	false	enum
									exploits	exploits	false	enum
									lateralMovement	lateral movement	false	enum
									penetration	penetration	false	enum
									preExecution	on-write	false	enum
									preExecutionSuspicious	pre execution suspicious	false	enum
									pup	potentially unwanted applications (PUP)	false	enum
									remoteShell	remote shell	false	enum
									reputation	reputation	false	enum
							forensicsAutoTriggering	Forensics auto triggering configuration	false	Name	Description	Required	Value
										linuxEnabled	True if linux forensics is enabled	false	boolean
										linuxProfileId	The profile id for the linux forensics	false	string
										linuxProfileName	The profile name for the linux forensics	false	string
										macosEnabled	True if macos forensics is enabled	false	boolean
										macosProfileId	The profile id for the macos forensics	false	string
										macosProfileName	The profile name for the	false	string

										macos forensics			
									windowsEnabled	True if windows forensics is enabled	false	boolean	
									windowsProfileId	The profile id for the windows forensics	false	string	
									windowsProfileName	The profile name for the windows forensics	false	string	
							identityEndpointReporting	Endpoint reporting level	false	enum			
							identityOn	Identity module on/off	false	boolean			
							identityReportInterval	Identity telemetry report interval in minutes	false	integer			
							identityThrottlingInterval	Identity duplicate command consolidation interval in minutes	false	integer			
							identityUpdateInterval	Identity update interval in minutes	false	integer			
							inheritedFrom	Indicates the parent scope from which this policy is inherited, or	false	enum			

							'null' if it is not inherited (modified specifically for the current scope).	
						ioc	True if ioc is enabled	false	boolean
						iocAttributes	The Ioc attributes	false

Name	Description	Required	Value
autoInstallBrowserExtensions	Update auto install browser extensions	false	boolean
behavioralIndicators	Update behavioral indicators	false	boolean
commandScripts	Update command scripts	false	boolean
crossProcess	Update cross process	false	boolean
dataMasking	Update data masking	false	boolean
dllModuleLoad	Update DLL module load	false	boolean
dns	Network event - DNS	false	boolean
driver	Driver	false	boolean
fds	Full disk scan	false	boolean
file	File event	false	boolean
ip	Network event - IP	false	boolean
login	User login/ logout event	false	boolean
namedPipe	Named Pipe	false	boolean
namedPipeEx	Named Pipe	false	boolean

									tended	Extended				
									process	Process creation event	false	boolean		
									registry	Registry event	false	boolean		
									scheduledTask	Scheduled task event	false	boolean		
									smartFileMonitoring	Smart file monitoring	false	boolean		
									url	Ioc URI	false	boolean		
									windowsEventLogs	Windows Event Log	false	boolean		
									windowsEventLogsExtended	Windows Event Log Extended	false	boolean		
							iocSupported	Ioc supported for the scope	false	boolean				
							isDefault	True if this is the tenant policy	false	boolean				
							isDvPolicyPerEventType	FE indication as to how to display DV policy	false	boolean				
							mitigationMode	Mitigation modes	false	enum				
							mitigationModeSuspicious	Mitigation mode	false	enum				
							monitorOnExecute	Monitor on execute on/off	false	boolean				
							monitorOnWrite	Monitor on write	false	boolean				
							networkQuarantineOn	Network quarantine on	false	boolean				
							remoteOpsFor	Remote ops	false	Name	Description	Required	Value	

						ensics	forensics configuration		cpuLimit	CPU resources limit for collection process	false	integer
									enabled	Enabled	false	boolean
									maximumDailyUpload	Maximum size to upload daily	false	integer
									maximumDailyUploadLimit	Limit for the maximum size to upload daily	false	integer
									maximumFileSizeUpload	Maximum size for single file	false	integer
									maximumFileSizeUploadLimit	Limit for the maximum file size to upload	false	integer
									parsedArtifactsDestination	Default destination of parsed artifacts	false	enum
						remoteScriptOrchestration	Remote script orchestration upload limits configuration	false	Name	Description	Required	Value
									alwaysUploadStreamToCloud	Always upload streams to cloud	false	boolean
									maxDailyFileDownload	Maximum size (MB) to download daily	false	integer
									maxDailyFileDownloadLimit	Limit for the maximum size (MB) to download daily	false	integer
									maxDailyFileUpload	Maximum size (MB) to	false	integer

										upload daily			
									maxDailyFileUploadLimit	Limit for the maximum size (MB) to upload daily	false	integer	
									maxFileSize	Maximum size in bytes for single file	false	integer	
									maxFileSizeLimit	Limit for the maximum file size (MB) to upload	false	integer	
									maxLocalPackageDiskUsage	Maximum local disk usage (MB) for packages	false	integer	
									maxLocalPackageDiskUsageLimit	Limit for the maximum local disk usage (MB) for packages	false	integer	
							removeMacros	Determines if macros should be removed from macro threats	false	boolean			
							researchOn	Share data with SentinelOne	false	boolean			
							scanNewAgents	If True initiate full disk scan upon first registration	false	boolean			
							signedDriverBlockingOn	Suspicious signed driver blocking on/off	false	boolean			
							snapshotsOn	True if snapshots are	false	boolean			

							enabled		
						unsignedDriverBlockingOn	Suspicious unsigned driver blocking on/off	false	boolean
						updatedAt	Time of the last update to the policy	false	string
						userFullName	The user that created the policy	false	string
						userId	The user id	false	string
			siteType	Site types	false	enum			
			sku	[DEPRECATED] Use licenses instead	false	enum			
			suite	[DEPRECATED] Use licenses instead	false	enum			
			totalLicenses	Total licenses	false	integer			
			unlimitedExpiration	Is expiration unlimited, if not expiration should be supplied	false	boolean			
			unlimitedLicenses	Is the site unlimited, if not then total_licenses must be supplied	false	boolean			

Regenerate Site Key

PUT /web/api/v2.1/sites/{site_id}/regenerate-key

Regenerate the key for the given Site.
To get the site_id, use "sites".

Response Messages

200 - Success

401 - Unauthorized access - please sign in and retry.

403 - No permission for regenerating a key.

404 - Site not found

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>registrationToken</td><td>Registration token</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Reactivate Site

PUT /web/api/v2.1/sites/{site_id}/reactivate

Reactivate an expired Site.
You must have an Admin role with scope access that includes this Site, and you must have a license for the Site.
To get the site_id, run "sites".

Response Messages

200 - Site reactivated

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

404 - Site not found

Response Schema

Name	Description	Required	Value
data	Response data	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>success</td><td>Indicates a successful operation</td><td>false</td><td>boolean</td></tr></table>
errors	Errors	false	array

Body Schema

Name	Description	Required	Value
data	Data	true	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>expiration</td><td>New expiration date for the site</td><td>false</td><td>string</td></tr><tr><td>unlimited</td><td>If false an expiration should be supplied</td><td>false</td><td>boolean</td></tr></table>

Expire Site

POST /web/api/v2.1/sites/{site_id}/expire-now

Expire the Site of the given ID (run "sites" to get the ID).
You must have an Admin role with scope access that includes this Site.

Response Messages

200 - Expire site now

401 - Unauthorized access - please sign in and retry.

404 - Site not found

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
accountId	Account id	false	string
accountName	Account name	false	string
activeLicenses	Number of active licenses for the site	false	integer
createdAt	Timestamp of site creation	false	string
creator	Full name of the creating user	false	string
creatorId	Id of the creating user	false	string
description	The user-defined description for the Site	false	string
expiration	Expiration	false	string

			externalId	Id of CRM external system	false	string
			healthStatus	Obsolete. Always true	false	boolean
			id	Site ID	false	string
			isDefault	Is default	false	boolean
			licenses	The site licenses	false	

Name	Description	Required	Value
bundles	The licenses Bundles	false	

Name	Description	Required	Value
displayName	The Bundle display name	false	string
majorVersion	The Bundle major version	false	integer
minorVersion	The Bundle minor version	false	integer
name	The Bundle internal api name	false	string
surfaces	The Surfaces in the Bundle	false	

Name	D
count	Th co in un co
name	Th na

Name	Description	Required	Value
totalSurfaces	The total number of Surfaces in this Bundle. -1 indicates unlimited count.	false	integer

Name	Description	Required	Value
modules	The licenses Add-ons	false	

Name	Description	Required	Value
displayName	The Add-on display name	false	string

										majorVersion	The Add-on major version	false	integer		
										name	The Add-on internal api name	false	string		
							settings	The licenses Settings	false	Name	Description	Required	Value		
										displayName	[DEPRECATED] The Setting display name	false	string		
										groupName	The Setting group name	false			
										setting	The Setting display name	false			
										settingGroup	[DEPRECATED] The Setting group name	false	string		
										settingGroupDisplayName	The Setting group display name	false	string		
			name	Name	false	string									
			registrationToken	[DEPRECATED] token generation in dedicated endpoint - /sites/<site_id>/token	false										
			siteType	Site type	false	string									
			sku	[DEPRECATED] The sku of product features active for this site	false	enum									
			state	Site state	false	enum									

			suite	[DEPRECATED] Use sku instead	false	enum
			totalLicenses	Total licenses	false	integer
			unlimitedExpiration	True if the Site has no expiration date	false	
			unlimitedLicenses	True if the Site has unlimited licenses	false	boolean
			updatedAt	Timestamp of last update	false	string
			usageType	Usage type	false	string
errors	Errors	false	array			

Update Sites

PUT /web/api/v2.1/sites/update-bulk

Change the properties of the Sites given by IDs.
To get the IDs, run 'sites'.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
data	Response data	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>affected</td><td>Number of entities affected by the requested operation</td><td>false</td><td>integer</td></tr></table>
errors	Errors	false	array

Body Schema

Name	Description	Required	Value
data	Data	true	

Name	Description	Required	Value
description	The description for the Site	false	string
expiration	Expiration	false	string
inherits	True if the policy is inherited from Account, False is not supported in bulk update	false	boolean
licenses	The licenses configuration for the sites	false	
siteType	Site type	false	enum
unlimitedExpiration	Is expiration unlimited	false	boolean

Name	Description	Required	Value
bundles	The list of Bundles selected	false	

Name	Description	Required	Value
name		true	string
majorVersion		false	integer
surfaces		false	

Name	Description
name	
count	Th of pe -1 un co

filter	Filter	true	

Name	Description	Required	Value
accountId	Account id	false	string
accountIds	List of Account IDs	false	string []

				to filter by		
			accountName__contains	Free-text filter by account name (supports multiple values)	false	string []
			activeLicenses	Active licenses	false	integer
			adminOnly	Show sites the user has Admin privileges to	false	boolean
			availableMoveSites	Only return sites the user can move agents to	false	boolean
			createdAt	Timestamp of site creation	false	string
			description	The description for the Site	false	string
			description__contains	Free-text filter by site description (supports multiple values)	false	string []
			expiration	Expiration	false	string
			externalId	Id in a CRM external system	false	string
			features	If sent return only sites that support this features	false	string []
			healthStatus	Health status	false	boolean
			isDefault	Is default	false	boolean
			module	Module	false	string

			name	Name	false	string
			name__contains	Free-text filter by site name (supports multiple values)	false	string []
			query	Full text search for fields: name, account_name, description. (Note: on single-account consoles account name will not be matched)	false	string
			registrationToken	Registration token	false	string
			siteIds	List of Site IDs to filter by	false	string []
			siteType	Site type	false	enum
			sku	Sku	false	string
			state	Site state	false	enum
			states	List of states to filter	false	string []
			suite	[DEPRECATED] Use sku instead	false	enum
			totalLicenses	Total licenses	false	integer
			updatedAt	Timestamp of last update	false	string

Get local upgrade site authorization

GET /web/api/v2.1/sites/{site_id}/local-authorization

Get the time when authorization of local upgrades expires, and the number of Agents authorized for local upgrade, in this Site.

Response Messages

200 - Success

401 - Unauthorized access - please sign in and retry.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>authorizedAgents</td><td>Authorized agents</td><td>false</td><td>integer</td></tr>
<tr><td>siteAuthorization</td><td>Site authorization</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Edit local upgrade site authorization

PUT /web/api/v2.1/sites/{site_id}/local-authorization

Edit when authorization of local upgrades expires. Returns the number of Agents authorized for local upgrade, in this Site.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>authorizedAgents</td><td>Authorized agents</td><td>false</td><td>integer</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

Name	Description	Required	Value
siteAuthorization	New expiration date for site local upgrades authorization	false	string

Get a CSV file of local upgrade site authorization data

GET /web/api/v2.1/sites/{site_id}/local-upgrade-approved-agents-csv

Get a CSV file containing the Agents authorized for local upgrade, in this Site.

Response Messages

200 - Success

401 - Unauthorized access - please sign in and retry.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>authorizedAgents</td><td>Authorized agents</td><td>false</td><td>integer</td></tr>
<tr><td>siteAuthorization</td><td>Site authorization</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

System

System Info

GET /web/api/v2.1/system/info

Get the Console build, version, patch, and release information.

Response Messages

200 - Success

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
data	Response data	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>build</td><td>Build</td><td>false</td><td>string</td></tr><tr><td>latestAgentVersion</td><td>Latest agent version</td><td>false</td><td>string</td></tr><tr><td>patch</td><td>Patch</td><td>false</td><td>string</td></tr><tr><td>release</td><td>Release</td><td>false</td><td>string</td></tr><tr><td>version</td><td>Version</td><td>false</td><td>string</td></tr></table>
errors	Errors	false	array

System Status

GET /web/api/v2.1/system/status

Get an indication of the system's health status.
This command returns a positive response when the Management Console and API server are up and running. This command does not require authentication.
Rate limit: 1 call per second for each IP address that communicates with the Console.

Response Messages

200 - Success

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>health</td><td>System health indicator. Always returns "ok" when it is up and running</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Database Status

GET /web/api/v2.1/system/status/db

[DEPRECATED] Works the same way as "System Status" endpoint.
This command does not require authentication.
Rate limit: 1 call per second for each IP address that communicates with the Console.

Response Messages

200 - Success

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>health</td><td>System health indicator. Always returns "ok" when it is up and running</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Cache Status

GET /web/api/v2.1/system/status/cache

[DEPRECATED] Works the same way as "System Status" endpoint.
This command does not require authentication.
Rate limit: 1 call per second for each IP address that communicates with the Console.

Response Messages

200 - Success

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>health</td><td>System health indicator. Always returns "ok" when it is up and running</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Get System Config

GET /web/api/v2.1/system/configuration

Get the configuration of your SentinelOne system.
The response shows basic information of the deployed SKUs and licenses, 2FA, and the Management URL.

Parameters

accountids	optional	List of Account IDs to filter by. Example: "225494730938493804,225494730938493915".
siteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
accessibleUrl	External DNS name of the management	false	string
advancedMode	True if advanced mode is enabled.	false	boolean
advancedModeAllowChanges	True if advanced mode value can be updated from this scope.	false	boolean

			allowDuplicateSite	[DEPRECATED] Allow site admins to duplicate sites in their accounts	false	boolean
			allowedDomains	list of allowed domains for user creation.	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>domain</td><td>Allowed domain name for user creation.</td><td>false</td><td>string</td></tr><tr><td>inherited</td><td>True if this is an inherited domain</td><td>false</td><td>boolean</td></tr></table>
			cloudIntelligenceOn	[DEPRECATED] Cloud intelligence on	false	boolean
			cloudLastConnectionTime	Cloud last connection time	false	string
			earlyAccess	True if early access mode is enabled.	false	boolean
			earlyAccessPlatforms	Early access platforms	false	string []
			globalSalesforceId	salesforce id field of tenant	false	string
			globalSharedConsole	shared console field of tenant	false	boolean
			globalTwoFaEnabled	Global two fa enabled	false	boolean
			licenses	List of available licenses	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>bundles</td><td>The licenses Bundles</td><td>false</td><td><table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>displayName</td><td>The Bundle display name</td><td>false</td><td>string</td></tr></table></td></tr></table>

									majorVersion	The Bundle major version	false	integer
									minorVersion	The Bundle minor version	false	integer
									name	The Bundle internal api name	false	string
									surfaces	The Surfaces in the Bundle	false	Name / D count / Th co in ur co name / Th na
									totalSurfaces	The total number of Surfaces in this Bundle. -1 indicates unlimited count.	false	integer
							modules	The licenses Add-ons	false	Name / Description / Required / Value displayName / The Add-on display name / false / string majorVersion / The Add-on major version / false / integer name / The Add-on internal api name / false / string
							settings	The licenses Settings	false	Name / Description / Required / Value displayName / [DEPRECATED] The Setting display name / false / string groupName / The Setting group name / false /

										setting	The Setting display name	false			
										settingGroup	[DEPRECATED] The Setting group name	false	string		
										settingGroupDisplayName	The Setting group display name	false	string		
			maxCompleteLicenses	[DEPRECATED] Complete Licenses	false	integer									
			maxControlLicenses	[DEPRECATED] Control licenses	false	integer									
			maxCoreLicenses	[DEPRECATED] Core licenses	false	integer									
			passwordExpiration	Time in days until a user password expires	false	integer									
			passwordExpirationRange	Password expiration range (read-only)	false	Name	Description	Required	Value						
						max	Maximum time in days until a user password expires	false	integer						
						min	Minimum time in days until a user password expires	false	integer						
			region	The region of the management	false	string									
			rememberMeLength	Time in minutes until a user session	false	integer									

				expires		
			rememberMeLengthRange	Remember me length range	false	Name | Description | Required | Value max | Maximum time interval in minutes before the session expires | false | integer min | Minimum time interval in minutes before the session expires | false | integer
			scalyrUrl	The Scalyr URL that sends data to this Console.	false	string
			tfaEnrollmentExpiration	2FA enrollment expiration period	false	
			uiInactivityTimeoutSeconds	Length of UI inactivity period	false	
			uiInactivityTimeoutSecondsRange	UI inactivity timeout range	false	Name | Description | Required | Value max | Maximum ui inactivity time in seconds before the session expires | false | integer min | Minimum ui inactivity time in seconds before the session expires | false | integer

			unlimitedComplete	[DEPRECATED] True if Complete licenses is unlimited	false	boolean
			unlimitedControl	[DEPRECATED] True if Control licenses is unlimited	false	boolean
			unlimitedCore	[DEPRECATED] True if Core licenses is unlimited	false	boolean
errors	Errors	false	array			

Set System Config

PUT /web/api/v2.1/system/configuration

Change the system configuration.
Before you run this, see Get System Config.
This command requires a Global Admin user or Support.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - Insufficient permissions

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
accessibleUrl	External DNS name of the management	false	string
advancedMode	True if advanced mode is enabled.	false	boolean
advancedModeAllowChanges	True if advanced mode value can be updated from this scope.	false	boolean
allowDuplicateSite	[DEPRECATED] Allow site admins to duplicate	false	boolean

				sites in their accounts		
			allowedDomains	list of allowed domains for user creation.	false	
			cloudIntelligenceOn	[DEPRECATED] Cloud intelligence on	false	boolean
			cloudLastConnectionTime	Cloud last connection time	false	string
			earlyAccess	True if early access mode is enabled.	false	boolean
			earlyAccessPlatforms	Early access platforms	false	string []
			globalSalesforceId	salesforce id field of tenant	false	string
			globalSharedConsole	shared console field of tenant	false	boolean
			globalTwoFaEnabled	Global two fa enabled	false	boolean
			licenses	List of available licenses	false	

Name	Description	Required	Value
domain	Allowed domain name for user creation.	false	string
inherited	True if this is an inherited domain	false	boolean

Name	Description	Required	Value
bundles	The licenses Bundles	false	

Name	Description	Required	Value
displayName	The Bundle display name	false	string
majorVersion	The Bundle major version	false	integer
minorVersion	The Bundle	false	integer

										minor version		
									name	The Bundle internal api name	false	string
									surfaces	The Surfaces in the Bundle	false	
									totalSurfaces	The total number of Surfaces in this Bundle. -1 indicates unlimited count.	false	integer
							modules	The licenses Add-ons	false			
							settings	The licenses Settings	false			

Name	Description	Required	Value
count	Th co in ur co		
name	Th na		

Name	Description	Required	Value
displayName	The Add-on display name	false	string
majorVersion	The Add-on major version	false	integer
name	The Add-on internal api name	false	string

Name	Description	Required	Value
displayName	[DEPRECATED] The Setting display name	false	string
groupName	The Setting group name	false	
setting	The Setting display name	false	

										settingGroup	[DEPRECATED] The Setting group name	false	string		
										settingGroupDisplayName	The Setting group display name	false	string		
			maxCompleteLicenses	[DEPRECATED] Complete Licenses	false	integer									
			maxControlLicenses	[DEPRECATED] Control licenses	false	integer									
			maxCoreLicenses	[DEPRECATED] Core licenses	false	integer									
			passwordExpiration	Time in days until a user password expires	false	integer									
			passwordExpirationRange	Password expiration range (read-only)	false	Name	Description	Required	Value						
						max	Maximum time in days until a user password expires	false	integer						
						min	Minimum time in days until a user password expires	false	integer						
			region	The region of the management	false	string									
			rememberMeLength	Time in minutes until a user session expires	false	integer									
			rememberMeL	Remember	false										

			engthRange	me length range		Name | Description | Required | Value max | Maximum time interval in minutes before the session expires | false | integer min | Minimum time interval in minutes before the session expires | false | integer
			scalyrUrl	The Scalyr URL that sends data to this Console.	false	string
			tfaEnrollment Expiration	2FA enrollment expiration period	false	
			uiInactivityT imeoutSecon ds	Length of UI inactivity period	false	
			uiInactivity TimeoutSeco ndsRange	UI inactivity timeout range	false	Name | Description | Required | Value max | Maximum ui inactivity time in seconds before the session expires | false | integer min | Minimum ui inactivity time in seconds before the session expires | false | integer
			unlimitedCom	[DEPRECATE	false	boolean

			plete	D] True if Complete licenses is unlimited		
			unlimitedControl	[DEPRECATED] True if Control licenses is unlimited	false	boolean
			unlimitedCore	[DEPRECATED] True if Core licenses is unlimited	false	boolean
errors	Errors	false	array			

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accessibleUrl</td><td>External DNS name of the management</td><td>false</td><td>string</td></tr>
<tr><td>advancedMode</td><td>Advanced mode</td><td>false</td><td>boolean</td></tr>
<tr><td>allowDuplicateSite</td><td>[DEPRECATED] Allow site admins to duplicate sites in their accounts</td><td>false</td><td>boolean</td></tr>
<tr><td>allowedDomains</td><td>list of allowed domains for user creation.</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>domain</td><td>Allowed domain name for user creation.</td><td>false</td><td>string</td></tr>
<tr><td>inherited</td><td>True if this is an inherited domain</td><td>false</td><td>boolean</td></tr>
</table>
</td></tr>
<tr><td>cloudIntelligenceOn</td><td>[DEPRECATED] Cloud intelligence on</td><td>false</td><td>boolean</td></tr>
<tr><td>cloudLastConnectionTime</td><td>Cloud last connection time</td><td>false</td><td>string</td></tr>
<tr><td>earlyAccess</td><td>Early access</td><td>false</td><td>boolean</td></tr>
<tr><td>earlyAccessPlatforms</td><td>Early access platforms</td><td>false</td><td>string []</td></tr>
<tr><td>globalTwoFaEnabled</td><td>Global two fa enabled</td><td>false</td><td>boolean</td></tr>
<tr><td>passwordExpiration</td><td>Time in days until a user password expires</td><td>false</td><td>integer</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><td></td><td></td><td></td><td>
<table>
<tr><td>rememberMeLength</td><td>Time in minutes until a user session expires</td><td>false</td><td>integer</td></tr>
<tr><td>tfaEnrollmentExpiration</td><td>2FA expiration period</td><td>false</td><td></td></tr>
<tr><td>uiInactivityTimeoutSeconds</td><td>Length of UI inactivity period</td><td>false</td><td></td></tr>
</table>
</td></tr>
<tr><td>filter</td><td>Filter section determines the configuration scope. Provide a site ID or leave empty for global configuration.</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>siteIds</td><td>List of Site IDs to filter by</td><td>false</td><td>string []</td></tr>
</table>
</td></tr>
</table>

System Environment

GET /web/api/v2.1/system/env

Get environment details of the system

Response Messages

200 - Success

Response Schema

Name	Description	Required	Value
data	Response data	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>env</td><td>Env</td><td>false</td><td>string</td></tr><tr><td>isProd</td><td>Is prod</td><td>false</td><td>boolean</td></tr><tr><td>url</td><td>Url</td><td>false</td><td>string</td></tr></table>
errors	Errors	false	array

Tag Manager

Create a new endpoint tag

POST /web/api/v2.1/tag-manager

Each tag must contain a type (endpoints) and key, Value is optional but recommended. A description is optional.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
createdAt	Created at	false	string
createdById	A reference to the user which created the tag	false	string
description	Description	false	string
id	Tag ID	false	string
key	Key	false	string
scopeId	An ID reference to the containing scope	false	string
scopeLevel	Name of	false	string

			scope		
			type	e.g: manual-tagging	false	string
			updatedAt	Updated at	false	string
			updatedById	A reference to the user which updated the tag	false	string
			value	Value	false	string
errors	Errors	false	array

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>filter</td><td>Filter</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>groupIds</td><td>List of Group IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>siteIds</td><td>List of Site IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>tenant</td><td>Indicates a tenant scope request</td><td>false</td><td>boolean</td></tr>
</table>
</td></tr>
<tr><td>data</td><td>Data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>key</td><td>Key</td><td>true</td><td>string</td></tr>
<tr><td>type</td><td>Type</td><td>true</td><td>string</td></tr>
<tr><td>value</td><td>Value</td><td>true</td><td>string</td></tr>
<tr><td>description</td><td>Description</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
</table>

Delete tags

DELETE /web/api/v2.1/tag-manager

Delete all tags that match the filters.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>affected</td><td>Number of entities affected by the requested operation</td><td>false</td><td>integer</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>filter</td><td>Filter</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>groupIds</td><td>List of Group IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>includeChildren</td><td>Return tags from children scope levels</td><td>false</td><td>boolean</td></tr>
<tr><td>includeParents</td><td>Return tags from parent scope levels</td><td>false</td><td>boolean</td></tr>
<tr><td>query</td><td>Free text search on fields key, value, description</td><td>false</td><td>string</td></tr>
<tr><td>siteIds</td><td>List of Site IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>tagIds</td><td>List of tag IDs</td><td>false</td><td>string []</td></tr>
<tr><td>tenant</td><td>Indicates a tenant scope request</td><td>false</td><td>boolean</td></tr>
</table>
</td></tr>
</table>

Edit an existing tag

PUT /web/api/v2.1/tag-manager/{tag_id}

Change the key, value, or description of a tag.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
createdAt	Created at	false	string
createdById	A reference to the user which created the tag	false	string
description	Description	false	string
id	Tag ID	false	string
key	Key	false	string
scopeId	An ID reference to the containing scope	false	string
scopeLevel	Name of scope	false	string
type	e.g: manual-tagging	false	string
updatedAt	Updated at	false	string

			updatedById: A reference to the user which updated the tag — false — string value: Value — false — string
errors	Errors	false	array

Body Schema

Name	Description	Required	Value
data	Data	true	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>description</td><td>Description</td><td>false</td><td>string</td></tr><tr><td>key</td><td>Key</td><td>false</td><td>string</td></tr><tr><td>value</td><td>Value</td><td>false</td><td>string</td></tr></table>

Tags

Get Tags

GET /web/api/v2.1/tags

Get tags.

Parameters

type	required	Type in. Example: "firewall".
accountids	optional	List of Account IDs to filter by. Example: "225494730938493804,225494730938493915".
countonly	optional	If true, only total number of items will be returned, without any of the actual objects.
cursor	optional	Cursor position returned by the last request. Use to iterate over more than 1000 items. Example: "YWdlbnRfaWQ6NTgwMjkzODE=".
disablepagination	optional	If true, all tags for requested filters will be returned
groupids	optional	List of Group IDs to filter by. Example: "225494730938493804,225494730938493915".
ids	optional	List of IDs to filter by. Example: "225494730938493804,225494730938493915".
kind	optional	Returns tags of this specific kind
limit	optional	Limit number of returned items (1-1000). Example: "10".
name__contains	optional	Free-text filter by tag name. Example: "tag_name,tag_na".
onlyparents	optional	If true returns all tags possible to inherit from parent scopes, otherwise returns all tags already inherited and tags from this scope.
query	optional	Free text search on tag name
scope	optional	Return tags from given scope level. Example: "account".
siteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".
skip	optional	Skip first number of items (0-1000). To iterate over more than 1000

		items, use "cursor". Example: "150".
skipcount	optional	If true, total number of items will not be calculated, which speeds up execution time.
sortby	optional	The column to sort the results by. Example: "id".
sortorder	optional	Sort direction. Example: "asc".
tenant	optional	Indicates a tenant scope request

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>pagination</td><td>Pagination information</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>totalItems</td><td>Total number of items found matching your query</td><td>true</td><td>integer</td></tr>
<tr><td>nextCursor</td><td>Pass this value as "cursor" on your next request, to get the next page of results (Will be "null" when last page reached)</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>type</td><td>Type</td><td>true</td><td>enum</td></tr>
</table>
</td></tr>
</table>

			affectedScopes: Affected scopes; false; integer createdAt: Timestamp of site creation; false; string creator: Location creator name; false; string creatorId: Location creator ID; false; string description: Description; false; string id: Id; false; string kind: Kind is a MGMT side indication to categorize special tags like `vulnerability`; false; string linkedRules: Linked rules; false; integer name: Name; false; string scope: Scope; false; enum scopeId: Scope id; false; string scopeName: Scope name; false; string updatedAt: Timestamp of last update; false; string updater: Location updater name; false; string updaterId: Location updater; false; string
errors	Errors	false	array

Create Tags

POST /web/api/v2.1/tags

Add tags to create user-defined logical groups.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
type	Type	true	enum
affectedScopes	Affected scopes	false	integer
createdAt	Timestamp of site creation	false	string
creator	Location creator name	false	string
creatorId	Location creator ID	false	string
description	Description	false	string
id	Id	false	string
kind	Kind is a MGMT side indication to categorize special tags like `vulnerability`	false	string

			linkedRules | Linked rules | false | integer name | Name | false | string scope | Scope | false | enum scopeId | Scope id | false | string scopeName | Scope name | false | string updatedAt | Timestamp of last update | false | string updater | Location updater name | false | string updaterId | Location updater | false | string
errors	Errors	false	array

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>name</td><td>Name</td><td>true</td><td>string</td></tr>
<tr><td>type</td><td>Type</td><td>true</td><td>enum</td></tr>
<tr><td>description</td><td>Description</td><td>false</td><td>string</td></tr>
<tr><td>id</td><td>Id</td><td>false</td><td>string</td></tr>
<tr><td>kind</td><td>Kind</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>filter</td><td>Filter</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>groupIds</td><td>List of Group IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>siteIds</td><td>List of Site IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>tenant</td><td>Indicates a tenant scope request</td><td>false</td><td>boolean</td></tr>
</table>
</td></tr>
</table>

Delete Tags

DELETE /web/api/v2.1/tags

Delete tags by given filter.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
data	Response data	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>affected</td><td>Number of entities affected by the requested operation</td><td>false</td><td>integer</td></tr></table>
errors	Errors	false	array

Body Schema

Name	Description	Required	Value
filter	Filter	false	

Name	Description	Required	Value
accountIds	List of Account IDs to filter by	false	string []
groupIds	List of Group IDs to filter by	false	string []
ids	List of IDs to filter by	false	string []
kind	Returns tags of this specific kind	false	string
name__contains	Free-text filter by tag name	false	string []
onlyParents	If true returns all tags possible to inherit from parent scopes, otherwise returns all tags already inherited and tags from this scope.	false	boolean
query	Free text search on tag name	false	string
scope	Return tags from given scope level	false	enum
siteIds	List of Site IDs to filter by	false	string []
tenant	Indicates a	false	boolean

				tenant scope request		
			type	Type in	false	string []

Delete Tag by ID

DELETE /web/api/v2.1/tags/{tag_id}

Delete tag by ID.

Response Messages

200 - Success

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
data	Response data	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>affected</td><td>Number of entities affected by the requested operation</td><td>false</td><td>integer</td></tr></table>
errors	Errors	false	array

Edit Tag

PUT /web/api/v2.1/tags/{tag_id}

Edit tag

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
data	Response data	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>type</td><td>Type</td><td>true</td><td>enum</td></tr><tr><td>affectedScopes</td><td>Affected scopes</td><td>false</td><td>integer</td></tr><tr><td>createdAt</td><td>Timestamp of site creation</td><td>false</td><td>string</td></tr><tr><td>creator</td><td>Location creator name</td><td>false</td><td>string</td></tr><tr><td>creatorId</td><td>Location creator ID</td><td>false</td><td>string</td></tr><tr><td>description</td><td>Description</td><td>false</td><td>string</td></tr><tr><td>id</td><td>Id</td><td>false</td><td>string</td></tr><tr><td>kind</td><td>Kind is a MGMT side indication to categorize special tags like `vulnerability`</td><td>false</td><td>string</td></tr></table>

			linkedRules | Linked rules | false | integer name | Name | false | string scope | Scope | false | enum scopeId | Scope id | false | string scopeName | Scope name | false | string updatedAt | Timestamp of last update | false | string updater | Location updater name | false | string updaterId | Location updater | false | string
errors	Errors	false	array

Body Schema

Name	Description	Required	Value
data	Data	true	

Name	Description	Required	Value
description	Description	false	string
id	Id	false	string
kind	Kind	false	string
name	Name	false	string

Tasks

Get Task Configuration

GET /web/api/v2.1/tasks-configuration

Get the task configuration of a scope.

Parameters

tasktype	required	Task type. Example: "agents_upgrade".
accountids	optional	List of Account IDs to filter by. Example: "225494730938493804,225494730938493915".
countonly	optional	If true, only total number of items will be returned, without any of the actual objects.
cursor	optional	Cursor position returned by the last request. Use to iterate over more than 1000 items. Example: "YWdlbnRfaWQ6NTgwMjkzODE=".
groupids	optional	List of Group IDs to filter by. Example: "225494730938493804,225494730938493915".
limit	optional	Limit number of returned items (1-1000). Example: "10".
siteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".
skip	optional	Skip first number of items (0-1000). To iterate over more than 1000 items, use "cursor". Example: "150".
skipcount	optional	If true, total number of items will not be calculated, which speeds up execution time.
sortby	optional	The column to sort the results by. Example: "id".
sortorder	optional	Sort direction. Example: "asc".
tenant	optional	Indicates a tenant scope request

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - Insufficient permissions

404 - Configuration not found

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>inheritParentConcurrencyConfig</td><td>Inherit parent's scope Max Concurrent configuration</td><td>true</td><td>boolean</td></tr>
<tr><td>inheritParentMaintenanceConfig</td><td>Inherit parent's scope Maintenance windows configuration</td><td>true</td><td>boolean</td></tr>
<tr><td>maxConcurrent</td><td>Max concurrent</td><td>true</td><td>integer</td></tr>
<tr><td>timezoneGmt</td><td>Timezone gmt</td><td>true</td><td>string</td></tr>
<tr><td>concurrencyConfigUpdatedAt</td><td>Timestamp of last concurrency configuration update</td><td>false</td><td>string</td></tr>
<tr><td>concurrencyConfigUpdatedBy</td><td>User name of last updated concurrency configuration</td><td>false</td><td>string</td></tr>
<tr><td>maintenanceConfigUpdatedAt</td><td>Timestamp of last maintenance configuration update</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
</table>

			maintenanceConfigUpdatedBy: User name of last updated maintenance configuration; false; string maintenanceWindowsByDay: Stores the maintenance time for each day; false; object parentMaxConcurrent: scope's parent max concurrent limit, must not exceed; false; integer taskType: Defines task's type and priority; false; enum
errors	Errors	false	array

Create Task

PUT /web/api/v2.1/tasks-configuration

Create a task configuration.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - Operation is not allowed

404 - Configuration not found

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
inheritParentConcurrencyConfig	Inherit parent's scope Max Concurrent configuration	true	boolean
inheritParentMaintenanceConfig	Inherit parent's scope Maintenance windows configuration	true	boolean
maxConcurrent	Max concurrent	true	integer
timezoneGmt	Timezone gmt	true	string
concurrencyConfigUpdated	Timestamp of last	false	string

			At concurrency configuration update concurrencyConfigUpdatedBy User name of last updated concurrency configuration false string maintenanceConfigUpdatedAt Timestamp of last maintenance configuration update false string maintenanceConfigUpdatedBy User name of last updated maintenance configuration false string maintenanceWindowsByDay Stores the maintenance time for each day false object parentMaxConcurrent scope's parent max concurrent limit, must not exceed false integer taskType Defines task's type and priority false enum
errors	Errors	false	array

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>inheritParentConcurrencyConfig</td><td>Inherit parent's scope Max Concurrent configuration</td><td>true</td><td>boolean</td></tr>
<tr><td>inheritParentMaintenanceConfig</td><td>Inherit parent's scope Maintenance windows configuration</td><td>true</td><td>boolean</td></tr>
<tr><td>maxConcurrent</td><td>Max concurrent</td><td>true</td><td>integer</td></tr>
<tr><td>timezoneGmt</td><td>Timezone gmt</td><td>true</td><td>string</td></tr>
<tr><td>maintenanceWindowsByDay</td><td>Stores the maintenance time for each day</td><td>false</td><td>object</td></tr>
</table>
</td></tr>
<tr><td>filter</td><td>Filter</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>taskType</td><td>Defines task's type and priority</td><td>true</td><td>enum</td></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>groupIds</td><td>List of Group IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>siteIds</td><td>List of Site IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>tenant</td><td>Indicates a tenant scope request</td><td>false</td><td>boolean</td></tr>
</table>
</td></tr>
</table>

Has Child Scopes

GET /web/api/v2.1/tasks-configuration/has-explicit-subscope

From a given scope, see if there are scopes under it that have local, explicit tasks. The response returns True if a sub-scope has a local (not inherited) task configuration.

Parameters

tasktype	required	Task type. Example: "agents_upgrade".
accountids	optional	List of Account IDs to filter by. Example: "225494730938493804,225494730938493915".
countonly	optional	If true, only total number of items will be returned, without any of the actual objects.
cursor	optional	Cursor position returned by the last request. Use to iterate over more than 1000 items. Example: "YWdlbnRfaWQ6NTgwMjkzODE=".
groupids	optional	List of Group IDs to filter by. Example: "225494730938493804,225494730938493915".
limit	optional	Limit number of returned items (1-1000). Example: "10".
siteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".
skip	optional	Skip first number of items (0-1000). To iterate over more than 1000 items, use "cursor". Example: "150".
skipcount	optional	If true, total number of items will not be calculated, which speeds up execution time.
sortby	optional	The column to sort the results by. Example: "id".
sortorder	optional	Sort direction. Example: "asc".
tenant	optional	Indicates a tenant scope request

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - User is not allowed in this scope

404 - Configuration not found

Response Schema

Name	Description	Required	Value
data	Response data	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>flag</td><td>Returns boolean value for the request</td><td>false</td><td>boolean</td></tr></table>
errors	Errors	false	array

Get Child Scope Task Configuration

GET /web/api/v2.1/tasks-configuration/explicit-subscopes

Get the task configuration of child scopes of the given scope, if the tasks are not inherited.

Parameters

tasktype	required	Task type. Example: "agents_upgrade".
accountids	optional	List of Account IDs to filter by. Example: "225494730938493804,225494730938493915".
countonly	optional	If true, only total number of items will be returned, without any of the actual objects.
cursor	optional	Cursor position returned by the last request. Use to iterate over more than 1000 items. Example: "YWdlbnRfaWQ6NTgwMjkzODE=".
groupids	optional	List of Group IDs to filter by. Example: "225494730938493804,225494730938493915".
limit	optional	Limit number of returned items (1-1000). Example: "10".
query	optional	Query
siteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".
skip	optional	Skip first number of items (0-1000). To iterate over more than 1000 items, use "cursor". Example: "150".
skipcount	optional	If true, total number of items will not be calculated, which speeds up execution time.
sortby	optional	The column to sort the results by. Example: "id".
sortorder	optional	Sort direction. Example: "asc".
tenant	optional	Indicates a tenant scope request

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - User is not allowed in this scope

404 - Configuration not found

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>pagination</td><td>Pagination information</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>totalItems</td><td>Total number of items found matching your query</td><td>true</td><td>integer</td></tr>
<tr><td>nextCursor</td><td>Pass this value as "cursor" on your next request, to get the next page of results (Will be "null" when last page reached)</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountId</td><td>Account id</td><td>false</td><td>string</td></tr>
<tr><td>accountName</td><td>Account name</td><td>false</td><td>string</td></tr>
<tr><td>groupId</td><td>Group id</td><td>false</td><td>string</td></tr>
<tr><td>groupName</td><td>Group name</td><td>false</td><td>string</td></tr>
<tr><td>siteId</td><td>Site id</td><td>false</td><td>string</td></tr>
<tr><td>siteName</td><td>Site name</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Threat Intelligence

Get Threat Intelligence user config

GET /web/api/v2.1/threat-intelligence/user-config

Get the Threat Intelligence user config that match the filter.

Parameters

accountids	optional	List of Account IDs to filter by. Example: "4,2,6,4,1,8,0,3,0,2,1,2,0,7,3,7,6,2".
tenant	optional	Indicates a tenant scope request

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
createdAt	The time at which the user config was created in SentinelOne DB	true	string
updatedAt	The time at which the user config was last	true	string

			updated in SentinelOne DB		
			description	User defined description of the user config.	false	string
			disableThreat	The flag to disable Threat Intelligence Indicator based Threat creation for the entire account.	false	boolean
			excludeTii	Exclude tii	false	string []
			scopeId	The group/site/account id depending on the scope_level.	false	string
			scopeLevel	Scope level of the user config	false	enum
errors	Errors	false	array

Create Threat Intelligence user config

POST /web/api/v2.1/threat-intelligence/user-config

Create Threat Intelligence user config.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
createdAt	The time at which the user config was created in SentinelOne DB	true	string
updatedAt	The time at which the user config was last updated in SentinelOne DB	true	string
description	User defined description of the user config.	false	string
disableThreat	The flag to disable Threat Intelligence	false	boolean

			Indicator based Threat creation for the entire account.		
			excludeTii	Exclude tii	false	string []
			scopeId	The group/ site/account id depending on the scope_level.	false	string
			scopeLevel	Scope level of the user config	false	enum
errors	Errors	false	array			

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>description</td><td>User defined description of the user config.</td><td>false</td><td>string</td></tr>
<tr><td>disableThreat</td><td>The flag to disable Threat Intelligence Indicator based Threat creation for the entire account.</td><td>false</td><td>boolean</td></tr>
<tr><td>excludeTii</td><td>Exclude tii</td><td>false</td><td>string []</td></tr>
</table>
</td></tr>
<tr><td>filter</td><td>Filter</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>groupIds</td><td>List of Group IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>siteIds</td><td>List of Site IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>tenant</td><td>Indicates a tenant scope request</td><td>false</td><td>boolean</td></tr>
</table>
</td></tr>
</table>

Delete Threat Intelligence user config

DELETE /web/api/v2.1/threat-intelligence/user-config

Delete Threat Intelligence user config that match the filter.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>affected</td><td>Number of entities affected by the requested operation</td><td>false</td><td>integer</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

Name	Description	Required	Value
accountIds	List of Account IDs to filter by	false	string []
tenant	Indicates a tenant scope request	false	boolean

Get IOCs

GET /web/api/v2.1/threat-intelligence/iocs

Get the IOCs of a specified Account that match the filter.

Parameters

accountids	optional	List of Account IDs to filter by. Example: "4,2,6,4,1,8,0,3,0,2,1,2,0,7,3,7,6,2".
batchid	optional	Unique ID of the uploaded indicators batch. Example: "atmtn000000028a881bcf939dc6d92ab55443".
category__in	optional	The categories of the Threat Intelligence indicator, e.g. the malware type associated with the IOC
countonly	optional	If true, only total number of items will be returned, without any of the actual objects.
creationtime__gt	optional	Creation Time as set by the user greater than. Example: "2021-07-12T20:33:29.007906Z".
creationtime__gte	optional	Creation Time as set by the user greater or equal than. Example: "2021-07-13T20:33:29.007906Z".
creationtime__lt	optional	Creation Time as set by the user lesser than. Example: "2021-07-13T20:33:29.007906Z".
creationtime__lte	optional	Creation Time as set by the user lesser or equal than. Example: "2021-07-11T20:33:29.007906Z".
creator__contains	optional	Free-text filter by the user uploaded the Threat Intelligence indicator (supports multiple values). Example: "admin@sentinelone.com".
cursor	optional	Cursor position returned by the last request. Use to iterate over more than 1000 items. Example: "YWdlbnRfaWQ6NTgwMjkzODE=".
description__contains	optional	Free-text filter by the description of the indicator (supports multiple values). Example: "Malicious-activity".
externalid	optional	The unique identifier of the indicator as provided by the Threat Intelligence source. Example: "e277603e-1060-5ad4-9937-c26c97f1ca68".
limit	optional	Limit number of returned items (1-1000). Example: "10".
name__contains	optional	Free-text filter by the Indicator name (supports multiple values).

		Example: "foo.dll".
skip	optional	Skip first number of items (0-1000). To iterate over more than 1000 items, use "cursor". Example: "150".
skipcount	optional	If true, total number of items will not be calculated, which speeds up execution time.
sortby	optional	The column to sort the results by. Example: "id".
sortorder	optional	Sort direction. Example: "asc".
source	optional	List of the sources of the identified Threat Intelligence indicator. Example: "AlienVault".
tenant	optional	Indicates a tenant scope request
type	optional	The type of the Threat Intelligence indicator. Example: "IPv4".
updatedat__gt	optional	The time at which the indicator was last updated in SentinelOne DB greater than. Example: "2021-07-13T20:33:29.007906Z".
updatedat__gte	optional	The time at which the indicator was last updated in SentinelOne DB greater or equal than. Example: "2021-07-13T20:33:29.007906Z".
updatedat__lt	optional	The time at which the indicator was last updated in SentinelOne DB lesser than. Example: "2021-07-13T20:33:29.007906Z".
updatedat__lte	optional	The time at which the indicator was last updated in SentinelOne DB lesser or equal than. Example: "2021-07-13T20:33:29.007906Z".
uploadtime__gt	optional	The time at which the Threat Intelligence indicator was uploaded to SentinelOne DB greater than. Example: "2022-07-13T20:33:29.007906Z".
uploadtime__gte	optional	The time at which the Threat Intelligence indicator was uploaded to SentinelOne DB greater or equal than. Example: "2022-07-13T20:33:29.007906Z".
uploadtime__lt	optional	The time at which the Threat Intelligence indicator was uploaded to SentinelOne DB lesser than. Example: "2021-07-13T20:33:29.007906Z".
uploadtime__lte	optional	The time at which the Threat Intelligence indicator was uploaded to SentinelOne DB lesser or equal than. Example: "2022-07-13T20:33:29.007906Z".
uuids	optional	A list of unique Ids of the parent process of the indicator of compromise. Example: "2,c,f,f,a,e,8,7,1,1,9,7,f,2,0,d,8,6,4,f,e,8,3,6,3,e,e,e,6,6,5,1".
value	optional	The value of the Threat Intelligence indicator. Example:

		"175.45.176.1".

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>pagination</td><td>Pagination information</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>totalItems</td><td>Total number of items found matching your query</td><td>true</td><td>integer</td></tr>
<tr><td>nextCursor</td><td>Pass this value as "cursor" on your next request, to get the next page of results (Will be "null" when last page reached)</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>source</td><td>The source of the identified Threat Intelligence indicator</td><td>true</td><td>string</td></tr>
<tr><td>type</td><td>The type of the Threat Intelligence</td><td>true</td><td>enum</td></tr>
</table>
</td></tr>
</table>

				indicator		
			value	The value of the Threat Intelligence indicator	true	string
			batchId	Unique ID of the uploaded Threat Intelligence indicators batch	false	string
			campaignNames	Campaign names	false	string []
			category	Category	false	string []
			creationTime	The time at which the Threat Intelligence indicator was originally created (as indicated by the TI source)	false	string
			creator	The user that uploaded the Threat Intelligence indicator	false	string
			description	Description of the Threat Intelligence indicator	false	string
			externalId	The unique identifier of the indicator as provided by the Threat Intelligence source	false	string
			intrusionSets	Intrusion sets	false	string []
			labels	Labels	false	string []

			malwareNames	Malware names	false	string []
			metadata	The metadata of the Threat Intelligence indicator	false	string
			method	The comparison method used by SentinelOne to trigger the event	false	enum
			mitreTactic	Mitre tactic	false	string []
			name	Threat Intelligence indicator name	false	string
			originalRiskScore	The relative level of risk associated with the Threat Intelligence indicator. An integer between 0 and 100, inclusive.	false	integer
			pattern	The detection pattern for this Indicator (expressed as a STIX Pattern, e.g. Comparison expression/ Boolean Operators etc.)	false	string
			patternType	Characterize the pattern language that	false	string

				the indicator pattern is expressed in		
			reference	Reference	false	string []
			scope	Scope of the ioc	false	enum
			scopeId	The group/ site/account id depending on the scope. null if it is global.	false	string
			severity	The potential impact of the Threat Intelligence indicator. Designed to work based on OCSF format for scores 0-7.	false	integer
			threatActors	Threat actors	false	string []
			threatActorTypes	Threat actor types	false	string []
			updatedAt	The time at which the indicator was last updated in SentinelOne DB	false	string
			uploadTime	The time at which the Threat Intelligence indicator was uploaded to SentinelOne DB	false	string
			uuid	Unique Id of the Threat	false	string

			Intelligence indicator		
			validUntil	The date from which the indicator will no longer be monitored	false	string
errors	Errors	false	array

Create IOCs

POST /web/api/v2.1/threat-intelligence/iocs

Add an IoC to the Threat Intelligence database.
These values under data are required fields: "source", "type", "value", and "method".
"Type" and "method" must be in upper case.
The "validUntil" field is mandatory, and must contain a date, for example, 2021-03-20 09:14:47.779000. "validUntil" determines when the IOC expires.
If the expiration date ("validUntil") is left blank, by default it will be the upload date plus a default offset value:
- 14 days for IPs
- 90 days for URLs and domains
- 180 days for file hashes (SHA1, SHA256, and MD5)
The maximum offset values allowed are:
- 30 days for IPs
- 180 days for URLs and Domains
- 180 days for hashes (SHA1, SHA256, and MD5)
The upload date is when the API gets a request to create an IOC.
If the expiration date is later than the upload date plus the the maximum offset value allowed, it will be adjusted to the upload date plus the maximum offset value allowed.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
source	The source of the identified Threat Intelligence indicator	true	string
type	The type of the Threat Intelligence	true	enum

				indicator		
			value	The value of the Threat Intelligence indicator	true	string
			batchId	Unique ID of the uploaded Threat Intelligence indicators batch	false	string
			campaignNames	Campaign names	false	string []
			category	Category	false	string []
			creationTime	The time at which the Threat Intelligence indicator was originally created (as indicated by the TI source)	false	string
			creator	The user that uploaded the Threat Intelligence indicator	false	string
			description	Description of the Threat Intelligence indicator	false	string
			externalId	The unique identifier of the indicator as provided by the Threat Intelligence source	false	string
			intrusionSets	Intrusion sets	false	string []
			labels	Labels	false	string []

			malwareNames	Malware names	false	string []
			metadata	The metadata of the Threat Intelligence indicator	false	string
			method	The comparison method used by SentinelOne to trigger the event	false	enum
			mitreTactic	Mitre tactic	false	string []
			name	Threat Intelligence indicator name	false	string
			originalRiskScore	The relative level of risk associated with the Threat Intelligence indicator. An integer between 0 and 100, inclusive.	false	integer
			pattern	The detection pattern for this Indicator (expressed as a STIX Pattern, e.g. Comparison expression/ Boolean Operators etc.)	false	string
			patternType	Characterize the pattern language that	false	string

				the indicator pattern is expressed in		
			reference	Reference	false	string []
			scope	Scope of the ioc	false	enum
			scopeId	The group/ site/account id depending on the scope. null if it is global.	false	string
			severity	The potential impact of the Threat Intelligence indicator. Designed to work based on OCSF format for scores 0-7.	false	integer
			threatActors	Threat actors	false	string []
			threatActorTypes	Threat actor types	false	string []
			updatedAt	The time at which the indicator was last updated in SentinelOne DB	false	string
			uploadTime	The time at which the Threat Intelligence indicator was uploaded to SentinelOne DB	false	string
			uuid	Unique Id of the Threat	false	string

				Intelligence indicator		
			validUntil	The date from which the indicator will no longer be monitored	false	string
errors	Errors	false	array			

Body Schema

Name	Description	Required	Value
data	Data	false	

Name	Description	Required	Value
source	The source of the identified Threat Intelligence indicator	true	string
type	The type of the Threat Intelligence indicator	true	enum
value	The value of the Threat Intelligence indicator	true	string
campaignNames	Campaign names	false	string []
category	Category	false	string []
creationTime	The time at which the Threat Intelligence indicator was originally created (as indicated by the TI source)	false	string
creator	The user that uploaded the Threat Intelligence indicator	false	string
description	Description of the Threat Intelligence indicator	false	string
externalId	The unique identifier of the indicator	false	string

				as provided by the Threat Intelligence source		
			intrusionSets	Intrusion sets	false	string []
			labels	Labels	false	string []
			malwareNames	Malware names	false	string []
			metadata	The metadata of the Threat Intelligence indicator	false	string
			method	The comparison method used by SentinelOne to trigger the event	false	enum
			mitreTactic	Mitre tactic	false	string []
			name	Threat Intelligence indicator name	false	string
			originalRiskScore	The relative level of risk associated with the Threat Intelligence indicator. An integer between 0 and 100, inclusive.	false	integer
			pattern	The detection pattern for this Threat Intelligence indicator (expressed as a STIX	false	string

				Pattern, e.g. Comparison expression/ Boolean Operators etc.)		
			patternType	Characterize the pattern language that the Threat Intelligence indicator pattern is expressed in	false	
			reference	Reference	false	string []
			severity	The potential impact of the Threat Intelligence indicator. Designed to work based on OCSF format for scores 0-7.	false	integer
			threatActors	Threat actors	false	string []
			threatActorTypes	Threat actor types	false	string []
			validUntil	Expiration date for the Threat Intelligence indicator	false	string
filter	Filter	false	Name	Description	Required	Value
			accountIds	List of Account IDs to filter by	false	string []
			groupIds	List of Group IDs to filter by	false	string []

			siteIds	List of Site IDs to filter by	false	string []
			tenant	Indicates a tenant scope request	false	boolean

Delete IOCs

DELETE /web/api/v2.1/threat-intelligence/iocs

Delete an IoC from the Threat Intelligence database that matches a filter using the accountID and one other field.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>affected</td><td>Number of entities affected by the requested operation</td><td>false</td><td>integer</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>filter</td><td>Filter</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>batchId</td><td>Unique ID of the uploaded indicators batch</td><td>false</td><td>string</td></tr>
<tr><td>category__in</td><td>The categories of the Threat Intelligence indicator, e.g. the malware type associated with the IOC</td><td>false</td><td>string</td></tr>
<tr><td>creationTime__gt</td><td>Creation Time as set by the user greater than</td><td>false</td><td>string</td></tr>
<tr><td>creationTime__gte</td><td>Creation Time as set by the user greater or equal than</td><td>false</td><td>string</td></tr>
<tr><td>creationTime__lt</td><td>Creation Time as set by the user lesser than</td><td>false</td><td>string</td></tr>
<tr><td>creationTime__lte</td><td>Creation Time as set by the user lesser or equal than</td><td>false</td><td>string</td></tr>
<tr><td>creator__contains</td><td>Free-text filter by the user</td><td>false</td><td>string []</td></tr>
</table>
</td></tr>
</table>

				uploaded the Threat Intelligence indicator (supports multiple values)		
			description__contains	Free-text filter by the description of the indicator (supports multiple values)	false	string []
			externalId	The unique identifier of the indicator as provided by the Threat Intelligence source	false	string
			name__contains	Free-text filter by the Indicator name (supports multiple values)	false	string []
			source	List of the sources of the identified Threat Intelligence indicator	false	string []
			tenant	Indicates a tenant scope request	false	boolean
			type	The type of the Threat Intelligence indicator	false	enum
			updatedAt__gt	The time at which the	false	string

				indicator was last updated in SentinelOne DB greater than		
			updatedAt__gte	The time at which the indicator was last updated in SentinelOne DB greater or equal than	false	string
			updatedAt__lt	The time at which the indicator was last updated in SentinelOne DB lesser than	false	string
			updatedAt__lte	The time at which the indicator was last updated in SentinelOne DB lesser or equal than	false	string
			uploadTime__gt	The time at which the Threat Intelligence indicator was uploaded to SentinelOne DB greater than	false	string
			uploadTime__gte	The time at which the Threat Intelligence indicator was	false	string

				uploaded to SentinelOne DB greater or equal than		
			uploadTime__lt	The time at which the Threat Intelligence indicator was uploaded to SentinelOne DB lesser than	false	string
			uploadTime__lte	The time at which the Threat Intelligence indicator was uploaded to SentinelOne DB lesser or equal than	false	string
			uuids	A list of unique Ids of the parent process of the indicator of compromise	false	string []
			value	The value of the Threat Intelligence indicator	false	string

Threat Notes

Get Threat Notes

GET /web/api/v2.1/threats/{threat_id}/notes

Get the threat notes that match the filter.

Parameters

countonly	optional	If true, only total number of items will be returned, without any of the actual objects.
creator__like	optional	Threat Note creator name (partially or full). Example: "John".
creatorid	optional	Threat Note creator ID. Example: "225494730938493804".
cursor	optional	Cursor position returned by the last request. Use to iterate over more than 1000 items. Example: "YWdlbnRfaWQ6NTgwMjkzODE=".
limit	optional	Limit number of returned items (1-1000). Example: "10".
skip	optional	Skip first number of items (0-1000). To iterate over more than 1000 items, use "cursor". Example: "150".
skipcount	optional	If true, total number of items will not be calculated, which speeds up execution time.
sortby	optional	The column to sort the results by. Example: "id".
sortorder	optional	Sort direction. Example: "asc".

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>pagination</td><td>Pagination information</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>totalItems</td><td>Total number of items found matching your query</td><td>true</td><td>integer</td></tr>
<tr><td>nextCursor</td><td>Pass this value as "cursor" on your next request, to get the next page of results (Will be "null" when last page reached)</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>createdAt</td><td>Timestamp of date creation</td><td>false</td><td>string</td></tr>
<tr><td>creator</td><td>Threat Note creator name</td><td>false</td><td>string</td></tr>
<tr><td>creatorId</td><td>Threat Note creator id</td><td>false</td><td>string</td></tr>
<tr><td>edited</td><td>Identify if the the note changed</td><td>false</td><td>boolean</td></tr>
<tr><td>id</td><td>Threat Note ID</td><td>false</td><td>string</td></tr>
<tr><td>text</td><td>Threat Note text</td><td>false</td><td>string</td></tr>
<tr><td>updatedAt</td><td>Timestamp of last update</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Add Note to Multiple

POST /web/api/v2.1/threats/notes

Add a threat note to multiple threats.

Response Messages

200 - Threats note successfully created

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
data	Response data	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>affected</td><td>Number of entities affected by the requested operation</td><td>false</td><td>integer</td></tr></table>
errors	Errors	false	array

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>text</td><td>Threat Note text</td><td>true</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>filter</td><td>Filter</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>agentIds</td><td>List of Agent IDs</td><td>false</td><td>string []</td></tr>
<tr><td>agentIsActive</td><td>Include Agents currently connected to the Management Console</td><td>false</td><td>boolean</td></tr>
<tr><td>agentMachineTypes</td><td>Include Agent machine types</td><td>false</td><td>string []</td></tr>
<tr><td>agentMachineTypesNin</td><td>Excluded Agent machine types</td><td>false</td><td>string []</td></tr>
<tr><td>agentTagsData</td><td>Filter threats by assigned tags to the related agent. Given in form of a JSON where each key represents a tag key, and each value represents a list of string values to</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
</table>

				filter by. To filter by unassigned tag values, use __nin suffix in the tag key.		
			agentVersions	Include Agent versions	false	string []
			agentVersionsNin	Excluded Agent versions	false	string []
			analystVerdicts	Filter threats by a specific analyst verdict	false	string []
			analystVerdictsNin	Exclude threats with specific analyst verdicts	false	string []
			awsRole__contains	Free-text filter by aws role(supports multiple values)	false	string []
			awsSecurityGroups__contains	Free-text filter by aws securityGroups(supports multiple values)	false	string []
			awsSubnetIds__contains	Free-text filter by aws subnet ids (supports multiple values)	false	string []
			azureResourceGroup__contains	Free-text filter by azure resource group(support	false	string []

				s multiple values)		
			classifications	List of threat classifications to search	false	string []
			classificationsNin	List of threat classifications not to search	false	string []
			classificationSources	Classification sources list	false	string []
			classificationSourcesNin	Classification sources list to exclude	false	string []
			cloudAccount__contains	Free-text filter by cloud account (supports multiple values)	false	string []
			cloudImage__contains	Free-text filter by cloud image (supports multiple values)	false	string []
			cloudInstanceId__contains	Free-text filter by cloud instance id(supports multiple values)	false	string []
			cloudInstanceSize__contains	Free-text filter by cloud instance size(supports multiple values)	false	string []
			cloudLocation__contains	Free-text filter by cloud location (supports multiple	false	string []

				values)		
			cloudNetwork__contains	Free-text filter by cloud network (supports multiple values)	false	string []
			cloudProvider	Agents from which cloud provider	false	string []
			cloudProviderNin	Exclude Agents from these cloud provider	false	string []
			collectionIds	List of collection IDs to search	false	string []
			commandLineArguments__contains	Free-text filter by threat command line arguments (supports multiple values)	false	string []
			computerName__contains	Free-text filter by computer name (supports multiple values)	false	string []
			confidenceLevels	Filter threats by a specific confidence level	false	string []
			confidenceLevelsNin	Exclude threats with specific confidence level	false	string []

			containerImageName__contains	Free-text filter by the endpoint container image name (supports multiple values)	false	string []
			containerLabels__contains	Free-text filter by the endpoint container labels (supports multiple values)	false	string []
			containerName__contains	Free-text filter by the endpoint container name (supports multiple values)	false	string []
			contentHash__contains	Free-text filter by file content hash (supports multiple values)	false	string []
			contentHashes	List of sha1 hashes to search for	false	string []
			countsFor	comma-separated list of fields to be shown	false	string
			createdAt__gt	Created at greater than.	false	string
			createdAt__gte	Created at greater or equal than.	false	string

			createdAt__lt	Created at lesser than.	false	string
			createdAt__lte	Created at lesser or equal than.	false	string
			detectionAgentDomain__contains	Free-text filter by Agent domain at detection time (supports multiple values)	false	string []
			detectionAgentVersion__contains	Free-text filter by Agent version at detection time (supports multiple values)	false	string []
			detectionEngines	Included engines	false	string []
			detectionEnginesNin	Excluded engines	false	string []
			displayName	Display name	false	string
			engines	Included engines	false	string []
			enginesNin	Excluded engines	false	string []
			externalTicketExists	The threat contains ticket number	false	boolean
			externalTicketId__contains	Free-text filter by the threat external ticket ID (supports multiple	false	string []

				values)		
			externalTicketIds	External ticket ID for the threat	false	string []
			failedActions	At least one action failed on the threat	false	boolean
			filePath__contains	Free-text filter by file path (supports multiple values)	false	string []
			gcpServiceAccount__contains	Free-text filter by gcp service account (supports multiple values)	false	string []
			groupIds	List of Group IDs to filter by	false	string []
			hasAgentTags	Include only Threats whose Agent is assigned any tags if True, or none if False	false	boolean
			ids	List of threat IDs	false	string []
			incidentStatuses	Filter threats by a specific incident status	false	string []
			incidentStatusesNin	Exclude threats with specific incident statuses	false	string []

			initiatedBy	Only include threats from specific initiating sources	false	string []
			initiatedByNin	Exclude threats with specific initiating sources	false	string []
			initiatedByUsername__contains	Free-text filter by the username that initiated that threat (supports multiple values)	false	string []
			k8sClusterName__contains	Free-text filter by the endpoint Kubernetes cluster name (supports multiple values)	false	string []
			k8sControllerLabels__contains	Free-text filter by the endpoint Kubernetes controller labels (supports multiple values)	false	string []
			k8sControllerName__contains	Free-text filter by the endpoint Kubernetes controller name (supports multiple values)	false	string []

			k8sNamespaceLabels__contains	Free-text filter by the endpoint Kubernetes namespace labels (supports multiple values)	false	string []
			k8sNamespaceName__contains	Free-text filter by the endpoint Kubernetes namespace name (supports multiple values)	false	string []
			k8sNodeLabels__contains	Free-text filter by the endpoint Kubernetes node labels (supports multiple values)	false	string []
			k8sNodeName__contains	Free-text filter by the endpoint Kubernetes node name (supports multiple values)	false	string []
			k8sPodLabels__contains	Free-text filter by the endpoint Kubernetes pod labels (supports multiple values)	false	string []
			k8sPodName__contains	Free-text filter by the	false	string []

				endpoint Kubernetes pod name (supports multiple values)		
			limit	Limit	false	integer
			mitigatedPreemptively	If the threat was detected pre-execution or post-execution	false	boolean
			mitigationStatuses	Filter threats by a specific status	false	string []
			mitigationStatusesNin	Filter threats not by a specific status	false	string []
			noteExists	The threat contains at least one note	false	boolean
			originatedProcess__contains	Free-text filter by the originated process name of the threat (supports multiple values)	false	string []
			osArchs	Included OS Architectures	false	string []
			osNames		false	string []
			osNamesNin		false	string []
			osTypes	Included OS types	false	string []
			osTypesNin	Excluded OS types	false	string []
			pendingActio	At least one	false	boolean

			ns	action is pending for the Agent for the threat		
			publisherName__contains	Free-text filter by threat's publisher name (supports multiple values)	false	string []
			query	Full text search for fields: threat_details, content_hash, computer_name, file_path, uuid, detection_agent_version, realtime_agent_version, detection_agent_domain, command_line_arguments, initiated_by_username, storyline, originated_process, k8s_cluster_name, k8s_node_name, k8s_node_labels, k8s_namespace_name, k8s_namespace_labels,	false	string

				k8s_controller_name, k8s_controller_labels, k8s_pod_name, k8s_pod_labels, container_name, container_image_name, container_labels, external_ticket_id		
			realtimeAgentVersion__contains	Free-text filter by Agent version at current time (supports multiple values)	false	string []
			rebootRequired	A reboot is required on any endpoint for at least one action on the threat	false	boolean
			resolved	This is used for backward-compatibility with API 2.0.	false	boolean
			siteIds	List of Site IDs to filter by	false	string []
			storyline__contains	Free-text filter by threat storyline (supports multiple values)	false	string []

			storylines	List of Agent context to search for	false	string []
			tenant	Indicates a tenant scope request	false	boolean
			threatDetails__contains	Free-text filter by threat details(supports multiple values)	false	string []
			updatedAt__gt	Updated at greater than.	false	string
			updatedAt__gte	Updated at greater or equal than.	false	string
			updatedAt__lt	Updated at lesser than.	false	string
			updatedAt__lte	Updated at lesser or equal than.	false	string
			uuid__contains	Free-text filter by Agent UUID (supports multiple values)	false	string []

Update Threat Note

PUT /web/api/v2.1/threats/{threat_id}/notes/{note_id}

Change the text of a threat note.

Response Messages

200 - Threat note successfully updated

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
createdAt	Timestamp of date creation	false	string
creator	Threat Note creator name	false	string
creatorId	Threat Note creator id	false	string
edited	Identify if the the note changed	false	boolean
id	Threat Note ID	false	string
text	Threat Note text	false	string
updatedAt	Timestamp of last update	false	string

errors	Errors	false	array

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>text</td><td>Threat Note text</td><td>true</td><td>string</td></tr>
</table>
</td></tr>
</table>

Delete Threat Note

DELETE /web/api/v2.1/threats/{threat_id}/notes/{note_id}

Delete a threat note.

Response Messages

200 - Threat note successfully deleted

401 - Unauthorized access - please sign in and retry.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td><table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>success</td><td>Indicates a successful operation</td><td>false</td><td>boolean</td></tr></table></td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Threats

Get Threats

GET /web/api/v2.1/threats

Get data of threats that match the filter.
Best Practice: Use the filters. Each threat gives a number of data lines that will quickly fill the page limit.

> **BEST PRACTICE**
> Use the filters. Each threat gives a number of data lines that will quickly fill the page limit.

Parameters

accountids	optional	List of Account IDs to filter by. Example: "225494730938493804,225494730938493915".
agentids	optional	List of Agent IDs. Example: "225494730938493804,225494730938493915".
agentisactive	optional	Include Agents currently connected to the Management Console
agentmachinetypes	optional	Include Agent machine types. Example: "unknown".
agentmachinetypesnin	optional	Excluded Agent machine types. Example: "unknown".
agenttagsdata	optional	Filter threats by assigned tags to the related agent. Given in form of a JSON where each key represents a tag key, and each value represents a list of string values to filter by. To filter by unassigned tag values, use __nin suffix in the tag key. Example: "{"key1": ["value1_1", "value1_2"], "key2__nin": ["value2"]}".
agentversions	optional	Include Agent versions. Example: "2.5.1.1320".
agentversionsnin	optional	Excluded Agent versions. Example: "2.5.1.1320".
analystverdicts	optional	Filter threats by a specific analyst verdict. Example: "true_positive,suspicious".
analystverdictsnin	optional	Exclude threats with specific analyst verdicts. Example: "true_positive,suspicious".
awsrole__contains	optional	Free-text filter by aws role(supports multiple values)

awssecuritygroups__contains	optional	Free-text filter by aws securityGroups(supports multiple values)
awssubnetids__contains	optional	Free-text filter by aws subnet ids (supports multiple values)
azureresourcegroup__contains	optional	Free-text filter by azure resource group(supports multiple values)
classifications	optional	List of threat classifications to search
classificationsnin	optional	List of threat classifications not to search
classificationsources	optional	Classification sources list. Example: "Cloud".
classificationsourcesnin	optional	Classification sources list to exclude. Example: "Cloud".
cloudaccount__contains	optional	Free-text filter by cloud account (supports multiple values)
cloudimage__contains	optional	Free-text filter by cloud image (supports multiple values)
cloudinstanceid__contains	optional	Free-text filter by cloud instance id(supports multiple values)
cloudinstancesize__contains	optional	Free-text filter by cloud instance size(supports multiple values)
cloudlocation__contains	optional	Free-text filter by cloud location (supports multiple values)
cloudnetwork__contains	optional	Free-text filter by cloud network (supports multiple values)
cloudprovider	optional	Agents from which cloud provider
cloudprovidernin	optional	Exclude Agents from these cloud provider
collectionids	optional	List of collection IDs to search. Example: "225494730938493804,225494730938493915".
commandlineargument s__contains	optional	Free-text filter by threat command line arguments (supports multiple values). Example: "/usr/sbin/,wget".
computername__contains	optional	Free-text filter by computer name (supports multiple values). Example: "john-office,WIN".
confidencelevels	optional	Filter threats by a specific confidence level. Example: "malicious".
confidencelevelsnin	optional	Exclude threats with specific confidence level. Example: "malicious".
containerimagename__contains	optional	Free-text filter by the endpoint container image name (supports multiple values)

containerlabels__contains	optional	Free-text filter by the endpoint container labels (supports multiple values)
containername__contains	optional	Free-text filter by the endpoint container name (supports multiple values)
contenthash__contains	optional	Free-text filter by file content hash (supports multiple values). Example: "5f09bcff3".
contenthashes	optional	List of sha1 hashes to search for. Example: "d,d,d,5,0,3,0,a,3,d,0,2,9,f,3,8,4,5,f,c,1,0,5,2,4,1,9,8,2,9,f,0,8,f,3,1,2,2,4,0".
countonly	optional	If true, only total number of items will be returned, without any of the actual objects.
countsfor	optional	comma-separated list of fields to be shown. Example: "osTypes,machineTypes".
createdat__gt	optional	Created at greater than. Example: "2018-02-27T04:49:26.257525Z".
createdat__gte	optional	Created at greater or equal than. Example: "2018-02-27T04:49:26.257525Z".
createdat__lt	optional	Created at lesser than. Example: "2018-02-27T04:49:26.257525Z".
createdat__lte	optional	Created at lesser or equal than. Example: "2018-02-27T04:49:26.257525Z".
cursor	optional	Cursor position returned by the last request. Use to iterate over more than 1000 items. Example: "YWdlbnRfaWQ6NTgwMjkzODE=".
detectionagentdomain__contains	optional	Free-text filter by Agent domain at detection time (supports multiple values). Example: "sentinel,sentinelone.com".
detectionagentversion__contains	optional	Free-text filter by Agent version at detection time (supports multiple values). Example: "1.1.1.1,2.2.".
detectionengines	optional	Included engines. Example: "reputation".
detectionenginesnin	optional	Excluded engines. Example: "reputation".
displayname	optional	Display name
engines	optional	Included engines. Example: "reputation".
enginesnin	optional	Excluded engines. Example: "reputation".
externalticketexists	optional	The threat contains ticket number
externalticketid__cont	optional	Free-text filter by the threat external ticket ID (supports multiple

ains		values)
externalticketids	optional	External ticket ID for the threat
failedactions	optional	At least one action failed on the threat
filepath__contains	optional	Free-text filter by file path (supports multiple values). Example: "\MyUser\Downloads".
gcpserviceaccount__contains	optional	Free-text filter by gcp service account (supports multiple values)
groupids	optional	List of Group IDs to filter by. Example: "225494730938493804,225494730938493915".
hasagenttags	optional	Include only Threats whose Agent is assigned any tags if True, or none if False
ids	optional	List of threat IDs. Example: "225494730938493804,225494730938493915".
incidentstatuses	optional	Filter threats by a specific incident status. Example: "unresolved,in_progress".
incidentstatusesnin	optional	Exclude threats with specific incident statuses. Example: "unresolved,in_progress".
initiatedby	optional	Only include threats from specific initiating sources. Example: "agent_policy,dv_command".
initiatedbynin	optional	Exclude threats with specific initiating sources. Example: "agent_policy,dv_command".
initiatedbyusername__contains	optional	Free-text filter by the username that initiated that threat (supports multiple values). Example: "John,John Doe".
k8sclustername__contains	optional	Free-text filter by the endpoint Kubernetes cluster name (supports multiple values)
k8scontrollerlabels__contains	optional	Free-text filter by the endpoint Kubernetes controller labels (supports multiple values)
k8scontrollername__contains	optional	Free-text filter by the endpoint Kubernetes controller name (supports multiple values)
k8snamespacelabels__contains	optional	Free-text filter by the endpoint Kubernetes namespace labels (supports multiple values)
k8snamespacename__contains	optional	Free-text filter by the endpoint Kubernetes namespace name (supports multiple values)
k8snodelabels__contai	optional	Free-text filter by the endpoint Kubernetes node labels (supports

ns		multiple values)
k8snodename__contains	optional	Free-text filter by the endpoint Kubernetes node name (supports multiple values)
k8spodlabels__contains	optional	Free-text filter by the endpoint Kubernetes pod labels (supports multiple values)
k8spodname__contains	optional	Free-text filter by the endpoint Kubernetes pod name (supports multiple values)
limit	optional	Limit number of returned items (1-1000). Example: "10".
mitigatedpreemptively	optional	If the threat was detected pre-execution or post-execution
mitigationstatuses	optional	Filter threats by a specific status. Example: "not_mitigated".
mitigationstatusesnin	optional	Filter threats not by a specific status. Example: "not_mitigated".
noteexists	optional	The threat contains at least one note
originatedprocess__contains	optional	Free-text filter by the originated process name of the threat (supports multiple values)
osarchs	optional	Included OS Architectures. Example: "32 bit".
osnames	optional	
osnamesnin	optional	
ostypes	optional	Included OS types. Example: "macos".
ostypesnin	optional	Excluded OS types. Example: "macos".
pendingactions	optional	At least one action is pending for the Agent for the threat
publishername__contains	optional	Free-text filter by threat's publisher name (supports multiple values). Example: "GOOGLE,Apple Inc.".
query	optional	Full text search for fields: threat_details, content_hash, computer_name, file_path, uuid, detection_agent_version, realtime_agent_version, detection_agent_domain, command_line_arguments, initiated_by_username, storyline, originated_process, k8s_cluster_name, k8s_node_name, k8s_node_labels, k8s_namespace_name, k8s_namespace_labels, k8s_controller_name, k8s_controller_labels, k8s_pod_name, k8s_pod_labels, container_name, container_image_name, container_labels, external_ticket_id
realtimeagentversion__contains	optional	Free-text filter by Agent version at current time (supports multiple values). Example: "1.1.1.1,2.2.".
rebootrequired	optional	A reboot is required on any endpoint for at least one action on the

		threat
resolved	optional	This is used for backward-compatibility with API 2.0.
siteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".
skip	optional	Skip first number of items (0-1000). To iterate over more than 1000 items, use "cursor". Example: "150".
skipcount	optional	If true, total number of items will not be calculated, which speeds up execution time.
sortby	optional	The column to sort the results by. Example: "id".
sortorder	optional	Sort direction. Example: "asc".
storyline__contains	optional	Free-text filter by threat storyline (supports multiple values). Example: "0000C2E97648,0006FC73-77B4-470F-AAC7-".
storylines	optional	List of Agent context to search for
tenant	optional	Indicates a tenant scope request
threatdetails__contains	optional	Free-text filter by threat details(supports multiple values). Example: "malware.exe,virus.exe".
updatedat__gt	optional	Updated at greater than. Example: "2018-02-27T04:49:26.257525Z".
updatedat__gte	optional	Updated at greater or equal than. Example: "2018-02-27T04:49:26.257525Z".
updatedat__lt	optional	Updated at lesser than. Example: "2018-02-27T04:49:26.257525Z".
updatedat__lte	optional	Updated at lesser or equal than. Example: "2018-02-27T04:49:26.257525Z".
uuid__contains	optional	Free-text filter by Agent UUID (supports multiple values). Example: "e92-01928,b055".

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
pagination	Pagination information	true	

Name	Description	Required	Value
totalItems	Total number of items found matching your query	true	integer
nextCursor	Pass this value as "cursor" on your next request, to get the next page of results (Will be "null" when last page reached)	false	string

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
agentDetectionInfo	Agent detection time information	false	

Name	Description	Required	Value
accountId	Orig account id	false	string
accountName	Orig account name	false	string
agentDetectionState	The Agent's detection state at time of detection	false	string
agentDomain	Network domain	false	string
agentIpV4	Orig agent ip v4	false	string
agentIpV6	Orig agent ip v6	false	string
agentLastLoggedInUpn	UPN of last logged in user	false	string
agentLastLog	mail from AD	false	string

						gedInUserMail	of last logged in user		
						agentLastLoggedInUserName	Orig logged user	false	string
						agentMitigationMode	Agent mitigation mode policy	false	enum
						agentOsName	Orig agent os name	false	string
						agentOsRevision	Orig agent os revision	false	string
						agentRegisteredAt	Time of first registration to management console	false	string
						agentUuid	UUID of the agent	false	string
						agentVersion	Orig agent version	false	string
						cloudProviders	Cloud providers for this agent	false	object
						externalIp	Orig agent external ip	false	string
						groupId	Orig group id	false	string
						groupName	Orig group name	false	string
						siteId	Orig site id	false	string
						siteName	Orig site name	false	string
				agentRealtimeInfo	Agent realtime information	false	Name	Description	Required	Value
							accountId	Account id	false	string
							accountName	Account name	false	string
							activeThreats	Active	false	integer

	threats		
agentComputerName	Computer name	false	string
agentDecommissionedAt	Decommissioned at	false	boolean
agentDomain	Domain	false	string
agentId	Id	false	string
agentInfected	Agent infected	false	boolean
agentIsActive	Is active	false	boolean
agentIsDecommissioned	Is decommissioned	false	boolean
agentMachineType	Machine type	false	enum
agentMitigationMode	Agent mitigation mode policy	false	enum
agentNetworkStatus	Network status	false	enum
agentOsName	Os name	false	string
agentOsRevision	Os revision	false	string
agentOsType	OS type	false	enum
agentUuid	Uuid	false	string
agentVersion	Agent version	false	string
groupId	Group id	false	string
groupName	Group name	false	string
networkInterfaces	Device's network interfaces	false	

Name	Description	Required	Value
id	Id	false	string
inet	IPv4 addresses	false	string []
inet6	IPv6 addresses	false	string []

									name Name false string physical Interface's MAC address false string
						operationalState	Agent operational state	false	string
						rebootRequired	A reboot is required on the endpoint for at least one threat	false	boolean
						scanAbortedAt	Abort time of last scan (If applicable)	false	string
						scanFinishedAt	Finish time of last scan (If applicable)	false	string
						scanStartedAt	Start time of last scan	false	string
						scanStatus	Scan status	false	enum
						siteId	Site id	false	string
						siteName	Site name	false	string
						storageName	Storage Name	false	string
						storageType	Storage Type	false	string
						userActionsNeeded	A list of pending user actions. List items possible values: "none, user_action_needed, reboot_needed, upgrade_needed, incompatible_os,	false	string []

							unprotected, rebootless_without_dynamic_detection, extended_exclusions_partially_accepted, reboot_required, pending_deprecation, ne_not_running, ne_cf_not_active".		
			containerInfo	Threat container information	false	Name / Description / Required / Value id / Id / false / string image / Image / false / string isContainerQuarantine / True if the container is quarantined / false / boolean labels / Labels / false / string [] name / Name / false / string			
			id	Threat ID	false	string			
			indicators	Indicators	false	Name / Description / Required / Value category / Category / false / string categoryId / [DEPRECATED] / false / integer description / Description / false / string ids / List of all the indicators IDs / false / integer [] tactics / Tactics / false / Name / Description / Required / Value name / Name / false / string source / Source / false / string techniques / Techniques / false / Name / D			

														link	Li
														name	Na
			kubernetesInfo	Threat kubernetes information	false										
			mitigationStatus	Threat mitigation information	false										

Name	Description	Required	Value
cluster	Cluster	false	string
controllerKind	Controller kind	false	string
controllerLabels	Controller labels	false	string []
controllerName	Controller name	false	string
isContainerQuarantine	True if the container is quarantined	false	boolean
namespace	Namespace	false	string
namespaceLabels	Namespace labels	false	string []
node	Node	false	string
nodeLabels	Node labels	false	string []
pod	Pod	false	string
podLabels	Pod labels	false	string []

Name	Description	Required	Value
action	Action	false	enum
actionsCounters	Actions counters	false	
agentSupportsReport	The Agent generates a full mitigation	false	boolean

Name	Description	Required	Value
failed	Failed	false	integer
notFound	Not found	false	integer
pendingReboot	Pending reboot	false	integer
success	Success	false	integer
total	Total	false	integer

							report		
						groupNotFound	Agent could not find the threat	false	boolean
						lastUpdate	Timestamp of last mitigation status update	false	string
						latestReport	Report download URL. If None, there is no report	false	string
						mitigationEndedAt	The time the Agent finished the mitigation	false	string
						mitigationStartedAt	The time the Agent started the mitigation	false	string
						reportId	ID of the mitigation report	false	string
						status	Status	false	enum
				threatInfo	Threat information	false	Name	Description	Required	Value
							sha1	SHA1 hash of file content	true	string
							analystVerdict	Analyst verdict	false	enum
							analystVerdictDescription	Analyst verdict description	false	
							automatically Resolved	Automatically resolved	false	boolean
							browserType	Browser type	false	string
							certificateId	File Certificate ID	false	string

						classification	Classification of the threat	false	string	
						classificationSource	Source of the threat Classification	false	enum	
						cloudFilesHashVerdict	Cloud files hash verdict	false	string	
						collectionId	Collection id	false	string	
						confidenceLevel	SentinelOne threat confidence level	false	enum	
						createdAt	Timestamp of date creation in the Management Console.	false	string	
						detectionEngines	List of engines that detected the threat	false		
						detectionType	Detection type	false	enum	
						engines	[Deprecated] List of engines that detected the threat	false		
						externalTicketExists	External ticket exists	false		
						externalTicketId	External ticket id	false	string	
						failedActions	At least one action failed on the threat	false	boolean	
						fileExtension	File extension	false	string	
						fileExtensionType	File extension type	false	string	
						filePath	File path	false		

						fileSize	File size	false	integer
						fileVerificationType	File verification type	false	string
						identifiedAt	Identified at	false	string
						incidentStatus	Incident status	false	enum
						incidentStatusDescription	Incident status description	false	
						initiatedBy	Source of threat	false	enum
						initiatedByDescription	Initiated by description	false	
						initiatingUserId	Initiating user id	false	string
						initiatingUsername	Initiating username	false	string
						isFileless	Is fileless	false	
						isValidCertificate	True if the certificate is valid	false	boolean
						macroModules	List of macro modules	false	Name: moduleName; Description: Name of macro module; Required: false; Value: string Name: sha1; Description: SHA-1 of the macro module; Required: false; Value: string
						maliciousProcessArguments	Malicious process arguments	false	string
						md5	Md5	false	string
						mitigatedPreemptively	True is the threat was blocked before	false	boolean

							execution		
						mitigationStatus	Mitigation status	false	enum
						mitigationStatusDescription	Mitigation status description	false	
						originatorProcess	Originator process	false	string
						pendingActions	At least one action is pending on the threat	false	boolean
						processUser	Process user	false	string
						publisherName	Certificate publisher	false	string
						reachedEventsLimit	Has number of OS events for this threat reached the limit, resulting in a partial attack storyline	false	boolean
						rebootRequired	A reboot is required on the endpoint for at least one action on the threat	false	boolean
						sha256	SHA256 hash of file content	false	string
						storyline	Storyline identifier from agent	false	string
						threatId	Threat id	false	string
						threatName	Threat name	false	string
						updatedAt	Timestamp of last update	false	string

			whiteningOptions	Whitening options	false	string []
errors	Errors	false	array			

Mitigate Threats

POST /web/api/v2.1/threats/mitigate/{action}

Apply a mitigation action to a group of threats that match the filter. Valid values for mitigation: "kill", "quarantine", "remediate", "rollback-remediation", "un-quarantine","network-quarantine".
Your user role must have permissions to mitigate threats - Admin, IR Team, SOC. Only threats which you have permission to mitigate are countedas "affected" in response field.
Rollback is applied only on Windows. Remediate is applied only on macOS and Windows.

Response Messages

200 - Threat successfully mitigated

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
affected	Number of entities affected by the requested operation	false	integer
details	Single threat mitigation information	false	

Name	Description	Required	Value
reports	List of latest mitigation reports created by the action trigger.	false	

Name	Description	Required	Value
action	Action	false	enum
actionsCounters	Actions counters	false	

Name	D
failed	Fa
notFound	No
pendingReboot	Pe re

												success	Su	
												total	To	
									agentSupportsReport	The Agent generates a full mitigation report	false	boolean		
									groupNotFound	Agent could not find the threat	false	boolean		
									lastUpdate	Timestamp of last mitigation status update	false	string		
									latestReport	Report download URL. If None, there is no report	false	string		
									mitigationEndedAt	The time the Agent finished the mitigation	false	string		
									mitigationStartedAt	The time the Agent started the mitigation	false	string		
									reportId	ID of the mitigation report	false	string		
									status	Status	false	enum		
						skipped	List of skipped mitigation actions with additional details.	false	Name	Description	Required	Value		
									action	Action	false	enum		
									description	Description	false	string		
									reason	Reason	false	enum		
						threatId	Threat id	false	string					
errors	Errors	false	array											

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>filter</td><td>Use any of the filtering options to control the list of affected threats. You can use any combination of filters to narrow down the list (For example "apply to only active threats from Linux endpoints"). You can also leave this field empty to apply to all available threats.</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>agentIds</td><td>List of Agent IDs</td><td>false</td><td>string []</td></tr>
<tr><td>agentIsActive</td><td>Include Agents currently connected to the Management Console</td><td>false</td><td>boolean</td></tr>
<tr><td>agentMachineTypes</td><td>Include Agent machine types</td><td>false</td><td>string []</td></tr>
<tr><td>agentMachineTypesNin</td><td>Excluded Agent machine types</td><td>false</td><td>string []</td></tr>
<tr><td>agentTagsData</td><td>Filter threats by assigned tags to the related agent. Given in form of a JSON where each key represents a tag key, and each value represents a list of string values to filter by. To filter by unassigned tag values, use __nin</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
</table>

				suffix in the tag key.		
			agentVersions	Include Agent versions	false	string []
			agentVersionsNin	Excluded Agent versions	false	string []
			analystVerdicts	Filter threats by a specific analyst verdict	false	string []
			analystVerdictsNin	Exclude threats with specific analyst verdicts	false	string []
			awsRole__contains	Free-text filter by aws role(supports multiple values)	false	string []
			awsSecurityGroups__contains	Free-text filter by aws securityGroups(supports multiple values)	false	string []
			awsSubnetIds__contains	Free-text filter by aws subnet ids (supports multiple values)	false	string []
			azureResourceGroup__contains	Free-text filter by azure resource group(supports multiple values)	false	string []
			classifications	List of threat classifications to search	false	string []

			classificationsNin	List of threat classifications not to search	false	string []
			classificationSources	Classification sources list	false	string []
			classificationSourcesNin	Classification sources list to exclude	false	string []
			cloudAccount__contains	Free-text filter by cloud account (supports multiple values)	false	string []
			cloudImage__contains	Free-text filter by cloud image (supports multiple values)	false	string []
			cloudInstanceId__contains	Free-text filter by cloud instance id(supports multiple values)	false	string []
			cloudInstanceSize__contains	Free-text filter by cloud instance size(supports multiple values)	false	string []
			cloudLocation__contains	Free-text filter by cloud location (supports multiple values)	false	string []
			cloudNetwork__contains	Free-text filter by cloud network (supports	false	string []

				multiple values)		
			cloudProvider	Agents from which cloud provider	false	string []
			cloudProvideerNin	Exclude Agents from these cloud provider	false	string []
			collectionIds	List of collection IDs to search	false	string []
			commandLineArguments__contains	Free-text filter by threat command line arguments (supports multiple values)	false	string []
			computerName__contains	Free-text filter by computer name (supports multiple values)	false	string []
			confidenceLevels	Filter threats by a specific confidence level	false	string []
			confidenceLevelsNin	Exclude threats with specific confidence level	false	string []
			containerImageName__contains	Free-text filter by the endpoint container image name	false	string []

				(supports multiple values)		
			containerLabels__contains	Free-text filter by the endpoint container labels (supports multiple values)	false	string []
			containerName__contains	Free-text filter by the endpoint container name (supports multiple values)	false	string []
			contentHash__contains	Free-text filter by file content hash (supports multiple values)	false	string []
			contentHashes	List of sha1 hashes to search for	false	string []
			countsFor	comma-separated list of fields to be shown	false	string
			createdAt__gt	Created at greater than.	false	string
			createdAt__gte	Created at greater or equal than.	false	string
			createdAt__lt	Created at lesser than.	false	string
			createdAt__lte	Created at lesser or equal than.	false	string

			detectionAgentDomain__contains	Free-text filter by Agent domain at detection time (supports multiple values)	false	string []
			detectionAgentVersion__contains	Free-text filter by Agent version at detection time (supports multiple values)	false	string []
			detectionEngines	Included engines	false	string []
			detectionEnginesNin	Excluded engines	false	string []
			displayName	Display name	false	string
			engines	Included engines	false	string []
			enginesNin	Excluded engines	false	string []
			externalTicketExists	The threat contains ticket number	false	boolean
			externalTicketId__contains	Free-text filter by the threat external ticket ID (supports multiple values)	false	string []
			externalTicketIds	External ticket ID for the threat	false	string []
			failedActions	At least one	false	boolean

				action failed on the threat		
			filePath__contains	Free-text filter by file path (supports multiple values)	false	string []
			gcpServiceAccount__contains	Free-text filter by gcp service account (supports multiple values)	false	string []
			groupIds	List of Group IDs to filter by	false	string []
			hasAgentTags	Include only Threats whose Agent is assigned any tags if True, or none if False	false	boolean
			ids	List of threat IDs	false	string []
			incidentStatuses	Filter threats by a specific incident status	false	string []
			incidentStatusesNin	Exclude threats with specific incident statuses	false	string []
			initiatedBy	Only include threats from specific initiating sources	false	string []
			initiatedByNi	Exclude	false	string []

			n	threats with specific initiating sources		
			initiatedByUsername__contains	Free-text filter by the username that initiated that threat (supports multiple values)	false	string []
			k8sClusterName__contains	Free-text filter by the endpoint Kubernetes cluster name (supports multiple values)	false	string []
			k8sControllerLabels__contains	Free-text filter by the endpoint Kubernetes controller labels (supports multiple values)	false	string []
			k8sControllerName__contains	Free-text filter by the endpoint Kubernetes controller name (supports multiple values)	false	string []
			k8sNamespaceLabels__contains	Free-text filter by the endpoint Kubernetes namespace labels	false	string []

				(supports multiple values)		
			k8sNamespaceName__contains	Free-text filter by the endpoint Kubernetes namespace name (supports multiple values)	false	string []
			k8sNodeLabels__contains	Free-text filter by the endpoint Kubernetes node labels (supports multiple values)	false	string []
			k8sNodeName__contains	Free-text filter by the endpoint Kubernetes node name (supports multiple values)	false	string []
			k8sPodLabels__contains	Free-text filter by the endpoint Kubernetes pod labels (supports multiple values)	false	string []
			k8sPodName__contains	Free-text filter by the endpoint Kubernetes pod name (supports multiple values)	false	string []

			limit	Limit	false	integer
			mitigatedPreemptively	If the threat was detected pre-execution or post-execution	false	boolean
			mitigationStatuses	Filter threats by a specific status	false	string []
			mitigationStatusesNin	Filter threats not by a specific status	false	string []
			noteExists	The threat contains at least one note	false	boolean
			originatedProcess__contains	Free-text filter by the originated process name of the threat (supports multiple values)	false	string []
			osArchs	Included OS Architectures	false	string []
			osNames		false	string []
			osNamesNin		false	string []
			osTypes	Included OS types	false	string []
			osTypesNin	Excluded OS types	false	string []
			pendingActions	At least one action is pending for the Agent for the threat	false	boolean
			publisherName__contains	Free-text filter by	false	string []

				threat's publisher name (supports multiple values)		
			query	Full text search for fields: threat_details, content_hash, computer_name, file_path, uuid, detection_agent_version, realtime_agent_version, detection_agent_domain, command_line_arguments, initiated_by_username, storyline, originated_process, k8s_cluster_name, k8s_node_name, k8s_node_labels, k8s_namespace_name, k8s_namespace_labels, k8s_controller_name, k8s_controller_labels, k8s_pod_name,	false	string

				k8s_pod_labels, container_name, container_image_name, container_labels, external_ticket_id		
			realtimeAgentVersion__contains	Free-text filter by Agent version at current time (supports multiple values)	false	string []
			rebootRequired	A reboot is required on any endpoint for at least one action on the threat	false	boolean
			resolved	This is used for backward-compatibility with API 2.0.	false	boolean
			siteIds	List of Site IDs to filter by	false	string []
			storyline__contains	Free-text filter by threat storyline (supports multiple values)	false	string []
			storylines	List of Agent context to search for	false	string []
			tenant	Indicates a tenant scope	false	boolean

			request		
			threatDetails__contains	Free-text filter by threat details(supports multiple values)	false	string []
			updatedAt__gt	Updated at greater than.	false	string
			updatedAt__gte	Updated at greater or equal than.	false	string
			updatedAt__lt	Updated at lesser than.	false	string
			updatedAt__lte	Updated at lesser or equal than.	false	string
			uuid__contains	Free-text filter by Agent UUID (supports multiple values)	false	string []
data	Data	false	

Add to Blocklist

POST /web/api/v2.1/threats/add-to-blacklist

Add threats that have a SHA1 hash and that match the filter to the Blocklist of the target scope: Global, Account, Site, or Group.
Your role must have permissions to change the Blocklist - Admin, IR Team, SOC - and your user scope access must include the Agent. The target scope is the Group, Site, or Account of the Agent.

Response Messages

200 - Hash threat added to black list

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
affected	Number of entities affected by the requested operation	false	integer
details	Result details for each threat	false	

Name	Description	Required	Value
analystVerdict	Result of changing the threat's analyst verdict as part of adding the threat to blocklist or exclusions	false	enum
result	Result of adding the threat to	false	enum

							blocklist or exclusions		
						threatId	Threat id	false	string
errors	Errors	false	array						

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>targetScope</td><td>Scope to be used for Restrictions</td><td>true</td><td>enum</td></tr>
<tr><td>description</td><td>Description</td><td>false</td><td>string</td></tr>
<tr><td>externalTicketId</td><td>External ticket id</td><td>false</td><td>string</td></tr>
<tr><td>note</td><td>Note</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>filter</td><td>Use any of the filtering options to control the list of affected threats. You can use any combination of filters to narrow down the list (For example "apply to only active threats from Linux endpoints"). You can also leave this field empty to apply to all available threats.</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>agentIds</td><td>List of Agent IDs</td><td>false</td><td>string []</td></tr>
<tr><td>agentIsActive</td><td>Include Agents currently connected to the Management Console</td><td>false</td><td>boolean</td></tr>
<tr><td>agentMachineTypes</td><td>Include Agent machine types</td><td>false</td><td>string []</td></tr>
<tr><td>agentMachineTypesNin</td><td>Excluded Agent machine types</td><td>false</td><td>string []</td></tr>
<tr><td>agentTagsData</td><td>Filter threats by assigned tags to the related agent. Given in form of a JSON where each key</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
</table>

				represents a tag key, and each value represents a list of string values to filter by. To filter by unassigned tag values, use __nin suffix in the tag key.		
			agentVersions	Include Agent versions	false	string []
			agentVersionsNin	Excluded Agent versions	false	string []
			analystVerdicts	Filter threats by a specific analyst verdict	false	string []
			analystVerdictsNin	Exclude threats with specific analyst verdicts	false	string []
			awsRole__contains	Free-text filter by aws role(supports multiple values)	false	string []
			awsSecurityGroups__contains	Free-text filter by aws securityGroups(supports multiple values)	false	string []
			awsSubnetIds__contains	Free-text filter by aws subnet ids (supports multiple	false	string []

				values)		
			azureResourceGroup__contains	Free-text filter by azure resource group(supports multiple values)	false	string []
			classifications	List of threat classifications to search	false	string []
			classificationsNin	List of threat classifications not to search	false	string []
			classificationSources	Classification sources list	false	string []
			classificationSourcesNin	Classification sources list to exclude	false	string []
			cloudAccount__contains	Free-text filter by cloud account (supports multiple values)	false	string []
			cloudImage__contains	Free-text filter by cloud image (supports multiple values)	false	string []
			cloudInstanceId__contains	Free-text filter by cloud instance id(supports multiple values)	false	string []
			cloudInstanceSize__contains	Free-text filter by cloud instance size(supports multiple values)	false	string []

			cloudLocation__contains	Free-text filter by cloud location (supports multiple values)	false	string []
			cloudNetwork__contains	Free-text filter by cloud network (supports multiple values)	false	string []
			cloudProvider	Agents from which cloud provider	false	string []
			cloudProviderNin	Exclude Agents from these cloud provider	false	string []
			collectionIds	List of collection IDs to search	false	string []
			commandLineArguments__contains	Free-text filter by threat command line arguments (supports multiple values)	false	string []
			computerName__contains	Free-text filter by computer name (supports multiple values)	false	string []
			confidenceLevels	Filter threats by a specific confidence level	false	string []

			confidenceLevelsNin	Exclude threats with specific confidence level	false	string []
			containerImageName__contains	Free-text filter by the endpoint container image name (supports multiple values)	false	string []
			containerLabels__contains	Free-text filter by the endpoint container labels (supports multiple values)	false	string []
			containerName__contains	Free-text filter by the endpoint container name (supports multiple values)	false	string []
			contentHash__contains	Free-text filter by file content hash (supports multiple values)	false	string []
			contentHashes	List of sha1 hashes to search for	false	string []
			countsFor	comma-separated list of fields to be shown	false	string
			createdAt__g	Created at	false	string

			t	greater than.		
			createdAt__gte	Created at greater or equal than.	false	string
			createdAt__lt	Created at lesser than.	false	string
			createdAt__lte	Created at lesser or equal than.	false	string
			detectionAgentDomain__contains	Free-text filter by Agent domain at detection time (supports multiple values)	false	string []
			detectionAgentVersion__contains	Free-text filter by Agent version at detection time (supports multiple values)	false	string []
			detectionEngines	Included engines	false	string []
			detectionEnginesNin	Excluded engines	false	string []
			displayName	Display name	false	string
			engines	Included engines	false	string []
			enginesNin	Excluded engines	false	string []
			externalTicketExists	The threat contains ticket number	false	boolean
			externalTicketId__contains	Free-text filter by the	false	string []

				threat external ticket ID (supports multiple values)		
			externalTicketIds	External ticket ID for the threat	false	string []
			failedActions	At least one action failed on the threat	false	boolean
			filePath__contains	Free-text filter by file path (supports multiple values)	false	string []
			gcpServiceAccount__contains	Free-text filter by gcp service account (supports multiple values)	false	string []
			groupIds	List of Group IDs to filter by	false	string []
			hasAgentTags	Include only Threats whose Agent is assigned any tags if True, or none if False	false	boolean
			ids	List of threat IDs	false	string []
			incidentStatuses	Filter threats by a specific incident status	false	string []
			incidentStatu	Exclude	false	string []

			sesNin	threats with specific incident statuses		
			initiatedBy	Only include threats from specific initiating sources	false	string []
			initiatedByNin	Exclude threats with specific initiating sources	false	string []
			initiatedByUsername__contains	Free-text filter by the username that initiated that threat (supports multiple values)	false	string []
			k8sClusterName__contains	Free-text filter by the endpoint Kubernetes cluster name (supports multiple values)	false	string []
			k8sControllerLabels__contains	Free-text filter by the endpoint Kubernetes controller labels (supports multiple values)	false	string []
			k8sControllerName__contains	Free-text filter by the endpoint Kubernetes	false	string []

				controller name (supports multiple values)		
			k8sNamespaceLabels__contains	Free-text filter by the endpoint Kubernetes namespace labels (supports multiple values)	false	string []
			k8sNamespaceName__contains	Free-text filter by the endpoint Kubernetes namespace name (supports multiple values)	false	string []
			k8sNodeLabels__contains	Free-text filter by the endpoint Kubernetes node labels (supports multiple values)	false	string []
			k8sNodeName__contains	Free-text filter by the endpoint Kubernetes node name (supports multiple values)	false	string []
			k8sPodLabels__contains	Free-text filter by the endpoint Kubernetes pod labels	false	string []

				(supports multiple values)		
			k8sPodName__contains	Free-text filter by the endpoint Kubernetes pod name (supports multiple values)	false	string []
			limit	Limit	false	integer
			mitigatedPreemptively	If the threat was detected pre-execution or post-execution	false	boolean
			mitigationStatuses	Filter threats by a specific status	false	string []
			mitigationStatusesNin	Filter threats not by a specific status	false	string []
			noteExists	The threat contains at least one note	false	boolean
			originatedProcess__contains	Free-text filter by the originated process name of the threat (supports multiple values)	false	string []
			osArchs	Included OS Architectures	false	string []
			osNames		false	string []
			osNamesNin		false	string []
			osTypes	Included OS	false	string []

				types		
			osTypesNin	Excluded OS types	false	string []
			pendingActions	At least one action is pending for the Agent for the threat	false	boolean
			publisherName__contains	Free-text filter by threat's publisher name (supports multiple values)	false	string []
			query	Full text search for fields: threat_details, content_hash, computer_name, file_path, uuid, detection_agent_version, realtime_agent_version, detection_agent_domain, command_line_arguments, initiated_by_username, storyline, originated_process, k8s_cluster_name, k8s_node_name, k8s_node_labe	false	string

				ls, k8s_namespace_name, k8s_namespace_labels, k8s_controller_name, k8s_controller_labels, k8s_pod_name, k8s_pod_labels, container_name, container_image_name, container_labels, external_ticket_id		
			realtimeAgentVersion__contains	Free-text filter by Agent version at current time (supports multiple values)	false	string []
			rebootRequired	A reboot is required on any endpoint for at least one action on the threat	false	boolean
			resolved	This is used for backward-compatibility with API 2.0.	false	boolean
			siteIds	List of Site IDs to filter by	false	string []
			storyline__contains	Free-text filter by	false	string []

				threat storyline (supports multiple values)		
			storylines	List of Agent context to search for	false	string []
			tenant	Indicates a tenant scope request	false	boolean
			threatDetails__contains	Free-text filter by threat details(supports multiple values)	false	string []
			updatedAt__gt	Updated at greater than.	false	string
			updatedAt__gte	Updated at greater or equal than.	false	string
			updatedAt__lt	Updated at lesser than.	false	string
			updatedAt__lte	Updated at lesser or equal than.	false	string
			uuid__contains	Free-text filter by Agent UUID (supports multiple values)	false	string []

Fetch Threat File

POST /web/api/v2.1/threats/fetch-file

Fetch a file associated with the threat that matches the filter. Your user role must have permissions to Fetch Threat File - Admin, IR Team, SOC.

Response Messages

200 - Number of affected agents

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>affected</td><td>Number of entities affected by the requested operation</td><td>false</td><td>integer</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>password</td><td>File encryption password</td><td>true</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>filter</td><td>Use any of the filtering options to control the list of affected threats. You can use any combination of filters to narrow down the list (For example "apply to only active threats from Linux endpoints"). You can also leave this field empty to apply to all available threats. Note: Filter must match exactly one threat. Bulk operations are not supported.</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>agentIds</td><td>List of Agent IDs</td><td>false</td><td>string []</td></tr>
<tr><td>agentIsActive</td><td>Include Agents currently connected to the Management Console</td><td>false</td><td>boolean</td></tr>
<tr><td>agentMachineTypes</td><td>Include Agent machine types</td><td>false</td><td>string []</td></tr>
<tr><td>agentMachineTypesNin</td><td>Excluded Agent machine types</td><td>false</td><td>string []</td></tr>
<tr><td>agentTagsData</td><td>Filter threats by assigned tags to the related agent. Given in form of a JSON where each key represents a tag key, and each value represents a list of string</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
</table>

				values to filter by. To filter by unassigned tag values, use __nin suffix in the tag key.		
			agentVersions	Include Agent versions	false	string []
			agentVersionsNin	Excluded Agent versions	false	string []
			analystVerdicts	Filter threats by a specific analyst verdict	false	string []
			analystVerdictsNin	Exclude threats with specific analyst verdicts	false	string []
			awsRole__contains	Free-text filter by aws role(supports multiple values)	false	string []
			awsSecurityGroups__contains	Free-text filter by aws securityGroups(supports multiple values)	false	string []
			awsSubnetIds__contains	Free-text filter by aws subnet ids (supports multiple values)	false	string []
			azureResourceGroup__contains	Free-text filter by azure resource	false	string []

				group(supports multiple values)		
			classifications	List of threat classifications to search	false	string []
			classificationsNin	List of threat classifications not to search	false	string []
			classificationSources	Classification sources list	false	string []
			classificationSourcesNin	Classification sources list to exclude	false	string []
			cloudAccount__contains	Free-text filter by cloud account (supports multiple values)	false	string []
			cloudImage__contains	Free-text filter by cloud image (supports multiple values)	false	string []
			cloudInstanceId__contains	Free-text filter by cloud instance id(supports multiple values)	false	string []
			cloudInstanceSize__contains	Free-text filter by cloud instance size(supports multiple values)	false	string []
			cloudLocation__contains	Free-text filter by cloud location (supports	false	string []

				multiple values)		
			cloudNetwork__contains	Free-text filter by cloud network (supports multiple values)	false	string []
			cloudProvider	Agents from which cloud provider	false	string []
			cloudProviderNin	Exclude Agents from these cloud provider	false	string []
			collectionIds	List of collection IDs to search	false	string []
			commandLineArguments__contains	Free-text filter by threat command line arguments (supports multiple values)	false	string []
			computerName__contains	Free-text filter by computer name (supports multiple values)	false	string []
			confidenceLevels	Filter threats by a specific confidence level	false	string []
			confidenceLevelsNin	Exclude threats with specific confidence	false	string []

				level		
			containerImageName__contains	Free-text filter by the endpoint container image name (supports multiple values)	false	string []
			containerLabels__contains	Free-text filter by the endpoint container labels (supports multiple values)	false	string []
			containerName__contains	Free-text filter by the endpoint container name (supports multiple values)	false	string []
			contentHash__contains	Free-text filter by file content hash (supports multiple values)	false	string []
			contentHashes	List of sha1 hashes to search for	false	string []
			countsFor	comma-separated list of fields to be shown	false	string
			createdAt__gt	Created at greater than.	false	string
			createdAt__gte	Created at greater or	false	string

				equal than.		
			createdAt__lt	Created at lesser than.	false	string
			createdAt__lte	Created at lesser or equal than.	false	string
			detectionAgentDomain__contains	Free-text filter by Agent domain at detection time (supports multiple values)	false	string []
			detectionAgentVersion__contains	Free-text filter by Agent version at detection time (supports multiple values)	false	string []
			detectionEngines	Included engines	false	string []
			detectionEnginesNin	Excluded engines	false	string []
			displayName	Display name	false	string
			engines	Included engines	false	string []
			enginesNin	Excluded engines	false	string []
			externalTicketExists	The threat contains ticket number	false	boolean
			externalTicketId__contains	Free-text filter by the threat external ticket ID (supports	false	string []

				multiple values)		
			externalTicketIds	External ticket ID for the threat	false	string []
			failedActions	At least one action failed on the threat	false	boolean
			filePath__contains	Free-text filter by file path (supports multiple values)	false	string []
			gcpServiceAccount__contains	Free-text filter by gcp service account (supports multiple values)	false	string []
			groupIds	List of Group IDs to filter by	false	string []
			hasAgentTags	Include only Threats whose Agent is assigned any tags if True, or none if False	false	boolean
			ids	List of threat IDs	false	string []
			incidentStatuses	Filter threats by a specific incident status	false	string []
			incidentStatusesNin	Exclude threats with specific incident statuses	false	string []

			initiatedBy	Only include threats from specific initiating sources	false	string []
			initiatedByNin	Exclude threats with specific initiating sources	false	string []
			initiatedByUsername__contains	Free-text filter by the username that initiated that threat (supports multiple values)	false	string []
			k8sClusterName__contains	Free-text filter by the endpoint Kubernetes cluster name (supports multiple values)	false	string []
			k8sControllerLabels__contains	Free-text filter by the endpoint Kubernetes controller labels (supports multiple values)	false	string []
			k8sControllerName__contains	Free-text filter by the endpoint Kubernetes controller name (supports multiple values)	false	string []

			k8sNamespaceLabels__contains	Free-text filter by the endpoint Kubernetes namespace labels (supports multiple values)	false	string []
			k8sNamespaceName__contains	Free-text filter by the endpoint Kubernetes namespace name (supports multiple values)	false	string []
			k8sNodeLabels__contains	Free-text filter by the endpoint Kubernetes node labels (supports multiple values)	false	string []
			k8sNodeName__contains	Free-text filter by the endpoint Kubernetes node name (supports multiple values)	false	string []
			k8sPodLabels__contains	Free-text filter by the endpoint Kubernetes pod labels (supports multiple values)	false	string []
			k8sPodName__contains	Free-text filter by the	false	string []

				endpoint Kubernetes pod name (supports multiple values)		
			mitigatedPreemptively	If the threat was detected pre-execution or post-execution	false	boolean
			mitigationStatuses	Filter threats by a specific status	false	string []
			mitigationStatusesNin	Filter threats not by a specific status	false	string []
			noteExists	The threat contains at least one note	false	boolean
			originatedProcess__contains	Free-text filter by the originated process name of the threat (supports multiple values)	false	string []
			osArchs	Included OS Architectures	false	string []
			osNames		false	string []
			osNamesNin		false	string []
			osTypes	Included OS types	false	string []
			osTypesNin	Excluded OS types	false	string []
			pendingActions	At least one action is pending for	false	boolean

				the Agent for the threat		
			publisherName__contains	Free-text filter by threat's publisher name (supports multiple values)	false	string []
			query	Full text search for fields: threat_details, content_hash, computer_name, file_path, uuid, detection_agent_version, realtime_agent_version, detection_agent_domain, command_line_arguments, initiated_by_username, storyline, originated_process, k8s_cluster_name, k8s_node_name, k8s_node_labels, k8s_namespace_name, k8s_namespace_labels, k8s_controller_name,	false	string

				k8s_controller_labels, k8s_pod_name, k8s_pod_labels, container_name, container_image_name, container_labels, external_ticket_id		
			realtimeAgentVersion__contains	Free-text filter by Agent version at current time (supports multiple values)	false	string []
			rebootRequired	A reboot is required on any endpoint for at least one action on the threat	false	boolean
			resolved	This is used for backward-compatibility with API 2.0.	false	boolean
			siteIds	List of Site IDs to filter by	false	string []
			storyline__contains	Free-text filter by threat storyline (supports multiple values)	false	string []
			storylines	List of Agent	false	string []

				context to search for		
			tenant	Indicates a tenant scope request	false	boolean
			threatDetails__contains	Free-text filter by threat details(supports multiple values)	false	string []
			updatedAt__gt	Updated at greater than.	false	string
			updatedAt__gte	Updated at greater or equal than.	false	string
			updatedAt__lt	Updated at lesser than.	false	string
			updatedAt__lte	Updated at lesser or equal than.	false	string
			uuid__contains	Free-text filter by Agent UUID (supports multiple values)	false	string []

Disable Engines

POST /web/api/v2.1/threats/engines/disable

If your list of threats shows too many False Positives, use this command to troubleshoot the Agent Engines that return unexpected results in your deployment. Valid values: "penetration", "dataFiles","exploits", "reputation", "executables", "preExecutionSuspicious", "preExecution", "lateralMovement", and "pup".

Response Messages

200 - Engines disabled

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>success</td><td>Indicates a successful operation</td><td>false</td><td>boolean</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

Name	Description	Required	Value
data	Data	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>engines</td><td>List of engines</td><td>false</td><td>string []</td></tr></table>

Exclusion Options

GET /web/api/v2.1/threats/{threat_id}/whitening-options

Get the Exclusion types that can be created from the detection data.
For example, if a threat is a file with a detected SHA1 hash and pathname, the values of the whiteningOptions in the response are "path" and "file_hash". This command requires the ID of the threat, which you can get from "threats" (see Get Threats). To create an Exclusion, see Exclusions.

Response Messages

200 - Success

401 - Unauthorized access - please sign in and retry.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>threatPolicy</td><td>Threat policy</td><td>false</td><td>string</td></tr>
<tr><td>threatType</td><td>Threat type</td><td>false</td><td>string []</td></tr>
<tr><td>whiteningOptions</td><td>Available exclusion options</td><td>false</td><td>string []</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Get Events

GET /web/api/v2.1/threats/{threat_id}/explore/events

Get all threat events.

Parameters

countonly	optional	If true, only total number of items will be returned, without any of the actual objects.
cursor	optional	Cursor position returned by the last request. Use to iterate over more than 1000 items. Example: "YWdlbnRfaWQ6NTgwMjkzODE=".
eventid	optional	Filter by a specific process key and its children
eventsubtypes	optional	Filter events by sub-type. Example: "PROCESSCREATION".
eventtypes	optional	Filter events by type. Example: "events".
limit	optional	Limit number of returned items (1-1000). Example: "10".
processname__like	optional	Filter by process name (substring)
skip	optional	Skip first number of items (0-1000). To iterate over more than 1000 items, use "cursor". Example: "150".
skipcount	optional	If true, total number of items will not be calculated, which speeds up execution time.
sortby	optional	The column to sort the results by. Example: "id".
sortorder	optional	Sort direction. Example: "asc".

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value

<table>
<tr><td>pagination</td><td>Pagination information</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>totalItems</td><td>Total number of items found matching your query</td><td>true</td><td>integer</td></tr>
<tr><td>nextCursor</td><td>Pass this value as "cursor" on your next request, to get the next page of results (Will be "null" when last page reached)</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>agentDomain</td><td>Agent domain</td><td>true</td><td>string</td></tr>
<tr><td>agentGroupId</td><td>Agent group id</td><td>true</td><td>string</td></tr>
<tr><td>agentId</td><td>Agent id</td><td>true</td><td>string</td></tr>
<tr><td>agentInfected</td><td>Agent infected</td><td>true</td><td>boolean</td></tr>
<tr><td>agentIp</td><td>Agent ip</td><td>true</td><td>string</td></tr>
<tr><td>agentIsActive</td><td>Agent is active</td><td>true</td><td>boolean</td></tr>
<tr><td>agentIsDecommissioned</td><td>Agent is decommissioned</td><td>true</td><td>boolean</td></tr>
<tr><td>agentMachineType</td><td>Agent machine type</td><td>true</td><td>string</td></tr>
<tr><td>agentName</td><td>Agent name</td><td>true</td><td>string</td></tr>
<tr><td>agentNetworkStatus</td><td>Agent network status</td><td>true</td><td>string</td></tr>
<tr><td>agentOs</td><td>OS type</td><td>true</td><td>enum</td></tr>
</table>
</td></tr>
</table>

			agentUuid	Agent uuid	true	string
			agentVersion	Agent version	true	string
			createdAt	Created at	true	string
			id	Id	true	string
			objectType	Object type	true	enum
			processName	Process name	true	string
			siteId	Site id	true	string
			siteName	Site name	true	string
			activeContentFileId	Active content file id	false	string
			activeContentHash	Active content hash	false	string
			activeContentPath	Active content path	false	string
			connectionStatus	Connection status	false	string
			direction	Direction	false	string
			dnsRequest	Dns request	false	string
			dnsResponse	Dns response	false	string
			dstIp	Dst ip	false	string
			dstPort	Dst port	false	integer
			eventType	Event type	false	string
			fileFullName	File full name	false	string
			fileId	File id	false	string
			fileMd5	File md5	false	string
			fileSha1	File sha1	false	string
			fileSha256	File sha256	false	string
			fileSize	File size	false	string
			fileType	File type	false	string
			hasActiveContent	Has active content	false	boolean
			indicatorCategory	Indicator category	false	string
			indicatorDesc	Indicator	false	string

			ription	description		
			indicatorMetadata	Indicator metadata	false	string
			indicatorName	Indicator name	false	string
			loginsBaseType	Logins base type	false	string
			loginsUserName	Logins user name	false	string
			md5	Md5	false	string
			networkMethod	Network method	false	string
			networkSource	Network source	false	string
			networkUrl	Network url	false	string
			oldFileMd5	Old file md5	false	string
			oldFileName	Old file name	false	string
			oldFileSha1	Old file sha1	false	string
			oldFileSha256	Old file sha256	false	string
			parentPid	Parent pid	false	string
			parentProcessGroupId	Parent process group id	false	string
			parentProcessIsMalicious	Parent process is malicious	false	boolean
			parentProcessName	Parent process name	false	string
			parentProcessUniqueKey	Parent process unique key	false	string
			pid	Pid	false	string
			processCmd	Process cmd	false	string
			processDisplayName	Process display name	false	string

			processGroupId	Process group id	false	string
			processImagePath	Process image path	false	string
			processImageSha1Hash	Process image sha1 hash	false	string
			processIntegrityLevel	Process integrity level	false	string
			processIsMalicious	Process is malicious	false	boolean
			processIsRedirectedCommandProcessor	Process is redirected command processor	false	string
			processIsWow64	Process is wow64	false	string
			processRoot	Process root	false	string
			processSessionId	Process session id	false	string
			processStartTime	Process start time	false	string
			processSubSystem	Process sub system	false	string
			processUniqueKey	Process unique key	false	string
			processUserName	Process user name	false	string
			protocol	Protocol	false	string
			publisher	Publisher	false	string
			registryClassification	Registry classification	false	string
			registryId	Registry id	false	string
			registryPath	Registry path	false	string
			relatedToThreat	Related to threat	false	boolean
			rpid	Rpid	false	string

			sha1 | Sha1 | false | string sha256 | Sha256 | false | string signatureSignedInvalidReason | Signature signed invalid reason | false | string signedStatus | Signed status | false | string srcIp | Src ip | false | string srcPort | Src port | false | integer storyline | Storyline | false | string taskName | Task name | false | string taskPath | Task path | false | string threatStatus | Threat status | false | string tid | Tid | false | string trueContext | [DEPRECATED] Use "storyline" instead | false | string user | User | false | string verifiedStatus | Verified status | false | string
errors	Errors	false	array

Add to Exclusions

POST /web/api/v2.1/threats/add-to-exclusions

Add a threat to exclusions. The "whitening option" is required.
When you create an exclusion, you override the "malicious" verdict of the Agent for a detection. This can open holes in your security deployment. Use with caution.
Best practice: Use the most specific definition of the exclusion possible and the lowest mode possible.

> **BEST PRACTICE**
>
> Use the most specific definition of the exclusion possible and the lowest mode possible.

Response Messages

200 - Added to exclusions

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
data	Response data	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>affected</td><td>Number of entities affected by the requested operation</td><td>false</td><td>integer</td></tr><tr><td>details</td><td>Result details for each threat</td><td>false</td><td><table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>analystVerdict</td><td>Result of changing the threat's analyst verdict as part of adding the threat to</td><td>false</td><td>enum</td></tr></table></td></tr></table>

							blocklist or exclusions		
						result	Result of adding the threat to blocklist or exclusions	false	enum
						threatId	Threat id	false	string
errors	Errors	false	array						

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>targetScope</td><td>Scope to be used for Exclusions</td><td>true</td><td>enum</td></tr>
<tr><td>type</td><td>Selected Exclusion type</td><td>true</td><td>enum</td></tr>
<tr><td>actions</td><td>Actions to perform</td><td>false</td><td>string []</td></tr>
<tr><td>description</td><td>Description</td><td>false</td><td>string</td></tr>
<tr><td>externalTicketId</td><td>External ticket id</td><td>false</td><td>string</td></tr>
<tr><td>macroModules</td><td>Macro modules</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>description</td><td>Description</td><td>false</td><td>string</td></tr>
<tr><td>hashes</td><td>Hashes</td><td>false</td><td>string []</td></tr>
</table>
</td></tr>
<tr><td>mode</td><td>Exclusion mode (path exclusion only)</td><td>false</td><td>enum</td></tr>
<tr><td>note</td><td>Note</td><td>false</td><td>string</td></tr>
<tr><td>pathExclusionType</td><td>Excluded path for a path exclusion list</td><td>false</td><td>string</td></tr>
<tr><td>value</td><td>Optional. If not provided, the relevant value from the Threat will be used</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>filter</td><td>Use any of the filtering options to control the list of</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
</table>
</td></tr>
</table>

	affected threats. You can use any combination of filters to narrow down the list (For example "apply to only active threats from Linux endpoints"). You can also leave this field empty to apply to all available threats.		agentIds	List of Agent IDs	false	string []	
			agentIsActive	Include Agents currently connected to the Management Console	false	boolean	
			agentMachineTypes	Include Agent machine types	false	string []	
			agentMachineTypesNin	Excluded Agent machine types	false	string []	
			agentTagsData	Filter threats by assigned tags to the related agent. Given in form of a JSON where each key represents a tag key, and each value represents a list of string values to filter by. To filter by unassigned tag values, use __nin suffix in the tag key.	false	string	
			agentVersions	Include Agent versions	false	string []	
			agentVersionsNin	Excluded Agent versions	false	string []	
			analystVerdic	Filter threats	false	string []	

			ts	by a specific analyst verdict		
			analystVerdictsNin	Exclude threats with specific analyst verdicts	false	string []
			awsRole__contains	Free-text filter by aws role(supports multiple values)	false	string []
			awsSecurityGroups__contains	Free-text filter by aws securityGroups(supports multiple values)	false	string []
			awsSubnetIds__contains	Free-text filter by aws subnet ids (supports multiple values)	false	string []
			azureResourceGroup__contains	Free-text filter by azure resource group(supports multiple values)	false	string []
			classifications	List of threat classifications to search	false	string []
			classificationsNin	List of threat classifications not to search	false	string []
			classificationSources	Classification sources list	false	string []
			classificationSourcesNin	Classification sources list to exclude	false	string []

			cloudAccount__contains	Free-text filter by cloud account (supports multiple values)	false	string []
			cloudImage__contains	Free-text filter by cloud image (supports multiple values)	false	string []
			cloudInstanceId__contains	Free-text filter by cloud instance id(supports multiple values)	false	string []
			cloudInstanceSize__contains	Free-text filter by cloud instance size(supports multiple values)	false	string []
			cloudLocation__contains	Free-text filter by cloud location (supports multiple values)	false	string []
			cloudNetwork__contains	Free-text filter by cloud network (supports multiple values)	false	string []
			cloudProvider	Agents from which cloud provider	false	string []
			cloudProviderNin	Exclude Agents from these cloud provider	false	string []

			collectionIds	List of collection IDs to search	false	string []	
			commandLineArguments__contains	Free-text filter by threat command line arguments (supports multiple values)	false	string []	
			computerName__contains	Free-text filter by computer name (supports multiple values)	false	string []	
			confidenceLevels	Filter threats by a specific confidence level	false	string []	
			confidenceLevelsNin	Exclude threats with specific confidence level	false	string []	
			containerImageName__contains	Free-text filter by the endpoint container image name (supports multiple values)	false	string []	
			containerLabels__contains	Free-text filter by the endpoint container labels (supports multiple	false	string []	

				values)		
			containerName__contains	Free-text filter by the endpoint container name (supports multiple values)	false	string []
			contentHash__contains	Free-text filter by file content hash (supports multiple values)	false	string []
			contentHashes	List of sha1 hashes to search for	false	string []
			countsFor	comma-separated list of fields to be shown	false	string
			createdAt__gt	Created at greater than.	false	string
			createdAt__gte	Created at greater or equal than.	false	string
			createdAt__lt	Created at lesser than.	false	string
			createdAt__lte	Created at lesser or equal than.	false	string
			detectionAgentDomain__contains	Free-text filter by Agent domain at detection time (supports multiple values)	false	string []

			detectionAgentVersion__contains	Free-text filter by Agent version at detection time (supports multiple values)	false	string []	
			detectionEngines	Included engines	false	string []	
			detectionEnginesNin	Excluded engines	false	string []	
			displayName	Display name	false	string	
			engines	Included engines	false	string []	
			enginesNin	Excluded engines	false	string []	
			externalTicketExists	The threat contains ticket number	false	boolean	
			externalTicketId__contains	Free-text filter by the threat external ticket ID (supports multiple values)	false	string []	
			externalTicketIds	External ticket ID for the threat	false	string []	
			failedActions	At least one action failed on the threat	false	boolean	
			filePath__contains	Free-text filter by file path (supports multiple values)	false	string []	
			gcpServiceAc	Free-text	false	string []	

			count__contains	filter by gcp service account (supports multiple values)			
			groupIds	List of Group IDs to filter by	false	string []	
			hasAgentTags	Include only Threats whose Agent is assigned any tags if True, or none if False	false	boolean	
			ids	List of threat IDs	false	string []	
			incidentStatuses	Filter threats by a specific incident status	false	string []	
			incidentStatusesNin	Exclude threats with specific incident statuses	false	string []	
			initiatedBy	Only include threats from specific initiating sources	false	string []	
			initiatedByNin	Exclude threats with specific initiating sources	false	string []	
			initiatedByUsername__contains	Free-text filter by the username that initiated that threat	false	string []	

				(supports multiple values)			
			k8sClusterName__contains	Free-text filter by the endpoint Kubernetes cluster name (supports multiple values)	false	string []	
			k8sControllerLabels__contains	Free-text filter by the endpoint Kubernetes controller labels (supports multiple values)	false	string []	
			k8sControllerName__contains	Free-text filter by the endpoint Kubernetes controller name (supports multiple values)	false	string []	
			k8sNamespaceLabels__contains	Free-text filter by the endpoint Kubernetes namespace labels (supports multiple values)	false	string []	
			k8sNamespaceName__contains	Free-text filter by the endpoint Kubernetes namespace name	false	string []	

				(supports multiple values)			
			k8sNodeLabels__contains	Free-text filter by the endpoint Kubernetes node labels (supports multiple values)	false	string []	
			k8sNodeName__contains	Free-text filter by the endpoint Kubernetes node name (supports multiple values)	false	string []	
			k8sPodLabels__contains	Free-text filter by the endpoint Kubernetes pod labels (supports multiple values)	false	string []	
			k8sPodName__contains	Free-text filter by the endpoint Kubernetes pod name (supports multiple values)	false	string []	
			limit	Limit	false	integer	
			mitigatedPreemptively	If the threat was detected pre-execution or post-execution	false	boolean	
			mitigationStatuses	Filter threats by a specific	false	string []	

				status			
			mitigationStatusesNin	Filter threats not by a specific status	false	string []	
			noteExists	The threat contains at least one note	false	boolean	
			originatedProcess__contains	Free-text filter by the originated process name of the threat (supports multiple values)	false	string []	
			osArchs	Included OS Architectures	false	string []	
			osNames		false	string []	
			osNamesNin		false	string []	
			osTypes	Included OS types	false	string []	
			osTypesNin	Excluded OS types	false	string []	
			pendingActions	At least one action is pending for the Agent for the threat	false	boolean	
			publisherName__contains	Free-text filter by threat's publisher name (supports multiple values)	false	string []	
			query	Full text search for fields:	false	string	

				threat_details, content_hash, computer_name, file_path, uuid, detection_agent_version, realtime_agent_version, detection_agent_domain, command_line_arguments, initiated_by_username, storyline, originated_process, k8s_cluster_name, k8s_node_name, k8s_node_labels, k8s_namespace_name, k8s_namespace_labels, k8s_controller_name, k8s_controller_labels, k8s_pod_name, k8s_pod_labels, container_name, container_image_name, container_labels, external_ticket_id			

			realtimeAgentVersion__contains	Free-text filter by Agent version at current time (supports multiple values)	false	string []	
			rebootRequired	A reboot is required on any endpoint for at least one action on the threat	false	boolean	
			resolved	This is used for backward-compatibility with API 2.0.	false	boolean	
			siteIds	List of Site IDs to filter by	false	string []	
			storyline__contains	Free-text filter by threat storyline (supports multiple values)	false	string []	
			storylines	List of Agent context to search for	false	string []	
			tenant	Indicates a tenant scope request	false	boolean	
			threatDetails__contains	Free-text filter by threat details(supports multiple values)	false	string []	
			updatedAt__gt	Updated at greater than.	false	string	

			updatedAt__gte	Updated at greater or equal than.	false	string	
			updatedAt__lt	Updated at lesser than.	false	string	
			updatedAt__lte	Updated at lesser or equal than.	false	string	
			uuid__contains	Free-text filter by Agent UUID (supports multiple values)	false	string []	

Export Threats

GET /web/api/v2.1/threats/export

Export data of threats (as seen in the Console > Incidents) that match the filter. Note: Use the filter. This command exports only 20,000 items (each datum is an item).

Parameters

accountids	optional	List of Account IDs to filter by. Example: "225494730938493804,225494730938493915".
agentids	optional	List of Agent IDs. Example: "225494730938493804,225494730938493915".
agentisactive	optional	Include Agents currently connected to the Management Console
agentmachinetypes	optional	Include Agent machine types. Example: "unknown".
agentmachinetypesnin	optional	Excluded Agent machine types. Example: "unknown".
agenttagsdata	optional	Filter threats by assigned tags to the related agent. Given in form of a JSON where each key represents a tag key, and each value represents a list of string values to filter by. To filter by unassigned tag values, use __nin suffix in the tag key. Example: "{"key1": ["value1_1", "value1_2"], "key2__nin": ["value2"]}".
agentversions	optional	Include Agent versions. Example: "2.5.1.1320".
agentversionsnin	optional	Excluded Agent versions. Example: "2.5.1.1320".
analystverdicts	optional	Filter threats by a specific analyst verdict. Example: "true_positive,suspicious".
analystverdictsnin	optional	Exclude threats with specific analyst verdicts. Example: "true_positive,suspicious".
awsrole__contains	optional	Free-text filter by aws role(supports multiple values)
awssecuritygroups__contains	optional	Free-text filter by aws securityGroups(supports multiple values)
awssubnetids__contains	optional	Free-text filter by aws subnet ids (supports multiple values)
azureresourcegroup__contains	optional	Free-text filter by azure resource group(supports multiple values)
classifications	optional	List of threat classifications to search
classificationsnin	optional	List of threat classifications not to search

classificationsources	optional	Classification sources list. Example: "Cloud".
classificationsourcesnin	optional	Classification sources list to exclude. Example: "Cloud".
cloudaccount__contains	optional	Free-text filter by cloud account (supports multiple values)
cloudimage__contains	optional	Free-text filter by cloud image (supports multiple values)
cloudinstanceid__contains	optional	Free-text filter by cloud instance id(supports multiple values)
cloudinstancesize__contains	optional	Free-text filter by cloud instance size(supports multiple values)
cloudlocation__contains	optional	Free-text filter by cloud location (supports multiple values)
cloudnetwork__contains	optional	Free-text filter by cloud network (supports multiple values)
cloudprovider	optional	Agents from which cloud provider
cloudprovidernin	optional	Exclude Agents from these cloud provider
collectionids	optional	List of collection IDs to search. Example: "225494730938493804,225494730938493915".
commandlineargument s__contains	optional	Free-text filter by threat command line arguments (supports multiple values). Example: "/usr/sbin/,wget".
computername__contains	optional	Free-text filter by computer name (supports multiple values). Example: "john-office,WIN".
confidencelevels	optional	Filter threats by a specific confidence level. Example: "malicious".
confidencelevelsnin	optional	Exclude threats with specific confidence level. Example: "malicious".
containerimagename__contains	optional	Free-text filter by the endpoint container image name (supports multiple values)
containerlabels__contains	optional	Free-text filter by the endpoint container labels (supports multiple values)
containername__contains	optional	Free-text filter by the endpoint container name (supports multiple values)
contenthash__contains	optional	Free-text filter by file content hash (supports multiple values). Example: "5f09bcff3".
contenthashes	optional	List of sha1 hashes to search for. Example: "d,d,d,5,0,3,0,a,3,d,0,2,9,f,3,8,4,5,f,c,1,0,5,2,4,1,9,8,2,9,f,0,8,f,3,1,2,2,

		4,0".
countsfor	optional	comma-separated list of fields to be shown. Example: "osTypes,machineTypes".
createdat__gt	optional	Created at greater than. Example: "2018-02-27T04:49:26.257525Z".
createdat__gte	optional	Created at greater or equal than. Example: "2018-02-27T04:49:26.257525Z".
createdat__lt	optional	Created at lesser than. Example: "2018-02-27T04:49:26.257525Z".
createdat__lte	optional	Created at lesser or equal than. Example: "2018-02-27T04:49:26.257525Z".
detectionagentdomain__contains	optional	Free-text filter by Agent domain at detection time (supports multiple values). Example: "sentinel,sentinelone.com".
detectionagentversion__contains	optional	Free-text filter by Agent version at detection time (supports multiple values). Example: "1.1.1.1,2.2.".
detectionengines	optional	Included engines. Example: "reputation".
detectionenginesnin	optional	Excluded engines. Example: "reputation".
displayname	optional	Display name
engines	optional	Included engines. Example: "reputation".
enginesnin	optional	Excluded engines. Example: "reputation".
externalticketexists	optional	The threat contains ticket number
externalticketid__contains	optional	Free-text filter by the threat external ticket ID (supports multiple values)
externalticketids	optional	External ticket ID for the threat
failedactions	optional	At least one action failed on the threat
filepath__contains	optional	Free-text filter by file path (supports multiple values). Example: "\MyUser\Downloads".
gcpserviceaccount__contains	optional	Free-text filter by gcp service account (supports multiple values)
groupids	optional	List of Group IDs to filter by. Example: "225494730938493804,225494730938493915".
hasagenttags	optional	Include only Threats whose Agent is assigned any tags if True, or none if False
ids	optional	List of threat IDs. Example:

		"225494730938493804,225494730938493915".
incidentstatuses	optional	Filter threats by a specific incident status. Example: "unresolved,in_progress".
incidentstatusesnin	optional	Exclude threats with specific incident statuses. Example: "unresolved,in_progress".
initiatedby	optional	Only include threats from specific initiating sources. Example: "agent_policy,dv_command".
initiatedbynin	optional	Exclude threats with specific initiating sources. Example: "agent_policy,dv_command".
initiatedbyusername__contains	optional	Free-text filter by the username that initiated that threat (supports multiple values). Example: "John,John Doe".
k8sclustername__contains	optional	Free-text filter by the endpoint Kubernetes cluster name (supports multiple values)
k8scontrollerlabels__contains	optional	Free-text filter by the endpoint Kubernetes controller labels (supports multiple values)
k8scontrollername__contains	optional	Free-text filter by the endpoint Kubernetes controller name (supports multiple values)
k8snamespacelabels__contains	optional	Free-text filter by the endpoint Kubernetes namespace labels (supports multiple values)
k8snamespacename__contains	optional	Free-text filter by the endpoint Kubernetes namespace name (supports multiple values)
k8snodelabels__contains	optional	Free-text filter by the endpoint Kubernetes node labels (supports multiple values)
k8snodename__contains	optional	Free-text filter by the endpoint Kubernetes node name (supports multiple values)
k8spodlabels__contains	optional	Free-text filter by the endpoint Kubernetes pod labels (supports multiple values)
k8spodname__contains	optional	Free-text filter by the endpoint Kubernetes pod name (supports multiple values)
mitigatedpreemptively	optional	If the threat was detected pre-execution or post-execution
mitigationstatuses	optional	Filter threats by a specific status. Example: "not_mitigated".
mitigationstatusesnin	optional	Filter threats not by a specific status. Example: "not_mitigated".
noteexists	optional	The threat contains at least one note
originatedprocess__co	optional	Free-text filter by the originated process name of the threat

ntains		(supports multiple values)
osarchs	optional	Included OS Architectures. Example: "32 bit".
osnames	optional	
osnamesnin	optional	
ostypes	optional	Included OS types. Example: "macos".
ostypesnin	optional	Excluded OS types. Example: "macos".
pendingactions	optional	At least one action is pending for the Agent for the threat
publishername__contains	optional	Free-text filter by threat's publisher name (supports multiple values). Example: "GOOGLE,Apple Inc.".
query	optional	Full text search for fields: threat_details, content_hash, computer_name, file_path, uuid, detection_agent_version, realtime_agent_version, detection_agent_domain, command_line_arguments, initiated_by_username, storyline, originated_process, k8s_cluster_name, k8s_node_name, k8s_node_labels, k8s_namespace_name, k8s_namespace_labels, k8s_controller_name, k8s_controller_labels, k8s_pod_name, k8s_pod_labels, container_name, container_image_name, container_labels, external_ticket_id
realtimeagentversion__contains	optional	Free-text filter by Agent version at current time (supports multiple values). Example: "1.1.1.1,2.2.".
rebootrequired	optional	A reboot is required on any endpoint for at least one action on the threat
resolved	optional	This is used for backward-compatibility with API 2.0.
siteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".
storyline__contains	optional	Free-text filter by threat storyline (supports multiple values). Example: "0000C2E97648,0006FC73-77B4-470F-AAC7-".
storylines	optional	List of Agent context to search for
tenant	optional	Indicates a tenant scope request
threatdetails__contains	optional	Free-text filter by threat details(supports multiple values). Example: "malware.exe,virus.exe".
updatedat__gt	optional	Updated at greater than. Example: "2018-02-27T04:49:26.257525Z".
updatedat__gte	optional	Updated at greater or equal than. Example:

		"2018-02-27T04:49:26.257525Z".
updatedat__lt	optional	Updated at lesser than. Example: "2018-02-27T04:49:26.257525Z".
updatedat__lte	optional	Updated at lesser or equal than. Example: "2018-02-27T04:49:26.257525Z".
uuid__contains	optional	Free-text filter by Agent UUID (supports multiple values). Example: "e92-01928,b055".

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Add to Blocklist (Deep Visibility)

POST /web/api/v2.1/threats/dv-add-to-blacklist

From Deep Visibility results, add a SHA1 hash to the Blocklist. Set the scope of the Blocklist: Global, Account, Site, or Group. The SHA1 and the Agent ID are required (see Deep Visibility > Get Events). Your role must have permissions to change the Blocklist - Admin, IR Team, SOC - and your user scope access must include the scope of the Agent. The target scope is the Group, Site, or Account of the Agent.
Deep Visibility requires Complete SKU.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
affected	Number of	false	integer

				entities affected by the requested operation		
errors	Errors	false	array			

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>targetScope</td><td>Scope of Restrictions to which each hash is added</td><td>true</td><td>enum</td></tr>
<tr><td>hashes</td><td>List of hashes with their source agents</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>agentId</td><td>Agent that reported the DV event</td><td>true</td><td>string</td></tr>
<tr><td>hash</td><td>Hash to add to Restrictions</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
</table>
</td></tr>
</table>

Mark as Threat (Deep Visibility)

POST /web/api/v2.1/threats/dv-mark-as-threat

Mark an event from Deep Visibility data as a threat. (see Deep Visibility > Get Events).Your role must have permissions to Mark as Threat - Admin, IR Team, SOC. The item becomes marked as a threat and the Management adds it to the blocklist. If this threat is detected on an endpoint, the Agent blocks it immediately.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>affected</td><td>Number of entities affected by the requested operation</td><td>false</td><td>integer</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>status</td><td>Desired status to mark the events with</td><td>true</td><td>enum</td></tr>
<tr><td>events</td><td>List of DV events with their agents</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>agentId</td><td>Agent that reported the DV event</td><td>true</td><td>string</td></tr>
<tr><td>storyline</td><td>Storyline of the marked event</td><td>true</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>initiatedBy</td><td>Initiated by</td><td>false</td><td>enum</td></tr>
</table>
</td></tr>
</table>

Export Mitigation Report

GET /web/api/v2.1/threats/mitigation-report/{report_id}

Export the mitigation report as a CSV file.

Response Messages

200 - Success

401 - Unauthorized access - please sign in and retry.

Updated Threat Incident

POST /web/api/v2.1/threats/incident

Update the incident details of a threat.

Response Messages

200 - Threats incident successfully updated

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>affected</td><td>Number of entities affected by the requested operation</td><td>false</td><td>integer</td></tr>
<tr><td>details</td><td>Result details for each</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
</table>
</td></tr>
</table>
</td></tr>
</table>

				threat		analystVerdict	Result of changing the threat's analyst verdict as part of changing the threat's status	false	enum
						result	Result of changing the threat's status	false	enum
						threatId	Threat id	false	string
errors	Errors	false	array						

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>incidentStatus</td><td>Incident status</td><td>true</td><td>enum</td></tr>
<tr><td>analystVerdict</td><td>The analyst verdict to set for the Threats</td><td>false</td><td>enum</td></tr>
</table>
</td></tr>
<tr><td>filter</td><td>Filter</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>agentIds</td><td>List of Agent IDs</td><td>false</td><td>string []</td></tr>
<tr><td>agentIsActive</td><td>Include Agents currently connected to the Management Console</td><td>false</td><td>boolean</td></tr>
<tr><td>agentMachineTypes</td><td>Include Agent machine types</td><td>false</td><td>string []</td></tr>
<tr><td>agentMachineTypesNin</td><td>Excluded Agent machine types</td><td>false</td><td>string []</td></tr>
<tr><td>agentTagsData</td><td>Filter threats by assigned tags to the related agent. Given in form of a JSON where each key represents a tag key, and</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
</table>

				each value represents a list of string values to filter by. To filter by unassigned tag values, use __nin suffix in the tag key.		
			agentVersions	Include Agent versions	false	string []
			agentVersionsNin	Excluded Agent versions	false	string []
			analystVerdicts	Filter threats by a specific analyst verdict	false	string []
			analystVerdictsNin	Exclude threats with specific analyst verdicts	false	string []
			awsRole__contains	Free-text filter by aws role(supports multiple values)	false	string []
			awsSecurityGroups__contains	Free-text filter by aws securityGroups(supports multiple values)	false	string []
			awsSubnetIds__contains	Free-text filter by aws subnet ids (supports multiple values)	false	string []

			azureResourceGroup__contains	Free-text filter by azure resource group(supports multiple values)	false	string []
			classifications	List of threat classifications to search	false	string []
			classificationsNin	List of threat classifications not to search	false	string []
			classificationSources	Classification sources list	false	string []
			classificationSourcesNin	Classification sources list to exclude	false	string []
			cloudAccount__contains	Free-text filter by cloud account (supports multiple values)	false	string []
			cloudImage__contains	Free-text filter by cloud image (supports multiple values)	false	string []
			cloudInstanceId__contains	Free-text filter by cloud instance id(supports multiple values)	false	string []
			cloudInstanceSize__contains	Free-text filter by cloud instance size(supports multiple values)	false	string []
			cloudLocation	Free-text	false	string []

			__contains	filter by cloud location (supports multiple values)		
			cloudNetwork__contains	Free-text filter by cloud network (supports multiple values)	false	string []
			cloudProvider	Agents from which cloud provider	false	string []
			cloudProvideRNin	Exclude Agents from these cloud provider	false	string []
			collectionIds	List of collection IDs to search	false	string []
			commandLineArguments__contains	Free-text filter by threat command line arguments (supports multiple values)	false	string []
			computerName__contains	Free-text filter by computer name (supports multiple values)	false	string []
			confidenceLevels	Filter threats by a specific confidence level	false	string []
			confidenceLe	Exclude	false	string []

			velsNin	threats with specific confidence level		
			containerImageName__contains	Free-text filter by the endpoint container image name (supports multiple values)	false	string []
			containerLabels__contains	Free-text filter by the endpoint container labels (supports multiple values)	false	string []
			containerName__contains	Free-text filter by the endpoint container name (supports multiple values)	false	string []
			contentHash__contains	Free-text filter by file content hash (supports multiple values)	false	string []
			contentHashes	List of sha1 hashes to search for	false	string []
			countsFor	comma-separated list of fields to be shown	false	string
			createdAt__gt	Created at greater than.	false	string

			createdAt__gte	Created at greater or equal than.	false	string
			createdAt__lt	Created at lesser than.	false	string
			createdAt__lte	Created at lesser or equal than.	false	string
			detectionAgentDomain__contains	Free-text filter by Agent domain at detection time (supports multiple values)	false	string []
			detectionAgentVersion__contains	Free-text filter by Agent version at detection time (supports multiple values)	false	string []
			detectionEngines	Included engines	false	string []
			detectionEnginesNin	Excluded engines	false	string []
			displayName	Display name	false	string
			engines	Included engines	false	string []
			enginesNin	Excluded engines	false	string []
			externalTicketExists	The threat contains ticket number	false	boolean
			externalTicketId__contains	Free-text filter by the threat external	false	string []

				ticket ID (supports multiple values)		
			externalTicketIds	External ticket ID for the threat	false	string []
			failedActions	At least one action failed on the threat	false	boolean
			filePath__contains	Free-text filter by file path (supports multiple values)	false	string []
			gcpServiceAccount__contains	Free-text filter by gcp service account (supports multiple values)	false	string []
			groupIds	List of Group IDs to filter by	false	string []
			hasAgentTags	Include only Threats whose Agent is assigned any tags if True, or none if False	false	boolean
			ids	List of threat IDs	false	string []
			incidentStatuses	Filter threats by a specific incident status	false	string []
			incidentStatusesNin	Exclude threats with specific	false	string []

				incident statuses		
			initiatedBy	Only include threats from specific initiating sources	false	string []
			initiatedByNin	Exclude threats with specific initiating sources	false	string []
			initiatedByUsername__contains	Free-text filter by the username that initiated that threat (supports multiple values)	false	string []
			k8sClusterName__contains	Free-text filter by the endpoint Kubernetes cluster name (supports multiple values)	false	string []
			k8sControllerLabels__contains	Free-text filter by the endpoint Kubernetes controller labels (supports multiple values)	false	string []
			k8sControllerName__contains	Free-text filter by the endpoint Kubernetes controller name	false	string []

				(supports multiple values)		
			k8sNamespaceLabels__contains	Free-text filter by the endpoint Kubernetes namespace labels (supports multiple values)	false	string []
			k8sNamespaceName__contains	Free-text filter by the endpoint Kubernetes namespace name (supports multiple values)	false	string []
			k8sNodeLabels__contains	Free-text filter by the endpoint Kubernetes node labels (supports multiple values)	false	string []
			k8sNodeName__contains	Free-text filter by the endpoint Kubernetes node name (supports multiple values)	false	string []
			k8sPodLabels__contains	Free-text filter by the endpoint Kubernetes pod labels (supports multiple	false	string []

				values)		
			k8sPodName__contains	Free-text filter by the endpoint Kubernetes pod name (supports multiple values)	false	string []
			limit	Limit	false	integer
			mitigatedPreemptively	If the threat was detected pre-execution or post-execution	false	boolean
			mitigationStatuses	Filter threats by a specific status	false	string []
			mitigationStatusesNin	Filter threats not by a specific status	false	string []
			noteExists	The threat contains at least one note	false	boolean
			originatedProcess__contains	Free-text filter by the originated process name of the threat (supports multiple values)	false	string []
			osArchs	Included OS Architectures	false	string []
			osNames		false	string []
			osNamesNin		false	string []
			osTypes	Included OS types	false	string []

			osTypesNin	Excluded OS types	false	string []
			pendingActions	At least one action is pending for the Agent for the threat	false	boolean
			publisherName__contains	Free-text filter by threat's publisher name (supports multiple values)	false	string []
			query	Full text search for fields: threat_details, content_hash, computer_name, file_path, uuid, detection_agent_version, realtime_agent_version, detection_agent_domain, command_line_arguments, initiated_by_username, storyline, originated_process, k8s_cluster_name, k8s_node_name, k8s_node_labels, k8s_namespa	false	string

				ce_name, k8s_namespace_labels, k8s_controller_name, k8s_controller_labels, k8s_pod_name, k8s_pod_labels, container_name, container_image_name, container_labels, external_ticket_id		
			realtimeAgentVersion__contains	Free-text filter by Agent version at current time (supports multiple values)	false	string []
			rebootRequired	A reboot is required on any endpoint for at least one action on the threat	false	boolean
			resolved	This is used for backward-compatibility with API 2.0.	false	boolean
			siteIds	List of Site IDs to filter by	false	string []
			storyline__contains	Free-text filter by threat storyline	false	string []

				(supports multiple values)		
			storylines	List of Agent context to search for	false	string []
			tenant	Indicates a tenant scope request	false	boolean
			threatDetails__contains	Free-text filter by threat details(supports multiple values)	false	string []
			updatedAt__gt	Updated at greater than.	false	string
			updatedAt__gte	Updated at greater or equal than.	false	string
			updatedAt__lt	Updated at lesser than.	false	string
			updatedAt__lte	Updated at lesser or equal than.	false	string
			uuid__contains	Free-text filter by Agent UUID (supports multiple values)	false	string []

Update Threat Analyst Verdict

POST /web/api/v2.1/threats/analyst-verdict

Change the verdict of a threat, as determined by a Console user.

Response Messages

200 - Threats analyst verdict successfully updated

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>affected</td><td>Number of entities affected by the requested operation</td><td>false</td><td>integer</td></tr>
<tr><td>details</td><td>Result details for each threat</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>result</td><td>Result of changing the threat's analyst verdict</td><td>false</td><td>enum</td></tr>
<tr><td>threatId</td><td>Threat id</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>analystVerdict</td><td>Analyst verdict</td><td>true</td><td>enum</td></tr>
</table>
</td></tr>
<tr><td>filter</td><td>Filter</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>agentIds</td><td>List of Agent IDs</td><td>false</td><td>string []</td></tr>
<tr><td>agentIsActive</td><td>Include Agents currently connected to the Management Console</td><td>false</td><td>boolean</td></tr>
<tr><td>agentMachineTypes</td><td>Include Agent machine types</td><td>false</td><td>string []</td></tr>
<tr><td>agentMachineTypesNin</td><td>Excluded Agent machine types</td><td>false</td><td>string []</td></tr>
<tr><td>agentTagsData</td><td>Filter threats by assigned tags to the related agent. Given in form of a JSON where each key represents a tag key, and each value represents a list of string values to</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
</table>

				filter by. To filter by unassigned tag values, use __nin suffix in the tag key.		
			agentVersions	Include Agent versions	false	string []
			agentVersionsNin	Excluded Agent versions	false	string []
			analystVerdicts	Filter threats by a specific analyst verdict	false	string []
			analystVerdictsNin	Exclude threats with specific analyst verdicts	false	string []
			awsRole__contains	Free-text filter by aws role(supports multiple values)	false	string []
			awsSecurityGroups__contains	Free-text filter by aws securityGroups(supports multiple values)	false	string []
			awsSubnetIds__contains	Free-text filter by aws subnet ids (supports multiple values)	false	string []
			azureResourceGroup__contains	Free-text filter by azure resource group(support	false	string []

				s multiple values)		
			classifications	List of threat classifications to search	false	string []
			classificationsNin	List of threat classifications not to search	false	string []
			classificationSources	Classification sources list	false	string []
			classificationSourcesNin	Classification sources list to exclude	false	string []
			cloudAccount__contains	Free-text filter by cloud account (supports multiple values)	false	string []
			cloudImage__contains	Free-text filter by cloud image (supports multiple values)	false	string []
			cloudInstanceId__contains	Free-text filter by cloud instance id(supports multiple values)	false	string []
			cloudInstanceSize__contains	Free-text filter by cloud instance size(supports multiple values)	false	string []
			cloudLocation__contains	Free-text filter by cloud location (supports multiple	false	string []

				values)		
			cloudNetwork__contains	Free-text filter by cloud network (supports multiple values)	false	string []
			cloudProvider	Agents from which cloud provider	false	string []
			cloudProviderNin	Exclude Agents from these cloud provider	false	string []
			collectionIds	List of collection IDs to search	false	string []
			commandLineArguments__contains	Free-text filter by threat command line arguments (supports multiple values)	false	string []
			computerName__contains	Free-text filter by computer name (supports multiple values)	false	string []
			confidenceLevels	Filter threats by a specific confidence level	false	string []
			confidenceLevelsNin	Exclude threats with specific confidence level	false	string []

			containerImageName__contains	Free-text filter by the endpoint container image name (supports multiple values)	false	string []
			containerLabels__contains	Free-text filter by the endpoint container labels (supports multiple values)	false	string []
			containerName__contains	Free-text filter by the endpoint container name (supports multiple values)	false	string []
			contentHash__contains	Free-text filter by file content hash (supports multiple values)	false	string []
			contentHashes	List of sha1 hashes to search for	false	string []
			countsFor	comma-separated list of fields to be shown	false	string
			createdAt__gt	Created at greater than.	false	string
			createdAt__gte	Created at greater or equal than.	false	string

			createdAt__lt	Created at lesser than.	false	string
			createdAt__lte	Created at lesser or equal than.	false	string
			detectionAgentDomain__contains	Free-text filter by Agent domain at detection time (supports multiple values)	false	string []
			detectionAgentVersion__contains	Free-text filter by Agent version at detection time (supports multiple values)	false	string []
			detectionEngines	Included engines	false	string []
			detectionEnginesNin	Excluded engines	false	string []
			displayName	Display name	false	string
			engines	Included engines	false	string []
			enginesNin	Excluded engines	false	string []
			externalTicketExists	The threat contains ticket number	false	boolean
			externalTicketId__contains	Free-text filter by the threat external ticket ID (supports multiple	false	string []

				values)		
			externalTicketIds	External ticket ID for the threat	false	string []
			failedActions	At least one action failed on the threat	false	boolean
			filePath__contains	Free-text filter by file path (supports multiple values)	false	string []
			gcpServiceAccount__contains	Free-text filter by gcp service account (supports multiple values)	false	string []
			groupIds	List of Group IDs to filter by	false	string []
			hasAgentTags	Include only Threats whose Agent is assigned any tags if True, or none if False	false	boolean
			ids	List of threat IDs	false	string []
			incidentStatuses	Filter threats by a specific incident status	false	string []
			incidentStatusesNin	Exclude threats with specific incident statuses	false	string []

			initiatedBy	Only include threats from specific initiating sources	false	string []
			initiatedByNin	Exclude threats with specific initiating sources	false	string []
			initiatedByUsername__contains	Free-text filter by the username that initiated that threat (supports multiple values)	false	string []
			k8sClusterName__contains	Free-text filter by the endpoint Kubernetes cluster name (supports multiple values)	false	string []
			k8sControllerLabels__contains	Free-text filter by the endpoint Kubernetes controller labels (supports multiple values)	false	string []
			k8sControllerName__contains	Free-text filter by the endpoint Kubernetes controller name (supports multiple values)	false	string []

			k8sNamespaceLabels__contains	Free-text filter by the endpoint Kubernetes namespace labels (supports multiple values)	false	string []
			k8sNamespaceName__contains	Free-text filter by the endpoint Kubernetes namespace name (supports multiple values)	false	string []
			k8sNodeLabels__contains	Free-text filter by the endpoint Kubernetes node labels (supports multiple values)	false	string []
			k8sNodeName__contains	Free-text filter by the endpoint Kubernetes node name (supports multiple values)	false	string []
			k8sPodLabels__contains	Free-text filter by the endpoint Kubernetes pod labels (supports multiple values)	false	string []
			k8sPodName__contains	Free-text filter by the	false	string []

				endpoint Kubernetes pod name (supports multiple values)		
			limit	Limit	false	integer
			mitigatedPreemptively	If the threat was detected pre-execution or post-execution	false	boolean
			mitigationStatuses	Filter threats by a specific status	false	string []
			mitigationStatusesNin	Filter threats not by a specific status	false	string []
			noteExists	The threat contains at least one note	false	boolean
			originatedProcess__contains	Free-text filter by the originated process name of the threat (supports multiple values)	false	string []
			osArchs	Included OS Architectures	false	string []
			osNames		false	string []
			osNamesNin		false	string []
			osTypes	Included OS types	false	string []
			osTypesNin	Excluded OS types	false	string []
			pendingActio	At least one	false	boolean

			ns	action is pending for the Agent for the threat		
			publisherName__contains	Free-text filter by threat's publisher name (supports multiple values)	false	string []
			query	Full text search for fields: threat_details, content_hash, computer_name, file_path, uuid, detection_agent_version, realtime_agent_version, detection_agent_domain, command_line_arguments, initiated_by_username, storyline, originated_process, k8s_cluster_name, k8s_node_name, k8s_node_labels, k8s_namespace_name, k8s_namespace_labels,	false	string

				k8s_controller_name, k8s_controller_labels, k8s_pod_name, k8s_pod_labels, container_name, container_image_name, container_labels, external_ticket_id		
			realtimeAgentVersion__contains	Free-text filter by Agent version at current time (supports multiple values)	false	string []
			rebootRequired	A reboot is required on any endpoint for at least one action on the threat	false	boolean
			resolved	This is used for backward-compatibility with API 2.0.	false	boolean
			siteIds	List of Site IDs to filter by	false	string []
			storyline__contains	Free-text filter by threat storyline (supports multiple values)	false	string []

			storylines	List of Agent context to search for	false	string []
			tenant	Indicates a tenant scope request	false	boolean
			threatDetails__contains	Free-text filter by threat details(supports multiple values)	false	string []
			updatedAt__gt	Updated at greater than.	false	string
			updatedAt__gte	Updated at greater or equal than.	false	string
			updatedAt__lt	Updated at lesser than.	false	string
			updatedAt__lte	Updated at lesser or equal than.	false	string
			uuid__contains	Free-text filter by Agent UUID (supports multiple values)	false	string []

Update Threat External Ticket ID

POST /web/api/v2.1/threats/external-ticket-id

Change the external ticket ID of a threat.

Response Messages

200 - Threats external ticket id successfully updated

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
data	Response data	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>affected</td><td>Number of entities affected by the requested operation</td><td>false</td><td>integer</td></tr></table>
errors	Errors	false	array

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>externalTicketId</td><td>External ticket id</td><td>true</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>filter</td><td>Filter</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>agentIds</td><td>List of Agent IDs</td><td>false</td><td>string []</td></tr>
<tr><td>agentIsActive</td><td>Include Agents currently connected to the Management Console</td><td>false</td><td>boolean</td></tr>
<tr><td>agentMachineTypes</td><td>Include Agent machine types</td><td>false</td><td>string []</td></tr>
<tr><td>agentMachineTypesNin</td><td>Excluded Agent machine types</td><td>false</td><td>string []</td></tr>
<tr><td>agentTagsData</td><td>Filter threats by assigned tags to the related agent. Given in form of a JSON where each key represents a tag key, and each value represents a list of string values to</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
</table>

				filter by. To filter by unassigned tag values, use __nin suffix in the tag key.		
			agentVersions	Include Agent versions	false	string []
			agentVersionsNin	Excluded Agent versions	false	string []
			analystVerdicts	Filter threats by a specific analyst verdict	false	string []
			analystVerdictsNin	Exclude threats with specific analyst verdicts	false	string []
			awsRole__contains	Free-text filter by aws role(supports multiple values)	false	string []
			awsSecurityGroups__contains	Free-text filter by aws securityGroups(supports multiple values)	false	string []
			awsSubnetIds__contains	Free-text filter by aws subnet ids (supports multiple values)	false	string []
			azureResourceGroup__contains	Free-text filter by azure resource group(support	false	string []

				s multiple values)		
			classifications	List of threat classifications to search	false	string []
			classificationsNin	List of threat classifications not to search	false	string []
			classificationSources	Classification sources list	false	string []
			classificationSourcesNin	Classification sources list to exclude	false	string []
			cloudAccount__contains	Free-text filter by cloud account (supports multiple values)	false	string []
			cloudImage__contains	Free-text filter by cloud image (supports multiple values)	false	string []
			cloudInstanceId__contains	Free-text filter by cloud instance id(supports multiple values)	false	string []
			cloudInstanceSize__contains	Free-text filter by cloud instance size(supports multiple values)	false	string []
			cloudLocation__contains	Free-text filter by cloud location (supports multiple	false	string []

				values)		
			cloudNetwork__contains	Free-text filter by cloud network (supports multiple values)	false	string []
			cloudProvider	Agents from which cloud provider	false	string []
			cloudProviderNin	Exclude Agents from these cloud provider	false	string []
			collectionIds	List of collection IDs to search	false	string []
			commandLineArguments__contains	Free-text filter by threat command line arguments (supports multiple values)	false	string []
			computerName__contains	Free-text filter by computer name (supports multiple values)	false	string []
			confidenceLevels	Filter threats by a specific confidence level	false	string []
			confidenceLevelsNin	Exclude threats with specific confidence level	false	string []

			containerImageName__contains	Free-text filter by the endpoint container image name (supports multiple values)	false	string []
			containerLabels__contains	Free-text filter by the endpoint container labels (supports multiple values)	false	string []
			containerName__contains	Free-text filter by the endpoint container name (supports multiple values)	false	string []
			contentHash__contains	Free-text filter by file content hash (supports multiple values)	false	string []
			contentHashes	List of sha1 hashes to search for	false	string []
			countsFor	comma-separated list of fields to be shown	false	string
			createdAt__gt	Created at greater than.	false	string
			createdAt__gte	Created at greater or equal than.	false	string

			createdAt__lt	Created at lesser than.	false	string
			createdAt__lte	Created at lesser or equal than.	false	string
			detectionAgentDomain__contains	Free-text filter by Agent domain at detection time (supports multiple values)	false	string []
			detectionAgentVersion__contains	Free-text filter by Agent version at detection time (supports multiple values)	false	string []
			detectionEngines	Included engines	false	string []
			detectionEnginesNin	Excluded engines	false	string []
			displayName	Display name	false	string
			engines	Included engines	false	string []
			enginesNin	Excluded engines	false	string []
			externalTicketExists	The threat contains ticket number	false	boolean
			externalTicketId__contains	Free-text filter by the threat external ticket ID (supports multiple	false	string []

				values)		
			externalTicketIds	External ticket ID for the threat	false	string []
			failedActions	At least one action failed on the threat	false	boolean
			filePath__contains	Free-text filter by file path (supports multiple values)	false	string []
			gcpServiceAccount__contains	Free-text filter by gcp service account (supports multiple values)	false	string []
			groupIds	List of Group IDs to filter by	false	string []
			hasAgentTags	Include only Threats whose Agent is assigned any tags if True, or none if False	false	boolean
			ids	List of threat IDs	false	string []
			incidentStatuses	Filter threats by a specific incident status	false	string []
			incidentStatusesNin	Exclude threats with specific incident statuses	false	string []

			initiatedBy	Only include threats from specific initiating sources	false	string []
			initiatedByNin	Exclude threats with specific initiating sources	false	string []
			initiatedByUsername__contains	Free-text filter by the username that initiated that threat (supports multiple values)	false	string []
			k8sClusterName__contains	Free-text filter by the endpoint Kubernetes cluster name (supports multiple values)	false	string []
			k8sControllerLabels__contains	Free-text filter by the endpoint Kubernetes controller labels (supports multiple values)	false	string []
			k8sControllerName__contains	Free-text filter by the endpoint Kubernetes controller name (supports multiple values)	false	string []

			k8sNamespaceLabels__contains	Free-text filter by the endpoint Kubernetes namespace labels (supports multiple values)	false	string []
			k8sNamespaceName__contains	Free-text filter by the endpoint Kubernetes namespace name (supports multiple values)	false	string []
			k8sNodeLabels__contains	Free-text filter by the endpoint Kubernetes node labels (supports multiple values)	false	string []
			k8sNodeName__contains	Free-text filter by the endpoint Kubernetes node name (supports multiple values)	false	string []
			k8sPodLabels__contains	Free-text filter by the endpoint Kubernetes pod labels (supports multiple values)	false	string []
			k8sPodName__contains	Free-text filter by the	false	string []

				endpoint Kubernetes pod name (supports multiple values)		
			limit	Limit	false	integer
			mitigatedPreemptively	If the threat was detected pre-execution or post-execution	false	boolean
			mitigationStatuses	Filter threats by a specific status	false	string []
			mitigationStatusesNin	Filter threats not by a specific status	false	string []
			noteExists	The threat contains at least one note	false	boolean
			originatedProcess__contains	Free-text filter by the originated process name of the threat (supports multiple values)	false	string []
			osArchs	Included OS Architectures	false	string []
			osNames		false	string []
			osNamesNin		false	string []
			osTypes	Included OS types	false	string []
			osTypesNin	Excluded OS types	false	string []
			pendingActio	At least one	false	boolean

			ns	action is pending for the Agent for the threat		
			publisherName__contains	Free-text filter by threat's publisher name (supports multiple values)	false	string []
			query	Full text search for fields: threat_details, content_hash, computer_name, file_path, uuid, detection_agent_version, realtime_agent_version, detection_agent_domain, command_line_arguments, initiated_by_username, storyline, originated_process, k8s_cluster_name, k8s_node_name, k8s_node_labels, k8s_namespace_name, k8s_namespace_labels,	false	string

				k8s_controller_name, k8s_controller_labels, k8s_pod_name, k8s_pod_labels, container_name, container_image_name, container_labels, external_ticket_id		
			realtimeAgentVersion__contains	Free-text filter by Agent version at current time (supports multiple values)	false	string []
			rebootRequired	A reboot is required on any endpoint for at least one action on the threat	false	boolean
			resolved	This is used for backward-compatibility with API 2.0.	false	boolean
			siteIds	List of Site IDs to filter by	false	string []
			storyline__contains	Free-text filter by threat storyline (supports multiple values)	false	string []

			storylines	List of Agent context to search for	false	string []
			tenant	Indicates a tenant scope request	false	boolean
			threatDetails__contains	Free-text filter by threat details(supports multiple values)	false	string []
			updatedAt__gt	Updated at greater than.	false	string
			updatedAt__gte	Updated at greater or equal than.	false	string
			updatedAt__lt	Updated at lesser than.	false	string
			updatedAt__lte	Updated at lesser or equal than.	false	string
			uuid__contains	Free-text filter by Agent UUID (supports multiple values)	false	string []

Download from cloud

GET /web/api/v2.1/threats/{threat_id}/download-from-cloud

Download threat file from cloud.

Response Messages

200 - Success

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
data	Response data	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>downloadUrl</td><td>Threat file download URL</td><td>false</td><td>string</td></tr><tr><td>fileName</td><td>Threat file name</td><td>false</td><td>string</td></tr></table>
errors	Errors	false	array

Disconnect Container

POST /web/api/v2.1/threats/actions/container-network-disconnect

Network quarantine a specific container

Response Messages

200 - Disconnect command was created

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
data	Response data	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>success</td><td>Indicates a successful operation</td><td>false</td><td>boolean</td></tr></table>
errors	Errors	false	array

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>containerId</td><td>Container id</td><td>true</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>filter</td><td>Use any of the filtering options to control the list of affected threats. You can use any combination of filters to narrow down the list (For example "apply to only active threats from Linux endpoints"). You can also leave this field empty to apply to all available threats.</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>agentIds</td><td>List of Agent IDs</td><td>false</td><td>string []</td></tr>
<tr><td>agentIsActive</td><td>Include Agents currently connected to the Management Console</td><td>false</td><td>boolean</td></tr>
<tr><td>agentMachineTypes</td><td>Include Agent machine types</td><td>false</td><td>string []</td></tr>
<tr><td>agentMachineTypesNin</td><td>Excluded Agent machine types</td><td>false</td><td>string []</td></tr>
<tr><td>agentTagsData</td><td>Filter threats by assigned tags to the related agent. Given in form of a JSON where each key represents a tag key, and each value represents a list of string values to filter by. To</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
</table>

				filter by unassigned tag values, use __nin suffix in the tag key.		
			agentVersions	Include Agent versions	false	string []
			agentVersionsNin	Excluded Agent versions	false	string []
			analystVerdicts	Filter threats by a specific analyst verdict	false	string []
			analystVerdictsNin	Exclude threats with specific analyst verdicts	false	string []
			awsRole__contains	Free-text filter by aws role(supports multiple values)	false	string []
			awsSecurityGroups__contains	Free-text filter by aws securityGroups(supports multiple values)	false	string []
			awsSubnetIds__contains	Free-text filter by aws subnet ids (supports multiple values)	false	string []
			azureResourceGroup__contains	Free-text filter by azure resource group(supports multiple	false	string []

				values)		
			classifications	List of threat classifications to search	false	string []
			classificationsNin	List of threat classifications not to search	false	string []
			classificationSources	Classification sources list	false	string []
			classificationSourcesNin	Classification sources list to exclude	false	string []
			cloudAccount__contains	Free-text filter by cloud account (supports multiple values)	false	string []
			cloudImage__contains	Free-text filter by cloud image (supports multiple values)	false	string []
			cloudInstanceId__contains	Free-text filter by cloud instance id(supports multiple values)	false	string []
			cloudInstanceSize__contains	Free-text filter by cloud instance size(supports multiple values)	false	string []
			cloudLocation__contains	Free-text filter by cloud location (supports multiple values)	false	string []

			cloudNetwork__contains	Free-text filter by cloud network (supports multiple values)	false	string []
			cloudProvider	Agents from which cloud provider	false	string []
			cloudProviderNin	Exclude Agents from these cloud provider	false	string []
			collectionIds	List of collection IDs to search	false	string []
			commandLineArguments__contains	Free-text filter by threat command line arguments (supports multiple values)	false	string []
			computerName__contains	Free-text filter by computer name (supports multiple values)	false	string []
			confidenceLevels	Filter threats by a specific confidence level	false	string []
			confidenceLevelsNin	Exclude threats with specific confidence level	false	string []
			containerIma	Free-text	false	string []

			geName__contains	filter by the endpoint container image name (supports multiple values)		
			containerLabels__contains	Free-text filter by the endpoint container labels (supports multiple values)	false	string []
			containerName__contains	Free-text filter by the endpoint container name (supports multiple values)	false	string []
			contentHash__contains	Free-text filter by file content hash (supports multiple values)	false	string []
			contentHashes	List of sha1 hashes to search for	false	string []
			countsFor	comma-separated list of fields to be shown	false	string
			createdAt__gt	Created at greater than.	false	string
			createdAt__gte	Created at greater or equal than.	false	string
			createdAt__lt	Created at	false	string

				lesser than.		
			createdAt__lte	Created at lesser or equal than.	false	string
			detectionAgentDomain__contains	Free-text filter by Agent domain at detection time (supports multiple values)	false	string []
			detectionAgentVersion__contains	Free-text filter by Agent version at detection time (supports multiple values)	false	string []
			detectionEngines	Included engines	false	string []
			detectionEnginesNin	Excluded engines	false	string []
			displayName	Display name	false	string
			engines	Included engines	false	string []
			enginesNin	Excluded engines	false	string []
			externalTicketExists	The threat contains ticket number	false	boolean
			externalTicketId__contains	Free-text filter by the threat external ticket ID (supports multiple values)	false	string []

			externalTicketIds	External ticket ID for the threat	false	string []
			failedActions	At least one action failed on the threat	false	boolean
			filePath__contains	Free-text filter by file path (supports multiple values)	false	string []
			gcpServiceAccount__contains	Free-text filter by gcp service account (supports multiple values)	false	string []
			groupIds	List of Group IDs to filter by	false	string []
			hasAgentTags	Include only Threats whose Agent is assigned any tags if True, or none if False	false	boolean
			ids	List of threat IDs	false	string []
			incidentStatuses	Filter threats by a specific incident status	false	string []
			incidentStatusesNin	Exclude threats with specific incident statuses	false	string []
			initiatedBy	Only include threats from	false	string []

				specific initiating sources		
			initiatedByNin	Exclude threats with specific initiating sources	false	string []
			initiatedByUsername__contains	Free-text filter by the username that initiated that threat (supports multiple values)	false	string []
			k8sClusterName__contains	Free-text filter by the endpoint Kubernetes cluster name (supports multiple values)	false	string []
			k8sControllerLabels__contains	Free-text filter by the endpoint Kubernetes controller labels (supports multiple values)	false	string []
			k8sControllerName__contains	Free-text filter by the endpoint Kubernetes controller name (supports multiple values)	false	string []
			k8sNamespace	Free-text	false	string []

			Labels__contains	filter by the endpoint Kubernetes namespace labels (supports multiple values)		
			k8sNamespaceName__contains	Free-text filter by the endpoint Kubernetes namespace name (supports multiple values)	false	string []
			k8sNodeLabels__contains	Free-text filter by the endpoint Kubernetes node labels (supports multiple values)	false	string []
			k8sNodeName__contains	Free-text filter by the endpoint Kubernetes node name (supports multiple values)	false	string []
			k8sPodLabels__contains	Free-text filter by the endpoint Kubernetes pod labels (supports multiple values)	false	string []
			k8sPodName__contains	Free-text filter by the endpoint	false	string []

				Kubernetes pod name (supports multiple values)		
			limit	Limit	false	integer
			mitigatedPreemptively	If the threat was detected pre-execution or post-execution	false	boolean
			mitigationStatuses	Filter threats by a specific status	false	string []
			mitigationStatusesNin	Filter threats not by a specific status	false	string []
			noteExists	The threat contains at least one note	false	boolean
			originatedProcess__contains	Free-text filter by the originated process name of the threat (supports multiple values)	false	string []
			osArchs	Included OS Architectures	false	string []
			osNames		false	string []
			osNamesNin		false	string []
			osTypes	Included OS types	false	string []
			osTypesNin	Excluded OS types	false	string []
			pendingActions	At least one action is	false	boolean

				pending for the Agent for the threat		
			publisherName__contains	Free-text filter by threat's publisher name (supports multiple values)	false	string []
			query	Full text search for fields: threat_details, content_hash, computer_name, file_path, uuid, detection_agent_version, realtime_agent_version, detection_agent_domain, command_line_arguments, initiated_by_username, storyline, originated_process, k8s_cluster_name, k8s_node_name, k8s_node_labels, k8s_namespace_name, k8s_namespace_labels, k8s_controlle	false	string

				r_name, k8s_controller_labels, k8s_pod_name, k8s_pod_labels, container_name, container_image_name, container_labels, external_ticket_id		
			realtimeAgentVersion__contains	Free-text filter by Agent version at current time (supports multiple values)	false	string []
			rebootRequired	A reboot is required on any endpoint for at least one action on the threat	false	boolean
			resolved	This is used for backward-compatibility with API 2.0.	false	boolean
			siteIds	List of Site IDs to filter by	false	string []
			storyline__contains	Free-text filter by threat storyline (supports multiple values)	false	string []

			storylines	List of Agent context to search for	false	string []
			tenant	Indicates a tenant scope request	false	boolean
			threatDetails__contains	Free-text filter by threat details(supports multiple values)	false	string []
			updatedAt__gt	Updated at greater than.	false	string
			updatedAt__gte	Updated at greater or equal than.	false	string
			updatedAt__lt	Updated at lesser than.	false	string
			updatedAt__lte	Updated at lesser or equal than.	false	string
			uuid__contains	Free-text filter by Agent UUID (supports multiple values)	false	string []

Reconnect Container

POST /web/api/v2.1/threats/actions/container-network-connect

Restore network to a container that was disconnected

Response Messages

200 - Reconnect command was created

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
data	Response data	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>success</td><td>Indicates a successful operation</td><td>false</td><td>boolean</td></tr></table>
errors	Errors	false	array

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>containerId</td><td>Container id</td><td>true</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>filter</td><td>Use any of the filtering options to control the list of affected threats. You can use any combination of filters to narrow down the list (For example "apply to only active threats from Linux endpoints"). You can also leave this field empty to apply to all available threats.</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountIds</td><td>List of Account IDs to filter by</td><td>false</td><td>string []</td></tr>
<tr><td>agentIds</td><td>List of Agent IDs</td><td>false</td><td>string []</td></tr>
<tr><td>agentIsActive</td><td>Include Agents currently connected to the Management Console</td><td>false</td><td>boolean</td></tr>
<tr><td>agentMachineTypes</td><td>Include Agent machine types</td><td>false</td><td>string []</td></tr>
<tr><td>agentMachineTypesNin</td><td>Excluded Agent machine types</td><td>false</td><td>string []</td></tr>
<tr><td>agentTagsData</td><td>Filter threats by assigned tags to the related agent. Given in form of a JSON where each key represents a tag key, and each value represents a list of string values to filter by. To</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
</table>

				filter by unassigned tag values, use __nin suffix in the tag key.		
			agentVersions	Include Agent versions	false	string []
			agentVersionsNin	Excluded Agent versions	false	string []
			analystVerdicts	Filter threats by a specific analyst verdict	false	string []
			analystVerdictsNin	Exclude threats with specific analyst verdicts	false	string []
			awsRole__contains	Free-text filter by aws role(supports multiple values)	false	string []
			awsSecurityGroups__contains	Free-text filter by aws securityGroups(supports multiple values)	false	string []
			awsSubnetIds__contains	Free-text filter by aws subnet ids (supports multiple values)	false	string []
			azureResourceGroup__contains	Free-text filter by azure resource group(supports multiple	false	string []

				values)		
			classifications	List of threat classifications to search	false	string []
			classificationsNin	List of threat classifications not to search	false	string []
			classificationSources	Classification sources list	false	string []
			classificationSourcesNin	Classification sources list to exclude	false	string []
			cloudAccount__contains	Free-text filter by cloud account (supports multiple values)	false	string []
			cloudImage__contains	Free-text filter by cloud image (supports multiple values)	false	string []
			cloudInstanceId__contains	Free-text filter by cloud instance id(supports multiple values)	false	string []
			cloudInstanceSize__contains	Free-text filter by cloud instance size(supports multiple values)	false	string []
			cloudLocation__contains	Free-text filter by cloud location (supports multiple values)	false	string []

			cloudNetwork__contains	Free-text filter by cloud network (supports multiple values)	false	string []
			cloudProvider	Agents from which cloud provider	false	string []
			cloudProviderNin	Exclude Agents from these cloud provider	false	string []
			collectionIds	List of collection IDs to search	false	string []
			commandLineArguments__contains	Free-text filter by threat command line arguments (supports multiple values)	false	string []
			computerName__contains	Free-text filter by computer name (supports multiple values)	false	string []
			confidenceLevels	Filter threats by a specific confidence level	false	string []
			confidenceLevelsNin	Exclude threats with specific confidence level	false	string []
			containerIma	Free-text	false	string []

			geName__contains	filter by the endpoint container image name (supports multiple values)		
			containerLabels__contains	Free-text filter by the endpoint container labels (supports multiple values)	false	string []
			containerName__contains	Free-text filter by the endpoint container name (supports multiple values)	false	string []
			contentHash__contains	Free-text filter by file content hash (supports multiple values)	false	string []
			contentHashes	List of sha1 hashes to search for	false	string []
			countsFor	comma-separated list of fields to be shown	false	string
			createdAt__gt	Created at greater than.	false	string
			createdAt__gte	Created at greater or equal than.	false	string
			createdAt__lt	Created at	false	string

				lesser than.		
			createdAt__lte	Created at lesser or equal than.	false	string
			detectionAgentDomain__contains	Free-text filter by Agent domain at detection time (supports multiple values)	false	string []
			detectionAgentVersion__contains	Free-text filter by Agent version at detection time (supports multiple values)	false	string []
			detectionEngines	Included engines	false	string []
			detectionEnginesNin	Excluded engines	false	string []
			displayName	Display name	false	string
			engines	Included engines	false	string []
			enginesNin	Excluded engines	false	string []
			externalTicketExists	The threat contains ticket number	false	boolean
			externalTicketId__contains	Free-text filter by the threat external ticket ID (supports multiple values)	false	string []

			externalTicketIds	External ticket ID for the threat	false	string []
			failedActions	At least one action failed on the threat	false	boolean
			filePath__contains	Free-text filter by file path (supports multiple values)	false	string []
			gcpServiceAccount__contains	Free-text filter by gcp service account (supports multiple values)	false	string []
			groupIds	List of Group IDs to filter by	false	string []
			hasAgentTags	Include only Threats whose Agent is assigned any tags if True, or none if False	false	boolean
			ids	List of threat IDs	false	string []
			incidentStatuses	Filter threats by a specific incident status	false	string []
			incidentStatusesNin	Exclude threats with specific incident statuses	false	string []
			initiatedBy	Only include threats from	false	string []

				specific initiating sources		
			initiatedByNin	Exclude threats with specific initiating sources	false	string []
			initiatedByUsername__contains	Free-text filter by the username that initiated that threat (supports multiple values)	false	string []
			k8sClusterName__contains	Free-text filter by the endpoint Kubernetes cluster name (supports multiple values)	false	string []
			k8sControllerLabels__contains	Free-text filter by the endpoint Kubernetes controller labels (supports multiple values)	false	string []
			k8sControllerName__contains	Free-text filter by the endpoint Kubernetes controller name (supports multiple values)	false	string []
			k8sNamespace	Free-text	false	string []

			Labels__contains	filter by the endpoint Kubernetes namespace labels (supports multiple values)		
			k8sNamespaceName__contains	Free-text filter by the endpoint Kubernetes namespace name (supports multiple values)	false	string []
			k8sNodeLabels__contains	Free-text filter by the endpoint Kubernetes node labels (supports multiple values)	false	string []
			k8sNodeName__contains	Free-text filter by the endpoint Kubernetes node name (supports multiple values)	false	string []
			k8sPodLabels__contains	Free-text filter by the endpoint Kubernetes pod labels (supports multiple values)	false	string []
			k8sPodName__contains	Free-text filter by the endpoint	false	string []

				Kubernetes pod name (supports multiple values)		
			limit	Limit	false	integer
			mitigatedPreemptively	If the threat was detected pre-execution or post-execution	false	boolean
			mitigationStatuses	Filter threats by a specific status	false	string []
			mitigationStatusesNin	Filter threats not by a specific status	false	string []
			noteExists	The threat contains at least one note	false	boolean
			originatedProcess__contains	Free-text filter by the originated process name of the threat (supports multiple values)	false	string []
			osArchs	Included OS Architectures	false	string []
			osNames		false	string []
			osNamesNin		false	string []
			osTypes	Included OS types	false	string []
			osTypesNin	Excluded OS types	false	string []
			pendingActions	At least one action is	false	boolean

				pending for the Agent for the threat		
			publisherName__contains	Free-text filter by threat's publisher name (supports multiple values)	false	string []
			query	Full text search for fields: threat_details, content_hash, computer_name, file_path, uuid, detection_agent_version, realtime_agent_version, detection_agent_domain, command_line_arguments, initiated_by_username, storyline, originated_process, k8s_cluster_name, k8s_node_name, k8s_node_labels, k8s_namespace_name, k8s_namespace_labels, k8s_controlle	false	string

				r_name, k8s_controller_labels, k8s_pod_name, k8s_pod_labels, container_name, container_image_name, container_labels, external_ticket_id		
			realtimeAgentVersion__contains	Free-text filter by Agent version at current time (supports multiple values)	false	string []
			rebootRequired	A reboot is required on any endpoint for at least one action on the threat	false	boolean
			resolved	This is used for backward-compatibility with API 2.0.	false	boolean
			siteIds	List of Site IDs to filter by	false	string []
			storyline__contains	Free-text filter by threat storyline (supports multiple values)	false	string []

			storylines	List of Agent context to search for	false	string []
			tenant	Indicates a tenant scope request	false	boolean
			threatDetails__contains	Free-text filter by threat details(supports multiple values)	false	string []
			updatedAt__gt	Updated at greater than.	false	string
			updatedAt__gte	Updated at greater or equal than.	false	string
			updatedAt__lt	Updated at lesser than.	false	string
			updatedAt__lte	Updated at lesser or equal than.	false	string
			uuid__contains	Free-text filter by Agent UUID (supports multiple values)	false	string []

Get Threat Timeline

GET /web/api/v2.1/threats/{threat_id}/timeline

Get a threat's timeline.

Parameters

accountids	optional	List of Account IDs to filter by. Example: "225494730938493804,225494730938493915".
activitytypes	optional	Return only these activity codes (comma-separated list). Example: "52,53,71,72".
countonly	optional	If true, only total number of items will be returned, without any of the actual objects.
cursor	optional	Cursor position returned by the last request. Use to iterate over more than 1000 items. Example: "YWdlbnRfaWQ6NTgwMjkzODE=".
groupids	optional	List of Group IDs to filter by. Example: "225494730938493804,225494730938493915".
limit	optional	Limit number of returned items (1-1000). Example: "10".
query	optional	Full text search for fields: hash, primary_description, secondary_description
siteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".
skip	optional	Skip first number of items (0-1000). To iterate over more than 1000 items, use "cursor". Example: "150".
skipcount	optional	If true, total number of items will not be calculated, which speeds up execution time.
sortby	optional	The column to sort the results by. Example: "id".
sortorder	optional	Sort direction. Example: "asc".

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>pagination</td><td>Pagination information</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>totalItems</td><td>Total number of items found matching your query</td><td>true</td><td>integer</td></tr>
<tr><td>nextCursor</td><td>Pass this value as "cursor" on your next request, to get the next page of results (Will be "null" when last page reached)</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountId</td><td>Related account (If applicable)</td><td>false</td><td>string</td></tr>
<tr><td>activityType</td><td>Activity type</td><td>false</td><td>integer</td></tr>
<tr><td>agentId</td><td>Related Agent (If applicable)</td><td>false</td><td>string</td></tr>
<tr><td>agentUpdatedVersion</td><td>Agent's new version (If applicable)</td><td>false</td><td>string</td></tr>
<tr><td>createdAt</td><td>Activity creation time (UTC)</td><td>false</td><td>string</td></tr>
<tr><td>data</td><td>Extra activity specific data</td><td>false</td><td>object</td></tr>
</table>
</td></tr>
</table>

			groupId | Related group (If applicable) | false | string hash | Threat file hash (If applicable) | false | string id | Activity ID | false | string osFamily | Agent's OS type (if applicable) | false | enum primaryDescription | Primary description | false | string secondaryDescription | Secondary description | false | string siteId | Related site (If applicable) | false | string threatId | Related threat (If applicable) | false | string updatedAt | Activity last updated time (UTC) | false | string userId | The user who invoked the activity (If applicable) | false | string
errors	Errors	false	array

Export Threat Timeline

GET /web/api/v2.1/export/threats/{threat_id}/timeline

Export a threat's timeline.

Parameters

accountids	optional	List of Account IDs to filter by. Example: "225494730938493804,225494730938493915".
activitytypes	optional	Return only these activity codes (comma-separated list). Example: "52,53,71,72".
groupids	optional	List of Group IDs to filter by. Example: "225494730938493804,225494730938493915".
query	optional	Full text search for fields: hash, primary_description, secondary_description
siteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Export Events

GET /web/api/v2.1/export/threats/{threat_id}/explore/events

Export threat events in CSV or JSON format.

Parameters

format	required	Exported file format. Example: "json".
eventid	optional	Filter by a specific process key and its children

eventsubtypes	optional	Filter events by sub-type. Example: "PROCESSCREATION".
eventtypes	optional	Filter events by type. Example: "events".
processname__like	optional	Filter by process name (substring)

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

---

update_exclusion

Update Exclusions

PUT /web/api/v2.1/unified-exclusions

Change the properties of an Exclusion through the data fields. To get the original data, run "exclusions" with a filter to give the item you want.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

404 - Exclusion not found

Response Schema

Name	Description	Required	Value
data	Response data	false	
errors	Errors	false	array

Body Schema

Name	Description	Required	Value
data	Data	true	
filter	Filter	true	

Name	Description	Required	Value
accountIds	List of Account IDs to filter by	false	string []
groupIds	List of Group IDs to filter by	false	string []
siteIds	List of Site IDs to filter by	false	string []
tenant	Indicates a tenant scope request	false	boolean

Updates

Latest Packages by OS

GET /web/api/v2.1/update/agent/latest-packages

[DEPRECATED] Use "Latest packages" API call instead ("GET /web/api/v2.1/update/agent/packages").

Parameters

accountids	optional	List of Account IDs to filter by. Example: "225494730938493804,225494730938493915".
packagetype	optional	Package type. Example: "Agent".
siteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
osTypes	Os types	true	

Name	Description	Required	Value
linux	Linux	false	

Name	Description	Required	Value
accounts	Accounts where the update package is	false	

Name	D
id	Id
name	Na

										available for download		
									createdAt	Created at	false	string
									fileExtension	File extension	false	enum
									fileName	File name	false	string
									fileSize	File size (bytes)	false	integer
									id	Id	false	string
									link	Link	false	
									majorVersion	Major version	false	string
									minorVersion	Minor version	false	string
									osArch	Package OS architecture (32/64 bit), applicable to Windows packages only	false	enum
									osType	Platform type	false	enum
									packageType	Package type	false	enum
									platformType	Platform type	false	enum
									rangerVersion	Ranger version if applicable	false	string
									scopeLevel	Package scope. If "global", it will be available in all sites. If "site", it will be available only to sites specified in the "siteIds" attribute.	false	enum
									sha1	Package hash	false	string
									sites	Sites where	false	Name | D

										the update package is available for download			id name
									status	Status	false	enum	
									supportedOsVersions	Supported os versions	false	string	
									updatedAt	Updated at	false	string	
									version	Agent version	false	string	
							macos	Macos	false	Name	Description	Required	Value
										accounts	Accounts where the update package is available for download	false	Name id name
										createdAt	Created at	false	string
										fileExtension	File extension	false	enum
										fileName	File name	false	string
										fileSize	File size (bytes)	false	integer
										id	Id	false	string
										link	Link	false	
										majorVersion	Major version	false	string
										minorVersion	Minor version	false	string
										osArch	Package OS architecture (32/64 bit), applicable to Windows packages only	false	enum
										osType	Platform type	false	enum
										packageType	Package type	false	enum
										platformType	Platform type	false	enum

									rangerVersion	Ranger version if applicable	false	string
									scopeLevel	Package scope. If "global", it will be available in all sites. If "site", it will be available only to sites specified in the "siteIds" attribute.	false	enum
									sha1	Package hash	false	string
									sites	Sites where the update package is available for download	false	Name / D id / Id name / Na
									status	Status	false	enum
									supportedOsVersions	Supported os versions	false	string
									updatedAt	Updated at	false	string
									version	Agent version	false	string
							windows	Windows	false	Name / Description / Required / Value		
									accounts	Accounts where the update package is available for download	false	Name / D id / Id name / Na
									createdAt	Created at	false	string
									fileExtension	File extension	false	enum
									fileName	File name	false	string
									fileSize	File size (bytes)	false	integer
									id	Id	false	string

									link	Link	false	
									majorVersion	Major version	false	string
									minorVersion	Minor version	false	string
									osArch	Package OS architecture (32/64 bit), applicable to Windows packages only	false	enum
									osType	Platform type	false	enum
									packageType	Package type	false	enum
									platformType	Platform type	false	enum
									rangerVersion	Ranger version if applicable	false	string
									scopeLevel	Package scope. If "global", it will be available in all sites. If "site", it will be available only to sites specified in the "siteIds" attribute.	false	enum
									sha1	Package hash	false	string
									sites	Sites where the update package is available for download	false	Name / D id / Id name / Na
									status	Status	false	enum
									supportedOsVersions	Supported os versions	false	string
									updatedAt	Updated at	false	string
									version	Agent version	false	string

						windowsLegacy	Windows legacy	false

Name	Description	Required	Value
accounts	Accounts where the update package is available for download	false	<table><tr><th>Name</th><th>De</th></tr><tr><td>id</td><td>Id</td></tr><tr><td>name</td><td>Na</td></tr></table>
createdAt	Created at	false	string
fileExtension	File extension	false	enum
fileName	File name	false	string
fileSize	File size (bytes)	false	integer
id	Id	false	string
link	Link	false	
majorVersion	Major version	false	string
minorVersion	Minor version	false	string
osArch	Package OS architecture (32/64 bit), applicable to Windows packages only	false	enum
osType	Platform type	false	enum
packageType	Package type	false	enum
platformType	Platform type	false	enum
rangerVersion	Ranger version if applicable	false	string
scopeLevel	Package scope. If "global", it will be available in all sites. If "site", it will be available only to sites specified in	false	enum

										the "siteIds" attribute.		
									sha1	Package hash	false	string
									sites	Sites where the update package is available for download	false	Name / id / name
									status	Status	false	enum
									supportedOsVersions	Supported os versions	false	string
									updatedAt	Updated at	false	string
									version	Agent version	false	string
			registrationToken	Registration token	false	string						
errors	Errors	false	array									

Get Latest Packages

GET /web/api/v2.1/update/agent/packages

Get the Agent packages that are uploaded to your Management.
The response shows the data of each package, including the IDs, which you can use in other commands.

Parameters

accountids	optional	List of Account IDs to filter by. Example: "225494730938493804,225494730938493915".
accountname__contains	optional	Free-text filter by account name
countonly	optional	If true, only total number of items will be returned, without any of the actual objects.
cursor	optional	Cursor position returned by the last request. Use to iterate over more than 1000 items. Example: "YWdlbnRfaWQ6NTgwMjkzODE=".
fileextension	optional	File extension. Example: ".msi".
fileextensions	optional	File extension. Example: ".msi".
filename__contains	optional	Free-text filter by file name
filesize__contains	optional	Free-text filter by file size
ids	optional	Package ID list. Example: "225494730938493804,225494730938493915".
limit	optional	Limit number of returned items (1-1000). Example: "10".
majorversions	optional	Package major versions
minorversion	optional	Package minor version
minorversions	optional	Package minor versions
osarches	optional	Package OS architecture (32/64 bit), applicable to Windows packages only. Example: "32 bit".
ostypes	optional	Os type in. Example: "macos".
packagetype	optional	Package type. Example: "Agent".
packagetypes	optional	Package type in. Example: "Agent".
platformtype	optional	Platform type. Example: "macos".

platformtypes	optional	Platform type in. Example: "macos".
query	optional	A free-text search term, will match applicable attributes
rangerversion	optional	Ranger version. Example: "2.5.1.1320".
rangerversion__contains	optional	Free-text filter by ranger version
sha1	optional	Package hash. Example: "2fd4e1c67a2d28fced849ee1bb76e7391b93eb12".
sha1__contains	optional	Free-text filter by SHA1 hash
siteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".
sitename__contains	optional	Free-text filter by site name
skip	optional	Skip first number of items (0-1000). To iterate over more than 1000 items, use "cursor". Example: "150".
skipcount	optional	If true, total number of items will not be calculated, which speeds up execution time.
sortby	optional	The column to sort the results by. Example: "id".
sortorder	optional	Sort direction. Example: "asc".
status	optional	Status in. Example: "ga".
version	optional	Agent version. Example: "2.5.1.1320".
versionstr__contains	optional	Free-text filter by version string

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
pagination	Pagination information	true	

Name	Description	Required	Value
totalItems	Total number	true	integer

				of items found matching your query		
			nextCursor	Pass this value as "cursor" on your next request, to get the next page of results (Will be "null" when last page reached)	false	string
data	Response data	false				

Name	Description	Required	Value
accounts	Accounts where the update package is available for download	false	

Name	Description	Required	Value
id	Id	true	string
name	Name	true	string

Name	Description	Required	Value
createdAt	Created at	false	string
fileExtension	File extension	false	enum
fileName	File name	false	string
fileSize	File size (bytes)	false	integer
id	Id	false	string
link	Link	false	
majorVersion	Major version	false	string
minorVersion	Minor version	false	string
osArch	Package OS architecture (32/64 bit), applicable to Windows packages only	false	enum

<table>
<tr><td></td><td></td><td></td><td>
<table>
<tr><td>osType</td><td>Platform type</td><td>false</td><td>enum</td></tr>
<tr><td>packageType</td><td>Package type</td><td>false</td><td>enum</td></tr>
<tr><td>platformType</td><td>Platform type</td><td>false</td><td>enum</td></tr>
<tr><td>rangerVersion</td><td>Ranger version if applicable</td><td>false</td><td>string</td></tr>
<tr><td>scopeLevel</td><td>Package scope. If "global", it will be available in all sites. If "site", it will be available only to sites specified in the "siteIds" attribute.</td><td>false</td><td>enum</td></tr>
<tr><td>sha1</td><td>Package hash</td><td>false</td><td>string</td></tr>
<tr><td>sites</td><td>Sites where the update package is available for download</td><td>false</td><td>
<table>
<tr><td>Name</td><td>Description</td><td>Required</td><td>Value</td></tr>
<tr><td>id</td><td>Id</td><td>true</td><td>string</td></tr>
<tr><td>name</td><td>Name</td><td>true</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>status</td><td>Status</td><td>false</td><td>enum</td></tr>
<tr><td>supportedOsVersions</td><td>Supported os versions</td><td>false</td><td>string</td></tr>
<tr><td>updatedAt</td><td>Updated at</td><td>false</td><td>string</td></tr>
<tr><td>version</td><td>Agent version</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Delete Packages

DELETE /web/api/v2.1/update/agent/packages

Delete Agent packages from your Management. Use the IDs from Get Latest Packages.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - Insufficient permissions

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>affected</td><td>Number of entities affected by the requested operation</td><td>false</td><td>integer</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

Name	Description	Required	Value
data	Data	true	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>ids</td><td>Package IDs to delete</td><td>false</td><td>string []</td></tr></table>

Update package

PUT /web/api/v2.1/update/agent/packages/{package_id}

Update the metadata for an existing package.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - Insufficient permissions

404 - Package not found

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
status	Status	true	enum
accounts	Accounts where the update package is available for download	false	

Name	Description	Required	Value
id	Id	true	string
name	Name	true	string

Name	Description	Required	Value
createdAt	Created at	false	string
fileExtension	File extension	false	enum
fileName	File name	false	string
fileSize	File size (bytes)	false	integer
id	Id	false	string
link	Link	false	
minorVersion	Minor version	false	string

<table>
<tr><td></td><td></td><td></td><td>
<table>
<tr><td>osArch</td><td>Package OS architecture (32/64 bit), applicable to Windows packages only</td><td>false</td><td>enum</td></tr>
<tr><td>osType</td><td>Platform type</td><td>false</td><td>enum</td></tr>
<tr><td>packageType</td><td>Package type</td><td>false</td><td>enum</td></tr>
<tr><td>platformType</td><td>Platform type</td><td>false</td><td>enum</td></tr>
<tr><td>rangerVersion</td><td>Ranger version if applicable</td><td>false</td><td>string</td></tr>
<tr><td>scopeLevel</td><td>Package scope. If "global", it will be available in all sites. If "site", it will be available only to sites specified in the "siteIds" attribute.</td><td>false</td><td>enum</td></tr>
<tr><td>sha1</td><td>Package hash</td><td>false</td><td>string</td></tr>
<tr><td>sites</td><td>Sites where the update package is available for download</td><td>false</td><td>
<table>
<tr><td>Name</td><td>Description</td><td>Required</td><td>Value</td></tr>
<tr><td>id</td><td>Id</td><td>true</td><td>string</td></tr>
<tr><td>name</td><td>Name</td><td>true</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>supportedOsVersions</td><td>Supported os versions</td><td>false</td><td>string</td></tr>
<tr><td>updatedAt</td><td>Updated at</td><td>false</td><td>string</td></tr>
<tr><td>version</td><td>Agent version</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

Name	Description	Required	Value
data	Data	true	

Name	Description	Required	Value
accountIds	List of accounts to make the package available in. Applicable only if scopeLevel is set to "account".	false	string []
minorVersion	Minor version	false	string
osArch	Package OS architecture (32/64 bit), applicable to Windows packages only	false	enum
rangerVersion	Ranger version if applicable	false	string
scopeLevel	Package scope. If "global", it will be available in all sites. If "site", it will be available only to sites specified in the "siteIds" attribute.	false	enum
siteIds	List of sites to make the package available in. Applicable only if	false	string []

				scopeLevel is set to "site".		
			status	Status	false	enum
			supportedOsVersions	Supported os versions	false	string
			version	Agent version	false	string

Upload Agent Package

POST /web/api/v2.1/upload/agent/software

If you have an On-Prem Management or you are a participant in the Beta program, you can use this command to upload an Agent package to the Management. Then you can deploy the Agent to update endpoints.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
status	Status	true	enum
accounts	Accounts where the update package is available for download	false	

Name	Description	Required	Value
id	Id	true	string
name	Name	true	string

Name	Description	Required	Value
createdAt	Created at	false	string
fileExtension	File extension	false	enum
fileName	File name	false	string
fileSize	File size (bytes)	false	integer
id	Id	false	string
link	Link	false	
minorVersion	Minor version	false	string
osArch	Package OS architecture (32/64 bit),	false	enum

<table>
<tr><td></td><td></td><td></td><td>
<table>
<tr><td></td><td>applicable to Windows packages only</td><td></td><td></td></tr>
<tr><td>osType</td><td>Platform type</td><td>false</td><td>enum</td></tr>
<tr><td>packageType</td><td>Package type</td><td>false</td><td>enum</td></tr>
<tr><td>platformType</td><td>Platform type</td><td>false</td><td>enum</td></tr>
<tr><td>rangerVersion</td><td>Ranger version if applicable</td><td>false</td><td>string</td></tr>
<tr><td>scopeLevel</td><td>Package scope. If "global", it will be available in all sites. If "site", it will be available only to sites specified in the "siteIds" attribute.</td><td>false</td><td>enum</td></tr>
<tr><td>sha1</td><td>Package hash</td><td>false</td><td>string</td></tr>
<tr><td>sites</td><td>Sites where the update package is available for download</td><td>false</td><td>
<table>
<tr><td>Name</td><td>Description</td><td>Required</td><td>Value</td></tr>
<tr><td>id</td><td>Id</td><td>true</td><td>string</td></tr>
<tr><td>name</td><td>Name</td><td>true</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>supportedOsVersions</td><td>Supported os versions</td><td>false</td><td>string</td></tr>
<tr><td>updatedAt</td><td>Updated at</td><td>false</td><td>string</td></tr>
<tr><td>version</td><td>Agent version</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

Name	Description	Required	Value
formData		false	

Name	Description	Required	Value
file	File	true	file
status	Status. Example: "ga".	true	enum
accountIds	List of accounts to make the package available in. Applicable only if scopeLevel is set to "account". Example: "225494730938493804,225494730938493915".	false	string []
minorVersion	Package minor version. Example: "SP1".	false	string
osType	Platform type. Example: "macos".	false	enum
platformType	Platform type. Example: "macos".	false	enum
scopeLevel	Package scope. If "global", it will be available in all sites. Otherwise, it will only be	false	enum

				available to the sites/ accounts specified in"siteIds"/"accountIds" attribute. Example: "site".		
			siteIds	List of sites to make the package available in. Applicable only if scopeLevel is set to "site". Example: "225494730938493804,225494730938493915".	false	string []
			version	Version. Example: "2.5.1.1320".	false	string

Upload System Package

POST /web/api/v2.1/upload/software

If you have an On-Prem Management or otherwise require a manual package upload, use this command to upload an Agent package or a Management package. Then you can deploy the update (see Deploy System Package).

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>success</td><td>Indicates a successful operation</td><td>false</td><td>boolean</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>formData</td><td></td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>file</td><td>File</td><td>true</td><td>file</td></tr>
</table>
</td></tr>
</table>

Deploy System Package

POST /web/api/v2.1/upload/software/deploy

If you have an On-Prem Management or you are a participant in the Beta program, you can upload a Management package and then use this command to deploy the new Management. You must first upload the package (see Upload System Package).

Response Messages

200 - Success

401 - Unauthorized access - please sign in and retry.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td><table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>success</td><td>Indicates a successful operation</td><td>false</td><td>boolean</td></tr></table></td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Download Agent Package

GET /web/api/v2.1/update/agent/download/{package_id}

[DEPRECATED] Download an agent package by package ID.Rate limit: 2 call per minute for each different user token

Response Messages

200 - Success

401 - Unauthorized access - please sign in and retry.

404 - Package not found

Download Package

GET /web/api/v2.1/update/agent/download/{site_id}/{package_id}

Download a package by site_id ("sites") and filename.
Rate limit: 2 call per minute for each user token.
Use this command to manually deploy Agent updates that cannot be deployed with the update-software command (see Agent Actions > Update Software) or through the Console.

Response Messages

200 - Success

401 - Unauthorized access - please sign in and retry.

404 - Package not found or bad site

Users

User by token

GET /web/api/v2.1/user

Get a user by token.

Parameters

accountids	optional	List of Account IDs to filter by. Example: "225494730938493804,225494730938493915".
groupids	optional	List of Group IDs to filter by. Example: "225494730938493804,225494730938493915".
siteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".
tenant	optional	Indicates a tenant scope request

Response Messages

200 - User retrieved correctly.

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
scope	User Scope	true	enum
agreedEula	True if EULA was agreed for user's sites	false	boolean
agreementUrl	Link to EULA agreement if it was not agreed yet	false	string
allowRemoteShell	[DEPRECATED] Unused field. The user's role will determine if	false	boolean

				it is allowed to use remote_shell.		
			apiToken	Api token	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>createdAt</td><td>Created at</td><td>false</td><td>string</td></tr><tr><td>expiresAt</td><td>Expires at</td><td>false</td><td>string</td></tr></table>
			canGenerateApiToken	Can generate api token	false	boolean
			dateJoined	Date joined	false	string
			elevatedSessionDurationMinutes	Defines for how many minutes can the user call protected actions once their session is elevated.	false	integer
			email	Email	false	string
			emailReadOnly	True if email cannot be modified	false	boolean
			emailVerified	True if user verification completed successfully	false	boolean
			firstLogin	First login	false	string
			fullName	Full name	false	string
			fullNameReadOnly	True if full name cannot be modified	false	boolean
			groupsReadOnly	[Deprecated]	false	boolean
			id	Id	false	string
			isExternalLoginUser	Is external login user	false	boolean
			isSystem		false	boolean
			lastLogin	Last login	false	string

			lowestRole	[DEPRECATED] in RBAC there's no 'lowest' role. Returns Admin if user has admin permission on all sites, otherwise a different role.	false	string
			primaryTwoFaMethod	Primary two fa method	false	string
			scopeRoles	Roles of the scope user	false	

Name	Description	Required	Value
accountName	Scope name	true	string
name	Scope name	true	string
id	Scope ID	false	string
roleId	ID of the wanted role	false	string
roleName	[DEPRECATED] Name of the role, will work only for predefined roles	false	string
roles	[DEPRECATED] List containing the desired role name in this scope. Use role_id or role_name instead.	false	string []

siteRoles	[DEPRECATED] Role and site ids for the user. Using scopeRoles is more	false	

Name	Description	Required	Value
id	Site ID	true	string
name	Site name	true	string
roleId	ID of the wanted role	false	string

				consistent.		roleName: [DEPRECATED] Name of the role, will work only for predefined roles; false; string roles: [DEPRECATED] List containing the desired role name in this scope. Use role_id instead.; false; string []
			source	Source	false	string
			tenantRoles	[DEPRECATED] Role ids for the tenant user. Using scopeRoles is more consistent.	false	undefined []
			twoFaConfigured	User 2FA Auth is configured	false	boolean
			twoFaEnabled	Two fa enabled	false	boolean
			twoFaEnabledReadOnly	True if two fa option cannot be modified	false	boolean
			twoFaStatus	State of 2FA setup	false	enum
errors	Errors	false	array			

List users

GET /web/api/v2.1/users

Get a list of users.

Parameters

accountids	optional	List of Account IDs to filter by. Example: "225494730938493804,225494730938493915".
apitokenexpiresat__between	optional	Date range for when the API token expires (format: <from_timestamp>-<to_timestamp>, inclusive). Example: "1514978890136-1514978650130".
apitokenexpiresat__gt	optional	API token expires after this timestamp. Example: "2018-02-27T04:49:26.257525Z".
apitokenexpiresat__gte	optional	API token expires after or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
apitokenexpiresat__lt	optional	API token expires before this timestamp. Example: "2018-02-27T04:49:26.257525Z".
apitokenexpiresat__lte	optional	API token expires before or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
cangenerateapitoken	optional	Can generate api token
countonly	optional	If true, only total number of items will be returned, without any of the actual objects.
createdat__between	optional	Date range for when the user was created (format: <from_timestamp>-<to_timestamp>, inclusive). Example: "1514978890136-1514978650130".
createdat__gt	optional	User was created after this timestamp. Example: "2018-02-27T04:49:26.257525Z".
createdat__gte	optional	User was created after or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
createdat__lt	optional	User was created before this timestamp. Example: "2018-02-27T04:49:26.257525Z".
createdat__lte	optional	User was created before or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
cursor	optional	Cursor position returned by the last request. Use to iterate over

		more than 1000 items. Example: "YWdlbnRfaWQ6NTgwMjkzODE=".
datejoined	optional	Date joined. Example: "2018-02-27T04:49:26.257525Z".
email	optional	Email. Example: "admin@sentinelone.com".
email__contains	optional	Match email partially (substring)
emailreadonly	optional	True if email cannot be changed
emailverified	optional	Return only verified/unverified users
firstlogin	optional	First login. Example: "2018-02-27T04:49:26.257525Z".
fullname	optional	Full name
fullname__contains	optional	Match full name partially (substring)
fullnamereadonly	optional	True if full name cannot be changed
groupsreadonly	optional	[DEPRECATED] True if permissions cannot be changed
hasvalidapitoken	optional	Has valid api token
ids	optional	List of user IDs to filter by. Example: "225494730938493804,225494730938493915".
lastactivation__between	optional	Date range for when the user was last active (format: <from_timestamp>-<to_timestamp>, inclusive). Example: "1514978890136-1514978650130".
lastactivation__gt	optional	User was last active after this timestamp. Example: "2018-02-27T04:49:26.257525Z".
lastactivation__gte	optional	User was last active after or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
lastactivation__lt	optional	User was last active before this timestamp. Example: "2018-02-27T04:49:26.257525Z".
lastactivation__lte	optional	User was last active before or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
lastlogin	optional	Last login. Example: "2018-02-27T04:49:26.257525Z".
limit	optional	Limit number of returned items (1-1000). Example: "10".
primarytwofamethod	optional	Primary two fa method
query	optional	Full text search for fields: full_name, email, description
roleids	optional	List of rbac roles to filter by. Example: "225494730938493804,225494730938493915".

siteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".
skip	optional	Skip first number of items (0-1000). To iterate over more than 1000 items, use "cursor". Example: "150".
skipcount	optional	If true, total number of items will not be calculated, which speeds up execution time.
sortby	optional	The column to sort the results by. Example: "id".
sortorder	optional	Sort direction. Example: "asc".
source	optional	User Source. Example: "mgmt".
sources	optional	Source in. Example: "mgmt".
twofaenabled	optional	Two fa enabled
twofastatus	optional	Two fa status
twofastatuses	optional	Two fa status in

Response Messages

200 - List of users retrieved successfully.

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
pagination	Pagination information	true	

Name	Description	Required	Value
totalItems	Total number of items found matching your query	true	integer
nextCursor	Pass this value as "cursor" on your next request, to get the next	false	string

				page of results (Will be "null" when last page reached)		
data	Response data	false	Name	Description	Required	Value
			scope	User Scope	true	enum
			agreedEula	True if EULA was agreed for user's sites	false	boolean
			agreementUrl	Link to EULA agreement if it was not agreed yet	false	string
			allowRemoteShell	[DEPRECATED] Unused field. The user's role will determine if it is allowed to use remote_shell.	false	boolean
			apiToken	Api token	false	Name / Description / Required / Value createdAt / Created at / false / string expiresAt / Expires at / false / string
			canGenerateApiToken	Can generate api token	false	boolean
			dateJoined	Date joined	false	string
			email	Email	false	string
			emailReadOnly	True if email cannot be modified	false	boolean
			emailVerified	True if user verification completed	false	boolean

				successfully		
			firstLogin	First login	false	string
			fullName	Full name	false	string
			fullNameReadOnly	True if full name cannot be modified	false	boolean
			groupsReadOnly	[Deprecated]	false	boolean
			id	Id	false	string
			isSystem		false	boolean
			lastLogin	Last login	false	string
			lowestRole	[DEPRECATED] in RBAC there's no 'lowest' role. Returns Admin if user has admin permission on all sites, otherwise a different role.	false	string
			primaryTwoFaMethod	Primary two fa method	false	string
			scopeRoles	Roles of the scope user	false	

Name	Description	Required	Value
accountName	Scope name	true	string
name	Scope name	true	string
id	Scope ID	false	string
roleId	ID of the wanted role	false	string
roleName	[DEPRECATED] Name of the role, will work only for predefined roles	false	string
roles	[DEPRECATED] List	false	string []

						containing the desired role name in this scope. Use role_id or role_name instead.
			siteRoles	[DEPRECATED] Role and site ids for the user. Using scopeRoles is more consistent.	false	Name | Description | Required | Value id | Site ID | true | string name | Site name | true | string roleId | ID of the wanted role | false | string roleName | [DEPRECATED] Name of the role, will work only for predefined roles | false | string roles | [DEPRECATED] List containing the desired role name in this scope. Use role_id instead. | false | string []
			source	Source	false	string
			tenantRoles	[DEPRECATED] Role ids for the tenant user. Using scopeRoles is more consistent.	false	undefined []
			twoFaConfigured	User 2FA Auth is configured	false	boolean
			twoFaEnabled	Two fa enabled	false	boolean

			twoFaEnabledReadOnly: True if two fa option cannot be modified; false; boolean twoFaStatus: State of 2FA setup; false; string
errors	Errors	false	array

Create User

POST /web/api/v2.1/users

Create a new user.

Response Messages

200 - User created successfully.

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - Not enough permissions to create user.

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
scope	User Scope	true	enum
agreedEula	True if EULA was agreed for user's sites	false	boolean
agreementUrl	Link to EULA agreement if it was not agreed yet	false	string
allowRemoteShell	[DEPRECATED] Unused field. The user's role will determine if it is allowed to use remote_shell.	false	boolean
apiToken	Api token	false	

						Name / Description / Required / Value createdAt / Created at / false / string expiresAt / Expires at / false / string
			canGenerateApiToken	Can generate api token	false	boolean
			dateJoined	Date joined	false	string
			elevatedSessionDurationMinutes	Defines for how many minutes can the user call protected actions once their session is elevated.	false	integer
			email	Email	false	string
			emailReadOnly	True if email cannot be modified	false	boolean
			emailVerified	True if user verification completed successfully	false	boolean
			firstLogin	First login	false	string
			fullName	Full name	false	string
			fullNameReadOnly	True if full name cannot be modified	false	boolean
			groupsReadOnly	[Deprecated]	false	boolean
			id	Id	false	string
			isExternalLoginUser	Is external login user	false	boolean
			isSystem		false	boolean
			lastLogin	Last login	false	string
			lowestRole	[DEPRECATED] in RBAC there's no	false	string

				'lowest' role. Returns Admin if user has admin permission on all sites, otherwise a different role.		
			primaryTwoFaMethod	Primary two fa method	false	string
			scopeRoles	Roles of the scope user	false	

Name	Description	Required	Value
accountName	Scope name	true	string
name	Scope name	true	string
id	Scope ID	false	string
roleId	ID of the wanted role	false	string
roleName	[DEPRECATED] Name of the role, will work only for predefined roles	false	string
roles	[DEPRECATED] List containing the desired role name in this scope. Use role_id or role_name instead.	false	string []

siteRoles	[DEPRECATED] Role and site ids for the user. Using scopeRoles is more consistent.	false	

Name	Description	Required	Value
id	Site ID	true	string
name	Site name	true	string
roleId	ID of the wanted role	false	string
roleName	[DEPRECATED] Name of the role, will	false	string

						work only for predefined roles
					roles	[DEPRECATED] List containing the desired role name in this scope. Use role_id instead.
			source	Source	false	string
			tenantRoles	[DEPRECATED] Role ids for the tenant user. Using scopeRoles is more consistent.	false	undefined []
			twoFaConfigured	User 2FA Auth is configured	false	boolean
			twoFaEnabled	Two fa enabled	false	boolean
			twoFaEnabledReadOnly	True if two fa option cannot be modified	false	boolean
			twoFaStatus	State of 2FA setup	false	enum
errors	Errors	false	array			

Body Schema

Name	Description	Required	Value
data	Data	true	

Name	Description	Required	Value
email	The email of the user	true	string
fullName	Full name of the user	true	string
scope	User scope	true	enum
allowRemoteShell	[DEPRECATED] Unused field. The user's role will determine if it is allowed to use remote_shell.	false	boolean
password	User password. Not allowed if automatic onboarding feature is enabled.	false	string
scopeRoles	List of id and role id, id is mandatory for user in scope account/site. Role name is deprecated and will work only for predefined roles, please use role id. User in tenant (global) role does not	false	

Name	Description	Required	Value
id	Scope ID	false	string
roleId	ID of the wanted role	false	string
roleName	[DEPRECATED] Name of the role, will work only for predefined roles	false	string
roles	[DEPRECATED] List containing the desired	false	string []

				need to provide an id.		role name in this scope. Use role_id or role_name instead.
			siteRoles	[DEPRECATED] Please use scopeRoles instead.	false	

Name	Description	Required	Value
id	Site ID	true	string
name	[DEPRECATED] Site name	false	string
roleId	ID of the wanted role	false	string
roleName	[DEPRECATED] Name of the role, will work only for predefined roles	false	string
roles	[DEPRECATED] List containing the desired role name in this scope. Use role_id instead.	false	string []

			tenantRoles	[DEPRECATED] Use roles instead. List of tenant roles.	false	string []
			twoFaEnabled	Two fa enabled	false	boolean

Export Users

GET /web/api/v2.1/export/users

Export User data to a CSV, for Users that match the filter.

Parameters

accountids	optional	List of Account IDs to filter by. Example: "225494730938493804,225494730938493915".
apitokenexpiresat__between	optional	Date range for when the API token expires (format: <from_timestamp>-<to_timestamp>, inclusive). Example: "1514978890136-1514978650130".
apitokenexpiresat__gt	optional	API token expires after this timestamp. Example: "2018-02-27T04:49:26.257525Z".
apitokenexpiresat__gte	optional	API token expires after or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
apitokenexpiresat__lt	optional	API token expires before this timestamp. Example: "2018-02-27T04:49:26.257525Z".
apitokenexpiresat__lte	optional	API token expires before or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
cangenerateapitoken	optional	Can generate api token
createdat__between	optional	Date range for when the user was created (format: <from_timestamp>-<to_timestamp>, inclusive). Example: "1514978890136-1514978650130".
createdat__gt	optional	User was created after this timestamp. Example: "2018-02-27T04:49:26.257525Z".
createdat__gte	optional	User was created after or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
createdat__lt	optional	User was created before this timestamp. Example: "2018-02-27T04:49:26.257525Z".
createdat__lte	optional	User was created before or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
datejoined	optional	Date joined. Example: "2018-02-27T04:49:26.257525Z".
email	optional	Email. Example: "admin@sentinelone.com".

email__contains	optional	Match email partially (substring)
emailreadonly	optional	True if email cannot be changed
emailverified	optional	Return only verified/unverified users
firstlogin	optional	First login. Example: "2018-02-27T04:49:26.257525Z".
fullname	optional	Full name
fullname__contains	optional	Match full name partially (substring)
fullnamereadonly	optional	True if full name cannot be changed
groupsreadonly	optional	[DEPRECATED] True if permissions cannot be changed
hasvalidapitoken	optional	Has valid api token
ids	optional	List of user IDs to filter by. Example: "225494730938493804,225494730938493915".
lastactivation__between	optional	Date range for when the user was last active (format: <from_timestamp>-<to_timestamp>, inclusive). Example: "1514978890136-1514978650130".
lastactivation__gt	optional	User was last active after this timestamp. Example: "2018-02-27T04:49:26.257525Z".
lastactivation__gte	optional	User was last active after or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
lastactivation__lt	optional	User was last active before this timestamp. Example: "2018-02-27T04:49:26.257525Z".
lastactivation__lte	optional	User was last active before or at this timestamp. Example: "2018-02-27T04:49:26.257525Z".
lastlogin	optional	Last login. Example: "2018-02-27T04:49:26.257525Z".
primarytwofamethod	optional	Primary two fa method
query	optional	Full text search for fields: full_name, email, description
roleids	optional	List of rbac roles to filter by. Example: "225494730938493804,225494730938493915".
siteids	optional	List of Site IDs to filter by. Example: "225494730938493804,225494730938493915".
source	optional	User Source. Example: "mgmt".
sources	optional	Source in. Example: "mgmt".
twofaenabled	optional	Two fa enabled

twofastatus	optional	Two fa status
twofastatuses	optional	Two fa status in

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Get User

GET /web/api/v2.1/users/{user_id}

Get a user by ID.

Response Messages

200 - User retrieved successfully.

401 - Unauthorized access - please sign in and retry.

403 - Insufficient permissions.

404 - Could not retrieve user.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>scope</td><td>User Scope</td><td>true</td><td>enum</td></tr>
<tr><td>account</td><td>Relevant if the user is a site level user or single account</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>id</td><td>The id of the account</td><td>false</td><td>string</td></tr>
<tr><td>name</td><td>The name of the account</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
</table>
</td></tr>
</table>

			agreedEula	True if EULA was agreed for user's sites	false	boolean
			agreementUrl	Link to EULA agreement if it was not agreed yet	false	string
			allowRemoteShell	[DEPRECATED] Unused field. The user's role will determine if it is allowed to use remote_shell.	false	boolean
			apiToken	Api token	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>createdAt</td><td>Created at</td><td>false</td><td>string</td></tr><tr><td>expiresAt</td><td>Expires at</td><td>false</td><td>string</td></tr></table>
			canGenerateApiToken	Can generate api token	false	boolean
			dateJoined	Date joined	false	string
			elevatedSessionDurationMinutes	Defines for how many minutes can the user call protected actions once their session is elevated.	false	integer
			email	Email	false	string
			emailReadOnly	True if email cannot be modified	false	boolean
			emailVerified	True if user verification completed successfully	false	boolean
			firstLogin	First login	false	string

			fullName	Full name	false	string
			fullNameReadOnly	True if full name cannot be modified	false	boolean
			groupsReadOnly	[Deprecated]	false	boolean
			id	Id	false	string
			isExternalLoginUser	Is external login user	false	boolean
			isSystem		false	boolean
			lastLogin	Last login	false	string
			lowestRole	[DEPRECATED] in RBAC there's no 'lowest' role. Returns Admin if user has admin permission on all sites, otherwise a different role.	false	string
			pages	Pages	false	

Name	Description	Required	Value
identifier	Identifier	false	string
name	Name	false	string
permissions	Permissions	false	

Name	Description	Required	Value
additionalDescription	Additional description	false	string
dependsOn	Depends on	false	string []
description	Description	false	string
disabledReason	Disabled reason	false	string
disabledReasonCode	Disabled reason code	false	string
groupName	Group name	false	string
identifier	Identifier	false	string

										title	Title	false	string
										type	Type	false	string
										value	Value	false	boolean
			primaryTwoFaMethod	Primary two fa method	false	string							
			scopeRoles	Roles of the scope user	false	Name	Description	Required	Value				
						accountName	Scope name	true	string				
						name	Scope name	true	string				
						id	Scope ID	false	string				
						roleId	ID of the wanted role	false	string				
						roleName	[DEPRECATED] Name of the role, will work only for predefined roles	false	string				
						roles	[DEPRECATED] List containing the desired role name in this scope. Use role_id or role_name instead.	false	string []				
			siteRoles	[DEPRECATED] Role and site ids for the user. Using scopeRoles is more consistent.	false	Name	Description	Required	Value				
						id	Site ID	true	string				
						name	Site name	true	string				
						roleId	ID of the wanted role	false	string				
						roleName	[DEPRECATED] Name of the role, will work only for predefined	false	string				

						roles
						roles: [DEPRECATED] List containing the desired role name in this scope. Use role_id instead. — false — string []
			source	Source	false	string
			tenantRoles	[DEPRECATED] Role ids for the tenant user. Using scopeRoles is more consistent.	false	undefined []
			twoFaConfigured	User 2FA Auth is configured	false	boolean
			twoFaEnabled	Two fa enabled	false	boolean
			twoFaEnabledReadOnly	True if two fa option cannot be modified	false	boolean
			twoFaStatus	State of 2FA setup	false	enum
errors	Errors	false	array			

Delete User

DELETE /web/api/v2.1/users/{user_id}

Delete a user by ID.

Response Messages

200 - User deleted successfully.

401 - Unauthorized access - please sign in and retry.

403 - Insufficient permissions.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>success</td><td>Indicates a successful operation</td><td>false</td><td>boolean</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Update User

PUT /web/api/v2.1/users/{user_id}

Change properties of the user of the given ID.

Response Messages

200 - User updated successfully.

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - Forbidden.

404 - User not found.

409 - User or Email already taken.

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
scope	User Scope	true	enum
agreedEula	True if EULA was agreed for user's sites	false	boolean
agreementUrl	Link to EULA agreement if it was not agreed yet	false	string
allowRemoteShell	[DEPRECATED] Unused field. The user's role will determine if	false	boolean

				it is allowed to use remote_shell.		
			apiToken	Api token	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>createdAt</td><td>Created at</td><td>false</td><td>string</td></tr><tr><td>expiresAt</td><td>Expires at</td><td>false</td><td>string</td></tr></table>
			canGenerateApiToken	Can generate api token	false	boolean
			dateJoined	Date joined	false	string
			elevatedSessionDurationMinutes	Defines for how many minutes can the user call protected actions once their session is elevated.	false	integer
			email	Email	false	string
			emailReadOnly	True if email cannot be modified	false	boolean
			emailVerified	True if user verification completed successfully	false	boolean
			firstLogin	First login	false	string
			fullName	Full name	false	string
			fullNameReadOnly	True if full name cannot be modified	false	boolean
			groupsReadOnly	[Deprecated]	false	boolean
			id	Id	false	string
			isExternalLoginUser	Is external login user	false	boolean
			isSystem		false	boolean
			lastLogin	Last login	false	string

			lowestRole	[DEPRECATED] in RBAC there's no 'lowest' role. Returns Admin if user has admin permission on all sites, otherwise a different role.	false	string
			primaryTwoFaMethod	Primary two fa method	false	string
			scopeRoles	Roles of the scope user	false	

Name	Description	Required	Value
accountName	Scope name	true	string
name	Scope name	true	string
id	Scope ID	false	string
roleId	ID of the wanted role	false	string
roleName	[DEPRECATED] Name of the role, will work only for predefined roles	false	string
roles	[DEPRECATED] List containing the desired role name in this scope. Use role_id or role_name instead.	false	string []

			siteRoles	[DEPRECATED] Role and site ids for the user. Using scopeRoles is more	false	

Name	Description	Required	Value
id	Site ID	true	string
name	Site name	true	string
roleId	ID of the wanted role	false	string

				consistent.		roleName: [DEPRECATED] Name of the role, will work only for predefined roles; false; string roles: [DEPRECATED] List containing the desired role name in this scope. Use role_id instead.; false; string []
			source	Source	false	string
			tenantRoles	[DEPRECATED] Role ids for the tenant user. Using scopeRoles is more consistent.	false	undefined []
			twoFaConfigured	User 2FA Auth is configured	false	boolean
			twoFaEnabled	Two fa enabled	false	boolean
			twoFaEnabledReadOnly	True if two fa option cannot be modified	false	boolean
			twoFaStatus	State of 2FA setup	false	enum
errors	Errors	false	array			

Body Schema

Name	Description	Required	Value
data	Data	true	

Name	Description	Required	Value
scope	User scope	true	enum
allowRemoteShell	[DEPRECATED] Unused field. The user's role will determine if it is allowed to use remote_shell.	false	boolean
canGenerateApiToken	Can generate api token	false	boolean
currentPassword	User password, new name for backward compatibility	false	string
email	[DEPRECATED] The email of the user	false	string
fullName	Full name of the user	false	string
id	Id	false	string
password	User password	false	string
scopeRoles	List of id and role id, id is mandatory for user in scope account/site. Role name is deprecated and will work only for predefined roles, please	false	

Name	Description	Required	Value
id	Scope ID	false	string
roleId	ID of the wanted role	false	string
roleName	[DEPRECATED] Name of the role, will work only for predefined roles	false	string

				use role id. User in tenant (global) role does not need to provide an id.		roles: [DEPRECATED] List containing the desired role name in this scope. Use role_id or role_name instead. false string []
			siteRoles	[DEPRECATED] Please use scopeRoles instead.	false	Name: id; Description: Site ID; Required: true; Value: string Name: name; Description: [DEPRECATED] Site name; Required: false; Value: string Name: roleId; Description: ID of the wanted role; Required: false; Value: string Name: roleName; Description: [DEPRECATED] Name of the role, will work only for predefined roles; Required: false; Value: string Name: roles; Description: [DEPRECATED] List containing the desired role name in this scope. Use role_id instead.; Required: false; Value: string []
			tenantRoles	[DEPRECATED] Use roles instead. List of tenant roles.	false	string []
			twoFaCode	Two-Factor Authorization code	false	string
			twoFaEnabled	Two fa enabled	false	boolean

Bulk Delete Users

POST /web/api/v2.1/users/delete-users

Delete all users that match the filter.

Response Messages

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Body Schema

Name	Description	Required	Value
filter	Filter	true	

Name	Description	Required	Value
apiTokenExpiresAt__between	Date range for when the API token expires (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
apiTokenExpiresAt__gt	API token expires after this timestamp	false	string
apiTokenExpiresAt__gte	API token expires after or at this timestamp	false	string
apiTokenExpiresAt__lt	API token expires before this timestamp	false	string
apiTokenExpiresAt__lte	API token expires	false	string

				before or at this timestamp		
			canGenerateApiToken	Can generate api token	false	boolean
			createdAt__between	Date range for when the user was created (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			createdAt__gt	User was created after this timestamp	false	string
			createdAt__gte	User was created after or at this timestamp	false	string
			createdAt__lt	User was created before this timestamp	false	string
			createdAt__lte	User was created before or at this timestamp	false	string
			dateJoined	Date joined	false	string
			email	Email	false	string
			email__contains	Match email partially (substring)	false	string []
			emailReadOnly	True if email cannot be changed	false	boolean
			emailVerified	Return only verified/	false	boolean

				unverified users		
			firstLogin	First login	false	string
			fullName	Full name	false	string
			fullName__contains	Match full name partially (substring)	false	string []
			fullNameReadOnly	True if full name cannot be changed	false	boolean
			groupsReadOnly	[DEPRECATED] True if permissions cannot be changed	false	boolean
			hasValidApiToken	Has valid api token	false	boolean
			ids	List of user IDs to filter by	false	string []
			lastActivation__between	Date range for when the user was last active (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			lastActivation__gt	User was last active after this timestamp	false	string
			lastActivation__gte	User was last active after or at this timestamp	false	string
			lastActivation__lt	User was last active before this	false	string

			timestamp		
			lastActivation__lte	User was last active before or at this timestamp	false	string
			lastLogin	Last login	false	string
			primaryTwoFaMethod	Primary two fa method	false	string
			query	Full text search for fields: full_name, email, description	false	string
			roleIds	List of rbac roles to filter by	false	string []
			source	User Source	false	enum
			sources	Source in	false	string []
			twoFaEnabled	Two fa enabled	false	boolean
			twoFaStatus	Two fa status	false	string
			twoFaStatuses	Two fa status in	false	string []
data	Data	false	

Generate iFrame Token

POST /web/api/v2.1/users/generate-iframe-token

Get a new iFrame token with the provided limitations.

Response Messages

200 - User created successfully.

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - Not enough permissions to create user.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>iframeToken</td><td>User's iframe token</td><td>true</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>accountId</td><td>Account id</td><td>true</td><td>string</td></tr>
<tr><td>agentUuids</td><td>A list of included UUIDs</td><td>false</td><td>string []</td></tr>
<tr><td>role</td><td>[DEPRECATED]Name of the role</td><td>false</td><td>string</td></tr>
<tr><td>roleName</td><td>RBAC role name</td><td>false</td><td>string</td></tr>
<tr><td>userName</td><td>The username that will be displayed</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
</table>

Enable 2FA

POST /web/api/v2.1/users/2fa/enable

Enable two-factor authentication for a given user.

Response Messages

200 - 2FA successfully enabled

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - No permission for the action

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>success</td><td>Indicates a successful operation</td><td>false</td><td>boolean</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

Name	Description	Required	Value
data	Data	true	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>id</td><td>User ID</td><td>true</td><td>string</td></tr><tr><td>currentPassword</td><td>Current password</td><td>false</td><td>string</td></tr><tr><td>twoFaCode</td><td>Two-Factor Authorization code</td><td>false</td><td>string</td></tr></table>

Disable 2FA

POST /web/api/v2.1/users/2fa/disable

Disable Two-Factor Authentication for one user. This requires the ID of the user (run "users").

Response Messages

200 - 2FA successfully disabled

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - No permission for the action

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>success</td><td>Indicates a successful operation</td><td>false</td><td>boolean</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>id</td><td>User ID</td><td>true</td><td>string</td></tr>
<tr><td>currentPassword</td><td>Current password</td><td>false</td><td>string</td></tr>
<tr><td>twoFaCode</td><td>Two-Factor Authorization code</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
</table>

Generate API Token

POST /web/api/v2.1/users/generate-api-token

Get the API token for the authenticated user.

Response Messages

200 - API token delivered to user

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>token</td><td>User's API token</td><td>true</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>forceLegacy</td><td>Temporary attribute for WA: If the flag is set to True the legacy token will be generated even if the auth_tokens global switch is turned on</td><td>false</td><td>boolean</td></tr>
</table>
</td></tr>
</table>

Revoke API Token

POST /web/api/v2.1/users/revoke-api-token

Revoke an API token.

Response Messages

200 - Api token revoked

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - Insufficient permissions

404 - User not found

Response Schema

Name	Description	Required	Value
data	Response data	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>success</td><td>Indicates a successful operation</td><td>false</td><td>boolean</td></tr></table>
errors	Errors	false	array

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>true</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>id</td><td>User ID</td><td>true</td><td>string</td></tr>
<tr><td>currentPassword</td><td>Current password</td><td>false</td><td>string</td></tr>
<tr><td>twoFaCode</td><td>Two-Factor Authorization code</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
</table>

API Token by User ID

GET /web/api/v2.1/users/{user_id}/api-token-details

Get the details of the API token generated for a given user.

Response Messages

200 - Success

401 - Unauthorized access - please sign in and retry.

403 - Insufficient permissions

404 - User not found

Response Schema

Name	Description	Required	Value
data	Response data	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>createdAt</td><td>Created at</td><td>false</td><td>string</td></tr><tr><td>expiresAt</td><td>Expires at</td><td>false</td><td>string</td></tr></table>
errors	Errors	false	array

API Token Details

POST /web/api/v2.1/users/api-token-details

Get details of the API token that matches the filter.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

Response Schema

Name	Description	Required	Value
data	Response data	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>createdAt</td><td>Created at</td><td>false</td><td>string</td></tr><tr><td>expiresAt</td><td>Expires at</td><td>false</td><td>string</td></tr></table>
errors	Errors	false	array

Body Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>apiToken</td><td>Api token</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
</table>

Enable 2FA App

POST /web/api/v2.1/users/enable-app

Enable support for the 2FA app (such as Duo or Google Authenticator) that your Console users will use to log in.

Response Messages

200 - 2FA app enabled

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>success</td><td>Indicates a successful operation</td><td>false</td><td>boolean</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

Name	Description	Required	Value
data	Data	true	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>code</td><td>Code</td><td>false</td><td>string</td></tr><tr><td>id</td><td>Id</td><td>false</td><td>string</td></tr></table>

Request 2FA App

POST /web/api/v2.1/users/request-app

Request 2FA App response.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
data	Response data	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>code</td><td>Code</td><td>false</td><td>string</td></tr><tr><td>qrCode</td><td>Qr code</td><td>false</td><td>string</td></tr></table>
errors	Errors	false	array

Body Schema

Name	Description	Required	Value
currentPassword	User password	false	string

Change Password

POST /web/api/v2.1/users/change-password

Change the user password.

Response Messages

200 - Password changed

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - Insufficient permissions

404 - User not found

Response Schema

Name	Description	Required	Value
data	Response data	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>success</td><td>Indicates a successful operation</td><td>false</td><td>boolean</td></tr></table>
errors	Errors	false	array

Body Schema

Name	Description	Required	Value
data	Data	true	

Name	Description	Required	Value
id	User ID	true	string
confirmNewPassword	Confirm new password	false	string
currentPassword	Current password	false	string
newPassword	New password	false	string
twoFaCode	Two-Factor Authorization code	false	string

Auth App

POST /web/api/v2.1/users/auth/app

Authenticate a user with a third-party app, such as DUO or Google Authenticator, for deployments that require Two Factor Authentication.

Response Messages

200 - Authenticated

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>token</td><td>Generated authentication token</td><td>true</td><td>string</td></tr>
<tr><td>csrf</td><td>Generated csrf token</td><td>false</td><td>string</td></tr>
<tr><td>status</td><td>User verification status</td><td>false</td><td>enum</td></tr>
<tr><td>twoFaMethod</td><td>Two-factor authentication method (if enabled)</td><td>false</td><td>enum</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

Name	Description	Required	Value
data	Data	true	

Name	Description	Required	Value
code	Code	false	string
rememberMe	User should be remembered across sessions	false	boolean

Sign EULA

POST /web/api/v2.1/users/auth/eula

Mark the End User License Agreement (EULA) as signed for user scopes.

Response Messages

200 - Authenticated

401 - Unauthorized access - please sign in and retry.

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>success</td><td>Indicates a successful operation</td><td>false</td><td>boolean</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Check Global User

GET /web/api/v2.1/users/tenant-admin-auth-check

See if logged in user is a user with the Global scope of access.

Response Messages

200 - User is Global.

401 - Unauthorized access - please sign in and retry.

403 - Insufficient permissions

Response Schema

Name	Description	Required	Value
data	Response data	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>success</td><td>Indicates a successful operation</td><td>false</td><td>boolean</td></tr></table>
errors	Errors	false	array

Check Remote Shell Permissions

GET /web/api/v2.1/users/rs-auth-check

See if the logged in user is allowed to use Remote Shell.

Response Messages

200 - User is allowed to use remote shell feature.

401 - Unauthorized access - please sign in and retry.

403 - Insufficient permissions

Response Schema

Name	Description	Required	Value
data	Response data	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>success</td><td>Indicates a successful operation</td><td>false</td><td>boolean</td></tr></table>
errors	Errors	false	array

Check Viewer

GET /web/api/v2.1/users/viewer-auth-check

See if the logged in user has only viewer permissions.

Response Messages

200 - User is a viewer.

401 - Unauthorized access - please sign in and retry.

Response Schema

Name	Description	Required	Value
data	Response data	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>success</td><td>Indicates a successful operation</td><td>false</td><td>boolean</td></tr></table>
errors	Errors	false	array

Email Verification

POST /web/api/v2.1/users/onboarding/verify

When a new user verifies their email, the Management gets a token. Use this command to verify the token and set a new password.

Response Messages

200 - User successfully verified

400 - Invalid user input received. See error details for further information.

401 - Verification failed

404 - A user matching the input verification token wasn't found

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>success</td><td>Indicates a successful operation</td><td>false</td><td>boolean</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

Name	Description	Required	Value
data	Data	true	

Name	Description	Required	Value
password	User selected password	true	string
token	Verification token	true	string
resetPasswordFlow	Reset password flow	false	boolean

Validate Verification Token

GET /web/api/v2.1/users/onboarding/validate-token

When a new user verifies their email, the Management gets a token. Use this command to validate the token.

Parameters

token	required	Verification token
resetpasswordflow	optional	Reset password flow

Response Messages

200 - Token is valid

400 - Invalid user input received. See error details for further information.

401 - Verification failed

404 - A user matching the input verification token wasn't found

Response Schema

Name	Description	Required	Value
data	Response data	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>success</td><td>Indicates a successful operation</td><td>false</td><td>boolean</td></tr></table>
errors	Errors	false	array

Send Verification Email

POST /web/api/v2.1/users/onboarding/send-verification-email

Send verification email to users that match the filter. Warning: Active users will be locked out of the Management Console until they verify (unless set_user_password_methods is on)their email. If your Management Console has Onboarding enabled, when you create a new user, the user gets an email invitation. If the user does not respond in time or loses the email, you can send it again. You can send the email invitation to multiple users. Your SMTP server must be correctly configured in Settings > SMTP for the Global scope. Changing the Global SMTP settings requires an Admin role with Global scope or Support.

Response Messages

200 - Success

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - Insufficient permissions

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>affected</td><td>Number of entities affected by the requested operation</td><td>false</td><td>integer</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

Name	Description	Required	Value
filter	Filter	true	

Name	Description	Required	Value
apiTokenExpiresAt__between	Date range for when the API token expires (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
apiTokenExpiresAt__gt	API token expires after this timestamp	false	string
apiTokenExpiresAt__gte	API token expires after or at this timestamp	false	string
apiTokenExpiresAt__lt	API token expires before this timestamp	false	string
apiTokenExpiresAt__lte	API token expires before or at this timestamp	false	string
canGenerateApiToken	Can generate api token	false	boolean
createdAt__between	Date range for when the user was created (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string

			createdAt__gt	User was created after this timestamp	false	string
			createdAt__gte	User was created after or at this timestamp	false	string
			createdAt__lt	User was created before this timestamp	false	string
			createdAt__lte	User was created before or at this timestamp	false	string
			dateJoined	Date joined	false	string
			email	Email	false	string
			email__contains	Match email partially (substring)	false	string []
			emailReadOnly	True if email cannot be changed	false	boolean
			emailVerified	Return only verified/ unverified users	false	boolean
			firstLogin	First login	false	string
			fullName	Full name	false	string
			fullName__contains	Match full name partially (substring)	false	string []
			fullNameReadOnly	True if full name cannot be changed	false	boolean
			groupsReadOnly	[DEPRECATED] True if	false	boolean

				permissions cannot be changed		
			hasValidApiToken	Has valid api token	false	boolean
			ids	List of user IDs to filter by	false	string []
			lastActivation__between	Date range for when the user was last active (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			lastActivation__gt	User was last active after this timestamp	false	string
			lastActivation__gte	User was last active after or at this timestamp	false	string
			lastActivation__lt	User was last active before this timestamp	false	string
			lastActivation__lte	User was last active before or at this timestamp	false	string
			lastLogin	Last login	false	string
			primaryTwoFaMethod	Primary two fa method	false	string
			query	Full text search for fields: full_name, email,	false	string

			description		
			roleIds	List of rbac roles to filter by	false	string []
			source	User Source	false	enum
			sources	Source in	false	string []
			twoFaEnabled	Two fa enabled	false	boolean
			twoFaStatus	Two fa status	false	string
			twoFaStatuses	Two fa status in	false	string []
data	Data	false	

Reset 2FA

POST /web/api/v2.1/users/reset-2fa

Reset 2FA for users.

Response Messages

200 - 2FA reset completed

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - Insufficient permissions

404 - User not found

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>affected</td><td>Number of entities affected by the requested operation</td><td>false</td><td>integer</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

Name	Description	Required	Value
data	Data	true	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>enroll</td><td>[DEPRECATED] Not used, deprecated</td><td>false</td><td>boolean</td></tr><tr><td>ids</td><td>A list of user ids</td><td>false</td><td>string []</td></tr></table>

Delete 2FA

POST /web/api/v2.1/users/delete-2fa

Delete 2FA for users.

Response Messages

200 - 2FA delete completed

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - Insufficient permissions

404 - User not found

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>affected</td><td>Number of entities affected by the requested operation</td><td>false</td><td>integer</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

Name	Description	Required	Value
data	Data	true	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>ids</td><td>A list of user ids</td><td>false</td><td>string []</td></tr></table>

Enroll 2FA

POST /web/api/v2.1/users/enroll-2fa

Enroll users for 2FA setup.

Response Messages

200 - 2FA enrollment completed

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - Insufficient permissions

404 - User not found

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>affected</td><td>Number of entities affected by the requested operation</td><td>false</td><td>integer</td></tr>
<tr><td>expiration</td><td>The number of hours until 2FA enrollment expires</td><td>false</td><td></td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

Name	Description	Required	Value
data	Data	true	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>ids</td><td>A list of user ids</td><td>false</td><td>string []</td></tr></table>

Redirect to SSO

GET /web/api/v2.1/users/login/sso-saml2

If SSO is enabled for a deployment or scope, and a user attempts to log in with name and password, this command redirects the login to SSO.

Parameters

email	optional	Email address of the user trying to log in. Example: "me@sentinelone.com".
scopeid	optional	The scope the desired SSO IdP is configured on. email is irrelevant when using scope_id. If both are provided, email is ignored. Example: "225494730938493804".

Response Messages

302 - Login redirected.

400 - Invalid user input received. See error details for further information.

401 - Not authenticated user.

Redirect to SSO for re-authentication

GET /web/api/v2.1/users/sso-saml2/re-auth

Initiates re-authentication with user's identity provider.

Response Messages

302 - Redirect user to their IDP for re-authentication.

401 - Unauthorized access - please sign in and retry.

403 - User is not allowed to re-authenticate with their IDP

500 - Error in SAML handler initialization.

Auth by SSO

POST /web/api/v2.1/users/login/sso-saml2/{scope_id}

Authenticate a Single Sign-On response over SAML v2 protocol.

Response Messages

302 - SSO authenticated.

401 - Not authenticated user.

404 - Site not found.

Login

POST /web/api/v2.1/users/login

Authenticate a user by username and password and return an authentication token. Rate limit: 1 call per second for each different IP address that communicates with the Console.

Response Messages

200 - User authenticated successfully.

400 - Invalid user input received. See error details for further information.

401 - Login failed. May be the result of bad credentials, or a wrong authentication method if SSO or 2FA is required. A temporary token might be provided to do the required next step. The error code defines the cause and the next step.
Basic error codes:<ul><li>4010010 - authentication failed,</li><li>4010020 - SSO login required - /users/login/sso-saml2,</li><li>4010040 - generic login error,</li><li>4010080 - user is locked,</li></ul>Error codes related to password changes and expiration:<ul><li>4010091 - user must change password - /users/login/set-password,</li><li>4010092 - password expired - /users/login/set-password,</li><li>4010093 - password expires soon - /users/login-continue.</li></ul>Error codes related to LDAP (Active Directory):<ul><li>4010050 - generic LDAP error,</li><li>4010060 - user has no email,</li><li>4010070 - user is disabled.</li></ul>Error codes related to 2FA:<ul><li>4010035 - 2FA configuration - /users/request-app,</li><li>4010030 - 2FA required - /users/auth/app,</li><li>4010031 - 2FA not enrolled,</li><li>4010032 - 2FA enrollment expired.</li></ul>

Response Schema

Name	Description	Required	Value
data	Response	false	

	data		<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>token</td><td>Generated authentication token</td><td>true</td><td>string</td></tr><tr><td>csrf</td><td>Generated csrf token</td><td>false</td><td>string</td></tr><tr><td>status</td><td>User verification status</td><td>false</td><td>enum</td></tr><tr><td>twoFaMethod</td><td>Two-factor authentication method (if enabled)</td><td>false</td><td>enum</td></tr></table>
errors	Errors	false	array

Body Schema

Name	Description	Required	Value
password	Your password	true	string
username	The user email	true	string
rememberMe	User should be remembered across sessions	false	boolean

Logout

POST /web/api/v2.1/users/logout

Log out the authenticated user.

Response Messages

200 - User logged out successfully.

401 - Unauthorized access - please sign in and retry.

Login by API Token

POST /web/api/v2.1/users/login/by-api-token

Log in to the API with a token. To learn more about temporary and 6-month tokens and how to generate them, see https://support.sentinelone.com/hc/en-us/articles/360004195934.

Response Messages

200 - user logged in

400 - Invalid user input received. See error details for further information.

401 - User authentication failed

Response Schema

Name	Description	Required	Value
data	Response data	false	

Name	Description	Required	Value
token	User token	true	string
realUser	When logging in from Atlas, specifies the actual user who logged	false	string

			<table><tr><td></td><td>in</td><td></td><td></td></tr><tr><td>redirectTo</td><td>Relative url to redirect to</td><td>false</td><td>string</td></tr><tr><td>redirectToParams</td><td>Query params for the redirect to, without '?' prefix</td><td>false</td><td>string</td></tr><tr><td>removedSavedScope</td><td>Removed saved scope</td><td>false</td><td>string</td></tr></table>
errors	Errors	false	array

Body Schema

Name	Description	Required	Value
data	Data	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>apiToken</td><td>Api token</td><td>false</td><td>string</td></tr><tr><td>reason</td><td>When logging in from Atlas, specifies the login reason</td><td>false</td><td>string</td></tr></table>

Login by Token

GET /web/api/v2.1/users/login/by-token

Log in with user token.

Parameters

token	required	User token. Example: "bfd9070c1afa88516d3cdfd722e62fe433e42bad6bb14da27088140ad785585f8582adaccd56fb69".
redirectto	optional	Relative url to redirect to
redirecttoparams	optional	Query params for the redirect to, without '?' prefix
removedsavedscope	optional	Removed saved scope

Response Messages

200 - user logged in

400 - Invalid user input received. See error details for further information.

401 - User authentication failed

Continue with login due to upcoming password expiration or SSO 2FA setup

POST /web/api/v2.1/users/login-continue

For SSO 2FA setup tokens, allows users to skip setting up the 2FA and proceed with their login.
Accepts a temporary token from SSO login flow with error code 4010035.

For password expiration tokens, allows users to decide if they want to change their soon to expire password now or later.
Users can also choose not to receive the notification again for this password cycle.
Accepts a temporary token from /users/login with error code 4010093.

Response Messages

200 - Login can continue

400 - Invalid user input received. See error details for further information.

401 - Unauthorized.
In password expiration flow, a temporary token might be provided to do the required next step. The error code defines the cause and the next step.
Error codes:<ul><li>4010010 - invalid token,</li><li>4010094 - change password with /users/login/set-password</li></ul>

Response Schema

Name	Description	Required	Value
data	Response data	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>token</td><td>Generated authentication token</td><td>true</td><td>string</td></tr><tr><td>csrf</td><td>Generated csrf token</td><td>false</td><td>string</td></tr></table>
errors	Errors	false	array

Body Schema

Name	Description	Required	Value
data	Data	true	

Name	Description	Required	Value
token	Temporary JWT	true	string
dontShowAgain	Indicates if the user wants to skip the continue next time	false	boolean
resetPassword	Indicates if the user wants to change the password	false	boolean

Set a New Password

POST /web/api/v2.1/users/login/set-password

Sets a new password for the user.
Used by forced password reset and password expiration flows.
Accepts temporary tokens from /users/login with error codes 4010091 and 4010092.

Response Messages

200 - Password was set

400 - Invalid user input received. See error details for further information.

401 - Unauthorized

Response Schema

<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>data</td><td>Response data</td><td>false</td><td>
<table>
<tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr>
<tr><td>token</td><td>Generated authentication token</td><td>true</td><td>string</td></tr>
<tr><td>csrf</td><td>Generated csrf token</td><td>false</td><td>string</td></tr>
</table>
</td></tr>
<tr><td>errors</td><td>Errors</td><td>false</td><td>array</td></tr>
</table>

Body Schema

Name	Description	Required	Value
data	Data	true	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>password</td><td>The new password</td><td>true</td><td>string</td></tr><tr><td>token</td><td>Verification token</td><td>true</td><td>string</td></tr></table>

Prompt reset password

POST /web/api/v2.1/users/login/send-reset-password-email

Prompt reset password for users.

Response Messages

200 - Prompt reset password completed

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - Insufficient permissions

Response Schema

Name	Description	Required	Value
data	Response data	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>affected</td><td>Number of entities affected by the requested operation</td><td>false</td><td>integer</td></tr></table>
errors	Errors	false	array

Body Schema

Name	Description	Required	Value
filter	Filter	true	

Name	Description	Required	Value
apiTokenExpiresAt__between	Date range for when the API token expires (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
apiTokenExpiresAt__gt	API token expires after this timestamp	false	string
apiTokenExpiresAt__gte	API token expires after or at this timestamp	false	string
apiTokenExpiresAt__lt	API token expires before this timestamp	false	string
apiTokenExpiresAt__lte	API token expires before or at this timestamp	false	string
canGenerateApiToken	Can generate api token	false	boolean
createdAt__between	Date range for when the user was created (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string

			createdAt__gt	User was created after this timestamp	false	string
			createdAt__gte	User was created after or at this timestamp	false	string
			createdAt__lt	User was created before this timestamp	false	string
			createdAt__lte	User was created before or at this timestamp	false	string
			dateJoined	Date joined	false	string
			email	Email	false	string
			email__contains	Match email partially (substring)	false	string []
			emailReadOnly	True if email cannot be changed	false	boolean
			emailVerified	Return only verified/ unverified users	false	boolean
			firstLogin	First login	false	string
			fullName	Full name	false	string
			fullName__contains	Match full name partially (substring)	false	string []
			fullNameReadOnly	True if full name cannot be changed	false	boolean
			groupsReadOnly	[DEPRECATED] True if	false	boolean

				permissions cannot be changed		
			hasValidApiToken	Has valid api token	false	boolean
			ids	List of user IDs to filter by	false	string []
			lastActivation__between	Date range for when the user was last active (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			lastActivation__gt	User was last active after this timestamp	false	string
			lastActivation__gte	User was last active after or at this timestamp	false	string
			lastActivation__lt	User was last active before this timestamp	false	string
			lastActivation__lte	User was last active before or at this timestamp	false	string
			lastLogin	Last login	false	string
			primaryTwoFaMethod	Primary two fa method	false	string
			query	Full text search for fields: full_name, email,	false	string

			description		
			roleIds	List of rbac roles to filter by	false	string []
			source	User Source	false	enum
			sources	Source in	false	string []
			twoFaEnabled	Two fa enabled	false	boolean
			twoFaStatus	Two fa status	false	string
			twoFaStatuses	Two fa status in	false	string []
data	Data	false	

Reset password on next login

POST /web/api/v2.1/users/login/force-reset-password-on-login

Force users to reset their password on next login.

Response Messages

200 - Users marked to reset password on next login successfully

400 - Invalid user input received. See error details for further information.

401 - Unauthorized access - please sign in and retry.

403 - Insufficient permissions

Response Schema

Name	Description	Required	Value
data	Response data	false	<table><tr><th>Name</th><th>Description</th><th>Required</th><th>Value</th></tr><tr><td>affected</td><td>Number of entities affected by the requested operation</td><td>false</td><td>integer</td></tr></table>
errors	Errors	false	array

Body Schema

Name	Description	Required	Value
filter	Filter	true	

Name	Description	Required	Value
apiTokenExpiresAt__between	Date range for when the API token expires (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
apiTokenExpiresAt__gt	API token expires after this timestamp	false	string
apiTokenExpiresAt__gte	API token expires after or at this timestamp	false	string
apiTokenExpiresAt__lt	API token expires before this timestamp	false	string
apiTokenExpiresAt__lte	API token expires before or at this timestamp	false	string
canGenerateApiToken	Can generate api token	false	boolean
createdAt__between	Date range for when the user was created (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string

			createdAt__gt	User was created after this timestamp	false	string
			createdAt__gte	User was created after or at this timestamp	false	string
			createdAt__lt	User was created before this timestamp	false	string
			createdAt__lte	User was created before or at this timestamp	false	string
			dateJoined	Date joined	false	string
			email	Email	false	string
			email__contains	Match email partially (substring)	false	string []
			emailReadOnly	True if email cannot be changed	false	boolean
			emailVerified	Return only verified/ unverified users	false	boolean
			firstLogin	First login	false	string
			fullName	Full name	false	string
			fullName__contains	Match full name partially (substring)	false	string []
			fullNameReadOnly	True if full name cannot be changed	false	boolean
			groupsReadOnly	[DEPRECATED] True if	false	boolean

				permissions cannot be changed		
			hasValidApiToken	Has valid api token	false	boolean
			ids	List of user IDs to filter by	false	string []
			lastActivation__between	Date range for when the user was last active (format: <from_timestamp>-<to_timestamp>, inclusive)	false	string
			lastActivation__gt	User was last active after this timestamp	false	string
			lastActivation__gte	User was last active after or at this timestamp	false	string
			lastActivation__lt	User was last active before this timestamp	false	string
			lastActivation__lte	User was last active before or at this timestamp	false	string
			lastLogin	Last login	false	string
			primaryTwoFaMethod	Primary two fa method	false	string
			query	Full text search for fields: full_name, email,	false	string

			description		
			roleIds	List of rbac roles to filter by	false	string []
			source	User Source	false	enum
			sources	Source in	false	string []
			twoFaEnabled	Two fa enabled	false	boolean
			twoFaStatus	Two fa status	false	string
			twoFaStatuses	Two fa status in	false	string []
data	Data	false	