



# Version Houston

---

User Guide for Management Console

16 October 2019

Copyright © 2019 SentinelOne

This document contains SentinelOne proprietary information owned by Sentinel Labs, Inc. ("SentinelOne"), and is provided for use only in connection with SentinelOne's Endpoint Protection Platform. This document may also contain confidential information, and may not be reproduced or otherwise used without the express permission of SentinelOne. SentinelOne reserves the right to amend this document in its sole discretion. SentinelOne® and the SentinelOne logos are the registered and unregistered trademarks of Sentinel Labs, Inc. Please contact SentinelOne with any questions.

# Table of Contents

1. FAQ [Multi-Site] .....	1
1.1. Architecture [Multi-Site] .....	1
2. Using the Management Console [Multi-Site] .....	5
2.1. Admin Scope [Multi-Site] .....	6
2.2. Logging in for the First Time [Multi-Site] .....	9
2.3. Logging in with SSO [Multi-Site] .....	10
2.4. Logging in with Two-Factor Authentication [Multi-Site] .....	11
2.5. Using the Dashboard [Multi-Site] .....	12
2.6. Filtering Activities [Multi-Site] .....	13
2.7. Using the Search Function [Multi-Site] .....	15
3. Installing Agents - Overview and Prerequisites [Multi-Site] .....	17
3.1. Uploading a Package for Agent Installation or Upgrade [Multi-Site] .....	18
3.2. Getting a Site or Group Token .....	20
3.3. Installing Multiple Agents [Multi-Site] .....	22
3.4. Installing on Windows Endpoints [Multi-Site] .....	23
3.4.1. Agent Installer Command Line Options [Multi-Site] .....	25
3.4.2. Windows Agent Installation Logs .....	28
3.4.3. Installing Windows Agents on VM or VDI .....	29
3.5. Installing on macOS Endpoints [Multi-Site] .....	30
3.5.1. Installing and Upgrading macOS Agent with Jamf .....	32
3.6. Linux Agent 3.x Installation .....	34
3.6.1. Agent Association .....	35
3.6.2. Agent Installation and Activation on Master Images .....	36
3.6.3. Agent Activation .....	36
3.7. Installing on Linux Endpoints [Multi-Site] .....	36
3.8. Pending Action [Multi-Site] .....	38
3.9. Understanding Agent UUID .....	40
3.10. Upgrading a Selected List of Agents [Multi-Site] .....	41
3.11. Upgrading Agents From a Customized Location .....	43
3.12. Upgrading the Windows Agent from an Image .....	44
3.13. Updating Agents with SCCM .....	46
3.14. Upgrading Agents - Troubleshooting .....	47
4. Managing Sites and Licenses [Multi-Site] .....	49
4.1. Creating a New Site [Multi-Site] .....	51
4.2. Moving an Agent to a Different Site [Multi-Site] .....	53
4.3. Deleting a Site [Multi-Site] .....	54
4.4. Managing Accounts [Multi-Site] .....	55
5. Managing Agents [Multi-Site] .....	57
5.1. Windows Agent Event Logs .....	58
5.1.1. Using the Windows Event Viewer Logs .....	60
5.2. Uninstalling Agents from the Management Console [Multi-Site] .....	65
5.3. Uninstalling Agents from the CLI .....	66
5.4. Getting a Passphrase .....	68
5.5. Uninstall Requests [Multi-Site] .....	69
5.6. Rebooting an Endpoint from the Console [Multi-Site] .....	71
5.7. Shutting Down an Endpoint from the Console [Multi-Site] .....	73
5.8. Removing an Agent from the Console - Decommission [Multi-Site] .....	74
6. Analyzing, Mitigating, and Resolving Threats [Multi-Site] .....	77
6.1. Prioritizing Threats .....	78
6.2. Disconnecting Endpoints from the Network .....	79
6.3. Analyzing Threats [Multi-Site] .....	80

6.4. Mitigation Options .....	84
6.5. Resolve Options .....	85
6.6. Changing Mitigation - Unquarantine [Multi-Site] .....	86
6.7. On-Demand File Fetch [Multi-Site] .....	87
7. Running Full Disk Scan [Multi-Site] .....	94
7.1. Running Full Disk Scan on Installation [Multi-Site] .....	95
7.2. Full Disk Scan from CLI [Multi-Site] .....	96
7.3. Seeing Full Disk Scan Status and Results [Multi-Site] .....	97
8. Managing Policies [Multi-Site] .....	99
8.1. Changing a Policy [Multi-Site] .....	99
8.2. Policy Settings [Multi-Site] .....	101
8.3. Policy Engines [Multi-Site] .....	103
8.4. Agent Configuration Settings [Multi-Site] .....	106
8.5. Controlling On Write or On Execute [Multi-Site] .....	106
8.6. Policy Mode Best Practices .....	109
9. Managing Endpoint Filters and Groups [Multi-Site] .....	112
9.1. Creating Filters in Network [Multi-Site] .....	114
9.2. Creating Groups [Multi-Site] .....	118
9.3. Editing a Group [Multi-Site] .....	120
9.4. Ranking Dynamic Groups [Multi-Site] .....	122
9.5. Moving Agents between Static Groups [Multi-Site] .....	122
9.6. Deleting a Group [Multi-Site] .....	123
9.7. Exporting Endpoint Data .....	124
10. Managing the Blacklist [Multi-Site] .....	125
10.1. Adding a Hash to the Blacklist [Multi-Site] .....	126
11. Managing Exclusions [Multi-Site] .....	129
11.1. Creating Exclusions [Multi-Site] .....	130
11.2. Creating a Hash Exclusion [Multi-Site] .....	132
11.3. Creating a Path Exclusion [Multi-Site] .....	134
11.4. Best Practices for Exclusions .....	143
11.5. Excluding a File Type [Multi-Site] .....	145
11.6. Excluding a Signer Identity (Certificate) [Multi-Site] .....	146
11.7. Excluding a Browser [Multi-Site] .....	148
12. Managing Management Console Users [Multi-Site] .....	150
12.1. Creating New Management Console Users [Multi-Site] .....	150
12.2. Resending Verification Email [Multi-Site] .....	152
12.3. Changing a User's Password [Multi-Site] .....	153
12.4. Editing Management Console User Details [Multi-Site] .....	155
12.5. Generating API Tokens [Multi-Site] .....	157
12.6. Enabling Two-Factor Authentication [Multi-Site] .....	160
12.7. Configuring Session Timeout [Multi-Site] .....	164
12.8. Deleting a Console User [Multi-Site] .....	165
13. Deep Visibility .....	167
13.1. How to Use Deep Visibility [Multi-Site] .....	168
13.1.1. Running a Deep Visibility Query .....	171
13.1.2. View Query Results in a Table or Tree .....	173
13.2. Deep Visibility Query Syntax .....	179
13.3. Threat Hunting Use Cases .....	185
13.3.1. Hunting for Abnormal Scheduled Task Creation .....	185
13.3.2. Hunting for Living Off the Land Attacks .....	186
13.3.3. Responding to Incidents with Deep Visibility .....	188
13.4. Configuring Deep Visibility Data Collection [Multi-Site] .....	190
13.5. Searching for Behavioral Indicators .....	191
13.5.1. List of Indicator Names and Categories .....	193

13.6. List of Indicator Names and Categories .....	209
13.7. Saving Threat Hunting Queries and Watchlists [Multi-Site] .....	225
13.8. Working with Saved Deep Visibility Queries [Multi-Site] .....	227
13.9. Query with Custom Time Range [Multi-Site] .....	228
13.10. Managing the Browser Extension .....	230
13.11. Supported File Types for Deep Visibility .....	231
13.12. Hunter Chrome Extension for Deep Visibility .....	231
14. Creating Insight Reports [Multi-Site] .....	235
14.1. Editing and Deleting Reports [Multi-Site] .....	237
14.2. Downloading a Report [Multi-Site] .....	239
14.3. Raw Data Report .....	239
15. Management Console Integrations [Multi-Site] .....	241
15.1. Configuring Okta SSO [Multi-Site] .....	241
15.1.1. Using SSO Login Exclusively .....	242
15.2. Integrating SMTP Servers [Multi-Site] .....	251
15.2.1. Configuring Email Notifications [Multi-Site] .....	253
15.2.2. Clearing the SMTP Message Queue [Multi-Site] .....	254
15.3. Integrating Syslog Servers [Multi-Site] .....	255
15.3.1. Configuring Syslog Notifications [Multi-Site] .....	257
15.3.2. SentinelOne Syslog CEF2 Message Attributes [Multi-Site] .....	258
15.3.3. SentinelOne Syslog Events .....	287
15.3.4. Syslog Integration with Sumo Logic .....	293
16. Configuring Proxy Settings for Agents .....	295
16.1. Configuring a Proxy Server for Windows Agents .....	295
16.2. Windows Agent Proxy Modes .....	298
16.3. Configuring a Proxy for macOS Agents .....	302
16.4. Configuring a Proxy Server for Linux Agents .....	303
17. Advanced Mode [Multi-Site] .....	305
17.1. Advanced Mode Network Options .....	307
17.2. Agent Configuration Hierarchy [Multi-Site] .....	308
17.3. Advanced: Changing Agent Configuration Manually [Multi-Site] .....	308
17.4. Advanced: Changing Agent Configuration with Policy Override [Multi-Site] .....	311
17.5. Advanced: Enabling SHA 256 Hash Information for Threats [Multi-Site] .....	314
17.6. Advanced: Agent Migration between Management Consoles .....	316
18. Device Control .....	320
18.1. Device Control Settings .....	321
18.2. Device Control Rules and Rule Order .....	323
18.3. Creating and Editing Device Control Rules .....	325
18.4. Moving and Copying Device Control Rules .....	333
18.5. Seeing Device Control Activity Logs .....	336
18.6. Creating Device Control Rules from Events .....	339
18.7. End-User Interaction with Device Control .....	342
18.8. How to Find Device Identifier Information .....	342
19. SentinelOne Firewall Control .....	349
19.1. Firewall Control Settings .....	349
19.2. Firewall Control Rules and Rule Order .....	351
19.3. Creating and Editing Firewall Rules .....	352
19.4. Moving and Copying Firewall Rules .....	360
19.5. Importing and Exporting Firewall Rules .....	363
19.6. Using FQDN in Firewall Rules .....	365
19.7. Firewall Control and OS Security .....	367
19.8. Firewall Control - Event Logging .....	368
20. SentinelOne Remote Shell .....	372
20.1. Starting a Remote Shell Session .....	375

20.2. Remote Shell in the Activity Log .....	379
21. SentinelOne Application Risk Management .....	381
21.1. Managing All Risky Applications .....	381
21.2. Managing Risky Applications Installed On One Endpoint .....	385
21.3. Exporting Application Data .....	388
22. Location Aware Firewall .....	389
22.1. Configuring Locations .....	389
22.2. Defining Specific Location Parameters .....	392
22.3. Using Locations in Firewall Rules .....	397
22.4. Seeing an Endpoint's Location .....	401
22.5. Agent Calculation of its Location .....	402
22.6. Sentinelctl commands for Locations .....	403
22.6.1. get_current_location .....	403
22.6.2. locations current list .....	403
22.6.3. locations rules dump .....	404
23. Getting Logs for Support [Multi-Site] .....	405

# 1. FAQ [Multi-Site]

Console versions Central Park and later support multi-site architecture.

- What are the system requirements?

## [System Requirements](#)

- Where can I see the build numbers of the latest Agent releases?

You can see the latest releases, their build numbers, release dates, and links to release notes, in [Latest Information](#). We recommend that you **Follow** this page.

- What is Multi-Site?

## [Introduction to SentinelOne Multi-Site Management](#)

- The WebUI has search functions in different places. What can I search for?

## [Using the Search Function](#)

## 1.1. Architecture [Multi-Site]

**Management:** Central Park, Denali, Eiffel, Fuji, Grand Canyon, Houston

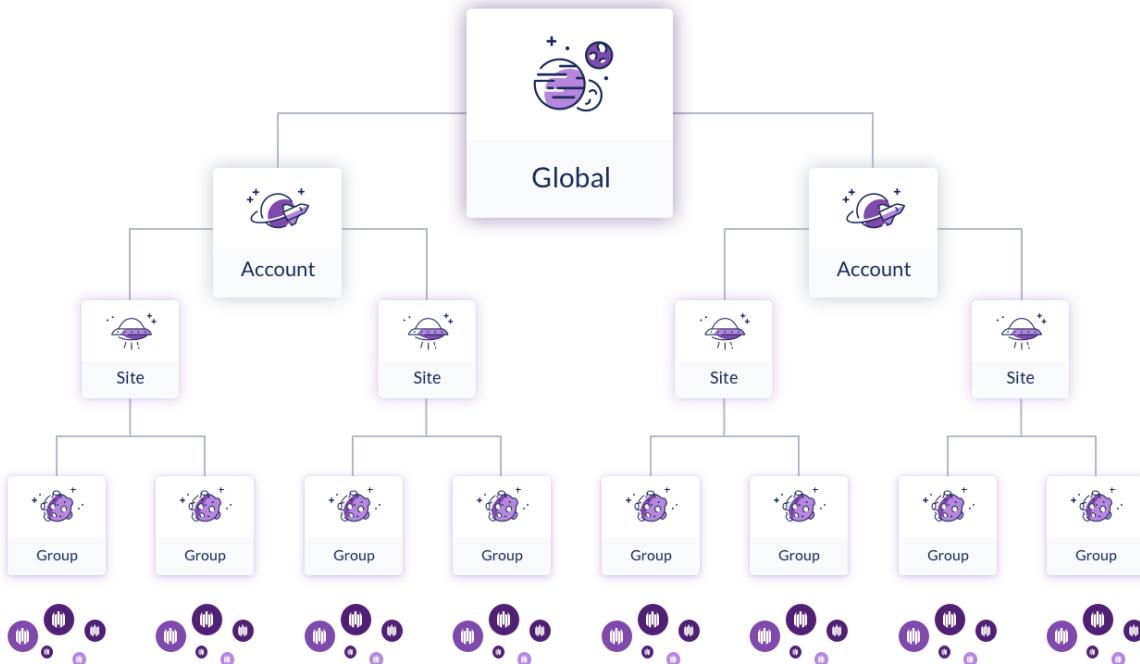
**Agents:** Windows 2.6+ | macOS 2.6+ | Linux 2.6+



This is the basic architecture of a SentinelOne deployment.

Component	Description
Cloud Intelligence Service	The SentinelOne proprietary intelligence on the cloud is a secure database of knowledge of malicious files, characteristics of behavior of infected endpoints, and much more. This data comes from proactive research, customer agent data, and feeds such as VirusTotal and ReversingLabs.
Management Console	The Management, hosted in the cloud or installed On-Prem at your site, is a web server, API, and engine scheduler. It communicates with the Cloud Intelligence Service and with your Agents. Every site has a private server and a browser-based WebUI Management Console to manage endpoints and users, track actions, analyze data, and mitigate threats with quick incident response.

Component	Description
Agent	Install the lightweight Agent on every endpoint (user computers and network servers). It detects and monitors behavior of the user and of the system (network activity, I/O transactions, memory transactions, installations, registry changes, and more) and communicates with the Management. The Agent engines give real-time prevention, detection, monitoring, remediation, and behavioral-based protection. Agents are managed by Scope.
Scope	Scope is the <b>boundary of influence</b> set to <i>Group</i> , <i>Site</i> , <i>Account</i> , or <i>Global</i> , for users, licenses, policies, blacklists, exclusions, packages, settings, reports, Deep Visibility, Device Control, Firewall Control, and Application management.
Account	One or more logical segments with permissions to configure features for specific Sites. An Account has permissions that were previously handled by SentinelOne or Globally for a whole deployment. Accounts are useful for deployments with multiple Sites for third-parties (such as MSSP) or that are controlled by multiple SOC officers. Each Account can have multiple Sites. An Account can have its own objects and settings and inherits from Global settings. (Management version Grand Canyon SP+)
Site	One or more physical or logical secured segments, each with its own objects and settings, specific or inherited from Global or from the Account. When you install an Agent, it is configured for a specific Site. A Site can belong to only one Account. (Management version Central Park+)
Group	One or more logical units of endpoints, for easier management, each with its own objects and settings, specific or inherited from Global settings, Account settings, or Site settings. A Group can belong to only one Site.



For example:

Company X has three physical sites in different time zones. Each site has thousands of computers and servers, running different operating systems. The Company X SOC team is five security officers.

The SOC manager, as the Global Admin, creates a first set of Sites, one for each physical site. The Global Admin creates two Account Admin user accounts for two of the security officers. One Account Admin manages one Site, and the other manages two Sites.

Each Account Admin reviews the topology of the users and endpoints. The first Account Admin creates two more Sites for a logical segmentation of the physical site. The second Account Admin also creates more Sites. The Account Admins create Site Admin user accounts for the other security officers. Each user has permissions over one or more Sites.

Everyone on the team can make groups of endpoints. The Global Admin manages the Global blacklist, exclusions, and default policy. The Account Admins can add hashes to the blacklists of the Sites in their scope. They can manage the exclusions and change the policy for the complete Account or a lower scope. The Site Admins take over the incident response for their endpoints. They also manage upgrades of the Agent versions for each group. The Account Admins and the Global Admin have permissions to take over or help if required.

## 2. Using the Management Console [Multi-Site]

**Management:** Central Park, Denali, Eiffel, Fuji, Grand Canyon, Houston

**Agents:** All

**Minimum Admin Scope:** Site Admin

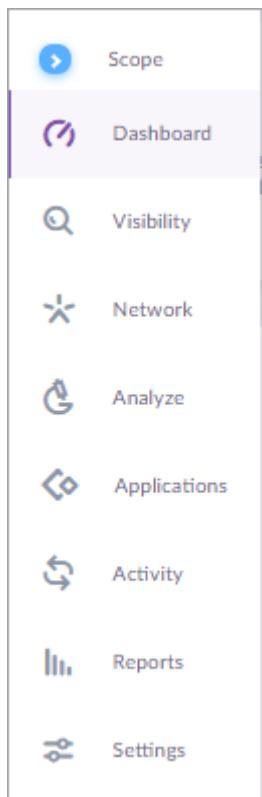
**Scope:** Selected Site, Account, or Global

Watch: [Introduction to Accounts](#)

Watch: [Tour of the Management Console](#)

Manage your SentinelOne Agents, threat mitigation, integrations, and other aspects of your SentinelOne environment from the Management Console.

Open the different views of the Management Console from the sidebar.



- **Scope** - Open the **Scope** pane and select a Group, Site, Account, or Global to manage it (from Grand Canyon SP3).
- **Dashboard** - See the status of endpoints and an overview of threats and detections. Open and sort the most recent detections.
- **Visibility** - Run Deep Visibility queries to see benign event information and set up watchlists for threat hunting.
- **Network** - Manage groups, policies, exclusions, and the blacklist, and run actions on endpoints. Manage Device Control and Firewall Control.

- **Analyze** - See all threats and detections and their status. Open the Forensics details and respond to threats and detections.
- **Applications** - Monitor applications installed on endpoints, from your Management Console.
- **Activity** - See and filter the full log of activities in your network.
- **Reports** - Get one-time and scheduled insight reports for different aspects of your environment.
- **Settings** - Configure Management Console settings, create users, manage Sites, and integrate third-party servers.

From version Grand Canyon SP3, select **Scope** to manage and see the scope hierarchy in the **Scope** pane.

Site	Endpoints
Austin	20
Cleveland	27
Default site	3
Philadelphia	13

- Click a scope in the list to see items that it contains.
- Search to find an Account, Site, or Group.
- Use the breadcrumbs at the top to see the hierarchy and navigate.

The information in the Management Console changes based on the selected scope and Admin scope.

Scope is the **boundary of influence** set to *Group*, *Site*, *Account*, or *Global*, for users, licenses, policies, blacklists, exclusions, packages, settings, reports, Deep Visibility, Device Control, Firewall Control, and Application management.

## 2.1. Admin Scope [Multi-Site]

**Management:** Central Park, Denali, Eiffel, Fuji, Grand Canyon, Houston

Account Admin supported from Grand Canyon SP3+

**Agents:** Windows 2.6+ | macOS 2.6+ | Linux 2.6+



The Global Admin manages the complete deployment and back-end configurations.  
This role is not available for our multi-tenant, cloud-based Management users.  
If you require Global Admin assistance, contact Support.



As an Account Admin, you manage your Accounts, the Sites in each Account, their endpoints, and their security objects. You can select and manage a specific Site or Group.

Your Accounts and Sites inherit settings and security objects from the Global scope. You can change most of the inherited settings and objects.



As a Site Admin you manage your Sites, their endpoints, and some of their security objects. You can select and manage Groups in the Site.

Your Sites inherit settings and security objects from the Account and Global Scopes. You can change many of the inherited settings and objects.

Watch: [Introduction to Accounts](#)

Watch: [Understanding Global and Site Assets](#)

(Turn on your audio)

Feature	Site Admin	Account Admin	Global Admin
Use Dashboard view	✓	✓	✓
Use Network view	✓	✓	✓
Create Site user	✓	✓	✓
Create Multi-Site user	✓	✓	✓
Delete Site user	✗	✓	✓
Create Account user	✗	✓	✓
Delete Account user	✗	✗	✓
Create Global user	✗	✗	✓
Define notifications	✓	✓	✓
Get a Site token	✓	✓	✓
Create Site	✗	✓	✓
Delete Site	✓	✓	✓

Feature	Site Admin	Account Admin	Global Admin
Change Site SKU			
Upload packages and set package Scope			
Upgrade Agents			
Move Agents between Groups			
Move Agents between Sites			
Uninstall Agent			
Define integrations (SSO, Syslog, SMTP)			
Actions on threats			
Generate reports			
Create Group (static / dynamic)			
Actions on Groups			
Filter activities			
Change policy			
Policy override			
Add blacklist			
Add exclusions			
Sites table			
Advanced mode			
Device Control			

Feature	Site Admin	Account Admin	Global Admin
Firewall Control	 Site	 Account	 Global
Applications			
Deep Visibility			
Remote Shell			

 \* - A Site Admin can use Remote Shell if given permission, but cannot enable it for other users.

 \* - Coming soon.

## 2.2. Logging in for the First Time [Multi-Site]

**Management:** Central Park, Denali, Eiffel, Fuji, Grand Canyon, Houston

**Agents:** All

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

As the first Management Console user in your local site, get the login credentials and URL from your SentinelOne contact.

### To open the Management Console:

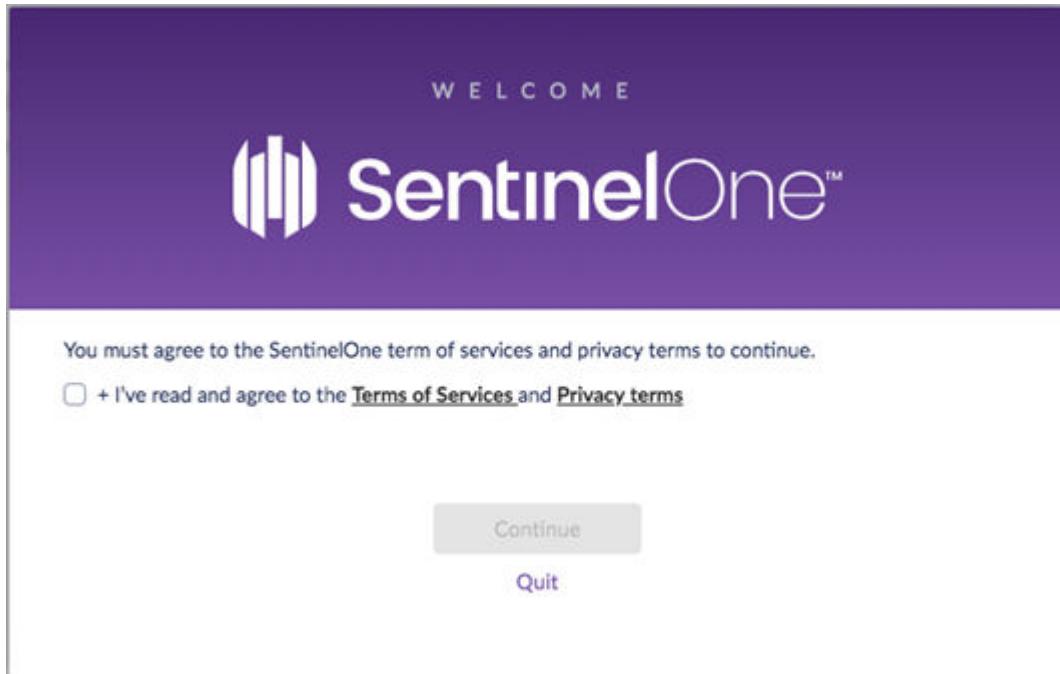
1. Open a supported browser on a computer with an active connection to the Internet (or to the On-Prem Management).
  2. In the address bar, enter the Management Console URL that you received from your SentinelOne contact.
- The SentinelOne Login opens.
3. Enter your email address and password.
  4. Optional: Select **Stay signed in** to save your credentials for future logins. Do not select this option if you log in from a public computer.

When **Stay signed in** is selected, the authentication still expires after the **Session Timeout** period in **Settings > Configuration**.

5. Click **Login**.

The Management Console opens in the browser.

- The first time you log in, the **Terms of Service** window opens.



- Click **Terms of Service** and **Privacy terms** to read them.
- Select that you agree to the terms.
- Click **Continue**.

## 2.3. Logging in with SSO [Multi-Site]

**Management:** Central Park, Denali, Eiffel, Fuji, Grand Canyon, Houston

**Agents:** All

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

The SentinelOne Management Console supports SAML with Okta for Single sign-on (SSO) services.

The SSO option shows automatically during login.

From Grand Canyon SP3, users are connected to an Account or Site based on their email domain and do not need to enter the name of a Site to login.

### To open the Management Console with SSO:

- Open a supported browser on a computer with an active connection to the Internet (or to the On-Prem Management).
- In the address bar, enter the Management Console URL that you received from your SentinelOne contact.

The SentinelOne Login opens.

If the Login window shows your username (email) and password, click **Login with SSO** to see the SSO login.

3. Click **Login with SSO**.
4. You are redirected to the SSO Provider's website. Enter your credentials.

You are redirected to the Management Console.

## 2.4. Logging in with Two-Factor Authentication [Multi-Site]

**Management:** Central Park, Denali, Eiffel, Fuji, Grand Canyon, Houston

**Agents:** All

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

The SentinelOne Management Console can work with Google Authenticator or Duo to require a code from the user's phone for login. Users must have a handheld device with the authenticator App installed.

If Two-Factor Authentication is required for a user, the Two-Factor Authentication window opens automatically during login.

See also: [Enabling Two-Factor Authentication](#).

### To open the Management Console with Two-Factor Authentication:

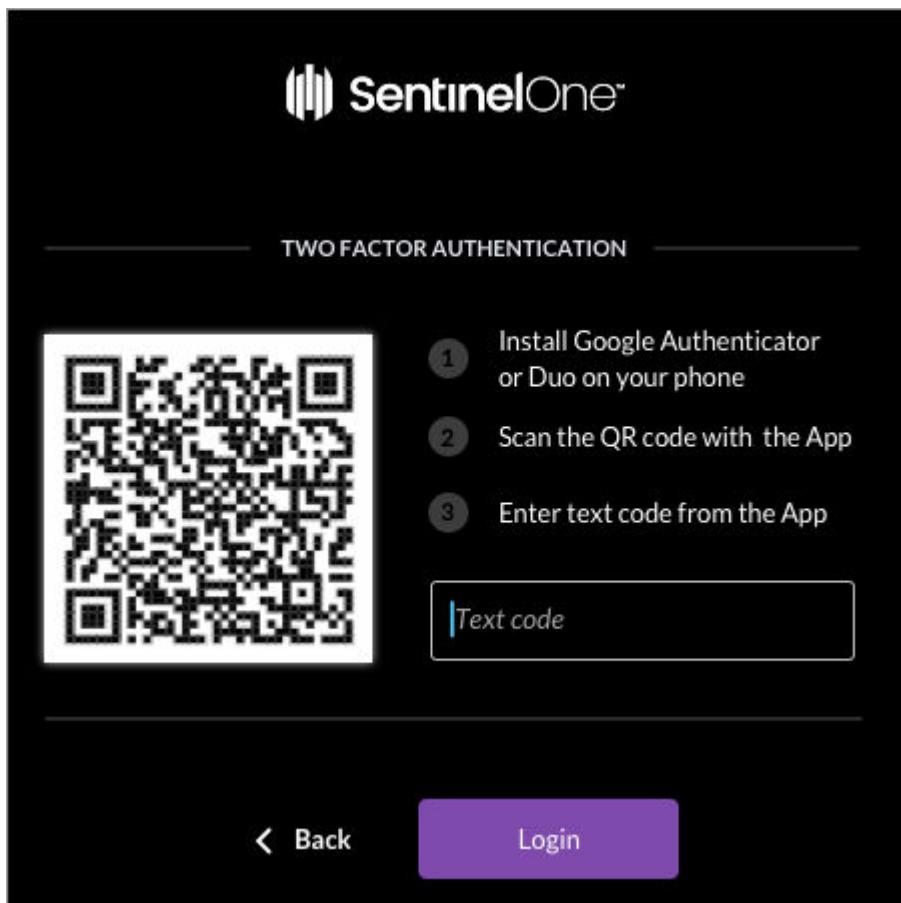
1. Open a supported browser on a computer with an active connection to the Internet (or to the On-Prem Management).
2. In the address bar, enter the Management Console URL that you received from your SentinelOne contact.

The SentinelOne Login opens.

3. Enter your email address and password.

The Two-Factor Authentication window opens.

The first time you use the App, you will need to scan a QR code, if you did not do that already.



4. Follow the instructions.
5. Enter the code from the authenticator App and press Enter.
6. If the authenticator shows more instructions (for example, Google Authenticator shows a series of codes to use offline), follow them and then click **Continue to Dashboard**.

## 2.5. Using the Dashboard [Multi-Site]

**Management:** Central Park, Denali, Eiffel, Fuji, Grand Canyon, Houston

**Agents:** All

**Minimum Admin Scope:** Site Admin

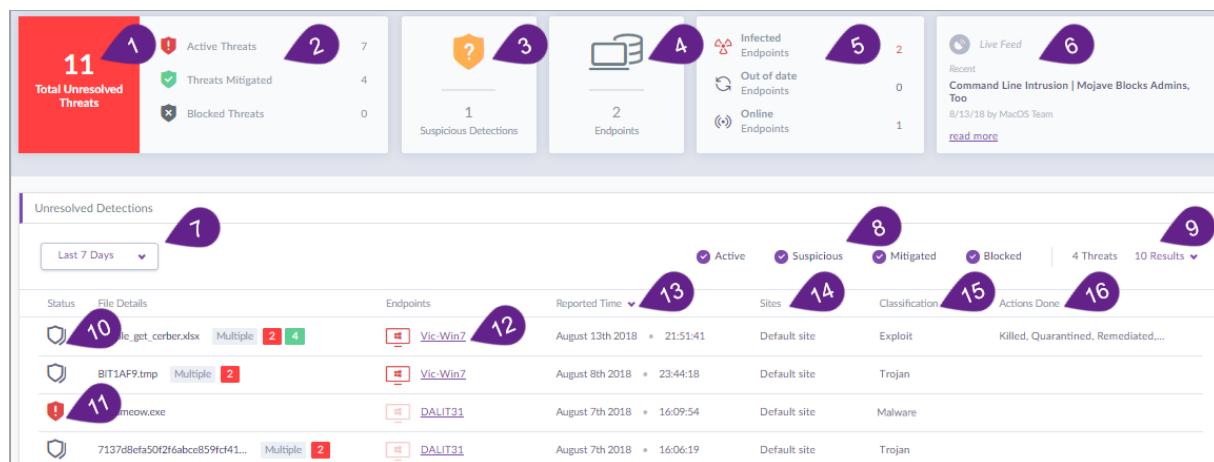
**Scope:** Selected Site, Account, or Global

Watch: [Tour of the Management Console](#)

In the Dashboard, see the status of endpoints and an overview of threats and detections.

The information shown depends on the scope selected.

**What can I do here?**



Item	Description
1	In the top pane, see an overview of threats, suspicious activity, and endpoint status in the environment, including the total number of unresolved threats.
2	Click <b>Active Threats</b> , <b>Threats Mitigated</b> , or <b>Blocked Threats</b> to open those items in the <b>Analyze</b> view.
3	Click <b>Suspicious Detections</b> to open those items in the <b>Analyze</b> view.
4	Click <b>Endpoints</b> to open all endpoints in the <b>Network</b> view.
5	Click <b>Infected</b> , <b>Out of date</b> , or <b>Online</b> endpoints to open those endpoints in the <b>Network</b> view.
6	Click the <b>Live Feed</b> to see the latest product messages and news.
7	Select the time period to show. The default is <b>Last 7 Days</b> .
8	Select or deselect a detection type to filter the results shown.
9	Select how many results to show in the page.
10	If there are multiple instances of the same threat, click the icon to open a new <b>Analyze</b> window with all instances of that threat.
11	Click a single item to open <b>Forensics details</b> .
12	Click the name of an endpoint to open the <b>Endpoint Details</b> .
13	See the date and time that the threat occurred.
14	See the Site or Sites where the detection occurred.
15,16	See the type of threat, and the mitigation actions done to it.

## 2.6. Filtering Activities [Multi-Site]

**Management:** Central Park, Denali, Eiffel, Fuji, Grand Canyon, Houston

**Agents:** All

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

From the Activity page, see all activities that occurred on your network. Use the filter buttons at the top of the page to see specific activities.

You can filter for one specific type of activity or select multiple filters to get a wider view. You can also select a timeframe for the search.

The screenshot shows the 'Activity Log' section of the SentinelOne interface. At the top, there are several filter buttons: 'Malware' (1), 'Exclusion (1)' (2), 'Operations (1)' (3), 'Mitigation' (4), 'Administrative (1)' (5), 'Select' (6), and 'Clear All' (7). To the right of these is a date range selector for April 2018 (8), with a 'From' field set to 00:00 and a 'To' field set to 09:15. Below the filters is a table of activity logs, each with a timestamp and a brief description. The first five rows show disk scan activities. The last row is partially visible. On the far right of the log table is a red circle containing the number 9, which points to the 'Apply' button in the date range selector. Another red circle containing the number 10 points to the 'Reset' button. A red circle containing the number 11 points to the 'Clear All' button at the top right.

## Activity Filters

Item	Description
1	Activity Filters: Make selections to show specific activities in the Activity Log below.
2	Activity Log: The results of the filters show here.
3	Malware Filter: Active, Mitigated, Blocked, Suspicious Activity
4	Exclusion Filter: Whitelist, Blacklist, Modified hash, Deleted hash, Cloud Whitelist, Cloud Blacklist, Cloud Modified hash, New Immune
5	Operations Filter: Management updated, Mitigation policy, Cloud intelligence, User added, SSO User added, User modified, SSO user modified, User deleted, Agent moved to Site, Agent moved to group, Group administration, Site administration
6	Mitigation Filter: Shut down, Disconnect from network, Threat kill, Threat quarantine, Threat remediate, Threat rollback
7	Administrative Filter: Agent subscribed, Agent updated, Uninstall requested, Uninstall sent, Agent uninstalled, Log operations, Fetch files operations, Agent decommissioned, Agent recommissioned, Full disk scan, Machine restarted, System update, Threat resolved, Mark as benign, Mark as threat, Passphrase
8	Select a timeframe. Click <b>Select</b> to open the calendar. Select dates from the calendar and, optionally, hours within the selected dates.
9	Click <b>Apply</b> to filter results by the selected dates and time.
10	Click <b>Reset</b> to clear the time setting.
11	Click <b>Clear All</b> to clear all filters.

To learn more about a threat or suspicious activity from the Activity list:

1. In Activity, click an item and click
2. Select an option:
  - **Analyze** - Opens the Forensics details.

- **Device Details** - Opens the Endpoint Details window with more options.

## 2.7. Using the Search Function [Multi-Site]

**Management:** Central Park, Denali, Eiffel, Fuji, Grand Canyon, Houston

**Agents:** Windows 2.6+ | macOS 2.6+ | Linux 2.6+

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

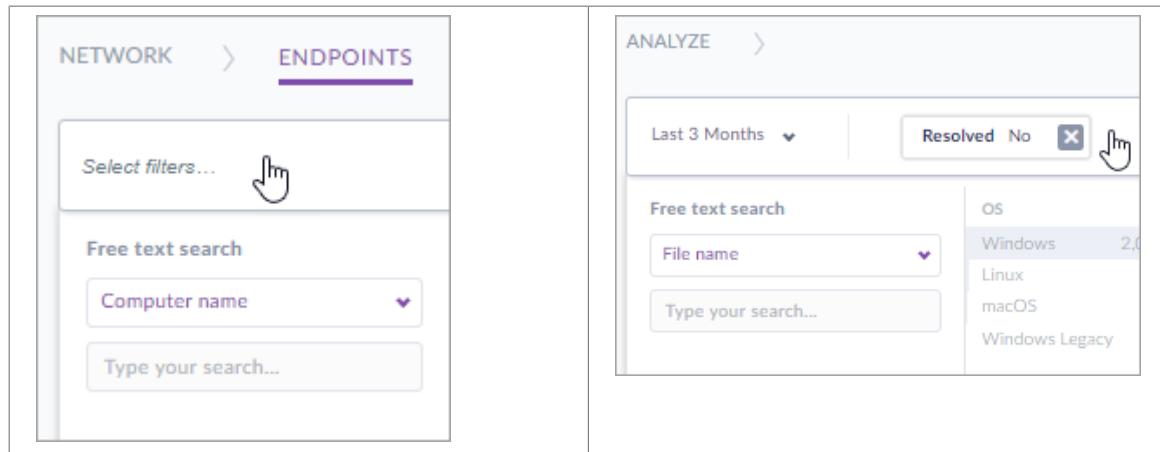
Different views in the Management Console have a search option. The search in each view applies to the objects of that view.

### Search Properties

View	Search for:
Analyze	From Fuji SP2, select a type and then enter a value. You can include multiple strings and types in the same search. If you have more than one of the same <b>type</b> , the Management Console filters for one OR the other. Filename (partial strings by default: extension is valid search string) Filepath Endpoint name Detection name SHA1 signature Full Disk Scan results ( <code>src:scan</code> ) Agent UUID (from Denali SP2)
Network > Endpoints** (Agent)	From Eiffel SP1, select a type and then enter a value. You can include multiple strings and types in the same search. If you have more than one of the same <b>type</b> , the Management Console filters for one OR the other. Local IP OS version (from Denali SP3) OS Name MAC Address Agent UUID (from Denali SP2) Computer name Last logged in user Visible IP All - Searches in all types
Exclusions	SHA1 signature Certificate signer File type Browser User who created the exclusion
Network > Blacklist	SHA1 signature
Settings > Users	User name User email

## To use the search function:

1. In **Network > Endpoints** or **Analyze**, click in the filters field. In other views, click the **Search** button.



In the other views, click the **Search** button: 

2. Enter the search criteria:

- In Analyze, select a timeframe. In **select type**, select the type of information to search for, then enter a string in the **Search** field.
- In Endpoints, in **select type**, select the type of information to search for, then enter a string in the **Search** field.

See also: [Creating Filters](#).

You can include multiple strings and types in the same search. If you have more than one of the same **type**, the Management Console filters for one OR the other.

3. Click a suggestion, or press **Enter** to see all results.

### 3. Installing Agents - Overview and Prerequisites [Multi-Site]

**Management:** Central Park, Denali, Eiffel, Fuji, Grand Canyon, Houston

**Agents:** Windows 2.6+ | macOS 2.6+ | Linux 2.6+

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

SentinelOne updates your Management Console with the latest Agent packages. Download the packages for the operating systems in your environment. You can use third-party tools to deploy the package to all of your endpoints by platform. Or you can install Agents individually.

If you have an On-Prem Management, contact your partner or vendor for the Agent packages that you need.

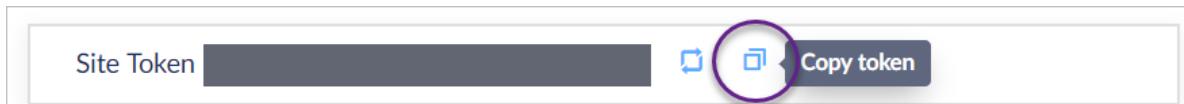
Watch: [How to work with Packages in the Management Console](#)

#### Before you begin:

- Make sure the endpoint meets the [System Requirements](#), including dependencies, patches, and configuration changes for specific operating systems. If the system requirements are not met, the installation will not complete.
- Best Practice: Uninstall third-party anti-virus software before you install SentinelOne. Other security software often prevents Agent installation or affects its performance. Install the Agent as quickly as possible after you uninstall the other security.

To run SentinelOne with third-party anti-virus software, contact SentinelOne Support to create the exclusions necessary for interoperability or see [Interoperability](#).

- During installation of new Agents, you must assign Agents to a Site using the Site Token. Get the Site Token from one Site, **Packages**.



From version Grand Canyon SP4, you can use a Group Token string during installation, instead of a Site Token string, to assign Agents directly to a static Group in a Site. Get the Group Token from one Site > one Group > **Network > Group Info**.

To upgrade existing Agents, see [Upgrading a Selected List of Agents \[Multi-Site\] \[41\]](#).

#### All Agents:

- If **Scan new Agents** is enabled in the policy of the Agent, Full Disk Scan starts when installation is complete. This applies to Windows Agent version 2.1 and later, macOS Agent version 2.5 and later, and Linux Agent version 2.6.3 and later.
- **Important for all endpoints:** We recommend that you enhance endpoint security with protection against physical theft and hacking (such as unauthorized disk mount modification). Enable full disk

encryption, apply OS patches, and maintain measures according to your vendor recommendations and corporate policies.

#### **Notes for Windows:**

- The Windows Agent installer works on supported Windows endpoints with default settings. If your environment is hardened with specific changes, see [Installing Windows Agents on Hardened Environments](#).
- Windows Agent installation does NOT require an immediate restart. Some of the SentinelOne engines work immediately after installation, and others work after the endpoint restarts.
  - The On Write mode, with Deep File Inspection and Reputation, is active immediately.
  - The Dynamic Engines (Behavioral AI) mode becomes active after you or the end-user restarts the endpoint. In the Management Console, the endpoint status is **Pending Reboot** until it restarts.
- To troubleshoot installation, see the [installation logs \[28\]](#).

#### **Notes for macOS:**

- To assign an Agent to a Site in a clean endpoint installation see [Installing on macOS Endpoints \[Multi-Site\] \[30\]](#).
- On 10.13 High Sierra and later, users must approve the kernel extension on their local computers. See [Installing on macOS High Sierra](#).

#### **Notes for Legacy Windows:**

- You can install with the /SILENT switch (case-sensitive).

## **3.1. Uploading a Package for Agent Installation or Upgrade [Multi-Site]**

**Management:** Central Park, Denali, Eiffel, Fuji, Grand Canyon, Houston

**Agents:** Windows 2.6+ | macOS 2.6+ | Linux 2.6+

**Minimum Admin Scope:** Account Admin

**Scope:** Selected Site, Account, or Global

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.

Upload the packages to the Management Console and then deploy the files to Agents.

Installation packages are Global (used for all Sites), for a selected Account (used for its Sites), or for a specific Site. Make sure that the **scope** of a package is correct for the intended Agents.

Upload Package		No Items Selected					Actions			Platform		Version		Status		File Name		Access Level		Scope Name		Available Date		SHA1		

**IMPORTANT:** If you install an Agent with the CLI, and then you upgrade from the Management Console, the upgrade configuration is according to the policy to which the Agent belongs. If the installer switches were different, they are overwritten with the policy switches.

Watch: [How to Upload Packages in the Management Console](#)

## To upload an Agent Installer file to the Management Console:

1. In the sidebar, click **Scope** and select a scope.
2. In the sidebar, click **Network** .
3. In the **Network** toolbar, click **Packages**.



**Note:** In the Packages page for one Site, you see the Site token for that Site. If you are in the Global or an Account scope, you do not see a token.

4. Click **Upload Package**.

The **New Package** window opens.

5. In **Update Platform**, select the OS of the package.
6. In **Version number**, enter the version number in this format: x.x.x.x. For example, 3.2.4.54  
If you do not enter 4 sections, a **Wrong version number** error shows.
7. In Status, enter **GA**, **EA**, or a different text that identifies the package status.
8. In **scope Level**, select **Global**, **Account**, or **Site**.  
If you select Account or Site, enter the names of the Accounts or Sites that can use the package.

New Package X

Platform \* Version \* Status

Access level

Global  Account  Site

Accounts \*  
Type account name

Type account name...

9. Click **Upload Package** to browse to the file.

10. Click **Save**.

The window stays open while the file uploads and you can see the progress.

Upgrade Agents from **Network > Endpoints > Actions > Update Software**.

### 3.2. Getting a Site or Group Token

**Management:** Central Park, Denali, Eiffel, Fuji, Grand Canyon, Houston

**Agents:** Windows 2.6+ | macOS 2.6+ | Linux 2.6+ |

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site

During the installation, you must assign Agents to a Site using the Site Token.

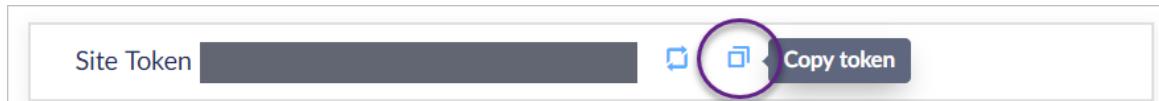
From version Grand Canyon SP4, you can use a Group Token string during installation, instead of a Site Token string, to assign Agents directly to a static Group in a Site.

### To get the Site Token:

1. In the sidebar, click **Scope**  and select a scope.  
Select one Site. If you are in any other scope, the Site Token does not show.
2. In the sidebar, click **Network** .
3. In the **Network** toolbar, click **Packages**.



4. In the **Site Token** section, click **Copy**.

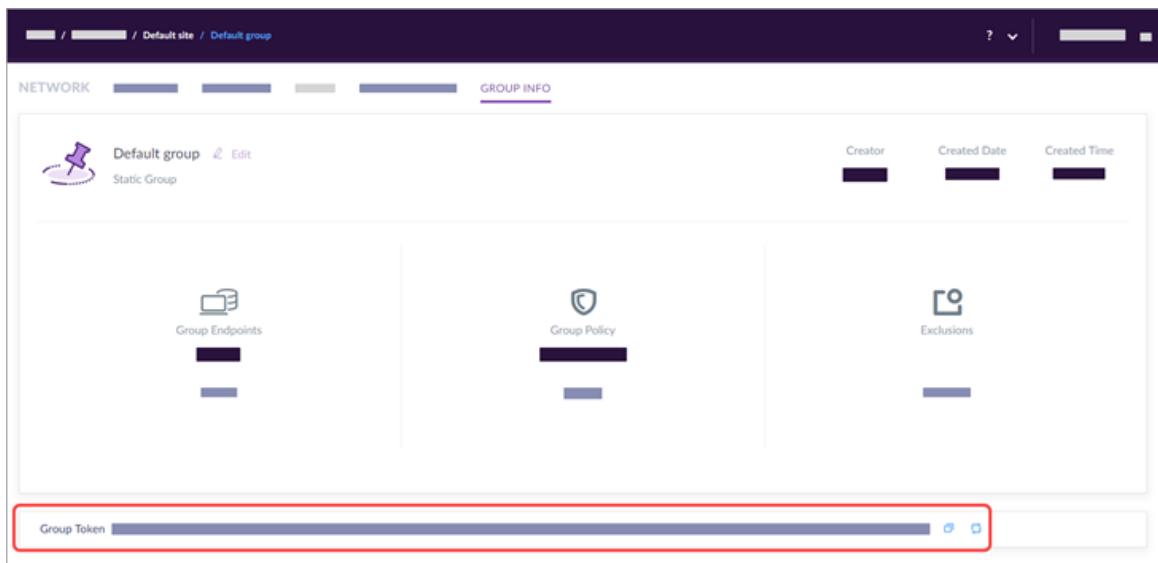


### To get a Group Token:

1. In the sidebar, click **Scope**  and select a scope.  
You must select one static Group.
2. In the sidebar, click **Network** .
3. In the **Network** toolbar, click **Group Info**.



4. In the **Group Token** section, click **Copy**.



### 3.3. Installing Multiple Agents [Multi-Site]

**Management:** Central Park, Denali, Eiffel, Fuji, Grand Canyon, Houston

**Agents:** Windows 2.6+ | macOS 2.6+ | Linux 2.6+

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

During the installation, you must assign Agents to a Site using the Site Token.

From version Grand Canyon SP4, you can use a Group Token string during installation, instead of a Site Token string, to assign Agents directly to a static Group in a Site. Get the Group Token from one Site > one Group > Network > Group Info.

#### To get the Site Token:

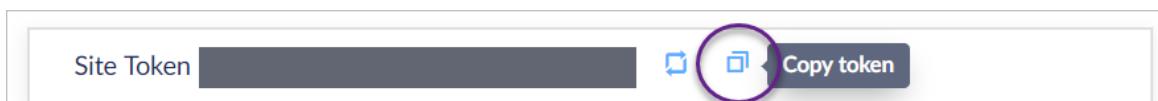
1. In the sidebar, click **Scope**  and select a scope.

Select one Site. If you are in any other scope, the Site Token does not show.

2. In the sidebar, click **Network** .
3. In the **Network** toolbar, click **Packages**.



4. In the **Site Token** section, click **Copy**.



## To install multiple Agents:

1. In the Network toolbar, click **Packages**.



Installation packages are Global (used for all Sites), for a selected Account (used for its Sites), or for a specific Site. Make sure that the **scope** of a package is correct for the intended Agents.

2. Click the Download icon  of the latest package for a platform.



3. Copy the package to a network drive that all endpoints can access.
4. Use a third-party tool to deploy the Agents.
5. Make sure to enter the Site Token or Group Token during installation.

**Important for all endpoints:** We recommend that you enhance endpoint security with protection against physical theft and hacking (such as unauthorized disk mount modification). Enable full disk encryption, apply OS patches, and maintain measures according to your vendor recommendations and corporate policies.

## 3.4. Installing on Windows Endpoints [Multi-Site]

**Management:** Central Park, Denali, Eiffel, Fuji, Grand Canyon, Houston

**Agents:** Windows 2.6+

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

The installation requires Administrator privileges.

During the installation, you must assign Agents to a Site using the Site Token.

From version Grand Canyon SP4, you can use a Group Token string during installation, instead of a Site Token string, to assign Agents directly to a static Group in a Site. Get the Group Token from one Site > one Group > **Network > Group Info**.

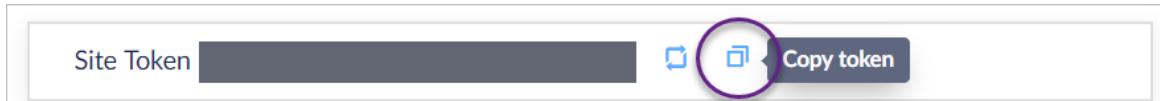
### To get the Site Token:

1. In the sidebar, click **Scope**  and select a scope.  
Select one Site. If you are in any other scope, the Site Token does not show.
2. In the sidebar, click **Network** .

- In the Network toolbar, click **Packages**.



- In the Site Token section, click **Copy**.



### To install the Agent on a Windows endpoint:

- Download the latest Windows Installer package.

Make sure the scope of the package includes the Site that the Agent will go to.

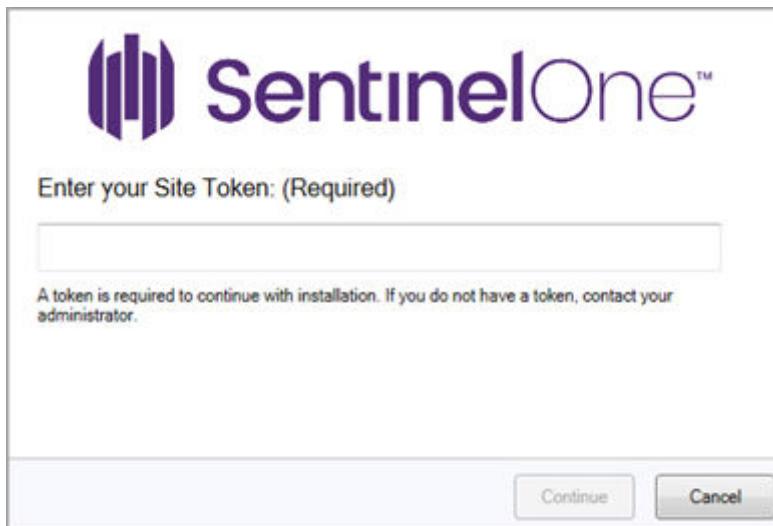


Best Practice: Download the file to the local endpoint.

- Run the Installer package and follow the instructions.

- To install with the interactive GUI wizard:

Run the installation package and enter the Site or Group Token when prompted in the installation wizard.



- To install silently without user interaction:

Run the installer in CLI with switches for the token and silent installation. For example: `C:\Users\S1\Desktop\Sentinel\Installer\Installer.exe /SITE_TOKEN=<string> /SILENT`

- Complete the installation:

The On Write mode, with Deep File Inspection and Reputation, is active immediately.

The Dynamic Engines (Behavioral AI) mode becomes active after you or the end-user restart the endpoint. In the Management Console, the endpoint status is **Pending Reboot** until it restarts.

### Show Me video: How to Install Windows Agents

**Important for all endpoints:** We recommend that you enhance endpoint security with protection against physical theft and hacking (such as unauthorized disk mount modification). Enable full disk encryption, apply OS patches, and maintain measures according to your vendor recommendations and corporate policies.

#### 3.4.1. Agent Installer Command Line Options [Multi-Site]

**Management:** Central Park, Denali, Eiffel, Fuji, Grand Canyon, Houston

**Agents:** Windows 2.6+

After you download an Agent installer file from the Management Console, you can use the Installer to install the Agent from the CLI.

You can configure many of these options from the [Agent Configuration Settings](#) in the policy.

These option switches are only for Windows Agents.

- You can run the [macOS Agent installer \[30\]](#) without configuration switches.
- The Linux Agent requires [the --site-token option \[36\]](#).

**IMPORTANT:** If you install an Agent with the CLI, and then you upgrade from the Management Console, the upgrade configuration is according to the policy to which the Agent belongs. If the installer switches were different, they are overwritten with the policy switches.

**Switches are case sensitive.**

For example:

```
C:\Users\S1\Desktop\Sentinel\Installer\Installer.exe /SITE_TOKEN=<string>/
SERVER_PROXY=http://proxyserver.com:3126 /
SERVER_PROXY_CREDENTIALS=myName:myPassword123
```

#### Windows Agent installation exit codes:

To see the exit code: From the same CMD or shell session that the installer was launched, run: echo %ErrorLevel%

- 0 = Success
- -1 (or other non-zero) = Failure

## Agent Installer Switches

Switch	Description
/SITE_TOKEN=<string>	<p>Assigns Agents to a Site or static Group.</p> <p>If you do not enter a Token, Agents go to the Default Site.</p> <p>Get the Site Token from one Site, <b>Packages</b>.</p> <p>Get the Group Token from one Site &gt; one Group &gt;<b>Network &gt; Group Info</b>.</p>
/Q /S /QUIET /SILENT	Silent installation (no UI, no user interaction, no reboot).
/NORESTART /REBOOT /FORCERESTART	<p>With a Silent installation switch, you can use an optional flag for endpoint reboot:</p> <ul style="list-style-type: none"> <li>Installs the agent without requiring a restart. Use for mass deployment, when you send a message to users, or to restart their computers that day.</li> <li>Reboot if needed.</li> <li>Always Reboot.</li> </ul>
/SERVER_ADDRESS=https://server_url	Sets the address of the Management to which the agent connects.
/SERVER_PROXY=mode	<p>Sets a proxy server between the Agent and its Management.</p> <p><b>Mode valid values:</b></p> <ul style="list-style-type: none"> <li>auto = use the Windows LAN settings (PAC file)</li> <li>system = use <b>Other</b> proxy (not from OS) configured in the local Agent</li> <li>user,fallback[:port] = user mode on Windows</li> <li>http://{IP / FQDN} : [port]</li> </ul> <p>(Supported from Agent versions 2.0)</p>
/SERVER_PROXY_CREDENTIALS=user:pass	Sets credentials to authenticate with the Management proxy. (Supported from Agent versions 2.0)

SWITCH	Description
/IOC_PROXY= <i>mode</i>	<p>Sets a proxy server between the Agent and the Deep Visibility EDR data server.</p> <p><b>Mode valid values:</b></p> <ul style="list-style-type: none"> <li>• <i>single</i> = use the same proxy for Management and for Deep Visibility</li> <li>• <i>auto</i> = use the Windows LAN settings (PAC file)</li> <li>• <i>system</i> = use <b>Other</b> proxy (not from OS) configured in the local Agent</li> <li>• <i>user,fallback[:port]</i> = user mode on Windows</li> <li>• <i>http://{IP   FQDN} : [port]</i></li> </ul> <p>(Supported from Agent version 2.8)</p>
/IOC_PROXY_CREDENTIALS=" <i>username:password</i> "	Sets the username and password to authenticate with the Deep Visibility proxy. (Supported from Agent version 2.8)
/FORCE_PROXY	<p>Prevents fallback to direct communication if the proxy is not available. (Supported from Agent versions 2.0)</p> <p>Important! If the Management proxy or the Deep Visibility proxy is configured with <i>user</i> mode, do not use Force Proxy</p>
/NOUI	Installs the Agent with the UI disabled (no tray icon or notifications). (From Windows Agent version 2.1.x, this option will be overwritten by the policy.)
/NOLOGGING	Disables Agent logging.
/chromeExtensionOff	Defines if the Deep Visibility Chrome Extension is installed as part of the Agent installation process. Without the flag, the Chrome Extension is installed. (Supported from Agent version 2.5.2.)

Switch	Description
/safeBootProtectionOff	<p>Disables the Safe Boot Protection feature.</p> <p>Use this flag ONLY if you use Veeam Backup solution, with the Veeam “Application-Aware processing” option enabled on the Windows endpoint.</p> <p>Without the flag, Safe Boot is enabled. (Supported from Agent versions 2.5.2 and 2.6.)</p>
/VDI	<p>This switch is for Windows Agents 2.6 to 3.0. It is <b>deprecated in Windows Agent version 3.1</b>. In Windows Agent version 3.3.3 and expected in 3.4 EA2, the /VDI switch is supported again.</p> <p>Install on Virtual Desktop Infrastructure or VMs with a Golden (Master) Image.</p> <p>Important! If you installed with this switch, do not upgrade these Agents through the Management Console. To upgrade to 3.1 and later, see <i>Upgrading from an Image</i>.</p> <p>If you install with this switch on Windows Agent 3.3.3+, you do not need to use the switch again when upgrading.</p>

**Note:** There is no installer switch to disable VSS and rollback. If you are sure you must disable the rollback feature, use the SentinelCtl option.

**Important for all endpoints:** We recommend that you enhance endpoint security with protection against physical theft and hacking (such as unauthorized disk mount modification). Enable full disk encryption, apply OS patches, and maintain measures according to your vendor recommendations and corporate policies.

### 3.4.2. Windows Agent Installation Logs

**Management:** Central Park, Denali, Eiffel, Fuji, Grand Canyon, Houston

**Agents:** Windows 2.7+

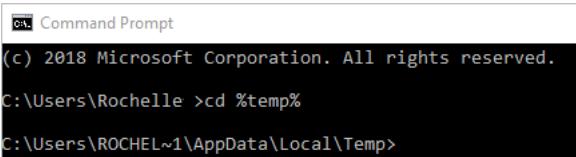
**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

Starting with 2.7, Windows Agents generate installation logs in clear text on the endpoints.

#### Log Location per Activity in Detail

Activity Type	Initiated By	Log Location
Clean Install	Management or GPO	%windir%\temp (%windir% is C:\Windows)

Activity Type	Initiated By	Log Location
Clean Install	End user	%temp% %temp% is C:\Users\username\AppData\Local\Temp If you use %temp%, it will always work. To use the actual full path, you must use replace <i>username</i> with the username of the person logged in to the endpoint. 
Clean Install	Logs are copied automatically after successful installation	C:\ProgramData\Sentinel\UserCrashDumps
Customize Installation Folder Name	End user	/ INSTALL_DIR="c:\Program Files\Customized_Folder_Name"
Upgrade	Any	C:\ProgramData\Sentinel\UserCrashDumps
Uninstall	Management or GPO	%windir%\temp
Uninstall	End user	%temp%

**Tip:** To troubleshoot installation issues, search the logs for "ERROR" or "FATAL".

### 3.4.3. Installing Windows Agents on VM or VDI

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

This is an overview of the recommended installation methods for Windows Agents on VM or VDI.

We are working on solutions to improve Windows Agent installations on all VM types.

#### Recommended Installation Methods

VM Installation Type	Method	Notes
Cold clone	Use the /VDI installation switch	From 3.3.3, after installation with the /VDI switch, you can upgrade Agents normally from the Management Console without the /VDI switch.

VM Installation Type	Method	Notes
Hot (live) clone and Persistent	Use the <code>/VDI</code> installation switch	Until the first reboot, cloned Agents will have the same UUID as the master image. If it reboots relatively fast, this is fine. If there will be a long time before the first reboot, it will cause control issues.
Hot (Live) clone and Non-Persistent or Hot clone without reboot soon	Before installation, contact SentinelOne Support with a request to enable automatic UUID management from the SentinelOne Management.	The ability to enable automatic UUID management depends on the Agent versions in your environment and the way they were deployed. It is not always possible.
All VM types on Agent version 3.1-3.3.2	Use the <code>sentinelctl agent_id -r -b</code> command	This method is supported for all versions, Hot and Cold clones. If it works well on your environment, use it with versions 3.3.3 and later. If there are issues, use the <code>/VDI</code> installation switch.

### 3.5. Installing on macOS Endpoints [Multi-Site]

**Management:** Central Park, Denali, Eiffel, Fuji, Grand Canyon, Houston

**Agents:** macOS 2.6+

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

Make sure you have [all the requirements](#) before you start the installation.

During the installation, you must assign Agents to a Site using the Site Token.

From version Grand Canyon SP4, you can use a Group Token string during installation, instead of a Site Token string, to assign Agents directly to a static Group in a Site. Get the Group Token from one Site > one Group > **Network** > **Group Info**.

#### To get the Site Token:

1. In the sidebar, click **Scope**  and select a scope.

Select one Site. If you are in any other scope, the Site Token does not show.

2. In the sidebar, click **Network** .

- In the Network toolbar, click **Packages**.



- In the Site Token section, click **Copy**.



## To install the Agent on one macOS endpoint:

- In the Network toolbar, click **Packages**.



- Download the latest macOS Installer package.

Make sure the scope of the package includes the Site that the Agent will go to.



Best Practice: Download the file to the local endpoint.

- Save the Site Token or Group Token in a plain text file in the same folder as the SentinelOne Installer package. Name the file: com.sentinelone.registration-token
- Run the installer: `$ sudo /usr/sbin/installer -pkg Desktop/Sentinel*.pkg -target /`

Or let the user install the Agent:

- Give the Token string to the user (for example, send a message or email with the token string).
- Users run the installation package and enter the Token string when prompted in the installation wizard. This is a new, optional step in installation with interactive UI, from macOS Agent version 2.6.



- Complete the installation:

On macOS 10.13 High Sierra and later, users must approve the kernel extension on their local computers, in **System Preferences > Security and Privacy > General tab > ALLOW**. See [Installing on macOS High Sierra](#).

**Important for all endpoints:** We recommend that you enhance endpoint security with protection against physical theft and hacking (such as unauthorized disk mount modification). Enable full disk encryption, apply OS patches, and maintain measures according to your vendor recommendations and corporate policies.

### Troubleshooting - If you forgot to copy the Site or Group Token to the endpoint:

1. After Agent installation, get the Token from the Management Console.
2. Run:

```
sudo sentinelctl set registration-token <path-to-token>
```

OR

```
sudo sentinelctl set registration-token -- <token> --passphrase
<passphrase>
```

### 3.5.1. Installing and Upgrading macOS Agent with Jamf

**Agents:** macOS 2.6+

Jamf is macOS software to build packages, manage inventory and images, and run remote updates. You can use Jamf, or other MDM software, to install the SentinelOne macOS Agent.

During the installation, you must assign Agents to a Site using the Site Token.

From version Grand Canyon SP4, you can use a Group Token string during installation, instead of a Site Token string, to assign Agents directly to a static Group in a Site. Get the Group Token from one Site > one Group > **Network > Group Info**.

#### To get the Site Token:

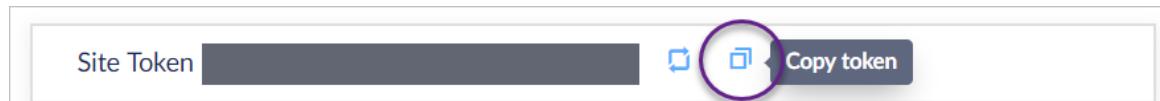
1. In the sidebar, click **Scope**  and select a scope.

Select one Site. If you are in any other scope, the Site Token does not show.

2. In the **Network** toolbar, click **Packages**.



3. In the **Site Token** section, click **Copy**.



## To install with Jamf:

1. In the Network toolbar, click **Packages**.



2. Download the PKG of the macOS Agent version to install.
3. Launch Jamf and log in.
4. Create a configuration profile with these values in the Approved Kernel Extensions:

Kext Bundle ID: com.sentinelone.sentinel-kext Developer ID: 4AYE5J54KN

The screenshot shows a configuration profile being created in Jamf. The 'Approved Team ID' section is expanded, showing a 'DISPLAY NAME' field containing 'SentinelOne' and a 'TEAM ID' field containing '4AYE5J54KN'. Below this, under 'Approved Kernel Extensions (Optional)', there is a table:

DISPLAY NAME	KERNEL EXTENSIO...
com_sentinelone_S entinelKext_26225 24880146	
Kext Bundle ID	com.sentinelone.se ntinel-kext

5. Click **Computer Management**.
6. Add the SentinelOne Agent PKG file to Jamf.
7. Click **Script** and enter these lines, with your values for the Site or Group Token and package version:

```
sudo echo "token" > /Library/Application\ Support/JAMF/Waiting\ Room/  
com.sentinelone.registration-token  
sudo /usr/sbin/installer -pkg /Library/Application\ Support/JAMF/Waiting  
\ Room/Sentinel-Release-version.pkg -target /
```

8. Click **Save**.

The Agent installs the next time the selected endpoints connect with Jamf.

## To upgrade with Jamf:

1. Download the PKG of the new macOS Agent version.
2. Launch Jamf and log in.
3. Create a configuration profile with the same kextvalues as the installation profile.

4. Add the new Agent PKG file to Jamf.
5. Click **Script** and enter this line, with your values for the PKG path and filename:

```
sudo sentinelctl upgrade-pkg PKG_pathname
```

6. Click **Save**.

The Agent updates the next time the selected endpoints connect with Jamf.

**To monitor status with Jamf:** You can monitor macOS endpoints with Jamf. Configure a custom Extension Attribute on the install base. Then deploy the script (below) that returns the status of the Agent on each endpoint. To learn how to configure Extension Attributes in Jamf, see the Jamf documentation (Computer Extension Attributes).

```
#!/bin/sh

# This script will check the status of the SentinelOne Agent
if command -v sentinelctl 1>/dev/null; then
    echo "<result> SentinelOne agent is installed in path `ps aux | grep -E 'sentineld\$' | awk '{ print $11 }'` | sed 's|sentineld|sentinelctl|g'` with version `sentinelctl version | awk '{print $2}'` and was connected to management console `sentinelctl online 2>/dev/null | head -n 1 | awk '{print $2}'` last time at `sentinelctl online 2>/dev/null | sed -n 2p | cut -c 11-` </result>"
else
    s1_agent=$(ps aux | grep -Ei "sentineld\$" | awk '{ print $11 }' | grep -v grep)
    if [ -z $s1_agent ]; then
        echo "<result>SentinelOne Agent is not Installed.</result>";
    else
        s1_agent=$(echo $s1_agent | sed 's|sentineld|sentinelctl|g')
        echo "<result>SentinelOne Agent is running but could not locate SentinelCtl in the default PATH /usr/local/bin. The full path is -$s1_agent </result> ";
    fi
fi
```

## 3.6. Linux Agent 3.x Installation

The SentinelOne Linux Agent version 3.x is a significant change to the Linux Agent.

The Linux Agent uses standard Linux packaging formats: RPM and DEB.

### To install the Linux Agent:

1. Log in as a privileged user, or run the command with sudo.
2. Run the installation command:

Package format	Command
RPM	<code>rpm -i --nodigest package_pathname</code>
DEB	<code>dpkg -i package_pathname</code>

Installation usually requires less than one minute.

Installation is not enough! You must implement the next steps: Associate and Activate.

3. Associate the Agent with your Management and a Site [35].
4. Activate the Agent [36].

When the installation completes, the files are extracted to the correct paths, and SentinelOne Agent services are ready. But the Agent does not start until it is configured and explicitly activated.

Note: You can simplify installation with [Ansible](#).

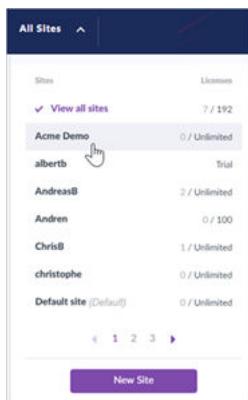
### 3.6.1. Agent Association

Every Agent belongs to a Site of a specific Management Console. If an installed Agent package is not bound to a specific Site, your Management Console cannot manage the Agent.

#### To get the Site Token:

1. In the sidebar, click **Scope**  and select a scope.

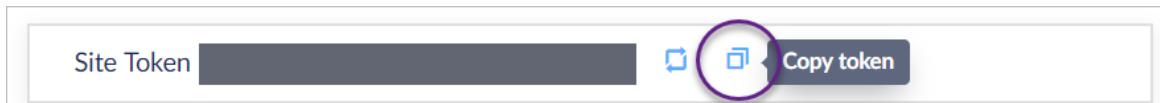
Select one Site. If you are in any other scope, the Site Token does not show.



2. In the **Network** toolbar, click **Packages**.



3. In the **Site Token** section, click **Copy**.



4. On the Linux endpoint, as a privileged user, run this command with the Site Token that you copied:

```
sudo /opt/sentinelone/bin/sentinelctl management token set site_token
```

Or, you can save the Site Token string in a plain text file and call a command to read the file. For example:

```
sudo /opt/sentinelone/bin/sentinelctl management token set $(cat /media/user/Downloads/site-key)
```

Expect this command to complete in seconds.

```
# sentinelctl management token set
eyJlcw...=MjMifQ==
Setting registration token...
Registration token successfully set
```

### 3.6.2. Agent Installation and Activation on Master Images



#### WARNING

**Important:** If you install the Agent on a master image, do not activate the Agent on the master image.

#### To install on a Master Image

1. Run the DEB or RPM installation command on the master image.
2. Associate the Agent with the site.
3. Create the clones.
4. Activate each Agent.

### 3.6.3. Agent Activation

When the Agent is installed and associated with the correct Console and Site, activate it:

```
sudo /opt/sentinelone/bin/sentinelctl control start
```

This command creates a unique identifier. The UUID is persistent on this endpoint and for the associated Management Console.

Expect this command to complete in seconds. It will show:

```
Starting agent...
Agent is running
```

The Agent shows in the Console.

Optional: To see the UUID:

```
# sudo /opt/sentinelone/bin/sentinelctl management uuid get
```

## 3.7. Installing on Linux Endpoints [Multi-Site]

**Management:** Central Park, Denali, Eiffel, Fuji, Grand Canyon, Houston

**Agents:** Linux 2.6.x

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

To learn how to install Linux Agent version 3.x, see the [Linux Agent version 3.0](#) guide.

Make sure you have [all the requirements \[17\]](#) before you start the installation.

See specific workarounds for the distributions you use:

- [Debian 9](#)
- [Fedora](#)
- [Oracle](#)

For virtual environments where cloning is possible or required, see [Duplicate UUID in Linux](#) to prevent or resolve issues of duplicate Linux Agent IDs.

During the installation, you must assign Agents to a Site using the Site Token.

From version Grand Canyon SP4, you can use a Group Token string during installation, instead of a Site Token string, to assign Agents directly to a static Group in a Site. Get the Group Token from one Site > one Group > **Network > Group Info**.

### To get the Site Token:

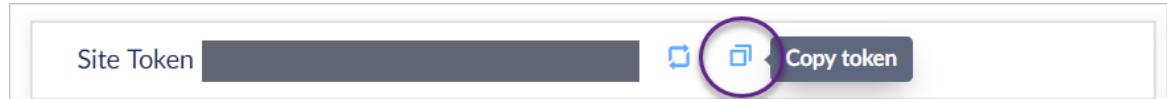
1. In the sidebar, click **Scope**  and select a scope.

Select one Site. If you are in any other scope, the Site Token does not show.

2. In the sidebar, click **Network** .
3. In the **Network** toolbar, click **Packages**.



4. In the **Site Token** section, click **Copy**.



### To install the 2.x Agent on a Linux endpoint:

1. In the **Network** toolbar, click **Packages**.



2. Download the latest Linux Installer package.

Make sure the scope of the package includes the Site that the Agent will go to.

Best Practice: Download the file to the local endpoint.

3. Make the BSX executable:

```
chmod +x path/SentinelAgent-version-Linux.bsx
```

4. Run the BSX installer.

#### **Installation with a Site or Group token:**

```
./SentinelAgent-version-Linux.bsx -s "string"
```

For example:

```
./SentinelAgent-2.6.1.1390-Linux.bsx -s  
"eyJlcw...5zzW"
```

#### **Installation with Site or Group Token and a proxy:**

```
./SentinelAgent-version-Linux.bsx -s "string" -p "address:port"
```

For example:

```
./SentinelAgent-2.6.1.1390-Linux.bsx -s  
"eyJlcw...5zzW" -p "192.0.2.5:80"
```

**Important for all endpoints:** We recommend that you enhance endpoint security with protection against physical theft and hacking (such as unauthorized disk mount modification). Enable full disk encryption, apply OS patches, and maintain measures according to your vendor recommendations and corporate policies.

## 3.8. Pending Action [Multi-Site]

**Management:** Central Park, Denali, Eiffel, Fuji, Grand Canyon, Houston

**Agents:** Windows 2.6+ | macOS 2.6+ | Linux 2.6+

Agents that require an action to become fully functional show as **Pending action** in the **Network** view of the Management Console and in the **Endpoint Details** window.

The **Pending action** statuses are described here. More than one status can show for one endpoint.

### **Agent Suppressed (macOS only)**

- **Explanation** - The Agent is running but not providing protection. This can happen if kernel extension permission or any other vital resource is missing.
- **Action required** - See the [Agent Requirements](#) for supported operating systems. Upgrade the Agent or the endpoint OS. Contact SentinelOne Support if you cannot find the source of the problem.

### **Missing Permissions**

- **Explanation** - The user permissions on the endpoint computer do not allow SentinelOne Agent installation. For example, if you install an Agent on macOS 10.13 High Sierra and higher, users must approve the kernel extension.
- **Action required** - For macOS 10.13 High Sierra and higher, see [macOS and SentinelOne Agent](#). For other operating systems, contact Technical Support.

## Unprotected (macOS only)

- **Explanation** - The Agent is unprotected because Anti-tampering is disabled or the OS protection tools are off.
- **Action required** - Enable Anti-tampering for the Agent. Make sure that it is enabled in the policy of the Agent. If it is already enabled in the policy, it is probably disabled in the Agent's local configuration.

## Incompatible OS (macOS only)

- **Explanation** - The Agent does not support the Operating System installed. Usually this happens when an endpoint's OS is upgraded to a version that the current Agent does not support. The Agent will suppress itself.
- **Action required** - See the [Agent Requirements](#) for supported operating systems. Upgrade the Agent or the endpoint OS. Contact SentinelOne Support if you cannot find the source of the problem.

## Reboot

- **Explanation** - A reboot is required to make the Agent fully functional. For example, some policy override configuration changes can require a reboot.

When a Windows Agent installs, some policy engines are active immediately and the On Execute engines (Behavioral AI) become active after a reboot.

- **Action required** - Reboot the endpoint manually or:

1. From the Management Console, select one endpoint, or all endpoints in a group or filter set.
2. Click **Actions > Reboot**.

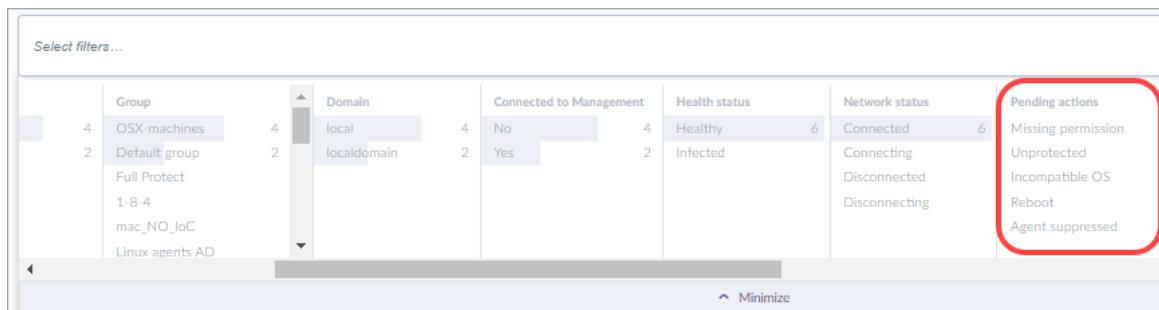
## To see all endpoints with a pending action:

1. In the sidebar, click **Scope**  and select a scope.
2. In the sidebar, click **Network** .

The list of endpoints in the selected scope opens.

3. Click **Filters**.

The filtering categories and options show.



Select filters...		Group	Domain	Connected to Management	Health status	Network status	Pending actions
4	OSX machines	4	local	4 No	4 Healthy	6 Connected	Missing permission
2	Default group	2	localdomain	2 Yes	2 Infected	6 Connecting	Unprotected
	Full Protect					Disconnected	Incompatible OS
	1:8:4					Disconnecting	Reboot
	mac_NO_IoC						Agent suppressed
	Linux agents AD						

4. **Pending actions** is one of the default filter categories. Click one or more options to show endpoints with those issues.
5. Optional: Click **Save Filter** to save the Filer Set or use it to create a Group.

From a Group or filter set, you can run actions on multiple endpoints, such as **Reboot** or **Shutdown**. You can easily track the status of the endpoints to make sure that the necessary actions are done.

Watch [How to Fix the Pending Action Status](#)

## 3.9. Understanding Agent UUID

**Management:** Fuji, Grand Canyon, Houston

**Agents:** Windows 3.1+

UUID is *Universally Unique ID*. Every Agent must have a UUID that is unique in the SentinelOne cloud. When an Agent registers with its Management, the Agent gets its UUID as part of the registration.

Property	Value
UUID	28558f791e58a840e25...
Other Properties	Multiple rows of short purple bars representing other endpoint details.

If you create endpoints from an image, there can be UUID errors. We are working to improve the process of creating endpoints from an image while preventing duplicate UUIDs.

### From version 3.3.3:

- The /VDI installation switch is now supported again. It is recommended for VM environments that use Cold cloning or Hot and Persistent cloning. See [Installing Windows Agents on VM or VDI](#).

If an Agent is installed with this installation switch, its UUID cannot be changed by the **Randomize UUID** command from the Management Console (available from the **Advanced** options)

- If the `sentinelctl.exe agent_id -r -b` command works well in your environment, continue to use that method.

From Windows Agent 3.1+ on Fuji+ through Windows Agent 3.3.2, install the Agent and then run the `sentinelctl` command on the master image:

```
sentinelctl.exe agent_id -r -b -k "<passphrase>"
```

On the next reboot after the command, the Agent generates a new UUID and saves it to a file. On consecutive reboots, the Agent will persistently use the saved UUID.

#### Common Errors from Master Image Cloning and Provisioning:

- Duplicate UUIDs** - The management sees all the Agents with the same UUID as one Agent, the last one to connect to the management. When a different endpoint with the same UUID connects, the properties (IP, user, hostname, and so on) change in the management. The impact is severe. Mitigation does not work. Other features are partial or produce unexpected results: Forensics, endpoint grouping, management commands.

#### Causes:

/VDI Switch (Agents 2.0 - 3.0)	sentinelctl agent_id (Agents 3.1+)
Physical machines with the same BIOS identifiers (machine S/N, machine key from Registry (Windows random key), virtual machine key in HyperV) User install without the /VDI switch Non-persistent live cloning (hot cloning)	User closes the master image without the <code>sentinelctl agent_id</code> command Non-persistent live cloning (hot cloning)

- Changed UUID** - The management shows the old UUID as offline and makes a new endpoint object for the new UUID. This breaks the associations and impacts mitigation and Deep Visibility.

#### Causes:

/VDI Switch (Agents 2.0 - 3.0)	sentinelctl agent_id (Agents 3.1+)
A platform identifier changed after reboot	User runs the <code>sentinelctl agent_id</code> command on an Agent that does not require it and then there is a reboot

#### To prevent duplicate UUIDs:

- Before the master image is used to clone or provision the endpoints, open the master image.
- On the master image, run:

```
sentinelctl.exe agent_id -r -b -k "<passphrase>"
```

- Close the image.

## 3.10. Upgrading a Selected List of Agents [Multi-Site]

**Management:** Central Park, Denali, Eiffel, Fuji, Grand Canyon, Houston

**Agents:** Windows 2.6+ | macOS 2.6+ | Linux 2.6+

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

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.

See also: [Uploading a Package for Agent Installation or Upgrade \[Multi-Site\] \[18\]](#).

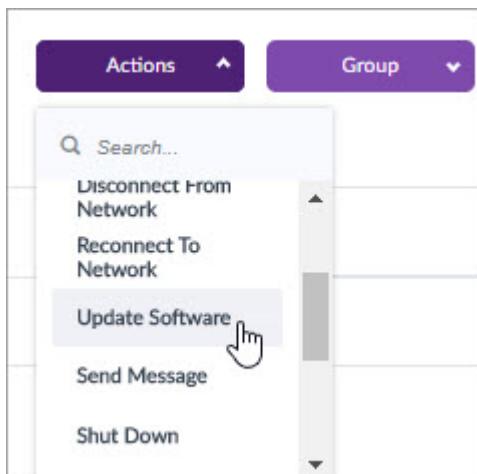
- **Best Practice:** Upgrade your SentinelOne Agents by group or filter results to the latest Agent version for each OS.
- **Priority of policy against local configuration:** When you upgrade an Agent with these steps, it gets the configuration of its policy. If you installed the Agent with CLI and switches, the installation configuration is overwritten by the policy configuration.
- **File maintenance:** When you upgrade a Windows Agent, the directories and files of the previous version (\Program Files\Sentinel One\Sentinel One Agent\version) are maintained until the next reboot.

Watch: [How to work with Installation Packages in the Management Console](#)

**Note:** Windows Agents use Background Intelligent Transfer Service (BITS) to run upgrades when the endpoint is idle, and stop upgrades when the endpoint needs network bandwidth for other activities. Therefore it can take a significant amount of time for the upgrade to complete.

### To upgrade a selected list of Agents:

1. In the sidebar, click **Scope**  and select a scope.
2. In the sidebar, click **Network** .
3. Select the Agents to update. Select a group or filter set, or select Agents manually.
4. Click **Actions**, and select **Update Software**.



5. In the **Update Software** window:
  - In **Platform**, select the OS of the Agents to update.  
If all Agents have the same OS, this is selected automatically.
  - In **Version**, select an installer file for the upgrade. The files from **Packages** show.
6. Click **Update Now**.
7. In the confirmation window, click **Update Software**.

### 3.11. Upgrading Agents From a Customized Location

**Management:** Houston

**Agents:** Windows 3.4+ | macOS 3.4+

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

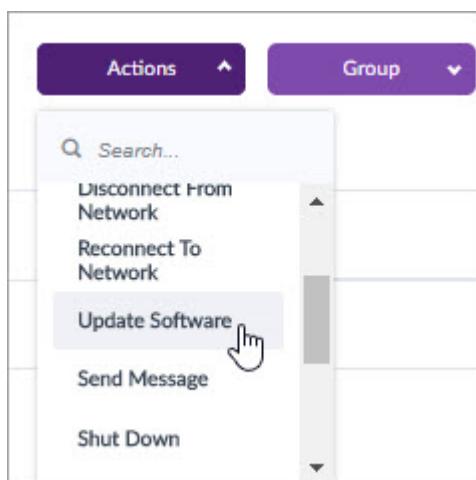
You can place an Agent upgrade package in a customized location. The Management sends a command to the Agent to upgrade itself using the upgrade package in the customized location.

The customized location must be entered as a full file path.

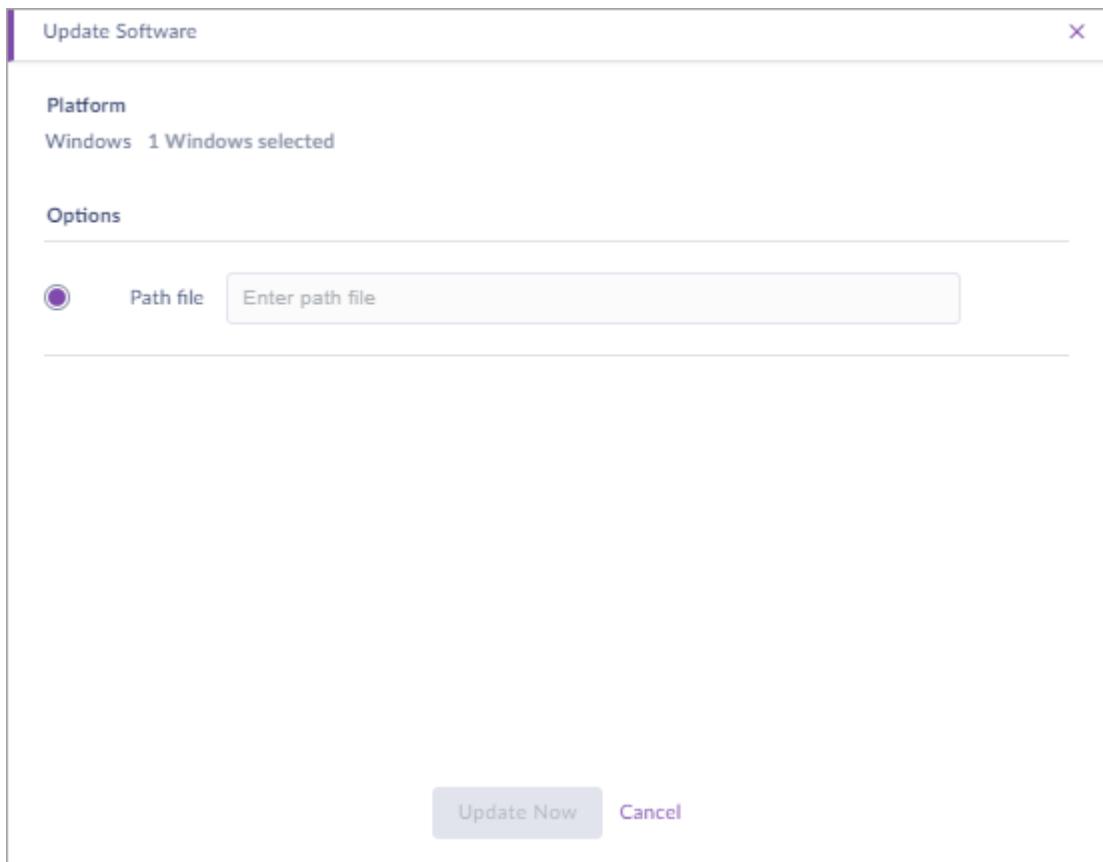
This feature is available for both Windows and macOS Agents.

#### To add a customized file path for upgrading Agents:

1. In the sidebar, click **Network** .
2. Select the Agents to update. Select a group or filter set, or select Agents manually.
3. Click **Actions**, and select **Update Software**.



4. Select **Path file** and enter the full file path.



5. Click **Update Now**.
6. In the confirmation window, click **Update Software**.

### 3.12. Upgrading the Windows Agent from an Image

**Management:** Fuji, Grand Canyon, Houston

**Agents:** Windows 3.1-3.3.2

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

**This is for specific versions only.**

**Priority of policy against local configuration:** When you upgrade an Agent with these steps, it gets the configuration of its policy. If you installed the Agent with CLI and switches, the installation configuration is overwritten by the policy configuration.

**File maintenance:** When you upgrade a Windows Agent, the directories and files of the previous version (`\Program Files\Sentinel One\Sentinel One Agent\version`) are maintained until the next reboot.

**Important! After any change or restart of the master image, before you close it:**

1. Open the Command Prompt with **Run as administrator**.

2. Go to the folder of **SentinelCtl.exe**:

```
"C:\Program Files\SentinelOne\Sentinel Agent version\"
```

3. Run:

```
sentinelctl.exe agent_id -r -b -k "<passphrase>"
```

4. Run:

```
sentinelCtl.exe agent_id -v
```

5. Make sure the output shows: **Randomize uuid on next boot: true**

If the output is not **true**, repeat the steps of this procedure.

If you do not do this, your Agents will not generate unique IDs. Every Agent must have a unique ID to function.

We give you the complete instructions for this command - when to run it and how to get the passphrase - in this document. We mention it now to emphasize the importance of this step.

#### **Recommendations for Optimal Deployment:**

- Use an image repository in your virtual environment to create protected machines from a master image.
- After you provision the endpoints, disconnect the master image from the Management.
- If possible, do not use hot cloning. If you must clone VMs while running, reboot the endpoints again before they are first used, after they are created.
- If you deploy non-persistent VMs, clean inactive Agents from the SentinelOne Management Console. In the policy of the Agents, set **Advanced > Auto decommission after \_\_ days offline** to a low number.

#### **To update the Windows Agent on the master image:**

1. Turn on the master image and make sure its Agent connects to the Management.
2. In the sidebar, click **Scope**  and select a scope.
3. In the sidebar, click **Network** .
4. Select the master image Agent.
5. Click **Actions**, and select **Update Software**.
6. In the **Update Software** window, select the installer for the upgrade.
7. Click **Update Now**.
8. In the confirmation window, click **Update Software**.
9. Run the **agent\_id** command on the master image to make sure every cloned endpoint will have an Agent with a UUID:

```
sentinelctl.exe agent_id -r -b -k "<passphrase>"
```

10. Run:

```
sentinelCtl.exe agent_id -v
```

11. Make sure the output shows: **Randomize uuid on next boot: true**

If the output is not **true**, repeat the steps of this procedure.

12. Close the image.

If you provision endpoints from the master image, the Agent is installed (not upgraded), with a new UUID. This disconnects the endpoint from the associated data (such as threat history and Deep Visibility Active EDR data). To upgrade the Agent on endpoints created from the master image, use the Management Console.

### To update Agents on child images:

1. In the sidebar, click **Scope**  and select a scope.
2. In the sidebar, click **Network** .
3. Select the Agents to update. Select a group or filter set, or select Agents manually.
4. Click **Actions**, and select **Update Software**.
5. In the **Update Software** window, select the installer for the upgrade.
6. Click **Update Now**.
7. In the confirmation window, click **Update Software**.

## 3.13. Updating Agents with SCCM

If you use 3rd-party tools, such as SCCM or Landesk (Ivanti), you can update your Windows Agents with a PowerShell script. Run the script locally on each endpoint. Make sure the Agent package is in a shared folder that the endpoint can access.

### Method:

1. The script creates a new folder on the endpoint.
2. The script copies the Agent installer from the shared folder to the new local folder.
3. The script executes the Agent installer.
4. Update runs in the background (silent installation).
5. When the update is done, the script outputs: `Install done`.

### Before running the script:

1. Modify `$Source` with the shared network folder.

2. Put the Agent installer in the Source path.
3. Modify \$Destination with a path on the endpoint.

**Script:**

```
$Source = "\\\vmware-host\Shared Folders\remotesharedir
\Agent.sentinel.local.exe"
$TimeStamp = get-date -f yyyyMMdd-hh\hmm
$Destination = "c:\Temp\SentinelOne_" + $TimeStamp

New-Item -ItemType directory -Path $Destination -Force | out-null
Write-Output "Copying SentinelOne installation to $Destination"
Copy-Item -Path $Source -Destination $Destination -Force
$SentinelOneInstallerFilename = Get-ChildItem $Destination | Select-Object
-First 1

$installProcess=Start-Process "$Destination\$SentinelOneInstallerFilename"
-ArgumentList "/Q" -Passthru
do {start-sleep -Milliseconds 500}
until ($installProcess.HasExited)
Write-Output "Install done"
```

## 3.14. Upgrading Agents - Troubleshooting

**Management:** Banff, Central Park, Denali, Eiffel, Fuji, Grand Canyon, Houston

**Agents:** Windows 2.5+ | macOS 2.5+ | Linux 2.5+

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

If the upgrade fails after the new file structure is created, and you try to uninstall the new Agent, the new directories are not deleted. This prevents a new installation with an error message.

**To fix:**

1. Go to the SentinelOne directory:
  - Windows: cd "C:\Program Files\SentinelOne"
  - See also: C:\windows\temp\sentinelinstaller\*.out and sentinelinstaller\*.dmp
  - macOS: cd /Library/Sentinel
  - Linux: cd /usr/local/sentinelagent
2. See the directories here:
  - Windows: dir
  - macOS: ls
  - Linux: ls

3. If you see multiple Agent directories, delete the directory of the failed installation:

- Windows: `del /f /q /s Sentinel*.*`
- macOS: `rmdir sentinel-agent.bundle`
- Linux: `rmdir . *.*`

#### More Logs:

- Windows Agent upgrade from the Console: **C:\windows\temp\**
- Windows Agent local upgrade: **C:\Users\user name\AppData\Local\Temp**
- Linux Agent upgrade: **/var/log/sentinelAgent**
- macOS Agent upgrade: **/Library/Logs/Sentinel** or run: `sudo sentinelctl logreport`

## 4. Managing Sites and Licenses [Multi-Site]

**Management:** Central Park, Denali, Eiffel, Fuji, Grand Canyon, Houston

**Agents:** All

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

SentinelOne lets you segment your organization in independent Sites. When you install an Agent, it is configured for a specific Site. Each Site must have enough licenses for the Agents in it.

Each Site belongs to an Account.

- All Sites in an Account must have different names.
- Sites in different Accounts can have the same name. For example, you can have a Site named IT in Account Company1, and a Site named IT in Account Company2.
- Sites can take licenses from their Account, and if a Site is deleted, its licenses go back to the Account automatically.

**To see license and basic Site information:**

- In **Network > Site Info:**



See a list of Agents, total licenses, Site expiration date, and Site creation information. Also see the Site Token and Site ID.

Austin Account: Account1000 Site ID: 655595382578875039

Creator	Created Date	Options
Agents	Complete Licenses	Expiration Date
<a href="#">See List</a>		

Site Token: eyJ1cmwiOiAiaHR0cHM6Ly9saW1vc1laWZmZWwuyXV0by5zZW50aW5ibG9uZS5sb2NhCIsICjzaXRlX2tleSi6IC40DBkNzhhMGVIZjYwNDExIn0= [Copy](#) [Share](#)

- In **Settings > Sites:**



See a full list of Sites in the environment, with SKU, total licenses and license in use, and Site creation and expiration information.

							<input type="text"/>	3 Sites	10 Results	Active
	Name	Account Name	SKU	Total Licenses	Active Agents	Created Date	Expiring Date			
<input checked="" type="checkbox"/>	Default site	Account1000	Core	Unlimited	0	Jun 24, 2019	Feb 27, 2020			
<input type="checkbox"/>	Austin	Account1000	Complete	1	0	Jun 24, 2019	Oct 31, 2019			
<input type="checkbox"/>	Philadelphia	Account1000	Complete	2	0	Jun 24, 2019	Oct 31, 2019			

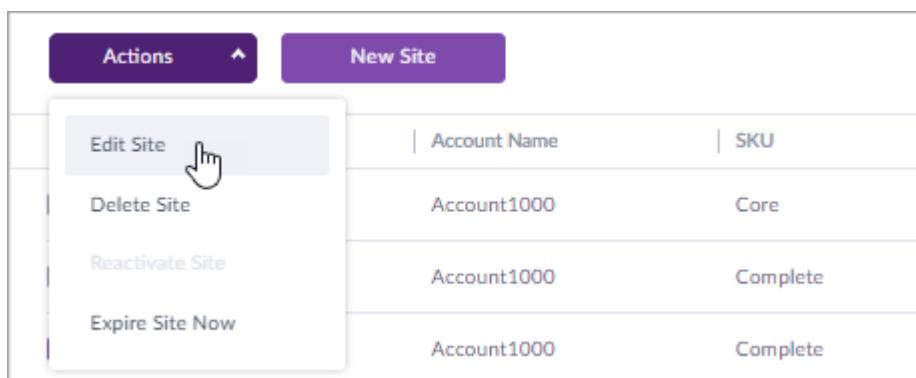
## To change license and Site information:

Account and Global Admins can change the Site name, type, and license information.

1. In the sidebar, click **Settings** .
2. In the **Settings** toolbar, click **Sites**.



3. Select a Site.
4. Click **Actions** and select **Edit Site**.



5. In the **Edit Site** window, you can change the **Site name**, upgrade the Site license from **Trial** to **Paid**, upgrade the SKU from **Core** to **Complete**, change the number of endpoint licenses, and change the Site **Expiration date**.

Site Name \*

Site Type  Trial  Paid

License Type  Core  Complete

Licenses number \*

  Unlimited licenses

Expiration Date \*

  Non-Expire

**Save** **Cancel**

- Click **Save**.

## 4.1. Creating a New Site [Multi-Site]

**Management:** Central Park, Denali, Eiffel, Fuji, Grand Canyon, Houston

**Agents:** All

**Minimum Admin Scope:** Account Admin

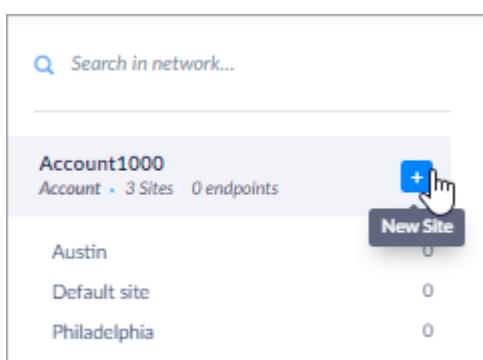
**Scope:** Account or Global

Account and Global Admins can create new Sites.

During Site creation you enter a name and license information and set the policy that the Site uses.

### To create a Site:

- From the Scope pane, stand on an Account and click **+**.



Or

In the **Settings** toolbar, click **Sites**.



Click **New Site**.

2. Enter a **Site Name**. This will be the name of the Site throughout the Management Console.

If you are not in an Account scope, select an Account from the list.

3. Click **Next**.

4. In **Site Type**:

**Site Properties**

**Site Type**  Paid  Trial

**License Type**  Core  Complete

**Licenses number \***  
100  Unlimited licenses

**Expiration Date \***  
Jun 30, 2020  Non-Expire

- Select the type of Site subscription:

- **Paid** - If you have a paid SentinelOne deployment.
- **Trial** - If you are using the Management Console as part of a trial or demo.
- **Number of licenses** - Enter the number of licenses purchased for the Site.

Each Agent automatically takes a license.

- **Expiration date** - Select the expiration date of the licenses.

5. Click **Next**.

6. In **Site Policy**, see that the new Site automatically inherits the Account or Global policy and its settings.

**i** Inherited from global default policy [Change Policy](#)

- Optional: Click **Change Policy** to make changes to the policy settings for this Site.
7. Click **Create Site**.
  8. In the Summary, see that the Site was created successfully.
  9. Optional: Click **Add Users** to add Site Admins for the new Site.
  10. Click **Done**.

## 4.2. Moving an Agent to a Different Site [Multi-Site]

**Management:** Central Park, Denali, Eiffel, Fuji, Grand Canyon, Houston

**Agents:** Windows 2.6+ | macOS 2.6+ | Linux 2.6+

**Minimum Admin Scope:** Account Admin

**Scope:** Selected Site, Account, or Global

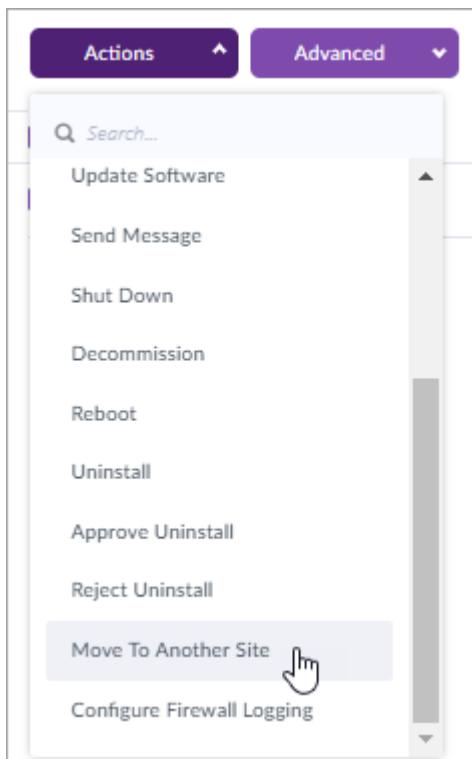
Agents are assigned to a Site when they are first installed with a Site Token.

Account and Global Admins can move Agents from one Site to a different Site. Agents go to the Default Group in the new Site.

You can select endpoints from different Sites to move.

### To move an Agent to a different Site:

1. In the sidebar, click **Scope**  and select a scope.
  2. In the sidebar, click **Network** .
- The list of endpoints in the selected scope opens.
3. Select one or more endpoints from the list.
  4. Click **Actions** and select **Move to Another Site**.



5. In the list of Sites that opens, select the new Site for the Agents.
6. Click **Move Agents**.
7. Select **Action Approved** and click **Move Agents**.

### 4.3. Deleting a Site [Multi-Site]

**Management:** Denali, Eiffel, Fuji, Grand Canyon, Houston

**Agents:** Windows 2.6+ | macOS 2.6+ | Linux 2.6

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

You can delete a Site that does not contain Agents.

A Site Admin can delete a Site from the Site Info or the Sites page if there are one or more other Sites in the Account.

If you delete a Site, its licenses move to the oldest Site in the Account.

#### To delete a Site from the Sites page:

1. In the sidebar, click **Settings** .
2. In the **Settings** toolbar, click **Sites**.



3. Select the Site to delete.
4. Click **Actions** and select **Delete Site**.  
If the Site contains Agents, the Delete option is not available.
5. In the warning message that opens, click **DELETE**.

### To delete a Site from the Site Info page:

1. In the sidebar, click **Scope**  and select a scope.

You must select a Site.

2. In the sidebar, click **Network** .
3. In the **Network** toolbar, click **Site Info**.



4. Click **Options** and select **Delete Site**.
5. In the warning message that opens, click **DELETE**.

## 4.4. Managing Accounts [Multi-Site]

**Management:** Grand Canyon, Houston

**Agents:** Windows 2.9+ | macOS 3.0+ | Linux 2.6+

**Minimum Admin Scope:** Account Admin

**Scope:** Account or Global

Accounts are created by a Global Admin or by SentinelOne.

Each Account contains Sites. Sites can inherit assets and settings from their Account.

Each Account has one or more SKUs set by SentinelOne. You can create Sites with an SKU that their Account has. To have both Core and Complete Sites in an Account, the Account must have both SKUs. If an Account has the Complete SKU, and you create a new Site in the Account, it will automatically have the Complete SKU.

### To see the details of an Account:

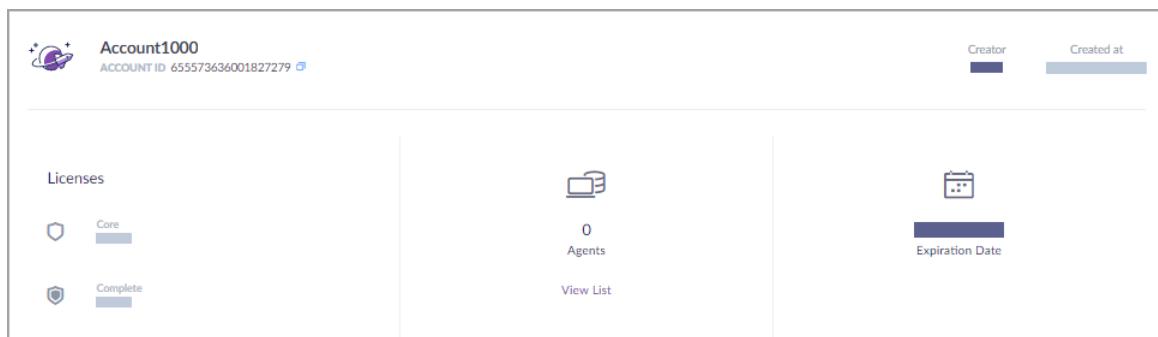
1. In the sidebar, click **Scope**  and select a scope.

You must be in one Account.

2. In the sidebar, click **Network** .
3. In the **Network** toolbar, click **Account Info**.



- See a summary of the Account: creation and expiration dates, licenses, Agents, and the Account ID.



## To see a summary of Accounts in your scope:

- In the sidebar, click **Settings**
- In the **Settings** toolbar, click **Accounts**.



- See a summary of the Sites, licenses, and Agents in each Account.

Account Name	Number Of Sites	Agents In Core SKU	Agents In Complete SKU	Active Agents	Created Date And Time

Click an Account to open its list of endpoints.

## 5. Managing Agents [Multi-Site]

**Management:** Central Park, Denali, Eiffel, Fuji, Grand Canyon, Houston

**Agents:** Windows 2.6+ | macOS 2.6+ | Linux 2.6+

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

When you install an Agent on an endpoint, the endpoint becomes part of the SentinelOne solution. You can manage the endpoint through its Agent with one-click commands on the Management Console.

See:

[Rebooting an Endpoint from the Console \[Multi-Site\] \[71\]](#)

[Shutting Down an Endpoint from the Console \[Multi-Site\] \[73\]](#)

[Removing an Agent from the Console - Decommission \[Multi-Site\] \[74\]](#)

[Getting Logs for Support](#)

[Running Full Disk Scan](#)

[Disconnecting Endpoints from the Network \(and reconnecting\)](#)

[Moving an Agent to a Different Site](#)

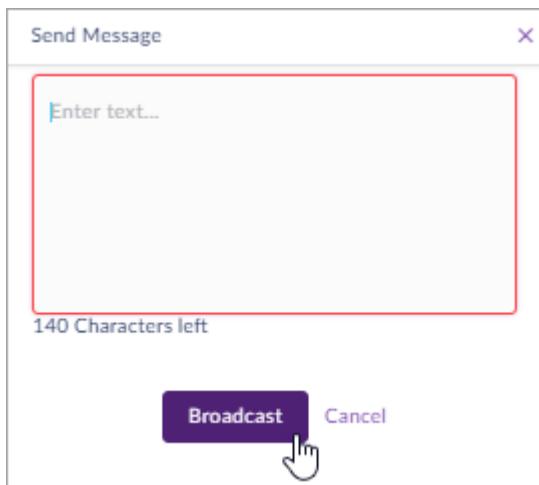
**Best practice:** If the endpoint is a user computer, let the user know you will remotely run commands on the computer.

**To send a message to users through the Management Console:**

1. In the sidebar, click **Network** .

The list of endpoints in the selected scope opens.

2. Select one or more endpoints.
3. Click **Actions** and then select **Send Message**.
4. In the window that opens, enter your message and then click **Broadcast**.



5. In the confirmation window, click **Broadcast** again.

## 5.1. Windows Agent Event Logs

**Management:** Houston

**Agents:** Windows 3.4+

From Windows Agent version 3.4, [SentinelOne Agent logs](#) are available in Windows Event Viewer on endpoints. These logs show you the SentinelOne activities that occur on the endpoint, especially when endpoints are offline, and help you troubleshoot issues. You can also use the logs to integrate with SIEM or other third-party solutions.

By default, the logs are available for all endpoints.

To use the logs for troubleshooting see [Using the Windows Event Viewer Logs \[60\]](#).

### To see the logs:

1. On an endpoint with a supported SentinelOne Agent, open Event Viewer.
2. In Event Viewer (Local), click **Applications and Services Logs > SentinelOne > Operational**.

Operational Number of events: 3

Level	Date and Time	Source	Event ID	Task Category
Information	29/07/2019 19:06:34	SentinelOne	3	Critical
Information	29/07/2019 19:06:34	SentinelOne	2	Critical
Information	29/07/2019 19:06:29	SentinelOne	1	Critical

Policy was changed in the Console:

```
{"agentLogging":true,"antiTampering":true,"automaticResponses":[{"mitigation.quarantineThreat"}],"collectDv":true,"deepVisibility":{"dns":{"operation":true},"file": {"creation":true,"deletion":true,"modification":true,"rename":true}, "http":{"operation":true}, "persistence":{"operation":true}, "process":{"creation":true,"exit":true,"termination":true}, "registry": {"keyCreated":true,"keyDelete":true,"keyExport":true,"keyImport":true,"keyRename":true}, "keySecurityChanged":true, "valueCreated":true, "valueDelete":true, "valueModified":true}, "scheduledTask": {"del":true,"reg":true}, "start":true, "trigger":true, "update":true}, "tcpv4": {"incoming":true,"listen":true,"outgoing":true}, "user":{"loggedin":true,"loggedout":true}}, "deviceControl": {"disableRPM":false,"enabled":true,"notifyUI":true,"report":["blocked"]}, "enginesWantedState": {"dataFiles": "local", "executables": "local", "exploits": "local", "fileLess": "local"}, "lateralMovement": "local", "penetration": "suppressed", "preExecution": "local", "preExecutionSuspicious": "local", "reputation": "local"}, "firewallControl": {"enabled":true,"locationAware":false,"notifyUI":false,"report":["blockedTraffic"]}, "keepAliveFailCount": 8, "keepAliveInterval": 30, "locationAwareness": [{"enabled":true,"reportLocations":true}, "maxNotificationSize": 10485760, "monitorBehavioralEvents": true, "onValidate": "reportToMgmt", "policyID": "", "processListRate": 10000, "remoteShell": [{"enabled":true,"pingIntervalSec":120,"pingRetry":3}, "researchCollect": true, "researchUpload": true, "scanModifiedFiles": true, "sendApplicationInventory": true, "sendHashesOfModifiedFiles": true, "sendRapidLogging": false, "sendThreatLogs": true, "showAgentUI": true, "vssSnapshots": true}]}
```

Log Name: SentinelOne/Operational  
 Source: SentinelOne Logged: 29/07/2019 19:06:34  
 Event ID: 2 Task Category: Critical  
 Level: Information Keywords:  
 User: SYSTEM Computer: [REDACTED]  
 OpCode: Info  
 More Information: [Event Log Online Help](#)

## Understanding the Logs

No.	Item	Description
1	Level	<b>Information</b> - Informative notification. No action is necessary. For example, the Agent's policy was changed. <b>Warning</b> - An event occurred that requires attention. Follow your organizational procedures. For example, malware was detected. <b>Error</b> - Something went wrong in the Agent operations. For example, the Agent could not connect to the management. Troubleshoot to resolve.
2	Date and Time	The date and time that the event occurred, synchronized with the endpoint time
3	Event ID	Unique ID per event. See the full list.
4	Task Category	For all SentinelOne logs, the Task Category shows <b>Critical</b> . DO NOT use this to decide the urgency of the event.
5	General tab	Shows a description of the event and the related data. Does not include sensitive data.
6	Details tab	Choose to show the event details in a structured view: <b>Friendly View</b> or <b>XML View</b> .

## Understanding the logs:

1. Look at the **Level** to see the type of event and if action is required.
2. Read the details in the **General** and **Details** tabs to understand the event.
3. If necessary, search for the **Event ID** here to see which actions are recommended.

## Log configuration:

- Use Policy override or the Agent configuration file to enable or disable logs and change the maximum log size.

- Except for the parameters listed below, all Event Viewer Management is controlled by your organization's administrators. All changes to Event Viewer configuration can affect the SentinelOne channel.

## Endpoint Log Parameters in SentinelOne Agent Configuration

Parameter	Description	Values
Agent.eventLog.customer	Set if Agent event logs are enabled or disabled	True - Logs are enabled False - Logs are disabled
Agent.eventLog.maxSizeMB	Maximum log size allowed. By default, when the maximum size is reached, the oldest logs are deleted. IT Admins can change this in the WEV configuration.	Default - 1024 MB (integer value) Min value 1MB. Max value 18014398509481 MB (max value of WEV64 bit limit)

### More technical details:

- The evtx file that created is in: %SystemRoot%\System32\Winevt\Logs\SentinelOne %4Operational.evtx

**Limitation:** The evtx file is not protected by SentinelOne Anti-Tampering.

- The SentinelOne **Operational** channel in Windows Event Viewer configuration can be changed from the channel properties in WEV or by sentinelctl config. The configuration in the channel properties is always updated.
  - If configuration is changed from the channel properties in WEV, the agent parameters in sentinelctl are not updated.
  - If configuration is changed from sentinelctl config, the configuration in the channel properties is updated.

### 5.1.1. Using the Windows Event Viewer Logs

**Management:** Houston

**Agents:** Windows 3.4+

See [Windows Agent Event Logs \[58\]](#) for more information on understanding and configuring logs.

#### To use this article :

- Get the Event ID of a log from Event Viewer (Local) > **Applications and Services Logs** > **SentinelOne** > **Operational**.
- Search this article for the Event ID.
- Follow the instructions in the **Next Steps** column to troubleshoot the issue.
- If the steps shown do not help you resolve the issue, contact SentinelOne Support.

For users with a login: [support.sentinelone.com](mailto:support.sentinelone.com)

To send an email: <[support@sentinelone.com](mailto:support@sentinelone.com)>

## Windows Events

Details	Event	Example message	Next Steps
ID: 1 Information v3.4+	Agent started	Windows Agent is starting in full mode. Agent version 3.x.x.x running on Windows 10.x.x.x.	None
ID: 2 Information v3.4+	Report policy change Needs to exclude engine status	Policy was changed in the Console: {"agentLogging":true,"antiTampering":true, ...}	None. Policy was changed successfully.
ID: 3 Information v3.4+	Override config change with the change	Policy was changed with override commands: {...}	None. Policy was changed successfully.
ID: 4 Error v3.4+	Error in registration with reason and without retry	Failed to register with management because it no longer exists. Not retrying.	1. Make sure you can log in to the Management Console. 2. Make sure the Site exists. If not, ask your SentinelOne contact.
ID: 5 Error v3.4+	Error in registration with reason and with possible action (retry timeout)	Failed to register with management: The server name or address could not be resolved (12007). Retrying in 30 seconds.	1. If the reason is Invalid CA certificate, check the <a href="#">CA certificate</a> on the local machine. 2. Make sure you can log in to the Management Console. 3. Make sure the Agent can connect to the Management through port 443.
ID: 6 Warning v3.4+	Remediation - failed to delete file - already deleted	Threat remediation: Failed to delete file C:\temp\test.txt because it was already deleted.	1. Make sure that the file does not exist in the given location. 2. Make sure that the System User account has permissions for the threat root folder.
ID: 7 Error v3.4+	Remediation - failed to delete file - windows error	Threat remediation: Failed to delete file C:\temp\test.txt. Error: The system cannot find the path specified.	Make sure that the destination path is not removable media or a network path, which are not supported.
ID: 8 Error v3.4+	Remediation - failed to rename file - file was deleted	Threat remediation: Failed to rename file C:\temp\test.txt to C:\temp\abc.doc because the file was deleted.	1. Make sure that the file does not exist in the given location. 2. Make sure that the System User account has permissions for the threat root folder.
ID: 9 Error v3.4+	Remediation - failed to rename file - parent directory doesn't exist	Threat remediation: Failed to rename file C:\temp\test.txt to C:\temp\abc.doc because the file's parent directory does not exist.	1. Make sure that the file does not exist in the given location. 2. Make sure that the System User account has permissions for the threat root folder.

Details	Event	Example message	Next Steps
ID: 10 Error v3.4+	Remediation - failed to rename file - destination path already exists	Threat remediation: Failed to rename file C:\temp\test.txt to C:\temp\abc.doc because the destination path already exists.	Make sure that the root file does not exist in the original location.
ID: 11 Error v3.4+	Remediation - failed to rename file - windows error	Threat remediation: Failed to rename file C:\temp\test.txt to C:\temp\abc.doc. Error: The process cannot access the file because another process has locked a portion of the file.	1. Reboot the machine. 2. Run another quarantine command from the Management Console.
ID: 12 Error v3.4+	Remediation - failed to restore file - no snapshots	Threat remediation: Failed to restore file C:\temp\test.txt to timestamp [time] because no snapshots were found up to the desired period.	Contact SentinelOne Support
ID: 13 Error v3.4+	Remediation - failed to restore file - file is being used by another process	Threat remediation: Failed to restore file C:\temp\test.txt to timestamp [time] because it is being used by another process.	1. Reboot the machine. 2. Run another quarantine command from the Management Console.
ID: 14 Error v3.4+	Remediation - failed to restore file - access denied	Threat remediation: Failed to restore file C:\temp\test.txt to timestamp [time] because access was denied.	Contact SentinelOne Support
ID: 15 Error v3.4+	Remediation - failed to restore registry value - doesn't exist	Threat remediation: Failed to restore registry value (key: HKLM\System\..., value: 5) because it does not exist.	Contact SentinelOne Support
ID: 16 Error v3.4+	Mitigation - group doesn't exist	Threat mitigation: Failed to kill malicious processes because the true context does not exist.	Make sure that the root process is not running.
ID: 17 Error v3.4+	Mitigation - another reboot	Threat mitigation completion after reboot requested another reboot. True Context ID: abc123, Mitigation action: Kill	A Core process is involved. Please reboot the machine.
ID: 18 Warning v3.4+	Mitigation - not killing process due to relation	Threat mitigation: Not killing process Notepad (Path: C:\Windows\System32\notepad.exe, Process ID: 1234) due to relation RelationInjected.	Contact SentinelOne Support
ID: 19 Error v3.4+	Mitigation - can't kill OS process	Threat mitigation: Cannot kill process Notepad (Path: C:\Windows\System32\notepad.exe, Process ID: 1234) because it is a core OS process.	A Core process is involved. Please reboot the machine.

Details	Event	Example message	Next Steps
ID: 20 Error v3.4+	Mitigation - not killing sentinel process	Threat mitigation: Cannot kill process Notepad (Path: C:\Windows\System32\notepad.exe, Process ID: 1234) because it is signed by SentinelOne.	Contact SentinelOne Support
ID: 21 Error v3.4+	Mitigation - failed to kill process	Threat mitigation: Cannot kill process Notepad (Path: C:\Windows\System32\notepad.exe, Process ID: 1234) due to an unknown error.	Contact SentinelOne Support
ID: 22 Error v3.4+	Mitigation - failed to kill threads	Threat mitigation: Cannot kill threads of process Notepad (Path: C:\Windows\System32\notepad.exe, Process ID: 1234) due to an unknown error.	Contact SentinelOne Support
ID: 23 Error v3.4+	Mitigation - failed to quarantine file - file is remote	Threat mitigation: Failed to quarantine file C:\temp\test.txt because the file is remote.	Mitigation is not supported for removable media or network paths.
ID: 24 Error v3.4+	Mitigation - failed to quarantine file - core OS process	Threat mitigation: Failed to quarantine file C:\temp\test.txt because the file belongs to a core OS process.	A Core process cannot be quarantined.
ID: 25 Error v3.4+	Mitigation - failed to scramble file - exception	Threat mitigation: Failed to scramble file C:\temp\test.txt. Error: Access is denied.	Make sure that the System User account has permissions for the threat root folder.
ID: 26 Warning v3.4+	Mitigation - failed to quarantine file - already quarantined	Threat mitigation: skipping quarantine of file C:\temp\test.txt because the file was already quarantined by another threat mitigation.	Make sure that root content does not exist in the original location.
ID: 27 Error v3.4+	Mitigation - failed to quarantine file - doesn't exist	Threat mitigation: Failed to quarantine file C:\temp\test.txt because the file does not exist.	Make sure that root content does not exist in the original location.
ID: 29 Error v3.4+	Mitigation - failed to quarantine file - exception	Threat mitigation: Failed to quarantine a file. Error: Access is denied.	Make sure that root content does not exist in the original location.
ID: 30 Error v3.4+	Mitigation - network quarantine - exception	Network quarantine failed. Error: Access is denied.	Make sure that root content does not exist in the original location.

Details	Event	Example message	Next Steps
ID: 31 Warning v3.4+	Report threat with root, group ID, engine, indicators, without logic	Malware detected! True Context ID: blabla1234 Root process name: Chrome Root process path: C:\Program Files (x86)\Google\Chrome\Application\chrome.exe Detection engine: Reputation	Malware detected. Follow your organizational procedures.
ID: 32 Warning v3.4+	Mitigation report for all mitigations.	Mitigation report True Context ID: xyz1234 Action: Remediate Result: Success	None
ID: 33 Error v3.4+	Unquarantine failure - file not found	Failed to unquarantine file C:\temp\test.txt because the file cannot be found.	Contact SentinelOne Support
ID: 34 Error v3.4+	Unquarantine failure - error restoring file times	Unquarantine: Failed to restore file times for [file path]. Error: [error]	Contact SentinelOne Support
ID: 35 Error v3.4+	Unquarantine failure - exception	Failed to unquarantine files affected by threat of True Context ID abcd1234. Error: [error]	Contact SentinelOne Support
ID: 36 Error v3.4+	Network unquarantine failure	Network unquarantine failed. Error: [error]	Contact SentinelOne Support
ID: 37 Error v3.4+	Local config change error - no passphrase	Policy not changed. Verification key not provided. Get the Agent passphrase and enter it with the -k flag.	Passphrase is missing from the command. See <a href="#">Sentinelctl on Windows Agents</a> .
ID: 38 Error v3.4+	Local config change error - wrong passphrase	Policy not changed. The provided verification key is incorrect.	1. Make sure that the passphrase in the command is correct. 2. See <a href="#">Sentinelctl on Windows Agents</a> .
ID: 39 Error v3.4+	Local config change error - can't set and undefine	Policy not changed. A parameter cannot be both set and undefined.	Make sure that all parameters are defined and none are missing.
ID: 40 Error v3.4+	Local config change error - no parameter	Policy not changed. Parameter was not provided.	Make sure that all parameters are defined and none are missing.
ID: 41 Error v3.4+	Local config change error - invalid URL	Policy not changed. The value acbd is not valid for server.mgmtServer: invalid URL.	A Value is not valid. Make sure that values are set correctly.
ID: 42 Error v3.4+	Local config change error - trailing slash in URL	Policy not changed. The value abcd/ is not valid. Remove the slash from the end of the URL.	Remove the slash from the end of the URL.

Details	Event	Example message	Next Steps
ID: 43 Error v3.4+	Local config change error - invalid proxy credentials	Policy not changed. The provided proxy credentials are invalid.	Check your <a href="#">proxy settings</a> .
ID: 44 Error v3.4+	Local config change error - failed to write value for UI language - windows error	Policy not changed. Failed to write value system for UI Language. Error: Access is denied.	Contact SentinelOne Support
ID: 45 Error v3.4+	Local config change error - invalid UI config property	Policy not changed. Invalid UI configuration property ui.bla.	Contact SentinelOne Support
ID: 46 Error v3.4+	Local config change error - invalid engine status	Policy not changed. Invalid engine status abcd123. Engine status must be one of: "off", "suppressed", "disable", "local".	Change the "Engine status" in the policy configuration. Engine status must be one of: "off", "suppressed", "disable", "local".
ID: 47 Error v3.4+	Local config change error - invalid parameter	Policy not changed. Invalid parameter hello.world: Key not found.	Make sure that the parameter shown is set correctly
ID: 48 Error v3.4+	Local config change error - invalid config	Policy not changed. Error: Value is not an integer. Parameter: agent.keepAliveInterval Invalid given value: true	Value must be an integer.
ID: 49 Error v3.4+	Local config change error - cannot undefine	Policy not changed. Cannot undefine parameter server.mgmtServer.	Make sure that the parameter shown is correct.

## 5.2. Uninstalling Agents from the Management Console [Multi-Site]

**Management:** Central Park, Denali, Eiffel, Fuji, Grand Canyon, Houston

**Agents:** Windows 2.6+ | macOS 2.6+ | Linux 2.6+

**Minimum Admin Scope:** Site Admin

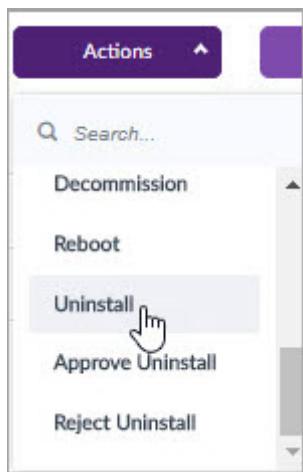
**Scope:** Selected Site, Account, or Global

You can uninstall Agents from the Management Console.

From the Management Console, you can select one or more endpoints for the action, or you can select all of a Group or filter set. You cannot select all endpoints shown if they are not in a Group or filter set.

## To uninstall Agents from the Management Console:

1. In the sidebar, click **Scope**  and select a scope.
  2. In the sidebar, click **Network** .
- The list of endpoints in the selected scope opens.
3. Select one endpoint OR all endpoints in a Group or filter set.
  4. Click **Actions > Uninstall**.



5. In the confirmation window that opens, select **Action approved** and click **Uninstall**.
6. To make sure that all remnants of the Agent are removed, [reboot the endpoints \[71\]](#) after Agent uninstallation.

### 5.3. Uninstalling Agents from the CLI

**Management:** Alhambra, Bahamas, Banff, Central Park, Denali, Eiffel, Fuji, Grand Canyon, Houston

**Agents:** Windows 2.0 +| macOS 2.0+ | Linux 2.0+

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

For Windows and macOS Agents, if Anti-Tampering is enabled, a [passphrase](#) is required to uninstall an Agent from the CLI.

To make sure that all remnants of the Agent are removed, [reboot the endpoints \[71\]](#) after Agent uninstallation.

#### To uninstall a local macOS Agent with CLI:

- Use the key in a terminal app to unprotect and then uninstall the Agent:

```
$ sudo sentinelctl unprotect --passphrase "passphrase"
```

```
==Sentinel protection has been disabled
$ sudo sentinelctl uninstall --local
```

## To uninstall the Linux Agent version 3.x with the sentinelctl CLI:

1. Save or copy the passphrase.
2. Log in to the endpoint as a privileged user and run:

```
sudo /opt/sentinelone/bin/sentinelctl control uninstall --passphrase
"string"
```

## To uninstall a local Linux Agent version 2.6 with CLI:

- Local Linux Agent on AMI, CentOS, OEL, or RHEL:

```
$ sudo rpm -e sentinelagent
```

- Local Linux Agent on Ubuntu:

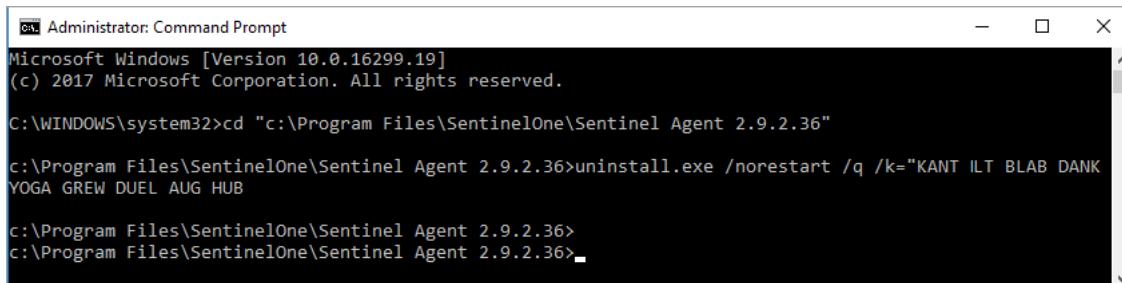
```
$ dpkg -r sentinelagent
```

## To uninstall a Windows Agent silently with CLI:

- **Uninstall with permissions:** From the Windows cmd, run:

```
> cd "C:\Program Files\SentinelOne\Sentinel Agent <version>"
> uninstall.exe /norestart /q /k=""
```

On success, there is no output. When uninstallation is done, the prompt shows. After a few seconds, the taskbar icon is removed.



## To send an Windows Agent uninstall request to an Admin:

- **Send uninstall request to administrator:** From the Windows cmd, run:

```
> cd "C:\Program Files\SentinelOne\Sentinel Agent <version>"
> uninstall.exe /norestart /q
```

On success, the output is:

> Error: You are not authorized to perform this operation. A notification was sent to the system administrator. Please contact your system administrator for details.

An uninstall request is sent to the Management Console.



## 5.4. Getting a Passphrase

**Management:** Banff, Central Park, Denali, Eiffel, Fuji, Grand Canyon, Houston

**Agents:** Windows 2.0+ | Legacy 1.8.4+ | macOS 2.0+ | Linux 2.0+

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

Some Agent features, such as CLI uninstall, require a passphrase (also known as a verification key).

**To get the passphrase for an endpoint from the Management Console:**

1. In the Management Console, click **Network**.
2. In the **Network** view, search for the endpoint.
3. Click the endpoint to open its details.
4. In the Details window, click **Actions** and select **Show passphrase**.

ENDPOINT DETAILS  
Desktop

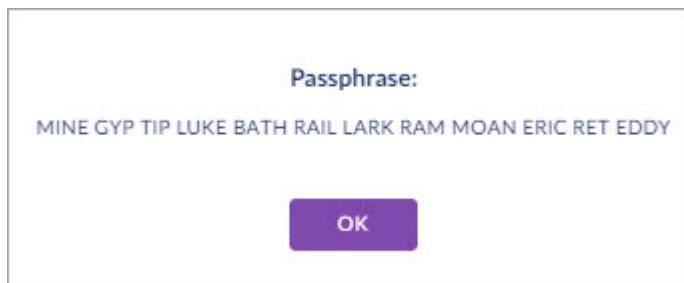
**GENERAL APP INVENTORY**

	Windows 10 (64 bit) Last active Last 4 minutes Site name gertner	Health status Last logged in u... Group name
Agent version	3.1.1.12 UPDATED	Console connected
Scan status	N/A	Network status
Memory	7.87 GB	Domain
CPU	4 X Intel(R) Core(TM) i5-...	Subscribed on
Core count	4	Console visible
Disk encryption	Off	IP Address
UUID	28558f791e58a840e25...	
<b>Network Adapters:</b>		
NAME	IP	MAC ADD

**Actions**

- Search...
- Remote Shell
- Search on Deep Visibility
- Send Message
- Show Applications
- Show Passphrase**
- Shut Down
- Uninstall
- Update Software
- View threats

- The Passphrase opens in a new window. Copy it to a file to use as needed.



## 5.5. Uninstall Requests [Multi-Site]

**Management:** Central Park, Denali, Eiffel, Fuji, Grand Canyon, Houston

**Agents:** Windows 2.6+ | macOS 2.6+ | Linux 2.6+

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

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 in the Management Console. After you approve a request, users see a message that the request was approved. They can restart to complete the Agent uninstallation.

We recommend that you do not approve these requests until:

- You understand the reason for the request
- You agree with the request
- You have alternative security for the endpoint until you install the Agent again

### To approve an uninstall request:

1. In the sidebar, click **Network** .

The list of endpoints in the selected scope opens.

2. Click **Select Filters**.
3. Click **Pending Uninstall > Yes**.

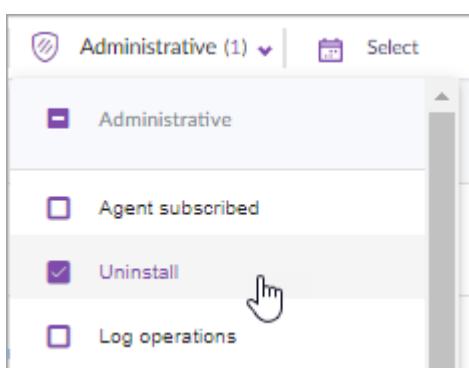
Scroll horizontally to see this filter.

Disk encryption	Pending uninstall	Architecture
Off	No 82508	64 bit
On	Yes 1352	32 bit

4. Select the endpoints to uninstall.
5. Click **Actions > Approve Uninstall**.
6. A confirmation message shows. Click **Approve**.

### To see uninstallation requests and activity:

1. In the sidebar, click **Activity** .
2. In **Activity Filters**, click **Administrative > Uninstall** to see all uninstallation activity and requests.



## How Windows users send an uninstall request:

1. Select Control Panel > Add or Remove Programs > **SentinelOne Agent**.
2. Click **Uninstall**.
3. In the window that opens, select **Online**, if the Agent is connected to the Management, or **Offline**, if it is not connected.
4. Click **Uninstall**.

If the Agent was online, the request is sent to the Management Console. If the request is approved, the user sees a window that asks for confirmation to uninstall the Agent. If the user clicks **Yes**, the Agent is removed (reboot required).

If the Agent was offline, the user must enter the **Verification Key** (passphrase) in the Uninstall window.

## To get the passphrase for offline Agent uninstallation:

1. In the **Endpoint Details** window of the endpoint, click **Actions > Show Passphrase**.

The screenshot shows the 'Endpoint Details' window for a 'Desktop' endpoint. The 'GENERAL' tab is selected. On the right, a purple 'Actions' button is open, displaying a list of options. The 'Show Passphrase' option is highlighted with a mouse cursor icon pointing at it. Other visible options include 'Remote Shell', 'Search on Deep Visibility', 'Send Message', 'Show Applications', 'Shut Down', 'Uninstall', 'Update Software', and 'View threats'.

GENERAL			APP INVENTORY		
	Windows 10 (64 bit) Last active Last 4 minutes Site name gertner	Health status Last logged in u: Group name			
Agent version	3.1.1.12 UPDATED	Console connec			
Scan status	N/A	Network status			
Memory	7.87 GB	Domain			
CPU	4 X Intel(R) Core(TM) i5-...	Subscribed on			
Core count	4	Console visible			
Disk encryption	Off	IP Address			
UUID	28558f791e58a840e25...				
Network Adapters:					
NAME	IP	MAC ADD			

2. Copy the output and give it to the user.

## 5.6. Rebooting an Endpoint from the Console [Multi-Site]

**Management:** Central Park, Denali, Eiffel, Fuji, Grand Canyon, Houston

**Agents:** Windows 2.6+ | macOS 2.6+ | Linux 2.6+

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

You can reboot endpoints from the Management Console. This is often required for performance or maintenance reasons.

#### Notes:

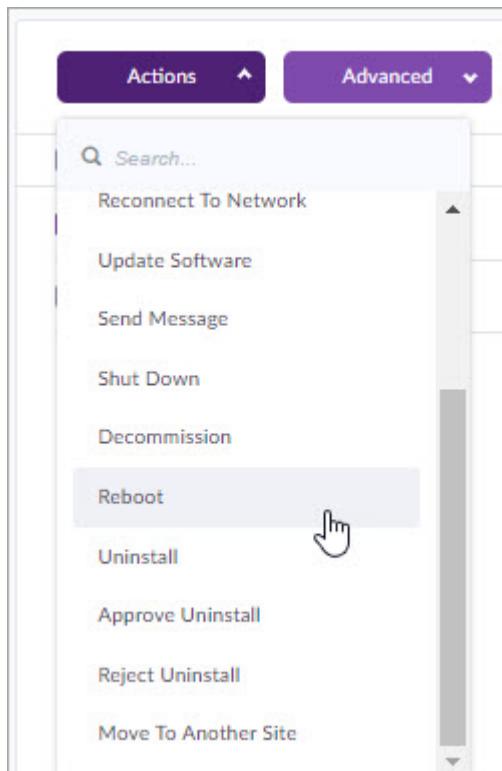
If the endpoint is offline, this option is not available.

There is no notification to the users. Data will be lost. **Best:** Send a message to the users through the console before you run the action.

From the Management Console, you can select one or more endpoints for the action, or you can select all of a Group or filter set. You cannot select all endpoints shown if they are not in a Group or filter set.

#### To restart an endpoint from the Management Console:

1. In the sidebar, click **Scope**  and select a scope.
  2. In the sidebar, click **Network** .
- The list of endpoints in the selected scope opens.
3. Select one endpoint OR all endpoints in a Group or filter set.
  4. Click **Actions > Reboot**.



5. In the confirmation window that opens, select **Action approved**. Click **Reboot**.

## 5.7. Shutting Down an Endpoint from the Console [Multi-Site]

**Management:** Central Park, Denali, Eiffel, Fuji, Grand Canyon, Houston

**Agents:** Windows 2.6+ | macOS 2.6+ | Linux 2.6+

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

You can shut down an endpoint remotely for performance, maintenance, or security reasons.

**Best Practice:** If an endpoint is infected, we recommend **Disconnect from Network** and not **Shutdown**. The Disconnect command secures the environment from infection while you analyze the cause and best response.

### Notes:

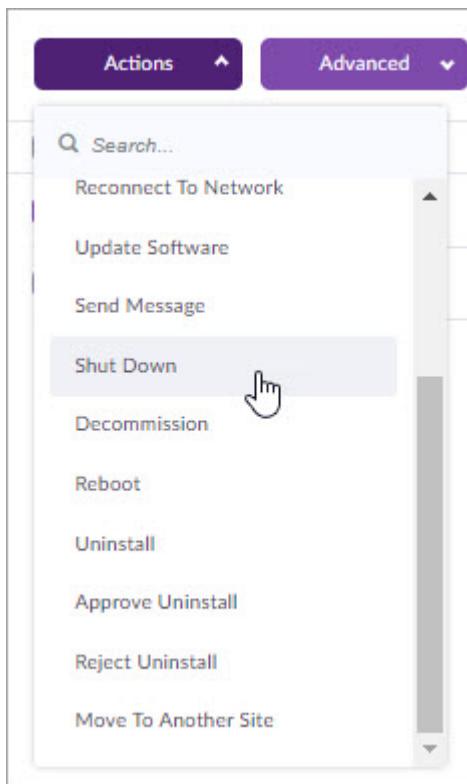
If the endpoint is offline, this option is not available.

There is no notification to the users. Data will be lost. **Best:** Send a message to the users through the console before you run the action.

From the Management Console, you can select one or more endpoints for the action, or you can select all of a Group or filter set. You cannot select all endpoints shown if they are not in a Group or filter set.

### To shut down an endpoint from the Management Console:

1. In the sidebar, click **Scope**  and select a scope.
  2. In the sidebar, click **Network** .
- The list of endpoints in the selected scope opens.
3. Select one endpoint OR all endpoints in a Group or filter set.
  4. Click **Actions > Shut Down**.



5. In the confirmation window that opens, select **Action approved**. Click **Shut down**.

You can also shut down one endpoint from the **Endpoint Details** window > **Actions** > **Shut Down**.

## 5.8. Removing an Agent from the Console - Decommission [Multi-Site]

**Management:** Central Park, Denali, Eiffel, Fuji, Grand Canyon, Houston

**Agents:** Windows 2.6+ | macOS 2.6+ | Linux 2.6+

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

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 Management Console.

From the Management Console, you can select one or more endpoints for the action, or you can select all of a Group or filter set. You cannot select all endpoints shown if they are not in a Group or filter set.

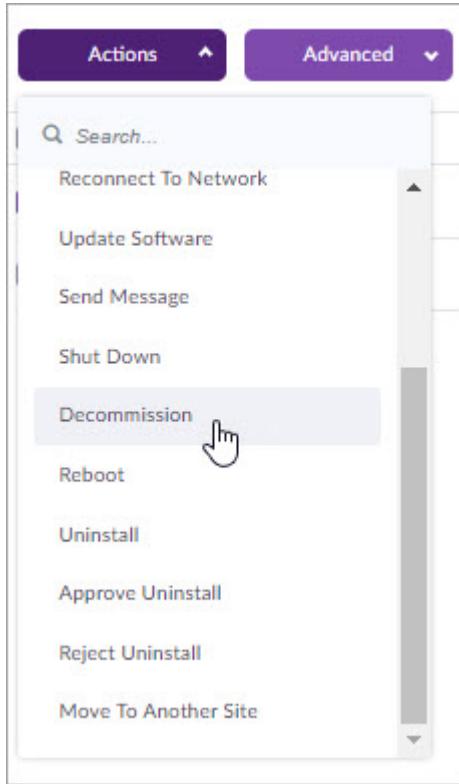
### To decommission an Agent:

1. In the sidebar, click **Scope**  and select a scope.

2. In the sidebar, click **Network** .

The list of endpoints in the selected scope opens.

3. Select one endpoint OR all endpoints in a Group or filter set.
4. Click **Actions > Decommission**.



5. In the confirmation window that opens, select **Action approved**. Click **Decommission**.

You can set endpoints for automatic decommission. In the policy, set a limit for the number of days an endpoint can be disconnected from the Management Console. When an endpoint reaches this limit, its policy removes the endpoint from the console. You can clear the console of disconnected endpoints, without uninstalling the Agent. When the Agent comes back online, it is recommissioned.

If you deploy non-persistent VMs, clean inactive Agents from the SentinelOne Management Console.

**Important:** If you set the **Auto Decommission** number of days to be too small, the number of endpoints with Agents and the number of endpoints you see on the Management Console can be significantly different and confusing. If you deploy virtual machines, set the number of days to fit your environment and policy for persistency.

### To set automatic decommission:

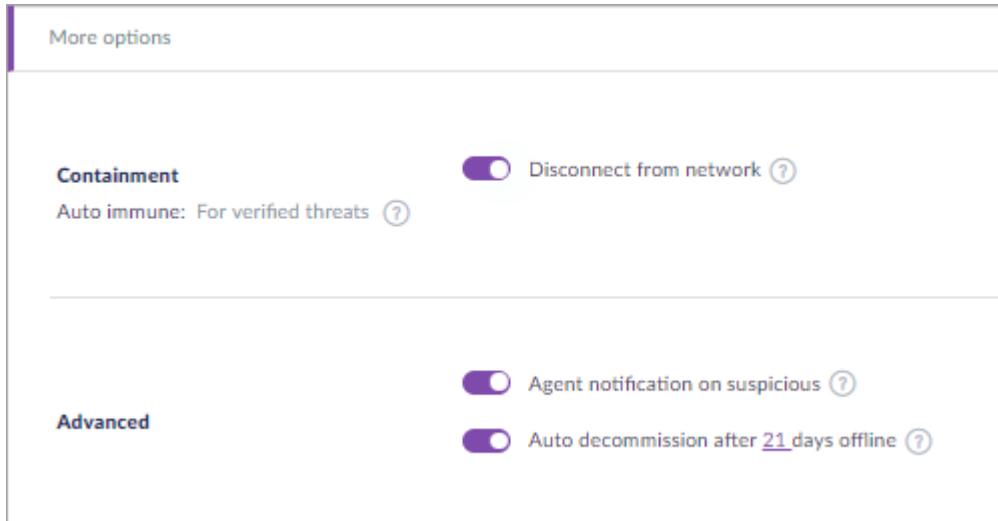
1. In the sidebar, click **Scope**  and select a scope.
2. In the **Network** toolbar, click **Policy**.



3. If the policy is not inherited, you can edit the settings. If the policy is inherited, click **Change Policy**.



4. Enable **Auto decommission after \_\_\_ days offline**.



5. Enter the number of days that offline Agents will show in the Management Console.
6. Click **Save**.
7. In the window that opens, click **Save**.

## 6. Analyzing, Mitigating, and Resolving Threats [Multi-Site]

**Management:** Central Park, Denali, Eiffel, Fuji, Grand Canyon, Houston

**Agents:** Windows 2.6+ | macOS 2.6+ | Linux 2.6+

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

Watch: [How to Analyze and Mitigate Threats in the Multi-Site Management Console](#)

A manual incident response plan usually requires a lot of time and resources. Gather data to define what is "good" and what is "unwanted" or "threatening". Identify events when you can or by signature. Notify the security team. Contain the infection. Investigate the attack to understand its severity and behavior. Remove all files that the attack installed, and recover files that it changed, if possible. Update reports of known malware and analyze how to respond faster next time.

SentinelOne significantly improves this workflow.

1. Our Agent learns what is good and what is threatening according to our research, real user and system behavior, and your optional specific tuning. The research is done for you.
2. SentinelOne identifies security incidents with its Dynamic Detection Engine (detects incorrect endpoint behavior from files, software, system, web, or user) and Static Detection Engine (stops malware before it can execute). Events are automatically categorized as safe, malicious, or unknown. The Management sends alerts for events relevant to you. The autonomous Agents mitigate known threats immediately.
3. The Management Console shows the storyline of threats. Your time to respond does not depend on the skills available or on access to all infected endpoints. You have the data automatically. You can mitigate with a click.
4. Update your blacklist (knowledge of malicious or unwanted items) with one click. Resolve false positives with a click. Generate reports in seconds.

For some incidents, the policy of the Agent automatically mitigates the threat and there is nothing more to do. For example, if the policy lets the Agent automatically mitigate threats discovered by a Pre-Execution engine (such as Reputation), no further mitigation action is required. For other incidents, the Agent waits for your decision. You can configure your Management to send alerts only for active threats that require your analysis.

### The threat analysis, mitigation, resolution workflow:

1. When you [get an alert for a security event](#), click **Analyze**.
2. Click **Disconnect from Network** [79], if relevant.

This option blocks network connections from an infected endpoint to make sure that the malware does not spread. The connection between the Agent and Management Console stays active.

3. [Analyze threats](#) [80] that are not mitigated automatically.
4. Click the recommended [mitigation option](#) [84].

5. [Resolve the incident \[85\]](#) to automate mitigation in the future.
6. If you disconnected the endpoint from the network, click **Reconnect to network**.

## 6.1. Prioritizing Threats

**Management:** Banff, Central Park, Denali, Eiffel, Fuji, Grand Canyon, Houston

**Agents:** All Agents

Watch: [How to Prioritize Threats](#)

### Prioritization

Open **Dashboard > THREATS** and set priority in this order:

1. Is the threat still active? See the threat mitigation status.

### Threat Mitigation Status

	Status	Priority	Description
	Multiple Detections	0	Indicates a list of similar detections. Expand the list to see the status of each detection.
	Active	0	The threat is active on the endpoints. You must act.
	Suspicious	1	The Agents detected something with a low confidence level. Analyze to decide if the detection is a threat or not.
	Mitigated	2	The Agents quarantined the threat and it is not a risk to the endpoint. Make sure that it did not cause damage or changes on the endpoint that need remediation.
	Blocked	3	The Agents mitigated the threat before it ran.

2. Look at the endpoint. Is the endpoint a server of a mission-critical application or organization-wide service? Is the endpoint the personal computer of a user with valuable data? For example, a threat on your CFO's computer is probably more important than a segment's application server.

If the endpoint is the highest priority, mitigate its threats first (see below).

3. For a multiple report threat, prioritize the Target endpoint.

If there is one Target endpoint, set the priority by endpoint function and value.

If multiple Agents reported the threat in one short time range, your organization or industry was targeted. Escalate the priority of the threat.

If there is a pattern in the timestamp differences between endpoints, the threat spreads itself. Escalate the priority of the threat.

**Best Practice:** For Active threats that spread, click **Disconnect from network** immediately. The endpoint can communicate only with the SentinelOne Management.

## 6.2. Disconnecting Endpoints from the Network

**Management:** Banff, Central Park, Denali, Eiffel, Fuji, Grand Canyon, Houston

**Agents:** All

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

Disconnect an endpoint from the network to put it in network quarantine.

**Best Practice:** For Active threats that spread, apply **Disconnect from network** immediately. The endpoint can communicate only with the SentinelOne Management.

Watch: [How to Disconnect Endpoints from the Network](#)

**To disconnect an endpoint from the network:**

- In **Network, Visibility, or Analyze**: select items and click **Actions > Disconnect from Network**.
- In **Endpoint Details** click **Actions > Disconnect from Network**.
- In the Forensics details of a threat, click **Disconnect from network** at the top.



**To reconnect an endpoint to the network:**

- In **Network**, select the endpoints and click **Actions > Reconnect to Network**.
- In **Endpoint Details**, click **Actions > Reconnect to Network**.

To open Endpoint Details from the Forensics details of a threat, click **Seen on network** and then click the endpoint name.

File Info	
	File: active_content.py Path: \Device\HarddiskVolume2\Users\Administrator\Desktop\ Command line arguments: "C:\Users\Administrator\Desktop\active_content.py"
	Machine: FB100 IP: [redacted] Domain: WORKGROUP Agent Version: 1.8.4.3714
	Identified: 09/26/2017 17:07:01 Reported at: 09/26/2017 17:06:59
	Seen on network: <a href="#">27 times</a>

## To automate Disconnect:

**Note:** From version 2.7, when **Disconnect from network** is enabled in the policy, endpoints are only disconnected if a threat is found after the threat is executed. Endpoints are not disconnected if a threat is detected pre-execution (by the Reputation or DFI engines) because the threat is not active.

1. In the policy, click **Change Policy**.

We recommend that you set this option for a group policy, and not a full site or the default policy.

2. Enable **Containment: Disconnect From Network**.

When an active threat is detected by an engine on execution (not pre-execution, such as the Reputation engine), the infected Agent is automatically disconnected from the network.

3. Click **Save**.

## To find endpoints that are disconnected from the network:

1. In **Network**, click **Select filters** to expand the filter options.
2. In **Network Status**, click **Disconnected**.

Select filters...									
Free text search	OS	Version	Type	Domain	Connected to Management	Health status	Network status	Pending actions	
Type your search...	Windows	13	2.8.0.11093	5	Desktop	13	WORKGROUP	12	Connected
	Linux	2	2.8.0.6418	4	Server	2	localdomain	4	Connecting
Enter text to match network or endpoint properties	macOS	1	2.7.0.6417	3	Laptop	1	sentinelone.local	1	Disconnected
	Windows Legacy		2.6.2.1455	2	Other				Disconnect
			2.8.0.1660	1					
			2.7.0.6458	1					

## 6.3. Analyzing Threats [Multi-Site]

**Management:** Central Park, Denali, Eiffel, Fuji, Grand Canyon, Houston

**Agents:** All

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

Watch: [How to Analyze and Mitigate Threats in the Multi-Site Management Console](#)

For each threat, answer these questions with the data in Forensics details.

- What did the threat attempt to do?

Look at the **Indicators** to see why the engine detected the file as malicious or suspicious. From Windows 2.8 and macOS 2.7 Agents, indicators for Behavioral AI detections include references to the Mitre Attack Matrix and use the Mitre methodology and terminology for easy cross-reference.

Suspicious activity detected. After investigation, consider marking as benign or as a threat.

**File Info**

- File: ida.exe
- Path: \Device\HerdiskVolume4\Program Files\IDA ... [Copy path](#)
- Device: [REDACTED]
- IP: [REDACTED]
- Domain: [REDACTED]
- Username: [REDACTED]
- Agent Version: 2.8.0.6703
- Site: [REDACTED]
- Group: [REDACTED]
- Identified: 10/29/2018 18:35:07
- Reported at: 10/29/2018 18:35:07
- Seen on network: 2 times

**Summary**

**S1 Risk levels:** Low

- SHA1: 85214dbb8231f53fa5fe6e50252c9605a668ebc [Google](#) [VirusTotal](#)
- Signer Identity: N/A
- Verifier: N/A
- Detecting engine: DBT - Executables [Open policy](#)

**Indicators**

**Abnormalities (2/18)**

- This binary contains abnormal section names which could be an indication that it was created with non-standard development tools
- This binary has an RWX section. It might contain self-modifying code.

**General (7/167)**

- Document behaves abnormally. MITRE: Execution (T1004)
- Suspicious library loaded into the process memory
- Code injection to a remote process. MITRE: Defense Evasion (T1055)
- Changed protection type of library in a remote process space. MITRE: Privilege Escalation
- Code injection to a remote process. MITRE: Defense Evasion (T1055)
- This binary imports functions used to raise kernel exceptions
- This binary imports debugger functions

Look at the **Attack Overview** to see the SentinelOne Severity rating and to get more statistics.

See the **Attack Story Line**. Did the threat try to change the registry? Did it try to change or remove specific files or paths?

- Did the threat succeed to create damage?
- How many endpoints did the threat infect? Click the **Seen on Network** link to see the list of endpoints.

(This is not always the same number as the number of reports of a threat that you see in the **Dashboard**. Until you mitigate a threat, one Agent can send multiple reports for one threat.)

## To see forensics for analysis:

In the sidebar, click **Dashboard**

Click a threat.

Status	File Details	Endpoints	Reported Time	Sites	Classification	Actions Done
	unreso.bat   Multiple   2	Multiple (2)	Jun 17th 2019 • 13:32:09	JD 1	Exploit	Killed, Quarantined, Remediated
	CryptoFortress.exe - Copy.bat	Limor-Xavier	Jun 13th 2019 • 11:50:56	ZDF SCH Site1	Malware	
	7395b2500791c1590a0b094b4ae923ea898fb1b4...	avi-Acc3	Jun 12th 2019 • 12:49:36	site 1	Malware	Killed, Quarantined
	0f3df543445c42c427a82bb340011c0f24850e227...	avi-Acc3	Jun 12th 2019 • 12:49:36	site 1	Malware	Killed, Quarantined
	be803f6cd7888e56e41427883155234ccf5b077...	avi-Acc3	Jun 12th 2019 • 12:49:36	site 1	Malware	
	ab9d3958659a59c1d168faf3b5225777c74d4b6cb...	avi-Acc3	Jun 12th 2019 • 12:49:36	site 1	Malware	
	7758fad4df30998ed8508cc22e3c198fa351807bfa...	avi-Acc3	Jun 12th 2019 • 12:49:35	site 1	Malware	Killed, Quarantined
	21d463d56afbcc2977377d798a7a46855a31cf2f...	avi-Acc3	Jun 12th 2019 • 12:49:35	site 1	Malware	
	fce3e99b01d5e254ce0ee7d1b0afabc7fb6c49ea0...	avi-Acc3	Jun 12th 2019 • 12:49:35	site 1	Virus	Killed, Quarantined
	4360230b343fa40c6a9d19d62198828bf81bdd397...	avi-Acc3	Jun 12th 2019 • 12:49:35	site 1	Malware	Killed, Quarantined

The **Analyze** page opens and shows the Forensics details of the threat.

**ACTIONS**  
Click on the desired mitigation action.

**CLASSIFICATION**  
**EXploit**

**STATUS**  
**UNRESOLVED**

**File Info**

- File: unreso.bat
- Path: \\Device\\HarddiskVolume2\\Users\\ADMIN\\Desktop\\unreso.bat
- Command line arguments: /c "C:\\Users\\ADMIN\\Desktop\\unreso.bat"
- Device: avi-Acc1
- Console visible IP: 10.0.0.100
- IP Address: 10.0.0.100
- Domain: WORKGROUP
- Username: AVI-ACC1\\ADMIN
- Agent Version: 3.3.0.7512
- Site: JD1
- Group: GR1
- Identified: 06/17/2019 13:32:09
- Reported at: 06/17/2019 13:32:09
- Seen on network: 2 times

**Summary**

**S1** Risk levels: N/A

SHA1: d87c71d23df90bd3f5b1855bd1bb3cd68f40e81e Recorded Future VirusTotal

Signer Identity: N/A

unreso.bat Ver: N/A

Detecting engine: Documents, Scripts Open policy

[Download threat file](#)

**NO NETWORK CONNECTIONS**

**ATTACK OVERVIEW**

**CATEGORIES (Events Count)**

Category	Events Count	(Severity)
File Operations (1)	1	LOW
System Manipulation (2)	2	HIGH

**EVENTS STATISTICS**

- FILES: 1
- NETWORK: 0
- PROCESSES: 2
- REGISTRY: 0

3 EVENTS  
67%  
33%

**ATTACK STORY LINE**

```

graph LR
    A((explorer.exe)) --> B((cmd.exe))
    B --> C((conhost.exe))
    
```

OR:

1. In the sidebar, click **Analyze**
2. Click in the filters field to open the filters.

**ANALYZE** Full site view

**Resolved: No**

**Resolved**   **No**

**Resolved**   **Yes**

**Last 7 Days**

**Selected** 10 Results

Resolved	OS	Engine	Mitigation Status	From scan	Resolved	Classification
No	Windows	Documents, Scr...	mitigated	No	No	Malware
Yes	macOS	DBT Executab...	active	Yes	Yes	OSX.Malware
	Windows Legacy	Anti Exploitatio...	suspicious			Benign
	Linux	On Write DFI	blocked			Hacktool
		Reputation				Downloader
		Intrusion Detec...				Virus

The **Resolved:No** filter is selected by default, to show only detections that are not resolved.

- Select the filter values (see below) to match the incidents you want to see now.

You can use the free text search with the filters.

- Optional: Select a different time period. Results from the **Last 7 Days** show by default.

- In the results, click a threat to open its Forensics details.

Note: If you click a threat with multiple instances , all of the instances open in the Analyze view.

## Analyze Filters

Filter	Valid Values
<b>Free text search</b>	Search for: Endpoint name, file path, filename, file extension, hash and username
<b>OS</b>	Windows, macOS, Linux, Windows Legacy
<b>Engine</b>	Agent engines that detected the threat (see below)
<b>Mitigation Status</b>	mitigated, suspicious, blocked, active
<b>From scan</b>	Yes, No (Detected by Full Disk Scan or not)
<b>Resolved</b>	Yes, No (Marked as <b>Resolved</b> by an admin or not)
<b>Classification</b>	Category of threat: malware, packed, benign, hacktool, downloader, virus, adware, trojan, worm, infostealer, dialer, network, OSX malware, backdoor, browser, Linux malware, ransomware, PUA, spyware, exploit, rootkit, lateral movement, interactive shell

### Examples of Analysis Filters

- You learned of a malicious hash infecting networks. To see if it infected your endpoints, you paste the hash in the **Free text search**.
- You want to prioritize threat analysis. You filter for **Mitigation Status = active** and **Resolved = No**.

## Engines

Engine	Description
reputation	An engine that uses the SentinelOne Cloud to make sure that no known malicious files are written to the disk or executed. This cannot be disabled.
pre_execution	DFI (Deep File Inspection) A preventive Static AI engine that scans for malicious files written to the disk. It supports portable executable (PE) files.
pre_execution_suspicious	DFI - Suspicious A Static AI engine that scans for suspicious files written to the disk. When in Protect mode, this engine is preventive. It supports portable executable (PE) files.

Engine	Description
executables	(Dynamic Behavioral Tracking) A Behavioral AI engine that implements advanced machine learning tools. This engine detects malicious activities in real-time, when processes execute.
pup	Potentially Unwanted Applications A Static AI engine on macOS devices that inspects applications that are not malicious, but are considered unsuitable for business networks.
exploits	A Behavioral AI engine, focused on exploits and all fileless attack attempts, such as web-related and command line exploits.
penetration	Detect Interactive Threat A Behavioral AI engine that protects against malicious commands run locally in interactive sessions of CLIs, such as CMD or PowerShell.
data_files	A Behavioral AI engine, focused on all types of documents and scripts.
lateral_movement	A Behavioral AI engine that detects attacks initiated by remote devices.

## 6.4. Mitigation Options

**Management:** Alhambra, Bahamas, Banff, Central Park, Denali, Eiffel, Fuji, Grand Canyon, Houston

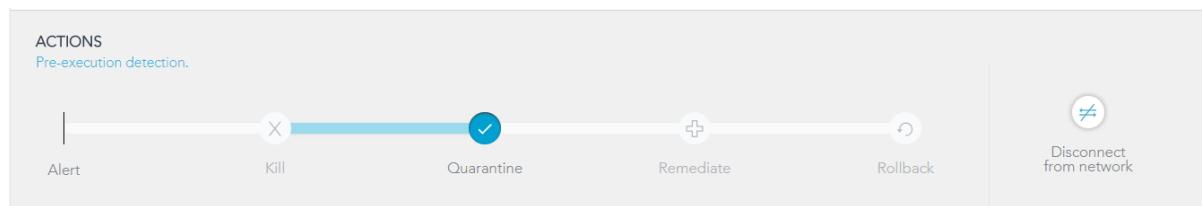
**Agents:** All

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

Watch: [How to Analyze and Mitigate Threats in the Multi-Site Management Console](#)

The Agent mitigates threats automatically, if its policy is set to **Protect**. When you analyze Active threats, you see the mitigation actions that the Agent applied automatically and if there are recommended actions.



- **Kill** - Stops processes. Active content in documents, executables, and sub-processes are stopped. The Agent enables Kill for processes that act against normal endpoint behavior or do not fit the actions of the application the process is hiding in.
- **Quarantine** - Stops processes, encrypts the executable, and moves it to a confined path. If a threat is known, the Agent automatically kills the threat before it can execute. The only mitigation action for you is **Quarantine**.

- **Disconnect from network** - (Also known as Network Quarantine or Network Isolation) The Agent can communicate only with the Management Console. The endpoint cannot communicate with other components on the network.

### Mitigate with Automated EDR

- **Remediate** - Stops processes, quarantines binaries, removes linked libraries, deletes seed files, and restores configuration of the OS, application, and user settings to the state before the attack began.
- **Rollback** - (Windows only) Restores the endpoint to a saved VSS snapshot, undoing the changes made by the process and its associated assets. This option is best for ransomware mitigation and disaster recovery.

Some platforms do not support all mitigation features:

- Windows XP, Server 2003, Server 2008, POSReady 2009 - do not support Quarantine, Remediate, Rollback, Disconnect from Network
- macOS versions - do not support Rollback
- Linux supported kernels - do not support Remediate, Rollback

## 6.5. Resolve Options

**Management:** Alhambra, Bahamas, Banff, Central Park, Denali, Eiffel, Fuji, Grand Canyon, Houston

**Agents:** All

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

Mark detections as **Resolved** when you finish handling them, to clean up your Dashboard and Analyze views.

Add items to the **blacklist** or mark items as **threat** or **benign** to automate your SentinelOne deployment for your definitions of *legitimate* and *malicious*.

- **Add to blacklist** (shows if the detection is marked as a threat) - To automate threat handling. The Management adds the item to the blacklist. If this threat is detected on an endpoint, the Agent blocks it immediately.

You still need to **Mark as resolved** to remove the threat from your Dashboard.

- **Mark as threat** (shows if the detection is marked as suspicious) - The item becomes marked as a threat and the Management adds it to the blacklist. If this threat is detected on an endpoint, the Agent blocks it immediately.

You still need to **Mark as resolved** to remove the threat from your Dashboard.

If the item was part of a threat group, other items in that threat group are also marked and threats and mitigated according to the policy.

- **Mark as resolved** - Remove the threat from the **Dashboard**.
- **Mark as benign** - For false positives. The Management adds the item to the Exclusions, marks the threat as resolved, and removes it from the **Dashboard** view.

Watch: [How to Add Hashes to the Blacklist](#)

From Bahamas and later: If you resolve issues with **Mark as Benign**, there are more options that add the item to the Global Exclusions or to the Exclusion list of the current site. Select a type (Hash, File full path, File Type) to add the exclusion by type.

## 6.6. Changing Mitigation - Unquarantine [Multi-Site]

If your policy is set to **Protect**, Agents automatically block and quarantine detected threats. The quarantine action encrypts the file, changes its properties (including filename), and moves it to a confined path. If the file is not harmful, you can undo the mitigation. You can also use these steps to undo a quarantine that you ran manually.

The Unquarantine option is available only if the mitigation status of the detection is **Quarantined**. It is not available if the file was deleted from the endpoint or if the endpoint was rolled back. It is not available if the detection was remediated or blocked. (To undo a **Kill** mitigation, change the blacklist hash to *exclusion*, and let the file write again).

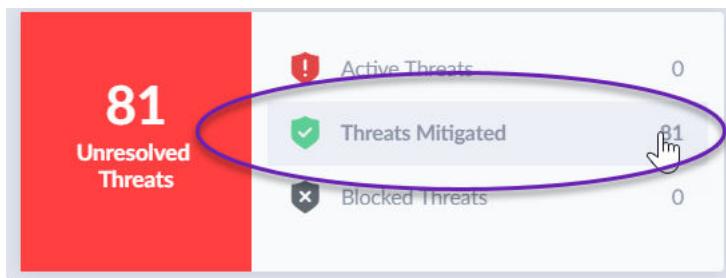
You cannot see unquarantine actions in the Activity log.

We recommend that you mark legitimate files with **Mark as benign**. If the file is on the Blacklist, Agents will block and quarantine it again.

Note: If the Agent is upgraded, you cannot unquarantine the files that it quarantined before the upgrade.

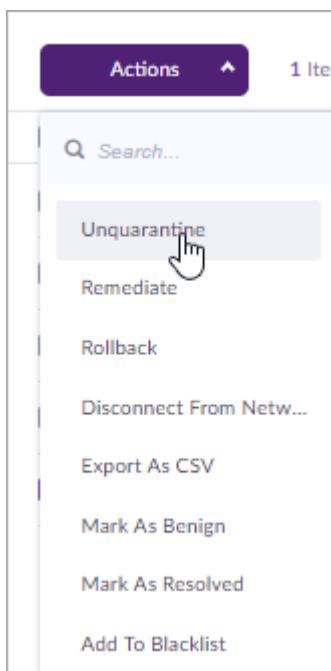
### To unquarantine a quarantined item:

1. In the sidebar, click **Scope**  and select a scope.
2. In the sidebar, click **Dashboard** .
3. Click **Threats Mitigated**.



OR: Click **Analyze** > **Select Filters** > **Mitigation Status = mitigated**.

4. In the Analyze page, select the detections for which the **Actions done** column shows **quarantined**.
5. Click **Actions** > **Unquarantine**.



## 6.7. On-Demand File Fetch [Multi-Site]

**Management:** Central Park, Denali, Eiffel, Fuji, Grand Canyon, Houston

**Agents:** Win 2.9+ | macOS 2.6+ | Linux 3.0+

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

To activate this feature, contact SentinelOne Support.

On-Demand file fetch lets you download files from an endpoint to the SentinelOne Management Console. There are two types of On-Demand file fetch:

- [Threat File Fetch \[87\]](#) - Get the file or files that are root of the threat (Win 2.9 +| macOS 3.0+).
- [Multi File Fetch \[90\]](#) - Get multiple files that you specify (Win 2.9 +| macOS 2.6+).

Watch: [How to use On-Demand File Fetch](#)

### Threat File Fetch

From the Forensics details of a threat, you can click **Download threat file** to get the file or files that are root of the threat.

This feature is enabled by default in most deployments.

For deployments in GovCloud, this feature is disabled by default. To enable it, contact SentinelOne Support.

### Specifications:

- Currently supported for Windows Agent version 2.9+ and macOS Agent version 3.0.

- Relevant files are automatically selected by the Agent.
- If a threat is fileless, this option is not available.

## To get threat files from an endpoint:

1. Open the Forensics details of a single detection from the **Dashboard** or the **Analyze** view.
2. In the Forensics details, click **Download threat file**.

The screenshot shows the 'File Info' section of the threat details. It includes the file path, command line arguments, device information (IP Address, Domain, Username, Agent Version, Site, Group), and a timestamp. The 'Download threat file' button is circled in red at the bottom of the section.

3. In the window that opens, enter a new password that you create

Remember the password - you will use it to open the file after you download it from the Management Console. To set the password, use 10 or more characters with a mix of upper and lower case letters, numbers, and symbols.

4. Click **Submit**.

The file is fetched from the endpoint, archived as a zip file, and encrypted with the password you entered.

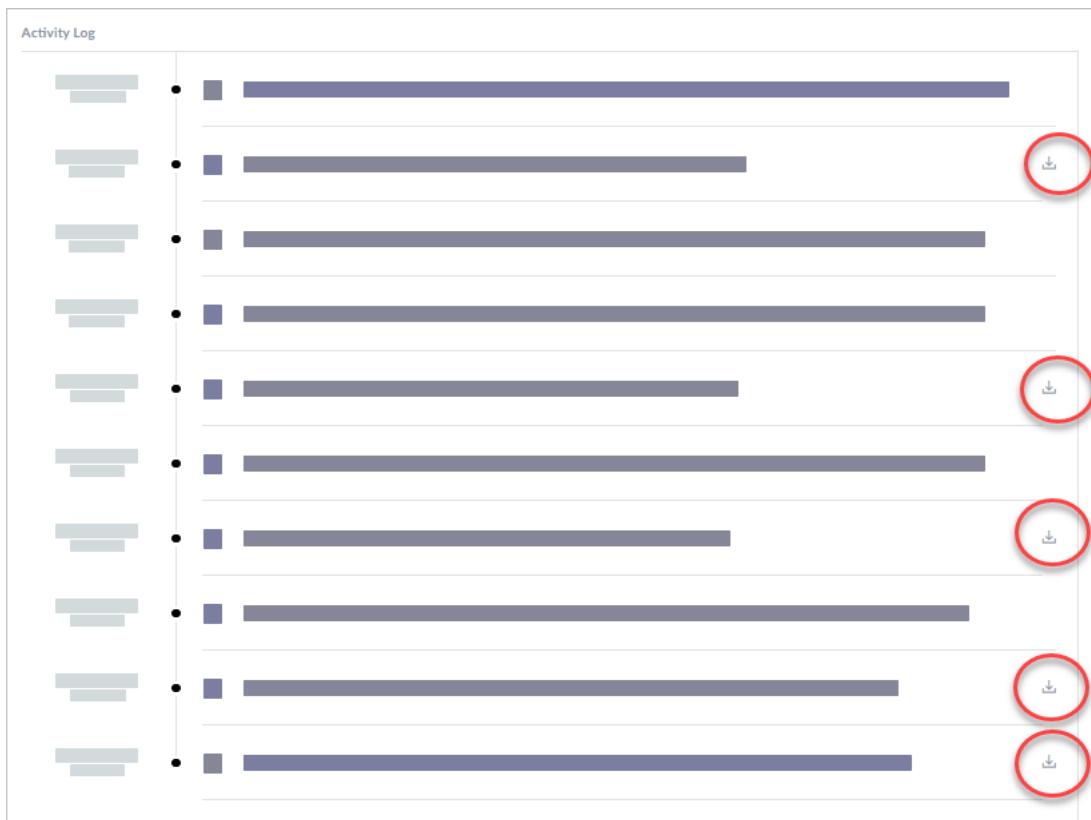
5. In the sidebar, click **Activity** .
6. Filter for **Fetch file operations**: Click **Administrative** and select **Fetch file operations**.

The screenshot shows a list of administrative activities for a single agent. The activities are listed in a tree view under the 'Administrative' category. The items are:

- Administrative
- Agent subscribed
- Agent updated
- Uninstall requested
- Uninstall sent
- Agent uninstalled
- Log operations
- Fetch files operations
- Agent decommissioned
- Agent recommissioned
- Full disk scan
- Machine Restarted

The 'Fetch files operations' item is currently selected, indicated by a highlighted background.

7. When the files are ready to download, an activity shows:  
**Agent successfully uploaded a threat file.** Click the download button in the item.



8. A warning shows that you are about to download a malicious file. Click **Confirm** if you want to download anyway.

The zip file downloads to the default **Downloads** folder on the Management Console computer. The file name is in the format **<hostname>\_<date>\_<time>.zip**.

9. When you extract the files, you are prompted for a password. Enter the password that you created when you initiated the threat file download and click **OK**.
10. Deal with the threat file cautiously.

Also see [Contents of the zip file \[93\]](#) below.

### Multi File Fetch

You can download multiple files that you specify from SentinelOne endpoints to the Management Console. Use this to analyze malware or for other operational needs.

For regulation compliance, this feature is disabled by default. To enable it, contact SentinelOne Support.

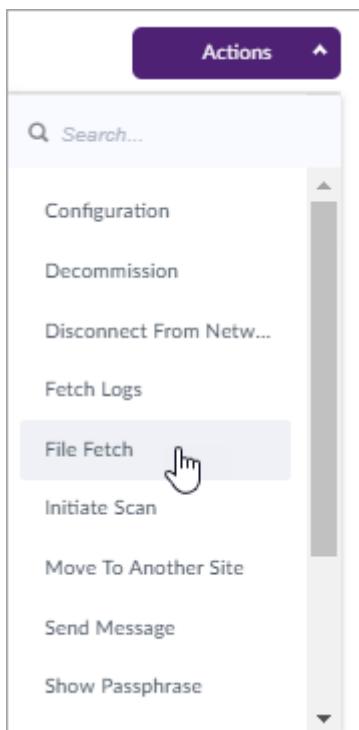
#### Specifications:

- Supported from Windows Agent version 2.9+ and macOS Agent version 2.6+.
- You can get up to ten files at one time, with a ten MB maximum size for each file.
- You can only get files by explicit, full pathnames. You cannot use: Wildcards, environment variables, non-regular files (such as /dev/\*), or sensitive files (such as SSH private keys).

- To minimize risk, run the Fetch File action on a single endpoint that you select manually from the Management Console.
- Fetched files are automatically deleted from the Management after 72 hours and are not available for download from the Management Console after that time.

## To run Multi Fetch File action on an endpoint:

1. In the sidebar, click **Network** .
2. Click an endpoint from the list to open its **Endpoint Details**.
3. Click **Actions > File Fetch**.



4. In the Fetch Files window, enter the **File Path** for the files to download.
  - Format for macOS - in the file path, use spaces and not backslashes.
    - Correct path example - /Users/Sierra/Desktop/files to send
    - Invalid path example - /Users/Sierra/Desktop/files\to\send
  - Format for Windows - Use paths that follow Windows filename limitations. Do NOT include characters / : \* ? " <> |.
    - Correct path example - C:\Users\Desktop\files to send
    - Invalid path example - C:\Users\Desktop\"? "
5. Click **Add**. You can add multiple file paths.
6. In **Password**, enter a password.

Remember the password - you will use it to open the zip file after you download it from the Management Console. To set the password, use 10 or more characters with a mix of upper and lower case letters, numbers, and symbols.

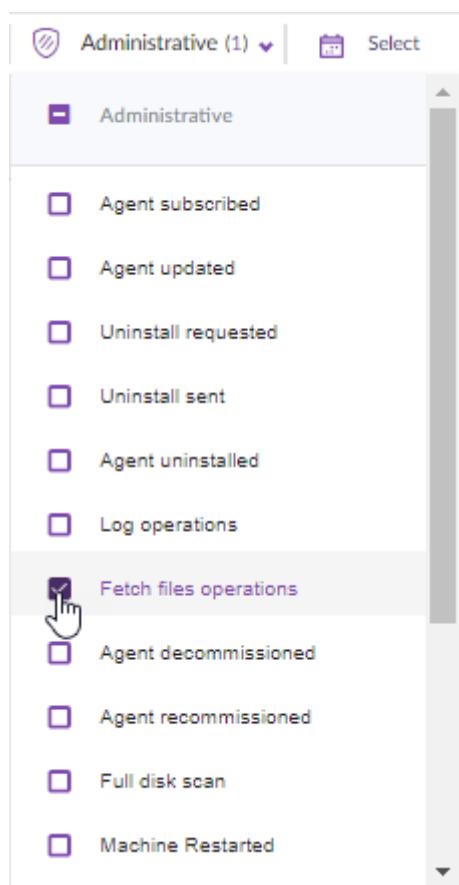
7. Click **Submit**.

The files are fetched from the endpoint, archived as a zip file, and encrypted with the password you entered.

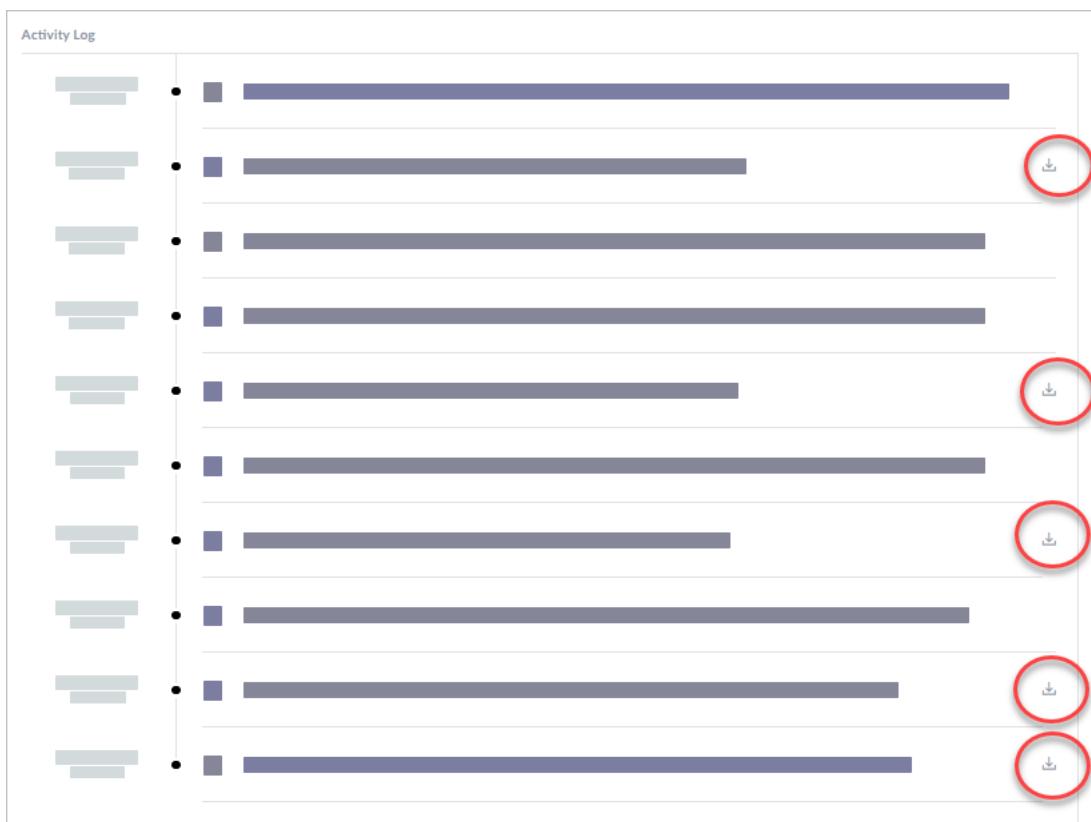
8. Click **OK**.

### To download the files from the Management Console:

1. In the sidebar, click **Activity** .
2. Filter for **Fetch file operations**: Click **Administrative** and select **Fetch file operations**.



3. When the files are ready to download, an activity shows that the Agent successfully uploaded an archive file. Click the download button of the activity.



The **Archive.zip** file downloads to the default **Downloads** folder on the Management Console computer.

- When you extract the files, you are prompted for a password. Enter the password that you created when you initiated the threat file download and click **OK**.

#### Contents of the zip file

The downloaded zip file has the fetched file or files and a metadata file, **manifest.json**, which shows for each file:

- The NT file path.
- The SHA-1 and SHA-256 hash
- Error messages related to the fetch operation.

Examples of errors: **No such file or directory**, for an invalid path, or **<invalid>** for a file type that is not allowed.

If you try to download a file after it was deleted from the Management, a message shows that it was deleted. Run the Fetch File action again to get the file.

## 7. Running Full Disk Scan [Multi-Site]

**Management:** Central Park, Denali, Eiffel, Fuji, Grand Canyon, Houston

**Agents:** Windows 2.6+| macOS 2.6+| Linux 2.6.3+

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

[Watch: How to Run Full Disk Scan on Demand](#)

Agents can run Full Disk Scan when an Agent is installed and by demand. It finds dormant suspicious activity, threats, and compliance violations, that are then mitigated according to the policy.

### Files included in the scan:

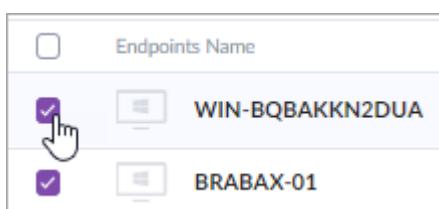
- The local file system of each endpoint. Full Disk Scan does not inspect network drives, which would require user credentials. To see which drives are local, run: C:\>WMIC logicaldisk get caption, description, drivetype
- Full Disk Scan inspects file headers. It looks at all EXEs, DLLs, SYS files, and more, on the fixed drives of the local system.
- The Agent scans files copied from an external drive to a local disk, or files run from an external drive. It does not scan or mitigate external drives.
- The Agent does not collect PII data from files.
- For folders and files that are included in Exclusions in the Agent policy, there is no mitigation.

**Note:** Full Disk Scan does not work based on hashes, and therefore it does not check each file against the blacklist. If a file is determined as suspicious by the Static-AI (DFI) engine, then the Agent calculates its hash and checks the blacklist to see if the hash exists there. If a file is executed, all aspects of the process are inspected, including hash-based analysis and checking if the file is on the blacklist.

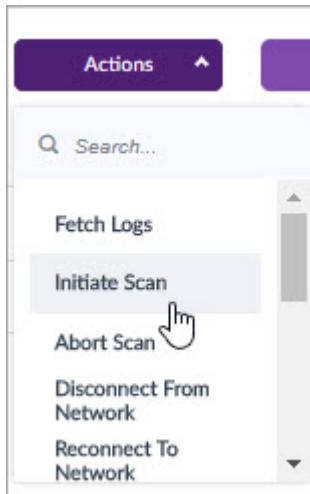
Full Disk Scan can run when the endpoint is offline, but when it is connected to the Management, it can use the most updated Cloud data to improve detection.

### To start a Full Disk Scan from the Management Console:

- In the sidebar, click **Scope**  and select a scope.
- In the sidebar, click **Network** .
- In the **Network** view, select one or more endpoints.



4. Click **Actions**, and select **Initiate Scan**.



5. In the window that shows, click **OK**.

#### To stop a scan:

1. In the **Network** view, select the Agents.
2. Click **Actions** and select **Abort Scan**.

## 7.1. Running Full Disk Scan on Installation [Multi-Site]

**Management:** Central Park, Denali, Eiffel, Fuji, Grand Canyon, Houston

**Agents:** Windows 2.6+ | macOS 2.6+| Linux 2.6.3

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

[Show Me video: How to Run Full Disk Scan on Agent Installation](#)

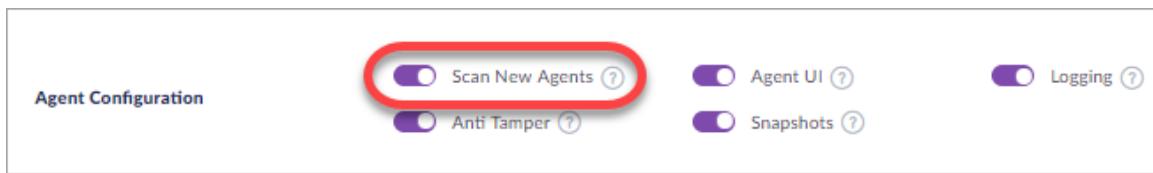
Full Disk Scan finds dormant suspicious activity, threats, and compliance violations, that are then mitigated according to the policy. Agents can run Full Disk Scan when the Agent is installed and by demand. You can configure Full Disk Scan on installation from the Management Console. When you enable **Scan new Agents** in the policy **Agent Configuration settings**, new Agents that get the policy are scanned immediately. The scan can run before the Agent reboots.

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.

To enable Full Disk Scan on installation from the CLI, see [Full Disk Scan from CLI \[96\]](#).

#### To enable Full Disk Scan on Agent installation from the Management Console:

1. Open a Global, Site, or group policy in Policy.
2. In the **Agent Configuration** section, make sure that **Scan new Agents** is enabled.



3. Click **Save**.

## 7.2. Full Disk Scan from CLI [Multi-Site]

**Management:** Central Park, Denali, Eiffel, Fuji, Grand Canyon, Houston

**Agents:** Windows 2.6+ | macOS 2.6+ | Linux 2.6.3+

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

See [sentinelctl](#) to learn more.

### Full Disk Scan Commands on Windows

Action	Command
Enable Full Disk Scan on Agent installation	<code>SentinelInstaller.exe /SITE_TOKEN=&lt;string&gt;/scheduleFullScan</code>
Initiate Full Disk Scan on a folder See <code>sentinelctl</code> . (Wildcards are not supported)	<code>sentinelctl scan_folder -i &lt;path&gt;</code> example: <code>sentinelctl scan_folder -i c:\Downloads</code>
Cancel a scan	<code>sentinelctl scan_folder -c</code>
See which drives are local (only local drives are scanned)	<code>C:\&gt;WMIC logicaldisk get caption, description, drivetype</code> Example of results: Caption Description DriveType C: Local Fixed Disk 3 D: Local Fixed Disk 3 E: Local Fixed Disk 3 F: CD-ROM Disc 5 G: Local Fixed Disk 3

### Full Disk Scan Commands on macOS

Action	Command
Enable Full Disk Scan on Agent installation	<code>sudo sentinelctl scan --run-asap {yes no}</code>
Initiate Full Disk Scan on a folder See <code>sentinelctl</code> . (Wildcards are not supported)	<code>sudo sentinelctl scan --local &lt;path&gt;</code>
Initiate complete Full Disk Scan	<code>sudo sentinelctl scan --full</code>
Wait until the scan is done	<code>sudo sentinelctl scan --block &lt;path&gt;</code>

Action	Command
See which drives are local (only local drives are scanned)	<code>sudo sentinelctl scan --info</code>

## Full Disk Scan Commands on Linux

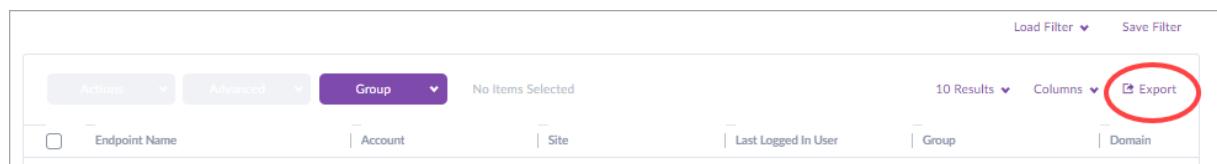
Action	Command
Initiate complete Full Disk Scan	<code>sudo /usr/local/sentinelagent/bin/sentinelctl --scan=start</code>
Cancel a scan	<code>sudo /usr/local/sentinelagent/bin/sentinelctl --scan=abort</code>
See scan status	<code>sudo /usr/local/sentinelagent/bin/sentinelctl --scan=status</code> Valid returns: N/A - Endpoint was never scanned because its Agent version is not supported or a scan was never run In progress - Endpoint got the scan command but did not yet report completion Aborted - Scan was started but aborted before completion Completed - Date and time of last scan, of completion report from Agent

## 7.3. Seeing Full Disk Scan Status and Results [Multi-Site]

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

From Management version Fuji SP2, you can easily output all of the details for selected endpoints, including their scan status. An **Export** option shows in the **Network** view. It exports all network endpoint information for each endpoint in the current filter (up to 20,000 endpoints) in CSV format.

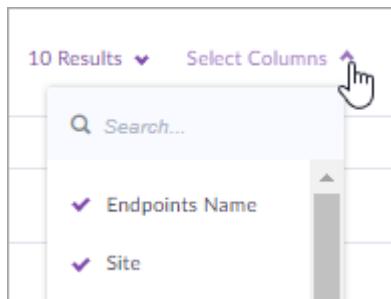


### To see the status of a scan:

1. In the Management Console, click **Network**.
2. In the **Network** view, see the **Scan Status** column. It shows one of these statuses:
  - **Completed** - Completed successfully with the date and time the scan finished.
  - **In progress** - The scan is running.
  - **Aborted** - The scan did not finish.
  - **N/A** - The Agent did not have a full disk scan.

**If the Scan Status column is not visible:**

1. In the Management Console, click **Network**.
2. Above the filter results, click **Select Columns**.



3. Scroll down to **Scan Status** and select it.

**To see results of a scan:**

1. In the Management Console, click **Analyze**.
2. In the **Analyze** view, in the **Search**, enter: `src:scan`
3. Click a line to see details of what was found and where.

[Show Me video: How to Run Full Disk Scan on Demand](#)

## 8. Managing Policies [Multi-Site]

**Management** : Central Park, Denali, Eiffel, Fuji, Grand Canyon, Houston

**Agents** : Windows 2.6+ | macOS 2.6+ | Linux 2.6+

**Minimum Admin Scope**: Site Admin

**Scope**: Selected Site, Account, or Global

A *policy* is a set of mitigation settings and configuration settings that define the behavior of SentinelOne Agents on endpoints.

### Policy Inheritance

- Each Account, Site, and Group can have their own policy, or they can inherit the policy from scopes above them.
- By default, each Account, Site, and Group inherits the Global policy. Global Admins can make changes to the Global policy. Admins can make changes to the policy for entities in their scope.
- For example, Groups inherit the policy defined for their Site. If the policy is not changed for the Site, Groups inherit the Account or Global policy.

Watch: [How to Manage Policies](#)

Watch: [Understanding Global and Site Assets: Policies, Blacklists, Exclusions, & Packages](#)

### To see a scope's policy:

1. In the sidebar, click **Scope**  and select a scope.
2. In the **Network** toolbar, click **Policy**.



Each policy contains:

- [Policy Settings \[Multi-Site\] \[101\]](#)
- [Policy Engines \[Multi-Site\] \[103\]](#)
- [Agent Configuration Settings \[Multi-Site\] \[106\]](#)

### 8.1. Changing a Policy [Multi-Site]

**Management**: Central Park, Denali, Eiffel, Fuji, Grand Canyon, Houston

**Agents**: Windows 2.6+ | macOS 2.6+ | Linux 2.6+

**Minimum Admin Scope**: Site Admin

**Scope**: Selected Site, Account, or Global

When you change a policy, the changes are automatically pushed to the Sites and Groups that use the policy.

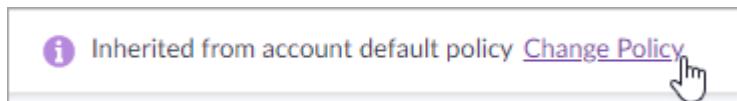
You can set the policy for a Site or Group when you create it, and you can change the policy after creation.

## To change the policy for a Site, Group, or Account:

1. In the sidebar, click **Scope**  and select a scope.
2. In the **Network** toolbar, click **Policy**.



3. If the scope inherits its policy and you want it to have its own policy instead, click **Change Policy**.



If the scope uses its own policy, it is open for changes. When you make a change, the **Save** button shows.

4. Edit the policy settings.
  - [Policy Settings \[Multi-Site\] \[101\]](#)
  - [Policy Engines \[Multi-Site\] \[103\]](#)
  - [Agent Configuration Settings \[Multi-Site\] \[106\]](#)
5. Click **Save**.
6. In the window that opens, click **Save**.

## To revert a policy to the default inherited policy:

1. In the sidebar, click **Scope**  and select a scope.
2. In the **Network** toolbar, click **Policy**.



3. Click **Revert to default inherited policy**.



4. In the window that opens, click **Save**.

## To change the Global policy:

Global Admins can change the Global policy. It is the default policy for all Accounts, Sites, and Groups.

1. In the sidebar, click **Scope**  and select a scope.

You must select Global.

2. In the **Network** toolbar, click **Policy**.



3. Edit the policy settings.

- [Policy Settings \[Multi-Site\] \[101\]](#)
- [Policy Engines \[Multi-Site\] \[103\]](#)
- [Agent Configuration Settings \[Multi-Site\] \[106\]](#)

4. Click **Save**.

5. In the window that opens, click **Save**.

## 8.2. Policy Settings [Multi-Site]

**Management:** Central Park, Denali, Eiffel, Fuji, Grand Canyon, Houston

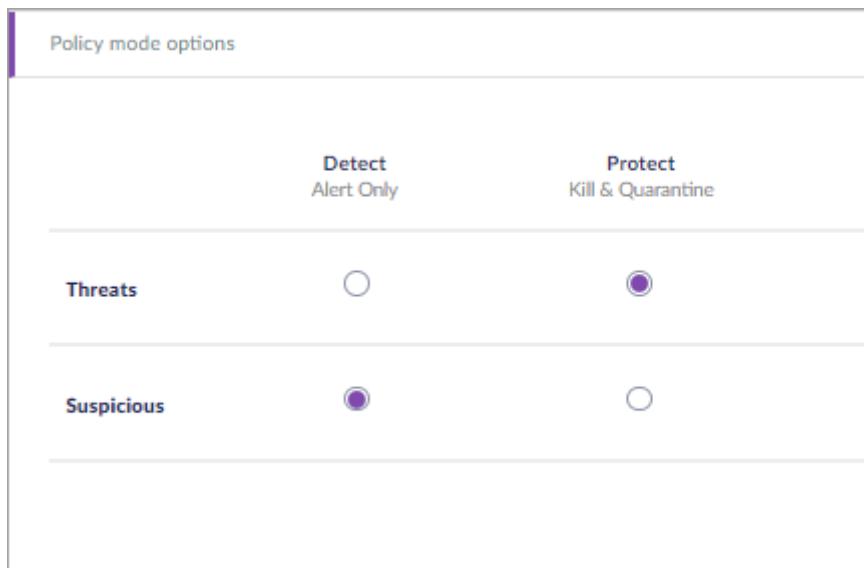
**Agents:** Windows 2.6+ | macOS 2.6+ | Linux 2.6+

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

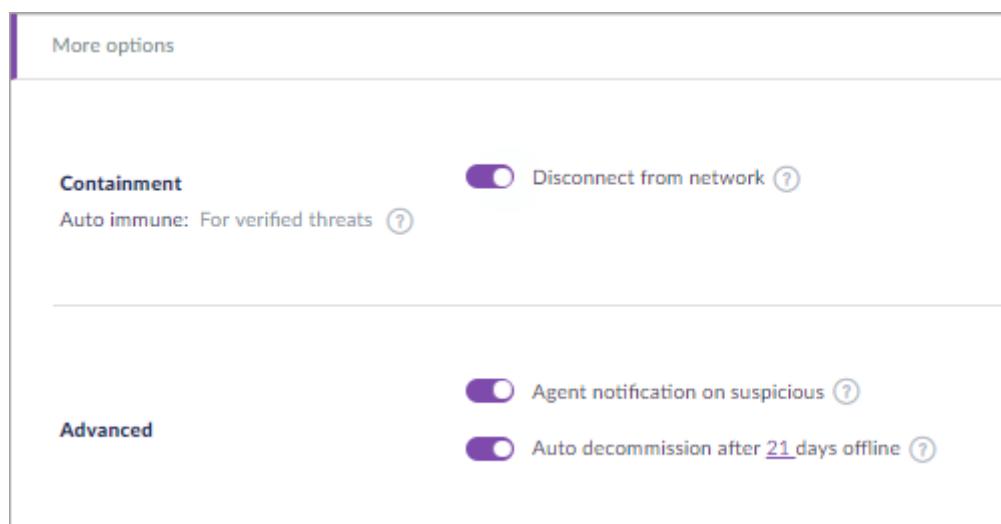
The mitigation settings in the **Policy mode options** define the Agent behavior for:

- **Threats** - Detections that are malicious, based on high confidence of the SentinelOne policy engines.
- **Suspicious** - Detections that might be malicious but require more analysis, based on SentinelOne policy engines.



## Policy Modes

Policy Mode Options	Setting	Description
<b>Threats</b>	<b>Protect</b>	Automatically kills and quarantines malware and sends <b>Mitigated Threat</b> alerts (recommended).
	<b>Detect</b>	Sends <b>Active Threat</b> alerts. Does not automatically mitigate. <b>Note:</b> In Windows Agent versions earlier than 3.1, the Agent blocks execution of threats that are known by Cloud Intelligence Service or on your blacklist. In Windows Agent versions 3.1 and later, and all macOS and Linux versions, no execution is blocked when in Detect mode.
<b>Suspicious</b>	<b>Protect</b>	Automatically kills and quarantines files and sends <b>Mitigated Threat</b> alerts.
	<b>Detect</b>	Sends <b>Suspicious Activity</b> alerts. Does not automatically mitigate.



## More Options

Option	Setting	Description
<b>Disconnect from Network</b>	<b>On</b>	Automatically blocks network connections from an infected endpoint to make sure that the malware does not spread. The connection between the Agent and Management stays active. Also called Network Quarantine. <b>Note:</b> From version 2.7, when <b>Disconnect from network</b> is enabled in the policy, endpoints are only disconnected if a threat is found after the threat is executed. Endpoints are not disconnected if a threat is detected pre-execution (by the Reputation or DFI engines) because the threat is not active.
	<b>Off</b>	Infected endpoints are not automatically disconnected from the network. You can disconnect them manually.
<b>Auto-immune for verified threats</b>	<b>On</b>	Adds known hashes to the blacklist for all Sites that encounter them. This is always On and cannot be turned Off.
<b>Agent notification on suspicious</b>	<b>On</b>	An alert opens on the endpoint computer for each threat or suspicious activity.
	<b>Off</b>	Alerts do not open on endpoint computers for detections.
<b>Auto Decommission after X days offline</b>	<b>On</b>	Removes Agents from the Management Console if there is no communication with an Agent. The Management automatically recommissions the Agent after it starts to communicate again.
	<b>Days Offline</b>	Click the number to change the number of days before an offline Agent is decommissioned.

Also see [Agent Configuration Settings \[Multi-Site\] \[106\]](#).

### 8.3. Policy Engines [Multi-Site]

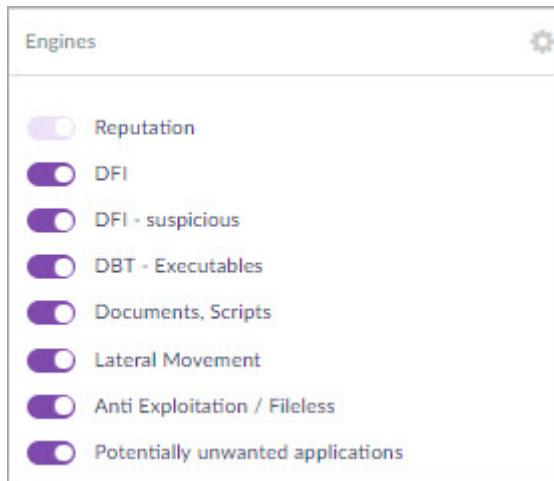
**Management:** Central Park, Denali, Eiffel, Fuji, Grand Canyon, Houston

**Agents:** Windows 2.6+ | macOS 2.6+ | Linux 2.6+

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

The **Engines** section of the policy shows the SentinelOne engines on the Agent that scan and inspect activity. All engines are **On** by default. We highly recommend that you keep the default settings.



The modes of SentinelOne engine behavior are:

- **On Write** - Use Static AI and Reputation engines to monitor files written to disk.
- **On Execute** - Monitor behavior and detect malicious activity when a process initiates.

## SentinelOne Engines

Engine Name	Description
Reputation	An engine that uses the SentinelOne Cloud to make sure that no known malicious files are written to the disk or executed. This cannot be disabled.
DFI (Deep File Inspection)	A preventive Static AI engine that scans for malicious files written to the disk. It supports portable executable (PE) files. For Windows Agents 2.7+: The engine runs scans upon file execution, in addition to when files are written to the disk. From Windows Agents 2.8+: The engine also scans PDF files. This engine was turned off (default setting) because of the number of False Positives. Microsoft Office files are not supported. Microsoft Office files are not supported.
DFI - Suspicious	A Static AI engine that scans for suspicious files written to the disk. When in Protect mode, this engine is preventive. It supports portable executable (PE) files.
DBT - Executables (Dynamic Behavioral Tracking)	A Behavioral AI engine that implements advanced machine learning tools. This engine detects malicious activities in real-time, when processes execute.
Documents, Scripts	A Behavioral AI engine, focused on all types of documents and scripts.
Lateral Movement	A Behavioral AI engine that detects attacks initiated by remote devices.

Engine Name	Description
Anti Exploitation / Fileless	A Behavioral AI engine, focused on exploits and all fileless attack attempts, such as web-related and command line exploits.
Potentially unwanted applications	A Static AI engine on macOS devices that inspects applications that are not malicious, but are considered unsuitable for business networks.
Detect Interactive Threat	<p>The Detect Interactive Threat engine is part of the Behavioral AI and focuses on insider threats (for example, an authenticated user runs malicious actions from a CMD or PowerShell command line). This engine detects malicious commands in interactive sessions. It does not detect non-interactive sessions. For example, if a Word document triggers a PowerShell session that runs malicious commands, a different engine will detect that.</p> <p><b>Detect Interactive Threat</b> is disabled by default. If you want to protect your endpoints from malicious commands that are entered in a CLI, enable this engine. But, if you enable this engine for endpoints of active users of CLIs, you may expect a number of false positives. (Windows only)</p>

The On Write mode, with Deep File Inspection and Reputation, is active immediately.

If **Full disk scan on install** is enabled in the policy of the Agent, it starts to scan the endpoint. This applies to Windows Agent version 2.1 and later, macOS Agent version 2.5 and later, and Linux Agent version 2.6.3 and later.

The Dynamic Engines (Behavioral AI) mode becomes active after you or the end-user restart the endpoint. In the Management Console, the endpoint status is **Pending Reboot** until it restarts.

If necessary, you can [disable the On Write or On Execute modes \[106\]](#) to use only part of the SentinelOne functionality. This is not recommended as it decreases security.

## Policy Engines by OS

Each policy shows all the engines that Agents can use. Some engines are supported on some operating systems but not on others. You can assign a policy to a group of Agents with mixed operating systems. There is no impact (and no message) if engines that some of the Agents cannot use are enabled.

Name	Windows	macOS	Linux 2.6	Linux 3.0
Reputation	✓	✓	✓	✓
DFI (Deep File Inspection)	✓	✓	✓	✓
DFI - Suspicious	✓			✓
DBT - Executables	✓	✓	✓	✓
Documents, Scripts	✓			
Lateral Movement	✓			
Anti Exploitation / Fileless	✓	✓		
Potentially unwanted applications		✓		
Detect Interactive Threat (Advanced Mode)	✓			

## 8.4. Agent Configuration Settings [Multi-Site]

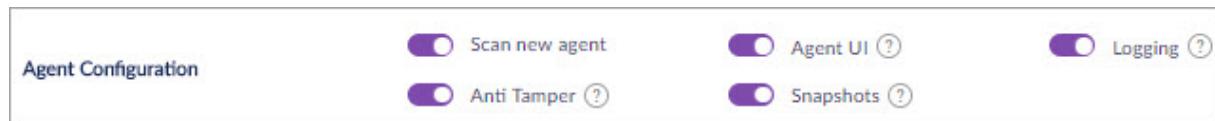
**Management:** Central Park, Denali, Eiffel, Fuji, Grand Canyon, Houston

**Agents:** Windows 2.6+ | macOS 2.6+ | Linux 2.6 SP2+

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

Use these options to configure Agent behavior on installation.



### Agent Configuration Settings

Setting	Description	Supported OS
Scan new Agents	Agents run a Full Disk Scan when they first connect to the Management.	Windows macOS Linux
Anti Tamper	Do not allow end-users or malware to change, uninstall, or disable the Agent. Best practice is to leave this on.	Windows macOS
Agent UI	Show the Agent tray icon, application, and alerts on endpoints. If disabled, end-users see no trace of the Agent.	Windows macOS
Snapshots	Keep VSS snapshots for rollback. If disabled, rollback is not available. Best practice is to leave this on.	Windows
Logging	Save logs for troubleshooting and Support. Best practice is to leave this on.	Windows

If you have the *Complete SKU*, these settings also show:

- **Deep Visibility Configuration** - [Enable Deep Visibility](#) Indicator of Compromise (IOC) searches and Threat Hunting and [select the data](#) to be sent in the **Deep visibility Configuration** area.
- **Remote Shell** - [Enable Remote Shell](#) capabilities for Agents that get this policy. Admins must have Remote Shell permissions configured to start a Remote Shell session.

## 8.5. Controlling On Write or On Execute [Multi-Site]

**Management:** Central Park, Denali, Eiffel, Fuji, Grand Canyon, Houston

**Agents:** Windows 2.6+ | macOS 2.6+ | Linux 3.0

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

We recommend that you use all of our [Policy Engines \[103\]](#) to maximize security. If necessary, you can disable the **On Write** or **On Execute** modes to use only part of the SentinelOne functionality.

## Disabling on Execute

**IMPORTANT:** This configuration is not recommended as it disables all behavioral detection and decreases security.

### Use Cases:

- For systems where saving resources is critical and the attack surface is controlled, for example, when there is limited internet access.
- For endpoints with limited disk space or memory requirements, like thin agents, or ATMs.

### Behavior:

If you disable **On Execute**, the Behavioral AI engines do not monitor On Execute behavior. The engines can be completely disabled (do not consume resources), or suppressed (monitor without alerts and consume some resources).

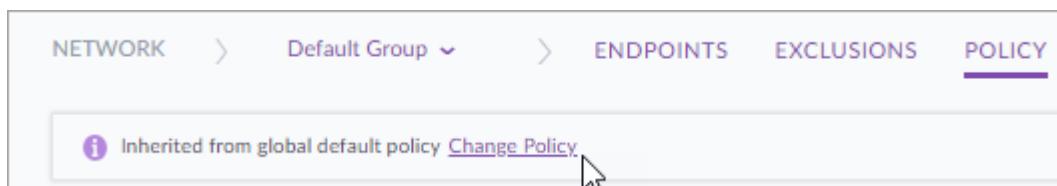
- **To completely disable Behavioral AI engines** - You must disable On Execute mode from the policy before it is ever enabled (immediately after installation, before reboot).
- **If the On Execute mode was already on** - If you disable On Execute mode in the policy after the first reboot, the Behavioral AI engines are active but suppressed. The Agents do not act on Behavioral AI detections or generate alerts, but the activity consumes some resources.

**Note:** If you enable the On-Execute engines at any time, all endpoints will be prompted to reboot and show **Pending Action** status until they reboot.

### Workflow to completely disable Behavioral AI engines:

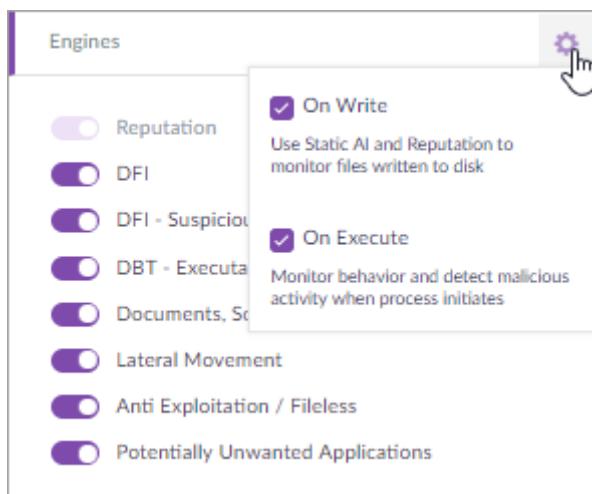
To completely disable Behavioral AI engines, the first policy that the endpoints get must already have **On Execute** disabled. You must plan for this before the Agent installation. There are two main ways to accomplish this:

- Disable **On Execute** in a Site's policy. When Agents connect to the Site for the first time with the Site Token, they will get this policy. You can then move the endpoints that need On-execute disabled to their own dynamic group and enable **On Execute** in the Site's policy.
  - Disable **On Execute** mode in a dynamic group that you prepare in advance of the Agent installation. When Agents connect to the Site that contains this group, they will get this policy.
1. Optional: In the Site that Agents will be in, disable **On Execute** in the policy.
  2. In the **Network** view, [create a filter](#) with criteria that apply to the endpoints on which you will disable On Execute mode. For example, filter for Windows Servers or for the OS of the thin clients.
  3. Click **GROUPS** and select **New Group** to [create a dynamic group](#) from the filter set.
  4. In the Group view, click **Change Policy**.



5. In the policy, disable **On Execute** mode:

- In the Engines section of a policy, click the gear button.



- Click **On Execute** to disable the mode.

6. Click **Save**.

7. Go to **Network > Group Ranking**.

- Drag the new dynamic group to the top of the list to make sure that the endpoints in it always stay in that group.
- Install Agents on the endpoints but DO NOT REBOOT.
- Open the dynamic group to make sure that all endpoints for which you want to disable On Execute mode are in the group.

If not, edit the group filters until all endpoints are included.

- Optional: Reboot the endpoints.

## Disabling On Write

**IMPORTANT:** This configuration is not recommended as it disables all Static AI detection and decreases security.

### Use Cases:

- An endpoint runs file shares
- Development stations with many executables written to disk

### Behavior:

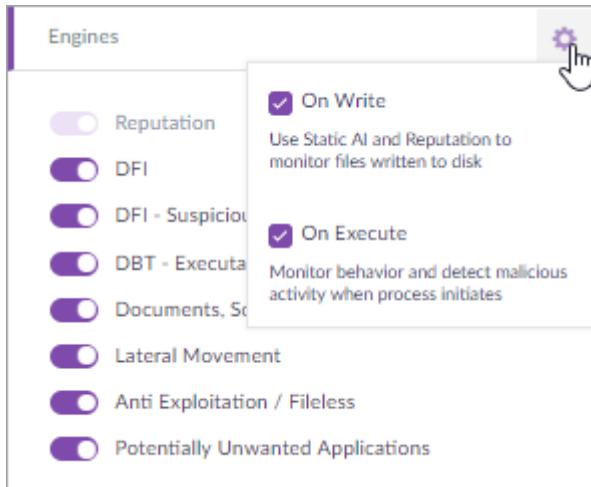
If you disable **On Write**, no action occurs when a file is copied to disk.

- No file reputation check when a file is written to the disk (the file reputation check is active on file execution).

- Deep File Inspection Static AI is disabled.
- Full Disk Scan is supported. The required service is active only during the scan.

## To manually disable On Write or On Execute mode:

1. In the Engines section of a policy, click the gear button.



2. Click **On Write** or **On Execute** to enable or disable the mode.
3. Save the policy.

## 8.6. Policy Mode Best Practices

We gathered best practices for policy management from SentinelOne experts and from our wide global install base. Best practices depend on why, how, and when you use policies.

**Important!** Manual judgment is required, based on your organization's culture, requirements, regulation compliance, and other proprietary factors. Keep in mind your Risk Level Management processes, as you balance your policies between security automation and performance.

### Definitions

Detect	Policy setting that determines Agent action: Send alerts, block execution of threats known to the Cloud Intelligence Service or Blacklist, but do not automatically mitigate with more actions.
Policy	Set of mitigation actions that defines the behavior of SentinelOne Agents and their <a href="#">detection engines</a> .
Protect	Policy setting that determines Agent action: Automatically mitigate malware with process kill (for known and unknown threats), file quarantine, and (if required) remediate or rollback, and then send Mitigated Threat alerts.  Note: If a benign detection is quarantined, you can unquarantine it in a <a href="#">multi-site console</a> or an <a href="#">earlier console</a> .
Suspicious	Detection result with a <b>low confidence</b> rating of being malicious, based on Agent detection engines, and a readiness level of <b>Validate</b> ,

usually requires manual analysis. The file or process behaves in a way that indicates it does or can do harm, or sets up child processes to do harm in the future.

Threat	Detection result with a <b>high confidence</b> rating and a readiness level of <b>Mitigate</b> .
--------	--

## Best Practices for Policy Mode Settings

Policy Mode Setting	Results
<b>Threats - Protect</b> <b>Suspicious - Detect</b>	<p><b>What to expect?</b>          (Default Policy) The Agent automatically mitigates threats with process kill and file quarantine. For suspicious detections, the Agent sends <b>Suspicious Activity</b> alerts without automatic mitigation.</p> <p><b>Risk Level:</b>          Medium. This policy is a balance between automatic mitigation of high-confidence threats and undisturbed business activity and performance, that could be interrupted if false-positives are blocked.</p> <p><b>When to use?</b>          This is the default recommended policy mode for mass deployments. It is the most popular with the SentinelOne install base.</p>
<b>Threats - Protect</b> <b>Suspicious - Protect</b>	<p><b>What to expect?</b>          All threats and suspicious activities are automatically mitigated.</p> <p><b>Risk Level:</b>          Low. Complete security automation.</p> <p><b>When to use?</b>          This policy can be relevant in different scenarios, such as:</p> <ul style="list-style-type: none"> <li>• Organizations that lack analyst headcount to manually handle all threats. The impact is the possibility of false-positives that would automatically block and quarantine benign events and applications.</li> <li>• Organizations with many endpoints that are constantly exposed to risk, such as a professional services group of users that connect daily to client environments with unknown risk.</li> <li>• Early adopter organizations with limited deployment. The impact is the need to search for false-positives and adjust to the default policy if endpoint performance is impacted.</li> </ul>

Policy Mode Setting	Results
<b>Threats - Detect</b> <b>Suspicious - Detect</b>	<p><b>What to expect?</b>  All malicious activities create <b>Active Threat</b> or <b>Suspicious Activity</b> alerts but no mitigation occurs.</p> <p><b>Note:</b> In Windows Agent versions earlier than 3.1, the Agent blocks execution of threats that are known by Cloud Intelligence Service or on your blacklist. In Windows Agent versions 3.1 and later, and all macOS and Linux versions, no execution is blocked when in Detect mode.</p> <p><b>Risk Level:</b>  High. Threats of all kinds will execute until you manually mitigate them.</p> <p><b>When to use?</b>  This is not recommended as an organization-wide long-term policy. The implied Risk Level is too high, and the benefits of an autonomous Agent that can prevent threats are not enabled. You can consider a Detect/Detect policy for endpoints with very high sensitivity to business process interrupts, such as production floor servers. But we recommend that you use this policy for a limited learning phase. This gives you the opportunity to closely monitor false-positive indications and resolve actual FPs with best-practice exclusions.</p>

#### A Common Use Case:

- The majority of endpoints get the default Protect/Detect policy.
- The server that manages the assembly line gets a Detect/Detect policy.
- A small group of endpoints that test the latest version of the Agent get a Protect/Protect policy for a limited time, to benchmark the false-positive ratio.

Show Me video: How to Create a Policy

## 9. Managing Endpoint Filters and Groups [Multi-Site]

**Management:** Central Park, Denali, Eiffel, Fuji, Grand Canyon, Houston

**Agents:** Windows 2.6+ | macOS 2.6+ | Linux 2.6+

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

Watch: [How to use Filters and Dynamic Groups in the Multi-Site Management Console](#)

In the Network view of the Management Console, you can:

- See your endpoints and their basic details.
- Filter [114] and search to find endpoints.
- Organize [118] endpoints into dynamic and static groups.
- Run **Actions** on endpoints.
- Select which columns show and sort the columns.

You can customize the columns that show to see different characteristics of the endpoints.

- Export [124] all network endpoint information for each endpoint in the current filter (up to 20,000 endpoints) in CSV format.

### Customizing your Network View

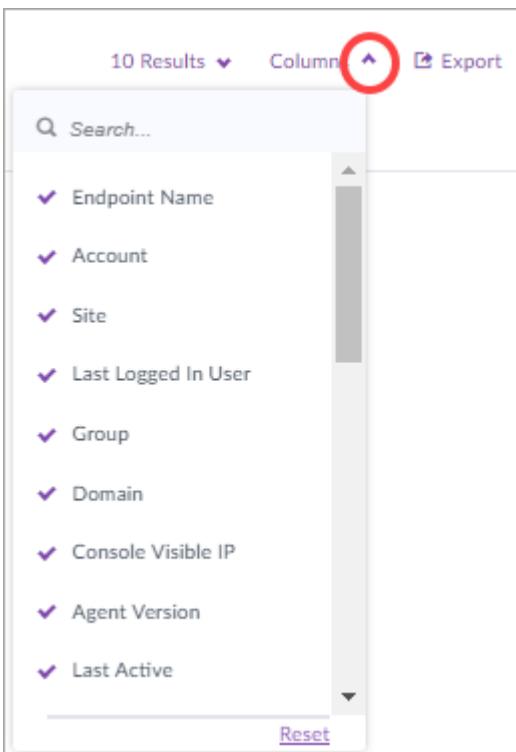
- **Tip:** From version Grand Canyon, you can drag and drop the columns in the **Network** to change the order and customize your view.
- **To sort the list by the data of a column:**

Click the arrow in the column header.

<input type="checkbox"/>	Endpoints Name	Site
<input type="checkbox"/>	BRABAX-01	Andreasb-site

- **To change which columns show:**

1. In the sidebar, click **Network** .
2. Click **Columns**.



3. Scroll through the list to select or deselect the properties.

The changed columns show on the page.

4. Click outside of the list to close it.

If necessary, scroll horizontally to see more columns in the view.

- **To revert to the default columns:**

1. In **Network**, click **Columns**.
2. At the bottom of the list, click **Reset**.

The changed columns show on the page.

**These details show by default:**

- **Endpoint Name** - Name of the protected device
- **Site** - The Site that the endpoint belongs to
- **Account** - The Account that the endpoint belongs to
- **Last Logged in User** - Name of the user that logged in most recently
- **Group** - Group that the endpoint belongs to
- **Domain** - Network domain that the endpoint belongs to
- **Console Visible IP** - External IP address of the Agent
- **Agent Version** - Version of the installed Agent

- **Last Active** - When the Agent last connected to the Management
- **Memory** - Amount of physical RAM
- **CPU count** - Number of CPUs

**These details are also available:**

- **Subscribed on** - First date and time that the agent connected to the management server
- **Health status** - Healthy or Infected
- **Device type** - Laptop, Desktop, Server
- **OS** - Operating System
- **OS Version** - Exact OS version, for example *Windows 10 (14393)* (from Grand Canyon)
- **Architecture** - 64 bit or 32 bit
- **MAC address** - Physical MAC address
- **Management connectivity** - Online or Offline
- **Network Status** - Is **Disconnect from Network** enabled or disabled
- **Update status** - Shows **Up to date** if the agent is using the latest version
- **Scan Status** - When the last scan was completed
- **IP addresses** - Internal IP addresses
- **Pending requests** - For example, pending uninstall requests
- **Disk Encryption** - On or Off
- **Vulnerability Status** - For Complete SKU only, shows if patches are required.
- **Console Migration Status** - Usually **N/A**. If an admin tries to migrate an Agent between Management Consoles, will show **Failed**, **Pending**, or **Migrated**.

## 9.1. Creating Filters in Network [Multi-Site]

**Management:** Central Park, Denali, Eiffel, Fuji, Grand Canyon, Houston

**Agents:** Windows 2.6+ | macOS 2.6+ | Linux 2.6+

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

Watch: [How to use Filters and Dynamic Groups in the Multi-Site Management Console](#)

Select one or more **Filters** to find endpoints that match specific criteria. You can:

- Use the filtered results to run actions on matching Agents.

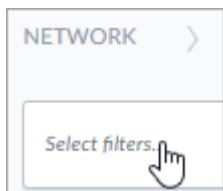
- Create a Dynamic group based on the filters (when one Site is selected).
- Save Filters as a Filter Set

Examples of filters:

- A filter for infected endpoints, to isolate them and mitigate issues.
- A filter for Agents that have pending actions.
- A filter for endpoints of an operating system, to track compliance and OS upgrades.

## To create a filter:

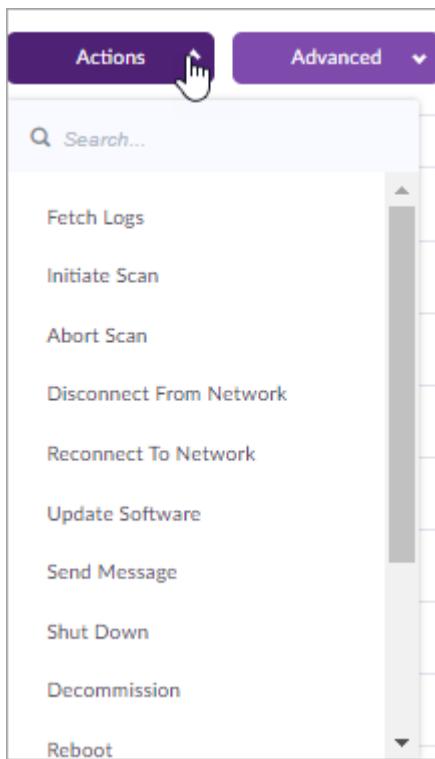
1. In the sidebar, click **Scope**  and select a scope.
2. In the sidebar, click **Network** .
3. Click **Select Filters**.



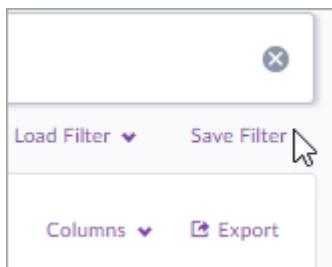
The filtering categories and options show. The number next to an option is the number of matched endpoints.

Select filters...											
<input type="button" value="Select filters..."/> Free text search... <input type="text" value="Type your search..."/> <small>Free text search on Agent's network computer name, IP &amp; Mac addresses, Domain and Group names, agent version and users</small>											
OS	Version	Type	Domain	Connected to Management	Health status	Network status	Pending actions	Scan status			
Windows	6	1 Unknown	local	1 No	5 Healthy	7 Connecting	Missing permission	In progress			
macOS	1	2.6.15880	WORKGROUP	5 Yes	2 Infected	7 Connected	N/A				
Linux	2.5.4.104	4 Laptop	BLUPP	1	3 Disconnected	7 Disconnecting	Reboot	Completed			
Windows Legacy	2.6.0.2494	1 Server		1 Desktop	7		Agent suppressed	Aborted			

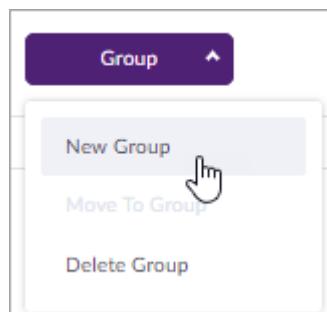
4. Select values from the categories.
5. Use the filter results:
  - Select one or more endpoints from the results, click **Actions**, and select an action to do.



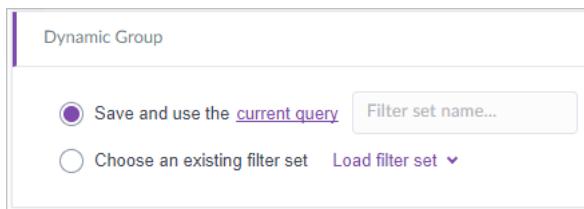
- Save a filter set. Click **Save Filter** (in earlier versions this option was called **Save New Set**).



- Make a Dynamic group (you must be in one Site to see **Group** options):
  - a. Click **Group > New Group**.



- b. In the Add New Group wizard, enter a name for the group.
- c. In the Group Type step, select **Dynamic Group**.
- d. In the next step, save the filter set with a new name.

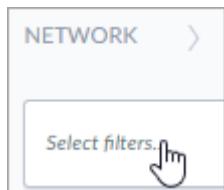


**If you create filters to make a Dynamic group, you cannot use these filter categories:**

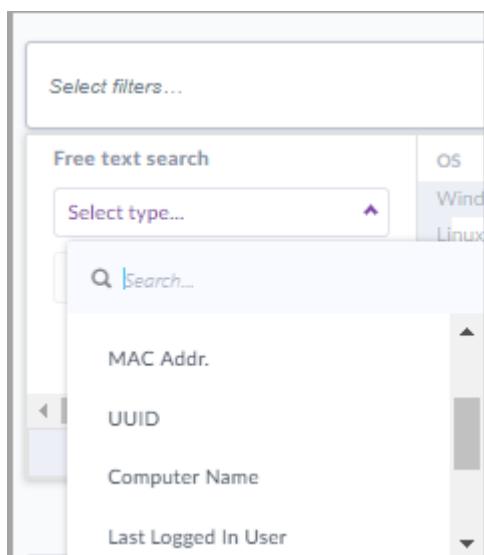
- Network status
- Pending uninstall
- Pending actions
- Update status
- Scan status
- Management connectivity
- Health status
- Group
- Last online

**To use the free text search:**

1. In **Network**, click **Select Filters**.



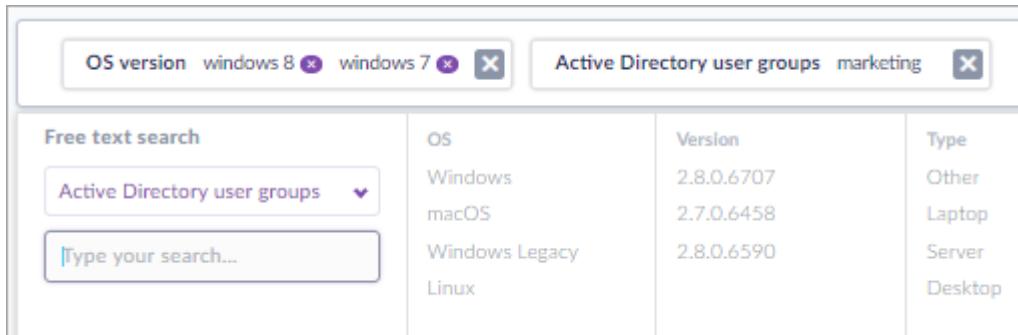
2. Under **Free text search**, select the **type** of information to search for.



- Enter the strings to search for.

You can include multiple strings and types in the same search. If you have more than one of the same **type**, the Management Console filters for one OR the other.

In this example, the Management Console filters for endpoints of Windows 7 OR 8, AND endpoints in the AD user group called "marketing".

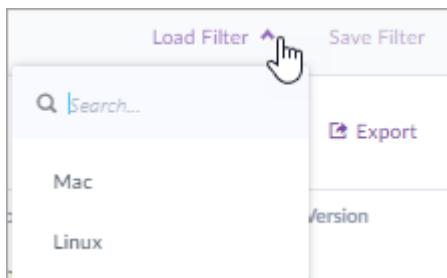


OS version windows 8		Active Directory user groups marketing	
OS	Version	Type	
Windows	2.8.0.6707	Other	
macOS	2.7.0.6458	Laptop	
Windows Legacy	2.8.0.6590	Server	
Linux	2.8.0.6590	Desktop	

- Press Enter.

### To load a filter set:

- In **Network**, click **Load Filter**.



- Select a saved filter set.

## 9.2. Creating Groups [Multi-Site]

**Management:** Central Park, Denali, Eiffel, Fuji, Grand Canyon, Houston

**Agents:** Windows 2.6+ | macOS 2.6+ | Linux 2.6+

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

Watch: [How to use Filters and Dynamic Groups in the Multi-Site Management Console](#)

Organize Agents of a Site in Groups to manage Agents easily and consistently. A Group has one policy and shared exclusions. For example, you can create a Group of all endpoints of one operating system version, to update all the Agents in one command.

Agents belong to a specific Site. An Agent can be in one Group. Therefore, a Group can be in only one Site.

- *DynamicGroups* are based on [filters \[114\]](#). Endpoints that match the criteria of the filters are automatically added to the Group. If an Agent fits in more than one Dynamic Group, the conflict is resolved by **Group Ranking**.

**Best Practice:** To create a Dynamic Group, first save the filter set.

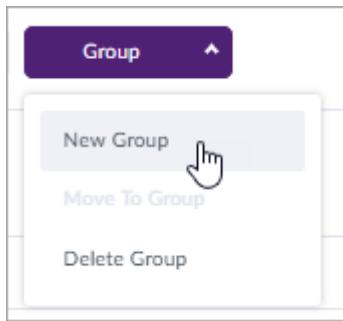
- *Static Groups* are based on manual selection. If an endpoint is in a Static Group, and the filters of a Dynamic Group match it, the endpoint is automatically moved to the Dynamic Group.

## To create a Group:

1. In the sidebar, click **Scope**  and select a scope.

You must select a Site.

2. In the sidebar, click **Network** .
3. Click **Group > New Group**.



The **Add New Group** wizard opens.

4. In **Group Name**, enter a descriptive name for the group. The name must be unique in the Site. Click **Next**.
5. In **Group Type**, select **Static Group** or **Dynamic Group**.



**Static Group**

Static groups are based on manual selection. Agents in a static group that match the filters of a dynamic group are automatically moved to the dynamic group.

**Select**

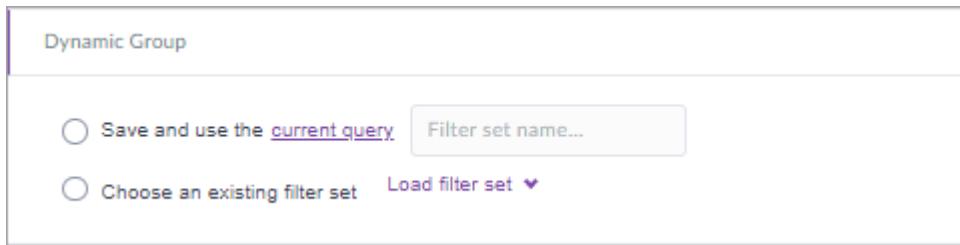


**Dynamic Group**

Dynamic groups are based on filters. Agents that match the criteria of the filters are automatically added to the group.

**Select**

6. If you select **Dynamic Group**, select the filter set. Click **Next**.



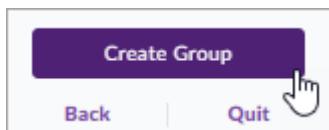
- In **Group Policy**, see the settings of the inherited policy.

If the Site has a policy, the Group inherits the Site policy settings. If the Site uses the Global default policy, the group inherits the Global policy settings.

If you want this group to have a different policy, click **Change Policy**, change the settings, and click **Save**.

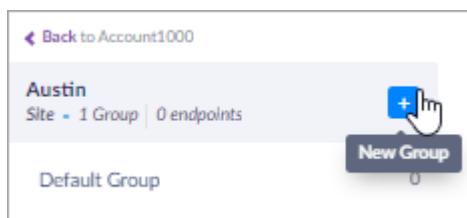


- Scroll down and click **Create Group**.



- Click **Done**.

**Note:** From Grand Canyon SP3, you can also create a new Group from the scope pane: stand on a Group and click +.



### 9.3. Editing a Group [Multi-Site]

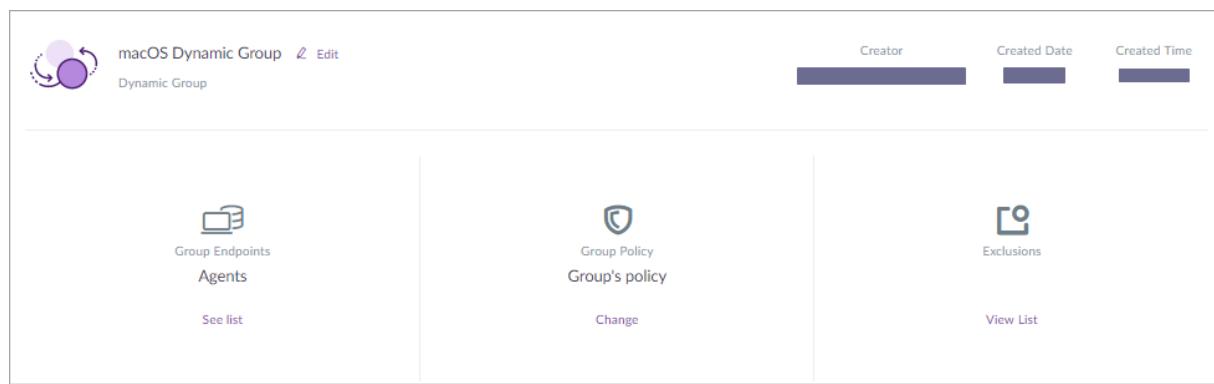
**Management:** Central Park, Denali, Eiffel, Fuji, Grand Canyon, Houston

**Agents:** Windows 2.6+ | macOS 2.6+ | Linux 2.6+

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

Edit a Group from the **Group Info** page to change its name, filter, or policy.



## To edit a Group:

1. In the sidebar, click **Scope**  and select a scope.

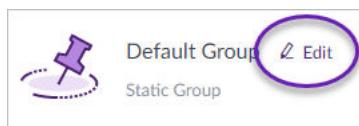
You must select a Group.

2. In the sidebar, click **Network** .
3. In the **Network** toolbar, click **Group Info**.

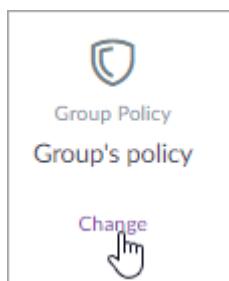


The details of the Group show.

4. To change the Group name: click **Edit**, enter the new name, and click **Save**.

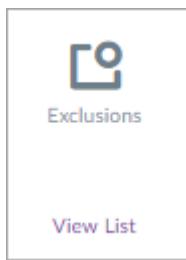


5. To change the policy of the group, under **Group Policy**, click **Change**.



- If the Group uses its own policy, it is open for changes. When you make a change, the **Save** button shows.
- If the Group uses the Global, Account or Site policy, and you want to change it, click **Change Policy**.

6. To change the exclusions of the Group, under **Exclusions**, click **View List**.



- To change the filter that a Dynamic Group uses, under **Dynamic Group is based on this filter**, select a different saved filter set.

## 9.4. Ranking Dynamic Groups [Multi-Site]

**Management:** Central Park, Denali, Eiffel, Fuji, Grand Canyon, Houston

**Agents:** Windows 2.6+ | macOS 2.6+ | Linux 2.6+

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site

Use **Group Ranking** to set the priority of Dynamic Groups for Agents. An Agent can belong to only one Group. If the Agent matches multiple Dynamic Groups, it goes to the Group with the highest rank.

If an endpoint is in a Static Group, and the filters of a Dynamic Group match it, the endpoint is automatically moved to the Dynamic Group.

### To change the priority of a Dynamic Group:

- In the sidebar, click **Scope** and select a scope.

You must select a Site.

- In the sidebar, click **Network** .
- In the Network toolbar, click **Group Ranking**.



- Drag Groups up or down to change their priority.
- Click **Save**.

## 9.5. Moving Agents between Static Groups [Multi-Site]

**Management:** Central Park, Denali, Eiffel, Fuji, Grand Canyon, Houston

**Agents:** Windows 2.6+ | macOS 2.6+ | Linux 2.6+

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site

You can add Agents to a Static Group and remove Agents from a Static Group. You can move an Agent from one Static Group to a different Static Group.

If you remove an Agent from a Static Group and do not put it in a different Group, it automatically moves to the Default Group.

You cannot manually add or remove Agents to or from Dynamic Groups.

### To move Agents from one Static Group to a different Static Group:

1. In the sidebar, click **Scope**  and select a scope.

You must select a Site.

2. In the sidebar, click **Network** .
3. Select Agents of the Site that are not assigned to Dynamic Groups.
4. Click **Group** and then select **Move to Group**.
5. Select a different Group for the Agents.
6. Click **Save**.

## 9.6. Deleting a Group [Multi-Site]

**Management:** Central Park, Denali, Eiffel, Fuji, Grand Canyon, Houston

**Agents:** Windows 2.6+ | macOS 2.6+ | Linux 2.6+

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site

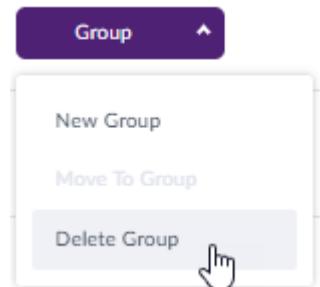
You can delete Groups if you do not need them. If you delete a Dynamic Group, its Agents move to the next Dynamic Group in the ranks. If the Agents do not fit a different Dynamic Group, or if you delete a Static Group, the Agents move to the **Default** Group.

### To delete a Group:

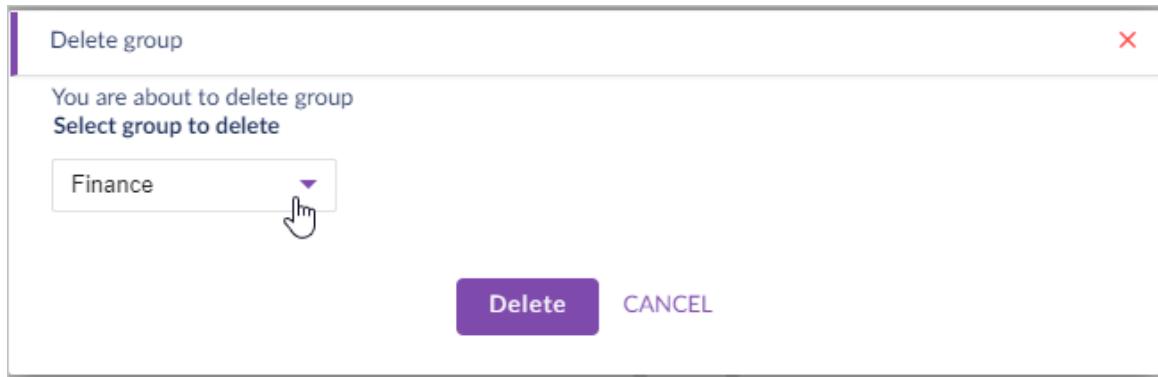
1. In the sidebar, click **Scope**  and select a scope.

You must select a Site.

2. In the sidebar, click **Network** .
3. Click **Group > Delete Group**.



4. In the **Delete Group** window, select a group.



5. Click **Delete**.

## 9.7. Exporting Endpoint Data

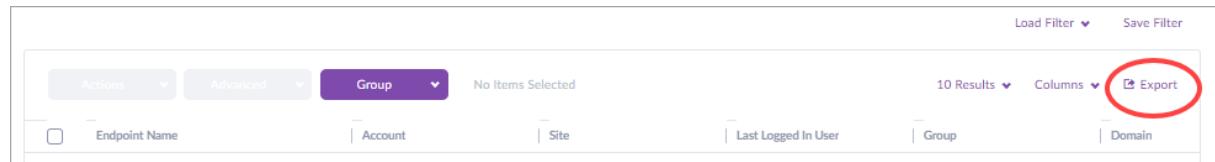
**Management:** Fuji, Grand Canyon, Houston

**Agents:** Windows 2.6+ | macOS 2.6+ | Linux 2.6+

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

From Fuji SP2, an **Export** option shows in the **Network** view. It exports all network endpoint information for each endpoint in the current filter (up to 10,000 endpoints) in CSV format.



### To export selected endpoint information:

1. In the sidebar, click **Scope**  and select a scope.
2. In the sidebar, click **Network** .
3. Optional: Search or filter to show specific endpoints.
4. Click **Export**.

The CSV file downloads to your default downloads folder.

## 10. Managing the Blacklist [Multi-Site]

**Management:** Central Park, Denali, Eiffel, Fuji, Grand Canyon, Houston

**Agents:** Windows 2.6+ | macOS 2.6+ | Linux 2.6+

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

SentinelOne Agents immediately identify files on the blacklist and block them from executing, based on the policy. Files on the blacklist are defined by their SHA1 hash. Agents identify files on the blacklist before they look at exclusions.

### Blacklist Hierarchy

- Sites, Accounts, and Global can each have their own blacklist items.
- From version Houston, Groups can also have their own blacklist items.
- Each scope also inherits blacklist items from the scopes above it.
  - An Account inherits all Global blacklist items.
  - A Site inherits all blacklist items of its Account, and all Global blacklist items.
  - A Group inherits all blacklist items of its Site, Account, and all Global blacklist items.

Watch: [Scope Hierarchy with Exclusions and Blacklists in the SentinelOne Management Console](#)

### To see blacklist items:

1. In the sidebar, click **Scope**  and select a scope.
2. In the sidebar, click **Network** .
3. In the **Network** toolbar, click **Blacklist**.



You see the blacklist of the selected scope. For example, if you are a Site Admin, you see the blacklist items of your Site.

The screenshot shows the Blacklist view for the Site scope. It displays two entries for Windows OS files. The columns are labeled: OS (checkbox), Hash (checkbox), Description (text input), Last Update (dropdown), and Scope (dropdown). The Scope dropdown is set to "Site". A red circle highlights the "Scope" column header.

OS	Hash	Description	Last Update	Scope
Windows	SHA1 Hash 1	File 1	2023-01-01	Site
Windows	SHA1 Hash 2	File 2	2023-01-02	Site

4. To see blacklist items that are inherited from the Account and the Global blacklist, click **Include global list results**.

	Add new	Delete selection								<input checked="" type="checkbox"/> Include global list results
	OS	Hash		Description	Last Update			Scope		
								Global		
								Global		

## 10.1. Adding a Hash to the Blacklist [Multi-Site]

**Management:** Central Park, Denali, Eiffel, Fuji, Grand Canyon, Houston

**Agents:** Windows 2.6+ | macOS 2.6+ | Linux 2.6+

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

Watch: [How to Add Hashes to the Blacklist](#)

You can add a hash to the blacklist manually, or add it to the blacklist automatically after it shows in your Management Console.

**Best Practice:** Always analyze a threat before you add the file to the blacklist.

**Note:** Items that you add to the blacklist do *not* automatically become *resolved*. When you finish investigating and handling a threat or detection, mark it as resolved.

### Scope of blacklist items:

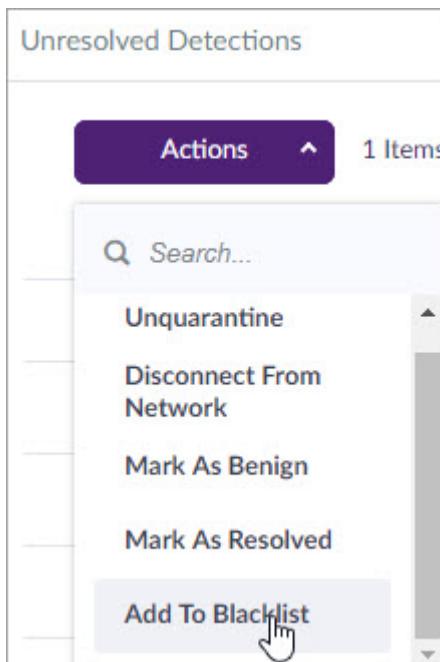
- Blacklist items apply to the scope you are in when you create them.
- For example, if you add a file to the blacklist from a Site, it goes in the Site blacklist.

### To add a file to the blacklist after it is marked as suspicious or a threat:

1. In the sidebar, click **Analyze**.
2. Select a threat or suspicious item.



3. Click **Actions** and select **Add to blacklist**.

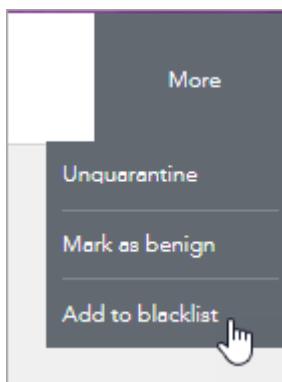


If the selected detection is **Suspicious**, select **Mark as Threat** to add the item to the blacklist and mark it as a threat.

4. In the window that shows, click **YES**.
5. If relevant, an option shows to select the scope of the blacklist item. Select a scope.

#### To add a file to the blacklist after threat investigation:

1. In the Management Console, click a threat in **Dashboard** or **Analyze**.
2. In the Forensics details that open, click **More** and select **Add to blacklist**.



If the selected detection is **Suspicious**, select **Mark as Threat** to add the item to the blacklist and mark it as a threat.

3. In the window that opens, confirm the action.

#### To add a file to the blacklist before it enters your network:

To add a file to the blacklist before it enters your network, you must know the SHA1 hash.

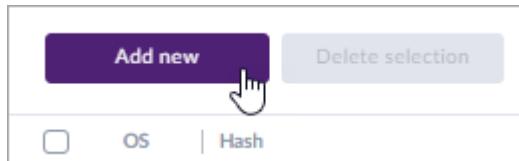
1. In the sidebar, click **Scope**  and select a scope.

2. In the sidebar, click **Network** .

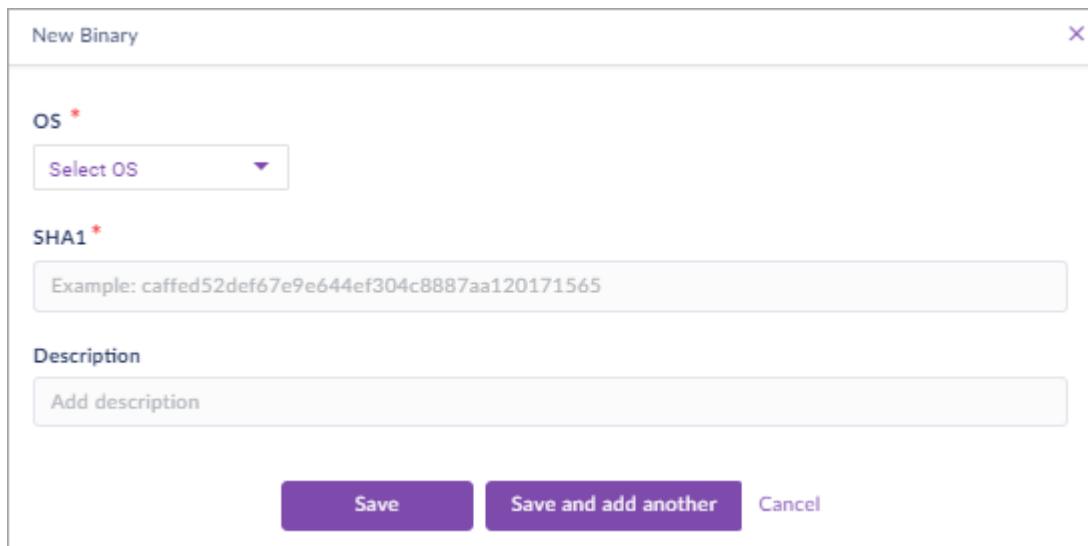
3. In the **Network** toolbar, click **Blacklist**.



4. Click **Add new**.



5. In the window that opens:



A screenshot of the 'New Binary' configuration dialog box. It contains three fields: 'OS \*' with a dropdown menu labeled 'Select OS', 'SHA1 \*' with a text input field containing the placeholder 'Example: caffed52def67e9e644ef304c8887aa120171565', and 'Description' with a text input field labeled 'Add description'. At the bottom are three buttons: 'Save' (purple), 'Save and add another' (purple), and 'Cancel' (light blue).

a. In **OS**, select the OS that this file will be blocked on.

b. In **SHA1**, enter the SHA1 hash.

c. In **Description**, enter a phrase to make it easy for you and other console users to identify this file.

6. Click **Save**.

# 11. Managing Exclusions [Multi-Site]

**Management:** Central Park, Denali, Eiffel, Fuji, Grand Canyon, Houston

**Agents:** Windows 2.6+ | macOS 2.6+ | Linux 2.6+

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

Agents sometimes mark benign items as potential threats. You can configure Exclusions to make your Agents suppress alerts and mitigation for these items.

See also [Creating a Path Exclusion \[Multi-Site\] \[134\]](#).

Watch: [Scope Hierarchy with Exclusions and Blacklists in the SentinelOne Management Console](#)

Watch: [How to work with Exclusions in the Multi-Site Console](#)

## Exclusion Hierarchy

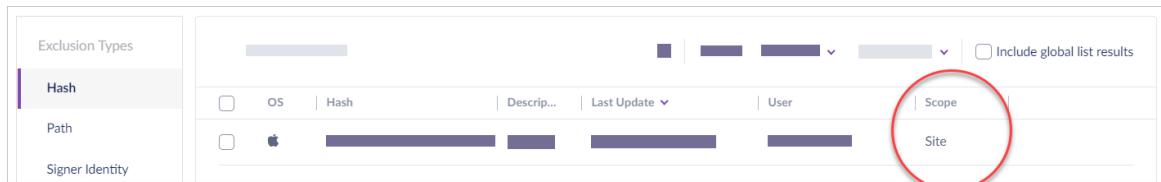
- Groups, Sites, Accounts, and Global can each have their own exclusions.
- Each scope also inherits exclusions from the scopes above it.
  - An Account inherits the Global exclusions.
  - A Site inherits the exclusions of its Account, and the Global exclusions.
  - A Group inherits the exclusions of its Site, its Account, and the Global exclusions.

## To see exclusions:

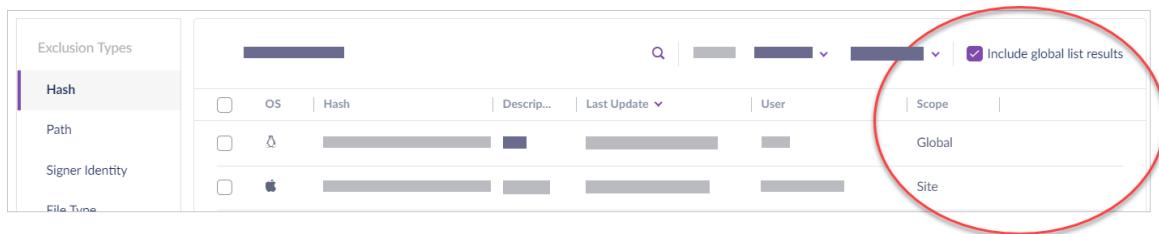
- In the sidebar, click **Scope**  and select a scope.
- In the sidebar, click **Network** .
- In the **Network** toolbar, click **Exclusions**.



The first exclusions are of the selected scope. For example, if you are a Site Admin, and you do not select a specific Group in the scope, you see the exclusions of your Site.



- To see exclusions that are inherited from the Account and the Global exclusions, click **Include global list results**.



## IMPORTANT

Be careful! If you create incorrect exclusions, you can open your environment to malware.

Also see [Best Practices for Exclusions](#) and [Not Recommended Exclusions](#).

You can create these types of exclusions: hash, path, certificate signer, file type, and browser.

**Note:** There are different modes of [Path type exclusions \[134\]](#). The options in version Eiffel and higher are different than in earlier versions.

### 11.1. Creating Exclusions [Multi-Site]

**Management:** Central Park, Denali, Eiffel, Fuji, Grand Canyon, Houston

**Agents:** Windows 2.6+ | macOS 2.6+ | Linux 2.6+

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

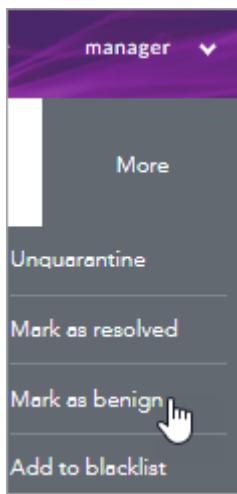
Watch: [How to work with Exclusions in the Multi-Site Console](#)

Create exclusions for a specified scope: Global, Account, Site, or Group.

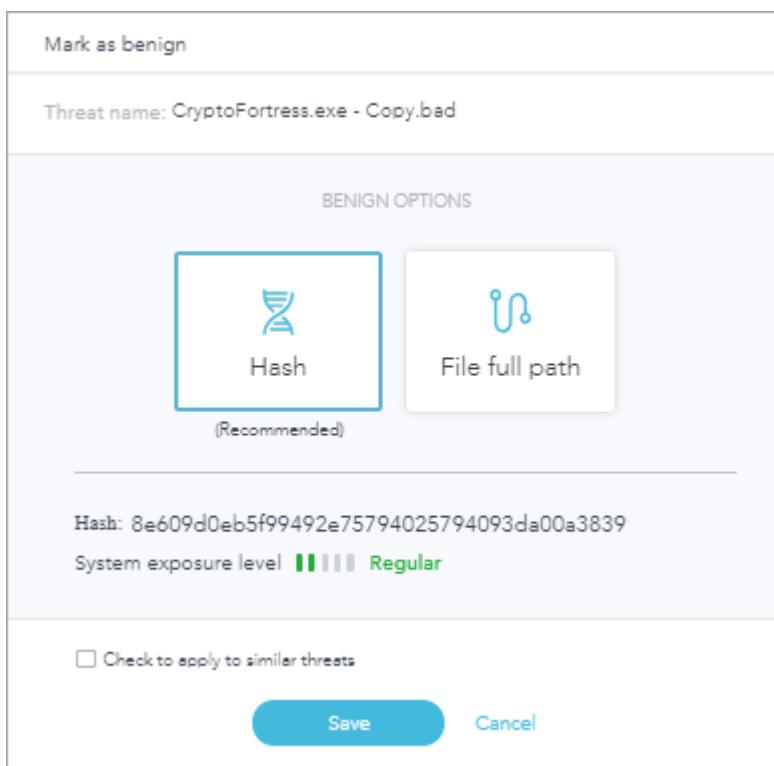
**Note:** For exclusions for interoperability or performance issues, see [Making a Path Exclusion \[134\]](#).

#### To add an exclusion automatically after threat analysis:

1. In the sidebar, click **Analyze**
  2. Click a threat.
- The Forensics details open.
3. Click **More > Mark as benign**.



- In the window that opens, select the type of exclusion to create.



- If you select **Check to apply to similar threats**, all threats with the same hash are marked as benign.
- Click **Save**.

**To add exclusions manually, see:**

- Creating a Path Exclusion [134] (Also for interoperability or performance issues)
- Creating a Hash Exclusion
- Excluding a File Type

- Excluding a Signer Identity (Certificate)
- Excluding a Browser
- Best Practices for Exclusions [143]

## 11.2. Creating a Hash Exclusion [Multi-Site]

**Management:** Central Park, Denali, Eiffel, Fuji, Grand Canyon, Houston

**Agents:** Windows 2.6+ | macOS 2.6+ | Linux 2.6+

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

Exclude a file based on its SHA1 hash.

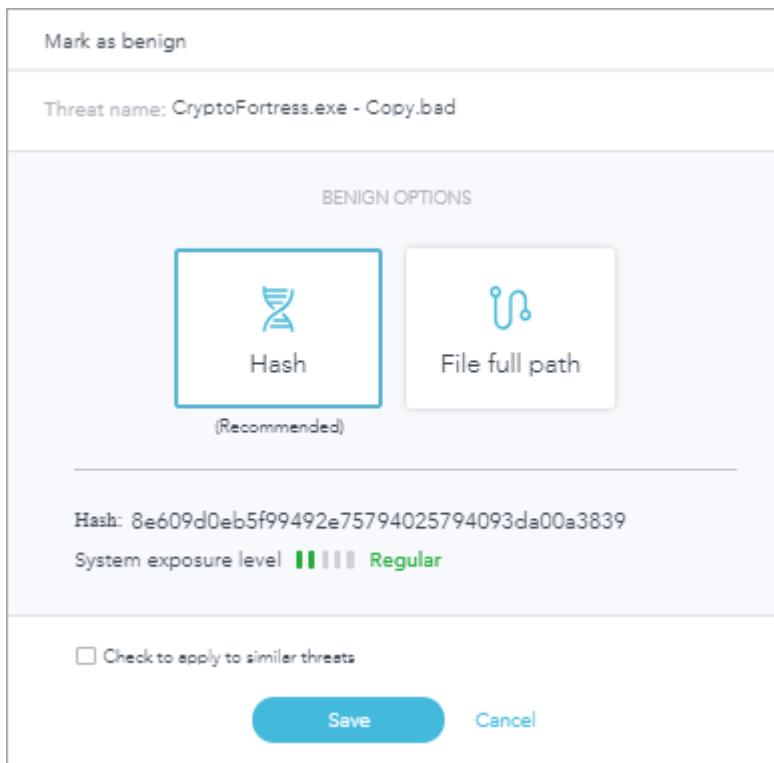
Note: Hash exclusions in Multi-Site Consoles are not supported in the Agent for Legacy Windows.

### To add a hash exclusion automatically after threat analysis:

1. In the sidebar, click **Analyze** .
2. Click **More > Mark as benign**.



3. In the window that opens, click **Hash**.



4. If you select **Check to apply to similar threats**, all threats with the same hash are marked as benign.
5. Click **Save**.

### To add a hash exclusion manually:

1. In the sidebar, click **Scope**  and select a scope.
2. In the sidebar, click **Network** .
3. In the **Network** toolbar, click **Exclusions**.



4. In **Exclusion Type**, click **Hash**.

**Note:** You only see the exclusions for the selected exclusion type. For example, If **Hash** is selected, only path exclusions show in the exclusion list. File Type exclusions are not visible at the same time.

5. Click **New exclusion**.
6. In the window that opens, enter the details of the exclusion. You can change the exclusion type here.

You must have the SHA1 hash to create the exclusion.

New Exclusion

Exclusion Type \* OS \*

Hash Select OS

SHA1 \*

Example: caffed52def67e9e644ef304c8887aa120171565

Description

Add description

Save Save and add another Cancel

7. In **Description**, enter a phrase to make it easy for you and other console users to identify this exclusion.
8. Click **Save**.

Watch: [How to work with Exclusions in the Multi-Site Console](#)

### 11.3. Creating a Path Exclusion [Multi-Site]

**Management:** Central Park, Denali, Eiffel, Fuji, Grand Canyon, Houston

**Agents:** Windows 2.6+ | macOS 2.6+ | Linux 2.6+

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

#### In this article:

- [Suppress Alerts Path Exclusions \(Default\) \[135\]](#)
- [Interoperability and Performance Focus Exclusions \(formerly No Monitor\) \[135\]](#)
- [Exclusion Modes in Detail \[135\]](#)
- [Which Exclusions work with which Agents \[136\]](#)
- [How to Exclude a Path from the Forensics of a Threat \[137\]](#)
- [How to Create a File or Folder Exclusion \(All Exclusion Modes\) \[138\]](#)

The scope of an exclusion is based on the view that you are in when you create the exclusion.

To use all path exclusions correctly, make sure to see [Best Practices for Exclusions \[143\]](#).



## IMPORTANT

Be careful! If you create incorrect exclusions, you can open your environment to malware. Consult with SentinelOne Support before you use **No monitor** or **Interoperability** or **Performance** exclusions.

Also see [Not Recommended Exclusions](#).

### **Suppress Alerts Path Exclusions (Default)**

Use default Path exclusions if you have false positive detections, and you want to suppress alerts from a file path or folder. When you exclude files or folders with default path exclusions, Agents monitor them but suppress alerts and do not mitigate.

- This exclusion type is supported for Windows, macOS, and Linux Agents.
- When you create an exclusion directly from a detection and select **File path**, this is the type of exclusion created.

**Caution:** Make sure the detection that the exclusion is based on is a false positive. Legitimate threats in the path will not be mitigated.

### **Interoperability and Performance Focus Exclusions (formerly No Monitor)**

**Interoperability** or **Performance Focus** path exclusions are sometimes necessary to resolve issues with specific files or processes. With these exclusions, Agents reduce monitoring and mitigation of the excluded items.

**Interoperability** or **Performance Focus** exclusions have more risk than **Suppress Alert** exclusions because all operations that start from or use the excluded item are not fully visible to SentinelOne Agents. This can affect mitigation if an excluded item is part of a malicious execution.

**For Interoperability and Performance Focus exclusions (formerly Do not Monitor or Do not Inject):** For processes that cannot be restarted, such as System processes or Anti-virus processes, you must reboot endpoints to apply or remove an exclusion. For processes that can be restarted, such as a browser, you can restart the process to apply or remove an exclusion. **Best Practice:** We recommend that you restart all affected endpoints to apply or remove an Interoperability or Performance Focus exclusion.

- Starting from Eiffel version Management with Windows 2.8 Agents, there are granular **Interoperability** and **Performance Focus** Exclusion modes.

### **Exclusion Modes in Detail**

To maximize security, try to resolve interoperability or performance issues with the least severe option. Try the exclusion modes in the order shown. Use the **Performance Focus** options only if the **Interoperability** options do not resolve the issues.

- **Suppress Alerts** (default Path exclusion): Do not display alerts or mitigate detections on the excluded processes.
  - More info: If the root of a threat group is suppressed, alerts for the child processes are also suppressed.

- Usage example: Stop false positives from a specific file or process.
- Caution: Make sure the detection that the exclusion is based on is a false positive. Legitimate threats in the path will not be mitigated.
- **Interoperability:** Reduce the monitoring level on the excluded processes.
  - More Info: This exclusion stops the Agent from injecting the Agent DLL to processes in the path. This reduces Agent interaction with these processes. The Agent continues to monitor and use kernel events.
  - Usage example: To solve interoperability issues related to the Agent code injection into other applications.
  - Caution: This lowers protection as it reduces events that the Agent monitors.
- **Interoperability - extended:** Reduce the monitoring level on the excluded processes and their child-processes (Same as the **Interoperability** option but includes child-processes.)
  - Usage example: To solve interoperability issues related to the Agent code injection into other applications, when the **Interoperability** option did not resolve the issue.
- **Performance Focus:** Disable monitoring of the excluded processes.
  - More info: It stops the Agent from injecting the Agent DLL to processes in the path and stops monitoring most kernel events. Agents do not use OS events that are generated by or for the excluded process.
  - Usage example: To solve issues where a specific application generates many events (like file operation, registry, process, memory) and causes a high CPU utilization on the endpoint, due to Agent event analysis.
  - Caution: This lowers protection significantly as the Agent does not monitor the excluded processes.
- **Performance Focus - extended:** Disable monitoring of the excluded processes and their child-processes. (Same as the **Performance Focus** but includes child processes.)
  - Usage example: To solve issues where a specific application generates many events due to Agent event analysis, when the Performance Focus option did not resolve the issue.

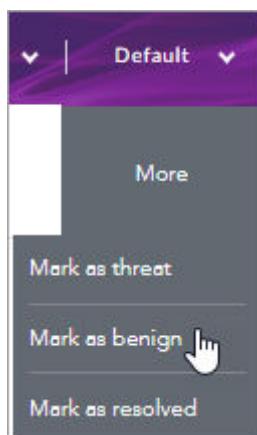
## Which Exclusions work with which Agents?

Agent	Suppress Alerts (Default)	Interoperability	Interoperability-extended	Performance Focus	Performance Focus - extended
<b>Windows 2.8 and higher</b>	Yes	Yes		Yes	Yes
<b>Windows 2.7 and lower</b>	Yes	No. Becomes Performance Focus		Yes	No. Becomes Performance Focus
<b>macOS 2.5 and higher</b>	Yes	No. Becomes Performance Focus		Yes	No. Becomes Performance Focus

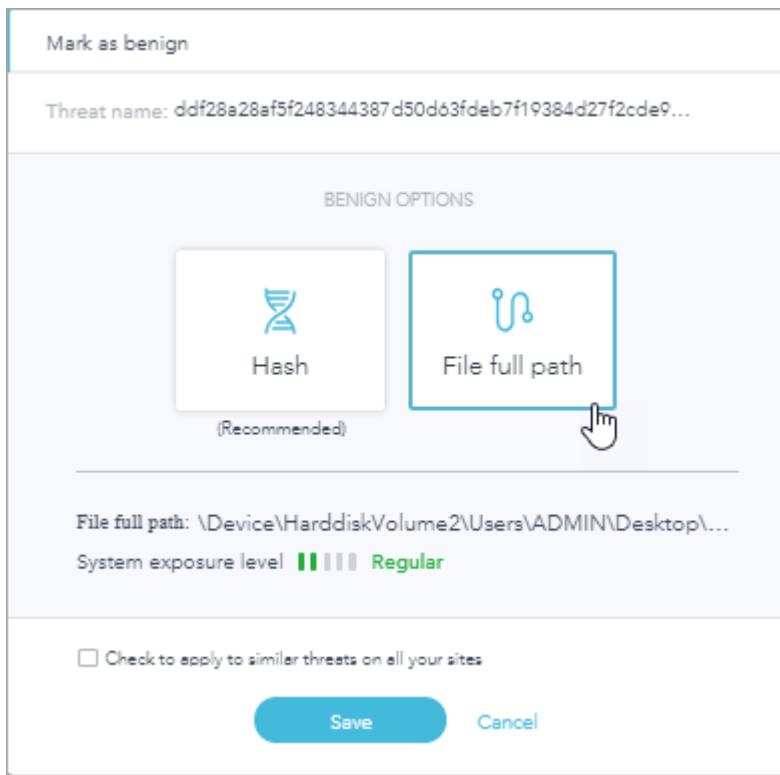
Agent	Suppress Alerts (Default)	Interoperability	Interoperability-extended	Performance Focus	Performance Focus - extended
Linux Agents (all)	Yes	No		No	No

## To exclude a path from the Forensics details of a threat:

1. In the sidebar, click **Scope**  and select a scope.
  2. In the sidebar, click **Analyze** .
  3. Click an item.
- The Forensics details opens.
4. Click **More** and select **Mark as benign**.



5. Click **File full path**.



6. Optional: Select **Check to apply to similar threats on all your sites** to do the same action for all detections related to this threat on all Sites that you administrate.
7. Click **Save**.

See the **Suppress alerts** exclusion in **Network > Exclusions > Path**.

Watch: [How to Create Path Exclusions in the SentinelOne Management Console](#)

### To create a file or folder exclusion:

1. In the sidebar, click **Scope**  and select a scope.
2. In the sidebar, click **Network** .
3. In the **Network** toolbar, click **Exclusions**.



4. In **Exclusion Type**, click **Path**.
5. Click **New Exclusion**.

The **New Exclusion** window opens.

New Exclusion

Exclusion Type \* OS \*

Path \* Windows

Path \* C:\work\

As Folder Change

Include Subfolders

Exclusions Mode More options ▾

Description Add description

Save Save and add another Cancel

6. In **OS**, select the operating system for the exclusion.
7. In **Path**, enter the full path to the folder, with these rules:

**Note:** See all rules for creating path exclusions in [Best Practices for Exclusions \[143\]](#).

#### Exclusion rules for Windows:

- The path can start with the drive letter. If the drive is not included, the exclusion applies to all drives. For example:
  - C:\calc.exe excludes CALC on the root of the C drive.
  - calc.exe excludes CALC on all directories and drives.
- If you select **Include Subfolders**, the path must end with a backslash (\).
- DO NOT USE a wildcard as the drive directory ( \*: or ?: ).

For example, do NOT use \*:\Program Files or ?:\\Program Files in an exclusion path. Instead, use \*\Program Files to exclude Program Files on all drives.

You CAN use the wildcard \* to refer to any character or characters, or the metacharacter ? to refer to one character that is NOT a drive letter.

- Examples with wildcard \* to refer to any character or characters:

C:\c\*c.exe excludes files that start with "c" and end with ".exe" on all directories and drives. This includes CALC.EXE, CAMC.EXE, CHARLIE.DOC.EXE

Example to exclude the Archives folder in a nested directory: C:\\*\Archives\

Example to exclude Go2Meeting for all users: C:\Users\\*\AppData\Local\GoToMeeting\\*\g2mlauncher.exe

- Example with metacharacter ? to refer to one character:

You CAN use: C:\test?\ to exclude C:\test1\ and C:\testf\.

Example to exclude a temp directory in all drives: harddiskvolume?\temp\

DO NOT USE ? as the drive letter. For example, do NOT use ?:\\test1\ in an exclusion path.

#### **Exclusion rules for Linux and macOS:**

- The path must be absolute: start with a forward slash (/ - ASCII char 47).
- The path must not contain a space in the beginning or end.
- If you select **Include Subfolders**, the path must end with a forward slash.
- **Linux** - Wildcards are not supported in Linux Agent versions 2.6 and earlier. They are supported in 3.0 and later, in the same manner as with the Windows Agent.
- **macOS** - The \* wildcard is supported in path exclusions.

For example:

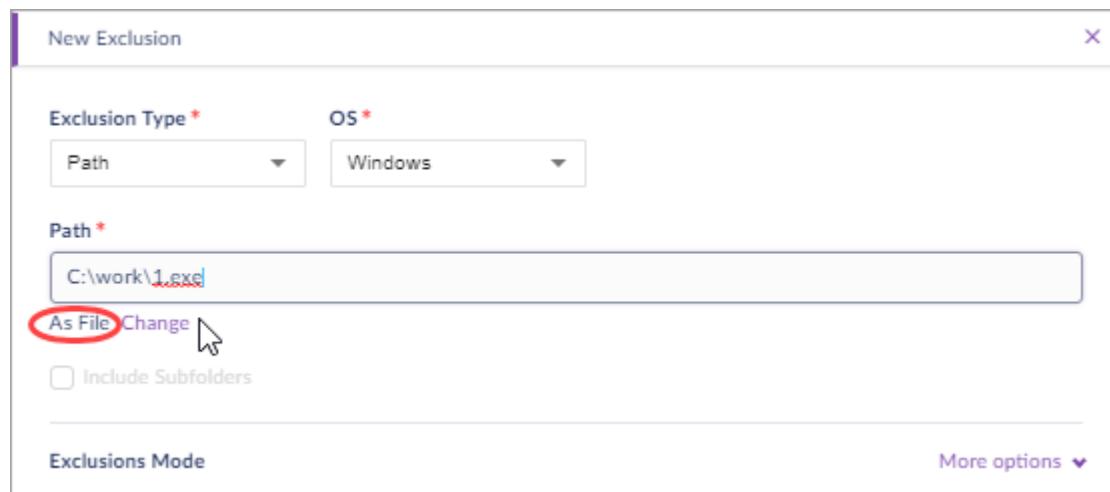
- /Users/\* /Applications/<NAME>.app/ excludes all users and app subfolders
- /Users/?\* /Desktop/<NAME>.app/ excludes all users and app subfolders and their subfolders
- /Users/<USER>/Desktop/<NAME>.app/\* excludes all files in this path.

8. After you enter a path, you see **As File** or **As Folder** next to the path.

**As File** - Only the single file is excluded (default).

**As Folder** - The whole folder at the path is excluded.

Click **Change** to switch between them.



The screenshot shows the 'New Exclusion' dialog box. At the top, there are dropdown menus for 'Exclusion Type \*' (set to 'Path') and 'OS \*' (set to 'Windows'). Below these is a 'Path \*' input field containing 'C:\work\1.xls'. To the right of the input field are two buttons: 'As File' (which is circled in red) and 'Change'. Below the input field is a checkbox for 'Include Subfolders'. At the bottom of the dialog, there are buttons for 'Exclusions Mode' and 'More options ▾'.

9. If you select **As Folder**, you can select **Include Subfolders**. This adds all the subfolders to the exclusion.

New Exclusion

Exclusion Type \* OS \*

Path Windows

Path \*

C:\work\

As Folder Change

Include Subfolders

Exclusions Mode More options ▾

The screenshot shows the 'New Exclusion' dialog box. It has fields for 'Exclusion Type' set to 'Path' and 'OS' set to 'Windows'. The 'Path' field contains 'C:\work\' and includes a link 'As Folder' which is circled in red. There is also a checked checkbox for 'Include Subfolders'. At the bottom right, there are buttons for 'Exclusions Mode' and 'More options'.

10. Select the [Exclusion Mode \[135\]](#):

**Eiffel and later:** Click **More Options**. For most exclusions, keep **Suppress Alerts** selected. To resolve interoperability issues, you will usually require a different option.

New Exclusion X

<b>Exclusion Type *</b>	<b>OS *</b>
<input style="width: 150px; height: 25px; border: 1px solid #ccc; padding: 2px; margin-bottom: 5px;" type="button" value="Path"/>	<input style="width: 150px; height: 25px; border: 1px solid #ccc; padding: 2px; margin-bottom: 5px;" type="button" value="Windows"/>
<b>Path *</b>	
<input style="width: 600px; height: 25px; border: 1px solid #ccc; padding: 2px;" type="text" value="C:\work\"/>	
As Folder <a href="#">Change</a>	
<input type="checkbox"/> Include Subfolders	
<hr/>	
<b>Exclusions Mode</b> <span style="float: right;"><a href="#">More options</a> </span>	
<input type="radio"/> <b>Suppress alerts</b> Do not display alerts on processes.	
<input type="radio"/> <b>Interoperability</b> Reduce the monitoring level on the processes. Usage example: to solve interoperability. Important: lowers protection.	
<input type="radio"/> <b>Interoperability - extended</b> Reduce the monitoring level of the processes, and their child-processes. Usage example: to solve interoperability. Important: lowers protection.	
<input type="radio"/> <b>Performance Focus</b> Disable monitoring of the processes. Usage example: to solve performance issues related to these processes. Important: Significantly lowers protection.	
<input type="radio"/> <b>Performance Focus - extended</b> Disable monitoring of the processes, and their child-processes. Usage example: to solve performance issues related to these processes. Important: Significantly lowers protection.	
<hr/>	
<b>Description</b> <input style="width: 600px; height: 25px; border: 1px solid #ccc; padding: 2px;" type="text" value="Add description"/>	
<input style="background-color: #800080; color: white; border: 1px solid #800080; padding: 5px; margin-right: 10px;" type="button" value="Save"/> <input style="background-color: #800080; color: white; border: 1px solid #800080; padding: 5px;" type="button" value="Save and add another"/> <input style="border: 1px solid #ccc; padding: 5px;" type="button" value="Cancel"/>	

**Denali and Central Park:** For most exclusions, keep **Monitor** selected. To resolve interoperability issues, deselect **Monitor**.

New Exclusion

Exclusion Type \* OS \*

Path Select OS

Path \*

Example: /bin/file or /bin/

Include Subfolders  Monitor

Description \*

Add description

Save Save and add another Cancel

11. Optional: In **Description**, explain the reason for the exclusion.

12. Click **Save**.

**For Interoperability and Performance Focus exclusions** (formerly Do not Monitor or Do not Inject): For processes that cannot be restarted, such as System processes or Anti-virus processes, you must reboot endpoints to apply or remove an exclusion. For processes that can be restarted, such as a browser, you can restart the process to apply or remove an exclusion. **Best Practice:** We recommend that you restart all affected endpoints to apply or remove an Interoperability or Performance Focus exclusion.

## 11.4. Best Practices for Exclusions

**Management:** All

**Agents:** All

When you make a path exclusion, we highly recommend that you add the exclusion to the smallest relevant scope of endpoints - a specific group. For example, do not add exclusions to the default policy of the default group. Create a group of endpoints that use the application to exclude.

See also: [NOT Recommended Exclusions](#)

**These rules apply to path (file and folder) exclusions for all versions:**

- You cannot put more than one exclusion path in one exclusion. AND, OR are not supported in exclusions.
- If you can exclude a hash, it is safest. Be aware that it will exclude only the specific version of a process and not all processes of this name.
- If you can exclude specific files rather than a path, that is safer. If an exploit inserts malware to an excluded path, we cannot protect the endpoints.
- The exclusion modes show from the highest level of security to the least secure. Use the most secure exclusion mode that resolves your issue.

- Environment variables are not supported. For example: Change: %appdata% To: C:\Users\Bob\AppData\Roaming\ Or use the \* wildcard to match all users: C:\Users\\*\AppData\Roaming\
- Regular expressions are not supported.
- **For Interoperability and Performance Focus exclusions** (formerly Do not Monitor or Do not Inject): For processes that cannot be restarted, such as System processes or Anti-virus processes, you must reboot endpoints to apply or remove an exclusion. For processes that can be restarted, such as a browser, you can restart the process to apply or remove an exclusion. **Best Practice:** We recommend that you restart all affected endpoints to apply or remove an Interoperability or Performance Focus exclusion.
- If you make an exclusion for an AppStacked application or snapvolume, use the folder SVROOT for the mount. For example: Change: C:\Program Files (x86)\Click\check.exe To: \* \SVROOT\Program Files (x86)\Click\check.exe to exclude C:\snapvolumes\{GUID}\SVROOT\Program Files (x86)\Click\check.exe
- Exclusions for Windows and macOS are *NOT* case sensitive. Exclusions for Linux are case sensitive.

#### **Exclusion rules for Windows:**

- The path can start with the drive letter. If the drive is not included, the exclusion applies to all drives. For example:
  - C:\calc.exe excludes CALC on the root of the C drive.
  - calc.exe excludes CALC on all directories and drives.
- If you select **Include Subfolders**, the path must end with a backslash (\).
- DO NOT USE a wildcard as the drive directory ( \*: or ?: ).

For example, do NOT use \*:\Program Files or ?::\Program Files in an exclusion path. Instead, use \*\Program Files to exclude Program Files on all drives.

You CAN use the wildcard \* to refer to any character or characters, or the metacharacter ? to refer to one character that is NOT a drive letter.

- Examples with wildcard \* to refer to any character or characters:

C:\c\*c.exe excludes files that start with "c" and end with "c.exe" on all directories and drives. This includes CALC.EXE, CAMC.EXE, CHARLIE.DOC.EXE

Example to exclude the Archives folder in a nested directory: C:\\*\Archives\

Example to exclude Go2Meeting for all users: C:\Users\\*\AppData\Local\GoToMeeting\\* \g2mlauncher.exe

- Example with metacharacter ? to refer to one character:

You CAN use: C:\test?\ to exclude C:\test1\ and C:\testf\.

Example to exclude a temp directory in all drives: harddiskvolume?\temp\

DO NOT USE ? as the drive letter. For example, do NOT use ?:\\test1\\ in an exclusion path.

### Exclusion rules for Linux and macOS:

- The path must be absolute: start with a forward slash ( / - ASCII char 47).
- The path must not contain a space in the beginning or end.
- If you select **Include Subfolders**, the path must end with a forward slash.
- **Linux** - Wildcards are not supported in Linux Agent versions 2.6 and earlier. They are supported in 3.0 and later, in the same manner as with the Windows Agent.
- **macOS** - The \* wildcard is supported in path exclusions.

For example:

- /Users/\* /Applications/<NAME>.app/ excludes all users and app subfolders
- /Users/?\* /Desktop/<NAME>.app/ excludes all users and app subfolders and their subfolders
- /Users/<USER>/Desktop/<NAME>.app/\* excludes all files in this path.

## 11.5. Excluding a File Type [Multi-Site]

**Management:** Central Park, Denali, Eiffel, Fuji, Grand Canyon, Houston

**Agents:** Windows 2.6+

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

You can exclude files of a given type from automatic mitigation.

This exclusion type is supported for Windows Agents.

### To exclude a file type:

1. In the sidebar, click **Scope**  and select a scope.
2. In the sidebar, click **Network** .
3. In the **Network** toolbar, click **Exclusions**.



4. In **Exclusion Types**, click **File Type**.
5. Click **New Exclusion**.
6. In the **New Exclusion** window, enter the details for the exclusion.

New Exclusion

Exclusion Type \* OS \*

File Type Windows

File Type \*

Example: pdf

Description \*

Add description

Save Save and add another Cancel

- In **File Type**, add the file type extension.

Wildcards are allowed. For example, use PPT for PowerPoint files. PP\* will exclude PPT, PPTX, PPTM, PPSX, PPSM, PPS, PPAM, PPA files.

- Optional: In **Description**, explain the reason for the exclusion.

For example, you exclude PPTX files from mitigation only for the endpoints in the Training department: "Training PPTX files".

- Click **Save**.

## 11.6. Excluding a Signer Identity (Certificate) [Multi-Site]

**Management:** Central Park, Denali, Eiffel, Fuji, Grand Canyon, Houston

**Agents:** Windows 2.6+ | macOS 2.6+

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

You can exclude files and software that are signed by a trusted source, with a certificate that is verified by the endpoint OS. Agents monitor events associated with the certificate signer but do not mitigate the signed items.

This exclusion type is supported for Windows and macOS Agents.

**IMPORTANT:** Do NOT create Signer Identity exclusions for all Microsoft or Adobe applications. This will significantly decrease your organization's security. If you are getting false alerts for a specific application, contact SentinelOne Technical Support to find a narrower exclusion to resolve the issue.



## IMPORTANT

Be careful! If you create incorrect exclusions, you can open your environment to malware.

Also see [Best Practices for Exclusions](#) and [Not Recommended Exclusions](#).

### To exclude items signed by a trusted source:

1. In **Analyze**, select the threat.
2. In the **Summary > Signer Identity** property, copy the string after **Cert id**:

The screenshot shows the 'Summary' section of the Analyze interface. It includes a risk level bar (S1), a hash value (31a5cbe06533946eaf8082154096e4b49bcf8e53) with links to Google and VirusTotal, and a 'Signer Identity' entry. The 'Signer Identity' entry is highlighted with a purple border and contains the text 'N/A NOTEPAD++ (Verified, Cert id: NOTEPAD++)'. Below it are file details ('notepad++.exe Ver: N/A') and a detecting engine ('DBT - Executables').

3. In the sidebar, click **Scope** and select a scope.
4. In the sidebar, click **Network** .
5. In the **Network** toolbar, click **Exclusions**.

The screenshot shows the Network toolbar with several tabs: NETWORK, ENDPOINTS, EXCLUSIONS (which is highlighted with a purple border), POLICY, DEVICE CONTROL, FIREWALL CONTROL, PACKAGES, BLACKLIST, SITE INFO, and GROUP RANKING.

6. Click **Signer Identity**.

The screenshot shows a dropdown menu titled 'Exclusion Types' with options: Hash, Path, Signer Identity (which is highlighted with a purple border), File Type, and Browser.

7. Click **New Exclusion**.

The **New Exclusion** opens.

**New Exclusion**

**Exclusion Type \*** **OS \***

Signer Identity Select OS

**Certificate ID \***

Type a Certificate ID

**About Certificate ID:**

1. Go to Analyze page and select the relevant threat
2. Copy CertID from Signer identify property (Summary section)
3. Paste to Text line

**Description \***

Add description

**Save** **Save and add another** **Cancel**

8. In **OS**, select an operating system.
9. In **Certificate ID**, paste the Certificate ID that you copied from the Forensics details page, exactly as shown after **Cert id**:

Wildcards are not supported.

10. Optional: In **Description**, explain the reason for the exclusion.
11. Click **Save**.

## 11.7. Excluding a Browser [Multi-Site]

**Management:** Central Park, Denali, Eiffel, Fuji, Grand Canyon, Houston

**Agents:** Windows 2.6+

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

Threats that come from a browser show as Exploit attempts in the Management Console. If an end-user browses to a site that hosts web exploits, which can introduce malware into your environment, the Agent detects a web exploit. It mitigates the browser session based on the policy and shows the threat in the system tray and Management Console.

In rare cases, to gain use of the browser, you can exclude the browser from active scanning.

This is supported for Windows Agents.



## CAUTION

This can leave your system vulnerable to web exploits.

### To exclude a browser:

1. In the sidebar, click **Scope**  and select a scope.
2. In the sidebar, click **Network** .
3. In the **Network** toolbar, click **Exclusions**.



4. In **Exclusion Types**, click **Browser**.
5. Click **New Exclusion**.

The screenshot shows the 'New Exclusion' dialog box. It has fields for 'Exclusion Type \*' (set to 'Browser'), 'OS \*' (set to 'Windows'), and 'Browser \*' (a dropdown menu showing 'Firefox' with a cursor icon over it, and other options like 'Edge', 'Internet Explorer', and 'Chrome'). There is also a 'Description \*' field with a placeholder 'Add description'. At the bottom are buttons for 'Save', 'Save and add another', and 'Cancel'.

6. In **Browser**, select a browser.
7. In **Description**, add text describing the exclusion.
8. Click **Save**.

# 12. Managing Management Console Users [Multi-Site]

Create [150] and edit [155] Management Console Admins, configure how they log in [153], and generate API tokens [157].

## 12.1. Creating New Management Console Users [Multi-Site]

**Management:** Central Park, Denali, Eiffel, Fuji, Grand Canyon, Houston

**Agents:** All

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

Create Management Console users to let your security team log in to the Management Console and manage endpoint security.

**Recommended:** After you create a user account, request SentinelOne Support Portal access for this user.

Watch: [How to Create Users](#)

To create users to manage all your Sites, you must have *Global* scope and *Admin* permissions.

To create users to manage Accounts, you must have Global Admin or Account Admin permissions for this Account.

To create users to manage a specific Site, you can have Global Admin, Account Admin, or Site Admin permissions for this Site.

You can create users for Sites over which you have Admin permissions. For example, if the user Alpha01 has Admin permissions for site X and Viewer permissions for site Y, Alpha01 can make users for Site X but not for site Y.

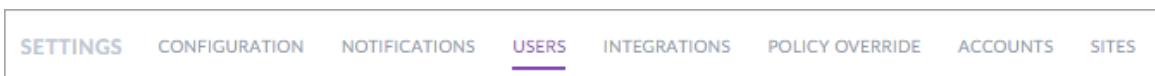
### To create a new user:

1. In the sidebar, click **Scope**  and select a scope.

If you are a Site or Account Admin, you must select one Site to open Settings.

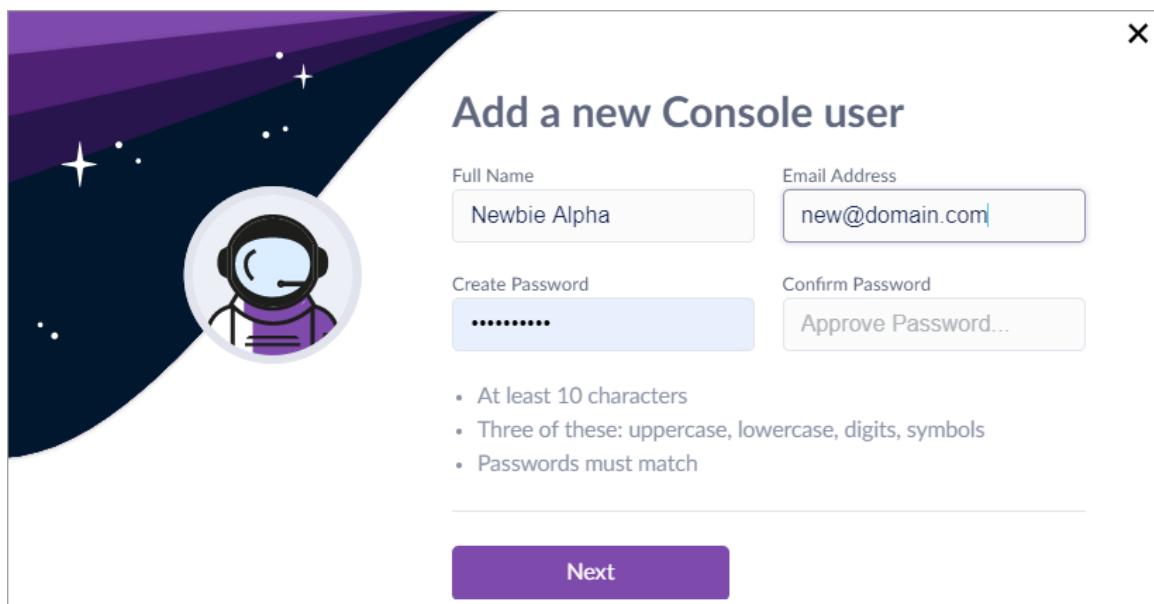
If your Admin scope is for multiple Sites, you can manage users for all your Sites, not only for the one you selected in **Scope**.

2. In the sidebar, click **Settings** .
3. In the **Settings** toolbar, click **Users**.



4. Click **New User**.

The **New User** window opens.



- Enter the user's **Full Name** and **Email Address**.

The email address becomes the username.

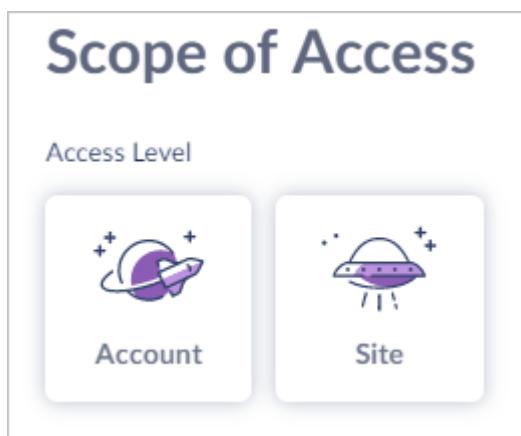
- Enter a **Password** for the user, and in **Confirm Password**, enter it again.

Passwords must:

- Have 10 or more characters.
- Contain 3 or more of these character types: Capital letters, lower case letters, numbers, special characters.
- NOT contain whitespace.

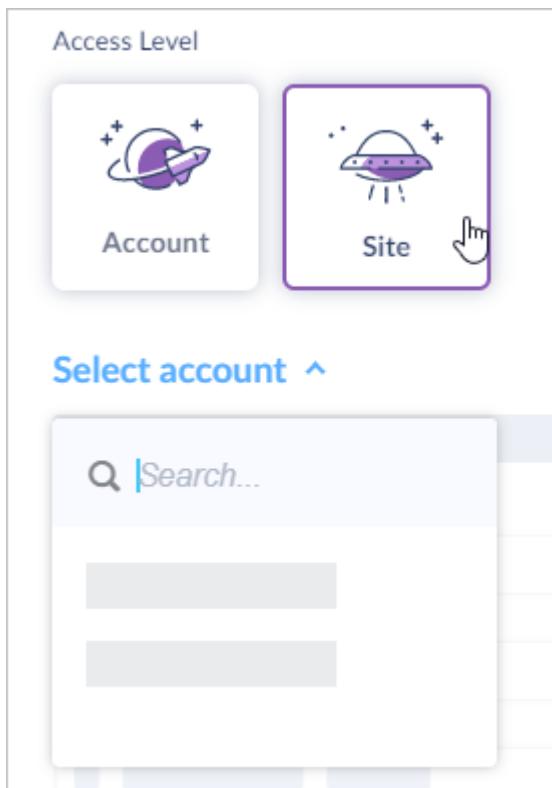
- Click **Next**.

- Select the **Access Level**.



If you are a Global Admin, you can select **Global**, **Account**, or **Site**. If you are an Account Admin, you can select **Account** or **Site**. If you are a Site Admin, **Site** is selected.

- If you are an Account Admin and you want to create a Site Admin or Site Viewer, you must select the Account that holds the Sites. Then the Sites of that Account are in the list.



10. Select each Account or Site over which the user will have permissions and then select the role: **Viewer** or **Admin**.

4/ 4 sites selected		
<input checked="" type="checkbox"/>	Default site	Admin ▾
<input checked="" type="checkbox"/>	Austin	Admin ▾
<input checked="" type="checkbox"/>	Philadelphia	Viewer ▾
<input checked="" type="checkbox"/>	Cleveland	Viewer ▾

11. Click **Create User**.  
12. Submit a request for the user to have Support Portal access.

Show Me video: How to Create Management Console Users

## 12.2. Resending Verification Email [Multi-Site]

**Management:** Grand Canyon, Houston

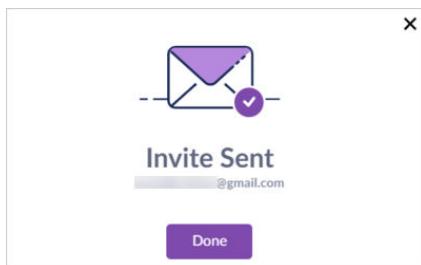
**Agents:** All

**Minimum Admin Scope:** Global Admin

**Scope:** Selected Site, Account, or Global

If your Management Console has **Onboarding** enabled (the default is disabled for all Cloud-based deployments), 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.

When you click **Create User**, the Console sends an invitation to the email of the user. Click **Done** in the **Invite Sent** window.



### To resend verification emails:

1. Log in to the Management Console as a Global Admin.
2. In the sidebar, click **Settings** .
3. In the **Settings** toolbar, click **Users**.



4. Click the checkbox of the user.
5. Click **Actions > Send Verification Emails**.
6. In the confirmation message, click **Confirm**.

## 12.3. Changing a User's Password [Multi-Site]

**Management:** Central Park, Denali, Eiffel, Fuji, Grand Canyon, Houston

**Agents:** All

**Minimum Admin Scope:** Account Admin

**Scope:** Selected Site, Account, or Global

From version Grand Canyon SP3, you must be an Account Admin to change the password for a Site Admin. Global Admins can change the password for Account Admins.

Password requirements:

- 10 to 25 characters

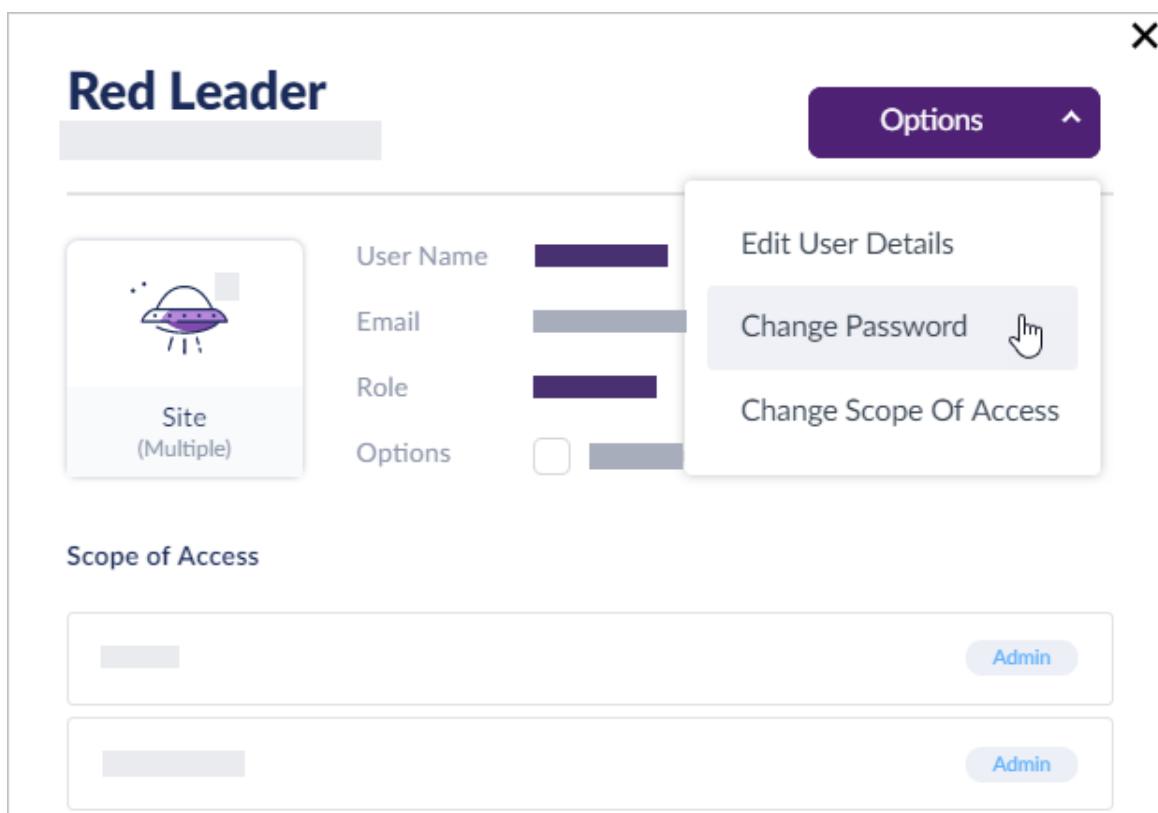
- 3 or more of these character types: Upper-case letters, lower-case letters, numbers, special characters
- No whitespace

## To change the password for a user:

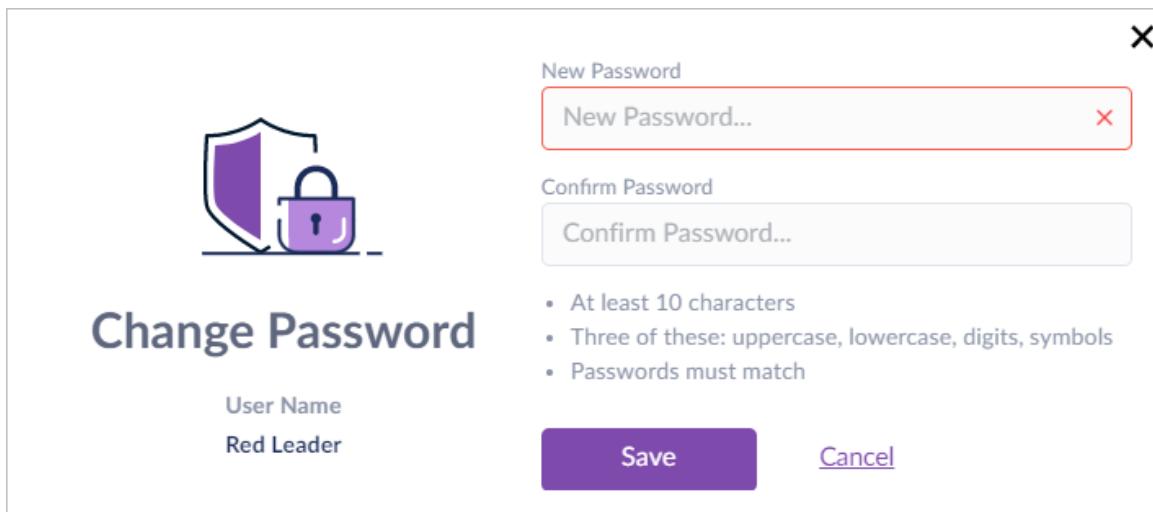
1. In the sidebar, click **Scope**  and select a scope.  
If you are a Site or Account Admin, you must select one Site to open Settings.
2. In the sidebar, click **Settings** .
3. In the **Settings** toolbar, click **Users**.



4. Click a username.
5. In the **Edit User** window, click **Options > Change Password**.



6. In the window that opens, enter the **New Password**, and then again in **Confirm Password**.



- Click **Save**.

## 12.4. Editing Management Console User Details [Multi-Site]

**Management:** Central Park, Denali, Eiffel, Fuji, Grand Canyon, Houston

**Agents:** All

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

You can update the user details, and **Role** and **Scope** of a user. For example, you can give new employees VIEWER permissions at first. When they are ready to join the Security Team and manage the security of your environment, you can give them ADMIN permissions.

From version Grand Canyon SP3, you must be an Account Admin to edit the user details for a Site Admin. Global Admins can edit user details for Account Admins.

Note: Account admins can change the scope of other Account admins to demote them to Site admins.

Note: Site Admins cannot enable Remote Shell for themselves or other users. Site Admins can enable 2FA for themselves.

### To edit details of a user:

- In the sidebar, click **Scope**  and select a scope.

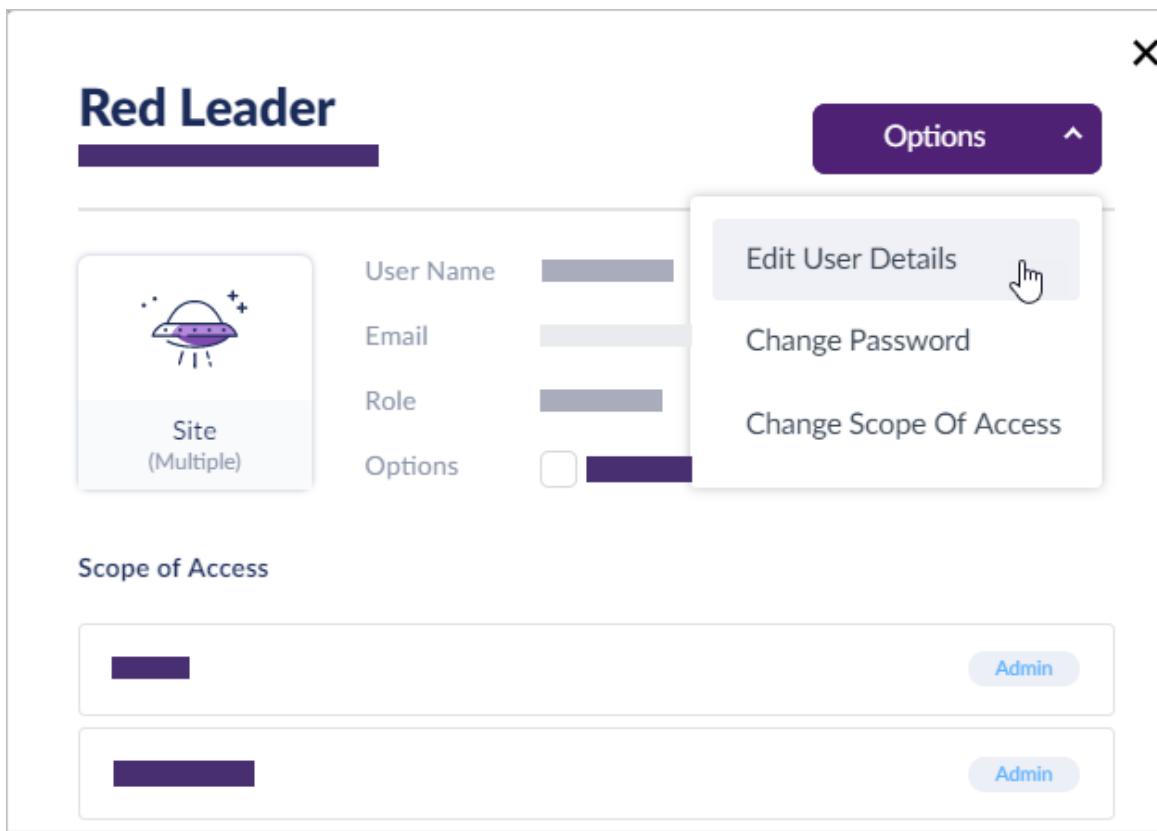
If you are a Site or Account Admin, you must select one Site to open Settings.

If your Admin scope is for multiple Sites, you can manage users for all your Sites, not only for the one you selected in **Scope**.

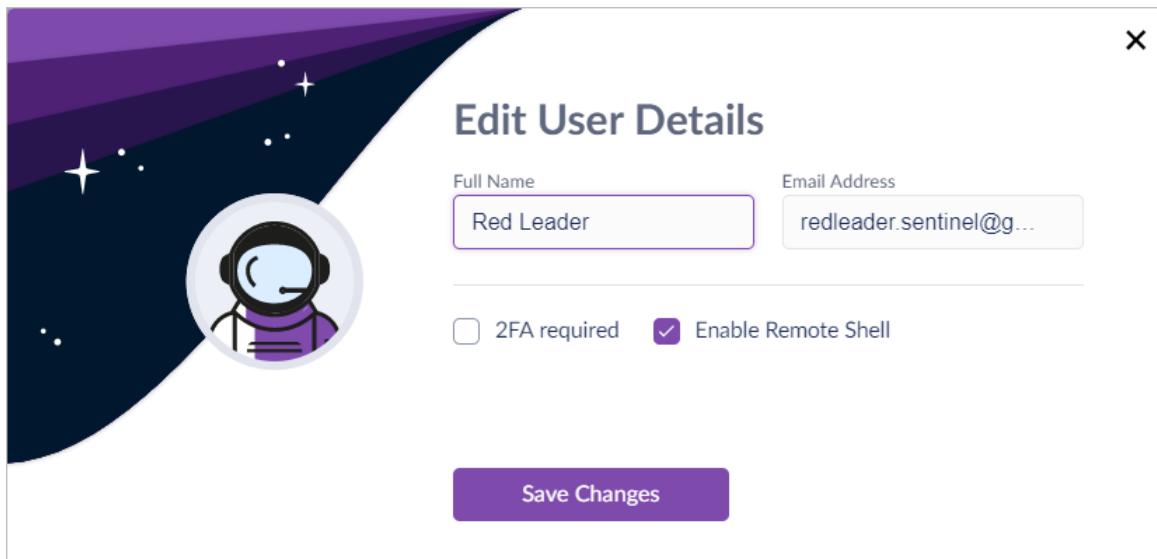
- In the sidebar, click **Settings** .
- In the **Settings** toolbar, click **Users**.



4. Click a username.
5. In the **Edit User** window, click **Options > Edit User Details**.



6. In the window that opens, change the user's **Full Name**, **Email Address**, whether this user requires Two-Factor Authentication (**2FA**), and whether this user can use **Remote Shell**.



Note: If Remote Shell is not enabled for your Management, you cannot enable it for users.

7. Click **Save Changes**.

## 12.5. Generating API Tokens [Multi-Site]

**Management:** Central Park, Denali, Eiffel, Fuji, Grand Canyon, Houston

**Agents:** All

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

The SentinelOne API is a REST web services API with functionality to replace or to enhance the console.

**Note:** The API has its own version number. It is not the same as the version of the Management or Agent. You can see the latest version of the API from the Management Console. Click **?** and select **API Doc**.

To use the API, you must have a token. The API uses the token to access the Management. A SentinelOne user can have one token.

- **token** - Use the temporary token if you want a quick response from the Management for a one-time workaround. This token is more secure because it is valid for a short time.

The first time you send an API request with your Management Console credentials, the **token** is in the response. This token survives for the amount of time configured in **Settings > Configuration > Session Timeout**.

- **ApiToken** - Use the ApiToken for long-running automation and other scripts. The ApiToken bypasses Two-Factor Authentication. Security for your ApiToken is your responsibility.

Generate the token file from the Management Console or API request with your login credentials. You can only generate an API token for yourself. This token is valid for six months. You can revoke it or regenerate it from the console (these options are in your User Details after you generate your token) or from the API (/web/api/v2.0/users/generate-api-token).

**ApiToken** is case sensitive and changed between API v1.6 and API v2.0.

### Best Practice:

- Put the downloaded ApiToken in a configuration file that your API requests use.
- Secure the ApiToken file itself against accidental leakage or malicious tampering.
- Set a reminder to regenerate the ApiToken before it expires and to update the configuration file.

### To generate a temporary token for one session:

1. Send this request:

```
POST https://your_management_url/web/api/v2.0/users/login
{
  "username": "console_username",
  "remember_me": "true",
  "password": "console_password"
}
```

- Get the session token from the response.

### To generate a 6-month ApiToken:

- Send this request:

```
POST https://your_management_url/web/api/v2.0/users/generate-api-token
```

- Save the token from the response to a file that your API requests use.

If the request fails with "Authentication Failed", you can run it from your Console > ? > **API Doc** > **Generate API token**.

**Generate API token**

**POST** /web/api/v2.0/users/generate-api-token

Returns the API token for the authenticated user.

— Test this endpoint

**RUN ON CONSOLE**

— RESPONSE SAMPLE

```
{
  "errors": [
    {}
  ],
  "data": {
    "token": "280079207634042955XDyEBWFHQ5q9iiTpmlrRM9Is1CCdLS7vcbGF9y4y"
  }
}
```

+ RESPONSE SCHEMA

### To generate a 6-month API Token for your own username in the Console:

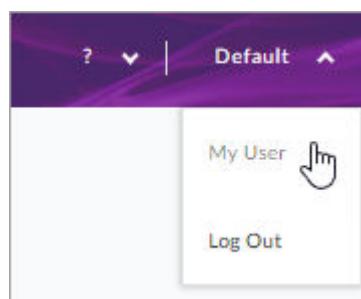
- In the sidebar, click **Scope**  and select a scope.

If you are a Site or Account Admin, you must select one Site to open Settings.

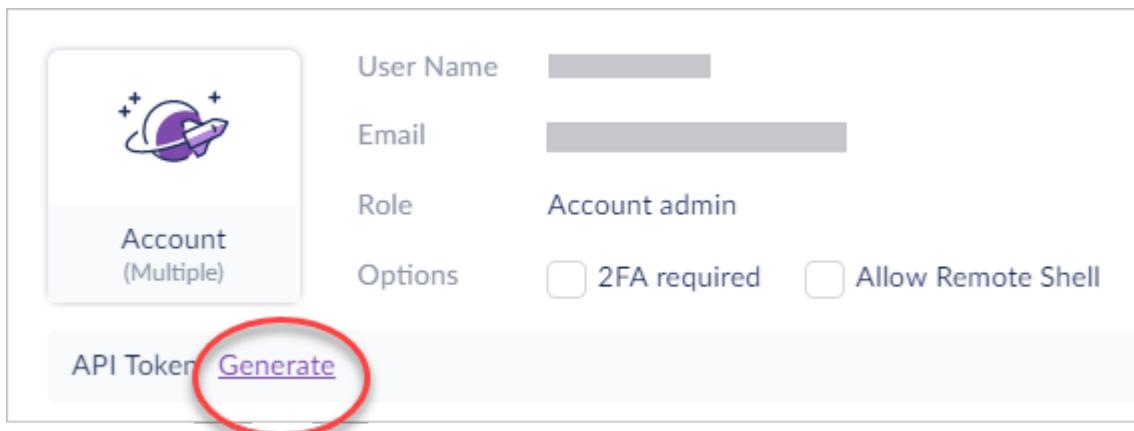
- In the sidebar, click **Settings** .
- In the **Settings** toolbar, click **Users**.



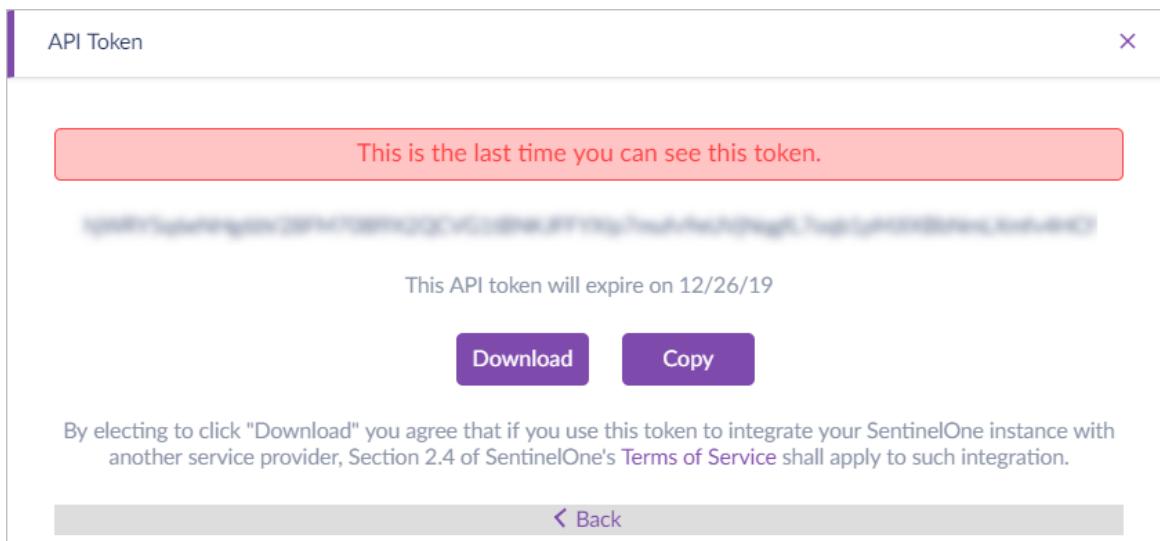
- Click your user name and select **My User**.



- Click **Generate**.

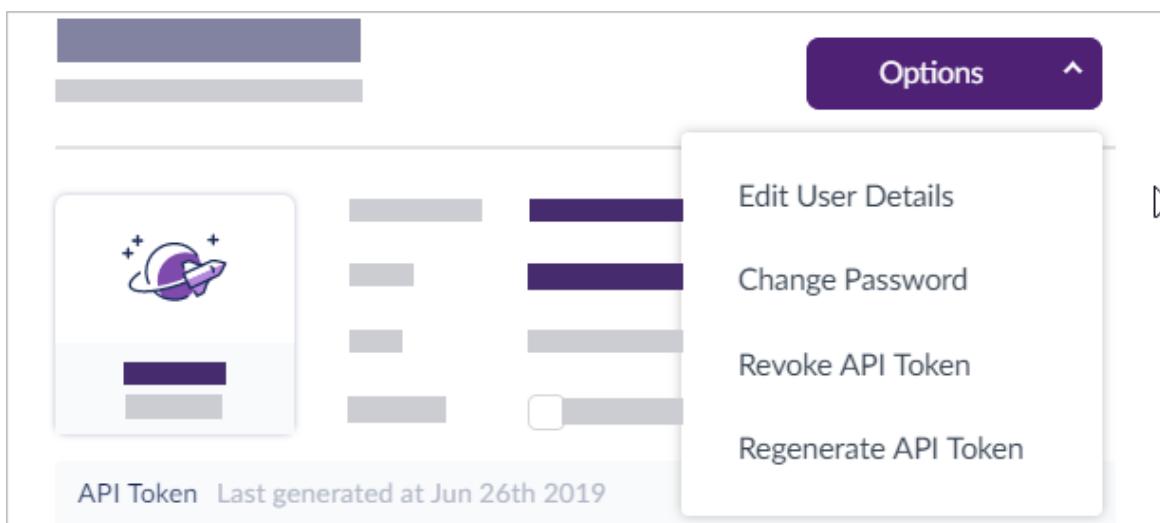


In the API Token window, click **Download** or **Copy**.



If you click Download, the text file is: **SentinelOne-Auth-API-Token.txt**

The options of your username change to include **Revoke API Token** and **Regenerate API Token**.



## To send authenticated requests to the API:

API endpoints accept a session token or an API token in a custom HTTP header (recommended) or in a query-string parameter.

- ApiToken in the HTTP header:

```
"Authorization: ApiToken string"
```

- Session token in the HTTP header:

```
"Authorization: Token string"
```

- ApiToken in a query-string parameter:

```
"apiToken=string"
```

**Example:** "GET https://my-mgmt.sentinelone.com/web/api/v2.0/agents?apiToken=280079207634042955XDyEBWFHQ5q9iiIpmLrRM9IsiCCdLS7vcbGF9y4y"

- Session token in a query-string parameter:

```
"token=string"
```

**Example:** "GET https://my-mgmt.sentinelone.com/web/api/v2.0/agents?token=abfa5b75910183ed40b62337e079dda58121db267558a873fde4ff537bd7ceb87cb185a8299fea73"

## 12.6. Enabling Two-Factor Authentication [Multi-Site]

**Management:** Central Park, Denali, Eiffel, Fuji, Grand Canyon, Houston

**Agents:** All

**Minimum Admin Scope:** Global Admin

**Scope:** Selected Site, Account, or Global

Increase your security with Two-Factor Authentication (2FA, Multi-Factor Authentication, MFA), which adds a second authentication method. For example, Google Authenticator and Duo Security send a code through a phone app. See the vendor documentation to select and configure the Two-Factor Authentication that you choose.

The changes you make apply to the selected scope.

If Two-Factor Authentication is required for the scope, users in the scope cannot disable it for themselves. If an Admin turns it off in the user settings, the QR code prompt will show on the next login to the Management Console.

**Note:** If **SSO** authentication is required for a user, you can configure 2FA also. 2FA authentication will NOT be required for that user's login to the Management Console, but will be required for features that require 2FA, such as Remote Shell.

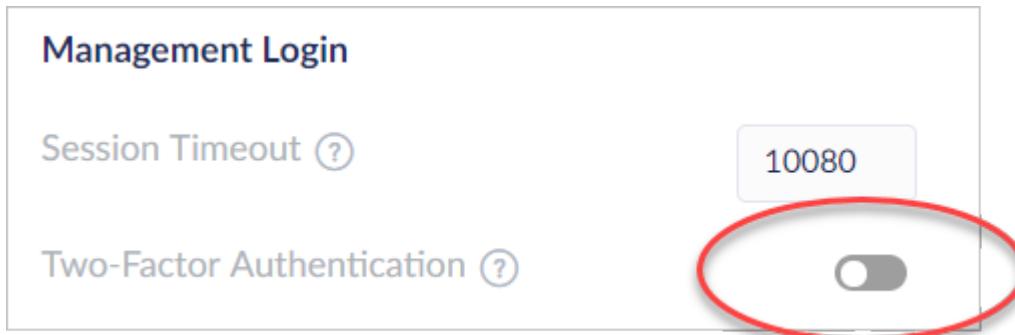
### To require Two-Factor Authentication for all users:

1. In the sidebar, click **Scope**  and select a scope.

If you are a Site or Account Admin, you must select one Site to open Settings.

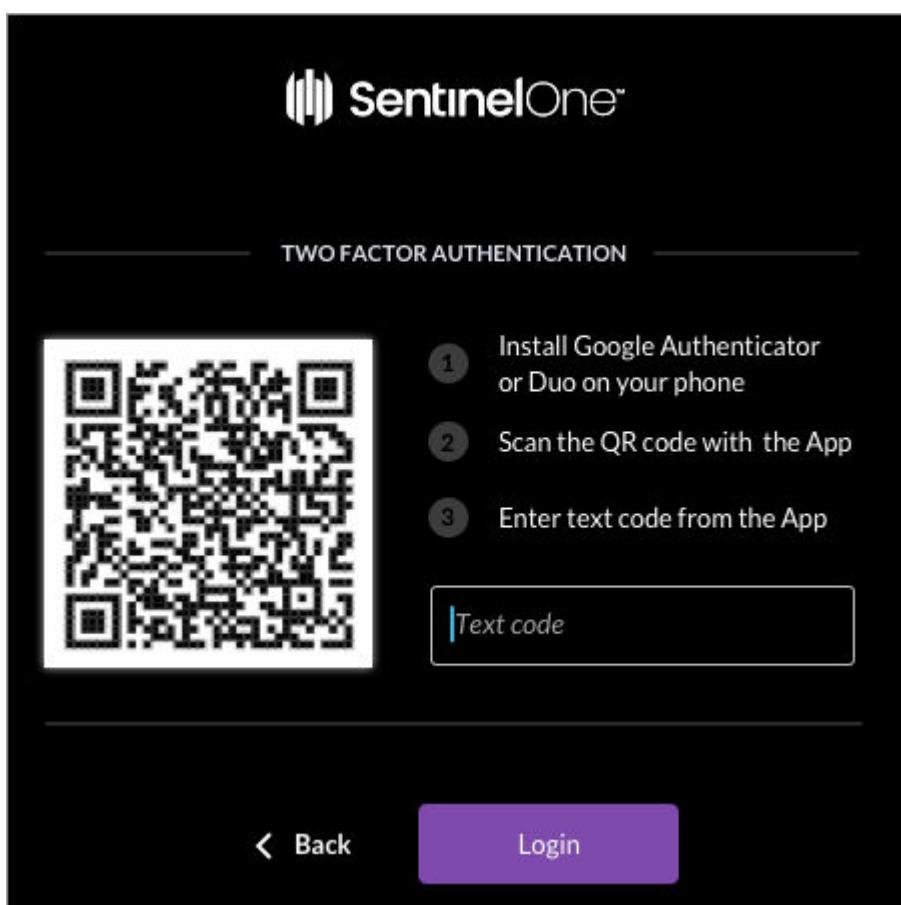
If your Admin scope is for multiple Sites, you can manage users for all your Sites, not only for the one you selected in **Scope**.

2. In the sidebar, click **Settings** .
3. In **Configuration > Management Login**, enable **Two factor authentication**.



4. Click **Save**.

Users will get the QR code and instructions on their next log in to the Management Console.



## To configure Two-Factor Authentication for one user:

1. In the sidebar, click **Scope**  and select a scope.

If you are a Site or Account Admin, you must select one Site to open Settings.

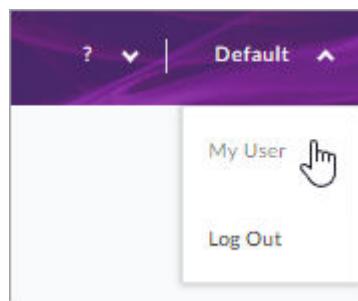
If your Admin scope is for multiple Sites, you can manage users for all your Sites, not only for the one you selected in **Scope**.

2. In the sidebar, click **Settings** .
3. In the **Settings** toolbar, click **Users**.



4. Click a username.

Or, to open your own user details, in the top right corner of the Management Console, click your user name and select **My User**.



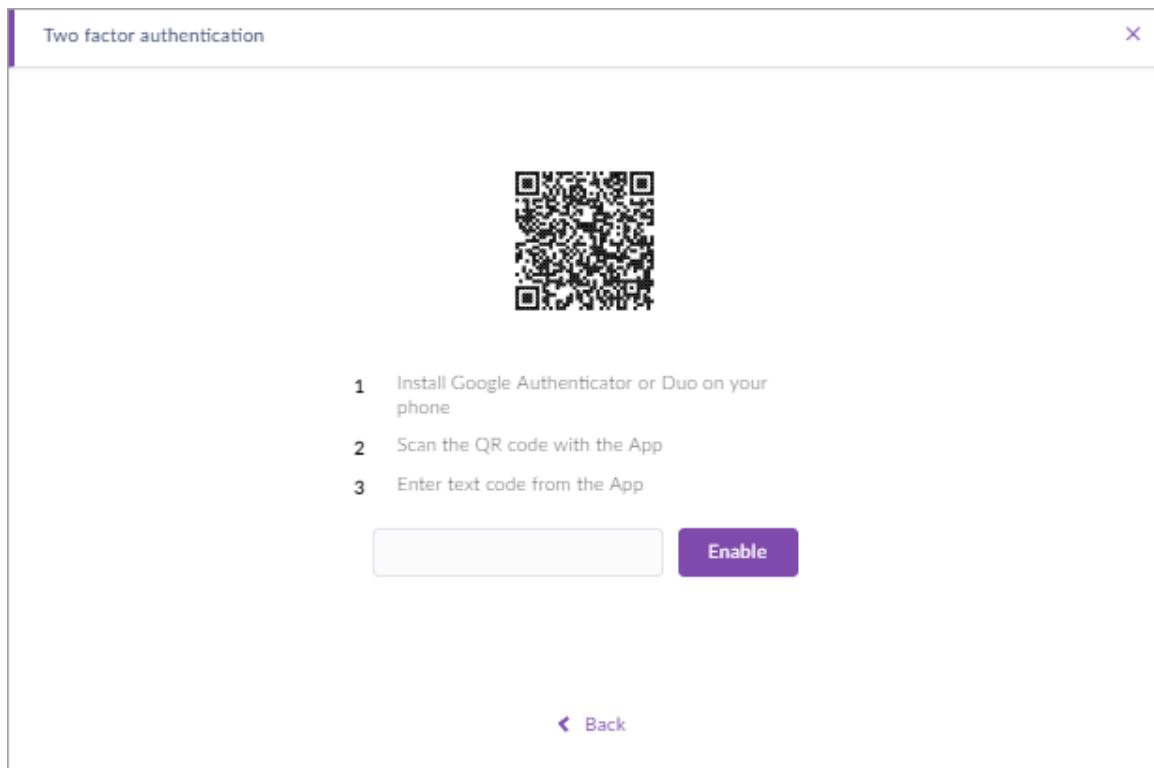
5. In the **Edit User** window, click **Options > Edit User Details**.

The screenshot shows the 'Red Leader' user profile page. On the left, there's a sidebar with a site icon and a 'Site (Multiple)' label. The main area displays 'User Name' (redacted), 'Email' (redacted), 'Role' (redacted), and 'Options' (checkbox). A dropdown menu from the 'Options' button contains 'Edit User Details' (with a hand cursor icon), 'Change Password', and 'Change Scope Of Access'. Below this is a 'Scope of Access' section with two items, each with a purple bar and an 'Admin' badge.

6. In the Edit User Details window, click **2FA required**.

The 'Edit User Details' modal is shown. It has fields for 'Full Name' (A Name) and 'Email Address' (alphaaccmgr@gmail.c...). At the bottom, there are two checkboxes: one checked labeled '2FA Required' and one unchecked labeled 'Enable Remote Shell'. A large purple 'Save Changes' button is at the bottom right.

7. If you are in your own user details, a page opens with a QR code to scan with your phone, and instructions. Follow the instructions.



If you enabled Two-Factor Authentication for different users, they will get the QR code and instructions on their next log in to the Management Console.

8. Click **Save Changes**.

## 12.7. Configuring Session Timeout [Multi-Site]

**Management:** Central Park, Denali, Eiffel, Fuji, Grand Canyon, Houston

**Agents:** All

**Minimum Admin Scope:** Global Admin

**Scope:** Selected Site, Account, or Global

Set a timeout for the Management Console, to protect your environment from unauthorized access. If an admin or viewer is away from the computer, the username logs out automatically when the session expires.

Each Site can have its own timeout setting and there are global timeout settings. Site Admins get the setting configured for the Site. Global Admins get the Global setting.

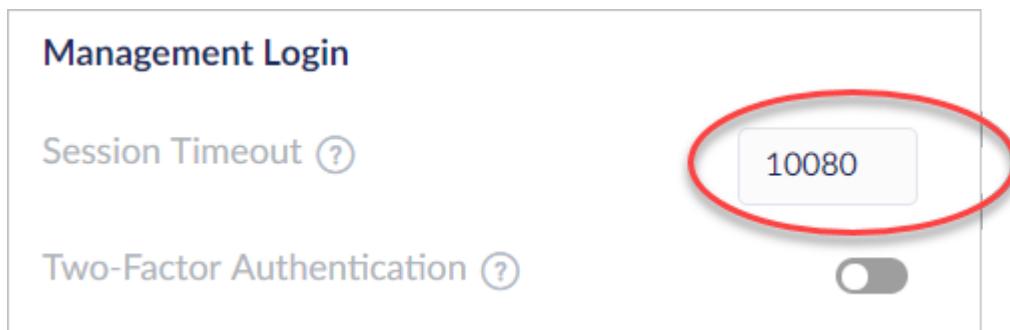
### To set session timeout:

1. In the sidebar, click **Scope**  and select a scope.

If you are a Site or Account Admin, you must select one Site to open Settings.

If your Admin scope is for multiple Sites, you can manage users for all your Sites, not only for the one you selected in **Scope**.

2. In the sidebar, click **Settings** .
3. In **Configuration > Management Login > Session Timeout**, enter the number of minutes a user is logged in, before the browser session times out.



4. Click **Save**.

## 12.8. Deleting a Console User [Multi-Site]

**Management:** Central Park, Denali, Eiffel, Fuji, Grand Canyon, Houston

**Agents:** All

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

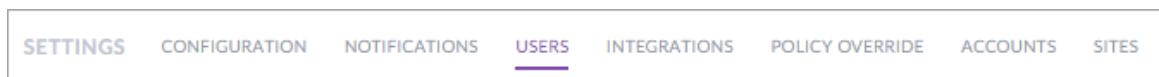
### To delete a console user:

1. In the sidebar, click **Scope**  and select a scope.

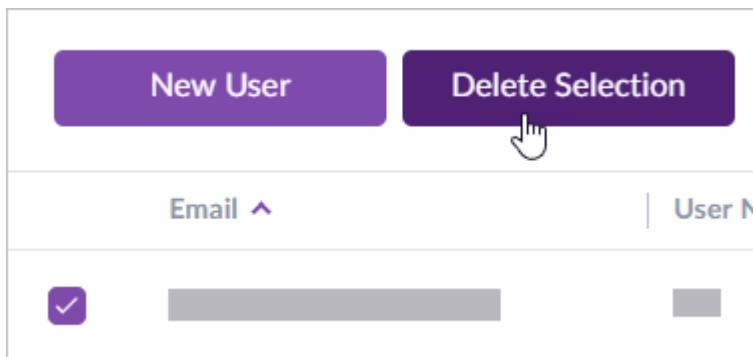
If you are a Site or Account Admin, you must select one Site to open Settings.

If your Admin scope is for multiple Sites, you can manage users for all your Sites, not only for the one you selected in **Scope**.

2. In the sidebar, click **Settings** .
3. In the **Settings** toolbar, click **Users**.



4. Click the checkbox of the user.
5. Click **Delete Selection**.



6. In the confirmation message, click **Confirm**.

## 13. Deep Visibility

**Management** : Central Park, Denali, Eiffel, Fuji, Grand Canyon, Houston

**Agents**: Windows 2.6+ | macOS 2.6+ | Linux 2.6+

**SKU**: Complete (not available with Core)

**Minimum Admin Scope**: Site Admin

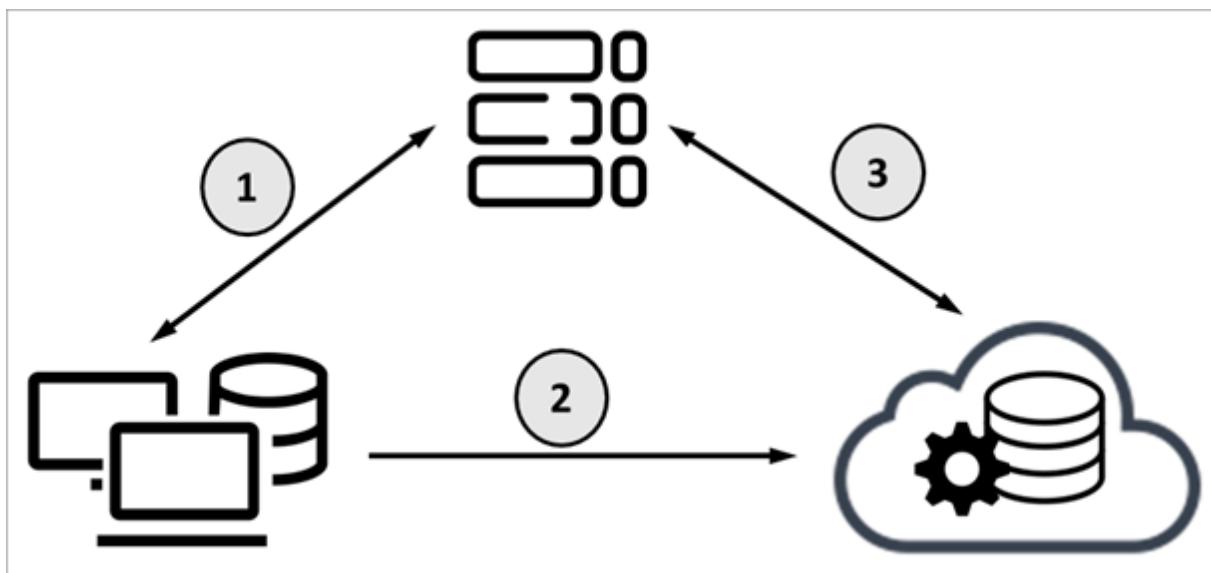
**Scope**: Selected Site, Account, or Global

<https://www.youtube.com/embed/AjLO3r2F0KQ?rel=0>

Watch: [Deep Visibility Demo 1- Overview and search for URL Connections](#)

SentinelOne Deep Visibility extends the ActiveEDR capabilities, with full visibility into endpoint data and threat hunting. Its patented kernel-based monitoring allows a near real-time search across endpoints for all indicators of compromise (IOC). It gives security teams the ability to augment real-time threat detection capabilities with a powerful threat hunting tool.

Our True Context ID lets security analysts understand the full story of what happened on a device, as each element of a story has the same exact True Context ID. Use it to hunt easily, see the full chain of events, and save time for your security teams.



### Deep Visibility Architecture

Item	Description
1	Agents send threat data to the SentinelOne Management. The Management shows data in the Console, based on the scope, and manages Agents.
2	Agents send benign event data to the Deep Visibility Cloud Database, which works with the Database query engine.

Item	Description
3	You create queries for Threat Hunting on the Management Console to the Deep Visibility Cloud. Deep Visibility sends the results back to the Management.

All data transmissions are encrypted, compressed, and sent over HTTPS. Agent data is available to you, and only you, for up to three months. From the time that an event occurs, the data is available in the Deep Visibility queries in minutes.

A gateway stands between your Agents and the Cloud Storage. The gateway authenticates all Agents with your Management. Your Management Console shows data from only your Agents. Your data is not given to others.

Detailed flow: Agents send data. It goes to the Deep Visibility Gateway, which sends data to the Cloud Database that processes big data. The Cloud Database sends to the Database query engine that reads the database. It sends to the query Gateway. The management server speaks with query GW which speaks with DB. MGMT can speak with Agent to do mitigation. Maximum data retention is 3 months.

With Windows Agent version 2.8 or higher, you can route Agent-to-Deep Visibility traffic through a proxy server, to the SentinelOne IOC gateway. This is the recommended configuration if you deploy the On-Prem Management. [See Configuring a Proxy Server for Agents](#).

macOS Agents automatically use the proxy server settings configured for each endpoint in the macOS system settings. See [Configuring a Proxy for macOS Agents](#).

### 13.1. How to Use Deep Visibility [Multi-Site]

**Management:** Eiffel, Fuji, Grand Canyon, Houston

**Agents:** Windows 2.6+ | macOS 2.6+ | Linux 2.6+

**SKU:** Complete (not available with Core)

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

Watch: [Deep Visibility Demo 1- Overview and search for URL Connections](#)

Watch: [Deep Visibility Demo 2- Focus on Process Tree and search for Known Threat](#)

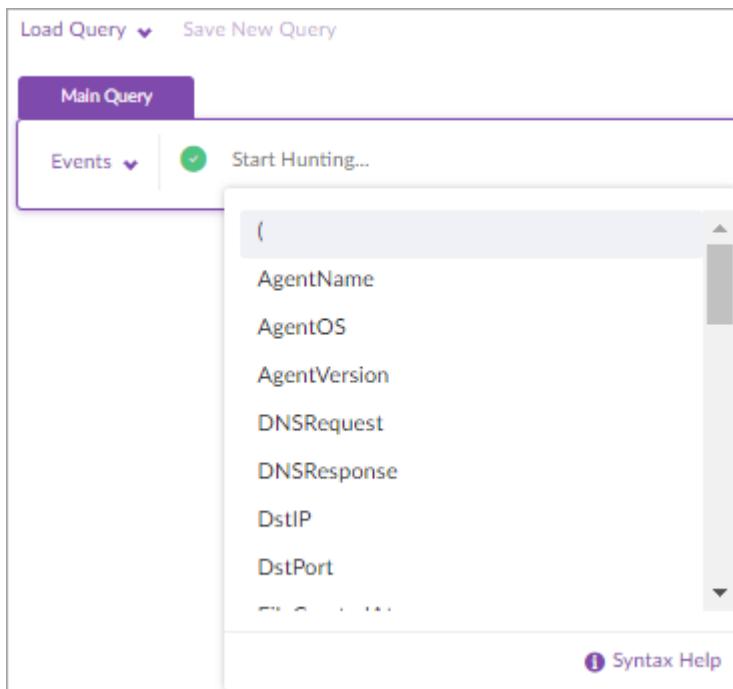
Run Threat Hunting queries and use Deep Visibility in the **Visibility** view of the Management Console.

If you are a Global Admin or a Multi-Site Admin, in the Global view, you see query results combined for all of your Sites.

The Deep Visibility workflow depends on your specific needs. This is an overview of different actions you can do in the **Visibility** view.

#### Create Powerful Queries

- Click in the Main Query to start a query. Start to type to get suggestions. You are prompted with suggestions for each part of the query. Use up to 10 operators in a search bar.



- Open up to 15 tabs at one time, with different queries in each. The tabs are named automatically for easy reference. You can edit the tab names.

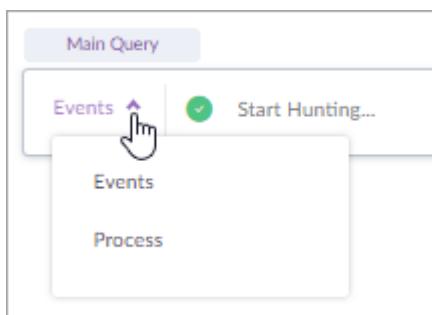


- Select a time frame for the query.



- Run a Sub-query on the data that has already been pulled from the SentinelOne Cloud in the Main Query. Each main query can have one Sub-query (From Eiffel SP3). Use this to refine your query quickly.

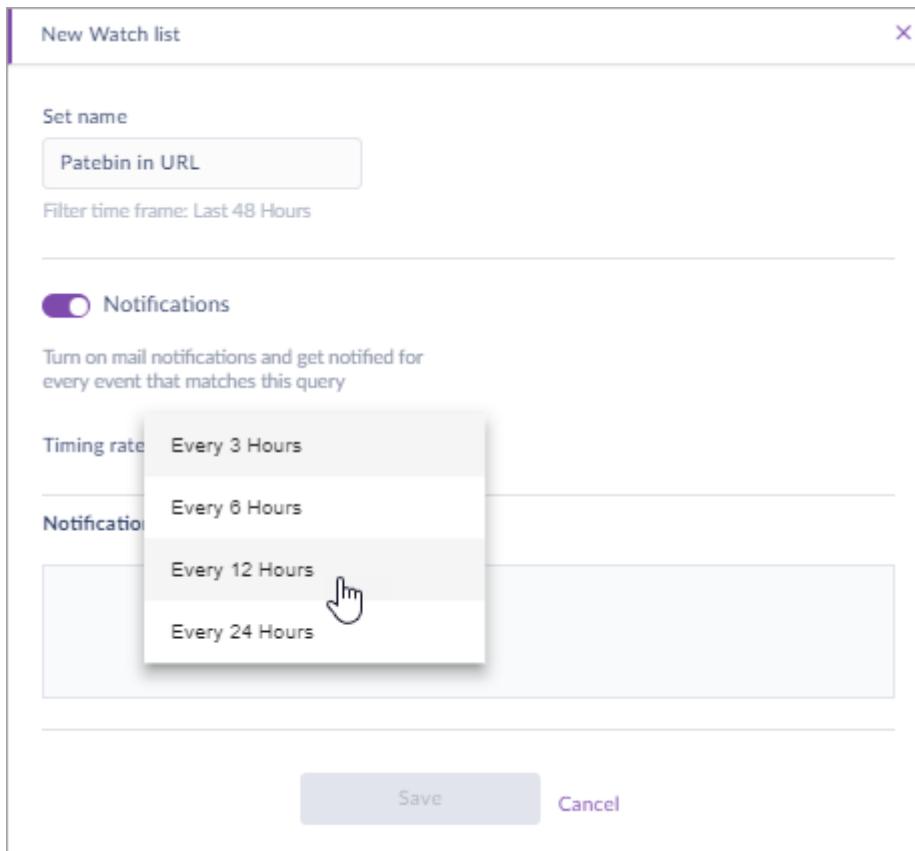
- In the query bar, choose to search for **Events** or **Processes**.



- Events** - All events that match your query exactly.
- Process** - All parent process events that match your query exactly.
- Save Threat Hunting Queries for future use.



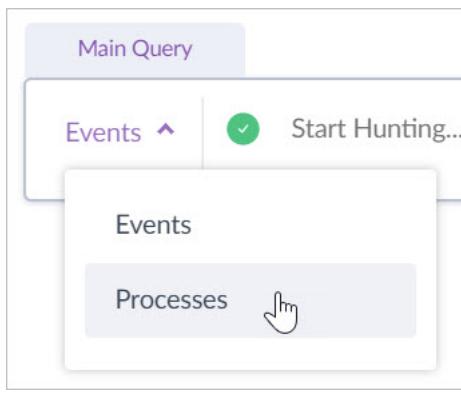
- Set up Threat Hunting watchlists - Create queries that run periodically and send notifications when they find results that match.



### 13.1.1. Running a Deep Visibility Query

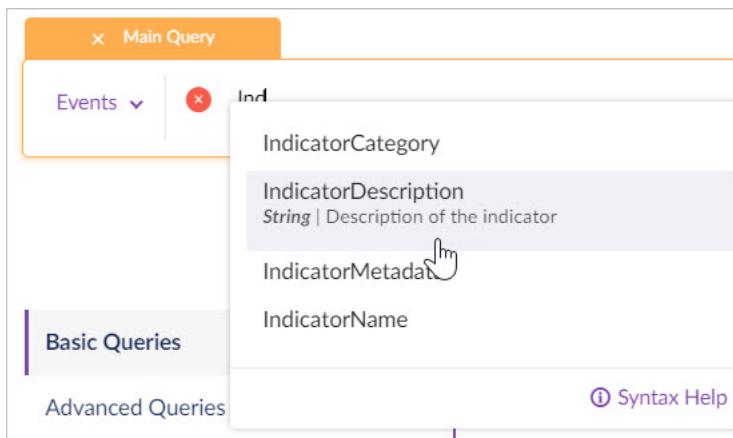
**To run a Deep Visibility query:**

1. In **Visibility**, select Events or Processes. By default, Deep Visibility searches **Events**. To search for Processes, click the arrow and select **Processes**.

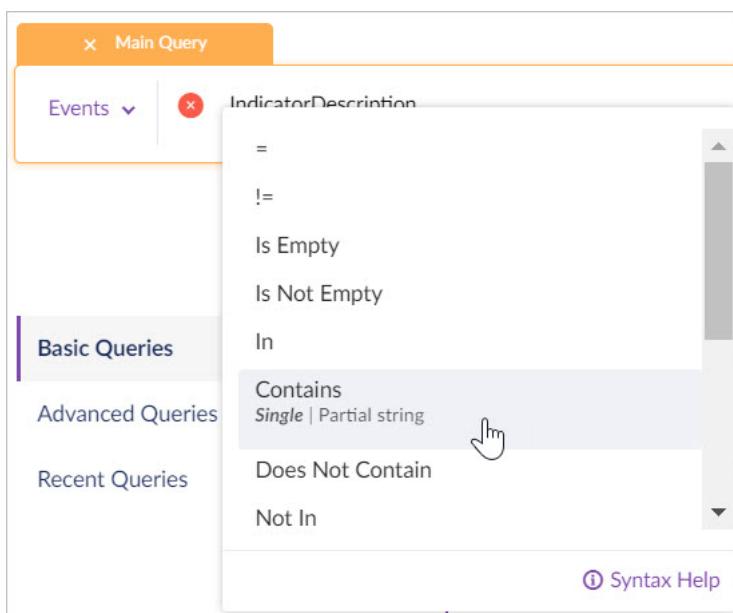


2. Select or enter a field, operator, and value.

As you enter a query, a prompt opens with valid values for the current part of a well-formatted query.



The query shows a red icon when the query is not complete or valid and a green icon when it is valid.



The screenshot shows the 'Main Query' interface. At the top, there's a header with an 'X' icon and the text 'Main Query'. Below it is a search bar containing the query 'IndicatorDescription Contains "shell"'. To the left of the search bar is a dropdown menu labeled 'Events' with a downward arrow. A green checkmark icon is positioned next to the search term.

If you want the query to use multiple phrases, select AND or OR.

3. Select a time frame for the query from the list.



4. Press enter from the query field or click .

The query results open in chronological order.

There is a limit of 10,000 results for each query. If you see that the count is 10,000, the query reached the limit. Narrow the scope of the search to get complete results.

### 13.1.2. View Query Results in a Table or Tree

You can view Deep Visibility query results in the default table view, or in the process tree view.

**To toggle between the views:**

Click an icon to **Change to table view** or **Change to tree view**.

The screenshot shows the Deep Visibility interface. At the top, there are buttons for 'Load Query' and 'Save New Query'. Below that is a 'Main Query' section with a dropdown for 'Events' and a button for 'Start Hunting...'. To the right of the search bar is a red box highlighting a small icon consisting of a grid and a right-pointing arrow. Further to the right are buttons for 'Last 48 Hours' and a magnifying glass icon.

## Table view

Object Type	Event Type	Endpoint	User	Time	Parent Process ID	Parent Process U...	Process Name	Parent Process Name
<input type="checkbox"/> PROCESS	Process Creation	DC01	NT AUTHORITY\SYSTEM	Apr 2, 2019 14:20:00	4568	57718997520604F6	Windows Modules Installer Worker	Windows Modules Installer

ENDPOINT INFO

Agent Os	windows
Site Id	373818223973368929
Agent Name	DC01
Site Name	crook
Agent Machine Type	server
Agent Version	3.0.2.35

MAIN ATTRIBUTES

Process UID	24158A5224719746
Object Type	PROCESS
True Context	DF337FEC2C267A90
Process ID	80
Event Type	Process Creation
User Name	NT AUTHORITY\SYSTEM
Created At	Apr 2, 2019 14:20:00

OTHER ATTRIBUTES

Image Path	C:\Windows\WinSxS\x64_microsoft.windows.servicingstack_31b13856x3d4e35_6.3.9600.17709_non_e_fa7932f59afc2e401TWworker.exe
Command Line	cmd /c C:\Windows\WinSxS\x64_microsoft.windows.servicingstack_31b13856x3d4e35_6.3.9600.17709_non_e_fa7932f59afc2e401TWworker.exe -Embedding
SHA256	24a54429df9d532d3
MDS	2b902ea3056aaabfbcc6b99d434ac2c9
Process Name	Windows Modules Installer Worker
Image SHA1 Hash	f246a5bb7647e82944c95a73bb6ce38eb7f673c
Parent PID	4568
Processor Start Time	Apr 2, 2019 14:20:00

- Starting with Eiffel SP2, searches run in exact mode. Only the event type queried shows in the results. For example, if you search for DNS Requests, you see **DNS** events, If you search for Modified files, you see **File** events.
- Use "!=" in queries to see exact results without selected values. For example, DstPort != "80" to find port traffic not on port 80.
- Click in a row to expand it and see details inline. You can expand multiple rows.

Object Type	Event Type	Endpoint	User	Time	Parent Process ID	Parent Process U...	Process Name	Parent Process Name
<input type="checkbox"/> PROCESS	Process Creation	DESKTOP-486...	N/A	Mar 25, 2019 13:56:49	2856	ED5D3A086A2BA44F	Microsoft Outlook Communications	Shell Infrastructure Host

ENDPOINT INFO

Agent Os	windows
Site Id	372324938066952202
Agent Name	DESKTOP-486NBKA
Site Name	Default site
Agent Machine Type	desktop
Agent Version	3.1.2.21

MAIN ATTRIBUTES

Process UID	6B06284CE568E920
Object Type	PROCESS
True Context	BFD6A8575AADB855
Process ID	2464
Event Type	Process Creation
Created At	Mar 25, 2019 13:56:49

OTHER ATTRIBUTES

Image Path	C:\Program Files\Microsoft\Windows\CurrentVersion\Windows Communication Foundation\37.8104.4237.0.x64_Bwekyb3dbbwvHxTir.exe
Command Line	cmd /c C:\Program Files\Microsoft\Windows\Communication\37.8104.4237.0.x64_Bwekyb3dbbwvHxTir.exe -ServerName=HxJPC_Server
SHA256	77762cadacee7bfaec2
MDS	bdb628458c699016354cf88d06b39457
Process Name	Microsoft Outlook Communications
Image SHA1 Hash	4324abc99eaa608c22ee741dc67159cd903ef619
Parent PID	2856

- Click next to a column header to see the column filter. Click it to select the values to show or to search in the column.

Select All      Clear

Search...

- Windows Update
- Windows PowerShell ISE
- Windows® installer
- VMware Tools Core Service
- SIH Client
- setup.exe

Save      Cancel

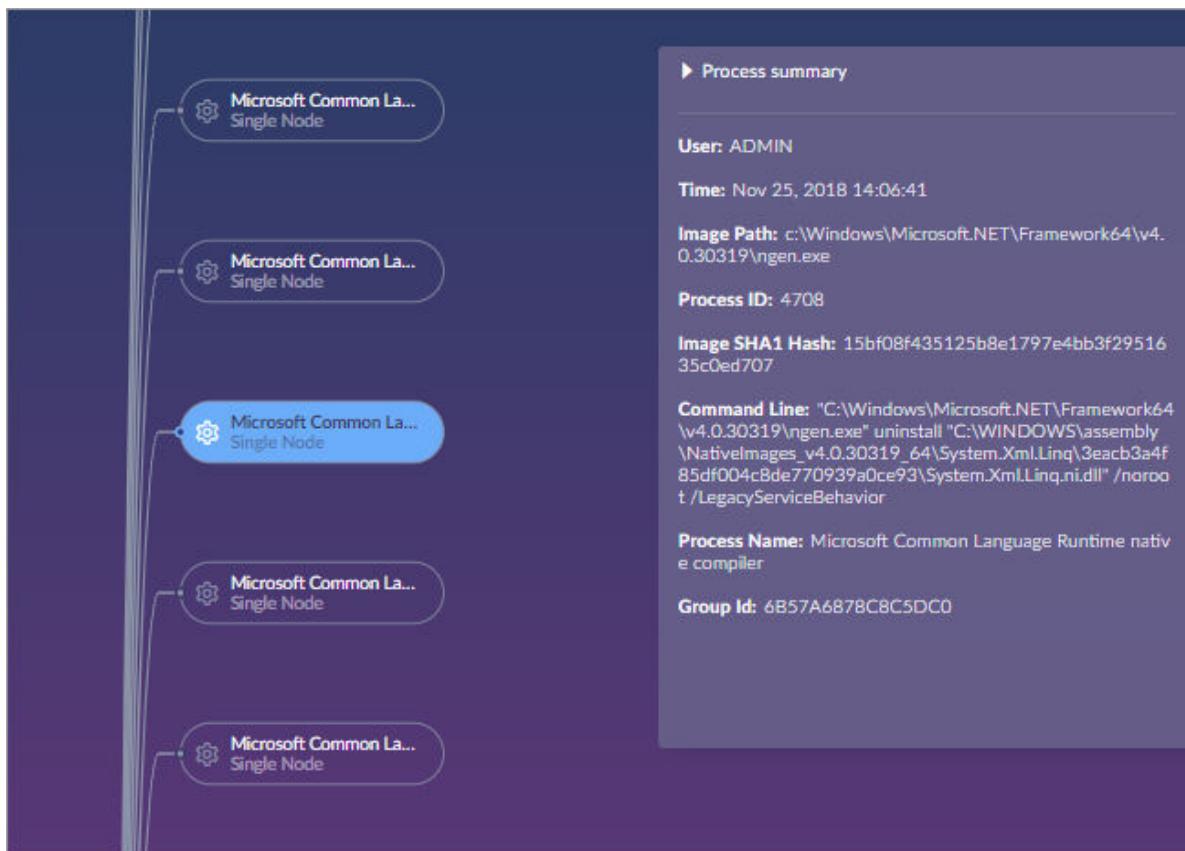
## Tree view



- Select an endpoint and process to see the events in the tree.

Process	Pid	Date
amazon-ssm-agent.exe	3848	Nov 27, 2018 11:39
amazon-ssm-agent.exe	2656	Nov 27, 2018 11:36
amazon-ssm-agent.exe	2124	Nov 27, 2018 11:34
amazon-ssm-agent.exe	2920	Nov 27, 2018 11:32
WMI Reverse Performance...	2120	Nov 27, 2018 11:32
Console Window Host	3980	Nov 27, 2018 11:32
Console Window Host	2856	Nov 27, 2018 11:32
UsaClient	2752	Nov 27, 2018 11:32
SIH Client	3880	Nov 27, 2018 11:32

- Click a node to highlight it. A summary of the highlighted node shows on the side and in the table below the tree.



- Use the Process Tree timeline to see exactly when the chain of events starts and ends. Highlighted nodes show as a point in the timeline. If you stand your cursor on a node, it also shows as a point in the timeline.



- Click in the tree and drag it to see different parts of the picture.
- Scroll up and down to zoom in and out.

## Use Query Results to Advance your Threat Hunting

- The query results include detailed information gathered from the SentinelOne Agents. Attributes in the query results include: Endpoint, User, Site ID, Path, Process ID, Process Name, SHA1 hash, SHA256 hash, MD5, command line argument, and True Context ID.
- Move the mouse over an attribute to open a floating menu bar.

A screenshot of the SentinelOne Cloud interface. On the left, there's a table with columns: Object Type (PROCESS), Event Type (Process Creation), and Endpoint (sonar). Below this is a section titled 'MAIN ATTRIBUTES' with details like Process UID (980EAA4F0866CBF1), Object Type (PROCESS), True Context (4AED976735C98909), etc. A context menu is open over the endpoint 'sonar', with options: 'New Main Query (new tab)', 'New Main Query (current tab)', 'Add to Main Query (current tab)', 'Add to Sub Query', 'Process Name' (530f6d0c595d62fba2d5cd6cad6ddab5ad0e8d24), 'Image SHA1 Hash' (530f6d0c595d62fba2d5cd6cad6ddab5ad0e8d24), 'Parent PID' (74064), 'Process Start Time' (Apr 8, 2019 03:43:43), 'Parent Process UID' (1B81356D4B26222B), and 'Parent Process Name' (Shell Infrastructure Host).

Use this to:

- Build a new Main Query in a new tab.
- Build a new Main Query in the current tab.
- Add the attribute to the Main Query in the current tab.
- Add the attribute to a Sub Query that will run on the data that has already been pulled from the SentinelOne Cloud in the Main Query.
- Use the True Context ID, a group of related events, based on the intelligent event query engine, to see only the information related to the specific event group.

A screenshot of the SentinelOne Cloud interface. On the left, there's a table with columns: Object Type (PROCESS), Event Type (Process Creation), and Endpoint (sonar). Below this is a section titled 'ENDPOINT INFO' with details like Agent Os (windows), Site Id (396839257262031622), Agent Name (sonar), etc. A context menu is open over the endpoint 'sonar', with options: 'New Main Query (new tab)', 'New Main Query (current tab)', 'Add to Main Query (current tab)', 'Add to Sub Query', 'True Context' (2B1F723B7EA3B73C), 'Process ID' (3056), 'Event Type' (Process Creation), 'User Name' (SONAR\sonar01), and 'Created At' (Apr 8, 2019 05:30:20).

- Copy attributes to your clipboard.

A screenshot of the SentinelOne Cloud interface showing a table with columns: Attribute, Process ID (2744), Process Name (SIH Client), MD5 (16750beaa479f928690ebe6f4e36f6b4), SHA1 (9f91389c1618cd52...), Full Path (\Device\HarddiskVol...), and Group Id (9b4efcb10947). A mouse cursor is hovering over the MD5 value, which is highlighted with a blue circle. A tooltip at the bottom of the table says '(CTRL+C to copy this content to clipboard)'.

- Sort columns and look for outliers.

Parent Process Name	
Adobe Reader and Acrobat Manager	
Host Process for Windows Services	
Host Process for Windows Services	

- Jump directly to a related threat from Deep Visibility.

A new **Related to Threat** column shows in the Deep Visibility results table. Scroll right to see it.

30 Results	50 Results	Columns
<b>Related To Threat</b>		
True		
True		
True		

If a Deep Visibility event is related to a detected threat, click **True** to go directly to the Forensics details of the threat in the Management Console. If there is no related threat, **False** shows.

## Take Action from the Visibility Page

- Select an event and click **Actions**. The options depend on the event type. They include:

<b>Actions</b>		4 Items selected
Disconnect From Network		
Fetch Logs		
Mark As Threat		
<input checked="" type="checkbox"/> PROCESS		Process Creation

- Disconnect From Network** - The Agent can communicate only with the Management Console. The endpoint cannot communicate with other components on the network.
- Fetch Logs** - When you click this, the Agent collects relevant logs.

To get the logs, click **Activity > Administrative > Log operations**. When the logs are on the Management Console, the download button will be available.

- Mark as threat** - This is available for a process or file, but not a DNS or URL. It creates an active threat on the Dashboard for all included hashes, adds the specific process to the blacklist, and kills the process if it is running on Agents.

- Click an endpoint name to open its details and run more **Actions**.

ENDPOINT DETAILS  
LAPTOP-3QCJ3N0D

**GENERAL APP INVENTORY**

	Windows 10 (64 bit) Last active 2 hours ago Site name wee	Health status Last logged in user Group name
Agent version	2.9.2.36 <b>UPDATED</b>	Console connection
Scan status	Completed ( Mar 16, 2023 )	Network status
Memory	7.89 GB	Domain
CPU	8 X Intel(R) Core(TM) i7-...	Subscribed on
Core count	8	Console visible
Disk encryption	Off	IP Address
UUID	e61e13e50d8c18b07c0...	

Network Adapters:

NAME	IP	MAC ADD
------	----	---------

**Actions**

- Search...
- Configuration
- Configure Firewall Logg...
- Decommission
- Disconnect From Netw...
- Fetch Logs
- File Fetch
- Initiate Scan
- Move To Another Site
- Reboot

## 13.2. Deep Visibility Query Syntax

Create powerful queries for relevant threat hunting. In the Management Console, click **Visibility**.

New Tab **+**

Load Query **▼** Save New Query

**1** Main Query

**2** Events **▼** Start Hunting...

### Syntax Notes

- Values are in quotes: "

- Queries with different logical operators: Group each query in parentheses ( )  
The parentheses are a syntax sign. Do not use them to make a query easier to read.
- Date and time format: *dd.mm.yyyy hh:mm*
- Case: Values are case-sensitive
- Delimiter: Default delimiter between multiple values is comma (,) with an optional space
- Valid syntax icon: Invalid syntax shows a red X icon in the query field, valid shows a green icon

## Deep Visibility Query Fields

Field	Valid Values	Example
AgentName	String: Hostname of endpoint on which Agent is installed	AgentName NOT IN ("GW", "gateway") Matches: Endpoints with hostnames that do not include "GW" or "gateway", such as: "DefaultGW" or "gateway1".
AgentOS	String: windows, osx, linux	AgentOS="osx" Matches: Endpoints running macOS
AgentVersion	String: Version number of SentinelOne Agent	AgentVersion CONTAINS "2.6" Matches: Endpoints with an Agent version number that contains "2.6"
ConnectionStatus	String	ConnectionStatus Does Not Contain "SUCCESS" Matches: Endpoints whose TCP connection status was unsuccessful
DNSRequest	String: DNS name	DNSRequest CONTAINS "cdn.onenote" Matches: DNS requests to cdn.onenote
DNSResponse	String: IP address, DNS, type, or similar data from a DNS response	DNSResponse IS NOT EMPTY AND AgentOS = "linux" Matches: Non-empty DNS responses to Linux endpoints
DstIP	String: IP address of the destination	DstIP = "192.0.2.1" Matches: Items arriving to this IP
DstPort	Numeric: Port number of destination	DstPort = 80 Matches: Items arriving to any host over this port
FileCreatedAt	DateTime: Date and time of file creation	FileCreatedAt BETWEEN "17.11.2018 00:00" AND "18.11.2018 23:59" Matches: Files created in this range
FileFullName	String: Path and filename	FileFullName CONTAINS ".pdf" Matches: PDF files

Field	Valid Values	Example
FileID	String: Unique ID of the file	FileId = "F32D8A2B-E426-4258-A65C-819415D897EF"
FileMD5	String: MD5 signature	FileMD5 CONTAINS "1bc29b36f623" Matches: Files with an MD5 that has this string in it
FileModifyAt	DateTime: Date and time of file change	FileModifyAt > "22.10.2018 00:00" Matches: Files changed before this date and time
FileSHA1	String: SHA1 signature	FileSHA1 IN ( "415ab40ae9","888" ) Matches: Files with a SHA1 with one of these partial strings
FileSHA256	String: SHA256 signature	FileSHA256 IS NOT EMPTY Matches: Files with a SHA256 signature
IndicatorCategory	String	indicatorCategory = "Injection" Matches: Events in the Injection category.
IndicatorDescription	String	indicatorDescription contains "T1084" Matches: Events that contain the MITRE technique T1084.
IndicatorMetadata	String	indicatorMetadata contains "KeyName" Matches: Events that contain KeyName.
IndicatorName	String	indicatorName = "SuspiciousLibraryLoad" Matches: Events that contain SuspiciousLibraryLoad.
NetworkMethod	String: GET, POST, PUT, DELETE	NetworkMethod = "POST" Matches: POST events
NetworkUrl	String: Complete URL	NetworkUrl CONTAINS "https://outlook.office365.com" Matches: Networking to this URL or its subdomains
OldFileName	String: Name of file before rename	OldFileName Contains "king" Matches: Event with Event Type "File Rename" (and shows current name)
OldFileSHA1	String: SHA1 of file before it was changed	OldFileSHA1 Is Not Empty
PID	Numeric: Process ID (usually copied from main query to new tab)	PID <= "500" OR PID >= "900" Matches: PIDs between 500 and 900

Field	Valid Values	Example
ParentPID	Numeric: ID of process that created a new process	ParentPID > "1" Matches: PIDs greater than 1 that created a child process
ParentProcessName	String: Name of process that spawned a child process	ParentProcessName Is Not Empty Matches: Process creation events
ParentProcessStartTime	DateTime: Time parent process started to run	ParentProcessName Contains "system" AND ParentProcessStartTime > "Jul 22, 2019 00:00:33" Matches: Processes such as "system_profile" that triggered a process creation event after half-past midnight on July 22.
ParentProcessUniqueKey	String: Unique ID of parent process	ParentProcessUniqueKey Contains "6EDC55FB"
ProcessCmd	String: Command arguments sent with a process	ProcessCmd ~ "delete %systemdrive%" Matches: Processes that send a command to delete the system drive
ProcessDisplayName	String: Display name of process	ProcessDisplayName Contains "Update" Matches: Processes with "Update" in the display name, such as the "upfc.exe" process with the display name: "Updateability From SCM"
ProcessImagePath	String: Pathname of running process	ProcessImagePath CONTAINS "\Hard" Matches: Processes running in the hard drive (or other folder that starts with "Hard")
ProcessImageSha1Hash	String: SHA1 signature of running process	ProcessImageSha1Hash IS_EMPTY Matches: Running Processes that do not have a SHA1 signature
ProcessIntegrityLevel	String: SYSTEM (operating system processes), HIGH (administrators), MEDIUM (non-administrators), LOW (temporary Internet files), UNTRUSTED	ProcessIntegrityLevel = "HIGH" Matches: Cleaners, system tasks, and other processes triggered by admin-level users and scripts
ProcessName	String: Name of process	ProcessName IS NOT EMPTY AND DstPort = "443" Matches: Any process going to port 443

Field	Valid Values	Example
ProcessSessionId	Numeric: ID of the terminal (cmd, shell, or other terminal) session on which the process ran	ProcessSessionId > "1"
ProcessStartTime	DateTime: Time process started to run	ProcessStartTime BETWEEN "22.10.2018 00:00" AND "22.10.2018 05:00" Matches: Processes that started in this range
ProcessSubSystem	String: SYS_WIN32, SYS_WSL, SUBSYSTEM_UNKNOWN	ProcessSubSystem = "SUBSYSTEM_UNKNOWN" Matches: Processes on non-Windows endpoints
ProcessUniqueKey	String: Unique ID of process	ProcessUniqueKey = "482B618E-9AEF-4791-AA4B-04DC6B52D421" Matches: Instances of this process
RegistryID	String: Registry Key Unique ID generated by the SentinelOne Agent for Windows endpoints	RegistryId Contains "3344" Matches: Events for registry value created, modified, or deleted, filtered for this partial string in the UID
RegistryPath	String: Full path location of the Registry Key entry	RegistryPath Is Not Empty Matches: Events for registry value created, modified, or deleted
Rpid	Numeric: PID after relinked	Rpid = "1048" Matches: Events for file creation and file rename, filtered for this ID
SignatureSignedInvalidReason	String	SignatureSignedInvalidReason Is Not Empty Matches: Unverified signatures with reason
Signer	String: Identity of file signer	Signer Is Empty Matches: Unsigned file events
Sitelid	String: SentinelOne Site token	Sitelid ~ "63517" Matches: The site with this partial string in its ID
SiteName	String: SentinelOne Site name	SiteName NOT IN ( "corp", "acme" ) Matches: All sites that do not have "corp" or "acme" in their names.
SrcIP	String: IP address of traffic source	SrcIP CONTAINS "10" Matches: Items from a source IP that includes "10"
SrcPort	Numeric: Port number of traffic source	SrcPort != "9" AND SrcIP CONTAINS "10" Matches: Items from any port other than 9 and an IP that includes "10"

Field	Valid Values	Example
TaskName	String: Name of a scheduled task, as generated by the Host	TaskName Is Not Empty Matches: Task events
TaskPath	String: Full path location of a scheduled task	TaskPath Contains "Google" Matches: Processes started from a Google path, such as C:\Program Files\Google\Update\GoogleUpdate.exe
Tid	String: Thread ID	Tid = "5340" Matches: File events with this thread ID
TrueContext	String: ID of all objects associated with a SentinelOne detection	TrueContext = "D7E32540-15AB-4916-8A55-A80E956FC5CC" Matches: All events or processes grouped with this detection
User	String: Name of endpoint user	User CONTAINS "admin" Matches: Items with a username that includes "admin"

## Deep Visibility Query Keywords and Operators

Operator	Valid for Field Types	Matches:
AND	All	Two true expressions
OR	All	One or both of two expressions
=	Numeric, String	Exact match
!=	Numeric, String	Items that do not have this string or number
<	Numeric, DateTime	Less than this number or earlier than this date
<=	Numeric, DateTime	Equal to or less than this number, or on this date or earlier
>	Numeric, DateTime	Greater than this number or later than this date
>=	Numeric, DateTime	Equal to or greater than this number, or on this date or later
~	String	Partial string
BETWEEN	Numeric, DateTime	Range of <i>start</i> AND <i>end</i>
CONTAINS	String	Partial string
DOES NOT CONTAIN	String	Items that do not have this partial string
IN	String	Items that have one or more of these strings
IS EMPTY	String	Null
IS NOT EMPTY	String	Items that have a value for this string

Operator	Valid for Field Types	Matches:
NOT IN	String	Items that do not have any of these strings
RegExp	String	Regular Expression, <a href="#">POSIX extended syntax</a>
ContainsCIS	String	Case-insensitive partial string
Does Not ContainCIS	String	Items that do not have this partial string, case-insensitive
StartsWith	String	Items that start with this partial string
StartsWithCIS	String	Items that start with this partial string, case-insensitive
EndsWith	String	Items that end with this partial string
EndsWithCIS	String	Items that end with this partial string, case-insensitive

### 13.3. Threat Hunting Use Cases

The next topics show general examples of how to use Deep Visibility in a real-world environment.

Each use case shows how Deep Visibility finds the context around a piece of information or event. There are many potential ways to follow through with a hunt. Each example shows one way.

- [Hunting for Living Off the Land Attacks \[186\]](#)
- [Hunting for Abnormal Scheduled Task Creation \[185\]](#)
- [Hunting for Abnormal Behavior by Known Characteristic](#)
- [Responding to Incidents with Deep Visibility \[188\]](#)

#### 13.3.1. Hunting for Abnormal Scheduled Task Creation

**Use Case:** Attacks often create a scheduled task. If a malicious process can get into this service, it can be used for persistence, to run a lateral movement attack during work hours with privileges, or other techniques.

**Example - searching for abnormally-created scheduled tasks:**

1. In the sidebar, click **Visibility** .
2. Create the query to search for abnormal schtasks processes:
  - a. In the Events or Processes drop-down, click **Processes**.
  - b. Click **ProcessCmd**.
  - c. Click **RegExp**.
  - d. In the given quotes, enter: `schtasks`
  - e. Press space and then click **AND**.
  - f. Click **ProcessName**.

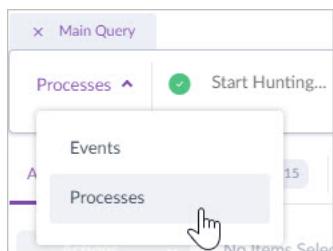
- g. Click !=.
  - h. In the given quotes add this string: Manages scheduled tasks
- OR: Click **IndicatorName**, = and in the given quotes enter this string: ScheduleTaskRegister
3. Select a time frame for the query.
  4. Press enter from the query field or click .
  5. If there is a result, we want to see all the processes, files, and events around that technique. Click the blue circle of the True Context ID and run a new query.

### 13.3.2. Hunting for Living Off the Land Attacks

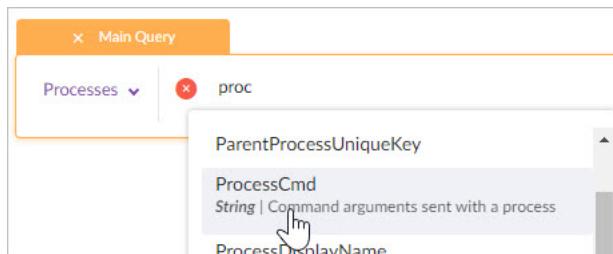
**Use Case:** Attackers often use legitimate endpoint processes to evade detection while they carry out malicious tasks. Let's see if your environment shows an indication of this compromise.

#### Example - searching for processes that create new users:

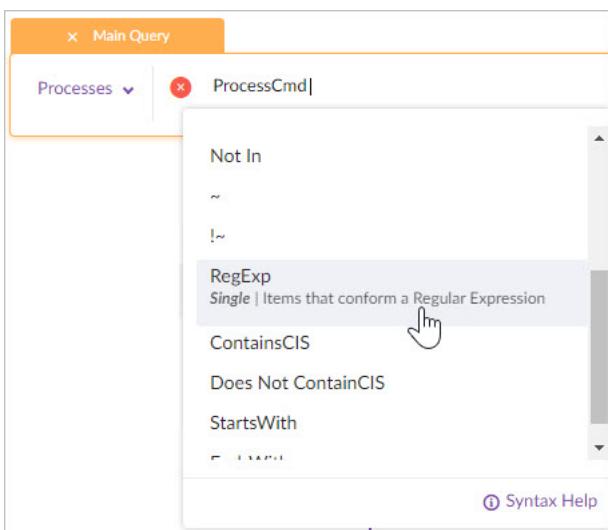
1. In the sidebar, click **Visibility** .
2. Click **Processes**.



3. Click in the query bar (where it shows **Start Hunting...**) and enter `Proc`. When the list of valid options shows, click **ProcessCmd**.



4. In the list of valid operators that shows, scroll down and click **RegExp**.



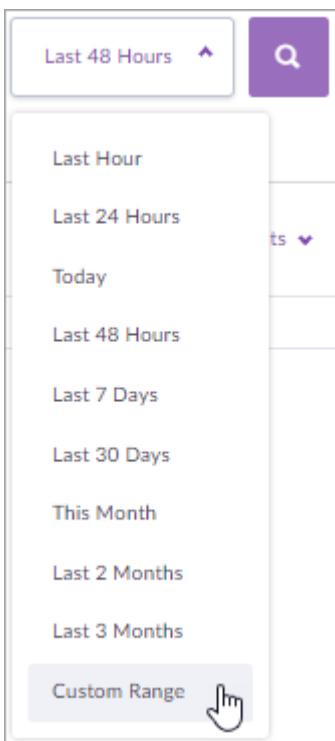
5. In the given quotes, enter: net\s+user(?:(!\s+/add)(?:.|\\n))\*\s+/add

This regular expression will find net users added by a process.

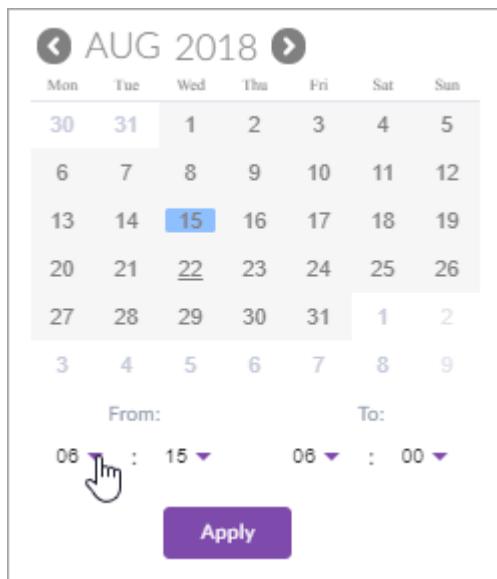


Notice the green checkmark. The query is valid.

6. Let's run our query on all processes detected in the last year. In the date range drop-down, click **Custom Range**.



- In the calendar that opens, click the arrow to go back to last year and then click the date of one year ago.



Click the forward arrow to get to today's date. In the current month, click the date. The cursor is released. Click **Apply**.

- Press enter from the query field or click

The query results open in chronological order.

All Events	Processes	Files	DNS	URL	Network Actions	Registry	Scheduled Tasks
No items Selected							
Endpoint	Object Type	Event Type	Time	True Context	User	Attribute	
█	PROCESS	Process Creation	Sep 23, 2019 08:03:52	0302266A31DF3722	NT AUTHORITY\SYSTEM	Agent Os windows	Process ID 4572 Process UID 8F6B7A828632F7
█	PROCESS	Process Creation	Sep 23, 2019 08:03:52	0302266A31DF3722	NT AUTHORITY\SYSTEM	Agent Os windows	Process ID 9488 Process UID C1B7F89E999FD+
█	PROCESS	Process Creation	Sep 23, 2019 07:33:52	0302266A31DF3722	NT AUTHORITY\SYSTEM	Agent Os windows	Process ID 9568 Process UID 0A380CFFAD3BC
█	PROCESS	Process Creation	Sep 23, 2019 07:33:52	0302266A31DF3722	NT AUTHORITY\SYSTEM	Agent Os windows	Process ID 3056 Process UID F45698E18FC64C
█	DNS	DNS-Resolved	Sep 23, 2019 08:04:33	0466AF3D6FFE180F	N/A	Agent Os windows	Process ID 1764 Process UID A51CA257BB9E1;
█	DNS	DNS-Resolved	Sep 23, 2019 07:34:02	0466AF3D6FFE180F	N/A	Agent Os windows	Process ID 1764 Process UID A51CA257BB9E1;

- Select one or more results and then click **Actions > Fetch Logs**.

Or, if you are sure the process is malicious, select the row of one endpoint and then click **Actions > Disconnect from Network**.

### 13.3.3. Responding to Incidents with Deep Visibility

**Use Case:** You mitigated a threat in your environment. Now you want to see if it is anywhere else in the network.

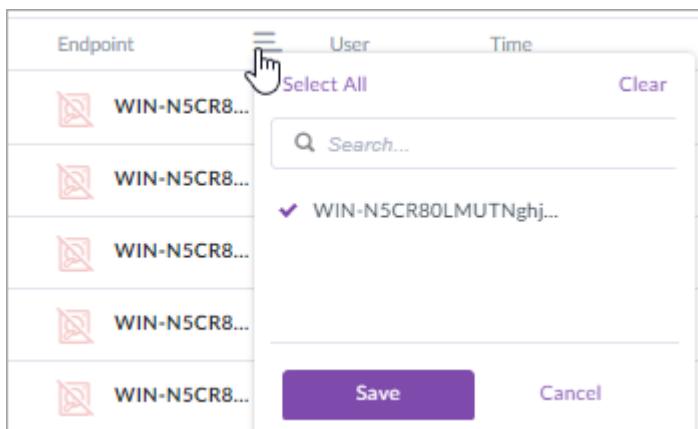
## Example: Investigate and Respond to a Threat with Deep Visibility:

1. In the Management Console > **Forensics details**, copy the SHA1 hash of the detection.
2. In the sidebar, click **Visibility** .
3. In the query field, select **FileSHA1** and **=**. In the given quotes, paste the copied SHA1.



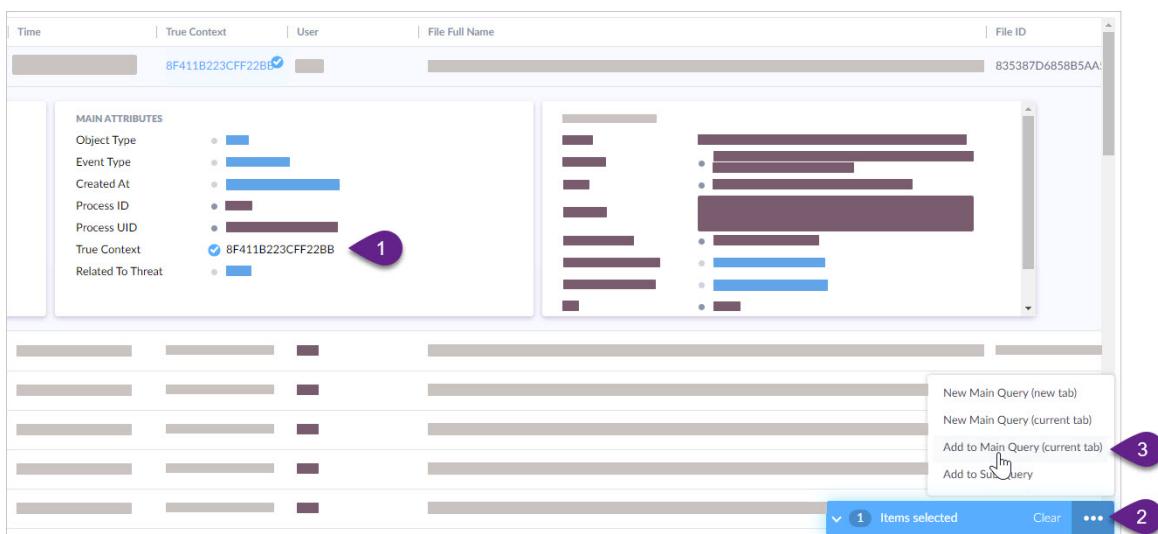
The screenshot shows the 'Editing the Main query' dialog. At the top, it says 'Editing the Main query'. Below that, there's a dropdown menu set to 'Events' and a search bar containing the query 'FileSha1 = "0193d486448ace72970ab36fb05e32233bf01d84"'.

4. See in the results which endpoints ever had the file installed.



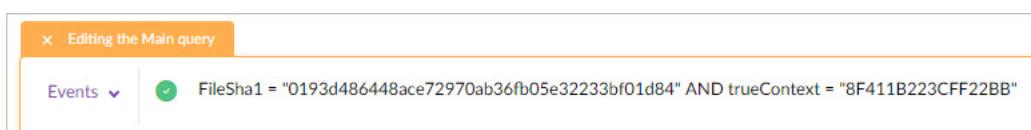
The screenshot shows the 'Select All' dialog. It lists several endpoints, each with a checkbox. One endpoint, 'WIN-N5CR8...', has its checkbox checked. At the bottom, there are 'Save' and 'Cancel' buttons.

5. Expand a row. Click the blue open circle of True Context ID. In the sub menu, click **Add to Main Query**.



The screenshot shows the 'True Context' details view. At the top, it displays 'Time', 'True Context', 'User', 'File Full Name', and 'File ID'. Below this, there's a table with columns for 'MAIN ATTRIBUTES' and other data. A blue circle highlights the 'True Context' column under 'MAIN ATTRIBUTES'. Callout 1 points to this circle. Callout 2 points to the bottom right corner of the screen where a context menu is open, showing options like 'New Main Query (new tab)', 'New Main Query (current tab)', 'Add to Main Query (current tab)', and 'Add to SubQuery'. Callout 3 points to the 'Add to Main Query (current tab)' option in the menu. At the bottom, there are buttons for '1 Items selected', 'Clear', and three dots.

The main query automatically adds the True Context ID syntax with **AND**.



The screenshot shows the 'Editing the Main query' dialog again. The query now includes 'FileSha1 = "0193d486448ace72970ab36fb05e32233bf01d84"' AND 'trueContext = "8F411B223CFF22BB"'.

6. Press enter.
7. From the results, continue to look for abnormalities, such as processes that run out of non-standard folders and files that are written to nonstandard locations. Use the suspicious results as pivot points.

## 13.4. Configuring Deep Visibility Data Collection [Multi-Site]

Deep Visibility is part of the SentinelOne Complete bundle and requires an extra license. If you do not see the options described here, contact SentinelOne to get the required licenses.

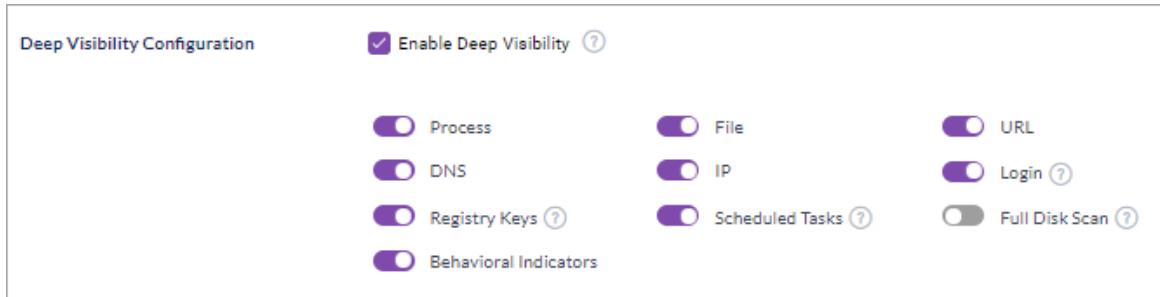
Enable Deep Visibility in the policy. The Deep Visibility settings can be different in the Global policy and in Site policies. In the policy settings, you can refine the data sent for Threat Hunting.

### To enable Deep Visibility:

1. In the sidebar, click **Network** .
2. In the **Network** toolbar, click **Policy**.



3. In **Deep Visibility Configuration**:



- a. Select **Enable Deep Visibility**.  
If this is not selected, Deep Visibility queries will have no results.
- b. Select the data types to be sent for Threat Hunting. You must keep **Process** selected.
4. Click **Save**.

Data Type	Source	Data Collected
Process	Processes created	<ul style="list-style-type: none"> <li>• Name, ID, and time of the process and its creator process</li> <li>• Command-line arguments used by the created process</li> <li>• Executable full path and SHA1 of the created process</li> </ul>

Data Type	Source	Data Collected
File	Supported file types [231] that were created, changed, or deleted by an event	Hash (MD5, SHA1, SHA256), full path, name of the process that created or changed the file Note for macOS Agent versions 3.4.0 and later: If the On-Write engines are disabled, file data is not collected.
URL	Sites visited in Safari, Chrome, and Microsoft browsers	URLs and URIs (string, source (wininet or Chrome), HTTP method, processes and creator processes, and (MS only) request and response. From wget, curl, and similar commands: DNS, IP addresses, and (macOS only) URLs
DNS	Every connection, including connections to <i>localhost</i>	Query name, query result, processes, and creator processes
IP	Outgoing network connections	TCPv4 connection attempts (source IP address and port, destination IP address and port, protocol, processes and creator processes)
Login	macOS end user login and logout	Username and login and logout time
Registry Keys	Registry Key events on Windows endpoints	Registry Key ID and name, logged in user, time of event, process that caused the event
Scheduled Tasks	Scheduled Task events on Windows endpoints	Task name, event type, logged in user, time of event, process that caused the event
Full Disk Scan	Files scanned by the Full Disk Scan	Files with extensions that are supported by the DFI engine
Behavioral Indicators	Indicators found by the Agent	Indicator Category, Indicator Description, Indicator Metadata, and Indicator Name

## 13.5. Searching for Behavioral Indicators

The ability to search for Mitre techniques in EDR vendors is a growing trend. Threat Hunting teams across security vectors require a correlation between their environments and Mitre knowledge. SentinelOne leverages our Dynamic Behavioral engine to show the behavior of processes in the endpoints. To make it easier and faster for you to use this knowledge, we map our behavioral indicators to the Mitre ATT&CK framework. You can create queries out-of-the-box and search for Mitre attack characteristics across your scope of endpoints. With other EDR vendors, you would have to create a multitude of complex hunting queries to cover all the findings of Mitre. With SentinelOne, all you need is the Mitre ID or another string in the description, the category, the name, or metadata.

The screenshot shows the 'Editing the Main query' interface. A search bar at the top contains the text 'indicator'. Below it, a dropdown menu is open, showing several options under 'IndicatorName': 'IndicatorCategory', 'IndicatorDescription', 'IndicatorMetadata', and 'IndicatorName String | Indicator name'. The 'IndicatorName String | Indicator name' option is highlighted. On the left, there are filters for 'Events' (selected), 'All Events 69', 'Actions', and 'Endpoint'. At the bottom right, there is a 'Syntax Help' link.

For example, in SentinelOne Deep Visibility, use this query to find any process or event with behavioral characteristics of the attack technique known as Process Injection:

```
IndicatorDescription Contains "T1055"
```

With a different vendor, you will need to create a complex regular expression query, and run it many times with changes for known characteristic tweaks. If you look at [Mitre's page for T1055](#), you notice that you will need a different query for macOS, Linux, and Windows. Then there are more than 50 examples of malware and compromised utilities. You would need a query for each.

#### To see Mitre-Behavior Indicator mapped results:

- Click the **Indicators** tab in the Visibility page to see the indicator data.

The screenshot shows the 'Indicators' tab selected in the navigation bar. It displays a table with the following columns: Endpoint, Indicator Name, Indicator Category, Indicator Description, and Indicator Metadata. There are six rows, each corresponding to a process named 'avi-win1' that has loaded a suspicious library. The 'Indicator Name' column lists 'SuspiciousLibraryLoad', 'Indicator Category' lists 'Injection', 'Indicator Description' lists 'Suspicious library loaded into the process memory', and 'Indicator Metadata' lists 'Library: \Device\HarddiskVolume2\'.

All Events 34	Indicators 34			
No Items Selected				
Endpoint	Indicator Name	Indicator Category	Indicator Description	Indicator Metadata
<input type="checkbox"/> avi-win1	SuspiciousLibraryLoad	Injection	Suspicious library loaded into the process memory	Library: \Device\HarddiskVolume2\'
<input type="checkbox"/> avi-win1	SuspiciousLibraryLoad	Injection	Suspicious library loaded into the process memory	Library: \Device\HarddiskVolume2\'
<input type="checkbox"/> avi-win1	SuspiciousLibraryLoad	Injection	Suspicious library loaded into the process memory	Library: \Device\HarddiskVolume2\'
<input type="checkbox"/> avi-win1	SuspiciousLibraryLoad	Injection	Suspicious library loaded into the process memory	Library: \Device\HarddiskVolume2\'
<input type="checkbox"/> avi-win1	SuspiciousLibraryLoad	Injection	Suspicious library loaded into the process memory	Library: \Device\HarddiskVolume2\'
<input type="checkbox"/> avi-win1	SuspiciousLibraryLoad	Injection	Suspicious library loaded into the process memory	Library: \Device\HarddiskVolume2\'

- Click a row to see more details. The Indicator Description includes a link to that technique's Mitre page.

**OTHER ATTRIBUTES**

Process Name	Microsoft OneDrive (32 bit) Setup
Indicator Name	RegistryCOMObject
Indicator Description	Application has registered itself to become persistent via COM object. <a href="#">MITRE: Persistence [T1084]</a>
Indicator Category	Persistence
Indicator Metadata	KeyName: \REGISTRY\USER\S-1-5-21-3498676248-3132314867-1953175905-1001 Classes\CLSID\{4410DC33-BC7C-496B-AA84-4AE3EEE75F7}\InProcServer32 ValueName: ValueData: \Device\HarddiskVolume2\Users\ADMIN\AppData\Local\Microsoft\OneDrive\19.123.0624.0005\amd64\F...
	<a href="#">Show More</a>

To enable the Agent to send behavioral indicator data:

Click Policy > Deep Visibility Configuration > Behavioral Indicators.

The screenshot shows the 'Deep Visibility Configuration' section. At the top, there is a checked checkbox labeled 'Enable Deep Visibility'. Below it, there are several toggle switches for different types of visibility: Process, File, URL, DNS, IP, Login, Registry Keys, Scheduled Tasks, and Behavioral Indicators. The 'Behavioral Indicators' toggle switch is highlighted with a red box.

### 13.5.1. List of Indicator Names and Categories

Use items from the Indicator Category listed here to perform **IndicatorCategory** queries on the on the Visibility page.

Use items from the Indicator Name listed here to perform **IndicatorName** queries on the Visibility page.

Use items from the Indicator Description listed here to perform **IndicatorDescription** queries on the Visibility page.

**Important:** The Visibility search is case-sensitive.

Engine	Indicator Category	Indicator Name	Indicator Description
Windows Dynamic	Boot Configuration Update	KMCIdisabled	Ability to load unverified drivers was enabled. MITRE: Persistence {T1215, T1050}
Windows Dynamic	Exploitation	StackPivot	Altered process code flow to enable running of malicious code (StackPivot behavior). MITRE: Execution {T1203}

Windows Dynamic	Persistence	SuspiciousPersistence	Application has registered itself to become persistent
Windows Dynamic	Persistence	WMI	Application has registered itself to become persistent via WMI. MITRE: Persistence {T1084}
Windows Dynamic	Persistence	SuspiciousPersistence	Application has registered itself to become persistent
Windows Dynamic	Privilege Escalation	UACBypass	Attempt to bypass UAC (User Account Control). MITRE: Privilege Escalation {T1088}, Defense Evasion {T1088}
Windows Dynamic	Privilege Escalation	UACBypass	Attempt to bypass UAC (User Account Control). MITRE: Privilege Escalation {T1088}, Defense Evasion {T1088}
Windows Dynamic	Privilege Escalation	NamedPipeImpersonation	Attempt to escalate System privileges via Meterpreter. MITRE: Privilege Escalation
Windows Dynamic	Privilege Escalation	NamedPipeImpersonation	Attempt to escalate System privileges via Meterpreter. MITRE: Privilege Escalation
Windows Dynamic	Persistence	StickyKeys	Backdoor was created on the machine. MITRE: Persistence {T1015}
Windows Dynamic	Ransomware	RansomwareBehavior	Behaves like ransomware. MITRE: Execution
Windows Dynamic	Ransomware	RansomwareBehavior	Behaves like ransomware. MITRE: Execution
Windows Dynamic	Ransomware	RansomwareBehavior	Behaves like ransomware. MITRE: Execution
Windows Dynamic	Infostealer	Mimikatz	Behaves like Mimikatz. MITRE: Credential Access {T1098, T1145, T1081}
Windows Dynamic	Exploitation	SandboxEscape	Breakout from Internet Explorer sandbox. MITRE: Execution

Windows Dynamic	Exploitation	SuspiciousVBScript	Breakout from Internet Explorer sandbox. MITRE: Execution
Windows Dynamic	Injection	SuspiciousInjection	Code injection to other process memory space via Reflection. MITRE: Defense Evasion {T1055}
Windows Dynamic	Exploitation	SuspiciousDocument	Document behaves abnormally. MITRE: Execution {T1064}
Windows Dynamic	Exploitation	Metasploit	Execution of a metasploit stager. MITRE: Execution {T1064}
Windows Dynamic	Injection	SuspiciousInjection	Code injection to a remote process. MITRE: Defense Evasion {T1055}
Windows Dynamic	Malware	SuspiciousScript	Executed suspicious shell command. MITRE: Execution {T1064}
Windows Dynamic	Malware	SuspiciousJava	Exploit attempt on Java. MITRE: Execution {T1203}
Windows Dynamic	Evasion	RegHiddenValue	Hiding registry key. MITRE: Defense Evasion {T1112}
Windows Dynamic	Evasion	ProcessModification	Internal process resource was manipulated in memory. MITRE: Defense Evasion
Windows Dynamic	Privilege Escalation	ExploitPrivesc	Local privilege escalation exploit. MITRE: Privilege Escalation {T1068}
Windows Dynamic	Injection	SuspiciousInjection	Code injection to a remote process. MITRE: Defense Evasion {T1055}
Windows Dynamic	Infostealer	MITB	Man in the browser attack. MITRE: Collection {T1185}
Windows Dynamic	Infostealer	MITMProxy	Man in the middle attack. MITRE: Credential Access {T1040}
Windows Dynamic	Post Exploitation	Meterpreter	Metasploit's Meterpreter behavior was identified. MITRE: Execution {T1064}

Windows Dynamic	Post Exploitation	Koadic	PowerShell post-exploitation script was executed. MITRE: Execution {T1064, T1086}
Windows Dynamic	Post Exploitation	MaliciousPowershell	PowerShell post-exploitation script was executed. MITRE: Execution {T1064, T1086}
Windows Dynamic	Post Exploitation	MaliciousPowershell	PowerShell post-exploitation script was executed. MITRE: Execution {T1064, T1086}
Windows Dynamic	Post Exploitation	MaliciousPowershell	PowerShell post-exploitation script was executed. MITRE: Execution {T1064, T1086}
Windows Dynamic	Post Exploitation	MaliciousPowershell	PowerShell post-exploitation script was executed. MITRE: Execution {T1064, T1086}
Windows Dynamic	Evasion	AvoidMitigationAttempt	Process characteristics were changed suspiciously. MITRE: Persistence, Defense Evasion
Windows Dynamic	Evasion	AvoidMitigationAttempt	Process characteristics were changed suspiciously. MITRE: Persistence, Defense Evasion
Windows Dynamic	Evasion	AvoidMitigationAttempt	Process tried to bypass Anti-Virus hooks. MITRE: Defense Evasion.
Windows Dynamic	Infostealer	SensitiveMemoryAccess	Read sensitive information from LSASS. MITRE: Credential Access {T1003}
Windows Dynamic	Evasion	HidingTracks	Hiding tracks of execution. MITRE: Defense Evasion {T1158}, Persistence {T1158}

Windows Dynamic	Infostealer	AccessSyskey	Sensitive user information was queried. MITRE: Credential Access {T1003}
Windows Dynamic	Exploitation	SandboxEscape	Shellcode execution was detected. MITRE: Execution
Windows Dynamic	Exploitation	SuspiciousShellcode	Shellcode execution was detected. MITRE: Execution
Windows Dynamic	Evasion	Doppelganger	Attempt to evade monitoring using the "Doppelganger" technique. MITRE: Defense Evasion {T1186}
Windows Dynamic	Evasion	ProcessHollowing	Attempt to evade monitoring using the "Process hollowing" technique. MITRE: Defense Evasion {T1093}
Windows Dynamic	Injection	SuspiciousInjection	Unusual code injection to a remote process. MITRE: Defense Evasion {T1055}, Privilege Escalation {T1055}
Windows Dynamic	Injection	SuspiciousInjection	Unusual code injection to a remote process. MITRE: Defense Evasion {T1055}, Privilege Escalation {T1055}
Windows Dynamic	Post Exploitation	SuspiciousDriverLoad	Unverified driver was loaded. MITRE: Persistence {T1215}
Windows Dynamic	Boot Configuration Update	WriteToMBR	Write action to protected section of the operating system. MITRE: Persistence {T1067}
Windows Dynamic	Exploitation	SensitiveMemoryAccess	Write action to LSASS process. MITRE: Credential Access {T1098}
Windows Dynamic	Evasion	HookRemovalAttempt	A function was unhooked. MITRE: Defense Evasion
Windows Dynamic	Exploitation	NullPageAllocation	Altered process code flow to enable running of malicious code. MITRE: Execution

Windows Dynamic	Exploitation	StackProtectionModification	Altered process code flow to enable running of malicious code. MITRE: Execution
Windows Dynamic	Evasion	AntiDebugging	Anti-debug technique was used. MITRE: Defense Evasion
Windows Dynamic	Evasion	AntiVm	Anti-VM technique was used. MITRE: Defense Evasion
Windows Dynamic	Persistence	WMI	Application has registered itself to become persistent via WMI. MITRE: Persistence {T1084}
Windows Dynamic	Persistence	DllHijack	Application has registered itself to become persistent. MITRE: Persistence
Windows Dynamic	Privilege Escalation	UACBypass	Attempt to bypass UAC (User Account Control). MITRE: Privilege Escalation {T1088}, Defense Evasion {T1088}
Windows Dynamic	Privilege Escalation	UACBypass	Attempt to bypass UAC (User Account Control). MITRE: Privilege Escalation {T1088}, Defense Evasion {T1088}
Windows Dynamic	Privilege Escalation	TokenManipulation	Authentication data manipulation. MITRE: Persistence {T1131}
Windows Dynamic	Infostealer	SuspiciousKeylogging	Behaves like a keylogger. MITRE: Credential Access {T1056}, Collection {T1056}
Windows Dynamic	Infostealer	SuspiciousKeylogging	Behaves like a keylogger. MITRE: Credential Access {T1056}, Collection {T1056}
Windows Dynamic	Infostealer		Behaves like a memory scraper. MITRE: Collection {T1005, T1119}
Windows Dynamic	Ransomware	RansomwareBehavior	Behaves like ransomware because of file operations. MITRE: Execution

Windows Dynamic	Ransomware	RansomwareBehavior	Behaves like ransomware because of file operations. MITRE: Execution
Windows Dynamic	Ransomware	RansomwareBehavior	Behaves like ransomware because of file operations. MITRE: Execution
Windows Dynamic	Ransomware	RansomwareBehavior	Behaves like ransomware. MITRE: Execution
Windows Dynamic	Injection	AtomBombing	Code injection to other process memory space using the "Atom bombing" technique. MITRE: Defense Evasion {T1055}, Privilege Escalation {T1055}
Windows Dynamic	Injection	SuspiciousInjection	Code migration into system process was detected. MITRE: Defense Evasion {T1055}, Privilege Escalation {T1055}
Windows Dynamic	Injection	SuspiciousInjection	Code was executed in a remote process. MITRE: Defense Evasion {T1055}, Privilege Escalation {T1055}
Windows Dynamic	Exploitation	SuspiciousDocument	Document behaves abnormally. MITRE: Execution {T1064}
Windows Dynamic	Injection	SuspiciousInjection	Code injection to a remote process. MITRE: Defense Evasion {T1055}
Windows Dynamic	Reconnaissance	SuspiciousLdapQuery	Domain information was gathered via LDAP query. MITRE: Discovery {T1087, T1069}
Windows Dynamic	Exploitation	KernelExploitAttempt	Information gathered for kernel exploitation. MITRE: Discovery {T1082}
Windows Dynamic	Evasion	HeavensGate	Manipulated code execution flow using the "Heaven's Gate" technique. MITRE: Execution

Windows Dynamic	Exploitation	ReverseShell	Remote shell was opened. MITRE: Command and Control {T1071}
Windows Dynamic	Exploitation	ReverseShell	Remote shell was opened. MITRE: Command and Control {T1071}
Windows Dynamic	Exploitation	SuspiciousShellcode	Shellcode execution was detected. MITRE: Execution {T1106, T1064}
Windows Dynamic	Exploitation	SuspiciousShellcode	Shellcode execution was detected. MITRE: Execution {T1106, T1064}
Windows Dynamic	Exploitation	SuspiciousShellcode	Shellcode execution from powershell was detected. MITRE: Execution {T1086, T1106, T1064}
Windows Dynamic	Exploitation	SandboxEscape	Shellcode execution was detected. MITRE: Execution {T1106, T1064}
Windows Dynamic	Exploitation	SuspiciousShellcode	Shellcode execution was detected. MITRE: Execution {T1106, T1064}
Windows Dynamic	Injection	SuspiciousLibraryLoad	Suspicious library loaded into the process memory
Windows Dynamic	Evasion	SuspiciousSMBTraffic	Suspicious SMB activity was detected. MITRE: Discovery {T1135}, Lateral Movement {T1077}
Windows Dynamic	Evasion	SuspiciousDNSTraffic	Suspicious DNS activity was detected MITRE: Command and Control {T1071}
Windows Dynamic	Evasion	AttemptToUseSyscallDirectly	Attempt to evade monitoring. MITRE: Defense Evasion
Windows Dynamic	Infostealer	BrowserInfoStealing	Chrome's sensitive information was accessed. MITRE: Collection {T1213}
Windows Dynamic	Infostealer	BrowserInfoStealing	Firefox's sensitive information was accessed. MITRE: Collection {T1213}

Windows Dynamic	Infostealer	DumpSAM	SAM database was exported. MITRE: Credential Dumping {T1003}
Windows Dynamic	Evasion	ProcessModification	Manipulated remote process structure. MITRE: Privilege Escalation {T1179}
Windows Dynamic	Evasion	ProcessModification	Manipulated remote process structure. MITRE: Privilege Escalation {T1179}
Windows Dynamic	Boot Configuration Update	IntegrityCheckDisabled	Disable kernel code integrity checks. MITRE: Defense Evasion
Windows Dynamic	Evasion	DeleteWindowsBackupCat	Process tampered the Windows Backup Catalog. MITRE: Defense Evasion
Windows Dynamic	Exploitation	ROP	Altered process code flow to enable running malicious code. MITRE: Execution
Windows Dynamic	Evasion	HideRemoteProcessWindow	Process tampered with Windows user interface
Windows Dynamic	Evasion	EventViewerTampering	Process tampered with the event viewer logs. MITRE: Defense Evasion {T1089}
Windows Dynamic	Evasion	EventViewerTampering	Process deleted the Event Viewer logs. MITRE: Defense Evasion {T1089}
Windows Dynamic	Persistence	Autorun	A file that enables automatic launching from external drive was created. MITRE: Initial Access {T1091}
Windows Dynamic	Evasion	FakeFileName	A file was created with an internal system name. MITRE: Persistence
Windows Dynamic	Evasion	HookRemovalAttempt	A function was unhooked. MITRE: Defense Evasion
Windows Dynamic	Evasion	Packer	A Library was unpacked into its own memory space. MITRE: Defense Evasion

Windows Dynamic	Injection	LoadUnrelatedLibrary	A library owned by one process was loaded to other process. MITRE: Defense Evasion {T1038}, Privilege Escalation {T1038}
Windows Dynamic	Evasion	AddCertificate	A new root certificate was added. MITRE: Defense Evasion {T1130}
Windows Dynamic	Persistence	UserAdd	A new user account was added. MITRE: Persistence {T1136}
Windows Dynamic	Persistence	DebuggerPersistence	Application registered itself to become persistent. MITRE: Persistence
Windows Dynamic	Persistence	SafeModeConfigurationModification	Application registered itself to become persistent in safe mode. MITRE: Persistence
Windows Dynamic	Evasion	SafeModeConfigurationModification	Application manipulated safe mode configuration: MITRE: Persistence
Windows Dynamic	Evasion	AddFirewallException	Application added firewall rule to allow network traffic. MITRE: Exfiltration {T1041}
Windows Dynamic	Injection	SuspiciousProtectionModification	Changed protection type of library in a remote process space. MITRE: Privilege Escalation
Windows Dynamic	Evasion	PreloadInjection	Code injection to other process memory space. MITRE: Defense Evasion {T1038}, Privilege Escalation {T1038}
Windows Dynamic	Injection	RemoteInjection	Code injection to a remote process. MITRE: Defense Evasion {T1055}
Windows Dynamic	Evasion	DisableSecurityCenterEvents	Disabled security center notifications. MITRE: Defense Evasion {T1089}
Windows Dynamic	Evasion	HiddenFilesDisplayModification	Disabled showing hidden files and folders. MITRE: Defense Evasion

Windows Dynamic	Infostealer	EnableMemoryPlaintextPasswords	The store of plaintext passwords in memory was disabled/enabled. MITRE: Credential Access
Windows Dynamic	Injection	RemoteInjection	Code injection to a remote process. MITRE: Defense Evasion {T1055}
Windows Dynamic	Privilege Escalation	PrivilegedInstruction	Execution of privileged instruction was identified. MITRE: Privilege Escalation
Windows Dynamic	Evasion	ModifyHostsFile	Host file was modified. MITRE: Defense Evasion
Windows Dynamic	Evasion	InternetExplorerConfigurationModification	Internet Explorer offline mode was disabled. MITRE: Defense Evasion {T1089}
Windows Dynamic	Evasion	InternetExplorerConfigurationModification	Internet zone checks were disabled. MITRE: Defense Evasion {T1089}
Windows Dynamic	Injection	RemoteLibraryInjection	Library was injected to a remote process. MITRE: Defense Evasion {T1055}, Privilege Escalation {T1055}
Windows Dynamic	Evasion	PreventProcessExecution	Prevented execution of a process. MITRE: Defense Evasion
Windows Dynamic	Evasion	DisableTaskManager	Prevented the Task Manager from starting. MITRE: Defense Evasion
Windows Dynamic	Evasion	DisableRegistryTools	Prevented Windows registry tools from starting. MITRE: Defense Evasion
Windows Dynamic	Evasion	DisablePasswordChange	Prevented the operating system from changing account password automatically. MITRE: Defense Evasion {T1089}
Windows Dynamic	Evasion	DisableFirewallStatusView	Process disabled the firewall status in the registry. MITRE: Defense Evasion {T1089}
Windows Dynamic	Evasion	WriteToADS	Process wrote to hidden file section. MITRE: Defense Evasion {T1096}

Windows Dynamic	Evasion	ASRViolation	Suspicious library was loaded into process memory. MITRE: Defense Evasion {T1038}, Privilege Escalation {T1038}
Windows Dynamic	Evasion	SuspiciousRegistryValue	Suspicious registry key was created. MITRE: Defense Evasion {T1112}
Windows Dynamic	Reconnaissance	SuspiciousWMIQuery	Suspicious WMI query was identified. MITRE: Execution {T1047}
Windows Dynamic	Evasion	AntiVirusOverride	Anti-Virus monitoring by Windows security center was overridden. MITRE: Defense Evasion {T1089}
Windows Dynamic	Evasion	SuspiciousChildRelation	User process created a process solely used by the system. MITRE: Execution
Windows Dynamic	Evasion	DisableWindowsDefender	Windows Defender was disabled. MITRE: Defense Evasion {T1089}
Windows Dynamic	Injection	LibraryRemoteWrite	Write action to a loaded library space in a remote process. MITRE: Defense Evasion {T1055}, Privilege Escalation {T1055}
macOS Dynamic	General	stackPivot	Stack pivoting exploitation attempt. MITRE: Execution {T1203}
macOS Dynamic	General	hiddenStartup	Process wrote a hidden file to achieve persistency. MITRE: Persistence {T1158}
macOS Dynamic	General	installMaliciousPlist	Process attempted to write a known malicious plist as launchd job. MITRE: Persistence {T1160}
macOS Dynamic	General	modifyBrowser	Process modified browser's executable. MITRE: Defense Evasion {T1036}
macOS Dynamic	General	modifySystem	Process modified a system file. MITRE: Defense Evasion {T1211}

macOS Dynamic	General	persistenceLaunchdJob	Process achieved persistency through launchd job. MITRE: Persistence {T1160}
macOS Dynamic	General	removeXprotect	Process attempted to remove XProtect from the computer. MITRE: Defense Evasion {T1144}
macOS Dynamic	General	deceptionMacho	Process attempted to write suspicious macho. MITRE: Remote File Copy {T1105}
macOS Dynamic	General	deceptionPlist	Process dropped a hidden suspicious plist to achieve persistency. MITRE: Persistence {T1150}
macOS Dynamic	General	knownMaliciousPlist	Process wrote a plist with known malicious name. MITRE: Privilege Escalation {T1150}, Persistence {T1150}, Defense Evasion {T1036}
macOS Dynamic	General	suspiciousPlist	Process wrote a plist with suspicious contents. : MITRE: Persistence {T1150}, Privilege Escalation {T1150}
macOS Dynamic	General	machoWrittenToTmp	Process wrote a MachO to tmp path. MITRE: Remote File Copy {T1105}
macOS Dynamic	General	injection	Process attempted to inject code to other process. MITRE: Privilege Escalation {T1055}
macOS Dynamic	General	launchDeceptionMacho	Process attempted to execute suspicious MachO. MITRE: Execution {T1203}
macOS Dynamic	General	readPersonalBrowserData	Process attempted to read private browsing data. MITRE: Credential Access {T1081}
Windows Dynamic	Persistence	ScheduleTaskRegister	Application has registered itself to become persistent via scheduled task. MITRE: Persistence {T1084}

Windows Dynamic	Persistence	ServiceCreate	Application has registered itself to become persistent via service. MITRE: Persistence {T1084}
Windows Dynamic	Persistence	RegistryAutorun	Application has registered itself to become persistent via an autorun. MITRE: Persistence {T1084}
Windows Dynamic	General		A threat was detected using static analysis
Windows Dynamic	Persistence	RegistryCOMObject	Application has registered itself to become persistent via COM object. MITRE: Persistence {T1084}
Windows Dynamic	General	CryptominerBehavior	In-browser cryptominer was detected
Windows Dynamic	Post Exploitation	HackTool	Penetration framework in use
Windows Dynamic	Exploitation	MaliciousRDPConnection	Malicious RDP connection detected
Windows Dynamic	General	CryptominerBehavior	Cryptominer was detected
Windows Dynamic	General	CryptominerBehavior	Cryptominer was detected
Windows Dynamic	Privilege Escalation	SuspiciousServiceCreation	Suspicious creation of a service
Windows Dynamic	Privilege Escalation	SuspiciousProcessAccess	Privileged process was accessed by a low privileges process.
Windows Dynamic	Privilege Escalation	TokenManipulation	Local privilege escalation using token manipulation MITRE: Privilege Escalation {T1134}
Windows Dynamic	Injection	DllHijack	Application was hijacked with a suspicious DLL. MITRE: Persistence {T1038}, Privilege Escalation {T1038}, Defense Evasion {T1038}
Windows Dynamic	Post Exploitation	SuspiciousDriverLoad	Unverified driver was loaded. MITRE: Persistence {T1215}
Windows Dynamic	Malware	SuspiciousProcessCreation	Abnormal process creation. MITRE: Execution {T1064}

Windows Dynamic	Evasion	SuspiciousRegistryValue	Suspicious registry key was created. MITRE: Defense Evasion {T1112}
Windows Dynamic	Evasion	SuspiciousRegistryValue	Suspicious registry key was created. MITRE: Defense Evasion {T1112}
Windows Dynamic	Exploitation	KernelExploitAttempt	Kernel exploit attempt. MITRE: Defense Evasion {T1112}
Windows Dynamic	Evasion	AntiVirusEvasion	Process tried to bypass the SentinelOne agent. MITRE: Defense Evasion {T1089}
Windows Dynamic	Evasion	AntiVirusEvasion	Process tried to bypass the SentinelOne agent. MITRE: Defense Evasion {T1089}
Windows Dynamic	Post Exploitation	ReverseShell	Reverse shell behavior was identified. MITRE: Execution {T1064}
Windows Dynamic	Privilege Escalation	SuspiciousHardLink	Suspicious hard link was created. MITRE:
Windows Dynamic	Infostealer	SensitiveMemoryAccess	Read sensitive information from LSASS. MITRE: Credential Access {T1003}
Windows Dynamic	Infostealer	ApplicationInfoStealing	FileZilla's sensitive information was accessed. MITRE: Collection {T1213}
Windows Dynamic	Infostealer	ApplicationInfoStealing	Opera's sensitive information was accessed. MITRE: Collection {T1213}
Linux Dynamic	Evasion	HiddenFileExecution	Execution of a hidden file. MITRE: Hidden Files and Directories {T1158}
Linux Dynamic	Evasion	Packer	Obfuscated script execution. MITRE: Scripting {T1064}, Deobfuscate/Decode Files or Information {T1140}
Linux Dynamic	Evasion	ExecutionWithoutPermissions	Using Dynamic Loader to execute a binary
Linux Dynamic	Evasion	EventTampering	Suspicious shell history log modification. MITRE: Bash History {T1139}

Linux Dynamic	Persistence	CronModification	Suspicious Cron modification. MITRE: Local Job Scheduling {T1168}
Linux Dynamic	General	MaliciousDownload	Download of a suspicious content. MITRE: Download New Code at Runtime {T1407}
Linux Dynamic	Infostealer	ReadShadow	Suspicious access to credentials. MITRE: Credential Dumping {T1003}, Credentials in Files {T1081}
Linux Dynamic	Persistence	ModifyShadow	Suspicious user credentials modifications. MITRE: Valid Accounts {T1078}
Linux Dynamic	Exploitation	ApacheSubshell	Apache webshell command execution. MITRE: Web Shell {T1100}, Web Service {T1102}
Linux Dynamic	Evasion	HidingTracks	Hiding tracks of execution. MITRE: File Deletion {T1107}
Linux Dynamic	Evasion	DisablingSecurityTools	Disabling Security Tools {T1089}
Linux Dynamic	Infostealer	ReadSSHKeys	Suspicious access to credentials. MITRE: Credential Dumping {T1003}, Private Keys {T1145}, Credentials in Files {T1081}
Linux Dynamic	Evasion	ModifiedLogonInfo	Suspicious access to logon info. MITRE: Indicator Removal on Host {T1070}
Linux Dynamic	Persistence	BashPersistence	Bash persistence. MITRE: .bash_profile and .bashrc {T1156}
Linux Dynamic	Malware	EvilGnome	Trojan.Linux.EvilGnome.A
Linux Dynamic	Evasion	SuspiciousFileName	Suspicious file name. MITRE: Space after Filename {T1151}
Linux Dynamic	Persistence	SetSUID	Set the setuid or setgid bits on a file. MITRE: Setuid and Setgid {T1166}

Linux Dynamic	Evasion	ModifyTimestamp	File timestamp modification. MITRE: Timestamp {T1099}
Linux Dynamic	Evasion	SuspiciousFileName	Execution of a file with a suspicious file name. MITRE: User Execution {T1204}
Linux Dynamic	Malware	SuspiciousDelete	Destroy data in a suspicious way. MITRE: Data Destruction {T1485}, Disk Content Wipe {T1488}
Linux Dynamic	Evasion	WriteToSuspiciousLocation	Create or write file in a known suspicious location. MITRE: Data Staged {T1074}
Linux Dynamic	Evasion	LogsModification	Modify a sensitive log file. MITRE: Indicator Removal on Host {T1070}
Linux Dynamic	Persistence	AutoStartPersistence	Autostart persistence.
Linux Dynamic	Persistence	RegisterServicePersistence	Create a service as a way to gain persistence. MITRE: Systemd Service {T1501}, Rootkit {T1014}

## 13.6. List of Indicator Names and Categories

Use items from the Indicator Category listed here to perform **IndicatorCategory** queries on the on the Visibility page.

Use items from the Indicator Name listed here to perform **IndicatorName** queries on the Visibility page.

Use items from the Indicator Description listed here to perform **IndicatorDescription** queries on the Visibility page.

**Important:** The Visibility search is case-sensitive.

Engine	Indicator Category	Indicator Name	Indicator Description
Windows Dynamic	Boot Configuration Update	KMCdisabled	Ability to load unverified drivers was enabled. MITRE: Persistence {T1215, T1050}
Windows Dynamic	Exploitation	StackPivot	Altered process code flow to enable running of malicious code (StackPivot behavior). MITRE: Execution {T1203}

Windows Dynamic	Persistence	SuspiciousPersistence	Application has registered itself to become persistent
Windows Dynamic	Persistence	WMI	Application has registered itself to become persistent via WMI. MITRE: Persistence {T1084}
Windows Dynamic	Persistence	SuspiciousPersistence	Application has registered itself to become persistent
Windows Dynamic	Privilege Escalation	UACBypass	Attempt to bypass UAC (User Account Control). MITRE: Privilege Escalation {T1088}, Defense Evasion {T1088}
Windows Dynamic	Privilege Escalation	UACBypass	Attempt to bypass UAC (User Account Control). MITRE: Privilege Escalation {T1088}, Defense Evasion {T1088}
Windows Dynamic	Privilege Escalation	NamedPipeImpersonation	Attempt to escalate System privileges via Meterpreter. MITRE: Privilege Escalation
Windows Dynamic	Privilege Escalation	NamedPipeImpersonation	Attempt to escalate System privileges via Meterpreter. MITRE: Privilege Escalation
Windows Dynamic	Persistence	StickyKeys	Backdoor was created on the machine. MITRE: Persistence {T1015}
Windows Dynamic	Ransomware	RansomwareBehavior	Behaves like ransomware. MITRE: Execution
Windows Dynamic	Ransomware	RansomwareBehavior	Behaves like ransomware. MITRE: Execution
Windows Dynamic	Ransomware	RansomwareBehavior	Behaves like ransomware. MITRE: Execution
Windows Dynamic	Infostealer	Mimikatz	Behaves like Mimikatz. MITRE: Credential Access {T1098, T1145, T1081}
Windows Dynamic	Exploitation	SandboxEscape	Breakout from Internet Explorer sandbox. MITRE: Execution

Windows Dynamic	Exploitation	SuspiciousVBScript	Breakout from Internet Explorer sandbox. MITRE: Execution
Windows Dynamic	Injection	SuspiciousInjection	Code injection to other process memory space via Reflection. MITRE: Defense Evasion {T1055}
Windows Dynamic	Exploitation	SuspiciousDocument	Document behaves abnormally. MITRE: Execution {T1064}
Windows Dynamic	Exploitation	Metasploit	Execution of a metasploit stager. MITRE: Execution {T1064}
Windows Dynamic	Injection	SuspiciousInjection	Code injection to a remote process. MITRE: Defense Evasion {T1055}
Windows Dynamic	Malware	SuspiciousScript	Executed suspicious shell command. MITRE: Execution {T1064}
Windows Dynamic	Malware	SuspiciousJava	Exploit attempt on Java. MITRE: Execution {T1203}
Windows Dynamic	Evasion	RegHiddenValue	Hiding registry key. MITRE: Defense Evasion {T1112}
Windows Dynamic	Evasion	ProcessModification	Internal process resource was manipulated in memory. MITRE: Defense Evasion
Windows Dynamic	Privilege Escalation	ExploitPrivesc	Local privilege escalation exploit. MITRE: Privilege Escalation {T1068}
Windows Dynamic	Injection	SuspiciousInjection	Code injection to a remote process. MITRE: Defense Evasion {T1055}
Windows Dynamic	Infostealer	MITB	Man in the browser attack. MITRE: Collection {T1185}
Windows Dynamic	Infostealer	MITMProxy	Man in the middle attack. MITRE: Credential Access {T1040}
Windows Dynamic	Post Exploitation	Meterpreter	Metasploit's Meterpreter behavior was identified. MITRE: Execution {T1064}

Windows Dynamic	Post Exploitation	Koadic	PowerShell post-exploitation script was executed. MITRE: Execution {T1064, T1086}
Windows Dynamic	Post Exploitation	MaliciousPowershell	PowerShell post-exploitation script was executed. MITRE: Execution {T1064, T1086}
Windows Dynamic	Post Exploitation	MaliciousPowershell	PowerShell post-exploitation script was executed. MITRE: Execution {T1064, T1086}
Windows Dynamic	Post Exploitation	MaliciousPowershell	PowerShell post-exploitation script was executed. MITRE: Execution {T1064, T1086}
Windows Dynamic	Post Exploitation	MaliciousPowershell	PowerShell post-exploitation script was executed. MITRE: Execution {T1064, T1086}
Windows Dynamic	Evasion	AvoidMitagationAttempt	Process characteristics were changed suspiciously. MITRE: Persistence, Defense Evasion
Windows Dynamic	Evasion	AvoidMitagationAttempt	Process characteristics were changed suspiciously. MITRE: Persistence, Defense Evasion
Windows Dynamic	Evasion	AvoidMitagationAttempt	Process tried to bypass Anti-Virus hooks. MITRE: Defense Evasion.
Windows Dynamic	Infostealer	SensitiveMemoryAccess	Read sensitive information from LSASS. MITRE: Credential Access {T1003}
Windows Dynamic	Evasion	HidingTracks	Hiding tracks of execution. MITRE: Defense Evasion {T1158}, Persistence {T1158}

Windows Dynamic	Infostealer	AccessSyskey	Sensitive user information was queried. MITRE: Credential Access {T1003}
Windows Dynamic	Exploitation	SandboxEscape	Shellcode execution was detected. MITRE: Execution
Windows Dynamic	Exploitation	SuspiciousShellcode	Shellcode execution was detected. MITRE: Execution
Windows Dynamic	Evasion	Doppelganger	Attempt to evade monitoring using the "Doppelganger" technique. MITRE: Defense Evasion {T1186}
Windows Dynamic	Evasion	ProcessHollowing	Attempt to evade monitoring using the "Process hollowing" technique. MITRE: Defense Evasion {T1093}
Windows Dynamic	Injection	SuspiciousInjection	Unusual code injection to a remote process. MITRE: Defense Evasion {T1055}, Privilege Escalation {T1055}
Windows Dynamic	Injection	SuspiciousInjection	Unusual code injection to a remote process. MITRE: Defense Evasion {T1055}, Privilege Escalation {T1055}
Windows Dynamic	Post Exploitation	SuspiciousDriverLoad	Unverified driver was loaded. MITRE: Persistence {T1215}
Windows Dynamic	Boot Configuration Update	WriteToMBR	Write action to protected section of the operating system. MITRE: Persistence {T1067}
Windows Dynamic	Exploitation	SensitiveMemoryAccess	Write action to LSASS process. MITRE: Credential Access {T1098}
Windows Dynamic	Evasion	HookRemovalAttempt	A function was unhooked. MITRE: Defense Evasion
Windows Dynamic	Exploitation	NullPageAllocation	Altered process code flow to enable running of malicious code. MITRE: Execution

Windows Dynamic	Exploitation	StackProtectionModification	Altered process code flow to enable running of malicious code. MITRE: Execution
Windows Dynamic	Evasion	AntiDebugging	Anti-debug technique was used. MITRE: Defense Evasion
Windows Dynamic	Evasion	AntiVm	Anti-VM technique was used. MITRE: Defense Evasion
Windows Dynamic	Persistence	WMI	Application has registered itself to become persistent via WMI. MITRE: Persistence {T1084}
Windows Dynamic	Persistence	DllHijack	Application has registered itself to become persistent. MITRE: Persistence
Windows Dynamic	Privilege Escalation	UACBypass	Attempt to bypass UAC (User Account Control). MITRE: Privilege Escalation {T1088}, Defense Evasion {T1088}
Windows Dynamic	Privilege Escalation	UACBypass	Attempt to bypass UAC (User Account Control). MITRE: Privilege Escalation {T1088}, Defense Evasion {T1088}
Windows Dynamic	Privilege Escalation	TokenManipulation	Authentication data manipulation. MITRE: Persistence {T1131}
Windows Dynamic	Infostealer	SuspiciousKeylogging	Behaves like a keylogger. MITRE: Credential Access {T1056}, Collection {T1056}
Windows Dynamic	Infostealer	SuspiciousKeylogging	Behaves like a keylogger. MITRE: Credential Access {T1056}, Collection {T1056}
Windows Dynamic	Infostealer		Behaves like a memory scraper. MITRE: Collection {T1005, T1119}
Windows Dynamic	Ransomware	RansomwareBehavior	Behaves like ransomware because of file operations. MITRE: Execution

Windows Dynamic	Ransomware	RansomwareBehavior	Behaves like ransomware because of file operations. MITRE: Execution
Windows Dynamic	Ransomware	RansomwareBehavior	Behaves like ransomware because of file operations. MITRE: Execution
Windows Dynamic	Ransomware	RansomwareBehavior	Behaves like ransomware. MITRE: Execution
Windows Dynamic	Injection	AtomBombing	Code injection to other process memory space using the "Atom bombing" technique. MITRE: Defense Evasion {T1055}, Privilege Escalation {T1055}
Windows Dynamic	Injection	SuspiciousInjection	Code migration into system process was detected. MITRE: Defense Evasion {T1055}, Privilege Escalation {T1055}
Windows Dynamic	Injection	SuspiciousInjection	Code was executed in a remote process. MITRE: Defense Evasion {T1055}, Privilege Escalation {T1055}
Windows Dynamic	Exploitation	SuspiciousDocument	Document behaves abnormally. MITRE: Execution {T1064}
Windows Dynamic	Injection	SuspiciousInjection	Code injection to a remote process. MITRE: Defense Evasion {T1055}
Windows Dynamic	Reconnaissance	SuspiciousLdapQuery	Domain information was gathered via LDAP query. MITRE: Discovery {T1087, T1069}
Windows Dynamic	Exploitation	KernelExploitAttempt	Information gathered for kernel exploitation. MITRE: Discovery {T1082}
Windows Dynamic	Evasion	HeavensGate	Manipulated code execution flow using the "Heaven's Gate" technique. MITRE: Execution

Windows Dynamic	Exploitation	ReverseShell	Remote shell was opened. MITRE: Command and Control {T1071}
Windows Dynamic	Exploitation	ReverseShell	Remote shell was opened. MITRE: Command and Control {T1071}
Windows Dynamic	Exploitation	SuspiciousShellcode	Shellcode execution was detected. MITRE: Execution {T1106, T1064}
Windows Dynamic	Exploitation	SuspiciousShellcode	Shellcode execution was detected. MITRE: Execution {T1106, T1064}
Windows Dynamic	Exploitation	SuspiciousShellcode	Shellcode execution from powershell was detected. MITRE: Execution {T1086, T1106, T1064}
Windows Dynamic	Exploitation	SandboxEscape	Shellcode execution was detected. MITRE: Execution {T1106, T1064}
Windows Dynamic	Exploitation	SuspiciousShellcode	Shellcode execution was detected. MITRE: Execution {T1106, T1064}
Windows Dynamic	Injection	SuspiciousLibraryLoad	Suspicious library loaded into the process memory
Windows Dynamic	Evasion	SuspiciousSMBTraffic	Suspicious SMB activity was detected. MITRE: Discovery {T1135}, Lateral Movement {T1077}
Windows Dynamic	Evasion	SuspiciousDNSTraffic	Suspicious DNS activity was detected MITRE: Command and Control {T1071}
Windows Dynamic	Evasion	AttemptToUseSyscallDirectly	Attempt to evade monitoring. MITRE: Defense Evasion
Windows Dynamic	Infostealer	BrowserInfoStealing	Chrome's sensitive information was accessed. MITRE: Collection {T1213}
Windows Dynamic	Infostealer	BrowserInfoStealing	Firefox's sensitive information was accessed. MITRE: Collection {T1213}

Windows Dynamic	Infostealer	DumpSAM	SAM database was exported. MITRE: Credential Dumping {T1003}
Windows Dynamic	Evasion	ProcessModification	Manipulated remote process structure. MITRE: Privilege Escalation {T1179}
Windows Dynamic	Evasion	ProcessModification	Manipulated remote process structure. MITRE: Privilege Escalation {T1179}
Windows Dynamic	Boot Configuration Update	IntegrityCheckDisabled	Disable kernel code integrity checks. MITRE: Defense Evasion
Windows Dynamic	Evasion	DeleteWindowsBackupCat	Process tampered the Windows Backup Catalog. MITRE: Defense Evasion
Windows Dynamic	Exploitation	ROP	Altered process code flow to enable running malicious code. MITRE: Execution
Windows Dynamic	Evasion	HideRemoteProcessWindow	Process tampered with Windows user interface
Windows Dynamic	Evasion	EventViewerTampering	Process tampered with the event viewer logs. MITRE: Defense Evasion {T1089}
Windows Dynamic	Evasion	EventViewerTampering	Process deleted the Event Viewer logs. MITRE: Defense Evasion {T1089}
Windows Dynamic	Persistence	Autorun	A file that enables automatic launching from external drive was created. MITRE: Initial Access {T1091}
Windows Dynamic	Evasion	FakeFileName	A file was created with an internal system name. MITRE: Persistence
Windows Dynamic	Evasion	HookRemovalAttempt	A function was unhooked. MITRE: Defense Evasion
Windows Dynamic	Evasion	Packer	A Library was unpacked into its own memory space. MITRE: Defense Evasion

Windows Dynamic	Injection	LoadUnrelatedLibrary	A library owned by one process was loaded to other process. MITRE: Defense Evasion {T1038}, Privilege Escalation {T1038}
Windows Dynamic	Evasion	AddCertificate	A new root certificate was added. MITRE: Defense Evasion {T1130}
Windows Dynamic	Persistence	UserAdd	A new user account was added. MITRE: Persistence {T1136}
Windows Dynamic	Persistence	DebuggerPersistence	Application registered itself to become persistent. MITRE: Persistence
Windows Dynamic	Persistence	SafeModeConfigurationModification	Application registered itself to become persistent in safe mode. MITRE: Persistence
Windows Dynamic	Evasion	SafeModeConfigurationModification	Application manipulated safe mode configuration: MITRE: Persistence
Windows Dynamic	Evasion	AddFirewallException	Application added firewall rule to allow network traffic. MITRE: Exfiltration {T1041}
Windows Dynamic	Injection	SuspiciousProtectionModification	Changed protection type of library in a remote process space. MITRE: Privilege Escalation
Windows Dynamic	Evasion	PreloadInjection	Code injection to other process memory space. MITRE: Defense Evasion {T1038}, Privilege Escalation {T1038}
Windows Dynamic	Injection	RemoteInjection	Code injection to a remote process. MITRE: Defense Evasion {T1055}
Windows Dynamic	Evasion	DisableSecurityCenterEvents	Disabled security center notifications. MITRE: Defense Evasion {T1089}
Windows Dynamic	Evasion	HiddenFilesDisplayModification	Disabled showing hidden files and folders. MITRE: Defense Evasion

Windows Dynamic	Infostealer	EnableMemoryPlaintextPasswords	The store of plaintext passwords in memory was disabled/enabled. MITRE: Credential Access
Windows Dynamic	Injection	RemoteInjection	Code injection to a remote process. MITRE: Defense Evasion {T1055}
Windows Dynamic	Privilege Escalation	PrivilegedInstruction	Execution of privileged instruction was identified. MITRE: Privilege Escalation
Windows Dynamic	Evasion	ModifyHostsFile	Host file was modified. MITRE: Defense Evasion
Windows Dynamic	Evasion	InternetExplorerConfigurationModification	Internet Explorer offline mode was disabled. MITRE: Defense Evasion {T1089}
Windows Dynamic	Evasion	InternetExplorerConfigurationModification	Internet zone checks were disabled. MITRE: Defense Evasion {T1089}
Windows Dynamic	Injection	RemoteLibraryInjection	Library was injected to a remote process. MITRE: Defense Evasion {T1055}, Privilege Escalation {T1055}
Windows Dynamic	Evasion	PreventProcessExecution	Prevented execution of a process. MITRE: Defense Evasion
Windows Dynamic	Evasion	DisableTaskManager	Prevented the Task Manager from starting. MITRE: Defense Evasion
Windows Dynamic	Evasion	DisableRegistryTools	Prevented Windows registry tools from starting. MITRE: Defense Evasion
Windows Dynamic	Evasion	DisablePasswordChange	Prevented the operating system from changing account password automatically. MITRE: Defense Evasion {T1089}
Windows Dynamic	Evasion	DisableFirewallStatusView	Process disabled the firewall status in the registry. MITRE: Defense Evasion {T1089}
Windows Dynamic	Evasion	WriteToADS	Process wrote to hidden file section. MITRE: Defense Evasion {T1096}

Windows Dynamic	Evasion	ASRViolation	Suspicious library was loaded into process memory. MITRE: Defense Evasion {T1038}, Privilege Escalation {T1038}
Windows Dynamic	Evasion	SuspiciousRegistryValue	Suspicious registry key was created. MITRE: Defense Evasion {T1112}
Windows Dynamic	Reconnaissance	SuspiciousWMIQuery	Suspicious WMI query was identified. MITRE: Execution {T1047}
Windows Dynamic	Evasion	AntiVirusOverride	Anti-Virus monitoring by Windows security center was overridden. MITRE: Defense Evasion {T1089}
Windows Dynamic	Evasion	SuspiciousChildRelation	User process created a process solely used by the system. MITRE: Execution
Windows Dynamic	Evasion	DisableWindowsDefender	Windows Defender was disabled. MITRE: Defense Evasion {T1089}
Windows Dynamic	Injection	LibraryRemoteWrite	Write action to a loaded library space in a remote process. MITRE: Defense Evasion {T1055}, Privilege Escalation {T1055}
macOS Dynamic	General	stackPivot	Stack pivoting exploitation attempt. MITRE: Execution {T1203}
macOS Dynamic	General	hiddenStartup	Process wrote a hidden file to achieve persistency. MITRE: Persistence {T1158}
macOS Dynamic	General	installMaliciousPlist	Process attempted to write a known malicious plist as launchd job. MITRE: Persistence {T1160}
macOS Dynamic	General	modifyBrowser	Process modified browser's executable. MITRE: Defense Evasion {T1036}
macOS Dynamic	General	modifySystem	Process modified a system file. MITRE: Defense Evasion {T1211}

macOS Dynamic	General	persistenceLaunchdJob	Process achieved persistency through launchd job. MITRE: Persistence {T1160}
macOS Dynamic	General	removeXprotect	Process attempted to remove XProtect from the computer. MITRE: Defense Evasion {T1144}
macOS Dynamic	General	deceptionMacho	Process attempted to write suspicious macho. MITRE: Remote File Copy {T1105}
macOS Dynamic	General	deceptionPlist	Process dropped a hidden suspicious plist to achieve persistency. MITRE: Persistence {T1150}
macOS Dynamic	General	knownMaliciousPlist	Process wrote a plist with known malicious name. MITRE: Privilege Escalation {T1150}, Persistence {T1150}, Defense Evasion {T1036}
macOS Dynamic	General	suspiciousPlist	Process wrote a plist with suspicious contents. : MITRE: Persistence {T1150}, Privilege Escalation {T1150}
macOS Dynamic	General	machoWrittenToTmp	Process wrote a MachO to tmp path. MITRE: Remote File Copy {T1105}
macOS Dynamic	General	injection	Process attempted to inject code to other process. MITRE: Privilege Escalation {T1055}
macOS Dynamic	General	launchDeceptionMacho	Process attempted to execute suspicious MachO. MITRE: Execution {T1203}
macOS Dynamic	General	readPersonalBrowserData	Process attempted to read private browsing data. MITRE: Credential Access {T1081}
Windows Dynamic	Persistence	ScheduleTaskRegister	Application has registered itself to become persistent via scheduled task. MITRE: Persistence {T1084}

Windows Dynamic	Persistence	ServiceCreate	Application has registered itself to become persistent via service. MITRE: Persistence {T1084}
Windows Dynamic	Persistence	RegistryAutorun	Application has registered itself to become persistent via an autorun. MITRE: Persistence {T1084}
Windows Dynamic	General		A threat was detected using static analysis
Windows Dynamic	Persistence	RegistryCOMObject	Application has registered itself to become persistent via COM object. MITRE: Persistence {T1084}
Windows Dynamic	General	CryptominerBehavior	In-browser cryptominer was detected
Windows Dynamic	Post Exploitation	HackTool	Penetration framework in use
Windows Dynamic	Exploitation	MaliciousRDPConnection	Malicious RDP connection detected
Windows Dynamic	General	CryptominerBehavior	Cryptominer was detected
Windows Dynamic	General	CryptominerBehavior	Cryptominer was detected
Windows Dynamic	Privilege Escalation	SuspiciousServiceCreation	Suspicious creation of a service
Windows Dynamic	Privilege Escalation	SuspiciousProcessAccess	Privileged process was accessed by a low privileges process.
Windows Dynamic	Privilege Escalation	TokenManipulation	Local privilege escalation using token manipulation MITRE: Privilege Escalation {T1134}
Windows Dynamic	Injection	DllHijack	Application was hijacked with a suspicious DLL. MITRE: Persistence {T1038}, Privilege Escalation {T1038}, Defense Evasion {T1038}
Windows Dynamic	Post Exploitation	SuspiciousDriverLoad	Unverified driver was loaded. MITRE: Persistence {T1215}
Windows Dynamic	Malware	SuspiciousProcessCreation	Abnormal process creation. MITRE: Execution {T1064}

Windows Dynamic	Evasion	SuspiciousRegistryValue	Suspicious registry key was created. MITRE: Defense Evasion {T1112}
Windows Dynamic	Evasion	SuspiciousRegistryValue	Suspicious registry key was created. MITRE: Defense Evasion {T1112}
Windows Dynamic	Exploitation	KernelExploitAttempt	Kernel exploit attempt. MITRE: Defense Evasion {T1112}
Windows Dynamic	Evasion	AntiVirusEvasion	Process tried to bypass the SentinelOne agent. MITRE: Defense Evasion {T1089}
Windows Dynamic	Evasion	AntiVirusEvasion	Process tried to bypass the SentinelOne agent. MITRE: Defense Evasion {T1089}
Windows Dynamic	Post Exploitation	ReverseShell	Reverse shell behavior was identified. MITRE: Execution {T1064}
Windows Dynamic	Privilege Escalation	SuspiciousHardLink	Suspicious hard link was created. MITRE:
Windows Dynamic	Infostealer	SensitiveMemoryAccess	Read sensitive information from LSASS. MITRE: Credential Access {T1003}
Windows Dynamic	Infostealer	ApplicationInfoStealing	FileZilla's sensitive information was accessed. MITRE: Collection {T1213}
Windows Dynamic	Infostealer	ApplicationInfoStealing	Opera's sensitive information was accessed. MITRE: Collection {T1213}
Linux Dynamic	Evasion	HiddenFileExecution	Execution of a hidden file. MITRE: Hidden Files and Directories {T1158}
Linux Dynamic	Evasion	Packer	Obfuscated script execution. MITRE: Scripting {T1064}, Deobfuscate/Decode Files or Information {T1140}
Linux Dynamic	Evasion	ExecutionWithoutPermissions	Using Dynamic Loader to execute a binary
Linux Dynamic	Evasion	EventTampering	Suspicious shell history log modification. MITRE: Bash History {T1139}

Linux Dynamic	Persistence	CronModification	Suspicious Cron modification. MITRE: Local Job Scheduling {T1168}
Linux Dynamic	General	MaliciousDownload	Download of a suspicious content. MITRE: Download New Code at Runtime {T1407}
Linux Dynamic	Infostealer	ReadShadow	Suspicious access to credentials. MITRE: Credential Dumping {T1003}, Credentials in Files {T1081}
Linux Dynamic	Persistence	ModifyShadow	Suspicious user credentials modifications. MITRE: Valid Accounts {T1078}
Linux Dynamic	Exploitation	ApacheSubshell	Apache webshell command execution. MITRE: Web Shell {T1100}, Web Service {T1102}
Linux Dynamic	Evasion	HidingTracks	Hiding tracks of execution. MITRE: File Deletion {T1107}
Linux Dynamic	Evasion	DisablingSecurityTools	Disabling Security Tools {T1089}
Linux Dynamic	Infostealer	ReadSSHKeys	Suspicious access to credentials. MITRE: Credential Dumping {T1003}, Private Keys {T1145}, Credentials in Files {T1081}
Linux Dynamic	Evasion	ModifiedLogonInfo	Suspicious access to logon info. MITRE: Indicator Removal on Host {T1070}
Linux Dynamic	Persistence	BashPersistence	Bash persistence. MITRE: .bash_profile and .bashrc {T1156}
Linux Dynamic	Malware	EvilGnome	Trojan.Linux.EvilGnome.A
Linux Dynamic	Evasion	SuspiciousFileName	Suspicious file name. MITRE: Space after Filename {T1151}
Linux Dynamic	Persistence	SetSUID	Set the setuid or setgid bits on a file. MITRE: Setuid and Setgid {T1166}

Linux Dynamic	Evasion	ModifyTimestamp	File timestamp modification. MITRE: Timestamp {T1099}
Linux Dynamic	Evasion	SuspiciousFileName	Execution of a file with a suspicious file name. MITRE: User Execution {T1204}
Linux Dynamic	Malware	SuspiciousDelete	Destroy data in a suspicious way. MITRE: Data Destruction {T1485}, Disk Content Wipe {T1488}
Linux Dynamic	Evasion	WriteToSuspiciousLocation	Create or write file in a known suspicious location. MITRE: Data Staged {T1074}
Linux Dynamic	Evasion	LogsModification	Modify a sensitive log file. MITRE: Indicator Removal on Host {T1070}
Linux Dynamic	Persistence	AutoStartPersistence	Autostart persistence.
Linux Dynamic	Persistence	RegisterServicePersistence	Create a service as a way to gain persistence. MITRE: Systemd Service {T1501}, Rootkit {T1014}

## 13.7. Saving Threat Hunting Queries and Watchlists [Multi-Site]

**Management:** Denali, Eiffel, Fuji, Grand Canyon, Houston

**Agents:** Windows 2.6+ | macOS 2.6+ | Linux 2.6+

**SKU:** Complete (not available with Core)

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

After you create Threat Hunting queries, you can save the queries to use again. You can run saved queries manually or set queries to run on a scheduled basis and send notifications to an Admin.

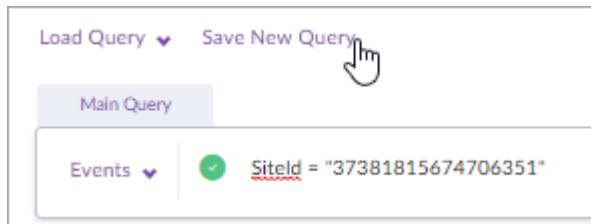
To create Threat Hunting watchlists, create queries that run periodically and send notifications when they find results that match. The admin that receives the notifications must have permissions (admin scope) to see the search in the Management Console.

Watch: [Creating Watchlists](#)

### To save a query:

1. In the sidebar, click **Visibility** .
2. Run a query.

3. Click **Save New Query**.



4. In the window that opens, in **Set name**, enter a name for the query.
5. Click **Save**.

### To configure a query to run periodically and send notifications:

1. In the sidebar, click **Visibility** .
2. Run a query.
3. Click **Save New Query**.
4. In the window that opens, in **Set name**, enter a name for the query.
5. Enable **Notifications**.

The screenshot shows a modal dialog box titled 'New Watch list'. It has a 'Set name' field containing 'Process def'. Below it is a note 'Filter time frame: Last 48 Hours'. Under the heading 'Notifications', there is a toggle switch labeled 'Notifications' with a description: 'Turn on mail notifications and get notified for every event that matches this query'. A 'Timing rate' section includes a 'Select time rate' dropdown. At the bottom, there is a 'Save' button and a 'Cancel' button.

6. In **Timing rate**, select the frequency at which the query will run.

7. In **Notification recipients**, enter the email addresses of admins to get notifications. Notifications are only sent if there are results that match the query. Admins must have Management Console permissions to see the results.
8. Click **Save**.

## 13.8. Working with Saved Deep Visibility Queries [Multi-Site]

**Management:** Denali, Eiffel, Fuji, Grand Canyon, Houston

**Agents:** Windows 2.6+ | macOS 2.6+ | Linux 2.6+

**SKU:** Complete (not available with Core)

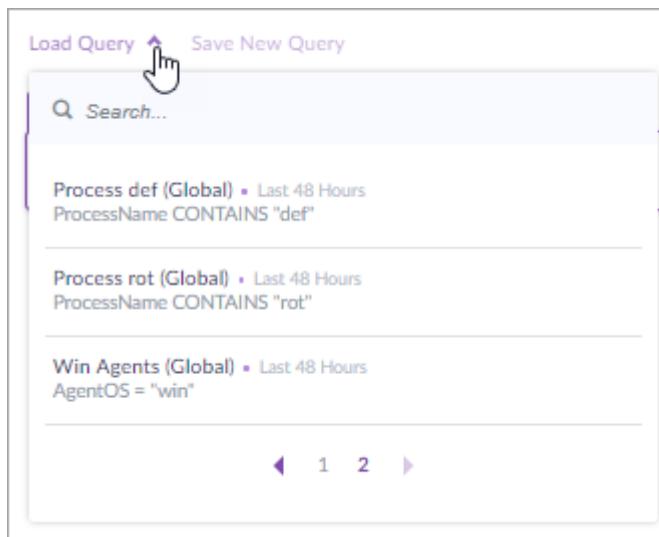
**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

After a Deep Visibility query is saved, you can run it, change its name and notification settings, and delete it.

### To run a saved query manually:

1. In the sidebar, click **Visibility** .
2. Click **Load Query**.



3. Optional: Use the **Search** field to search by the name of the saved query.
4. Select a query.

It runs and the results open in the **Visibility** view.

### To change or delete a saved query:

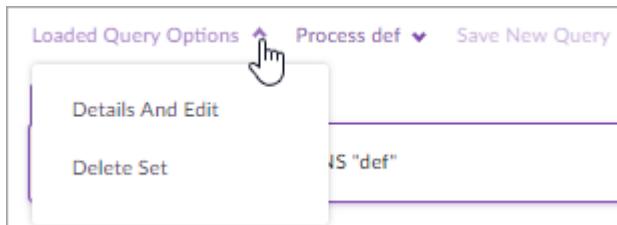
1. In the sidebar, click **Visibility** .

2. Click **Load Query**.

3. Select a query.

It runs and the results open in the **Visibility** view.

4. Click **Loaded Query Options**.



- To edit the query: Select **Details and Edit**.
- To Delete the query from the saved list: Select **Delete Query**.

### 13.9. Query with Custom Time Range [Multi-Site]

**Management:** Denali, Eiffel, Fuji, Grand Canyon, Houston

**Agents:** Windows 2.6+ | macOS 2.6+| Linux 2.6+

**SKU:** Complete (not available with Core)

**Minimum Admin Scope:** Site Admin

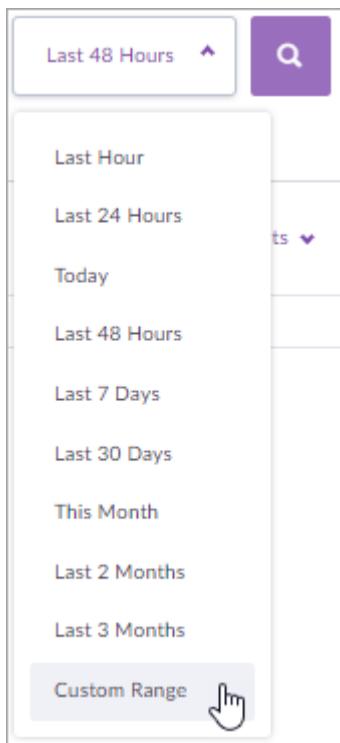
**Scope:** Selected Site, Account, or Global

Use a **Custom Range** to search for results in a specific window of time.

From Fuji management version, the time range can be as small as one minute.

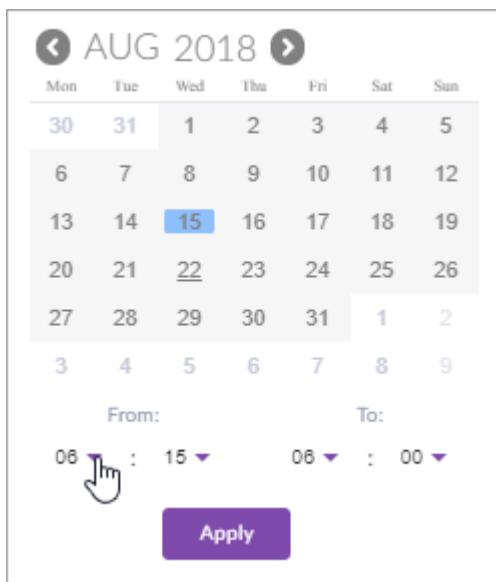
**To select a custom time frame:**

1. In the sidebar, click **Visibility** .
2. Enter a query.
3. For the time frame, select **Custom Range**.



4. Select the start date from the calendar.

Optional: Select the start hour - **From**.



5. Select the end date from the calendar.

Optional: Select the end hour - **To**.

**Note:** If the search is on the same day, click the date again as the end date.

6. Click **Apply**.

## 13.10. Managing the Browser Extension

**Management:** Banff, Central Park, Denali, Eiffel, Fuji, Grand Canyon, Houston

**Agents:** Windows 2.5+ | macOS 2.5.3+

**SKU:** Complete (not available with Core)

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

Deep Visibility collects URL data from an extension that is installed on Safari and Chrome, and from Internet Explorer and Edge without an extension.

The way to install and uninstall the browser extension depends on the endpoint OS and Agent version.

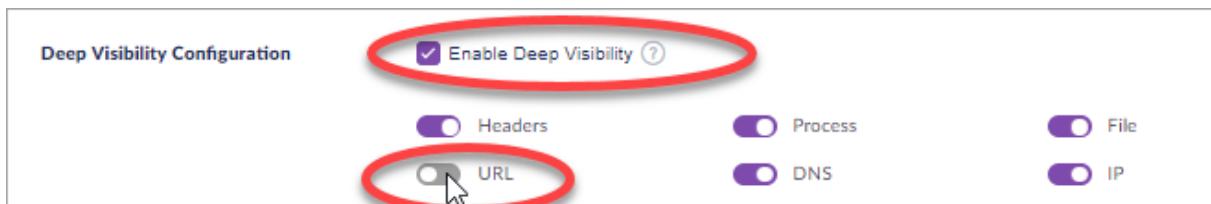
### In MacOS Agents version 2.5.3 and higher and 2.6 and higher:

The Deep Visibility browser extensions for Safari and Chrome are controlled by the policy of the Agents.

The behavior is slightly different in Safari and in Chrome.

- The Safari extension is *enabled* or *disabled* on endpoints.
- The Chrome extension is *installed* or *uninstalled* on endpoints.

The Agent enables or installs the extension if the policy is changed to enable **Deep Visibility > URL**. The Agent disables or uninstalls the extension if the **URL** option is disabled.



### In Windows Agents version 2.7 and higher:

The Chrome browser extension is installed or uninstalled on Agents based on the policy of the Agents.

- The Agent installs the extension if the policy is changed to enable **Deep Visibility > URL**. The Agent uninstalls the extension if the **URL** option is disabled.
- Internet Explorer and Edge do not have a browser extension, but they also work with Deep Visibility based on the settings configured in the policy.

### In Windows 2.5 - 2.6.X:

The browser extension is part of the Agent installation.

- To use Deep Visibility, you must [enable Chrome extensions in the GPO](#) before you install or upgrade to Agent version 2.5 or higher.

- Advanced: If you will not use Deep Visibility, use the [CLI Installer switch](#) to not install the Chrome extension.

## 13.11. Supported File Types for Deep Visibility

**Windows Supported File Types:**

Executables	Scripts	Microsoft Word	Microsoft Excel	Microsoft PowerPoint	Adobe
EXE	PS1,	DOC	XLS	PPT	
SCR	PY,	DOT	XLM	POT	
DLL	BAT	DOCX	XLSX	PPS	
SYS	VBS,	DOCM	XLSM	PPTX	
COM	WS,	DOTX	XLTX	PPTM	
MSI	AU3	DOTM	XLTM	POTX	
MSP	CMD	DOCB	XLSB	POTM	
JAR	INX		XLA	PPAM	
	ISU		XLAM	PPSX	
	RGS		XLL	PPSM	
	SCT		XLW	SLDX	
	PHP			SLDM	

**macOS Supported File Type:** Mach-O

**Linux Supported File Type:** ELF

## 13.12. Hunter Chrome Extension for Deep Visibility

**Management:** Fuji, Grand Canyon, Houston

**Agents:** Windows 2.6+ | macOS 2.6+ | Linux 2.6+

**SKU:** Complete (not available with Core)

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

SentinelOne Hunter Chrome Extension (Alpha release) works with SentinelOne Deep Visibility to hunt for indicators of interest, captured from your browser.

Hunter opens a query in your SentinelOne Deep Visibility Console page to search for the selected data across your organization.

Hunter captures these indicators from information open in your current browser tab: IP addresses, DNS requests, and hashes (MD5, SHA-1, and SHA-256).

To use Hunter, you must be an Admin user in an active SentinelOne Management Console with Deep Visibility.

### How to start using Hunter:

- Get the Hunter Chrome extension from  
<https://chrome.google.com/webstore/detail/sentinelone-hunter/bbnmecacdlabkdobimdklpgmllebgip>

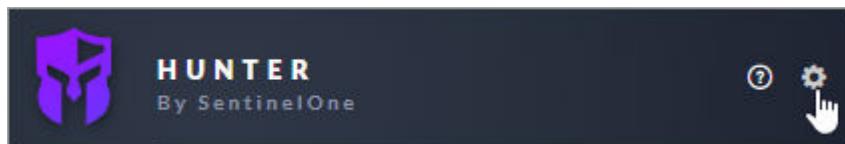
The SentinelOne Hunter icon shows in your browser extensions.



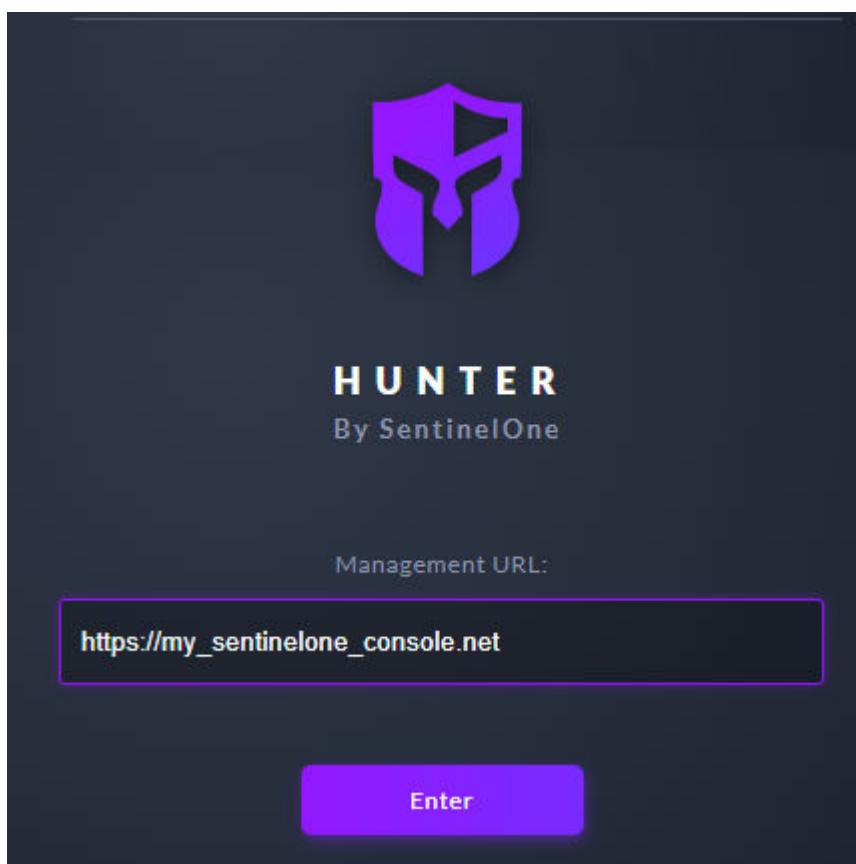
2. Click the extension to open it.

When you open it for the first time, it will likely show, **No results found**. To get results, enter a Management Console URL and open Hunter in a browser tab that contains indicators of interest.

3. Click the settings icon to set Hunter to work with your Deep Visibility environment.



4. In **Management URL**, enter the URL of an active SentinelOne Management Console with Deep Visibility and click **Enter**.



5. Browse to a URL that shows indicators that you want to investigate.
6. Click the Hunter icon to open it.

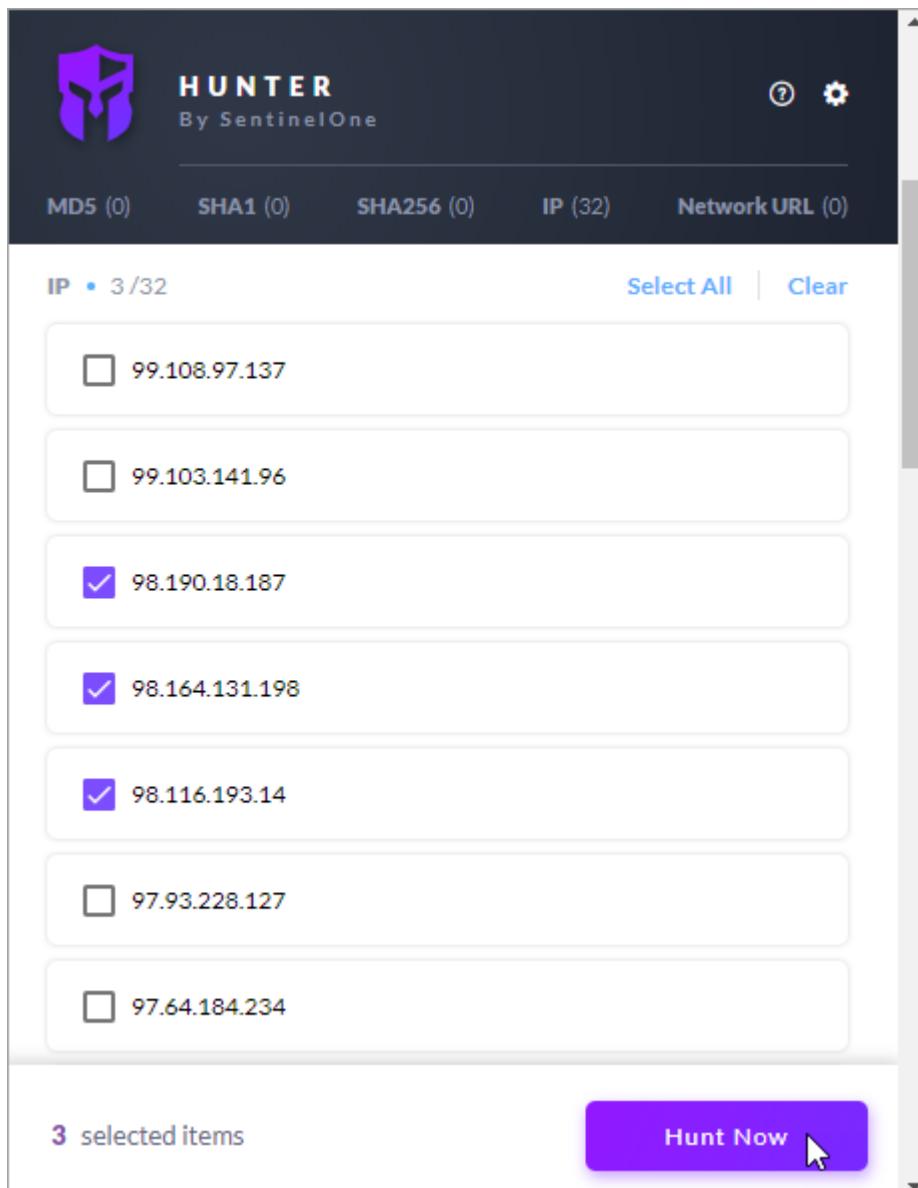
It opens with a list of the indicators that show in your current browser tab.

The screenshot shows the HUNTER tool interface by SentinelOne. At the top, there is a logo and the text "HUNTER By SentinelOne". Below the header, there are tabs for MD5 (0), SHA1 (0), SHA256 (0), IP (32), and Network URL (0). The IP tab is selected, showing "IP • 0 / 32". Below this, there is a "Select All" and "Clear" button. A list of IP addresses is displayed in a scrollable area, each with a checkbox next to it. The IP addresses listed are: 99.108.97.137, 99.103.141.96, 98.190.18.187, 98.164.131.198, 98.116.193.14, 97.93.228.127, 97.64.184.234, and 96.85.35.233.

7. Select one item and click **Hunt**.



Or Select multiple items and click **Hunt Now**.



8. A new query opens in Deep Visibility in your SentinelOne Management Console.

You can edit the query or run it as is to search for the indicators in your environment.

The screenshot shows the Deep Visibility query interface. At the top, there are search filters: "AgentName CONTAINS \"go\"", "processGroupId = \"8C4D8D76-6...\"", and "DstIP in \"98.190.18.187\", \"98.16...\"". Below the filters are buttons for "Load Query" and "Save New Query". The main query area has a title "Main Query" and a search bar with the condition "Events DstIP in \"98.190.18.187\", \"98.164.131.198\", \"98.116.193.14\"". There are also filters for "Last 48 Hours" and a search icon.

You can continue to make selections in Hunter to open new Deep Visibility queries.

**Known Limitation:** In the current release, queries for DNS requests might not find all matching information in Deep Visibility. This is because Deep Visibility searches for the exact URL and not entries that contain the URL. DNS requests show under **Network URL** in Hunter.

## 14. Creating Insight Reports [Multi-Site]

**Management:** Central Park, Denali, Eiffel, Fuji, Grand Canyon, Houston

**Agents:** All

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

Create one-time or scheduled Insight reports to see high-level and detailed information on the state of your endpoint security. Reports include statistics, trends, and summaries with easy to read and actionable information about your network.

You can see reports in the Management Console and automatically send them by email to the addresses that you enter.

### Examples of available Insight reports:

- Executive Insights
- Executive Insights by Group
- Threat Insights
- Mitigation and Response Insights
- Application Insights

### Scope of reports:

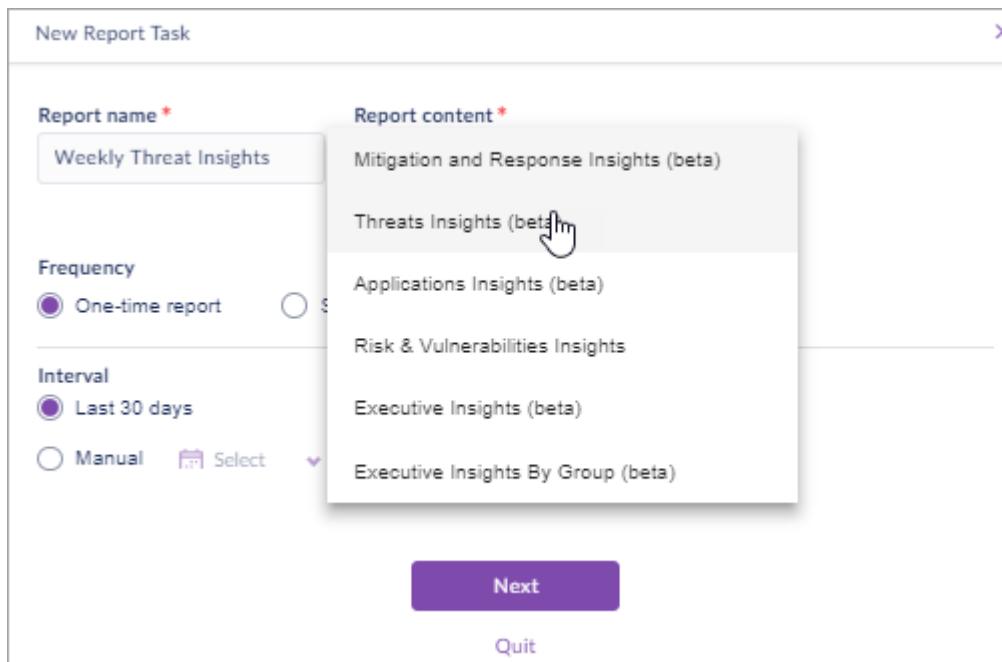
The scope of the report is based on the Management Console view you are in when you create the report.

- If you are in one Site, the scope of the report is that Site.
- If you are a Global Admin or an Admin of multiple Sites in the **Global** view, reports that you create include information combined for all Sites in your scope.
- If you select a report for a specific group, for example, **Executive Insights by Group**, a field shows to enter the **Group Name**.

### To create an Insight report:

1. In the sidebar, click **Scope**  and select a scope.
2. In the sidebar, click **Reports** .
3. In Reports, click **New Report Task**.

The **New Report Task** window opens.



4. In **Report name**, enter a name for the report.
5. In **Report content**, select the report type.
6. If the report is for a specific entity in the Management Console, you are prompted to enter the required information. For example, if you select **Executive Insights by Group**, you must enter the **Group Name**, as shown in the Management Console.
7. In **Frequency**, select if the report is generated **One time** or on a **Scheduled** basis.
8. In **Interval**, select the time period that the report includes.
  - **For a One-time report:**
    - Select **Last 30 Days** - the report will include information for the preceding 30 days.
    - Or
    - Select **Manual** and then select a time period on the calendar.

You cannot select dates in the future.
  - **For a Scheduled report:**
    - Select **Weekly** and choose a day of the week.

For example, if you select a **Weekly** report to generate on **Tuesday**, a report will be created on the next Tuesday, and then every Tuesday afterward.

Or

    - Select **First of every month**. The report will be generated on the first day of the next month and each month afterward.
9. Click **Next**.

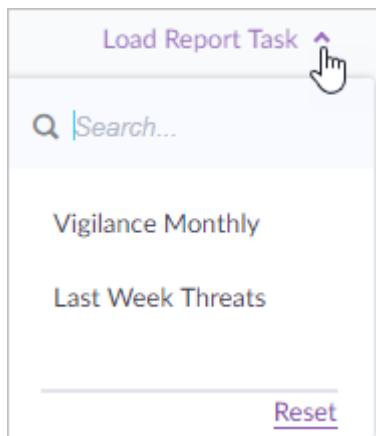
10. Optional: In **Recipients**, enter one or more email addresses to get the report. Separate addresses with a comma.

Note: To configure email recipients, set up SMTP in **Settings > Integrations**.

Recipients do not require Management Console privileges.

11. Click **Create**.

Only reports that ran show in the table. You can see the list of future reports in **Load Report Task**.



- [Integrating Your SMTP Server](#)
- [Downloading a Report \[Multi-Site\] \[239\]](#)
- [Editing and Deleting Reports \[Multi-Site\] \[237\]](#)

## 14.1. Editing and Deleting Reports [Multi-Site]

**Management:** Central Park, Denali, Eiffel, Fuji, Grand Canyon, Houston

**Agents:** All

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

You can delete a scheduled report so that it does not create more reports, or change its details. You can change a report's Name or Recipients. To change the type of report, frequency, or scope, create a new Report Task and delete the old one.

You can delete created reports from the Management Console when you do not need them, or save them in a different location.

### To edit or delete a scheduled report:

1. In the sidebar, click **Reports**
2. In **Reports**, click **Load Report Task**.

REPORTS

New Report Task Delete Selection No Items Selected

Load Report Task

14 Reports on the list 10 Results

- Select a report task from the list. Search for part of the task name, if necessary.

The task shows in the **Reports** view and **Actions** for the task are available.

- Click **Actions** and select **Edit** or **Delete**.

REPORTS

New Report Task Delete Selection No Items Selected

Date	Name	Scope	Site Name	Frequency	Int	Results
01/05/2018	Weekly test	Global	N/A	Weekly	Every Tuesday	Ready to download

Actions

Edit

Delete

weekly test

Results

- To delete the report task:

- Click **Delete**.

A confirmation window opens.

- Click **Confirm**.

- To change the name or recipients of the report:

- Click **Edit**.

The Edit Report Task window opens

- Change the details.

- Click **Next**.

- Click **Update**.

### To delete a created report:

- In the sidebar, click **Reports**.
  - Select the checkbox for the report you want to delete.
- You can select multiple reports to delete at the same time.
- Click **DELETE**.

New Report Task Delete Selection 1 report selected

Date Name Scope

01/05/2018 Global report Global

- In the confirmation window that opens, click **Confirm**.

## 14.2. Downloading a Report [Multi-Site]

**Management:** Central Park, Denali, Eiffel, Fuji, Grand Canyon, Houston

**Agents:** All

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

From the Reports view, Admin and Viewer users can download all created reports for Sites in their scope.

### To get a report:

- In the sidebar, click **Reports** .
- In Reports, select the report that you want to see.



Reports							13 Reports on the list
Date	Name	Scope	Site Name	Frequency	Interval	Status	
01/05/2018	Global report	Global	N/A	Manually	Last 30 days	Ready to download	<a href="#">Download PDF</a> <a href="#">Download HTML</a>

- Click **Download PDF** or **Download HTML**.

The report is downloaded to the default Downloads folder.

## 14.3. Raw Data Report

**Management:** Alhambra, Bahamas, Banff, Central Park, Denali, Eiffel, Fuji, Grand Canyon, Houston

**Agents:** All

To save Forensic data offline, open **RAW DATA REPORT** for a threat and download the report as a CSV or JSON file.

### To get a Raw Data Report:

- In the sidebar, click **Analyze** .
- In the **Forensics details**, scroll to the end.
- To see the data, expand **Raw Data Report**.

To get the report offline, click **Download** and select **JSON** or **CSV**.

The screenshot shows the 'ATTACK OVERVIEW' section of the SentinelOne interface. On the left, there's a sidebar with icons for various threat types. Below the sidebar, a tree view shows categories like 'ATTACK STORY LINE', 'RAW DATA REPORT' (which is expanded), 'FILE (280)', 'REGISTRY (1)', 'PROCESS (11)', 'NETWORK (1)', and 'OTHER (7)'. A purple oval highlights the 'RAW DATA REPORT' node. To the right of the tree is a table titled 'TIME' with four rows of data. The table has columns for 'TIME', 'PROCESS (PID)', and 'ACTION'. The first row shows a timestamp of 07/03/2018 18:27:39, a process of WINWORD.EXE (egyptairplus.doc) (6012), and an action of 'N/A'. The second row shows a timestamp of 07/03/2018 18:27:40, a process of WINWORD.EXE (egyptairplus.doc) (6012), and an action of 'modified a file'. The third row shows a timestamp of 07/03/2018 18:27:53, a process of powershell.exe (CLI interpreter) (3624), and an action of 'modified a file'. The fourth row shows a timestamp of 07/03/2018 18:27:53, a process of powershell.exe (CLI interpreter) (3624), and an action of 'modified a file'. A purple oval highlights the 'Download' button at the top right of the table area.

TIME	PROCESS (PID)	ACTION
07/03/2018 18:27:39	WINWORD.EXE (egyptairplus.doc) (6012)	N/A
07/03/2018 18:27:40	WINWORD.EXE (egyptairplus.doc) (6012)	modified a file
07/03/2018 18:27:53	powershell.exe (CLI interpreter) (3624)	modified a file
07/03/2018 18:27:53	powershell.exe (CLI interpreter) (3624)	modified a file

## Categories of Data

- Threat details
- Agent and endpoint details
- File of the threat: Creation timestamp, ID, display name, hash, permissions, size
- For each file that the threat used or created: Creation timestamp, source executable, action ("created file", "wrote to file", and so on), target (for example, if the action was "created file", the target is the pathname of the file that was created)
- For each network connection that the threat created or changed: Timestamp, source, action, target
- For each process that the threat started or changed: Timestamp, source with ID, action, target, CLI arguments
- For each registry and tag change: Timestamp, source (such as CLI interpreter), action, target

# 15. Management Console Integrations [Multi-Site]

**Management:** Central Park, Denali, Eiffel, Fuji, Grand Canyon, Houston

**Agents:** Windows 2.6+ | macOS 2.6+ | Linux 2.6+

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

Configure integration settings for SSO, SMTP, Syslog, and more in the Management Console in **Settings > Integrations**.

You can configure these settings for Global (applies to all Sites), for a selected Account (applies to its Sites), or for a selected Site.

## 15.1. Configuring Okta SSO [Multi-Site]

**Management:** Central Park, Denali, Eiffel, Fuji, Grand Canyon, Houston

**Agents:** All

**Minimum Admin Scope:** Account Admin

**Scope:** Selected Account or Global

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's documentation and support.

**Note:** There are many more options in 3rd Party SSO products than we explain here. If you are unfamiliar with the provider, we recommend that you leave the default values for settings that are not mentioned here.

### Requirements:

- An Okta user for each admin that will log in to the SentinelOne Management Console.

If you select **Auto-Provision** in the SentinelOne SSO configuration, the SentinelOne users will be created automatically from the Okta users on the first SSO login. If you already have the users configured in the SentinelOne Management Console, make sure that the emails match the emails in Okta.

- One Okta application for each Account. For each Okta application, assign the Management Console users that have permissions for that Account. **Important:** If **Auto-Provision** is enabled, all user created automatically will be Account admins. You can then demote them to be Site admins, where relevant

If you have a Okta application for Global SSO, you do not need for Account.

- If you have Global permissions and want everyone to be logged in with SSO, you can set one Okta application for Global, that uses the Global settings and contains Global admins. **Important:** If **Auto-Provision** is enabled, all users created automatically will be Global admins.

**Best Practices:** Use different browsers to configure Okta and SentinelOne, or do all Okta configurations and then log out of Okta. If you are logged in to Okta when you configure the Management Console, there will be errors.

### 15.1.1. Using SSO Login Exclusively

You can require users to log in to the Management Console with SSO only. This setting is Global and applies to all Sites.

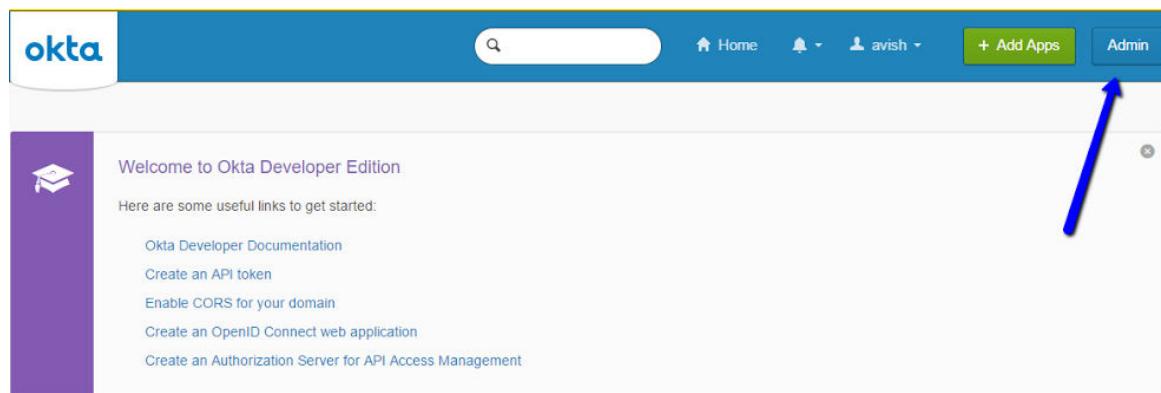
To use this feature, request it from SentinelOne Support.

When enabled:

- Regular login is disabled. Users must log in with SSO, with the regular [SSO login](#) workflow.
- Users cannot create New Users from the Management Console.
- Two-Factor Authentication and MFA are not enforced.

#### To set up Okta:

1. In your Okta dashboard, click **Admin**.



2. Click **Add Applications**.

The screenshot shows the Okta dashboard with a blue arrow pointing to the 'Add Applications' option in the 'Shortcuts' sidebar.

**Okta Dashboard**

**Status**

- No notifications to view!

**People** 1

Search people...

**Applications** 0

Search applications...

**Usage · Last 30 Days**

**Shortcuts**

- Add Applications (highlighted with a blue arrow)
- Assign Applications
- Add People
- Activate People
- Deactivate People
- Reset Passwords
- Unlock People

**Reports**

- Okta Usage
- Application Usage
- Suspicious Activity
- Current Assignments
- App Password Health
- Deprovisioning Details
- SMS Usage
- MFA Usage
- System Log
- SAML Capable Apps

**3. Click Create New App.**

The screenshot shows the Okta Applications page with a blue arrow pointing to the 'Create New App' button.

**Okta Applications**

← Back to Applications

**Add Application**

Can't find an app? **Create New App**

Apps you created (0) →

Category	App Name	Status	Action
TELADOC	TELADOC	Okta Verified	Add
&frankly	&frankly		Add

**4. In Platform, select Web.**

**5. In Sign on method, select SAML 2.0.**

### Create a New Application Integration

X

Platform: Web

Sign on method:

- Secure Web Authentication (SWA)  
Users credentials to sign in. This integration works with most apps.
- SAML 2.0  
Uses the SAML protocol to log users into the app. This is a better option than SWA, if the app supports it.
- OpenID Connect  
Uses the OpenID Connect protocol to log users into an app you've built.

**Create** **Cancel**

### To configure SSO in the Management Console:

1. In the sidebar, click **Scope**  and select a scope.

You must select **Global** or one Account. You cannot set a different SSO for one Site.

2. In the sidebar, click **Settings** .

3. In the **Settings** toolbar, click **Integrations**.



The screenshot shows the SSO configuration page in the SentinelOne Management Console. The page has a header 'SSO' and several input fields:

- Domain Name\***: A text input field containing a redacted domain name.
- Add Domain**: A link below the domain input.
- IDP redirect URL\***: A text input field containing a redacted URL.
- IssuerID**: A text input field containing a redacted URL.
- Default role**: A dropdown menu containing a redacted role name.
- IDP public certificate\***: Two text input fields, the top one containing a redacted URL and the bottom one containing a redacted file.
- Auto Provisioning**: A checked checkbox with a help icon.
- Assertion Consumer Service URL**: A text input field containing a redacted URL, with a 'Copy' button to its right.
- SP Entity ID**: A text input field containing a redacted URL, with a 'Copy' button to its right.
- Test**: A button at the bottom left of the form.

4. Click **Enable SSO**.
5. In **Domain Name**, enter one or more email domains. A domain name can be used globally or for one Account. You cannot enter the same domain name for more than one Account.
6. Optional: enable **Auto Provisioning**.

If you have Management Console users already configured, Auto Provisioning will make sure the user's Full Name is the same as in the SSO application. The email and role will stay the same.

If the SSO application has more users, Auto Provisioning automatically creates Console users from the entries.

If **Auto Provisioning** is not selected, no new users are created.

In **Settings > Users > Source**, you can see if a user was created or changed by Auto Provisioning (sso) or in the Console (SentinelOne).

If the Full Name of a Console-created user was changed by Auto Provisioning, the **Source** value changes to **SSO** only after the user logs in.

7. Copy the value in **Assertion Consumer Service URL** to the URL field of your SSO provider. In Okta, this is **Single sign on URL**.
8. Copy the value in **SP Entity ID** to the appropriate field of your SSO provider. In Okta, this is **Audience URI (SP Entity ID)**.
9. In the Okta **Attribute Statements** section, set up these attributes:

**Note:** The attributes are case-sensitive.

Name	Name Format	Value
email	Unspecified	user.email
full_name	Unspecified	user.firstName + " " + user.lastName
role	Unspecified	user.userType

## Roles

- If you configure the SAML assertion with the attribute **role**, with the value **admin** or **viewer** (all lower-case, exact spelling), the SentinelOne user will have that role.
- If the role attribute is not given, or has a value that is not **admin** or **viewer**, the console user will get the default role.

To set the default SentinelOne user role, click **Settings > INTEGRATIONS > SSO > Default role**.

- If the SAML request is to give SSO permissions to an existing user, the role does not change.

10. Click **Next**.
11. Click **I'm an Okta customer adding an internal app**.

3 Help Okta Support understand how you configured this application

Are you a customer or partner?

I'm an Okta customer adding an internal app

I'm a software vendor. I'd like to integrate my app with Okta

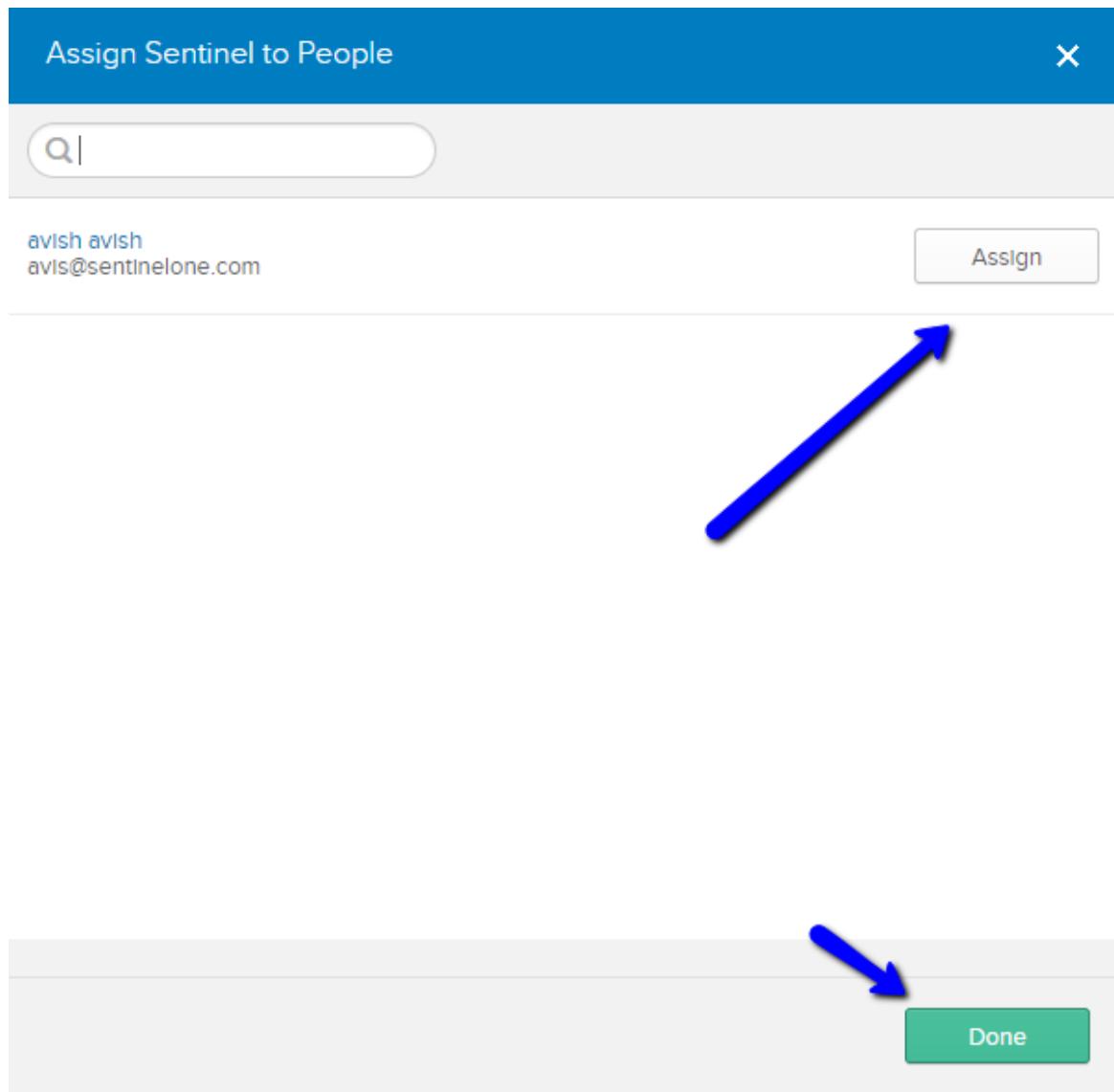
12. Click **Finish**.

**Make sure all your users are assigned to the SentinelOne app you created:**

1. In Okta, click **Assignments > Assign > People**.

The screenshot shows the Okta Applications interface for the 'Sentinel' application. At the top, there's a navigation bar with links for Dashboard, Directory, Applications, Security, Reports, Settings, and My Applications. Below the navigation, there's a card for the 'Sentinel' app with a gear icon, an 'Active' status dropdown, and a 'View Logs' button. Below the card, there are tabs: General, Sign On, Import, and Assignments (which is underlined). In the main content area, there's a search bar with 'Search...' and a dropdown for 'People'. On the left, there's a sidebar with 'FILTERS' and two options: 'People' (which is selected and highlighted in blue) and 'Groups'. The main list shows a single entry: 'avish avish' with the email 'avish@sentrilone.com'. To the right of this entry are 'Type' (set to 'Individual'), and edit and delete icons.

2. Add your Okta username. and click **Assign**.
3. Click **Done**.



### To configure SentinelOne for Okta:

1. In Okta Sign On > Settings, click View Setup Instructions.

[← Back to Applications](#)

  **Sentinel**  
Active   View Logs

General Sign On Import Assignments

---

### Settings

[Edit](#)

#### SIGN ON METHODS

The sign-on method determines how a user signs into and manages their credentials for an application. Some sign-on methods require additional configuration in the 3rd party application.

SAML 2.0

Default Relay State

SAML Library Version Current

 SAML 2.0 is not configured until you complete the setup instructions.  
[View Setup Instructions](#)

Identity Provider metadata is available if this application supports dynamic configuration.

#### CREDENTIALS DETAILS

Application username format  Okta username

Password reveal  Allow users to securely see their password (Recommended)

## 2. Click **Download Certificate**.



## How to Configure SAML 2.0 for Sent1 Application

The following is needed to configure Sent1

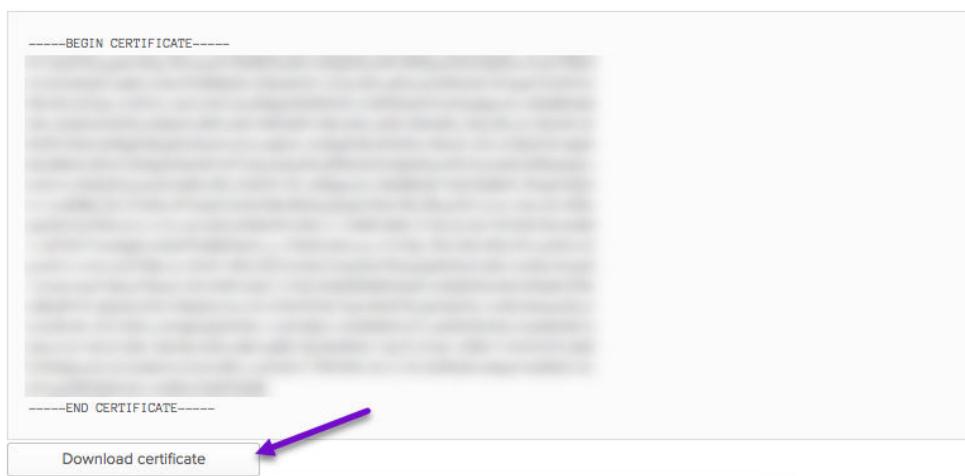
- ① Identity Provider Single Sign-On URL:

`https://sso/saml;`

- ② Identity Provider Issuer:

`http://www.okta.com/`

- ③ X.509 Certificate:



3. In Management Console > **SETTINGS** > **INTEGRATIONS** > **SSO**, copy the URL from the Okta Setup details to **IDP redirect URL**.
4. Copy the Okta Issuer ID to **IssuerID**.
5. Click the **IDP public certificate** link (**Upload or Change**).
6. Select the downloaded Okta certificate.
7. Click **Test**.

The configuration is sent to Okta in test mode. Your browser is redirected to the Okta URL. If you are not logged in, you must provide the credentials of an Okta user that you assigned to the SentinelOne app. Okta verifies the credentials and redirects your browser to the Management Console > **SSO**. The page shows the **Save** button.

**Note:** In test mode, no new user is created. You must use an assigned user.

If you are logged in to Okta when it redirects in test mode, you will get an error message that your Okta user does not have permissions to the SentinelOne app. On your browser, click **Back** until you are in the Management Console. Open a new tab or browser and explicitly log out of Okta.

8. Click **Save**.

9. Log out of the Management Console. Log in with SSO.

## 15.2. Integrating SMTP Servers [Multi-Site]

**Management:** Central Park, Denali, Eiffel, Fuji, Grand Canyon, Houston

**Agents:** Windows 2.6+ | macOS 2.6+ | Linux 2.6+

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

Configure integration with your SMTP server, to let the Management send alerts to security personnel and stakeholders.

In the view for one Account or Site, you can configure a server specifically for that scope. If a scope does not have a specific configuration, it uses the Global Integration settings.

After you complete the SMTP integration, configure notifications.

### To configure integration with SMTP:

1. In the sidebar, click **Scope**  and select a scope.  
If you are a Site Admin, you must select one Site to open **Settings**.
2. In the sidebar, click **Settings** .
3. In the **Settings** toolbar, click **Integrations**.



**SMTP** opens by default.

SMTP

[Clear pending email notifications](#)

Disable SMTP

**Basic details**

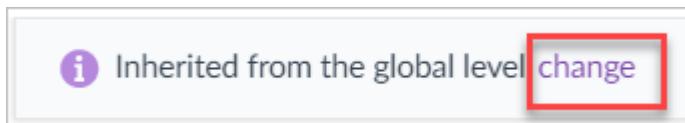
Host\* [REDACTED] : [REDACTED]  
No-reply email\* [REDACTED]  
Username [REDACTED]  
Password [change](#)

**Encryption**

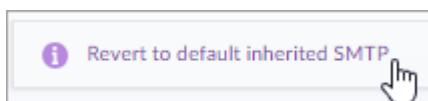
SSL  
 TLS  
 Turn off encryption

[Test](#)

- For Accounts and Sites: By default, the Global settings are inherited. Click **Change** to edit them.



If the Account or Site has different settings from the Global settings, you can click **Revert to default inherited SMTP** to use the Global settings.



- Enter the data of your SMTP email server.

## SMTP Server Integration

Field	Description
<b>Host</b>	Hostname and listening port of the SMTP server (valid for selected Encryption).
<b>No-reply email</b>	Optional. Enter a no-reply email address to be the sender of Management Console notifications
<b>Username / Password</b>	Enter the username and password of the system administrator with authorization to access the SMTP server.

- In **Encryption**, select **SSL**, **TLS**, or **Turn off encryption**.

7. Click **Test**.
8. If the test passed, click **SAVE**.

### 15.2.1. Configuring Email Notifications [Multi-Site]

**Management:** Central Park, Denali, Eiffel, Fuji, Grand Canyon, Houston

**Agents:** Windows 2.6+ | macOS 2.6+ | Linux 2.6+

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

After you integrate an SMTP Server, configure which SentinelOne activities trigger email notifications, and who gets the notifications

In the view for one Account or Site, you can configure a server specifically for that scope. If a scope does not have a specific configuration, it uses the Global Integration settings.

#### To configure email notifications:

1. In the sidebar, click **Scope**  and select a scope.  
If you are a Site Admin, you must select one Site to open **Settings**.
2. In the sidebar, click **Settings** .
3. In the **Settings** toolbar, click **Notifications**.



4. Click a **Notification Type**, for example, **Administrative** or **Malware**.



5. In the **Email** column, select which activities will trigger messages.
6. In the **Notification Types** list, click **Recipients**.

The screenshot shows the 'Notifications Recipients' page. On the left, a sidebar lists 'Notification Types' including Administrative, Device Control, Malware, Mitigation, Operations, and Exclusions / Blacklist. Below this is a section for 'Notification Settings'. At the bottom of the sidebar, the 'Recipients' link is highlighted with a red oval. At the top right of the main area, there is a purple button labeled 'New recipient' which is also highlighted with a red oval. Below it, there are two input fields, each containing a small user icon and a blurred email address.

7. Click **New recipient** to add each new email address.

### 15.2.2. Clearing the SMTP Message Queue [Multi-Site]

**Management:** Central Park, Denali, Eiffel, Fuji, Grand Canyon, Houston

**Agents:** All

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

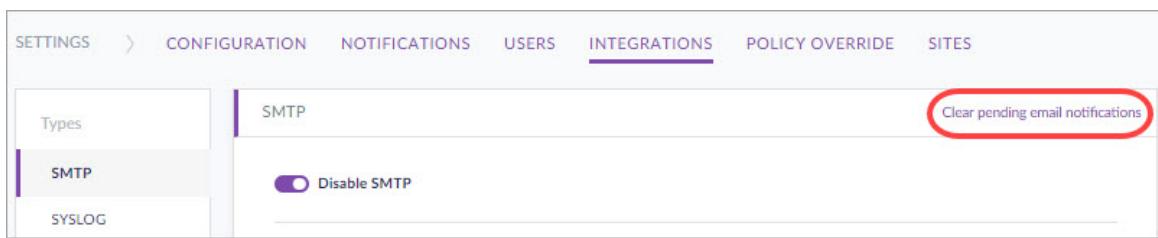
You can clean delete pending SMTP notification emails to clean up your message queue. For example, in a situation where configured message recipients left the company, and their messages stay as pending. Or if an admin's mailbox is full and messages cannot send successfully.

#### To clear pending emails from the SMTP queue:

1. In the sidebar, click **Scope**  and select a scope.  
If you are a Site or Account Admin, you must select one Site to open Settings.
2. In the sidebar, click **Settings** .
3. In the **Settings** toolbar, click **Integrations**.

The screenshot shows the 'Settings' toolbar with several tabs: SETTINGS, CONFIGURATION, NOTIFICATIONS, USERS, INTEGRATIONS (which is highlighted with a purple underline), POLICY OVERRIDE, ACCOUNTS, and SITES.

4. Click **SMTP**.
5. Click **Clear pending email notifications**.



## 15.3. Integrating Syslog Servers [Multi-Site]

**Management:** Central Park, Denali, Eiffel, Fuji, Grand Canyon, Houston

**Agents:** Windows 2.6+ | macOS 2.6+ | Linux 2.6+

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

Integrate your Syslog server to collect SentinelOne logs. Before you begin, ask the system administrator who configured or maintains the Syslog server if authentication certificates are used. If so, you need access to those certificates. Then configure your Syslog server integration with SentinelOne, with the steps here. When these steps are done, select events to be logged.

In the view for one Account or Site, you can configure a server specifically for that scope. If a scope does not have a specific configuration, it uses the Global Integration settings.

### To integrate your Syslog server:

1. In the sidebar, click **Scope**  and select a scope.  
If you are a Site or Account Admin, you must select one Site to open Settings.
2. In the sidebar, click **Settings** .
3. In the **Settings** toolbar, click **Integrations**.



4. Click **SYSLOG**.

SYSLOG

Host Your syslog host IP or host name : 0

SSL Use SSL secure connection

Formatting Information format CEF

Test Save DISCARD CHANGES

5. Click **Enable SYSLOG**.
6. In **Host**, enter the hostname and port of your syslog server.
7. To use SSL or TLS channel authentication and privacy, click **Use SSL secure connection**.  
If you do not select this, UDP is used.
8. In **Certificate**, you can upload server and client certificates to verify client/server authorization between the SentinelOne Management (client) and the syslog server (server). These options only show if **Use SSL secure connection** is selected. Passphrase certificates are not supported.  
Make sure you know how the Syslog server is configured, and that you have the correct certificates from that configuration.

SSL Use SSL secure connection

Certificate Certificates sent from/to the syslog server. Choose one out of three verification options: server only, client only or server & client verification

Server certificate Upload ?

Client certificate Upload ?

Client key Upload

- **Server certificate** - Select and upload a certificate to verify the syslog server identity.

- **Client certificate** - Select and upload a certificate to verify the SentinelOne Management as a client of the syslog server. Use a certificate file with a client key. A Client certificate is necessary if the server requires client authentication.
  - **Client key** - Select and upload the client key of a client/server key pair. A Client key is necessary, along with a Client certificate, if the server requires client authentication.
9. In **Formatting**, select the format for the logs: **CEF**, **CEF2**, **STIX**, **IOC**, **RFC-5424**.  
 For Rsyslog format, select **RFC-5424**.
10. Click **TEST**.
11. If the test passed, click **SAVE**.

### 15.3.1. Configuring Syslog Notifications [Multi-Site]

**Management:** Central Park, Denali, Eiffel, Fuji, Grand Canyon, Houston

**Agents:** Windows 2.6+ | macOS 2.6+ | Linux 2.6+

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

After you integrate a Syslog Server, configure which SentinelOne activities trigger Syslog messages.

In the view for one Account or Site, you can configure a server specifically for that scope. If a scope does not have a specific configuration, it uses the Global Integration settings.

#### To configure Syslog notifications:

1. In the sidebar, click **Scope**  and select a scope.  
 If you are a Site or Account Admin, you must select one Site to open Settings.
2. In the sidebar, click **Settings** .
3. In the **Settings** toolbar, click **Notifications**.



4. Click a **Notification Type**, for example, **Administrative** or **Malware**.



5. In the **Syslog** column, select which activities will trigger messages.
6. Click **Save**.

### 15.3.2. SentinelOne Syslog CEF2 Message Attributes [Multi-Site]

**Management Server:** Central Park, Denali, Eiffel, Fuji, Grand Canyon, Houston

**Agents:** Windows All

**Note:** Syslog notifications in RFC-5424 (Rsyslog) format use CEF2 attributes.

#### New Attributes in Grand Canyon

Attribute	Description	Applies to
accountId	The ID of the Account related to the activity	ALL activities from Grand Canyon SP3
accountName	The name of the Account related to the activity	ALL activities from Grand Canyon SP3

Attribute	Description	Applies to
activityID	The ID of the specific activity (from the Management Server) that caused this specific notification.	All activities
activityType	The numeric code of an <a href="#">event type</a> . This replaces eventID.	All activities

Attribute	Description	Applies to
sourceIpAddresses	IP address of the endpoint	AGENT_UPLOADED_REMOTE_SHELL_HISTO USER_TERMINATED_REMOTE_SHELL_SESS REMOTE_SHELL_TERMINATED (3203) REMOTE_SHELL_FAILED (3202) REMOTE_SHELL_CREATED (3201) START_REMOTE_SHELL (3200) AGENT_BLOCKED_FIREWALL_TRAFFIC (5232) AGENT_APPROVED_EVENT (5126) AGENT_BLOCKED_EVENT (5125)
sourceMacAddresses	MAC address of the endpoint.	
sourceAgentId	ID of the endpoint.	
sourceGroupId	ID of the Group the endpoint is in.	SCAN_COMPLETED (92) SCAN_ABORTED (91) FETCH_FILES (81) SCAN_STARTED (90) AGENT_UPLOADED_FETCHED_FILES (80)
sourceGroupName	Name of the Group the endpoint is in.	AGENT_MITIGATION_REPORT_QUARANTINE (2010) THREAT_MITIGATION_REPORT_QUARANTINE THREAT_MITIGATION_REPORT_ROLLBACK THREAT_MITIGATION_REPORT_REMEDIEATE THREAT_MITIGATION_REPORT_KILL_FAILED AGENT_MITIGATION_REPORT_QUARANTINE (2005) THREAT_MITIGATION_REPORT_QUARANTINE THREAT_MITIGATION_REPORT_ROLLBACK THREAT_MITIGATION_REPORT_REMEDIEATE THREAT_MITIGATION_REPORT_KILL_SUCCESS PROCESS_MARK_AS_THREAT (4009) THREAT_STATUS_CHANGED (4008) THREAT_SUSPICIOUS_UNRESOLVED (4011) THREAT_SUSPICIOUS_RESOLVED (4002) THREAT_MARK_AS_THREAT (4001) NEW_THREAT_SUSPICIOUS (4003) CLOUD_MARK_A_THREAT_AS_UNRESOLVED THREAT_RESOLVED_BY_CLOUD (28) THREAT_UNRESOLVED (34) THREAT_RESOLVED (21) NEW_THREAT_PREEMPTIVE_BLOCK (20) NEW_THREAT_NOT_MITIGATED (19) NEW_IMMUNE (2) NEW_THREAT_MITIGATED USER_RANDOMIZED_AGENT_UUID (89) USER_RESTARTED_MACHINE (74) REQUESTED_FULL_LOG_REPORT (65) USER_REQUESTED_PASSPHRASE (64) USER_SHUTDOWN_AGENT (63) USER_UNQUARANTINE_AGENT_NETWORK (61) USER_QUARANTINE_AGENT_NETWORK (61) USER_RECOMMISSIONED_AGENT (55) USER_DECOMMISSIONED_AGENT (54) USER_REJECTED_AGENT_UNINSTALL_REQ USER_APPROVED_AGENT_UNINSTALL_REQ AGENT_UPLOADED_FULL_LOG_REPORT (66) AGENT_UNINSTALLED (51) AGENT_REQUESTED_UNINSTALL (49) AGENT_RECOMMISSIONED (48) AGENT_DECOMMISSIONED (47) AGENT_UPDATED (43) AGENT_SUBSCRIBED (17)

Attribute	Description	Applies to
newValue	For specific configuration changes, this shows the new value, usually "true" or "false".	AUTO_DECOMMISSION_ON (44) AUTO_DECOMMISSION_OFF (45) SHOW_SUSPICIOUS_ON (4004) SHOW_SUSPICIOUS_OFF (4005)
deviceRuleBluetoothVersion	Bluetooth version used to define a rule.	Can apply to these Device Control events: DEVICE_RULE_CREATED (5120) DEVICE_RULE_MODIFIED (5121) DEVICE_RULE_DELETED (5122) DEVICE_RULES_reordered (5123) DEVICE_SETTINGS_MODIFIED (5124) AGENT_BLOCKED_EVENT (5125) AGENT_APPROVED_EVENT (5126) DEVICE_MOVED_RULE_FROM_SCOPE (5127) DEVICE_MOVED_RULE_TO_SCOPE (5128) DEVICE_COPIED_RULE_TO_SCOPE (5129)
deviceRuleBluetoothLmpVersion	Lmp version of the rule.	
deviceRuleBluetoothMinorClass	Bluetooth minor classes of the rule.	
endpointDeviceControlBluetoothVersion	Bluetooth version reported by the Agent in a Device event.	
endpointDeviceControlBluetoothMinorClass	Minor class reported by the Agent in a Device event.	
endpointDeviceControlBluetoothProfileUuids	Not in use-present but empty.	

### Attributes from Central Park through Fuji

Attribute Key	Description	Applies to	Type
cat	Type of notification, based on Settings > Notifications in the Management Console. For example, Mitigation or Operations.	Notification Type	String
deviceAddress	SentinelOne Management Console IPv4 addresses (in CEF sometimes referred to as dvc, alias)	All activities	IPv4

Attribute Key	Description	Applies to	Type
deviceHostFqdn	SentinelOne Management Console fully qualified domain name (in CEF sometimes referred to as dvchost, alias)	All activities	String
deviceHostName	SentinelOne Management Console fully qualified domain name (in CEF sometimes referred to as dvchost, alias)	All activities	String
deviceRuleAction	Action of the rule: Block or Allow	Device Control	String
deviceRuleDeviceClass	Device Class identifier	Device Control	String

Attribute Key	Description	Applies to	Type
deviceRuleId	Unique ID of a Device Control rule.	Device Control	String
deviceRuleInterface	Which interface the rule applies to	Device Control	String
deviceRuleName	Name of the rule from the Management Console	Device Control	String
deviceRuleProduct	Device Product ID	Device Control	String
deviceRuleSerial	Device Serial ID	Device Control	String
deviceRuleStatus	Status of the rule: Enabled or Disabled	Device Control	String
deviceRuleVendor	Device Vendor ID	Device Control	String
endpointDeviceControlClass	Device Class identifier	Device Control Notifications	String
endpointDeviceControlDeviceName	Name of the device	Device Control Notifications	String

Attribute Key	Description	Applies to	Type
endpointDeviceControlInterface	Which interface the rule applies to	Device Control Notifications	String
endpointDeviceControlProduct	Device Product ID	Device Control Notifications	String
endpointDeviceControlRuleId	Unique ID of a Device Control or Firewall Control rule.	Device Control Notifications	String
endpointDeviceControlSerial	Device Serial ID	Device Control Notifications	String
endpointDeviceControlVendor	Device Vendor ID	Device Control Notifications	String
endpointFirewallRuleApplication	Application in the rule	Firewall Control	String
endpointFirewallRuleDirection	Direction in the rule, inbound, outbound, or any	Firewall Control	String
endpointFirewallRuleLocalHost	Local Host in the rule	Firewall Control	String
endpointFirewallRuleLocalPort	Local Port in the rule	Firewall Control	String

Attribute Key	Description	Applies to	Type
endpointFirewallRuleProtocol	Protocol in the rule	Firewall Control	String
endpointFirewallRuleRemoteHost	Remote Host in the rule	Firewall Control	String
endpointFirewallRuleRemotePort	Remote Port in the rule	Firewall Control	String
eventDesc	Readable text to complement the ID and to headline the event in text	All activities	String
eventID	Unique ID for each SentinelOne provided Event, including activity, threat, agent, policy. Replaced by activity Type in Management version Grand Canyon	All activities	Integer

Attribute Key	Description	Applies to	Type
eventSeverity	<p>For severity always use 0 for clearing (okay) and 1 (lowest) to 10 (highest) - Please note that this attribute is different from the CEF header provided severity that is event catalog driven, in that this eventSeverity attribute is context dependent and provides additional information/granularity - for example, on threat detection</p> <p>map severit y based</p>	All activities	Integer [0-10]

Attribute Key	Description	Applies to	Type
fileHash	SHA1 value for the file checks um	Detections, Activity	String
fileName	Name of the file referenced by this threat - for static detections this is the file name and for behavioral this is the processes executable filename	Detection, Mitigation	String

Attribute Key	Description	Applies to	Type
filePath	Path of the file referenced by this threat - for static detections this is the path name and for behavioral this is the pathname for the process executable	Detection, Mitigation	String
firewallNotificationRuleAction	Action in the rule - Allow or Block	Firewall Control Notifications	String
firewallNotificationRuleId	Unique ID of a Firewall Control rule	Firewall Control Notifications	String
firewallNotificationRuleName	Name of the rule from the Management Console	Firewall Control Notifications	String

Attribute Key	Description	Applies to	Type
firewallNotificationTrafficDurationOfMeasurement	Duration of the aggregated firewall events for a rule	Firewall Control Notifications	String
firewallNotificationTrafficLocalHost	Local Host in the rule	Firewall Control Notifications	String
firewallNotificationTrafficLocalPort	Local Port in the rule	Firewall Control Notifications	String
firewallNotificationTrafficNumberOfEvents	Number of aggregated firewall events for a rule	Firewall Control Notifications	String
firewallNotificationTrafficPID	Process ID in the notification	Firewall Control Notifications	String
firewallNotificationTrafficProcessName	Process Name in the notification	Firewall Control Notifications	String
firewallNotificationTrafficProtocol	Protocol that the rule applies to	Firewall Control Notifications	String
firewallNotificationTrafficRemoteHost	Remote Host in the rule	Firewall Control Notifications	String

Attribute Key	Description	Applies to	Type
firewallNotificationTrafficRemotePort	Remote Port in the rule	Firewall Control Notifications	String
notificationScope	SITE - Notification relates to 1 Site ACCOUNT - Notification relates to an Account (from Grand Canyon SP3) GLOBAL - Notification relates to All Sites	Identifier in Multi-Site Console	"SITE", "ACCOUNT", or "GLOBAL"

Attribute Key	Description	Applies to	Type
originatorName	SentinelOne component event source : ["mgmt", "XXX-agent", "cloud" ...] by default should always use "mgmt", and if originating from agent, signify agent type ["macOS-agent", "Linux-agent", "Windows-agent" ...]	All activities	String
originatorUserId	For administrative actions use the administrator user (AD/SSO) SID if exists	Activity	String

Attribute Key	Description	Applies to	Type
originatorVersion	SentinelOne event originator component version.	Always	String
remoteShellEventDescription	Longer description for session termination or any other unusual event, generated by the Management or the Agent.	Remote Shell	String
remoteShellEventReason	Reason for session termination or any other unusual event, generated by the Management or the Agent.	Remote Shell	String

Attribute Key	Description	Applies to	Type
remoteShellSessionId	Unique ID generated for each session by the Management.	Remote Shell	String
rt	Cite the event originator reported timestamp as ArcSig ht string format (rt=May 06 2016 14:34:29 GMT +00:00). For example, for an agent detected threat this is the agent reported time of the event	Always	Timestamp
rt	Timestamp of the activity creation	Always	Timestamp

Attribute Key	Description	Applies to	Type
ruleId	Unique ID of a Device Control or Firewall Control rule.	Device Control or Firewall Control	String
ruleName	Name of the Device Control or Firewall Control rule from the Management Console	Device Control or Firewall Control	String
siteID	Site ID from the Management Console (Central Park and higher)	Identifier in Multi-Site Console	String
siteName	Site Name from the Management Console (Central Park and higher)	Identifier in Multi-Site Console	String

Attribute Key	Description	Applies to	Type
sourceAddress	Agent-perceived IPv4 address (of its hosting endpoint) as reported by the API on network_information.interfaces(0).inet, can be multiple (Note: the Agent-perceived interfaces(0) are reported as <b>source Addresses</b> , and other network interfaces are <b>source AddressesNN</b> where NN is the index of the network interface 1..n)	Detections, AgentStates, Activity(ServiceEvents having known client information - for example, browser or API remote call)	String

Attribute Key	Description	Applies to	Type
sourceAgentLastActivityTimestamps	Last time and date of the agent last activity reported to the Sentinel One mgmt server	Detection, Mitigation, AgentState	Timestamp
sourceAgentRegisterTimestamps	Last time the agent registered with the Last time and date of the agent last activity reported to the Sentinel One mgmt server	Detection, Mitigation, AgentState	Timestamp

Attribute Key	Description	Applies to	Type
sourceAgentUUID	Agent reported UUID (SentinelOne agent uniquely given identifier - typically taken from the endpoint OS provided hardware serial identifier attributes)	Detection, Mitigation, AgentState	String
sourceDnsDomain	Agent-perceived domain name (of its hosting endpoint) typically resolved to its associated DNS associated name	Detections, AgentStates, Activity(ServiceEvents having known client information - for example, browser or API remote call)	String

Attribute Key	Description	Applies to	Type
sourceFqdn	Agent reported on endpoint perceived hostname and DNS domain name	Detection, Mitigation, AgentState	String
sourceHostName	Agent-perceived hostname (of its hosting endpoint)	Detections, AgentStates, Activity(ServiceEvents having known client information - for example, browser or API remote call)	String
sourceHostSid	Use {agent.machine_sid} when exists	Detections, AgentStates, Activity(ServiceEvents having known client information - for example, browser or API remote call)	String

Attribute Key	Description	Applies to	Type
sourceMacAddress	<p>Agent-perceived Ethernet address (of its hosting endpoint) as reported by the API on network_information.interfaces(0).physical</p> <p>(Note: the Agent perceived interfaces(0) are reported as <b>source MacAddress</b> - and other network interfaces are <b>source MacAddress NN</b> where NN is the index of the network interface 1..n)</p>	Detection, Mitigation, AgentState	String

Attribute Key	Description	Applies to	Type
sourceMgmtPrecievedAddress	Management-perceived external IP address of the agent calling home from the endpoint	Detection, Mitigation, AgentState	String
sourceNetInterfaceName	Agent-perceived Ethernet address (of its hosting endpoint) as reported by the mgmt API on network_information.interfaces(0).physical	AgentState	String
sourceNetworkState	Endpoint-perceived network connectivity status (network_status)	Detection, Mitigation, AgentState	String

Attribute Key	Description	Applies to	Type
sourceOsRevision	Agent provide d OS revision information	Detection, Mitigation, AgentState	String
sourceOsType	Based on agentType info [macOS, Linux or Windows] as reported by the Agent os_type	Detection, Mitigation, AgentState	String
sourceThreatCount	Number of active threats associated with this endpoint	Detection, Mitigation, AgentState	Integer

Attribute Key	Description	Applies to	Type
sourceUserId	User or group number of the endpoint last known logged in user (last_logged_in_user_name) - typically this maps to LDAP/AD user logon name or sAMAccountName, and depending on the OS can have Linux, macOS value for 'root' or similar local user account ID Note: LDAP and AD integration is not supported on Management version 5 after Fuji.	Detections, AgentStates, Activity(ServiceEvents having known client information - for example, browser or API remote call)	String
SentinelOne	Version Houston		283

Attribute Key	Description	Applies to	Type
sourceUserName	<p>Current user name that is typically mapped to LDAP/AD name attribute or cn and in some cases the agent perceived local login username like 'root' for macOS and Linux.</p> <p>Note: LDAP and AD integration is not supported on Management versions after Fuji.</p>	Detections, AgentStates, Activity(ServiceEvents having known client information - for example, browser or API remote call)	String
sourceUserSid	<p>Use {agent.last_logged_in_user_sid} when exists</p>	Detections, AgentStates, Activity(ServiceEvents having known client information - for example, browser or API remote call)	String

Attribute Key	Description	Applies to	Type
suser	User that triggered the activity	All activities	Username
threatClassificationSource	threat.classifications.source	Detection, Mitigation	String
threatClassification	threat.classifications.classifications	Detection, Mitigation	String
threatClassifier	threat.classifier_name	Detection, Mitigation	String
threatCommandLineArguments	Threat associated process whose executable file, path, and in this attribute, its associated command line information as reported by the agent (i.e. malicious_process_arguments)	Detection, Mitigation	String

Attribute Key	Description	Applies to	Type
threatDetectingEngine	threat. engine _data. engine	Detection, Mitigation	String
threatID	SentinelOne threat identifier	Detection, Mitigation	String
threatMitigationStatusID	Use the SentinelOne API equivalent of mitigation_status values: 0 - Mitigated 1 - Active 2 - Blocked 3 - Suspicious 4 - Pending 5 - Suspicious canceled	Detection, Mitigation	Integer

Attribute Key	Description	Applies to	Type
threatMitigationStatusLabel	As described in the threat MitigationStatusID but giving the enum literal so "mitigated" for 0, "active" for 1 and so on...	Detection, Mitigation	String
vendor	Always equals "SentinelOne"	Always	String

### 15.3.3. SentinelOne Syslog Events

**Management:** Banff, Central Park, Denali, Eiffel, Fuji, Grand Canyon, Houston

**Agent:** All

For the most up-to-date Syslog event information, from the API, run:

```
curl --request POST https://origin/web/api/API VERSION/activities/types --header "Authorization: APIToken token" --header "Content-Type: application/json"
```

Where *API VERSION* is:

- Banff - **v1.6**
- Central Park, Denali, Eiffel, Fuji, Grand Canyon, Houston - **v2.0**

Starting with Management version Banff SP1, these Syslog events are recorded:

Event ID Activity Type ID	Activity Type	Category
1	Unknown	
17	Agent subscribed	Agents

Event ID Activity Type ID	Activity Type	Category
43	Agent updated	Agents
47	Agent decommissioned	Agents
48	Agent recommissioned	Agents
49	Agent requested uninstall	Agents
51	Agent uninstalled	Agents
66	Agent uploaded full log report	Agents
52	User approved agent uninstall request	User actions
53	User rejected agent uninstall request	User actions
54	User decommissioned agent	User actions
55	User recommissioned agent	User actions
61	User quarantined agent network	User actions
62	User unquarantined agent network	User actions
63	User shutdown agent	User actions
64	User requested passphrase	User actions
65	Requested full log report	User actions
74	User restarted machine	User actions
71	User initiated scan agent	Full disk scan
72	User aborted scan agent	Full disk scan
2	New immune	Black whitelist
3001	User added a white hash	Black whitelist
3002	User added a black hash	Black whitelist
3003	User modified hash	Black whitelist
3004	User deleted hash	Black whitelist
16	Software update added	Commands added
50	Uninstall added	Commands added
5	Agent software update downloaded	Commands downloaded
1001	Agent network quarantined	Agents
1002	Agent network unquarantined	Agents
18	New threat mitigated	Threats
19	New threat not mitigated	Threats
20	New threat preemptive block	Threats
21	Threat resolved	Threats
22	Threat benign	Threats
28	Threat resolved by Cloud	Threats
29	Cloud mark a threat as unresolved	Threats
30	Threat whiten by certificate	Threats
31	Threat whiten by browser	Threats
32	Threat whiten by path	Threats

Event ID Activity Type ID	Activity Type	Category
4003	New threat suspicious	Threats
4001	Threat mark as threat	Threats
4002	Threat suspicious resolved	Threats
4007	Threat suspicious benign	Threats
4008	Threat status changed	Threats
4009	Process mark as threat	Threats
4010	User annotated threat	Threats
2001	Threat mitigation report kill success	Mitigation reports
2002	Threat mitigation report remediate success	Mitigation reports
2003	Threat mitigation report rollback success	Mitigation reports
2004	Threat mitigation report quarantine success	Mitigation reports
2005	Agent mitigation report quarantine network success	Mitigation reports
2006	Threat mitigation report kill failed	Mitigation reports
2007	Threat mitigation report remediate failed	Mitigation reports
2008	Threat mitigation report rollback failed	Mitigation reports
2010	Agent mitigation report quarantine network failed	Mitigation reports
2011	User killed threat	Mitigation by user
2012	User remediated threat	Mitigation by user
2013	User rolled back threat	Mitigation by user
2014	User quarantined threat	Mitigation by user
2015	User unquarantined threat	Mitigation by user
2016	User marked application as threat	Mitigation by user
2021	Threat killed by policy	Mitigation by policy
2022	Threat remediated by policy	Mitigation by policy
2023	Threat rolled back by policy	Mitigation by policy
2024	Threat quarantined by policy	Mitigation by policy
2025	Threat quarantined network by policy	Mitigation by policy
23	User added	Settings
24	User modified	Settings
25	User deleted	Settings
26	Management updated	Settings
1023	SSO user added	Settings
1024	SSO user modified	Settings
4006	Remember me length modified	Settings
38	Immune settings modified	Settings
39	Research settings modified	Settings
40	Cloud intelligence settings modified	Settings

Event ID Activity Type ID	Activity Type	Category
41	Learning mode settings modified	Settings
42	Global two FA modified	Settings
44	Auto decommission on	Settings
45	Auto decommission off	Settings
	Auto decommission period modified	Settings
56	Auto mitigation actions modified	Settings
57	Quarantine network settings modified	Settings
58	Notification option level modified	Settings
59	Event severity level modified	Settings
60	Recipients configuration modified	Settings
4004	Show suspicious on	Settings
4005	Show suspicious off	Settings
67	User modified two FA	Settings
68	Engine policy modified	Settings
69	Policy threat mode modified	Settings
70	Agent notification on suspicious modified	Settings
73	Scan new agents modified	Settings
75	On access modified	Settings
76	Anti-tampering modified	Settings
77	Agent UI modified	Settings
78	Snapshots modified	Settings
79	Agent logging modified	Settings
80	Agent uploaded fetched files	Settings
81	Fetch files	Settings
82	Monitor on execute modified	Settings
83	Monitor on write modified	Settings
84	IOC modified	Settings
90	Scan started	Settings
91	Scan aborted	Settings
92	Scan completed	Settings
5000	AD sync started	Group change activities
5001	AD sync finished	Group change activities
5002	Dynamic group creation started	Group change activities
5003	Dynamic group creation finished	Group change activities
5004	Dynamic group update started	Group change activities
5005	Dynamic group update finished	Group change activities
5006	Group deleted	Group change activities
5007	Group info changed	Group change activities

Event ID Activity Type ID	Activity Type	Category
5008	Static group created	Group change activities
5009	Group content changed	Group change activities
5010	Group ranks changed	Group change activities

Starting with Management version Fuji, these Syslog events are recorded:

Event ID Activity Type ID	Activity	Category
93	USER_RESET_LOCAL_CONFIG	User actions
94	USER_MOVED_AGENT_TO_SITE	User actions
95	USER_MOVED_AGENT_TO_GROUP	User actions
96	USER_MOVED_AGENT_FROM_SITE	User actions
97	USER_COMMANDED_AGENT_TO_MOVE_TO_CONSOLE	User actions
98	AGENT_NOT_MOVED_TO_CONSOLE	User actions
99	AGENT_SUCCESSFULLY_MOVED_TO_CONSOLE	User actions
10000	AGENT_FAILED_TO_MOVE_TO_CONSOLE	agents
3005	CLOUD_ADDED_WHITE_HASH	black white list
3006	CLOUD_ADDED_BLACK_HASH	black white list
3007	CLOUD_MODIFIED_HASH	black white list
2009	THREAT_MITIGATION_REPORT_QUARANTINE_FAILED	mitigation reports
27	USER_LOGGED_IN	settings
33	USER_LOGGED_OUT	settings
46	AUTO_DECOMMISSION_PERIOD_MODIFIED	settings
85	FETCH_THREAT_FILE	settings
86	AGENT_UPLOADED_THREAT_FILE	settings
87	REMOTE_SHELL_MODIFIED	settings
88	USER_MODIFIED_REMOTE_SHELL	settings
5011	GROUP_POLICY_REVERTED	group changes activities
5020	SITE_CREATED	site activities
5021	SITE_INFO_CHANGED	site activities
5022	SITE_DELETED	site activities
5023	SITE_EXPIRED	site activities
5024	SITE_POLICY_REVERTED	site activities
5025	SITE_EXPIRED_NOW	site activities
5026	SITE_DUPLICATED	site activities
5027	SITE_KEY_REGENERATED	site activities
5120	DEVICE_RULE_CREATED	device activities

Event ID Activity Type ID	Activity	Category
5121	DEVICE_RULE_MODIFIED	device activities
5122	DEVICE_RULE_DELETED	device activities
5123	DEVICE_RULES_reordered	device activities
5124	DEVICE_SETTINGS_MODIFIED	device activities
5125	AGENT_BLOCKED_EVENT	device activities
5126	AGENT_APPROVED_EVENT	device activities
5127	DEVICE_MOVED_RULE_FROM_SCOPE	device activities
5128	DEVICE_MOVED_RULE_TO_SCOPE	device activities
5129	DEVICE_COPIED_RULE_TO_SCOPE	device activities
5220	FIREWALL_RULE_CREATED	firewall activities
5221	FIREWALL_RULE_MODIFIED	firewall activities
5222	FIREWALL_RULE_DELETED	firewall activities
5225	FIREWALL_SETTINGS_MODIFIED	firewall activities
5226	FIREWALL_RULES_reordered	firewall activities
5227	FETCH_FIREWALL_RULES	firewall activities
5228	AGENT_UPLOADED_FIREWALL_RULES	firewall activities
5229	FIREWALL_MOVED_RULE_FROM_SCOPE	firewall activities
5230	FIREWALL_MOVED_RULE_TO_SCOPE	firewall activities
5231	FIREWALL_COPIED_RULE_TO_SCOPE	firewall activities
5232	AGENT_BLOCKED_FIREWALL_TRAFFIC	firewall activities
5233	FIREWALL_LOGGING	firewall activities
3100	PACKAGE_ADDED	Package activities
3101	PACKAGE_MODIFIED	Package activities
3102	PACKAGE_DELETED	Deleted by user
3103	PACKAGE_PURGED	System restrictions on number of packages
3200	START_REMOTE_SHELL	Remote Shell
3201	REMOTE_SHELL_CREATED	Remote Shell
3202	REMOTE_SHELL_FAILED	Remote Shell
3203	REMOTE_SHELL_TERMINATED	Remote Shell
3204	USER_TERMINATED_REMOTE_SHELL_SESSION	Remote Shell
3400	AGENT_UPLOADED_REMOTE_SHELL_HISTORY	Remote Shell

Starting with Grand Canyon, these Syslog events are recorded:

Event ID Activity Type ID	Activity	Category
34	THREAT_UNRESOLVED	Threats
4011	THREAT_SUSPICIOUS_UNRESOLVED	Threats
35	VERIFICATION_EMAIL_SENT_TO_USER	Users
36	USER_VERIFICATION_COMPLETE	Users
1501	LOCATION_CREATED	Locations
1502	LOCATION_COPIED	Locations
1503	LOCATION_MODIFIED	Locations
1504	LOCATION_DELETED	Locations

#### 15.3.4. Syslog Integration with Sumo Logic

**Management:** Central Park, Denali, Eiffel, Fuji, Grand Canyon, Houston

**Agents:** All

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

For integration with Sumo Logic, you can define an SIEM token to add in the message ID of CEFv2 Syslog messages. The first procedure assumes you have `wget`.

##### To get a token and certificate from Sumo Logic:

1. Log in to the [Sumo Logic website](#).
2. Configure a Cloud Syslog Collector and Source, and generate a Cloud Syslog Source Token.
3. Download the crt server certificate file from [here](#).
4. From the path where the crt file is located, open a terminal.
5. Run:

```
wget -O digicert_ca.der https://www.digicert.com/CACerts/
DigiCertHighAssuranceEVRootCA.crt
openssl x509 -inform der -in digicert_ca.der -out digicert_ca.crt
```

##### To configure the Syslog messages from the Management Console:

1. In the sidebar, click **Scope**  and select a scope.  
If you are a Site or Account Admin, you must select one Site to open Settings.
2. In the sidebar, click **Settings** .
3. In the **Settings** toolbar, click **Integrations**.



4. Click **SYSLOG**.

5. Enable Syslog.

6. Enter the Syslog **Host** URL and port number.

7. Click **Use SSL secure connection**.

8. Click **Server certificate** > **Upload** and browse to the downloaded crt certificate file.

9. In Formatting:

- **Information format** - Select **CEF2**.
- **SIEM Token** - Paste the Cloud Syslog Source Token generated from Sumo Logic.

10. Click **Test**.

11. Click **Save**.

# 16. Configuring Proxy Settings for Agents

**Management:** Alhambra, Bahamas, Banff, Central Park, Denali, Eiffel, Fuji, Grand Canyon, Houston

**Agents:** Windows 2.0+ | Legacy 1.8.4+ | macOS 2.0+ | Linux 2.6+

For all SentinelOne Agent operating systems, you can route SentinelOne Agent -to-Management Console traffic through a web proxy server.

The configuration is different for each operating system.

## 16.1. Configuring a Proxy Server for Windows Agents

**Management:** Alhambra, Bahamas, Banff, Central Park, Denali, Eiffel, Fuji, Grand Canyon, Houston

**Agents:** Windows 2.0+

### Configure a Proxy Server:

- To connect to the Management. Communication between the Agent and the management is through the proxy.
- To connect to the SentinelOne IOC Cloud gateway. The Agent sends Deep Visibility data through the proxy.

With Windows Agent version 2.8, you can route Agent-to-Deep Visibility traffic through a proxy server, to the SentinelOne IOC gateway. This is the recommended configuration if you deploy the On-Prem Management.

### Choose a method to configure the proxy servers:

- If you explicitly define a proxy for Deep Visibility, you can configure it in the Management Console. You can apply this to all Agents, to all Agents of a Site, or to all Agents of a group.
- Install Agents with [Agent Installer Command Line Options](#).

Example of proxy configuration with a Windows installation flag and hostname:

```
C:\Users\user_name\Desktop>SentinelInstaller_3.1.5.63.exe /  
SITE_TOKEN=<string>/SERVER_PROXY=user,http://proxy.sentinelone.com:8080
```

- Use a [SentinelCTL command](#) to set the proxy mode on the endpoint.

To run sentinelctl on a Windows endpoint, run CMD as an administrator.

### Syntax

- The sentinelctl syntax to configure a proxy server to the management is:

```
sentinelctl config -p server.proxy -v {auto | none | system | http://  
{FQDN|IP}[:port] | user[,fallback_address[:port]]} -k "passphrase"
```

- The sentinelctl syntax to configure a proxy server to the Deep Visibility service is:

```
sentinelctl config -p agent.deepVisibility.proxy -v {auto | none | single | system | http://{FQDN|IP}[:port] | user[,fallback_address[:port]]} -k "passphrase"
```

- Example of proxy configuration using sentinelctl and an IP address:

```
sentinelctl config -p server.proxy -v user,http://192.0.2.1:8080
```

## Proxy Configuration Commands

Configure	SentinelInstaller	sentinelctl
Set the Management proxy server	/SERVER_PROXY	config -p server.proxy
Set Management proxy authentication	/SERVER_PROXY_CREDENTIALS	configure_proxy_credentials -m
Prevent a fallback to direct communication	/FORCE_PROXY	config -p communicatorConfig.forceProxy
Set the Deep Visibility proxy server	/IOC_PROXY	config -p agent.deepVisibility.proxy
Set authentication for the Deep Visibility proxy	/IOC_PROXY_CREDENTIALS	configure_proxy_credentials -d
Remove proxy settings		config -p server.proxy -v none

The configured Proxy Mode defines from where the Agent takes proxy information.

## Proxy Modes for Windows Agents

Proxy Mode	Description	Supported from
USER	Use a proxy address set by the active user. Optional: add a fallback proxy.	2.5 SP4, 2.6 EA2
custom	Use a static proxy address defined in the Agent configuration.	1.8.4
AUTO	Use proxy settings from the WPAD (Windows Proxy Auto Detect) service.	2.1
SYSTEM	Use the Windows System proxy, as defined by WinHTTP.	2.1
SINGLE	Use the same proxy server for management and for Deep Visibility connections (supports USER, AUTO, SYSTEM).	2.8
explicit	Use two proxy servers, one for management and one for Deep Visibility (supports USER, AUTO, SYSTEM).	2.8
direct	Do not use a proxy.	

See [Windows Agent Proxy Modes \[298\]](#) for details.

#### Examples of proxy configuration with the AUTO proxy mode:

##### To configure a Management proxy on Agent installation:

- Install Agents with the SERVER\_PROXY=auto and FORCE\_PROXY flags:

For example:

```
C:\Users\username\Desktop>SentinelInstaller_version.exe /  
SITE_TOKEN=<string>/SERVER_PROXY=auto /FORCE_PROXY
```

##### To configure proxies on an Agent after installation:

- Get the passphrase for an Agent.
- In a command line of the endpoint, go to the Agent directory:

```
> cd "C:\Program Files\SentinelOne\Sentinel Agent version"
```

- Run these commands:

```
> sentinelctl config -p server.proxy -v auto -k passphrase  
> sentinelctl config -p communicatorConfig.forceProxy -v true -k  
passphrase
```

- To use this proxy for Deep Visibility too:

```
> sentinelctl config -p ioc.proxy -v single -k passphrase
```

#### To configure a Deep Visibility proxy for multiple Agents from the Management Console:

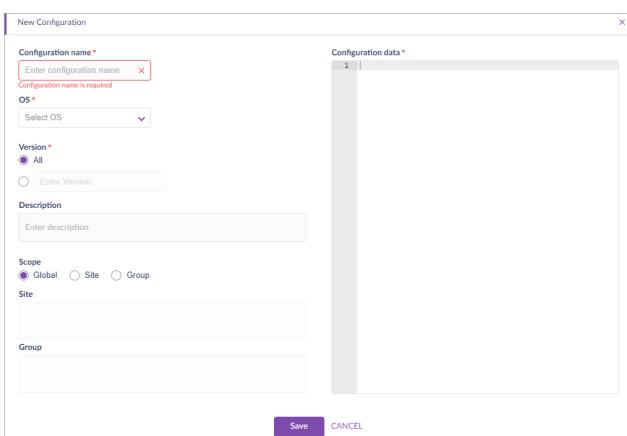
- In the sidebar, click **Settings** .

If the **Policy Override** tab is not visible, enable **Advanced Mode**.

- In the **Settings** toolbar, click **Policy Override**.



- Click **New Configuration**.



4. Enter values for the configuration properties.
5. In **Configuration data**, enter json to configure the Deep Visibility proxy server.

**Important:** All parts of the configuration that you do not enter in the window will be overwritten from the default configuration. Make sure to include all previous manual changes in the text you enter.

Syntax:

```
{
  "deepVisibility": {
    "proxy": "{single | auto | system | user,fallback[:port]} | http://{FQDN|IP}[:port]"
  }
}
```

Example:

```
{
  "deepVisibility": {
    "proxy": "user,http://172.16.0.12:8080"
  }
}
```

Note: Credentials cannot be set in **Policy Override**.

6. Click **Save**.

#### To revert to no proxy:

1. Get the Agent's passphrase.
2. In a command line of the endpoint, go to the Agent directory:

```
> cd "C:\Program Files\SentinelOne\Sentinel Agent version"
```

3. Run:

```
> sentinelctl config -p server.proxy -v none -k passphrase
```

If you run the command without a value to see the current value, it will show an empty string.

```
c:\Program Files\SentinelOne\Sentinel Agent 3.3.3.29>sentinelctl config
-p server.proxy
""
```

## 16.2. Windows Agent Proxy Modes

**Management:** Alhambra, Bahamas, Banff, Central Park, Denali, Eiffel, Fuji, Grand Canyon, Houston

**Agents:** Windows 2.0+

The configured Proxy Mode defines from where the Agent takes proxy information.

See also [Configuring a Proxy Server for Windows Agents \[295\]](#).

The Deep Visibility proxy adds only the value **single**, to use the same configuration as for a Management proxy. All other methods for proxy configuration are the same.

### **Proxy Modes:**

- Management Proxy Mode: AUTO [299]
- Management Proxy Mode: SYSTEM [299]
- Management Proxy Mode: CUSTOM [299]
- Management Proxy Mode: USER [299]
- Deep Visibility Proxy Mode: SINGLE [302]
- Deep Visibility Proxy Mode: EXPLICIT [302]
- Deep Visibility Proxy Mode: NONE [302]

### **Management Proxy Mode: AUTO**

Supported Agent versions: 2.1 GA+

1. Agents use the [Windows WPAD \(Windows Proxy Auto Detect\) service](#) to detect the proxy settings and connect through them.
2. If that fails, Agents try to connect directly to the Management Console, without a proxy.
3. If an Agent cannot connect, it will alternate between methods **a** and **b** until it succeeds.

### **Management Proxy Mode: SYSTEM**

Supported Agent versions: 2.1 GA+

- a. Agents use the Windows System proxy, as defined by [WinHTTP](#).
- b. If that fails, Agents try to connect directly to the Management Console, without a proxy.
- c. If an Agent cannot connect, it will alternate between methods **a** and **b** until it succeeds.

### **Management Proxy Mode: CUSTOM**

Supported Agent versions: 1.8.4+

- a. Agents try to connect to the defined URL.
- b. If the proxy address does not contain a valid proxy URL, or the Agent fails to communicate with the proxy, the Agent will try to communicate directly (without a proxy) with the Management.

### **Management Proxy Mode: USER**

Supported Agent versions: 2.5 SP4 GA+, 2.6 EA2+

- a. Agents use the proxy as set by the active user through the Windows control panel or Web browser (Internet Explorer, Edge, Chrome, Firefox).

- b. If connection through user proxy settings fails, Agents use the configured proxy address (`server.proxy`).

**Note:** If you use **Automatically detect settings**, and connection through the proxy settings fails, the Agent behavior follows the OS settings and tries to connect directly without a proxy. It does not use the server defined in `server.proxy`.

- c. If an Agent cannot connect, it will alternate between methods **a** and **b** until it succeeds.

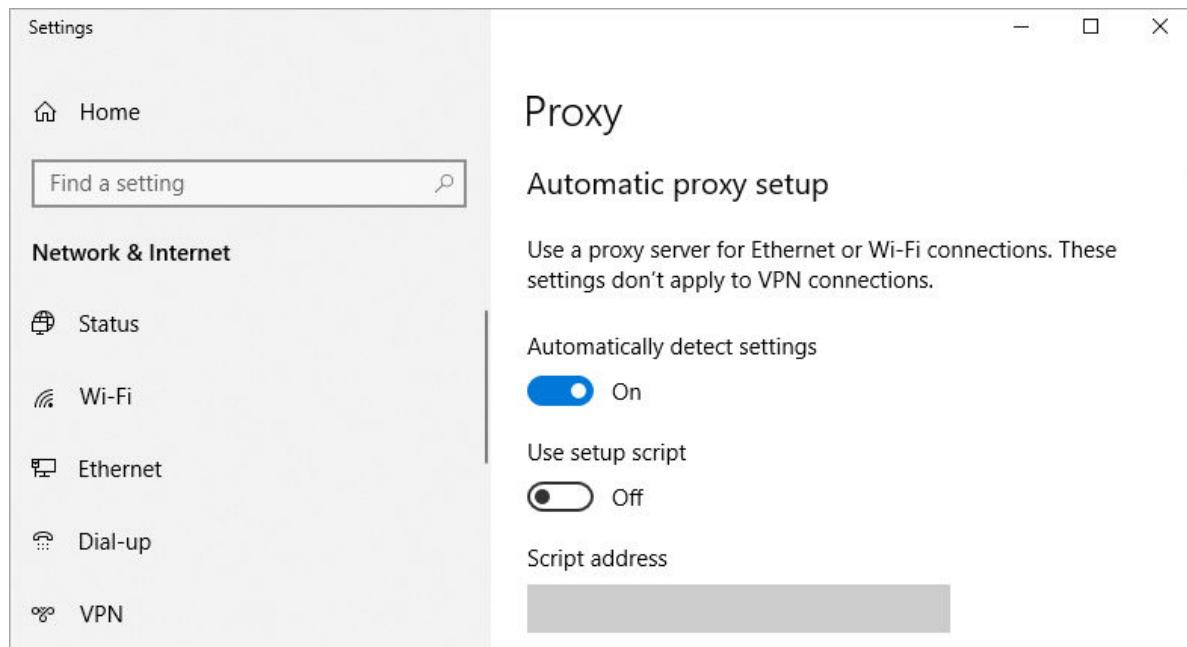
**Note:** You must log in through the local machine. If you log in through an RDP session, the Agent disconnects from the Management and will not access the proxy file.

#### Examples of User-Defined Proxy:

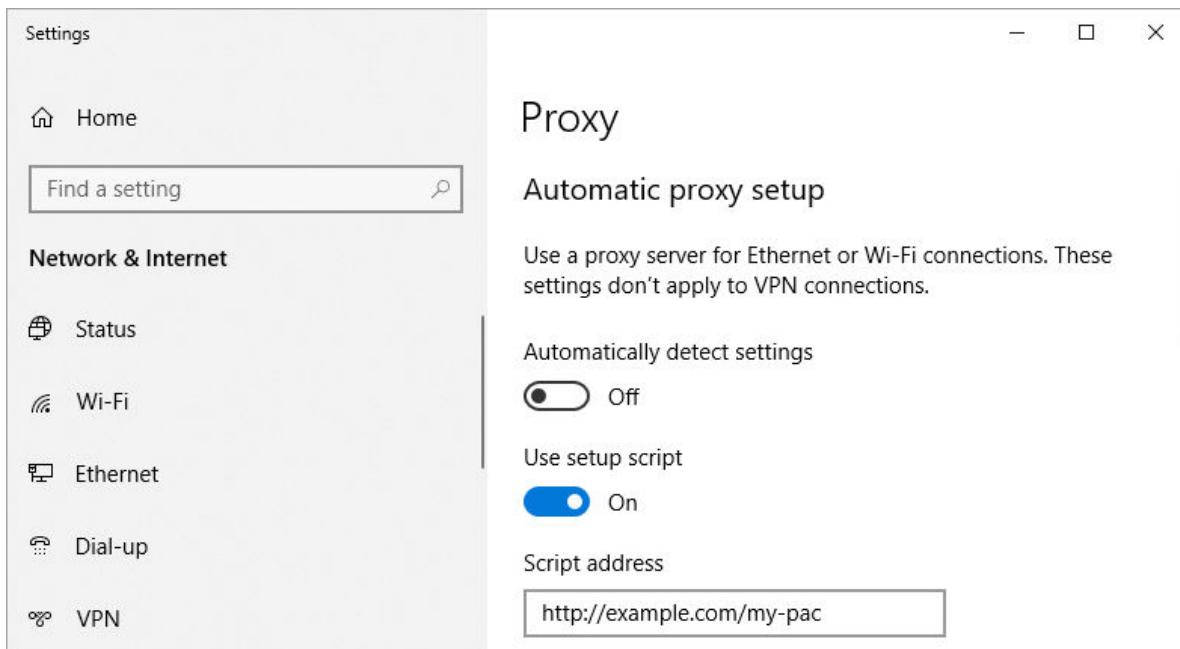
These examples are from **Windows Settings > Network & Internet > Proxy**. Similar settings are available from web browsers.

- In **Automatic proxy setup**, select **Automatically detect settings**. Windows attempts to automatically detect proxy settings with [Windows WPAD \(Windows Proxy Auto Detect\) service](#).

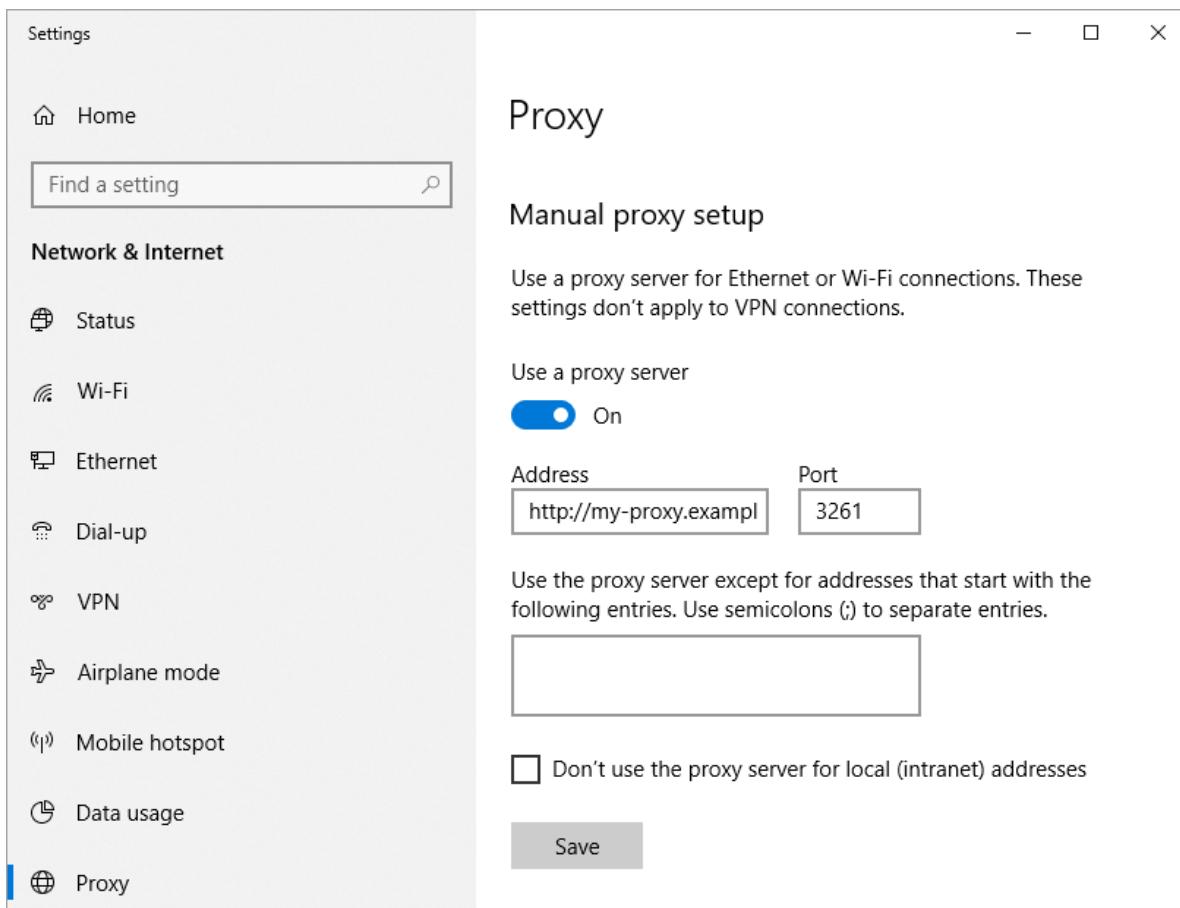
**Note:** If it fails, the Windows user settings allow connection without a proxy, and Agents will also use this OS setting.



- In **Automatic proxy setup**, select **Use setup script** and enter the address of a proxy settings PAC file. Windows uses the information in the PAC file.



- In **Manual proxy setup**, select **Use a proxy server** and enter the address and port.



- Notes on USER proxy mode:

- If more than one user proxy setting method is configured, Agents use the settings based on the priority defined by the operating system (**Automatically detect settings > Use setup script > Use a proxy server**).
- If the current user proxy settings are changed (for example, the current user changes them, or a user logs off and another user with different proxy settings logs on), but the Agent can still communicate with the management, communication continues and new user settings are not used.

### **Deep Visibility Proxy Mode: SINGLE**

Supported Agent versions: 2.8+

- Agents use one proxy (same mode, configuration, and behavior) to send Deep Visibility data to the SentinelOne service and to reach the management.
- This is the default mode for Deep Visibility proxy. If you send `sentinelctl config -p agent.deepVisibility.proxy` without a value, it is set to **SINGLE**.
- If the proxy configuration changes after the Agents start, the Agents apply the changes to reach both the management and the Deep Visibility service.

### **Deep Visibility Proxy Mode: EXPLICIT**

Supported Agent versions: 2.8+

- Agents use an explicitly defined proxy to send Deep Visibility data to the SentinelOne service.
- This mode is set with the proxy URL (not a keyword). It accepts an optional port number.
- The `sentinelctl` command **configure\_proxy\_credentials** sets the username and password for the proxy to the Deep Visibility service. Credentials are saved in the Windows Credential Manager.

### **Deep Visibility Proxy Mode: NONE**

Supported Agent versions: 2.8+

- Agents do not use a proxy to send Deep Visibility data to the SentinelOne service.
- Use this keyword to override a different setting. An empty value is not equal to "none". Empty means default, which is "single".

## **16.3. Configuring a Proxy for macOS Agents**

**Management:** Alhambra, Bahamas, Banff, Central Park, Denali, Eiffel, Fuji, Grand Canyon, Houston

**Agents:** macOS 2.0+

#### **Configure a Proxy Server:**

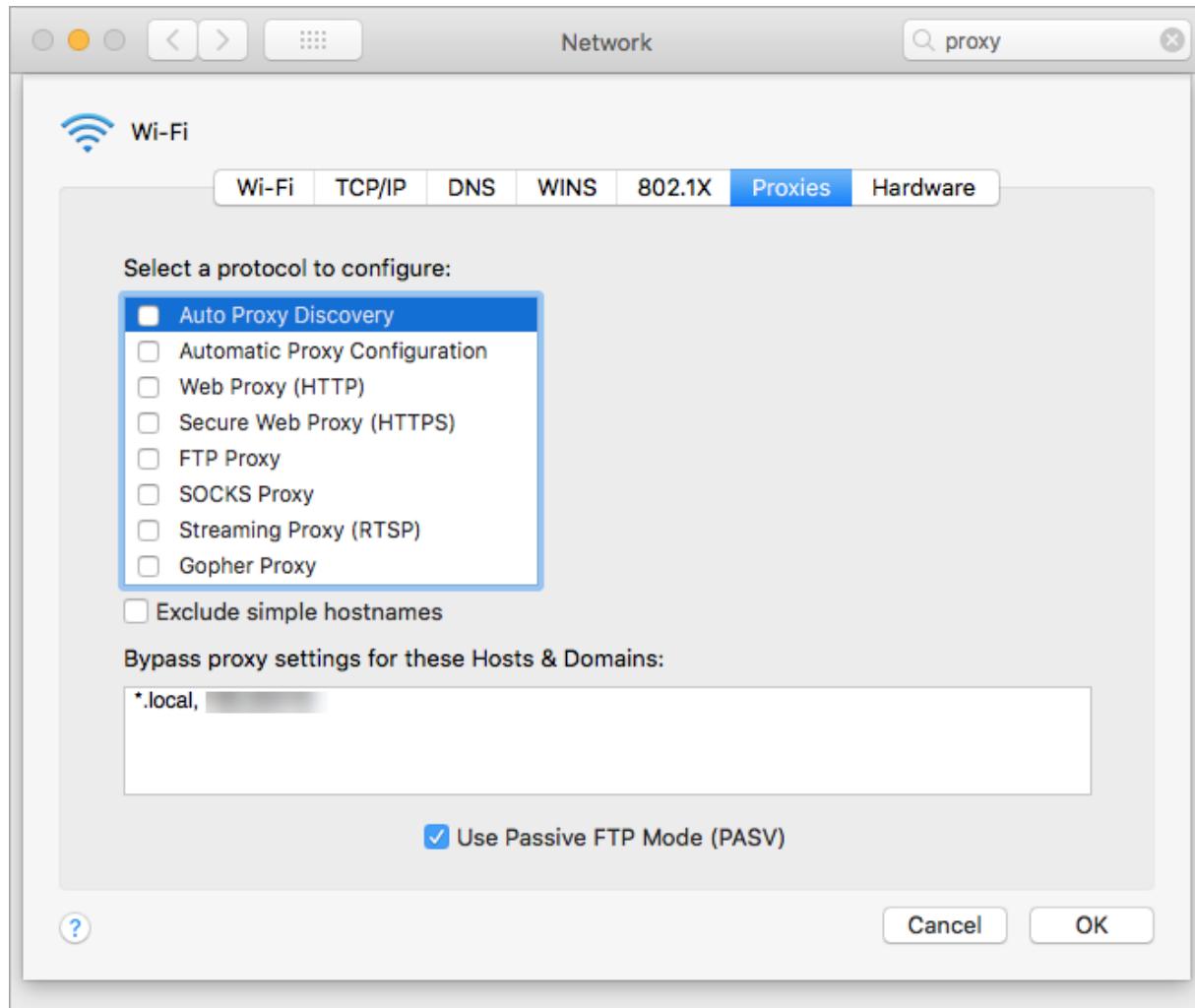
- To connect to the Management. Communication between the Agent and the management is through the proxy.

- To connect to the SentinelOne IOC Cloud gateway. The Agent sends Deep Visibility data through the proxy.

SentinelOne Agents automatically use the proxy server settings configured for each endpoint in the macOS system settings.

For more details, see the macOS documentation for the endpoint version.

#### *Proxy settings on macOS Sierra*



## 16.4. Configuring a Proxy Server for Linux Agents

**Management:** Banff, Central Park, Denali, Eiffel, Fuji, Grand Canyon, Houston

**Agents:** Linux 2.6.x, 3.0

You can route SentinelOne Agent-to-Management Console traffic through a web proxy server.

### Proxy Command for Agent version 3.0

Purpose	Get, set, or clear the proxy settings between the Agent and the Management. If you enter a username and password, the proxy is authenticated. To connect to an unauthenticated proxy, do not enter credentials.
---------	---

Synopsis	<code>sentinelctl management proxy {clear   get   set {http   https   socks5}://[user:password@]proxy-address:port}</code>
clear	Remove the proxy configuration.
get	See the configured proxy.
set protocol [user:password] address:port	Configure a proxy with an optional username and password (for authenticated proxy), IP address or FQDN of the proxy server, and its access port.
Example	<pre>\$ sudo /opt/sentinelone/bin/sentinelctl management proxy set https:// usr1:password@192.0.2.5:443</pre>

### Linux BSX Proxy Flag for Agent version 2.6.x

Purpose	Install the Linux Agent with a proxy configured.
Synopsis	<code>SentinelAgent-2.6.version-Linux.bsx -p "address:port"</code>
-p, --proxy	Flag for the IP address or FQDN of the proxy server and its access port. There is one space between the flag and the value, which is surrounded by quotes.
Notes	Only unauthenticated proxy configuration is supported.
Example	<pre>SentinelAgent-2.6.0.1386-Linux.bsx -p "https://192.0.2.5:80" -- SentinelAgent-2.6.0.1386-Linux.bsx --proxy "myproxy.ourdomain.com:8080"</pre>

## 17. Advanced Mode [Multi-Site]

**Management:** Central Park, Denali, Eiffel, Fuji, Grand Canyon, Houston

**Agents:** Windows 2.6+ | macOS 2.6+ | Linux 2.6+

**Minimum Admin Scope:** Account Admin

**Scope:** Account or Global

Advanced mode lets SentinelOne Technical Support or knowledgeable administrators run advanced operations. This mode gives powerful options that must be used correctly and with caution.

[Management Console: How to Enable and Use Advanced Mode video \(2.5 minutes\)](#)

### To enter Advanced mode:

1. In the sidebar, click **Settings** .

**Configuration** opens.



2. Enable **Advanced Mode**.

#### Management Login

Session Timeout 

10080

Two-Factor Authentication 



Advanced Mode 

Management URL

[https://\[REDACTED\].sentinelone.local](https://[REDACTED].sentinelone.local)

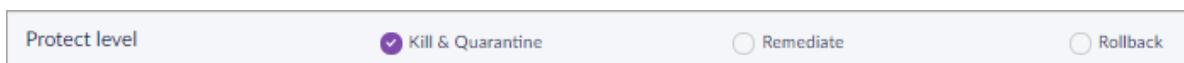
3. In the sidebar, click **Network** .

4. In the **Network** toolbar, click **Policy**.



### Advanced Mode Options

- **Policy > Protect Level.**



By default, when you set a policy to **Protect**, the Agents run Kill and Quarantine automatically. In Advanced Mode, you can change automatic mitigation to include **Remediate** or **Remediate and Rollback**.

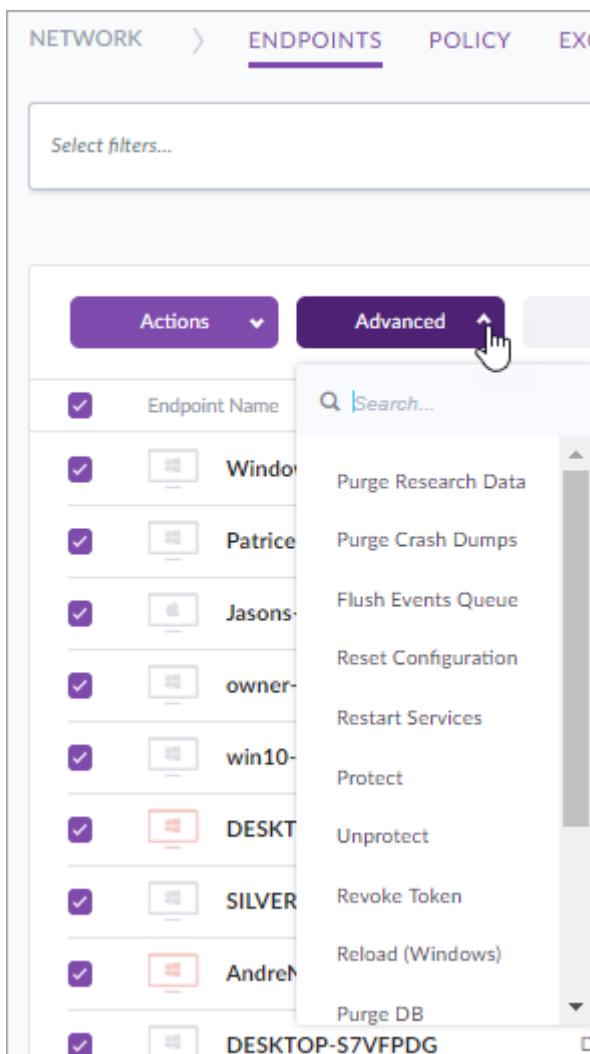
- **Policy > Detect Interactive Threat** engine. This is part of the Behavioral AI and focuses on insider threats (for example, an authenticated user runs malicious actions from a CMD or PowerShell command line). This engine detects malicious commands in interactive sessions.

**Detect Interactive Threat** is disabled by default. If you want to protect your endpoints from malicious commands that are entered in a CLI, enable this engine. But, if you enable this engine for endpoints of active users of CLIs, you may expect a number of false positives. (Windows only)

- **Settings > Policy Override**. Send a policy override to a Group, Site, or all Agents.

New Configuration			
Name	OS Type	Agent Version	Scope Type
Configuration 1	Windows	2.6.1.5901	Group (Default Group)

- **Network view > Advanced**.



## 17.1. Advanced Mode Network Options

Option	Description
Purge Research Data	After SentinelOne Research experts resolve your issue, you can clean the heavy logs from your Management.
Purge Crash Dumps	After SentinelOne Technical Support resolves your issue, they might recommend that you clean the heavy logs from your Management.
Flush Events Queue	Delete all notifications waiting to be sent. SentinelOne Technical Support might recommend this action if you set too many alerts to SMS, if you change the Syslog server, if Support actions handled notifications and they are no longer relevant, or other.
Reset Configuration	Change the configuration of the selected Agents to the default policy.
Restart Services	Restart the Agent services.
Mark As Up To Date	Mark this endpoint <b>Up To Date</b> if the Agent version running on the endpoint is the latest, but this endpoint is shown on the Dashboard as <b>Out of date</b> . This issue might occur if Agents that were sent a new version did not yet report Management.
Protect	If an Unprotect command was used, this configures the selected Agents to block configuration changes and uninstallation.
Unprotect	Forces the Agent to allow configuration changes.
Revoke Token	Forces the Agent token to expire, which causes the Agent to register again and get a new configuration immediately.
Reload (Windows)	Reloads the selected modules of the selected Agents: <b>Static</b> , <b>Log</b> , <b>Agent</b> , or <b>Monitor</b>
Purge DB	Do not use this without SentinelOne Technical Support! This is a debug command that can corrupt the database.
Control Crash Dumps	When you want to troubleshoot the Agent with SentinelOne Technical Support: In the window that opens, control if the selected Agents upload ( <b>Send</b> ) crash dumps to your instance in the Cloud, delete the dumps without upload (default), or if the Agents send crash dumps for a given number of seconds ( <b>Expiration</b> ).
Control Research Data	When you want to SentinelOne expert investigation on specific detections: In the window that opens, control if the selected Agents upload ( <b>Send</b> ) verbose detection data to your instance in the Cloud, delete data that you uploaded before, or upload data for a given number of seconds ( <b>Expiration</b> ).
Event Throttling	When SentinelOne Technical Support requires a clean, lite environment to troubleshoot an issue, they may recommend that you turn on this option for a limited time. In the window that opens, control if the selected Agents send events (threat alerts, on-access, system trace) to the Management, if they stop events (they still send Keep-Alive), or if they stop for a given number of seconds ( <b>Expiration</b> ).
Configuration	Edit the JSON configuration of the Agent. <b>Important:</b> Do not do this without SentinelOne Technical Support! Changes are applied on the next keep alive message.

## 17.2. Agent Configuration Hierarchy [Multi-Site]

**Management:** Central Park, Denali, Eiffel, Fuji, Grand Canyon, Houston

**Agents:** Windows 2.7+ | macOS 2.7+

**Minimum Admin Scope:** Account Admin

**Scope:** Selected Site, Account, or Global

From Central Park and 2.7 Agents, an improved, clear hierarchy determines how Windows and macOS Agents are configured.

The hierarchy for Agent configuration settings, from the highest priority is:

### For Windows Agents:

1. Configuration changed locally on an endpoint with sentinelctl commands, or changed in the Agent configuration file in Advanced Mode from **Network > Advanced > Configuration**.

LocalConfig.json

2. Configuration changed in Advanced Mode from **Settings > Policy Override**.

Group policy overrides have priority over Site policy overrides, and Site policy overrides have priority over Global policy overrides.

MgmtOverride.json

3. Agent Configuration settings in the policy.

Policy.json

4. Default or CLI configurations included in the installer package.

InstallationConfig.json

### For macOS Agents:

1. Configuration changed in Advanced Mode from **Settings > Policy Override**.

Group policy overrides have priority over Site policy overrides, and Site policy overrides have priority over Global policy overrides.

2. Configuration changed locally on an endpoint with sentinelctl commands, or changed in the Agent configuration file in Advanced Mode from **Network > Advanced > Configuration**.

3. Agent Configuration settings in the policy.

4. Default or CLI configurations included in the installer package.

## 17.3. Advanced: Changing Agent Configuration Manually [Multi-Site]

**Management:** Central Park, Denali, Eiffel, Fuji, Grand Canyon, Houston

**Agents:** Windows 2.6+ | macOS 2.6+

**Minimum Admin Scope:** Account Admin

**Scope:** Selected Site, Account, or Global

You can change the configuration settings for one or more selected Agents from the Network view.

The configuration changes require Global Admin permissions (or Support) and Advanced Mode enabled.

**Important:** Change configuration with caution and with guidance from SentinelOne Support.

See [Advanced: Changing Agent Configuration with Policy Override \[Multi-Site\] \[311\]](#) for 2.7 and higher Agents to change the configuration for a whole group, Site, or Globally.

**Note:** When you upgrade Agents, they will get manual configuration changes when they connect to the Management, after the upgrade.

### To change the configuration for one or more Agents:

1. In the Management Console, click **Network**.

If the **Advanced** button is not visible, enable [Advanced Mode \[305\]](#).

2. Select one endpoint.

**Best Practice:** Select only one endpoint to see the configuration of the Agent.

If you select multiple endpoints, the full configuration does not show.

3. Click **Advanced** and select **Configuration**.

The screenshot shows the 'ENDPOINTS' section of the SentinelOne web interface. In the 'Actions' dropdown menu, the 'Configuration' option is selected, indicated by a hand cursor icon over the button.

The configuration opens.

**Best Practice:** Copy the configuration of the Agent and save it in a backup text file.

4. Click **Edit**.
5. In **Configuration data**, enter the configuration lines to be changed.

- To change an independent line, write the line in curly brackets. For example:

```
{
  "keepAliveFailCount": 3,
  "keepAliveInterval": 3
}
```

- To change a dependent parameter, you must include the headline that it depends on and put the dependent parameters in additional curly brackets. For example:

```
{"communicatorConfig": {"forceProxy": true/false, "telemetry": true/false }}
```

**Important:** All parts of the configuration that you do not enter in the window will be overwritten from the default configuration. Make sure to include all previous manual changes in the text you enter.

**Best Practice:** Keep a record in your organization of all manual configuration changes made to Agents.

6. Click **Submit**.
7. Optional: Repeat the steps on more endpoints.

To remove configuration overrides, send a blank configuration with just curly brackets {} as the configuration. It will override the current configuration with the default configuration.

## 17.4. Advanced: Changing Agent Configuration with Policy Override [Multi-Site]

**Management:** Central Park, Denali, Eiffel, Fuji, Grand Canyon, Houston

**Agents:** Windows 2.7 | macOS 2.7

**Minimum Admin Scope:** Global Admin (Account Admin capability coming soon)

**Scope:** Selected Site, Account, or Global

**Watch:** [How to use Policy Override](#).

In Advanced Mode, you can use *Policy Override* In the Management Console, to override a default setting in the Agent configuration or policy. You can send a policy override to a group, to a Site, or to *Global*.

The configuration changes require 2.7 or later Agents and Global Admin permissions (or Support).

To change the configuration for one or more selected Agents and not a whole group, see: [Advanced: Changing Agent Configuration Manually \[Multi-Site\] \[308\]](#)

Starting from version 3.0 Agents with Fuji management, you can define a policy override entry to apply to all versions, OR to a specific version and build.

Each policy override entry shows in the Policy Override page. Click an entry to edit it.

Policy Overrides			
Name	OS Type	Agent Version	Scope Type
Configuration 1	Windows	2.6.1.5901	Group (Default Group)

**Note:** Policy overrides are defined for a specific build number OR for ALL Agents (from 3.0 Agents with Fuji). When you upgrade or add Agents with a different build number, duplicate each policy override entry that is for a specific version, or change the entry to apply to all Agents.

**Important:**

- Change configuration with caution and with guidance from SentinelOne Support.
- Each Agent can apply only ONE policy override entry.

- Each entry can contain multiple configuration changes, and you can add more configuration changes to an existing entry.
- Agents apply the entry with the narrowest scope and version that matches them.
  - If you have a policy override configuration entry for a specific Agent version, Agents with that version do NOT apply changes from a different entry that is for ALL versions.
  - If you have an entry for the Global scope and an entry for a Group scope, Agents in the Group apply the Group entry and NOT the Global entry.

## To configure Policy Override for a group, Site, or all Agents:

1. In the sidebar, click **Settings** .
2. If the **Policy Override** tab is not visible, enable **Advanced Mode**.
3. Plan the configuration changes.

**Important:** All parts of the configuration that you do not enter in the window will be overwritten from the other configuration sources. Make sure to include all previous manual changes in the text you will enter.

**Best Practice:** See the configuration of an Agent before you change it and save it in a backup text file:

- a. In **Network**, select an Agent and click **Advanced > Configuration**.
  - b. Copy the configuration to a text file and save it.
4. In the **Settings** toolbar, click **Policy Override**.



5. Click **New Configuration**.

6. Enter values for the configuration properties.

## New Configuration Values

Field	Description
Configuration name	Name of the policy override as an asset.
OS	Select the OS of the Agent configuration to change.
Version	Enter the version number of the Agent, in the format 2.X.X.XXXX. Or select All.
Description	Free text. Describe briefly what the change is and the reason.
scope	<b>Global</b> - This will change all Agents. <b>Site</b> - Enter the name of a Site. You can override the policy of the Agents of only one Site for each new configuration. When you begin to enter the name, Site names show as objects to select. You must select a Site name. <b>Group</b> - Enter and select a Site name. Then enter and select a Group name. Group policy overrides have priority over Site policy overrides, and Site policy overrides have priority over Global policy overrides.

7. In **Configuration data**, enter the configuration lines to be changed.

- To change an independent line, write the line in curly brackets. For example:

```
{
  "keepAliveFailCount": 3,
  "keepAliveInterval": 3
}
```

- To change a dependent parameter, you must include the headline that it depends on and put the dependent parameters in additional curly brackets. For example:

```
{"communicatorConfig": {"forceProxy": true/false, "telemetry": true/false }}
```

8. Click **Save**.

### To remove a policy override:

- In the sidebar, click **Settings** .
- In the **Settings** toolbar, click **Policy Override**.



- Select a configuration item.
- Click **Delete Selection**.

## To duplicate a policy override for Agents of a different version:

In 2.7 - 2.9 Agents, policy overrides are defined for a specific build number, in the format 2.7.X.XXXX. When these Agents are upgraded, or new Agents of a different version are added to the environment, you must configure the policy override for a new Agent **Version**.

When a package with a new Agent is added to your Management Console:

1. In the sidebar, click **Settings** .
2. In the **Settings** toolbar, click **Policy Override**.



3. Open an existing configuration from the table.
4. Copy the Configuration data and click **Cancel**.
5. Create a **New Configuration** for the new Agent version, or for **All** versions.
6. Paste in the copied configuration data.
7. Click **Save**.
8. Repeat for each existing configuration.

## 17.5. Advanced: Enabling SHA 256 Hash Information for Threats [Multi-Site]

**Management:** Central Park, Denali, Eiffel, Fuji, Grand Canyon, Houston

**Agents:** Windows 2.7+

**Minimum Admin Scope:** Account Admin

**Scope:** Selected Site, Account, or Global

Starting with Central Park SP4, the SHA 256 hash can show for each threat in the analysis page of the Management Console and in the API. This works on 2.7 and higher Windows Agents and is disabled by default.

The screenshot shows two threat entries in a table. Each entry includes the threat type (H), the SHA1 hash (f99e41b19cae9b623c95794589ffcd9cea1ba689), the SHA256 hash (866afe0e926e73e965febe3f05883ffaf3e1bdbcc9b63ac28aa2e11479327c5e), and links to Google and VirusTotal for further investigation.

[H]	SHA1: f99e41b19cae9b623c95794589ffcd9cea1ba689	<a href="#">Google</a>	<a href="#">VirusTotal</a>
[H]	SHA256: 866afe0e926e73e965febe3f05883ffaf3e1bdbcc9b63ac28aa2e11479327c5e	<a href="#">Google</a>	<a href="#">VirusTotal</a>

### Details

- The SHA 256 hash is only an informative field in threat forensics information, to allow queries for the threat in third-party databases. It is not supported in Exclusions, Blacklist, or searches in the Analyze page.
- SHA 256 hash information does not show for active content.

- Limitation: SHA 256 hash information does not show when a threat runs through a script (for example, Python or Batch). This will be resolved in later releases.

## To enable SHA 256 in the Console:

1. Make sure **Advanced Mode** is on.
  - For one or more selected Agents: Configure in **Network > Advanced > Configuration**.
  - For a Site, Group, or Global: Configure in **Settings > Policy Override**.
2. Find `mgmtReportedHashes`.

Get Configuration

Rans-win10X64 Updated: August 11th 2019 17:33:37

```
{
  "penetration": "local",
  "remoteShell": "local",
  "preExecution": "local",
  "lateralMovement": "local",
  "preExecutionSuspicious": "local"
},
"experimentalConfig": {
  "detectMaliciousBrowserSpawn": true
},
"filterSystemEvents": true,
"fullDiskScanConfig": {
  "shouldScanExtensions": false
},
"keepAliveFailCount": 8,
"maxCountCrashdumps": 10,
"mgmtReportedHashes": 1,
"remoteGroupTimeout": 300,
"remoteRpcRelinking": true,
"researchDataConfig": {
  "maxFiles": 100,
  "sendTimeout": 3600000,
  "eventsPerLog": 65536,
  "staticScansPerLog": 128,
  "staticCollectEnable": true,
  "staticCollectThreshold": 0.5
},
"safeBootProtection": true,
"allowUnsignedAssets": false,
"apcGetAtomProtected": false,
"maxNotificationSize": 10485760,
"preventMaliciousRdp": true
}
```

**Edit**

### Valid Values:

- 1 - SHA 1 only
  - 3 - SHA 1 and SHA 256
3. To change the value, click **Edit**.
  4. In the window that opens, enter this line to enable SHA 256:

```
{ "mgmtReportedHashes": 3 }
```

5. Click **Submit**.
6. Restart the endpoints.

### To enable SHA 256 in sentinelctl:

1. Run CMD as Administrator and enter these commands:

```
> cd "c:\Program Files\SentinelOne\Sentinel Agent version"
> sentinelctl config -p mgmtReportedHashes -v 3 -k "passphrase"
```

2. Restart the endpoints.

## 17.6. Advanced: Agent Migration between Management Consoles

**Management:** Fuji, Grand Canyon, Houston

**Agents:** Windows 3.0+ | macOS 3.0+

**Minimum Admin Scope:** Global Admin

**Scope:** Selected Site, Account, or Global

From Windows Agent version 2.9, and macOS Agent version 3.0, you can move Agents between different Management Console instances. For example, to move Agents from a POC Management Console to a paid Management Console.

### Specifications

- You must be a Global Admin of the Agent's old Site and a Site Admin for the new Site.
- When you run the operation, you enter the Site Token for the new Site.
- An Agent will try to connect to the new Management Console for 3 minutes. If the Agent cannot connect, it stays in the original Management Console.
- Local configuration files are kept with the Agent. New management assets take affect after the next keep alive communication with the new Management Console.
- Resolve all threats on Agents before you migrate them.
- The management will NOT migrate these endpoints:
  - Endpoints that do not meet the requirements to support migration (unsupported version or OS).
  - Endpoint with unresolved threats.

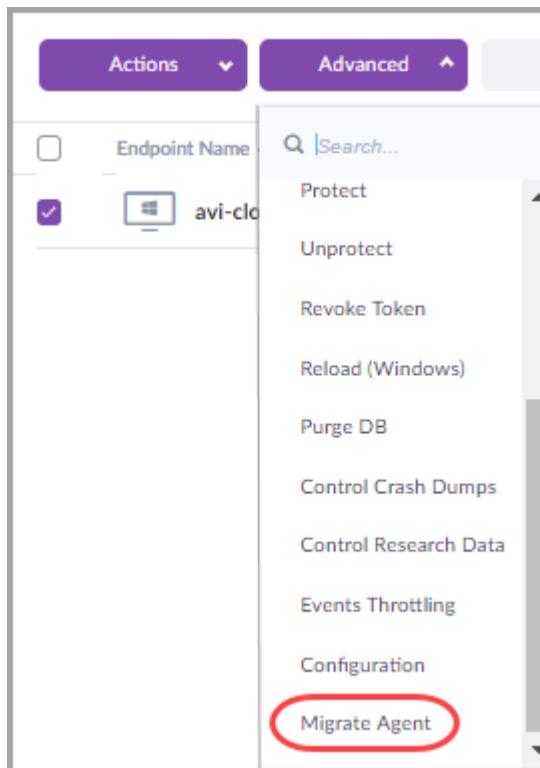
### To migrate an Agent:

1. In a Management Console with Advanced mode enabled, go to **Network > Endpoints**.
2. Select endpoints.

From the Management Console, you can select one or more endpoints for the action, or you can select all of a Group or filter set. You cannot select all endpoints shown if they are not in a Group or filter set.

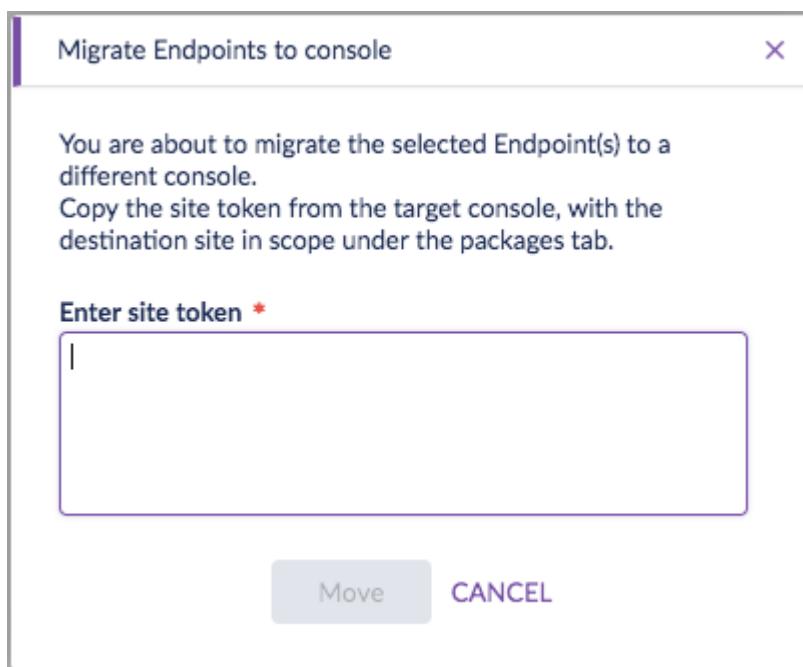
If you select an endpoint that cannot be migrated, the endpoint is skipped, but the operation still runs on supported endpoints.

3. Click **Advanced** and select **Migrate Agent**.



4. A window opens with instructions. Copy the Site token for the target Site from the **Network > Packages** page and paste it in the window.

You must be in the Site scope to see the Site Token.



5. Click **Move**.
6. Select **Approve** and click **OK**.

**To see Agent migration status in the Network view:**

In Network > Endpoints, use the filters or the columns to see the **Console Migration Status** of endpoints.

- In the Network filters scroll right to see the **Console Migration Status**.

The screenshot shows a table of endpoint data. The columns include: Status, Has local config, Disk encryption, Pending uninstall, Architecture, and Console migration status. The 'Console migration status' column has a red box drawn around it. The values in this column are: N/A, Failed, Pending, and Migrated. A mouse cursor is visible at the bottom right of the table area.

- Expand **Columns** to select the **Console Migration Status** column, or to make sure it is selected.

The screenshot shows a 'Columns' dropdown menu with a search bar and a list of items. The items are: MAC Address, Management Conne, Network Status, Update Status, Scan Status, IP Addresses, Pending Uninstall, Disk Encryption, and Console Migration S. The 'Console Migration S' item has a red box drawn around it, and a mouse cursor is pointing at it. A 'Reset' button is at the bottom of the list.

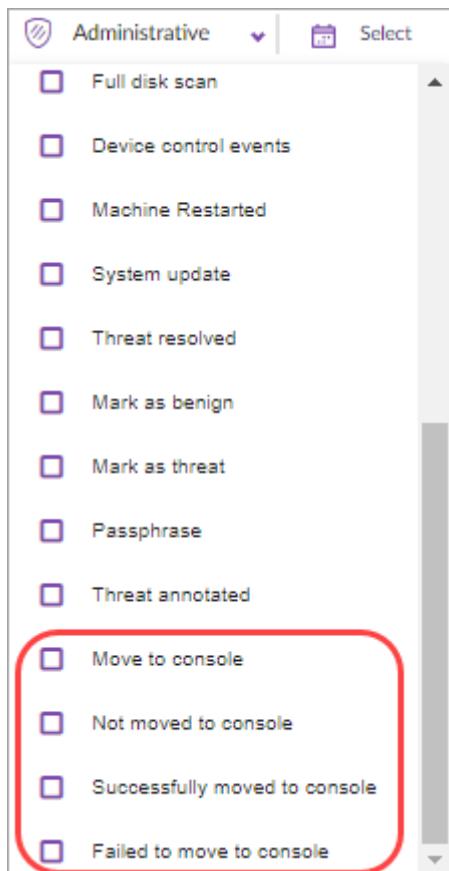
If necessary, scroll right in the Endpoints page to see the column.

- The potential value are:
  - **N/A** - No migration command was sent.

- **Pending** - The Agent is trying to migrate. After a maximum of four minutes, the status will change to **Migrated** or **Failed**.
- **Migrated** - The Agent moved successfully to the new Management Console. It shows as **Offline** in the original Management Console.
- **Failed** - The Agent failed to move and stays in the original Management Console.

### To see Agent migration activities in the Activity log:

You can filter for these activities in the Activity log:



- **Move to console** - A **Migrate Agent** command was sent to an endpoint.
- **Not moved to console** - A **Migrate Agent** command was sent to an endpoint, but it does not meet the requirements to support migration (unsupported version or OS).
- **Successfully moved to console** - An endpoint successfully migrated to a different Management Console.
- **Failed to move to console** - An endpoint failed to migrate to a different Management Console.

## 18. Device Control

**Management:** Eiffel, Fuji, Grand Canyon, Houston

**Agents:** Windows 2.8+ | macOS 2.7+

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

Device Control lets you control which external devices are allowed to be used with endpoints in your organization. Use Device Control to:

- Block external devices that are not required from connecting your Endpoints, to limit data leaks.
- Strictly control allowed devices to prevent malicious content that can enter your network through external devices and Bluetooth connections.

Watch: [Device Control Demo](#)

Device Control policy can be Global, for a Site, or for a Group. Groups and Sites can inherit policies or have their own.

Define the policy in the Management Console in **Network > Device Control**.

From Management Console version Eiffel, you can manage external USB devices with Windows and macOS Agents. From Management Console version Grand Canyon, you can also manage Bluetooth devices. This is supported with Windows and macOS Agents version 3.2 and higher.

Rules for Bluetooth are supported on Windows 10 and Windows Server 2012, 2016, and 2019.

The USB **Allow Read Only** feature is available with Management version Houston for Windows and macOS Agents version 3.4 and higher.



### IMPORTANT

**Important Recommendations for Device Control with Bluetooth:** If you plan to have one or more active Device Control rules with Bluetooth, we highly recommend that all Windows Agents in the Site are upgraded to version 3.1.3 or higher. In Windows Agents below that version, Bluetooth rules might unexpectedly impact rules for USB interface.

If you cannot upgrade all Agents to version 3.1.3 or higher, we recommend that you make a dynamic group for Agents that support Bluetooth , version 3.2.0 and higher, and make a separate Device Control policy with Bluetooth rules for that Group only.

The Device Control Policy includes Settings and Rules:

- **Settings [321]:** Turn Device Control on or off, define the inheritance settings, and select the **Activity** log settings. Define some settings for Bluetooth devices.
- Rules: [Create \[325\]](#) and [organize \[323\]](#) rules to allow or block connection of specific devices, or groups of devices, to endpoints, based on the device identifiers.

## 18.1. Device Control Settings

**Management:** Eiffel, Fuji, Grand Canyon, Houston

**Agents:** Windows 2.8+ | macOS 2.7+

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

In the Device Control settings, define the policy inheritance, turn Device Control on or off, and select which device events are reported to the Activity log. The same settings apply to Windows and macOS endpoints.

There are some settings for Bluetooth that only apply to Windows Agents. Device Control with Bluetooth is supported with management version Grand Canyon for Windows and macOS Agents version 3.2 and higher.

The **USB Allow Read Only** feature is available with Management version Houston for Windows and macOS Agents version 3.4 and higher.

By default, Device Control is disabled at the Global and Site level. When it is first enabled, all Sites and Groups inherit the Firewall Control policy from the Global or Site policy.

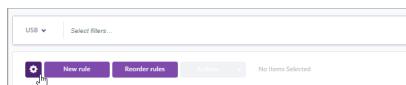
By default, Agents have Device Control disabled, until they connect to a Site or Group with an enabled Device Control policy.

### To configure Device Control settings:

1. In the sidebar, click **Scope**  and select a scope.
2. In the sidebar, click **Network** .
3. In the **Network** toolbar, click **Device Control**.

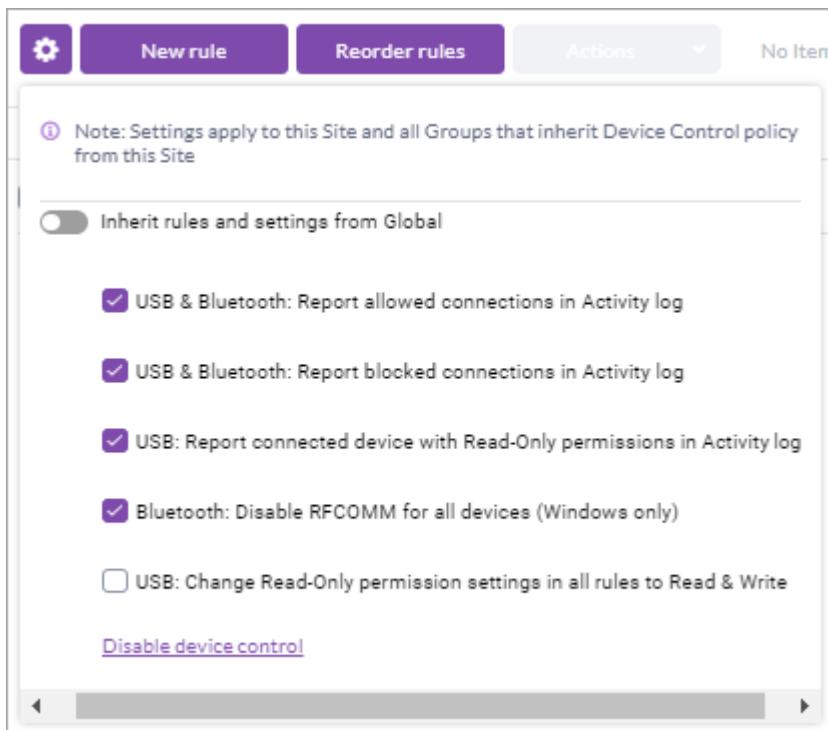


4. Click the Settings icon.



5. Click **Enable** Device Control, if it is not enabled.
6. For an Account, Site or Group: Use the toggle to turn the inheritance On or Off.

**Note:** If inheritance is On, the other settings are disabled because they are inherited. If you turn Off inheritance, the other settings become enabled.



7. Select which device events are reported to the Activity log:
    - **USB & Bluetooth: Report allowed connections in Activity log** - Creates logs when devices are connected and disconnected.
    - **USB & Bluetooth: Report blocked connections in Activity log** - Creates a log when a device is blocked.
    - **USB: Report connected device with Read-Only permissions in Activity log** - Creates a log event when a device with read-only permissions is connected.

This option is available from Management version Houston.
  8. **Bluetooth: Disable RFCOMM for all devices (Windows only)** - Use this setting to disable or enable the RFComm profile. Bluetooth RFComm can be blocked or allowed only for **ALL** Bluetooth devices. It cannot be blocked or allowed for specific devices.
  - Note:** Device Control rules that block or allow Bluetooth devices do not impact the RFComm functionality.
  9. **USB: Change Read-Only permission settings in all rules to Read & Write** - Use this setting to change the behavior of all read-only rules to allow both read and write. This setting is useful if read-only permission settings are causing issues with your system. The actual definition of the read-only rules do not change.
  - This option is available from Management version Houston.
  10. Optional: You can click **Disable Device Control**. This disables the feature for your current scope and all Sites and Groups that inherit Device Control settings from this scope.
- For a Site or Group, you must turn Off inheritance before you can disable Device Control.
- Existing rules remain in the policy but become inactive. When you enable Device Control again, the rules will become active with their latest **Enabled** or **Disabled** state

### Device Control Policy Inheritance:

- To make a Site inherit rules and settings from Global:

Turn On **Inherits rules and settings from Global** (on by default).

- The Site uses the Global settings and the Global rules.
- You can add Site rules.

- To give a Site its own policy:

Turn Off **Inherits rules and settings from Global**.

- The Site uses the settings that you configure.
  - The Site uses only Site rules.
- To make a Group inherit rules and settings from a Site that inherits from the Global settings (the Site has inheritance turned on):

Turn On **Inherits rules and settings from Global** (on by default).

- The Group uses Global settings, and Global and Site rules.
  - You can add Group rules.
- To make a Group inherit rules and settings from a Site that has its own policy (the Site has inheritance turned off):

Turn On **Inherits rules and settings from Site** (on by default).

- The Group uses the Site settings and the Site rules.
  - You can add Group rules.
- To give a Group its own policy:

Turn Off **Inherits rules and settings from Site**.

- The group uses the settings you configure.
- The Group uses only Group rules.

## 18.2. Device Control Rules and Rule Order

**Management:** Eiffel, Fuji, Grand Canyon, Houston

**Agents:** Windows 2.8+ | macOS 2.7+

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

Watch: [Introduction to Device Control Rules](#)

Device Control rules let you allow or block specific devices, or groups of devices, that connect to endpoints, based on device identifiers. When the Management sends policy information to Agents, it includes these rules.

When an external device connects to an endpoint, the SentinelOne Agent checks if it is allowed to run by the Device Control policy. The 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.

- If the matched rule has the **Block** Action, the Agent prevents the device from being used.
- If the matched rule has the **Allow** Action, the device can be used.

See [Creating and Editing Device Control Rules \[325\]](#) for the full list of Rule attributes.

#### The Agent applies the rules in this order:

1. Group rules from first to last.
2. Site rules from first to last.
3. Global rules from first to last.

New rules are added to the top of the relevant section of the Device Control policy.

The rules that apply to your current scope show in **Network > Device Control**. To see Site or Group rules, make sure you are in that scope.

A screenshot of the Device Control interface. The top navigation bar shows 'Bluetooth' and 'Select filters...'. Below the navigation are three buttons: 'New rule', 'Reorder rules', and 'No items Selected'. A status bar indicates '2 Rules' and '10 Results'. The main table has columns: Interface, Rule Name, Class, Bluetooth Minor Class, Bluetooth Version, Vendor ID, and Product ID. Two rows are listed: one for 'Bluetooth Minimum Bluetooth version Any Any 4.0 Any Any' and another for 'Bluetooth Peripheral Devices Peripheral (mouse, joystick, keyboard, ... Any Any Any)'.

From Grand Canyon, select the rule set that shows: **USB** or **Bluetooth**. The order of rules for one interface does not affect the other interface.

A screenshot of the Device Control interface. The top navigation bar shows 'USB' and 'Select filters...'. Below the navigation are three buttons: 'New rule', 'Reorder rules', and 'No items Selected'. A status bar indicates '2 Rules' and '10 Results'. The main table has columns: Rule Name, Class, and Vendor ID. One row is listed: 'USB'.

Click **Select filters** to filter the rules by rule attributes. Select the attributes to filter for or use the free text search.

A screenshot of the Device Control interface. The top navigation bar shows 'Bluetooth' and 'Select filters...'. Below the navigation are three buttons: 'New rule', 'Reorder rules', and 'No items Selected'. A status bar indicates '2 Rules' and '10 Results'. The main table has columns: Free text search, Scope, Status, Action, Device class, Vendor ID, Product ID, and Version. One row is listed: 'Site' (Scope), 'Enabled' (Status), 'Allow' (Action), 'Peripheral (mouse, joystick, keyboard, ...)' (Device class), '4.0' (Version). The 'Free text search' field contains 'Type your search...'.

#### To change the order of the rules:

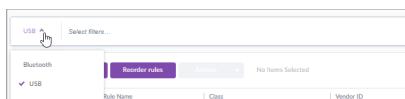
You can change the order of rules in your Admin scope. Account and Site Admins can change the order of rules for the Sites and Groups in their scope.

1. In the sidebar, click **Scope** and select a scope.

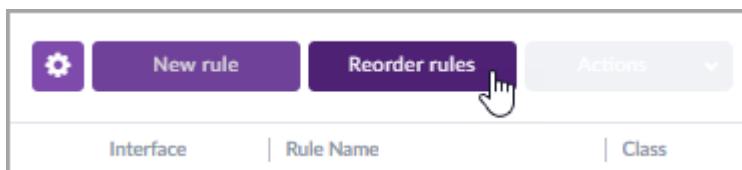
2. In the sidebar, click **Network** .
3. In the **Network** toolbar, click **Device Control**.



4. Select a rule set: **USB** or **Bluetooth** rules.



5. Click **Reorder rules**.



6. In the window that opens, drag and drop rules, or in the **Order** column, click the number of the rule and enter a new number.

Devices rules reordering									
Order	Interface	Rule Name	Class	Vendor ID	Product ID	Serial ID	Scope	Action	Status
1	USB	Allow Printer rule	Printer	Any	Any	Any	Site	Allow	Disabled
2	USB	Block Video rule	Video	Any	Any	Any	Site	Block	Disabled

7. Click **Save**.

### 18.3. Creating and Editing Device Control Rules

**Management:** Eiffel, Fuji, Grand Canyon, Houston

**Agents:** Windows 2.8+ | macOS 2.7+

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

Watch: [Creating Device Control Rules](#)

Create and edit rules for a specific scope to allow or block devices, based on device identifiers.

When you create a rule, it applies to the current scope of the **Network** view.

**Note:**

On Windows, if a USB device is already connected to an endpoint, new rules and rule changes do not affect it. Rules will apply the next time the device connects to the endpoint.

On macOS, changes apply to devices that are already connected to an endpoint.

Device Control with Bluetooth is supported with management version Grand Canyon for Windows and macOS Agents version 3.2 and higher.

The USB **Allow Read Only** feature is available with Management version Houston for Windows and macOS Agents version 3.4 and higher.

### Notes on Rules for Bluetooth

- Rules for the Bluetooth interface are based on Bluetooth device attributes
- On Windows, Bluetooth RFCOMM can be blocked or allowed only for **ALL** Bluetooth devices. It cannot be blocked or allowed for specific devices. For example, if you block a device but allow RFCOMM profile, connections from that device that use the RFCOMM profile will be allowed.
- On Windows, explicit rules for Bluetooth LE (Low Energy) devices based on Hardware attributes or Device version are not supported. You can Block all LE devices from connecting to endpoints by setting a rule to block all devices with Interface, **Bluetooth**.
- For Windows Bluetooth rules to take effect, 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.

### Device Control Rule Attributes for all Rules

Column	Description	Values
Interface	Physical interface to which the rule applies.	USB or Bluetooth
Rule Name	A descriptive name.	Free text, up to 50 characters. Must be unique within the scope.
scope	The scope for which the rule applies.	Group, Site, Account, or Global.
Action	Defines if Agents Block or Allow use of devices that match the rule parameters.	Allow* Block
Status	State of the rule.	Enabled - Active (if Device Control is enabled). Disabled - Not active.

\* From Management version Houston, the **Interface** is **USB**, **Allow** is replaced with the options **Allow Read & Write** and **Allow Read Only**.

### Device Control Rule Attributes per Interface

Column	Description	Interface	Values
Class	Device Class as defined by the Interface standard ( <a href="#">USB Device Class</a> or <a href="#">Bluetooth Major Device Class</a> ).	USB* Bluetooth	Class selected from the list, or <b>Any</b> if not defined.
Minor Class	Minor Device Class, as defined by the Interface standard ( <a href="#">Bluetooth Minor Device Class</a> ).	Bluetooth	First select a <b>Class</b> , then select a Minor class from the list.

Column	Description	Interface	Values
Vendor ID	Vendor Identifier.	USB Bluetooth	Free text for relevant devices or <b>Any</b> if not defined.
Product ID	Product Identifier, unique for a specific product module, per vendor ID, and Interface.	USB Bluetooth	Free text for relevant devices or <b>Any</b> if not defined.
Serial ID	Unique identifier of some physical USB devices.	USB	Free text for relevant devices or <b>Any</b> if not defined. Supported for USB mass storage devices only (support for all Device Classes will be added in future releases). N/A for other devices.
Bluetooth version	Select to define a Bluetooth rule by a Bluetooth standard version (which is also the Bluetooth LMP version).	Bluetooth	Select a version. For <b>Allow</b> rules, that version and higher are allowed. For <b>Block</b> rules, that version and lower are blocked.

\* If you select a class that applies to the whole device, the whole device is blocked. If you select a class that only applies to one interface of a device, the other interfaces will still be available.

**Note:** If the IDs of a device change, for example, due to a firmware upgrade, rules that were defined for the previous IDs will not work. Create new rules for the new IDs, or create rules based on Class.

### To create a rule:

1. In the sidebar, click **Scope**  and select a scope.
2. In the sidebar, click **Network** .
3. In the **Network** toolbar, click **Device Control**.



4. Click **New rule**.

It does not matter which rule set shows: **USB** or **Bluetooth**. You can make new rules for either interface.



5. In the window that opens, enter the details of the rule:

The screenshot shows a 'New Rule' dialog box with the following fields:

- Rule name:** An empty text input field.
- Interface:** A dropdown menu set to 'Select interface'.
- Rule Type:** A dropdown menu set to 'Select rule type'.
- Scope:** Set to 'All Sites'.
- Action:** Two radio buttons: 'Allow' (selected) and 'Block'.

At the bottom are two buttons: 'Continue' (in a purple box) and 'Cancel'.

- **Rule name** - Enter a descriptive name for the rule. The rule name must be different from other rule names in the scope.

**Best Practice:** Include the reason for the rule in the name.

- **Interface** - Select the type of device to which the rule applies.
- **Rule Type** - Select the criteria for the rule.
- **scope** - This is taken automatically from the current scope of the **Network** view.

If you want to give the rule a different scope, click **Cancel** and select a different scope in **Network**. Or you can [move the rule \[333\]](#) to a different scope later on.

- **Action** - Select **Allow** or **Block** to define if Agents block or allow use of devices that match the rule parameters.

From Management version Houston, when the **Interface** is **USB**, **Allow** is replaced with the options **Allow Read & Write** and **Allow Read Only**.

- Select **Allow Read & Write** to allow USB devices to connect to endpoints.
- Select **Allow Read Only** to allow mass storage devices access to connect to endpoints with read permissions, but block them from writing data.

**Note:** If you are upgrading to Houston, all previous rules set to **Allow** are automatically set to **Allow Read & Write** because **Allow** includes writing permissions.

New Rule

Rule name: Read Only

Interface: USB

Rule Type: Class

Scope: Global -> AAA

Action:

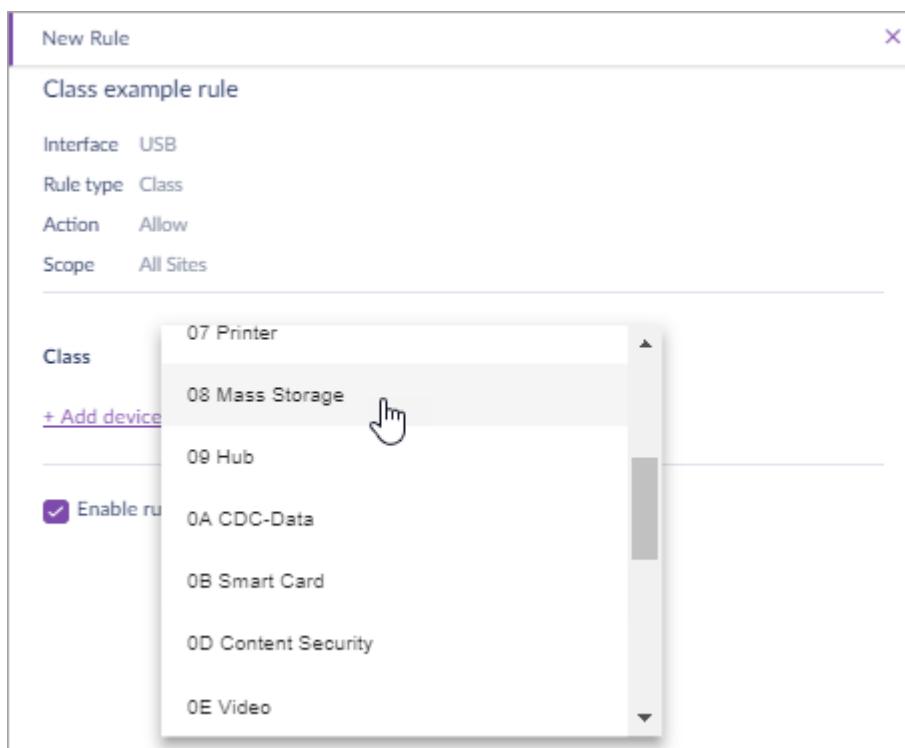
- Allow Read & Write
- Allow Read Only
- Block

Continue

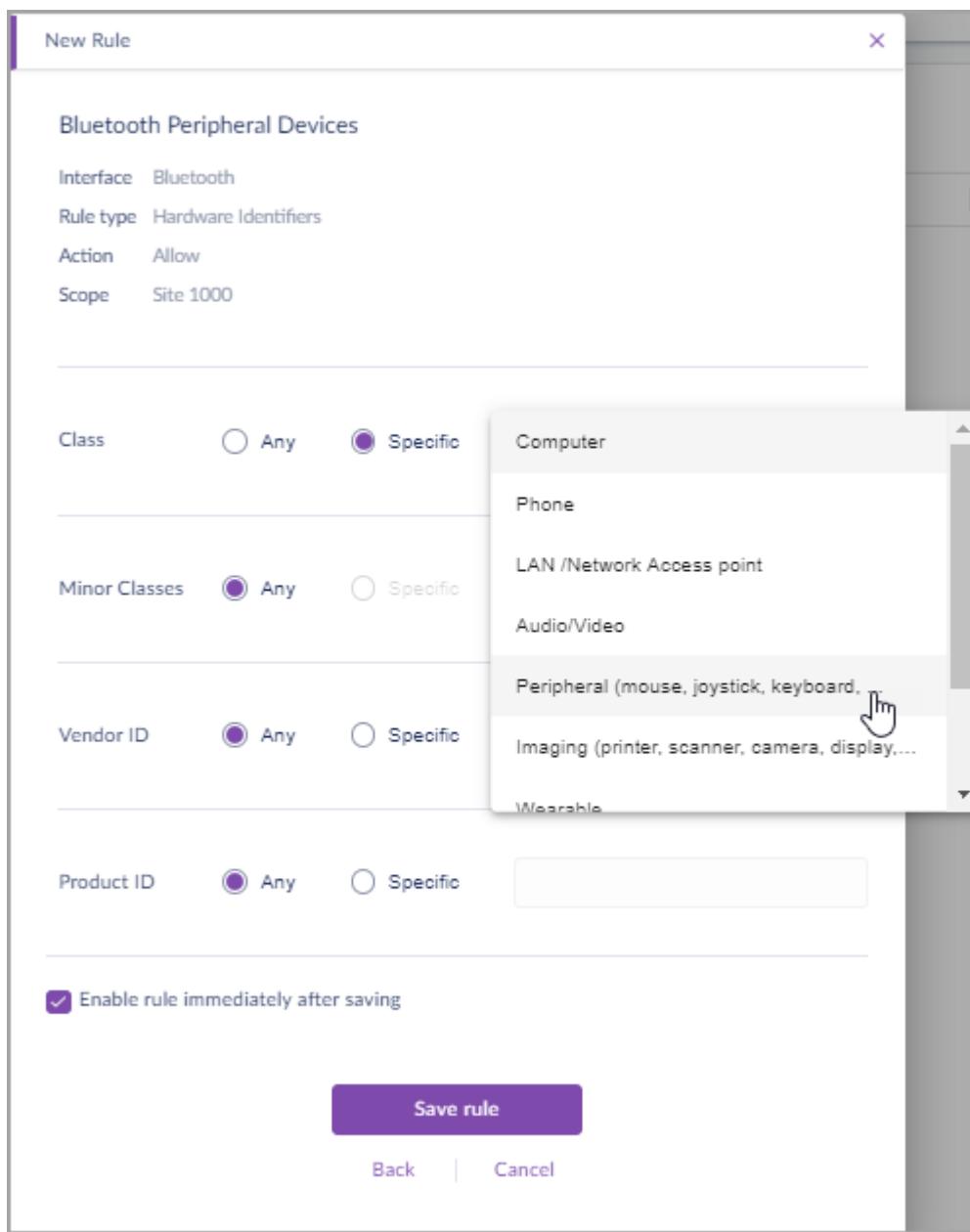
Cancel

6. Click **Continue**.
7. In the window that opens, define the specifics of the device identifiers.

For example, if you selected **USB Interface**, and **Class** as the Rule Type, select the class, such as Video or Mass Storage.



If you selected **Bluetooth** Interface and Hardware Identifiers, click **Specific** and define one of the identifiers.



8. Optional: If relevant, add more specific identifiers. If you add more identifiers, the rule only applies if all identifiers match a device.

Identifiers that are not explicitly defined are set to the default value, which is **Any**.

9. **Enable rule immediately after saving** is selected by default. This means that the rule becomes active immediately.

To create the rule in **Disabled** state, deselect this.

10. Click **Save rule**.

### To enable or disable a rule:

If a rule is **Disabled**, it is never active but shows in the policy with the **Disabled** Status.

If a rule is **Enabled**, it is active if Device Control is enabled. If Device Control is disabled for the rule's scope, the rule keeps the Status **Enabled** but is not active. It will become active automatically if Device Control is enabled.

1. In the sidebar, click **Network** .
2. In the **Network** toolbar, click **Device Control**.



- Select a rule and click **Actions**.

 New rule	 Reorder rules	 Actions	1 Item selected
Interface	Rule Name	Class	
 USB	Allow Printer rule	Printer	

- Or click on a rule.

 New rule	 Reorder rules	 Actions
Interface	Rule Name	
<input type="checkbox"/>  USB	Glob200	

In the **Rule Details** window, click **Options**.

3. Click **Enable or Disable**.

## To edit a rule:

**Note:** When you edit a rule, you cannot change the Rule Type or Interface.

1. In the sidebar, click **Network** .
2. In the **Network** toolbar, click **Device Control**.



3. Click a rule.
4. In the **Rule Details** window, click **Edit**.

Rule Details

USB device rule ▪ by Class

Options ▾

Scope	Site
Name	Allow Printer Rule
Action	Allow
Class	07h, Printer
<a href="#">+Add Vendor ID</a>	

Added by Default on October 09, 2018  
Last edited on October 09, 2018

● Rule is Active



5. Make changes in the **Rule Details**.

Rule Details

USB device rule ▪ by Class

Scope	site 2000 (site 2000)
Name*	Allow Printer rule
Action	<input checked="" type="radio"/> Allow <input type="radio"/> Block
Class	Printer
<a href="#">+ Add device vendor ID</a>	

Added by Default on October 09, 2018  
Last edited on October 09, 2018

● Rule is Active

**Save changes**

[Discard](#)

6. Click **Save changes**.

## 18.4. Moving and Copying Device Control Rules

**Management:** Eiffel, Fuji, Grand Canyon, Houston

**Agents:** Windows 2.8+ | macOS 2.7+

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

Watch: [Copying and Moving Device Control Rules](#)

You can *copy* a Device Control rule to use it in multiple Sites or groups. For example:

- You have a rule for Site A: Copy it to use it in all of Site B, or copy it to one Group of Site B.
- You have a rule in Group X, which is in Site A: Copy it to two other Groups in Site A.

You can *move* Device Control rules to change their scope. For example:

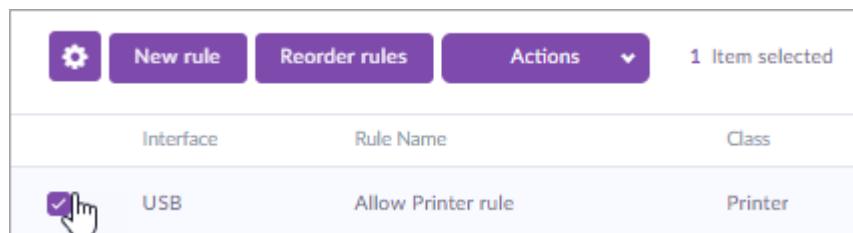
- You made a Group rule for one Group and want to change it to be a Site rule.
- You made a rule for Site A and want it to apply to Site B instead.

**To move Device Control rules between Sites or groups:**

1. In the sidebar, click **Scope**  and select a scope.
2. In the sidebar, click **Network** .
3. In the **Network** toolbar, click **Device Control**.

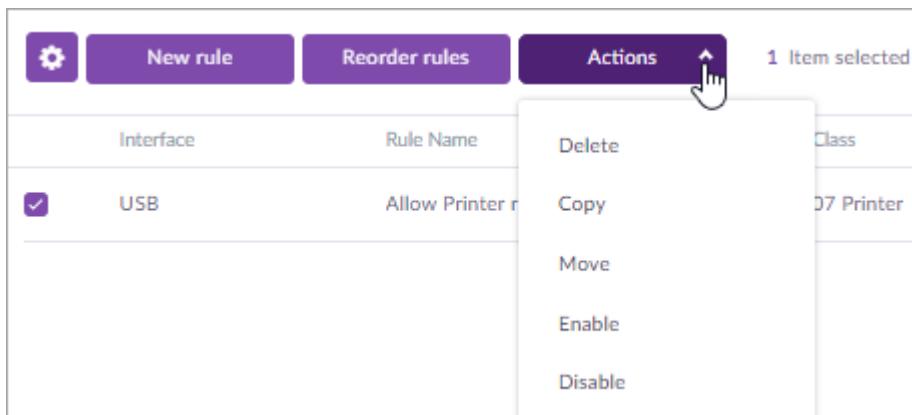


4. Select a rule or multiple rules.



Interface	Rule Name	Class
 USB	Allow Printer rule	Printer

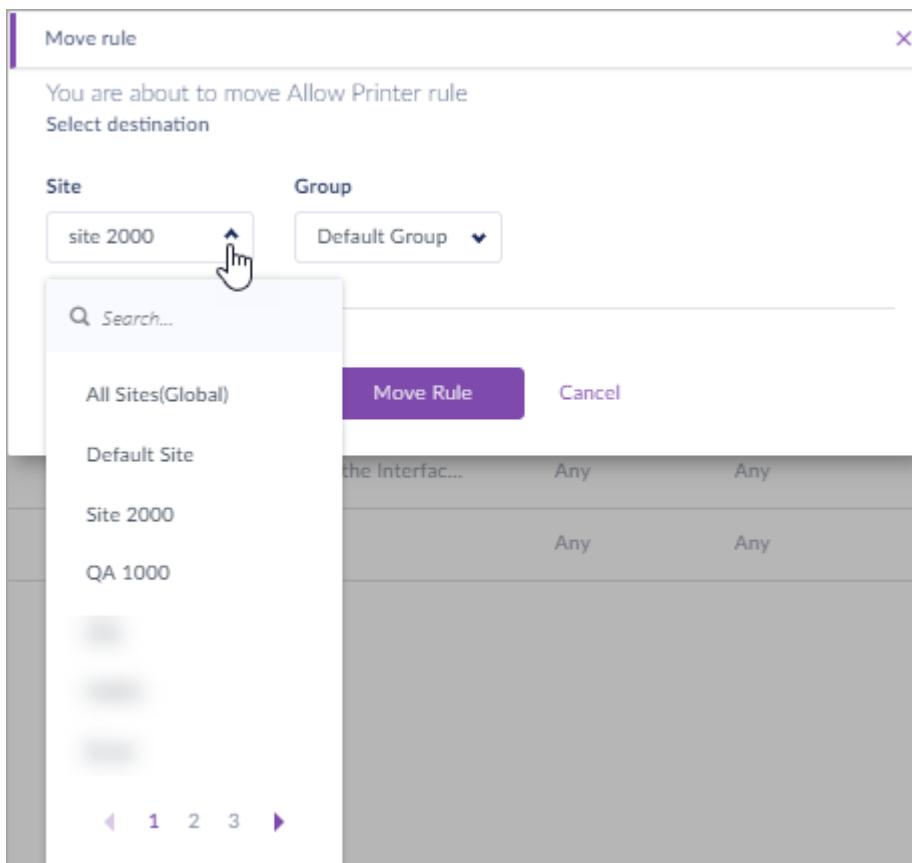
5. Click **Actions** and select **Move**.



A screenshot of the SentinelOne interface showing a list of rules. A context menu is open over a row for a rule named "Allow Printer". The menu includes options: Delete, Copy, Move, Enable, and Disable. A hand cursor is pointing at the "Move" option.

Interface	Rule Name	Actions
USB	Allow Printer	Delete Copy Move Enable Disable

6. Select the destination for the rule.



7. Click **Move**.

### To copy Device Control rules:

- In the sidebar, click **Scope**  and select a scope.
- In the sidebar, click **Network** .
- In the **Network** toolbar, click **Device Control**.



4. Select a rule or multiple rules.

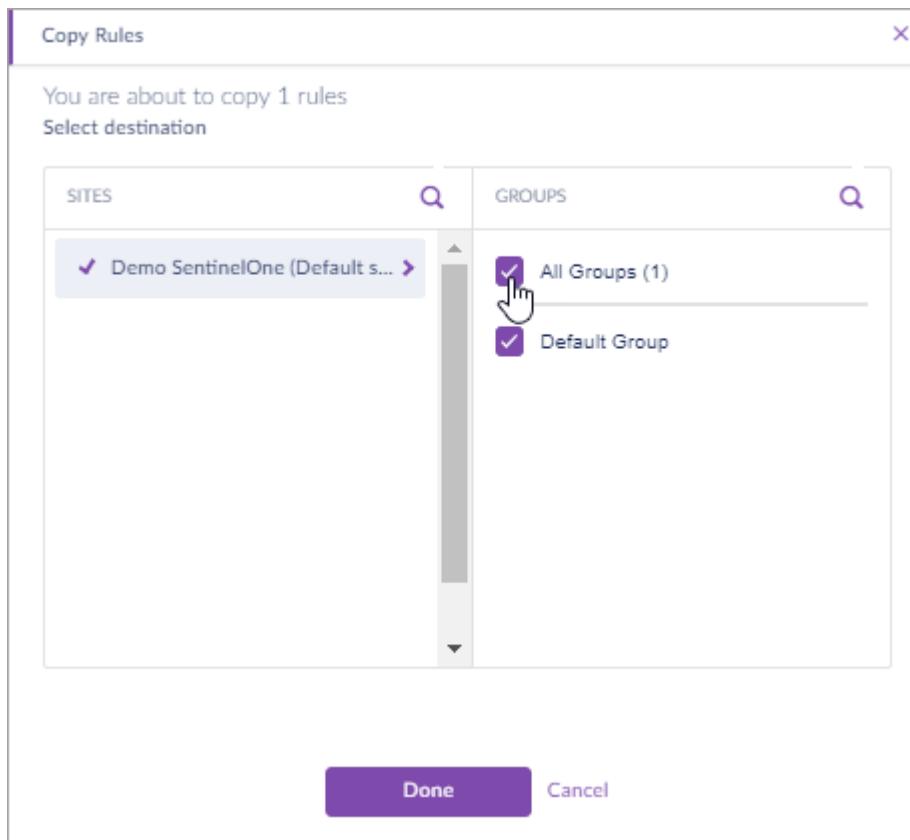
	New rule	Reorder rules	Actions	1 Item selected
Interface	Rule Name	Class		
<input checked="" type="checkbox"/>	USB	Allow Printer rule	Printer	

5. Click **Actions** and select **Copy**.

	New rule	Reorder rules	Actions	1 Item selected
Interface	Rule Name			
<input checked="" type="checkbox"/> USB	Allow Printer r			
			Delete	Class
			Copy	07 Printer
			Move	
			Enable	
			Disable	

6. In the **Copy Rules** window:

- a. In the **SITES** column, select a Site.
- b. In the **GROUPS** column, select **All Groups**, or one or more specific groups.



7. Click **Done**.

## 18.5. Seeing Device Control Activity Logs

**Management:** Eiffel, Fuji, Grand Canyon, Houston

**Agents:** Windows 2.8+ | macOS 2.7+

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

See all Device Control logs in the **Activity** view. The results shown are based on your current scope.

- Changes to rules and settings show under **Operations > Device Control**.
- Blocked, Connected, and Disconnected device events show under **Administrative > Device Control events**.
  - Connected and Disconnected device events show if **Report approved device events to activity log** is selected in the Device Control settings.
  - Blocked device events show if **Report blocked device events to activity log** is selected in the Device Control settings.

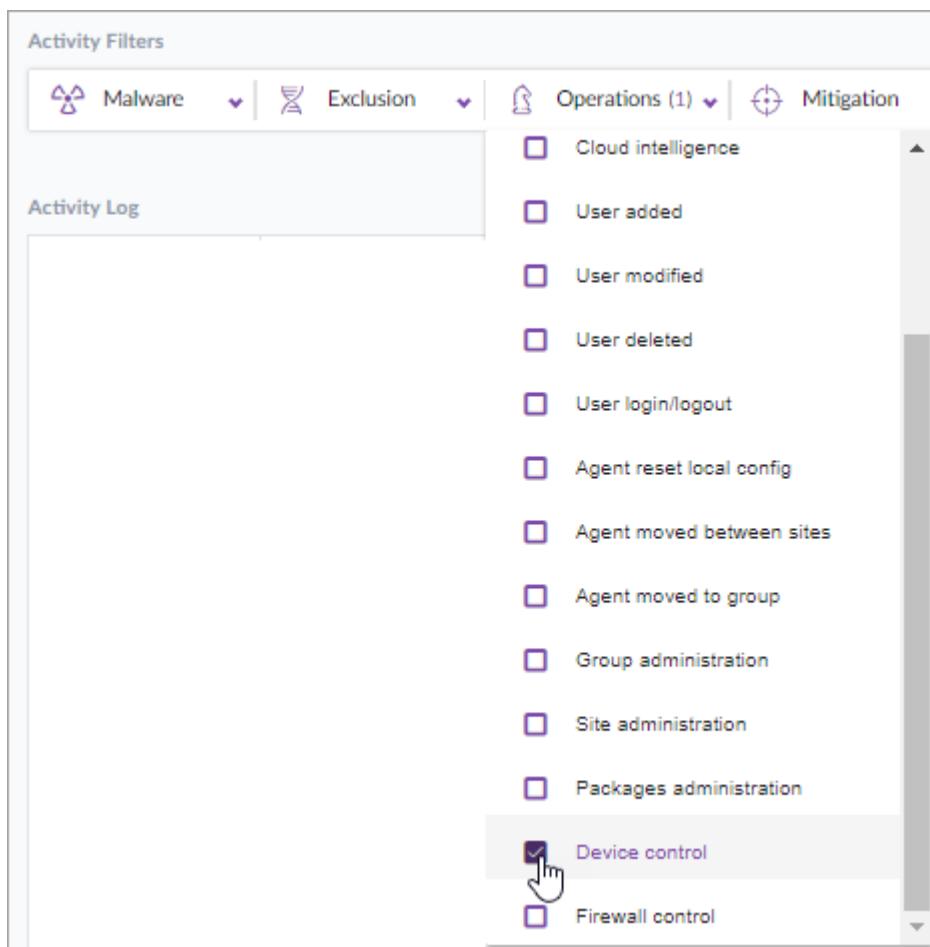
If necessary, you can [create a new rule from a blocked device event \[339\]](#) to allow a device.

- Move the cursor over a Blocked, Connected, or Disconnected device event to open the **Event Details**, which contains:

- A summary of the event.
- The date and time of the event.
- The endpoint name and logged in user.
- All of the device identifier details: Class, Interface, Vendor ID, Product ID, Serial ID (if relevant), Device Name.

## To see changes to Device Control rules and settings:

1. In the sidebar, click **Scope**  and select a scope.
2. In the sidebar, click **Activity** .
3. In **Operations**, click the down arrow to open the options.
4. Scroll down and select **Device Control**.

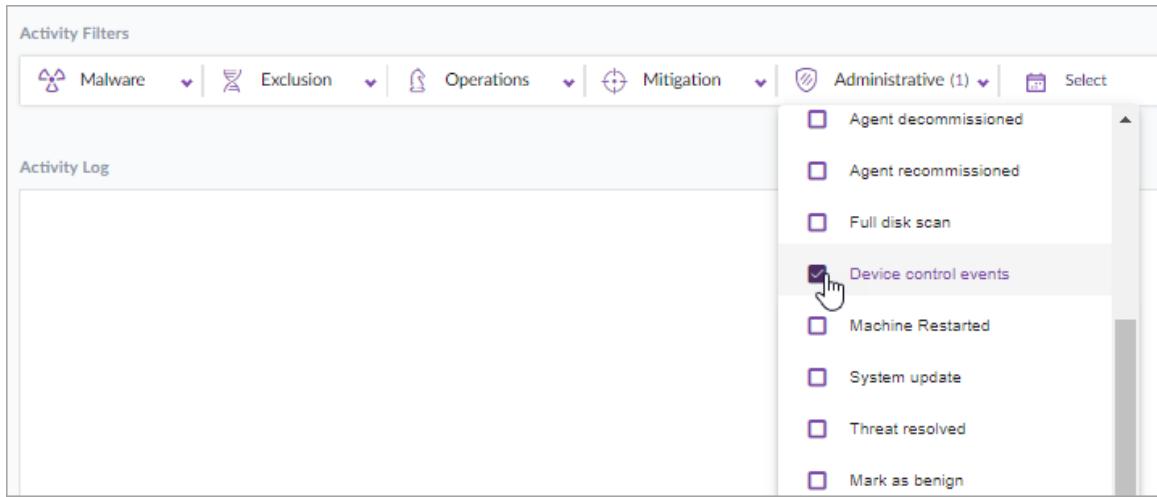


The screenshot shows the 'Activity Filters' section of the SentinelOne interface. At the top, there are three dropdown menus: 'Malware', 'Exclusion', and 'Operations (1)'. The 'Operations (1)' dropdown is currently expanded, displaying a list of activity types. The 'Device control' option is highlighted with a blue selection bar and a hand cursor icon over the checkbox, indicating it is selected. Other listed items include 'Cloud intelligence', 'User added', 'User modified', 'User deleted', 'User login/logout', 'Agent reset local config', 'Agent moved between sites', 'Agent moved to group', 'Group administration', 'Site administration', and 'Packages administration'.

## To see all reported Device Control events:

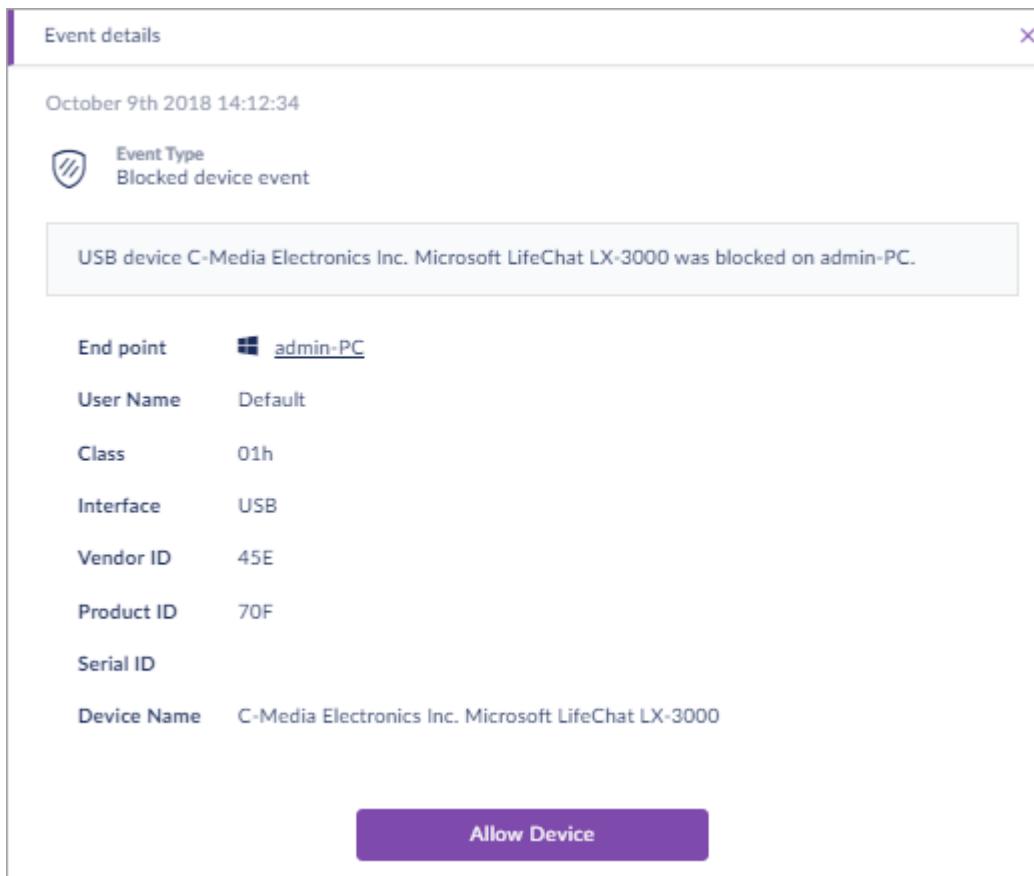
1. In the sidebar, click **Scope**  and select a scope.

2. In the sidebar, click **Activity** .
3. In **Administrative**, click the down arrow to open the options.
4. Scroll down and select **Device Control events**.



The screenshot shows the 'Activity Log' interface. At the top, there are several filter categories: Malware, Exclusion, Operations, Mitigation, and Administrative. The 'Administrative' category is expanded, showing a list of event types. The 'Device control events' option is highlighted with a mouse cursor icon over it.

5. Move the cursor over an event and click  > **Event details** to see the details of the event and the device identifiers.



The 'Event details' modal is displayed. It shows an event from October 9th, 2018, at 14:12:34. The event type is 'Blocked device event'. The details pane contains the following information:

USB device C-Media Electronics Inc. Microsoft LifeChat LX-3000 was blocked on admin-PC.	
End point	 <a href="#">admin-PC</a>
User Name	Default
Class	01h
Interface	USB
Vendor ID	45E
Product ID	70F
Serial ID	
Device Name	C-Media Electronics Inc. Microsoft LifeChat LX-3000

At the bottom of the modal is a purple button labeled 'Allow Device'.

6. If the device was blocked, an option shows to **Allow Device**. Optional: Click **Allow Device** to [create a new rule \[339\]](#) that allows device identifiers of this device.

## 18.6. Creating Device Control Rules from Events

**Management:** Eiffel, Fuji, Grand Canyon, Houston

**Agents:** Windows 2.8+ | macOS 2.7+

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

From a blocked Device Control event in the **Activity** view, you can create a rule to allow a specific device that was blocked for end-users. If a device connected successfully, no rule options are available from the event.

For example, you have a Site rule that blocks the video class of USB devices. However, your Marketing Department needs to use this type of device to record marketing videos. You can open a blocked Device Control event from the Activity log and make a new rule to allow the devices that they need.

The new rule can be very specific, to allow only a specific vendor or product, based on the details recorded in the logged event.

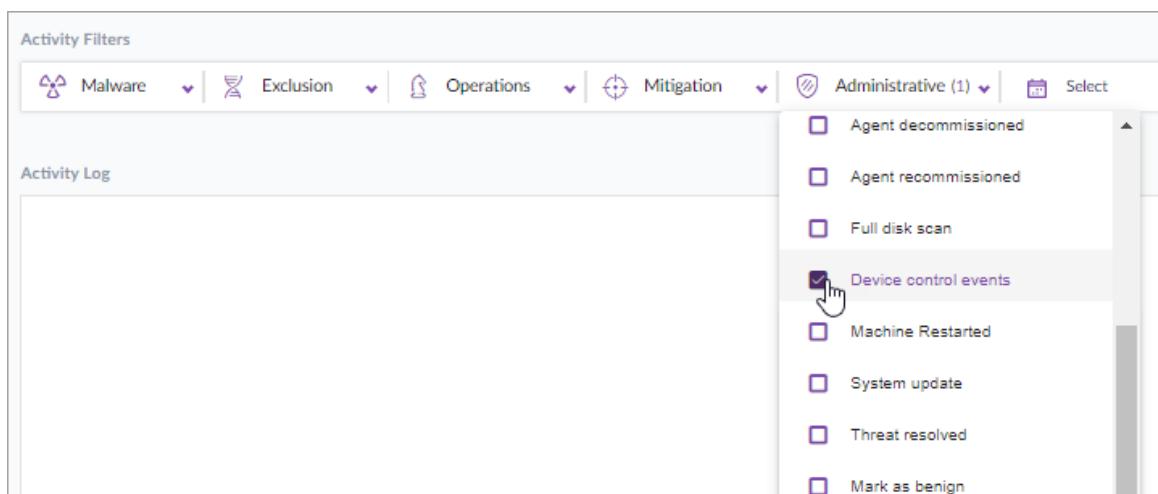
By default, the scope of the new rule is the endpoint's group. After you create the rule, you can [move or copy it \[333\]](#) to change its scope.

**Note:** If a device is already connected to an endpoint, new rules and rule changes do not affect it. To make a new or changed rule take effect on a device, remove the device and then re-connect it.

Watch: [Device Control Demo](#)

### To create a Device Control rule from the Activity log:

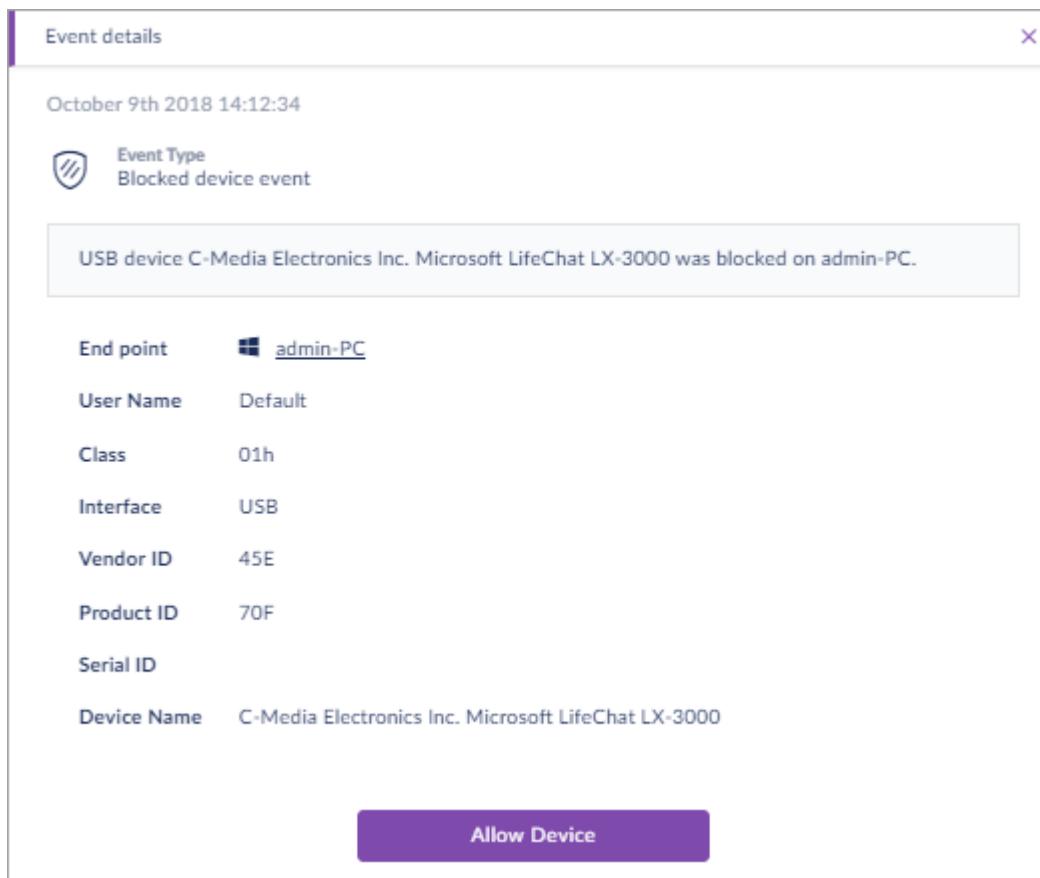
1. In the sidebar, click **Scope**  and select a scope.
2. In the sidebar, click **Activity** .
3. In **Administrative**, click the down arrow to open the options.
4. Scroll down and select **Device Control events**.



5. Move the cursor over a blocked event and click  > **Event details**.



6. In the **Event details** window, click **Allow Device** to open a new rule.



Event details X

October 9th 2018 14:12:34

 Event Type  
Blocked device event

USB device C-Media Electronics Inc. Microsoft LifeChat LX-3000 was blocked on admin-PC.

End point	 <a href="#">admin-PC</a>
User Name	Default
Class	01h
Interface	USB
Vendor ID	45E
Product ID	70F
Serial ID	(empty)
Device Name	C-Media Electronics Inc. Microsoft LifeChat LX-3000

**Allow Device**

7. In the **New Rule** window, enter the **Rule Name**.

New Rule

Rule name	Allow Virtual USB Hub rule
Interface	USB
Rule Type	Product ID
Scope	Default site (Default site) Default group
Action	<input checked="" type="radio"/> Allow <input type="radio"/> Block
<b>Continue</b>	
Cancel	

8. The rule is automatically based on the most specific identifiers available for the device.
  - If the device has a Serial ID (generally for mass storage devices), the rule is based on the Serial ID.
  - For most other devices, the rule is based on the Product ID and Vendor ID.If you want to change the Rule to include a wider range of devices, change the **Rule Type**.
9. Click **Continue**.
10. Enter missing information, if necessary.

New Rule

Allow Virtual USB Hub rule

Interface: USB  
Rule type: Product ID  
Action: Allow  
Scope: Default site (Default site) Default group

Product ID: 2

Vendor ID: QEE

Enable rule immediately after saving

**Save rule**

Back | Cancel

11. Click **Save rule**.

## 18.7. End-User Interaction with Device Control

**Management:** Eiffel, Fuji, Grand Canyon, Houston

**Agents:** Windows 2.8+ | macOS 2.7+

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

When an end-user inserts a device that is blocked by Device Control, a message shows on the endpoint.

Users *cannot* create requests automatically from these messages. This is to prevent an overload of requests for Security Admins.

Admins can easily [create new Device Control rules to Allow devices \[339\]](#) that were blocked, based on the Device Control event log in the **Activity** view.

## 18.8. How to Find Device Identifier Information

**Management:** Eiffel, Fuji, Grand Canyon, Houston

**Agents:** Windows 2.8+ | macOS 2.7+

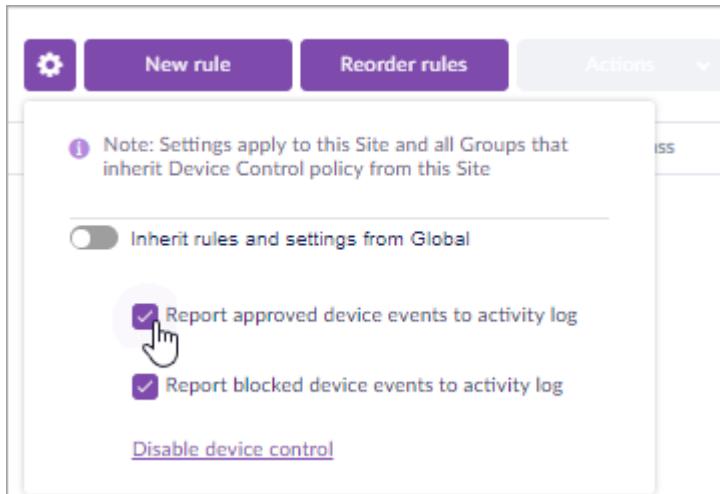
**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

Device Control rules are based on the device identifiers as reported by the hardware, not definitions that the Operating System uses for hardware.

### Getting Device Details from the Management Console

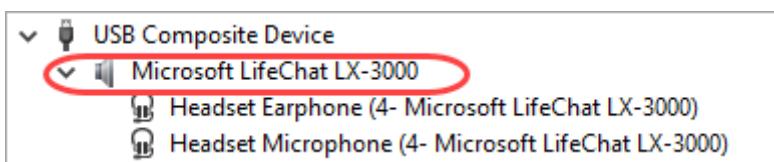
- If a device was connected to an endpoint with a SentinelOne Agent installed, you can see the device information in the Management Console, from the [event details \[336\]](#).
- The information for connected devices is reported if the option **Report approved device events to activity log** is enabled in the Device Control settings.



You can use **Windows Device Manager** or **macOS System Report > Hardware** to get the device identifier information for a device that connected to an endpoint. You can also use external tools that read the parameters of devices.

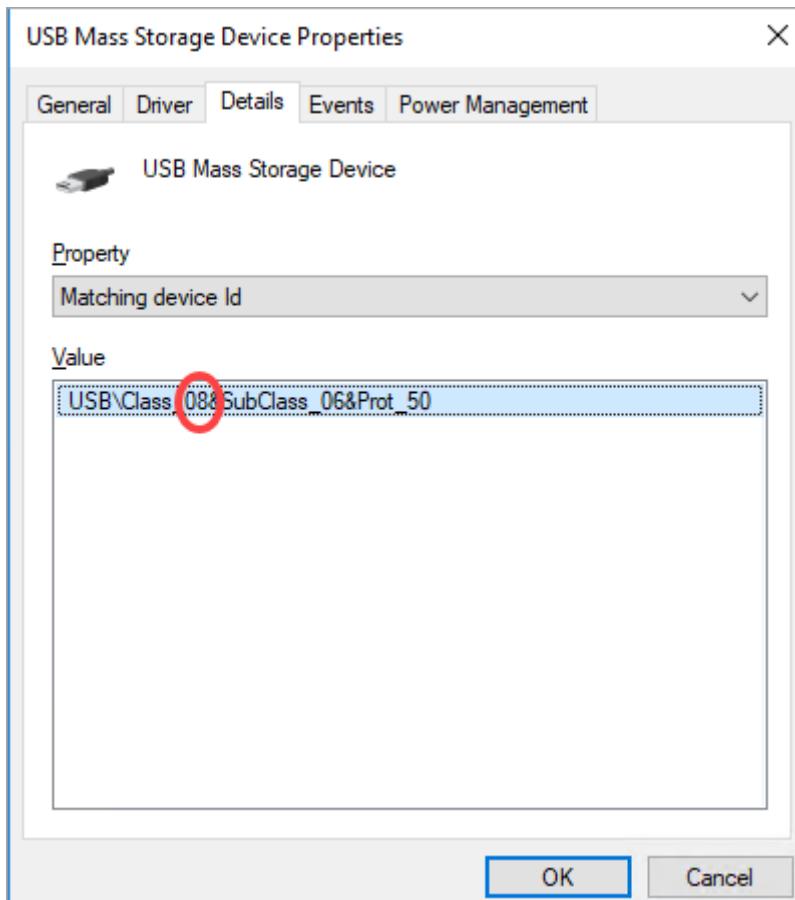
### To find device identifier information for an inserted USB device on Windows:

- From the Control Panel, open the Device Manager.
- Select a device from the tree.
- To find a composite device:
  - From the menu, select **View > Devices by Connection**.
  - Find **USB Composite Device**.
  - Select the root of the device. The different classes of the composite device show below the root. In this example, the root of the composite device is circled.



- In the **Details** tab, open the **Property** list and select a property to find the details:
  - Class - Select Matching device id.**

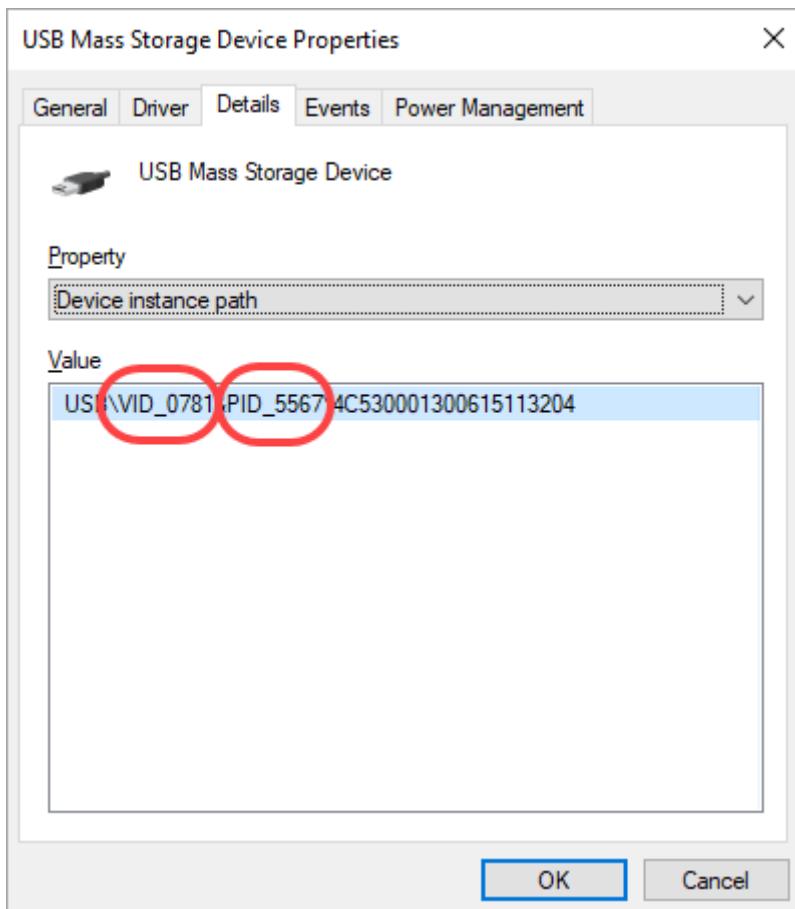
The Value shows Class\_XY, where XY is the class code that Device Control uses. For example, for the device shown below, the class is 08, which corresponds to the class, Mass Storage in Device Control rules.



- **Product ID and Vendor ID - Select Device instance path.**

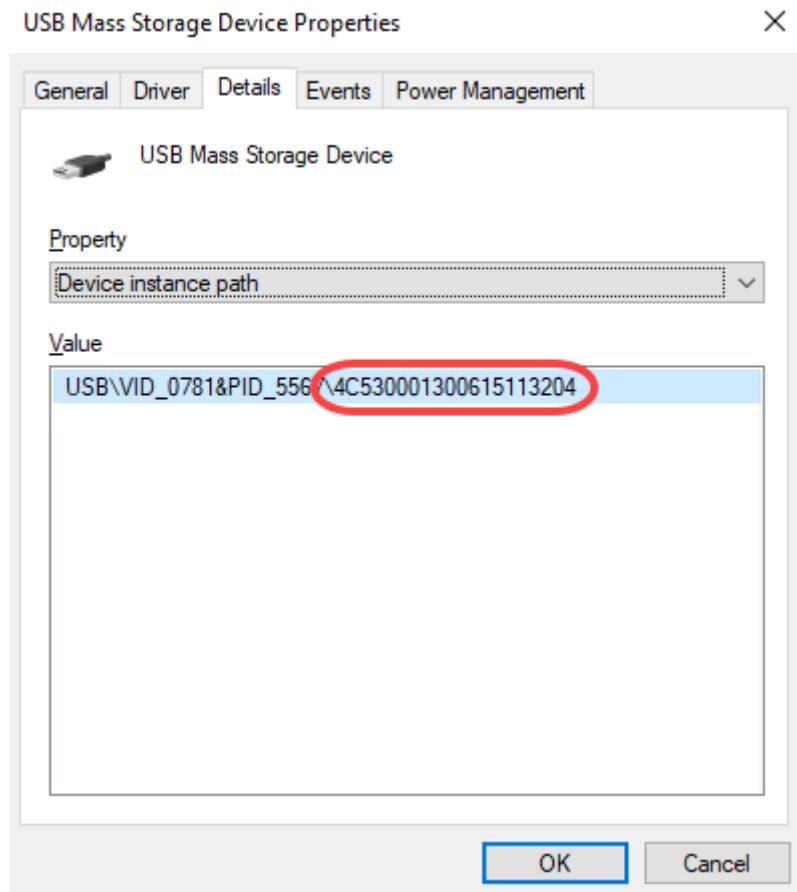
The Value shows VID\_WXYZ&PID\_ABCD, where:

- VID is the Vendor ID, 0781 in the example below
- PID is the Product ID, 5567 in the example below



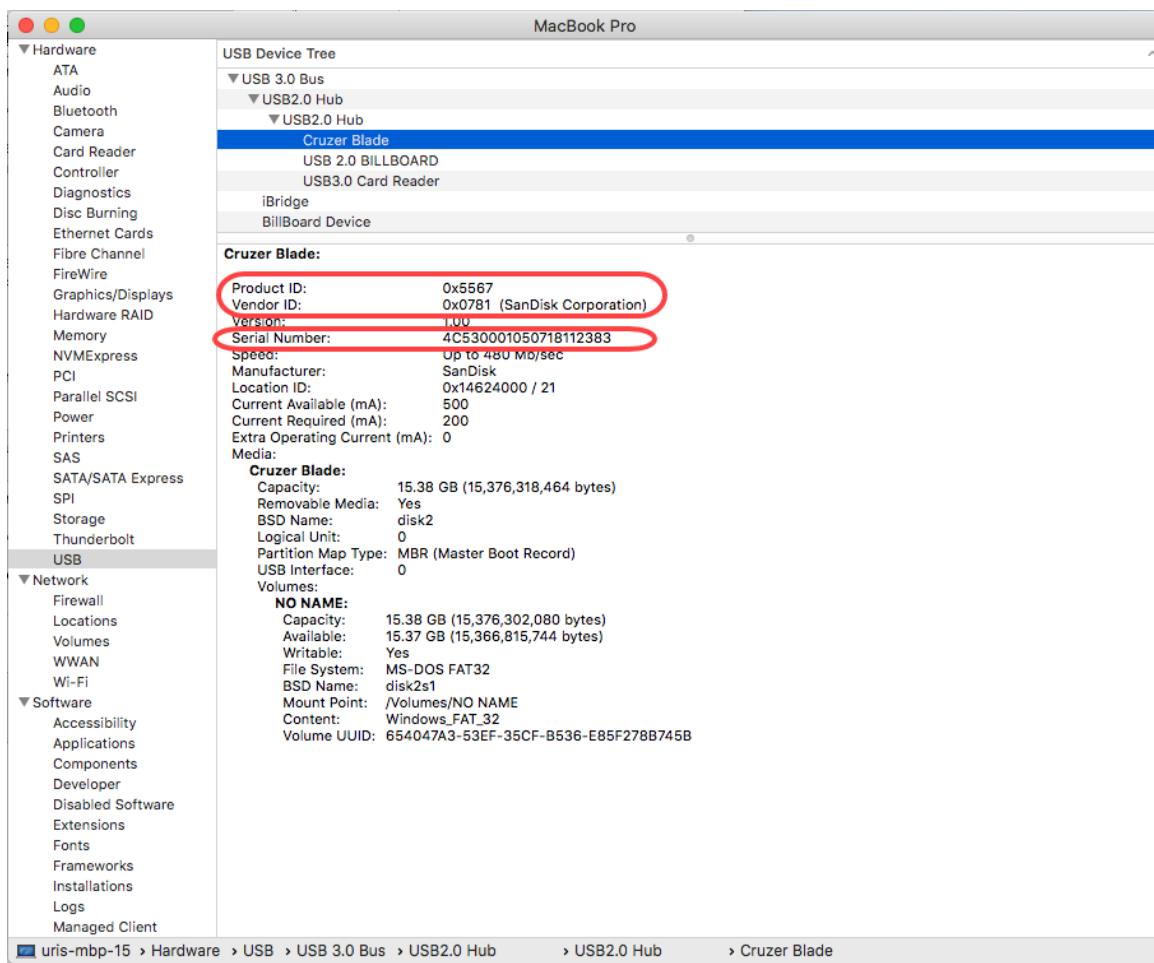
- **Serial ID** - Only mass storage devices have a Serial ID. Select **Device instance path**.

At the end of the value, after the last "\\" is a long string that is the serial ID, 4C530001300615113204 in the example below.



### To find device identifier information for an inserted USB device on macOS:

1. Click on the Apple icon and select **About This Mac**.
2. Click **System Report**.
3. In the navigation tree, select **Hardware > USB**.
4. Click a device to expand its details. See the **Product ID**, **Vendor ID**, and **Serial Number** (if it exists), as shown in this example:



## To find the Class used by Device Control on macOS:

The Class does not show on macOS computers through the UI. To get the information you need to run a command on the endpoint.

1. From the command line of an endpoint, run:

```
sudo sentinelctl device-control list
```

2. See the class shown for each interface, as shown in this example:

```
[mojaveuri:~ vagrant$ sudo sentinelctl device-control list
-- USB --
VMware VMware Virtual USB Mouse
  Vendor ID: 0x0e0f
  Product ID: 0x0003
  Class: 0x00 - Interface specific device
  SubClass: 0x00
  Allowed: yes
  Interfaces:
    [0]
      Class: 0x03 - HID (Human Interface Device)
      SubClass: 0x00
      Allowed: yes
    [1]
      Class: 0x03 - HID (Human Interface Device)
      SubClass: 0x00
      Allowed: yes

VMware VMware Virtual USB Keyboard
  Vendor ID: 0x05ac
  Product ID: 0x020b
  Class: 0x00 - Interface specific device
  SubClass: 0x00
  Allowed: yes
  Interfaces:
    [0]
      Class: 0x03 - HID (Human Interface Device)
      SubClass: 0x01
      Allowed: yes

SanDisk Cruzer Blade
  Vendor ID: 0x0781
  Product ID: 0x5567
  Serial Number: 4C530001050718112383
  Class: 0x00 - Interface specific device
  SubClass: 0x00
  Allowed: yes
  Interfaces:
    [0]
      Class: 0x08 - Mass Storage
      SubClass: 0x00
      Allowed: yes
```

# 19. SentinelOne Firewall Control

**Management:** Eiffel, Fuji, Grand Canyon, Houston

**Agents:** Windows 2.8+ | macOS 2.7+ | Linux 3.0

**SKU:** Complete (not available with Core)

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

**Firewall Control** lets you manage endpoint firewall settings from your SentinelOne Management Console. Use Firewall Control to define which network traffic, applications, and connections are allowed in and out of endpoints.

Firewall Control is with 2.8 Windows Agents, 2.7 macOS Agents, and 3.0 Linux Agents. It is part of the Complete bundle. If you have the Core bundle, you will not see Firewall Control in your Management Console.

Firewall Control policy can be Global, or for the selected Account , Site , or Group. Each scope can inherit policies or have their own.

Define the policy in the Management Console in **Network > Firewall Control**. The Firewall Control policy includes Settings and Rules:

- **Settings [349]:** Turn Firewall Control on or off and define the inheritance settings. Enable or disable Location Awareness. The same settings apply to Windows and macOS endpoints.
- **Rules [351]:** Create and organize rules to allow or block network traffic. There are different sets of rules for endpoints of each OS.

Changes to the Firewall Control policy show in **Activity > Operations > Firewall Control**.

There are no default rules. All traffic is allowed if you do not block it explicitly.

**Note:** When you enable SentinelOne Firewall Control on Windows endpoints, rules from other firewall solutions on the endpoint will become inactive.

## 19.1. Firewall Control Settings

**Management:** Eiffel, Fuji, Grand Canyon, Houston

**Agents:** Windows 2.8+ | macOS 2.7+ | Linux 3.0+

**SKU:** Complete (not available with Core)

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

**In the Firewall Control settings:**

- Define the policy inheritance.

- Turn Firewall Control on or off.
- From Houston management version, enable or disable [Firewall Location Awareness](#).

By default, 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.

By default, Agents have Firewall Control disabled, until they connect to a Site or Group with an enabled Firewall Control policy.

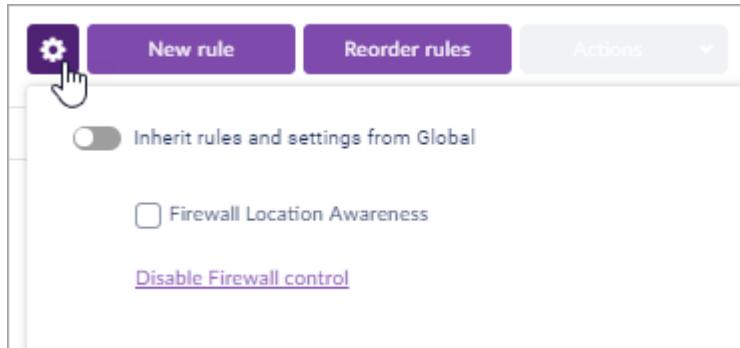
**Note:** When you enable SentinelOne Firewall Control on Windows endpoints, rules from other firewall solutions on the endpoint will become inactive.

## To configure Firewall Control settings:

1. In the sidebar, click **Scope**  and select a scope.
2. In the sidebar, click **Network** .
3. In the **Network** toolbar, click **Firewall Control**.



4. Click the Settings icon.



5. Click **Enable Firewall Control**, if it is not enabled.
6. For an Account, Site or Group: Use the toggle to turn the inheritance On or Off.
7. If inheritance is disabled, enable or disable **Firewall Location Awareness**.
8. Optional: You can click **Disable Firewall Control**. This disables the feature for your current scope and all Sites and Groups that inherit Firewall Control settings from this scope.

For an Account, Site or Group, you must turn Off inheritance before you can disable Firewall Control.

Existing rules remain in the policy but become inactive. When you enable Firewall Control again, the rules will become active with their latest **Enabled** or **Disabled** state

## Firewall Control Policy Inheritance:

- To make an Account, Site, or Group inherit rules and settings from the scope above it:

Turn On **Inherits rules and settings from <scope>** (on by default).

- An Account uses Global settings and Global rules.
- A Site uses the Account or Global settings and rules.
- A Group uses the Site or Account or Global settings and rules.
- You can add additional rules for the Account, Site, or Group.

- To give an Account, Site, or Group its own Firewall Control policy:

Turn Off **Inherits rules and settings from <scope>**.

- The Account , Site or Group uses its own settings.
- It only uses rules configured for that scope.

## 19.2. Firewall Control Rules and Rule Order

**Management:** Eiffel, Fuji, Grand Canyon, Houston

**Agents:** Windows 2.8+ | macOS 2.7+

**SKU:** Complete (not available with Core)

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

Firewall Control rules let you allow or block network traffic, based on the traffic identifiers reported by the operating system. There are different rules for Windows endpoints and for macOS endpoints. When the Management sends policy information to Agents, it includes these rules.

The screenshot shows the Firewall Control section of the SentinelOne web interface. At the top, there are tabs for NETWORK, Full site view, ENDPOINTS, EXCLUSIONS, POLICY, FIREWALL CONTROL (which is highlighted in purple), PACKAGES, BLACKLIST, SITE INFO, and GROUP RANKING. Below the tabs is a search bar labeled 'Select filters...'. Under the FIREWALL CONTROL tab, there's a button group with 'New rule' and 'Reorder rules', followed by an 'Actions' dropdown set to 'No Items Selected'. To the right, there are icons for creating and deleting rules, and a summary showing '2 Rules' and '10 Results'. A sidebar on the right lists operating systems: Windows (with a hand cursor over it), Windows, and macOS. At the bottom, there are columns for Name, Tag, Action, Application, Direction, Protocol, Local Host, Local Port, and Remove rule.

When network traffic enters or leaves an endpoint, the SentinelOne Agent allows or blocks it based on the Firewall Control policy.

- The Agent looks at the rules based on their order in the Firewall Control policy, from the top to the bottom.
- 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.
- If the matched rule has the **Block** Action, the Agent blocks the traffic. If the matched rule has the **Allow** Action, the traffic can pass.

The rules that apply to your current scope show in **Network > Firewall Control**.

Click **Select filters** to filter the rules by rule attributes. Select the attributes to filter for or use the free text search.

#### **The Agent applies the rules in this order:**

1. Group rules from first to last.
2. Site rules from first to last.
3. Account rules from first to last.
4. Global rules from first to last.

New rules are added to the top of the relevant section of the Firewall Control policy.

#### **To change the order of the rules:**

You can change the order of rules in your Admin scope. Account and Site Admins can change the order of rules for the Sites and Groups in their scope.

1. In the sidebar, click **Scope**  and select a scope.
  2. In the sidebar, click **Network** .
  3. In the **Network** toolbar, click **Firewall Control**.
- 
4. Select **Windows** or **MacOS**.
  5. Click **Reorder rules**.
  6. In the window that opens, drag and drop rules, or in the **Order** column, click the number of the rule and enter a new number.
  7. Click **Save**.

### **19.3. Creating and Editing Firewall Rules**

**Management:** Eiffel, Fuji, Grand Canyon, Houston

**Agents:** Windows 2.8+ | macOS 2.7+

**SKU:** Complete (not available with Core)

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

Watch: [How to Create a Firewall Control Rule](#)

Create rules for a specific scope and OS to allow or block network traffic.

When you create a rule, it applies to the current scope of the **Network** view.

- For network traffic to match a rule, all parameters of the rule must match the traffic.
- The default for each parameter is **Any**, which means that no restrictions are defined.
- 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.
- For all other rules, you can leave all parameters as **Any**, except one parameter that you choose to define explicitly.

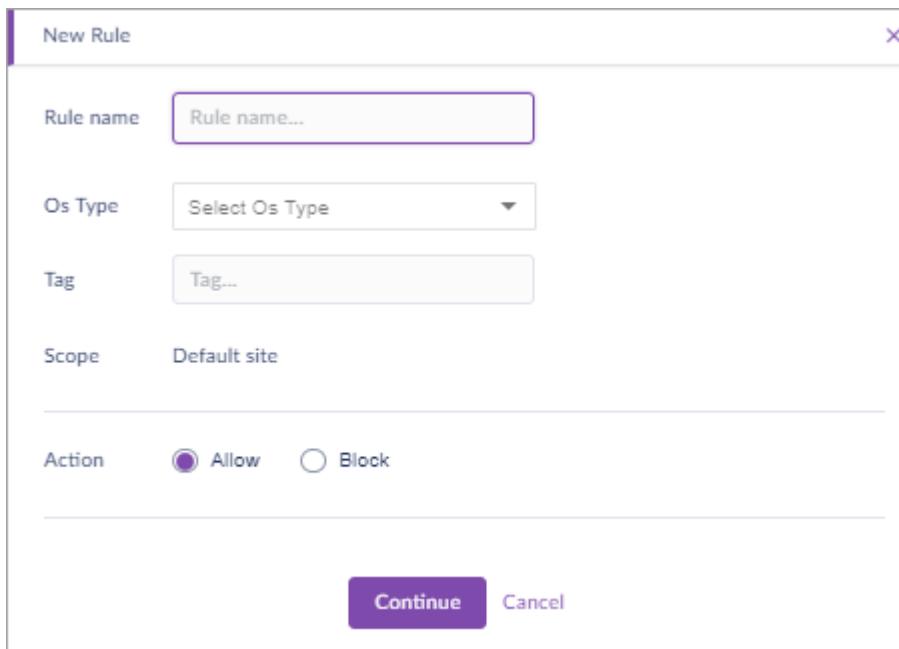
## Firewall Rule Attributes

Attribute	Description
Rule Name	A descriptive name of the rule. It must be a different name from other rules in the scope.
Protocol	An IP protocol the rule applies to. All standard protocols are supported. Select one protocol from the list. <b>Any</b> - Protocol is not defined.
Application	An application the rule applies to, in a specific location on the endpoint. The rules only applies to the application if it is in the defined location. Enter the full path name, including the application. <b>Any</b> - Protocol is not defined.
Direction	<b>Inbound</b> - The rule applies to traffic that is received on an endpoint. <b>Outbound</b> - The rules applies to traffic that leaves an endpoint. <b>Any</b> - The rule applies to inbound and outbound traffic. Optional: Define the <b>Local host</b> . Optional: Define the <b>Remote host</b> .
Local host	Enter the local IP address or range of addresses for endpoints that the rule applies to. For Inbound traffic, the local host is the destination. For Outbound traffic, the local host is the source. IPv4 or IPv6. <b>Any</b> - Local host is not defined. <b>Address</b> - Enter an IP Address. <b>CIDR</b> - Enter an IP range with CIDR format. <b>Range</b> - Enter an IP Address range start and end.
Local port	The local port or range of ports that the rule applies to. <b>Any</b> - Local port is not defined. <b>Single string</b> - Enter a port number <b>Range</b> - Enter a port number range start and end.
Remote hosts	Define one or more remote hosts as the source for Inbound traffic or the destination for Outbound traffic. IPv4 or IPv6. (Multiple Remote hosts are supported from Houston version) <b>Any</b> - Remote host is not defined. <b>FQDN</b> - Enter a hostname in FQDN format, for example, www.webserver.org or mailserver.example.com (Supported from Houston version) <b>Address</b> - Enter an IP Address. <b>CIDR</b> - Enter an IP range in CIDR notation. <b>Range</b> - Enter an IP Address range start and end.

Attribute	Description
Remote port	The remote port or range of ports that the rule applies to. <b>Any</b> - Remote port is not defined. <b>Single string</b> - Enter a port number <b>Range</b> - Enter a port number range start and end.
Locations	Add one or more locations from <b>Settings &gt; Locations</b> to make the rule apply only in specific locations. Uncheck the <b>All</b> option to select one or more specific Locations for the rule. See <a href="#">Location Aware Firewall</a> for more details. This parameter applies if <b>Firewall Location Awareness</b> is enabled in the Firewall Control settings for the scope of the rule.
Action	Define if Agents <b>Block</b> or <b>Allow</b> IP packets that match the rule parameters.
Status	State of the rule: <b>Enabled</b> - Active if Firewall Control is enabled. <b>Disabled</b> - Not active.

### To create a rule:

1. In the sidebar, click **Scope**  and select a scope.
  2. In the sidebar, click **Network** .
  3. In the **Network** toolbar, click **Firewall Control**.
- 
4. Click **New rule**.
  5. In the window that opens, enter the details of the rule:



The dialog box has the following fields:

- Rule name:** A text input field labeled "Rule name...".
- Os Type:** A dropdown menu labeled "Select Os Type".
- Tag:** A text input field labeled "Tag...".
- Scope:** A dropdown menu labeled "Default site".
- Action:** A radio button group with two options: "Allow" (selected) and "Block".

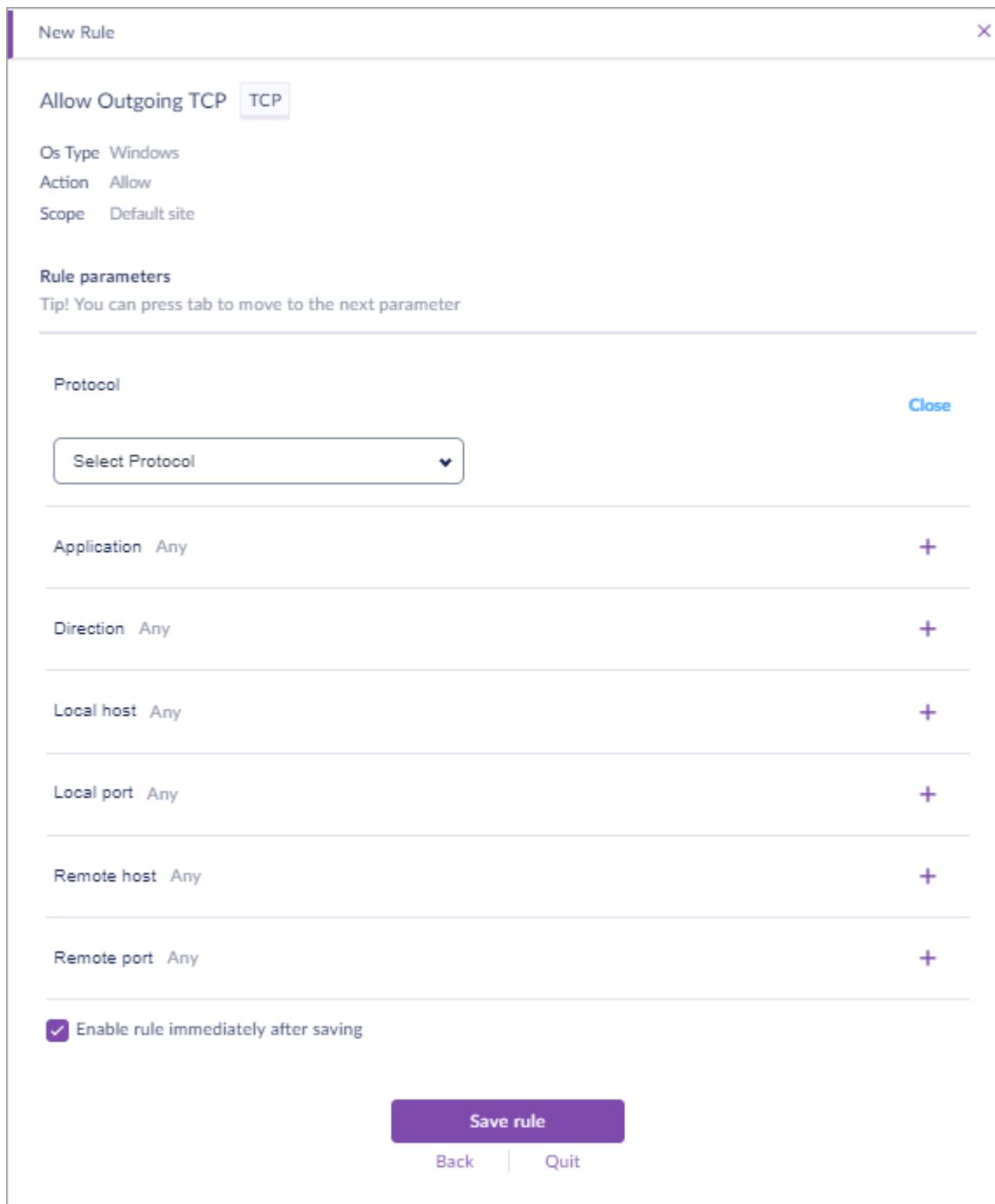
At the bottom of the dialog box are two buttons: **Continue** (purple) and **Cancel**.

- **Rule name** - Enter a descriptive name for the rule. The rule name must be different from other rule names in the scope.
- **OS Type** - Select the OS for the rule: **Windows** or **macOS**.
- **Tag** - Optional: Enter tags that you can search for in the rule base.
- **scope** - This is taken automatically from the current scope of the **Network** view.

If you want to give the rule a different scope, click **Cancel** and select a different scope in **Network**. Or you can move the rule to a different scope later on.

- **Action** - Select **Allow** or **Block** to define if Agents block or allow network traffic that matches the rule parameters.

6. Click **Continue**.
7. In the window that opens, define the [parameters of the rule \[353\]](#).



- Click **+** to expand each parameter.
- Click **Close** to minimize a parameter.
- Press **Tab** to move to the next parameter.

Parameters that are not explicitly defined are set to the default value, which is **Any**.

8. By default, a rule is *NOT* active until you enable it. Click **Enable rule immediately after saving** to create the rule in **Enabled** state.

(This is true for Consoles of version Fuji SP4 and later. If you have an earlier On-Prem management, rules are always enabled.)

- Click **Save rule**.

## To enable or disable a rule:

If a rule is **Disabled**, it is never active but shows in the policy with the **Disabled** Status.

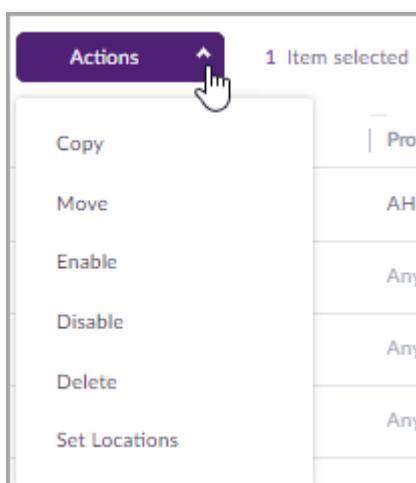
If a rule is **Enabled**, it is active if Firewall Control is enabled. If Firewall Control is disabled for the rule's scope, the rule keeps the Status **Enabled** but is not active. It will become active automatically if Firewall Control is enabled.

- In the sidebar, click **Network** .

In the **Network** toolbar, click **Firewall Control**.

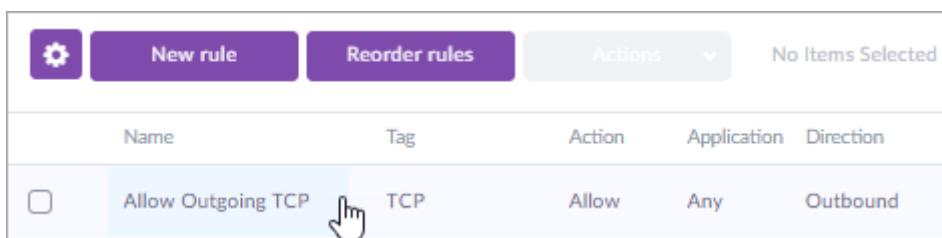


- Select a rule and click **Actions**.



or

- Click a rule.



In the **Rule Details** window, click **Options**.

Rule Details

Firewall rule • Windows

Options ↑

Scope	Site
Name	Allow Outgoing TCP
Action	Allow
Protocol	TCP
Application	Any
Direction	Outbound
Local host	Any
Local port	Any
Remote host	Any
Remote port	Any

Added by Shira Rosenfeld on October 18, 2018  
Last edited on October 18, 2018

● Rule is Active

2. Click **Enable or Disable**.

### To edit a rule:

1. In the sidebar, click **Network**

In the **Network** toolbar, click **Firewall Control**.



2. Click a rule.

Actions					No Items Selected
Name	Tag	Action	Application	Direction	
<input type="checkbox"/> Allow Outgoing TCP		Allow	Any	Outbound	

3. In the **Rule Details** window, click **Edit**.

Rule Details

Firewall rule ▾ Windows

Options ▾

Scope	Site
Name	Allow Outgoing TCP
Action	Allow
Protocol	TCP
Application	Any
Direction	Outbound
Local host	Any
Local port	Any
Remote host	Any
Remote port	Any

Added by Shira Rosenfeld on October 17, 2018  
Last edited on October 17, 2018

● Rule is disabled

Scope Site

Name Allow Outgoing TCP

Action Allow

Protocol TCP

Application Any

Direction Outbound

Local host Any

Local port Any

Remote host Any

Remote port Any

● Rule is disabled

4. Make changes in the **Rule Details**, or click **Continue** to open the next page of the **Rule Details** and change the rule parameters.

The screenshot shows the 'Rule Details' dialog box for a 'Firewall rule • Windows'. The rule name is 'Allow Outgoing TCP'. The 'Os Type' is set to 'Windows'. The 'Tag' is 'TCP'. The 'Scope' is 'All Sites'. The 'Action' is set to 'Allow' (radio button selected). Below the rule details, it shows the history: 'Added by Shira Rosenfeld on October 17, 2018' and 'Last edited on October 17, 2018'. A note indicates that the rule is disabled. At the bottom, there are buttons for 'Save changes' (highlighted in purple), 'Continue', and 'Discard'.

- Click **Save changes**.

## 19.4. Moving and Copying Firewall Rules

**Management:** Eiffel, Fuji, Grand Canyon, Houston

**Agents:** Windows 2.8+ | macOS 2.7+ | Linux 3.0+

**SKU:** Complete (not available with Core)

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

You can *copy* a Firewall Control rule to use it in multiple Sites or groups. For example:

- You have a rule for Site A: Copy it to use it in all of Site B, or copy it to one Group of Site B.
- You have a rule in Group X, which is in Site A: Copy it to two other Groups in Site A.

You can *move* Firewall Control rules to change their scope. For example:

- You made a Group rule for one Group and want to change it to be a Site rule.
- You made a rule for Site A and want it to apply to Site B instead.

## To move Firewall Control rules between Sites or Groups:

1. In the sidebar, click **Scope**  and select a scope.
2. In the sidebar, click **Network** .
3. In the **Network** toolbar, click **Firewall Control**.



4. Select a rule or multiple rules.

A screenshot of a table listing firewall rules. The columns are: Name, Tag, Action, Application, and Direction. One rule is selected, indicated by a checkmark and a hand cursor icon over the first column. The rule details are: Allow Outgoing TCP, TCP, Allow, Any, Outbound.

Name	Tag	Action	Application	Direction
Allow Outgoing TCP	TCP	Allow	Any	Outbound

5. Click **Actions** and select **Move**.

A screenshot of a dropdown menu under the **Actions** button. The menu items are: Copy, Move, Enable, Disable, Delete, and Set Locations. The **Move** option is highlighted with a mouse cursor icon.

6. Select the destination for the rule.

A screenshot of a dialog box titled "Move rule". It contains a message: "You are about to move Allow outgoing tcp" and "Select destination". Below this are two dropdown menus: "Site" set to "Default site" and "Group" set to "Default group". At the bottom are "Move Rule" and "Cancel" buttons.

7. Click **Move**.

### To copy Firewall Control rules:

1. In the sidebar, click **Scope**  and select a scope.
2. In the sidebar, click **Network** .
3. In the **Network** toolbar, click **Firewall Control**.

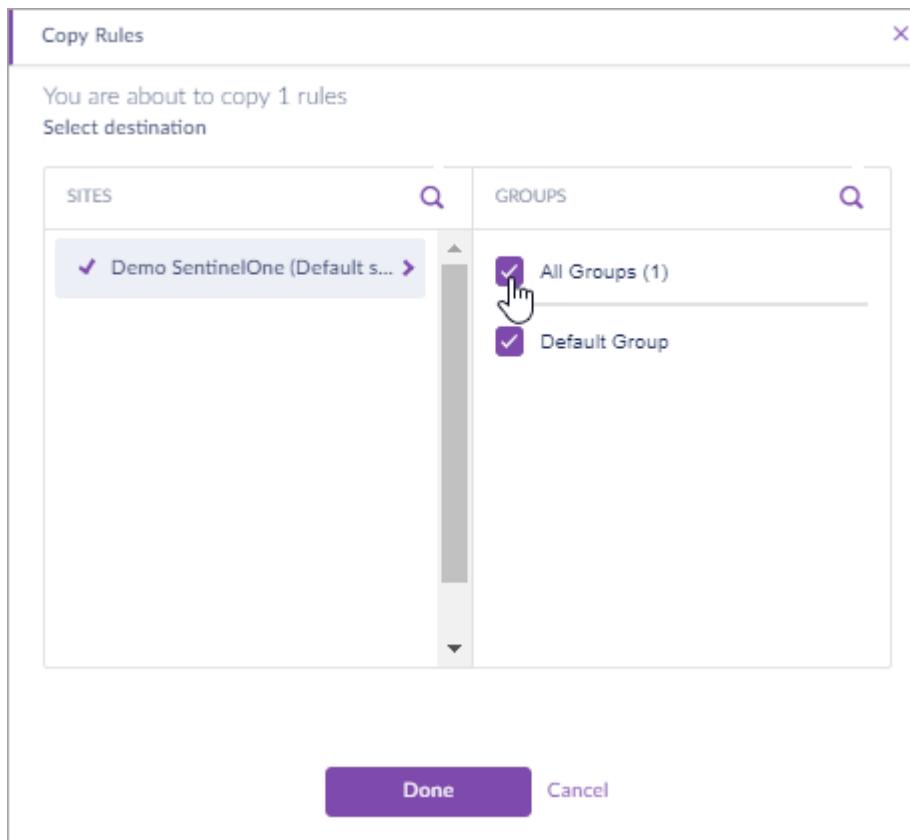


4. Select a rule or multiple rules.

A screenshot of a table listing Firewall Control rules. The columns are: Name, Tag, Action, Application, and Direction. One rule is selected, indicated by a hand cursor icon pointing at the first column of the row.

Name	Tag	Action	Application	Direction
Allow Outgoing TCP	TCP	Allow	Any	Outbound

5. Click **Actions** and select **Copy**.
6. In the **Copy Rules** window:
  - a. In the **SITES** column, select a Site.
  - b. In the **GROUPS** column, select **All Groups**, or one or more specific groups.



7. Click **Done**.

## 19.5. Importing and Exporting Firewall Rules

**Management:** Eiffel, Fuji, Grand Canyon, Houston

**Agents:** Windows 2.8+ | macOS 2.7+ | Linux 3.0+

**SKU:** Complete (not available with Core)

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

You can export Firewall Control rules from one Site and import them to another Site or a Group. You can also export rules from one SentinelOne deployment and import them into a different SentinelOne deployment.

When you import rules, all rules are imported to the current scope. For example, if you are in a Site that inherits the Global Firewall Control, policy, and you export the Firewall Control rules and import them to a different Site: All Global and Site rules become Site rules in the Site to which you imported.

### To export Firewall Control rules from the Management Console:

You can export rules to a .json file. All rules for your current scope are exported. This includes Global rules that might apply to the scope, even if you do not have permissions to edit them.

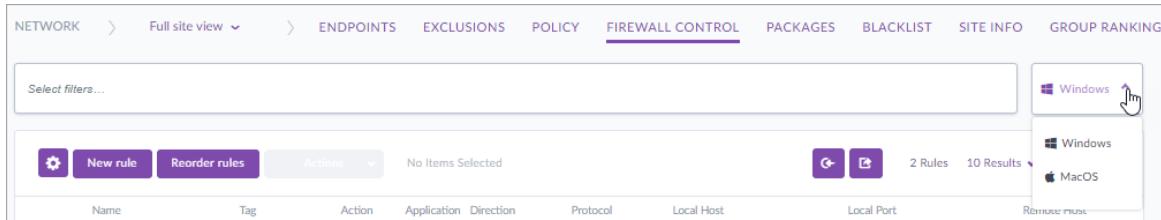
1. In the sidebar, click **Scope**  and select a scope.

2. In the sidebar, click **Network** .

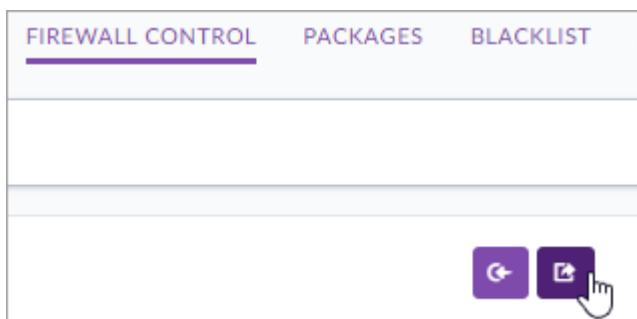
3. In the **Network** toolbar, click **Firewall Control**.



4. Select Windows or MacOS.



5. Click the Export rules icon.



The exported rules download in a .json file to the default Downloads folder of the computer from which you clicked Export rules.

## To import Firewall Control rules:

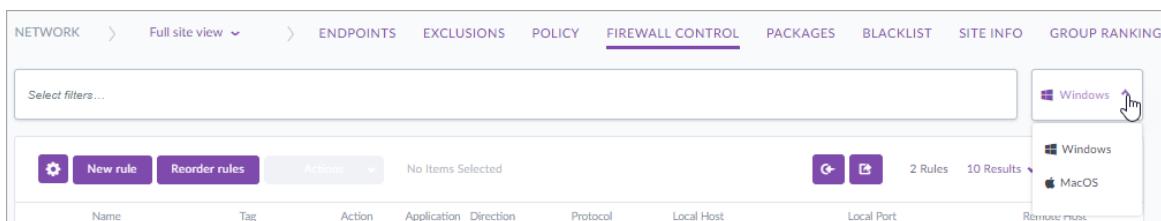
1. In the sidebar, click **Scope**  and select a scope.

2. In the sidebar, click **Network** .

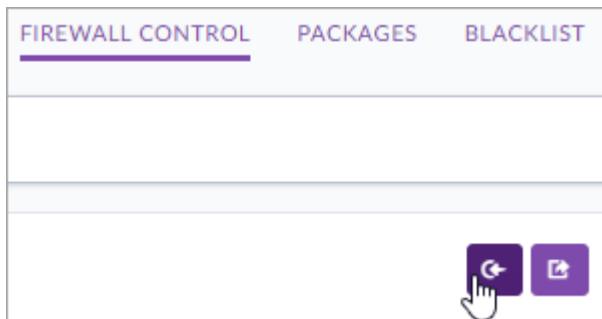
3. In the **Network** toolbar, click **Firewall Control**.



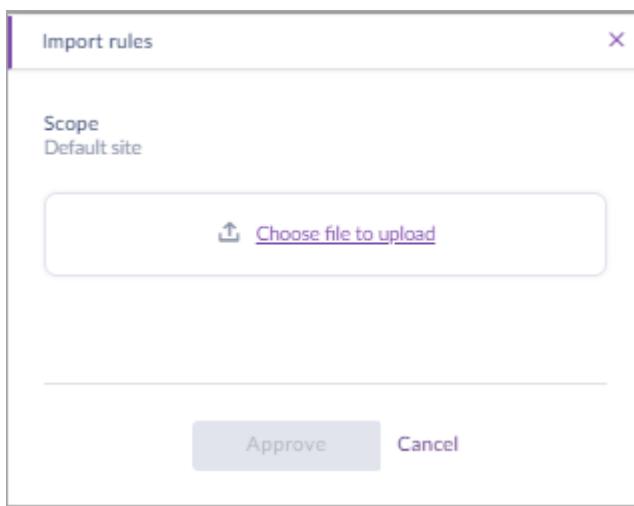
4. Select Windows or MacOS.



5. Click the Import rules icon.

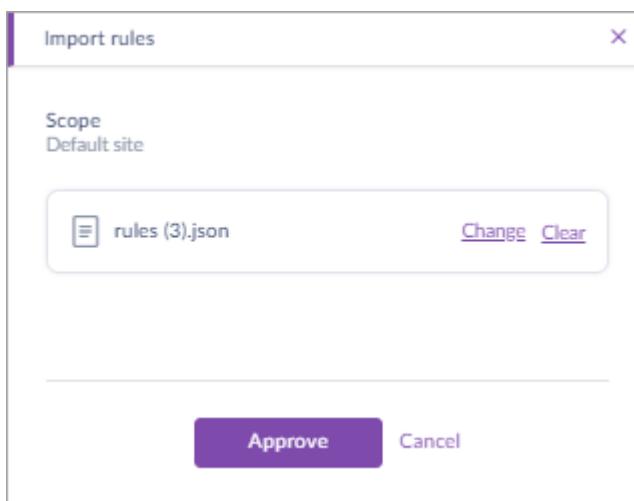


6. In the **Import Rules** window, click **Choose file to upload**.



7. Browse to the file location and click **Open**.

8. In the **Import Rules** window, click **Approve**.



## 19.6. Using FQDN in Firewall Rules

**Management:** Houston

**Agents:** Windows 3.4+ | macOS 3.4+ | Linux 3.0+

**SKU:** Complete (not available with Core)

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

From management version Houston with supported Agent versions, you can use FQDN hostnames as Remote hosts in Firewall Control rules.

This is in addition to IP address, range of IP addresses in CIDR notation, and range of IP addresses with a start and end.

Remote hosts ADDRESSES, FQDN, RANGE

Done

Address	192.0.2.5	Delete
FQDN	www.unwantedservice.com	Delete
Range	192.0.2.200 - 192.0.2.250	Delete

[Add more](#)

Note: Do not use FQDN rules on unsupported Agents. If a Windows Agent of version 3.3 gets an FQDN rule, there will be incorrect results.

For example:

- Make a rule to allow TCP outbound traffic over port 80 to specific servers in your organization, based on their FQDN name.
- Make a rule to block all traffic to a specific external server that currently poses a threat to the organization, based on its FQDN name, for example, a phishing server that your users are connecting to and uploading malicious files.

Actions		No Items Selected								12 Rules 10 Results	
Name	Tag	Application	Direction	Protocol	Remote Hosts	Remote Port	Scope	Locations			
<input type="checkbox"/> Block Malicious Server	Any	Any	Any	Any	Www.malicious-server.com	Any	Site	All			
<input type="checkbox"/> Allow JIRA (Port 8080)	Any	Any	Any	Any	Jira.company.com	8080	Site	All			

### How does the Agent allow or block activity based on FQDN?

When an Agent receives a Firewall Control policy with rules that control traffic to FQDNs, it translates the FQDNs into IP addresses. The Agent Firewall then allows or blocks traffic to those IP addresses.

The Agent dynamically updates the FQDN to IP translation to handle scenarios where the IP address seen by the endpoint changes. The Agent uses the Operating System DNS query APIs to translate FQDN to IP. If a value is not in the cache, it queries the DNS servers. For example:

- The endpoint DNS server changes.

- The remote server IP address changes.
- The Firewall Control policy changes.
- An FQDN entry in the Operating System DNS table is outdated.
- The Agent checks for IP updates periodically.

#### **Limitations for Remote Hosts defined by FQDN:**

- The number of FQDN entries in all rules is limited to 50 per scope. For example, 50 in a Group, 50 in a Site, and 50 in an Account.

The feature is not intended to integrate with external IP reputation feeds that can generate thousands of new FQDNs per day.

- The number of Remote host entries in one rule, including FQDN entries, is limited to 30.
- FQDN rules do not apply when an endpoint is set to route traffic through a proxy. In such cases, the FQDN rules will be ignored. To block traffic route through an organization's proxy, use the proxy filtering options.
- In some cases, (usually when there is DNS load balancing), the first IP packet might be allowed or blocked, despite the Firewall rule. Immediately afterwards the Agent will get the updated IP address and block or allow the traffic according to policy.
- Rules for a specific URL inside a Host (for example: <https://jira.company/issues>) are not supported. The rule must allow or block entire access to this FQDN.
- Wildcards are not supported.
- Unicode is not supported.

## **19.7. Firewall Control and OS Security**

**Management:** Eiffel, Fuji, Grand Canyon, Houston

**Agents:** Windows 2.8+ | macOS 2.7+ | Linux 3.0+

**SKU:** Complete (not available with Core)

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

#### **SentinelOne Firewall Control on Windows**

In Windows Security Center, SentinelOne Firewall Control is registered in two Network Firewall categories:

- NET\_FW\_RULE\_CATEGORY\_FIREWALL,
- NET\_FW\_RULE\_CATEGORY\_BOOT

The SentinelOne EPP registers as Virus protection.

The screenshot shows the Windows Control Panel under 'System and Security > Security and Maintenance'. It displays the status of various security components:

- Network firewall:** On, Sentinel Firewall Control is turned on.
- Virus protection:** On, Sentinel Agent is turned on.
- Internet security settings:** OK, All Internet security settings are set to their recommended levels.
- User Account Control:** On, UAC will notify you when apps try to make changes to the computer. A link to 'Change settings' is available.

**See also:** [How do I know what security settings are right for my computer?](#)

SentinelOne Firewall Control does not register in these categories:

- NET\_FW\_RULE\_CATEGORY\_STEALTH
- NET\_FW\_RULE\_CATEGORY\_CONSEC

Windows Firewall can be registered in the other two categories.

**Note:** When you enable SentinelOne Firewall Control on Windows endpoints, rules from other firewall solutions on the endpoint will become inactive.

### SentinelOne Firewall Control on Mac

In macOS SentinelOne is not registered as a firewall product. Firewall Control works in parallel to the macOS firewall, which can block unwanted Applications. If there is a conflict between the macOS firewall and the SentinelOne firewall, the SentinelOne firewall rules have priority.

## 19.8. Firewall Control - Event Logging

**Management:** Fuji, Grand Canyon, Houston

**Agents:** Windows 3.0+

**SKU:** Complete (not available with Core)

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

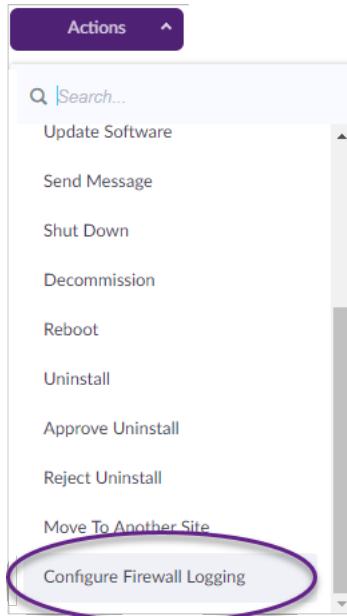
See [Firewall Control events](#) in **Activity** and read the local log file, written in clear text, for Firewall Control events of an endpoint with Firewall Control enabled. Enable the logs for specific endpoints, one Agent at a time.

**Note:** 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.

**Important:** Before you begin, make sure the Group and Site of the Agent has [Firewall Control enabled](#).

### To enable Firewall Control logs:

- In **Endpoint Details**: click **Actions > Configure Firewall Logging**.



- In **sentinelctl**:

```
sentinelctl config -p agent.firewallLogging.reportLog -v true - Enables log write and read on the endpoint.
```

```
sentinelctl config -p agent.firewallLogging.reportMgmt -v true - Enables Firewall Control events on this endpoint to show in the Activity page.
```

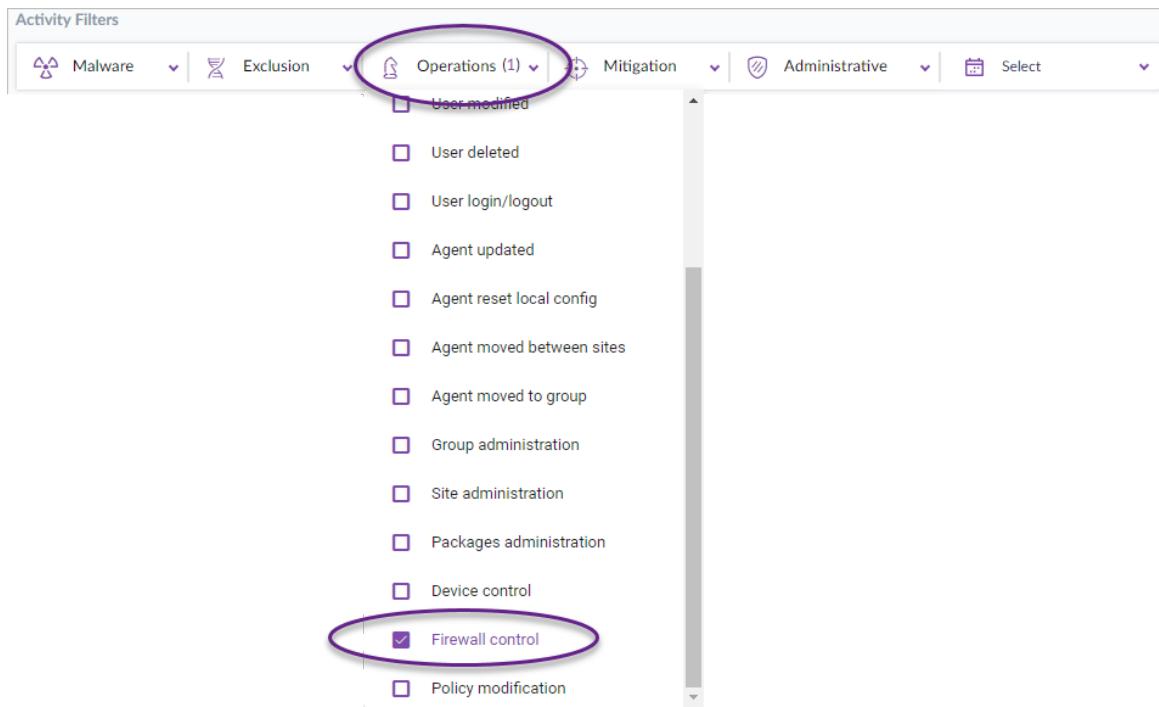
- In **Policy Override**:

```
{
  "firewallLogging": {
    "reportLog": true,
    "reportMgmt": true
  }
}
```

### To see Firewall Control in Activity:

1. In the sidebar, click **Scope** and select a scope.

2. In the sidebar, click **Activity** .
3. In the **Operations** menu, click **Firewall control**.



The screenshot shows the 'Activity Filters' interface. At the top, there are several dropdown menus: 'Malware', 'Exclusion', 'Operations (1)', 'Mitigation', 'Administrative', and 'Select'. The 'Operations (1)' menu is expanded, showing a list of activities. The 'Firewall control' option is circled with a purple oval.

- User modified
- User deleted
- User login/logout
- Agent updated
- Agent reset local config
- Agent moved between sites
- Agent moved to group
- Group administration
- Site administration
- Packages administration
- Device control
- Firewall control
- Policy modification

The **Activity Log** shows events such as: The management user *name* updated Firewall Control settings in *group or site*. Modified the settings parameter *parameter* from *value* to *value*.

### To read Firewall Control logs:

1. On the Windows endpoint, run: cd C:\ProgramData\Sentinel\logs
2. Find the logs with: visible

For example: SentinelOne\_visible\_0.log

You can open the Firewall Control logs in the text editor of your choice.

You can also send Firewall Control events to your syslog server. Select activities in **Settings > Notifications > Firewall Control**.

	Email	Syslog
1 Recipients, SMTP configured		Syslog configured
Rule Copied To Scope	<input type="checkbox"/>	<input type="checkbox"/>
Rule Created	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Rule Deleted	<input type="checkbox"/>	<input type="checkbox"/>
Rules Modified	<input type="checkbox"/>	<input type="checkbox"/>
Moved From Scope	<input type="checkbox"/>	<input type="checkbox"/>
Rule Moved To Scope	<input type="checkbox"/>	<input type="checkbox"/>
Rules Reordered	<input type="checkbox"/>	<input type="checkbox"/>
Settings Modified	<input type="checkbox"/>	<input type="checkbox"/>

## 20. SentinelOne Remote Shell

**Management:** Fuji, Grand Canyon, Houston

**Agents:** Windows 3.0+ | macOS 3.0+

**SKU:** Complete (not available with Core)

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

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 - directly and securely from the Management Console.

This lets you troubleshoot end-user issues from wherever you can access your Management Console.

Remote Shell is supported from Fuji Management with 3.0 Windows Agents and 3.0 macOS Agents.

Watch: [How to enable and use Remote Shell](#).

Remote Shell use cases:

- Faster troubleshooting made possible by admins not needing to be in physical contact with an endpoint device to solve problems.
- Increased support for remote users by removing the need for visits to IT departments.
- The ability to easily change local configuration without leaving the premises.
- Eliminating the need for memory dump and other advanced tools in deep forensic investigation.
- Terminating undesired applications or processes running on endpoint devices.
- Initiating remote controls in a secure manner.

The shell process runs with local administrator user permissions. If different permissions are necessary, you can authenticate with domain user credentials inside the Remote Shell session.

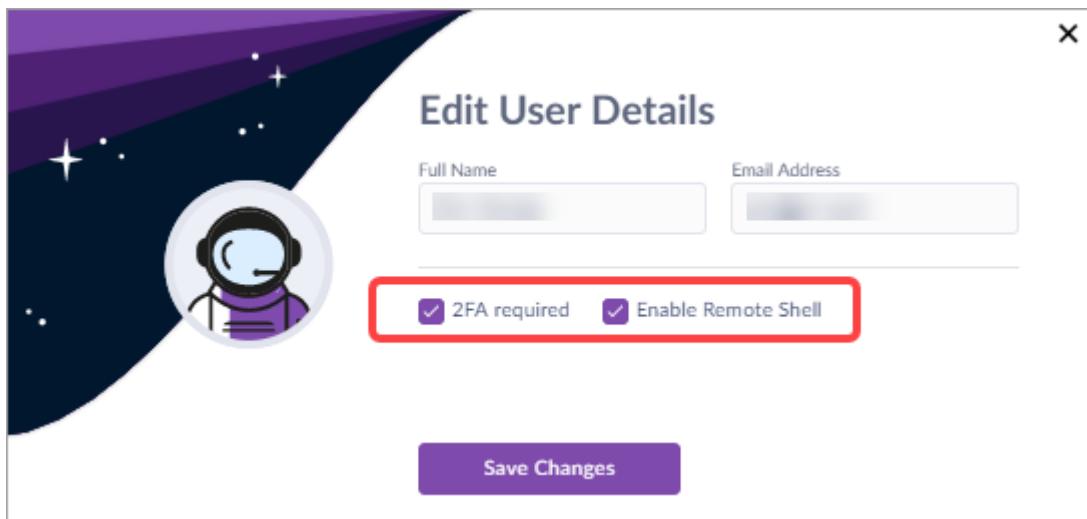
Agents apply all detection and protection logic on the Remote Shell activity.

### Requirements to use Remote Shell:

To make sure that Remote Shell is used securely and only for the intended purposes, there are many requirements for the feature.

#### • User Requirements:

- The user must be an Admin, not a Viewer, and have explicit permission to use Remote Shell. Enable **Remote Shell** in the user settings.



- The user must have Two-Factor Authentication configured.

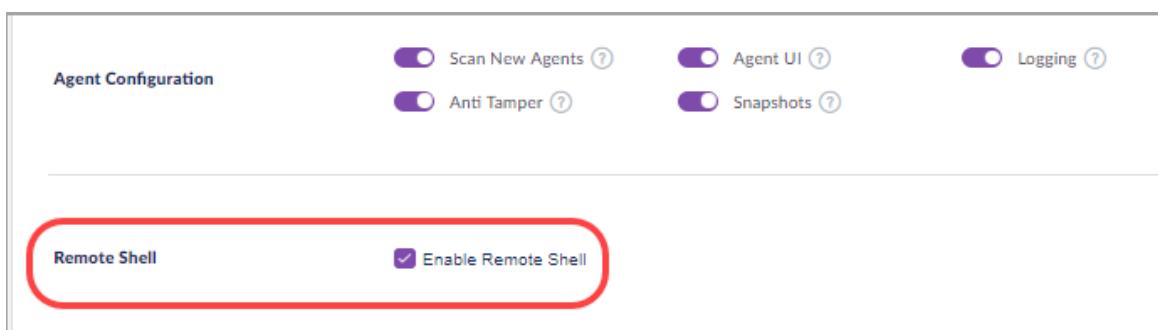
You can [enable Two-Factor Authentication](#) for a specific user or for a scope.

- A Global Admin can enable Remote Shell for other Admins. An Account Admin can enable it for Site Admins (but not for other Account Admins). All Admins can disable (and enable it again) in policies.

- Site Requirements:**

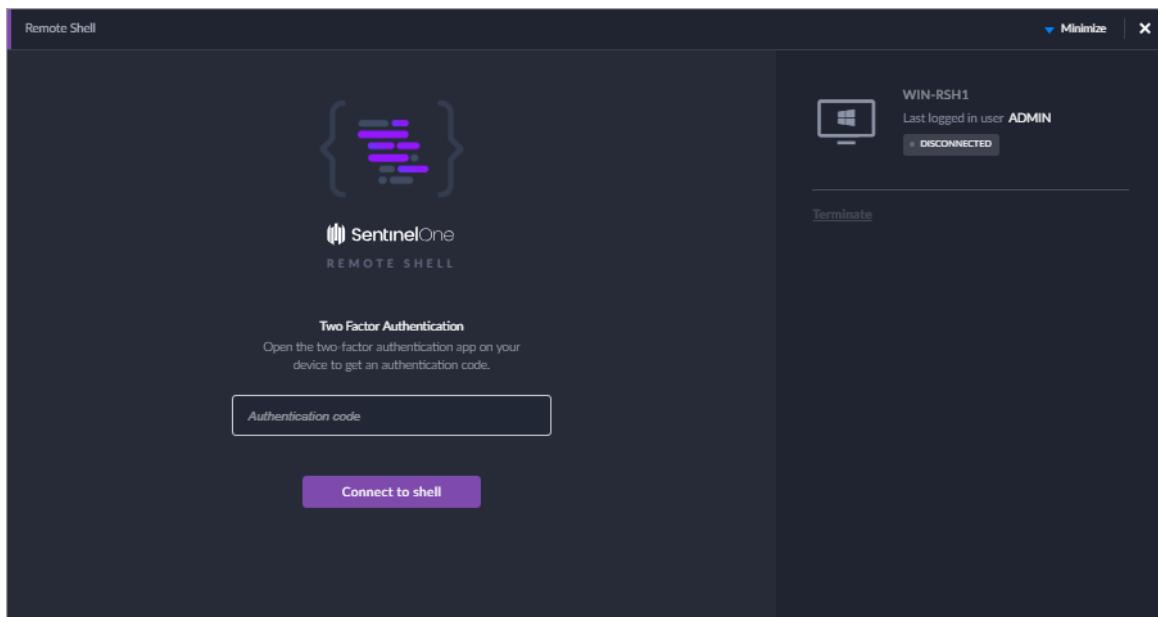
- Remote Shell requires the Complete SKU and is enabled by default in Sites with the Complete SKU.
- When Remote Shell is enabled for a Site, Remote Shell shows in the Management Console.

From the Remote Shell option in the policy, enable or disable the feature.



- Remote Shell Session Requirements:**

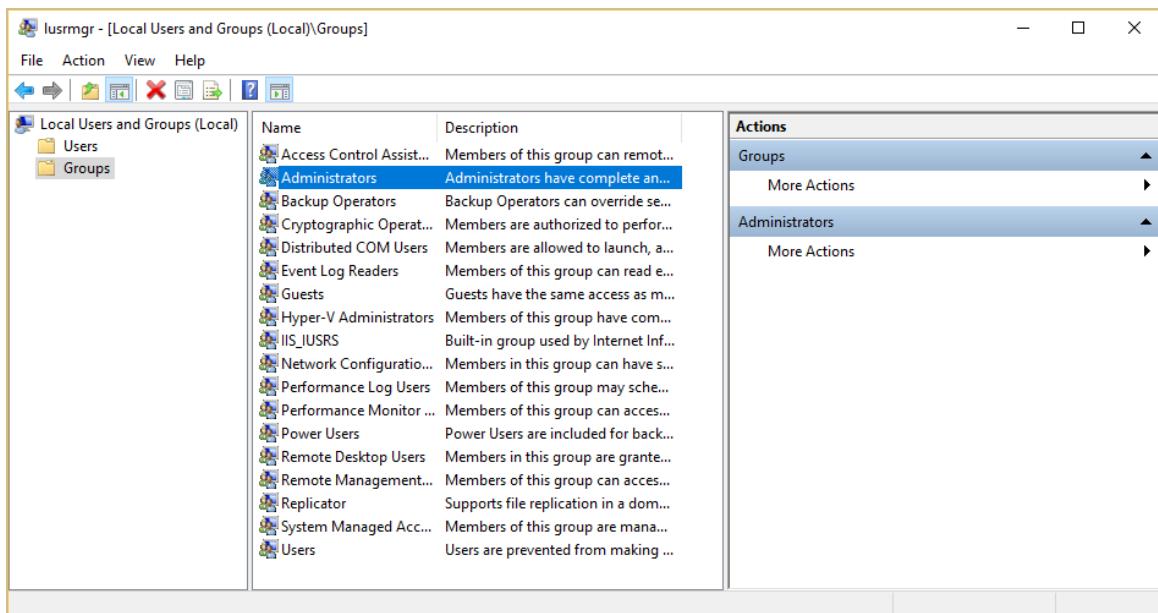
- One shell can be open on an endpoint. If a Remote Shell session is open, a different user cannot open a session on the endpoint.
- To open a session, you must enter a 2FA code from the 2FA App on your phone.



- At the start of a session, you create a password. The transcript of the session is encrypted with this password.
- Remote Shell sessions can be open on multiple endpoints at one time, but each session must be opened separately on each endpoint.

• **Endpoint Requirements:**

- The endpoint must have an OS and SentinelOne Agent version that support Remote Shell.
- The endpoint must have default settings for local **Administrators** users. The Agent creates a new user in the local **Administrators** group, and it requires default permissions.



- The Agent must be online and connected to the Management to open a Remote Shell session.

- If the endpoint is in Network Quarantine (disconnected from network), some commands will not work because the endpoint cannot access the network. If necessary, reconnect the endpoint to the network.

In an upcoming release, customized firewall rules for endpoints in Network Quarantine will be available, to let you open access to specific network resources.

- A session can be open or minimized on the endpoint.

Only the admin who runs the Remote Shell session can see the open or minimized session. If a different admin tries to open a session for the same endpoint, a message shows that a session is already open.

The screenshot shows the 'Endpoint Details' window for an endpoint named 'WIN-RSH1'. The window has tabs for 'GENERAL' and 'APP INVENTORY', with 'GENERAL' selected. It displays various system details:

	Site name	Default site	Group name	Default group
Agent version	3.0.0.0 <span>UPDATED</span>		Console connectivity	<span>Online</span>
Scan status	Aborted ( Dec 27, 2018 ...)		Network status	<span>Enabled</span>
Memory	2.00 GB		Domain	WORKGROUP
CPU	2 X Intel(R) Xeon(R) CPU...		Subscribed on	Dec 26, 2018 18:11
Core count	2		Console visible IP	
Disk encryption	Off		IP Address	
UUID	944ab6f6f08cdc48952c...			

Below this is a section for 'Network Adapters':

NAME	IP	MAC ADDRESS
Ethernet	10.0.82.128	00:50:56:91:83:99

At the bottom of the window, there is a session status bar:

Remote Shell Connected · Inactivity Timeout ▲ Expand

## 20.1. Starting a Remote Shell Session

**Management:** Fuji, Grand Canyon, Houston

**Agents:** Windows 3.0+ | macOS 3.0+

**SKU:** Complete (not available with Core)

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

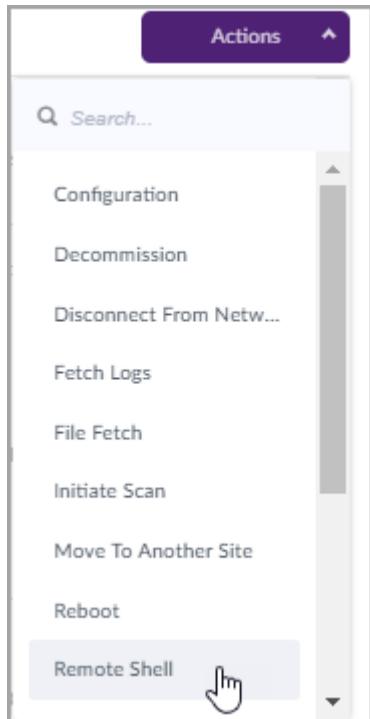
Make sure you have all [requirements \[372\]](#) before you start.

## To start a Remote Shell session on an endpoint:

1. In the Management Console, click an endpoint name to open the Endpoint Details.

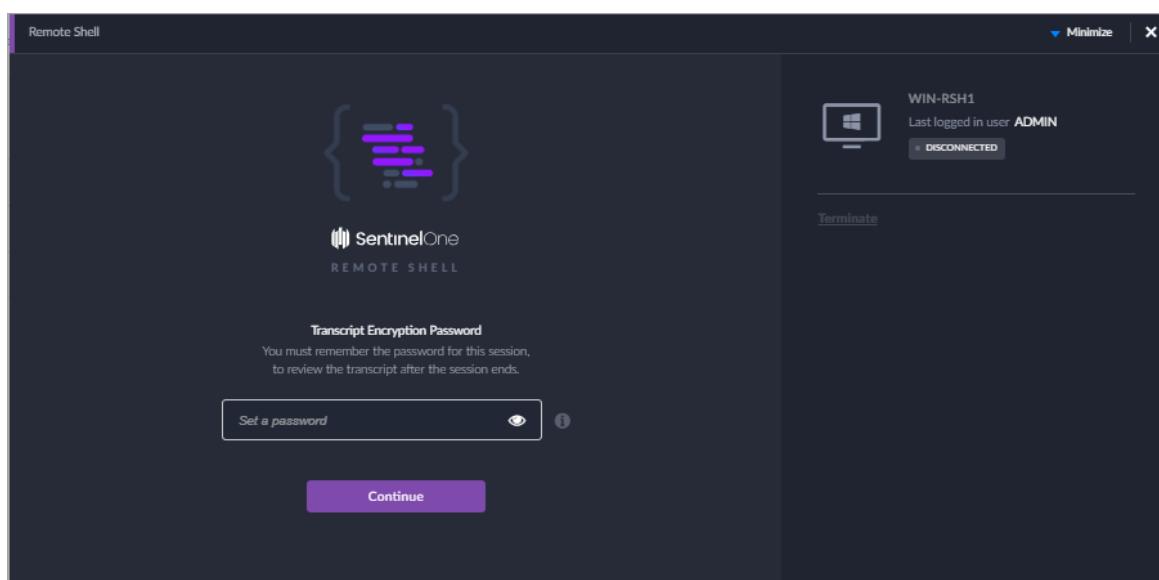
Or in Network > Endpoints, select an endpoint.

2. Click **Actions** and select **Remote Shell**.

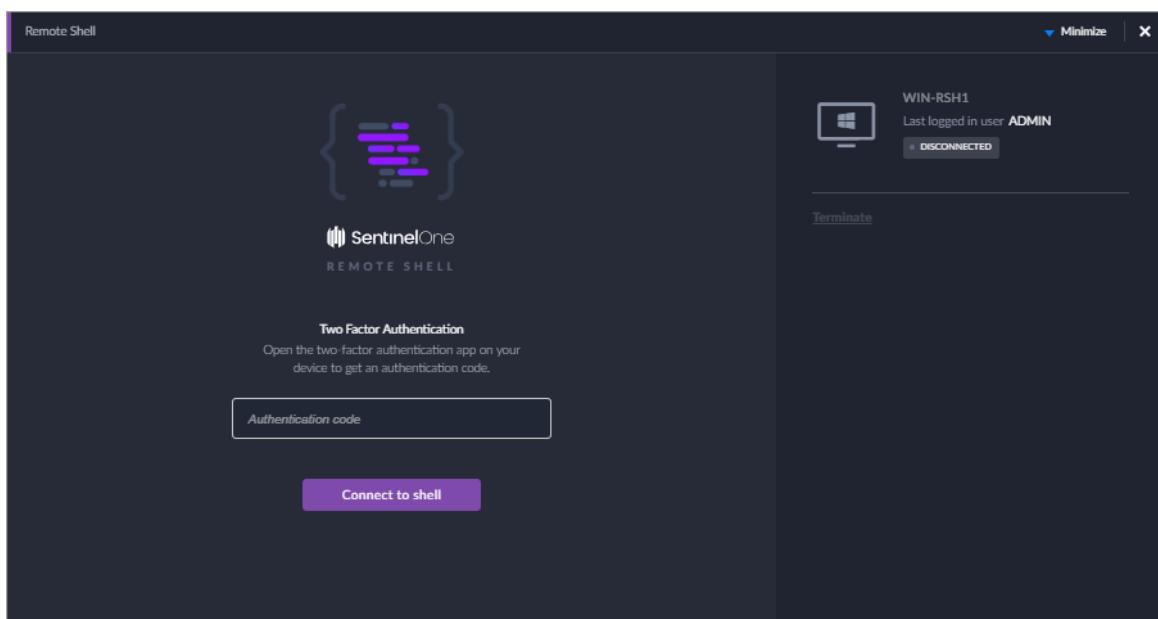


3. In the Remote shell window that opens, enter a new password that you create.

Remember the password - you will use it to open the session transcript after the session ends. To set the password, use 10 or more characters with a mix of upper and lower case letters, numbers, and symbols.

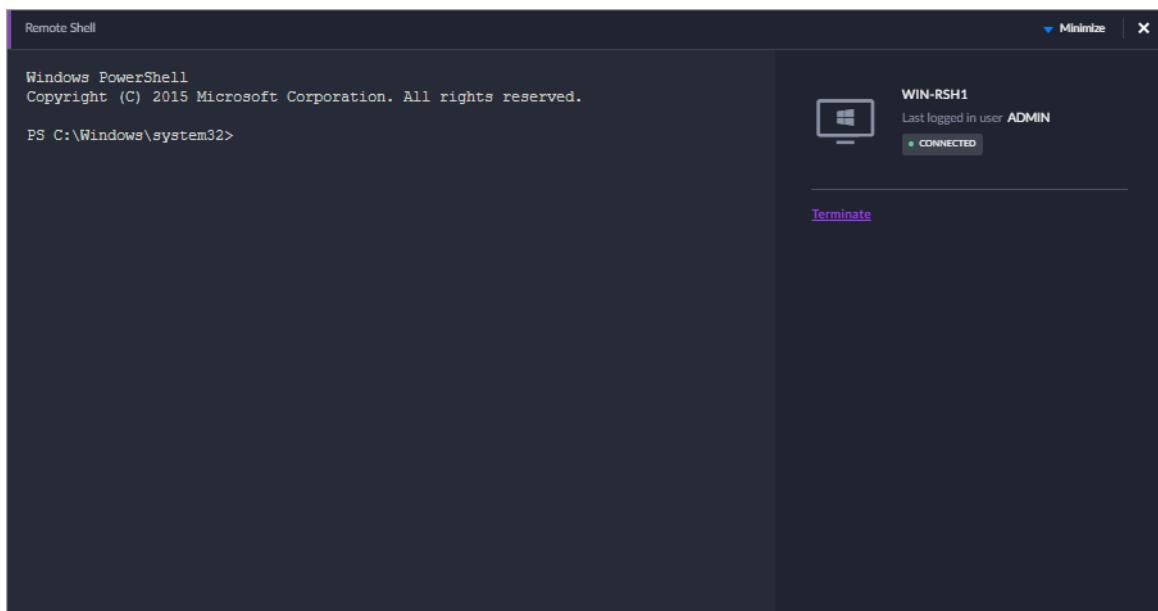


4. Click **Continue**.
5. Enter the 2FA code from the App on your phone.



6. Click **Connect to Shell**.
7. The shell opens.

Use PowerShell syntax in Windows or Bash syntax in macOS to run the desired activities.



8. Click **Terminate** when you are finished, or click the **X** to close the window.
- Idle sessions are terminated automatically after 30 minutes. A notification shows after 15 minutes of inactivity.
9. If a session is minimized, you can expand it from the Endpoint Details. Click **Expand** in the Remote Shell banner.

**ENDPOINT DETAILS**  
WIN-RSH1

**GENERAL APP INVENTORY Actions**

	Site name	Default site	Group name	Default group
Agent version	3.0.0.0 <b>UPDATED</b>		Console connectivity	<b>Online</b>
Scan status	Aborted ( Dec 27, 2018 ...)		Network status	<b>Enabled</b>
Memory	2.00 GB		Domain	<b>WORKGROUP</b>
CPU	2 X Intel(R) Xeon(R) CPU...		Subscribed on	Dec 26, 2018 18:11
Core count	2		Console visible IP	
Disk encryption	Off		IP Address	
UUID	944ab6f6f08cdc48952c...			

Network Adapters:

NAME	IP	MAC ADDRESS
Ethernet	10.0.82.128	00:50:56:91:83:99

**Remote Shell**  
Connected · Inactivity Timeout

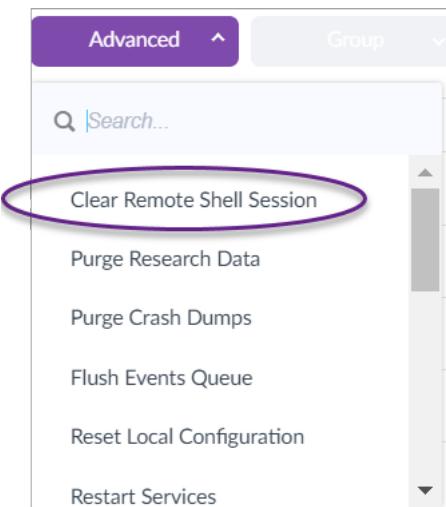
**Expand**

#### A session terminates in these situations:

- A user terminates it from the Management Console.
- The Agent goes offline.
- The Remote Shell is closed from the endpoint.
- There is a dynamic threat in the Remote Shell

#### To manually force a Remote Shell session to close:

1. In Network > Endpoints, select the endpoint.
2. Click **Advanced** and select **Clear Remote Shell Session**.



## 20.2. Remote Shell in the Activity Log

**Management:** Fuji, Grand Canyon, Houston

**Agents:** Windows 3.0+ | macOS 3.0+

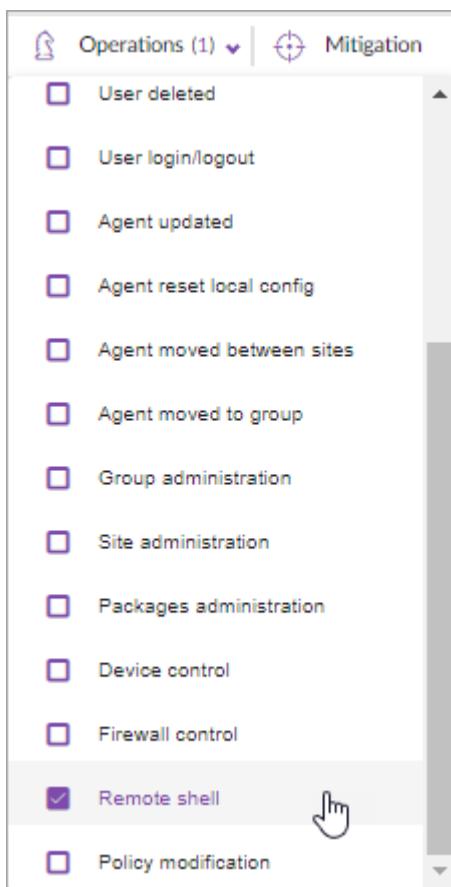
**SKU:** Complete (not available with Core)

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

**To see Remote Shell events in the Activity Log:**

1. In the sidebar, click **Activity** .
2. In the Activity Filters, click **Operations** and select **Remote Shell**.



3. These activities are reported:

- A user tries to start a Remote Shell session
- Remote Shell starts successfully.
- A user tries to terminate a session.
- A session is terminated.
- A session failed to start.
- The transcript of a session is available to download. It requires the password that was used to start the Remote Shell session.

Only users with Remote Shell permissions can download the transcript. Other users see the activity but not the download link.

# 21. SentinelOne Application Risk Management

**Management:** Fuji, Grand Canyon, Houston

**Agents:** Windows 2.6+ | macOS 2.6+

**SKU:** Complete (not available with Core)

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

**This feature is currently in EA.**

SentinelOne Application Risk lets you monitor applications installed on endpoints, from your SentinelOne Management Console.

Applications not updated with the latest patches are risky because they are vulnerable to exploits. With SentinelOne Application Risk you can see all applications that need to be patched, on all endpoints or on a specific endpoint. You can also see which endpoints have applications that need to be patched, and you can export application data.

The Agent takes a snapshot of the endpoint's 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 is supported from Fuji Management with 2.6+ Windows Agents and 2.6+ macOS Agents. It is part of the Complete SKU (not available with Core). If you have the Core bundle, you will not see Application Risk in your Management Console.

## 21.1. Managing All Risky Applications

**Management:** Fuji, Grand Canyon, Houston

**Agents:** Windows 2.6+ | macOS 2.6+

**SKU:** Complete (not available with Core)

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

**This feature is currently in EA.**

Watch: [How To Manage Risky Applications](#)

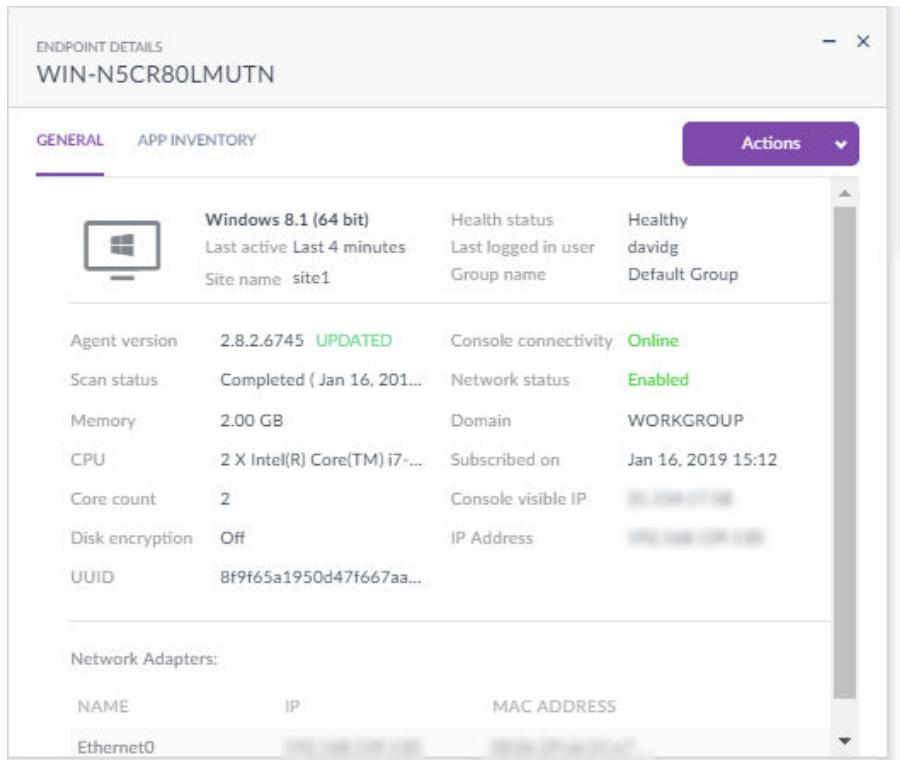
**To view all risky applications on all endpoints:**

1. In the sidebar, click **Scope**  and select a scope.
2. In the sidebar, click **Applications** .
3. The **APPLICATIONS** page shows all applications installed on all endpoints.

Select filters...							
	Type	Name	Endpoint	Risk	Installed Date	Version	Publisher
App	K-Lite Codec Pack 14.6.0 Full	WIN-NSCR80LMJTN	None	09/01/2019 02:00:00	14.6.0	KLCP	163.25 KB
App	Photo Booth	davides-Mac	None	23/08/2016 01:49:04	813	Apple Inc.	5.84 MB
App	Calculator	davides-Mac	None	20/10/2016 11:04:54	123	Apple Inc.	6.53 MB
App	iTunes	davides-Mac	None	02/11/2016 07:25:04	12.7.0	Apple Inc.	251.01 MB
App	Time Machine	davides-Mac	None	31/07/2016 03:48:53	1.3	Apple Inc.	1.24 MB
App	TextEdit	davides-Mac	None	04/08/2016 05:17:52	329	Apple Inc.	5.93 MB
App	System Preferences	davides-Mac	None	26/10/2016 01:17:46	14.0	Apple Inc.	5.72 MB
App	Stickies	davides-Mac	None	03/09/2016 03:31:55	1000	Apple Inc.	6.88 MB
App	Siri	davides-Mac	None	31/07/2016 03:48:20	1	Apple Inc.	1.78 MB
App	Reminders	davides-Mac	None	23/06/2016 03:50:33	441.11	Apple Inc.	6.26 MB

Value	Description
Type	Application

Value	Description						
Name	<p>Name of the installed application in the current scope (Global, Site, or Group). Click the application name to open the <b>APPLICATION DETAILS</b>. If the application is not up to date, click the link to open the vulnerability ID on the MITRE CVE site. From there you can patch the application, if a patch is available.</p> <div data-bbox="473 361 1346 1747" style="border: 1px solid #ccc; padding: 10px;"> <p style="text-align: center;"><b>APPLICATION DETAILS</b></p> <p><b>Microsoft Project 2000</b></p> <p>9.00.3821</p> <hr/> <p> <a href="#">WIN-N5CR80LMUTN</a></p> <hr/> <table border="0" style="width: 100%;"> <tr> <td style="width: 15%;">Size</td> <td>Type</td> <td>Publisher</td> </tr> <tr> <td>1.00 B</td> <td>App</td> <td>Microsoft Corporation</td> </tr> </table> <hr/> <p><b>CVE-2000-0419</b> Published on: <b>11/05/2000 04:00:00</b> The Office 2000 UA ActiveX Control is marked as "safe for scripting," which allows remote attackers to conduct unauthorized activities via the "Show Me" function in Office Help, aka the "Office 2000 UA Control" vulnerability. Base score: 7.5 High <a href="#">cve.mitre</a></p> <hr/> <p><b>CVE-2002-0860</b> Published on: <b>24/09/2002 04:00:00</b> The LoadText method in the spreadsheet component in Microsoft Office Web Components (OWC) 2000 and 2002 allows remote attackers to read arbitrary files through Internet Explorer via a URL that redirects to the target file. Base score: 5 Medium <a href="#">cve.mitre</a></p> <hr/> <p><b>CVE-2002-0861</b> Published on: <b>24/09/2002 04:00:00</b> Microsoft Office Web Components (OWC) 2000 and 2002 allows remote attackers to bypass the "Allow paste operations via script" setting, even when it is disabled, via the (1) Copy method of the Cell object or (2) the Paste method of the Range object. Base score: 7.5 High <a href="#">cve.mitre</a></p> <hr/> <p><b>CVE-2003-0347</b> Published on: <b>20/10/2003 04:00:00</b> Heap-based buffer overflow in VBE.DLL and VBE6.DLL of Microsoft Visual Basic for Applications (VBA) SDK 5.0 through 6.3 allows remote attackers to execute arbitrary code via a document with a long ID parameter. Base score: 10 Critical <a href="#">cve.mitre</a></p> <hr/> <p><b>CVE-2005-2127</b> Published on: <b>19/08/2005 04:00:00</b></p> </div>	Size	Type	Publisher	1.00 B	App	Microsoft Corporation
Size	Type	Publisher					
1.00 B	App	Microsoft Corporation					

Value	Description
Endpoint	Name of the endpoint. Click the endpoint link to open the <b>ENDPOINT DETAILS</b> .
	
Risk	The risk level of the applications. Low: CVSS score from 0.1 to 3.9 Medium: CVSS score from 4.0 to 6.9 High: CVSS score from 7.0 to 8.9 Critical: CVSS score from 9.0 to 10.0 No risk: The application poses no risk to the endpoint.
Installed Date	The day and time (DD/MM/YYYY HH:MM:SS) that the application was last installed or updated.
Version	The version number of the application.
Publisher	The publisher of the application (Microsoft, Apple, etc.)
Size	The size of the application.

4. Optional: Click **Select filters** to expand the filter options.

Select filters...				
Free text search	Site	OS	Machine type	Installed At
<input type="text" value="Application name"/> <input type="text" value="Type your search..."/>	site1 2	Windows 2 macOS Windows Legacy	Desktop 2 Other Laptop Server	<input type="button" value="Select"/>

Column	Description
Free text search	Search (free text), Application Name, Application Version, Publisher, Computer Name, UUID, OS Version
Site	Site name
OS	Operating System filter: Windows, macOS, Windows Legacy
Machine Type	Endpoint filter: Desktop, Laptop, Server, Other
Installed At	Date of latest application installation or update. Click <b>Select</b> to open the calendar. Select dates from the calendar and, optionally, hours within the selected dates.

5. To view applications by risk level, selecting the risk levels you want to see.



## 21.2. Managing Risky Applications Installed On One Endpoint

**Management:** Fuji, Grand Canyon, Houston

**Agents:** Windows 2.6+ | macOS 2.6+

**SKU:** Complete (not available with Core)

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

This feature is currently in EA.

Watch: [How To Manage Risky Applications](#)

### To view risky applications installed on one endpoint:

1. In the Management Console, click **NETWORK**.
2. Select an endpoint you want to analyze.

The **ENDPOINT DETAILS** window opens.

ENDPOINT DETAILS  
WIN-N5CR80LMUTN

GENERAL APP INVENTORY Actions ▾

	Windows 8.1 (64 bit) Last active Last 4 minutes Site name site1	Health status Last logged in user Group name	Healthy davidg Default Group
Agent version	2.8.2.6745 <span style="color: green;">UPDATED</span>	Console connectivity	Online
Scan status	Completed ( Jan 16, 201...	Network status	Enabled
Memory	2.00 GB	Domain	WORKGROUP
CPU	2 X Intel(R) Core(TM) i7-...	Subscribed on	Jan 16, 2019 15:12
Core count	2	Console visible IP	[REDACTED]
Disk encryption	Off	IP Address	[REDACTED]
UUID	8f9f65a1950d47f667aa...		

Network Adapters:

NAME	IP	MAC ADDRESS
Ethernet0	[REDACTED]	[REDACTED]

3. In the Endpoint Details window of the endpoint, click **Actions > Show Applications**.

**ENDPOINT DETAILS**  
**WIN-N5CR80LMUTN**

**GENERAL APP INVENTORY**

	Windows 8.1 (64 bit) Last active Last 4 minutes Site name site1	Health status Last logged in u... Group name
Agent version	2.8.2.6745 <b>UPDATED</b>	Console connectio...
Scan status	Completed ( Jan 16, 2019)	Network status
Memory	2.00 GB	Domain
CPU	2 X Intel(R) Core(TM) i7-...	Subscribed on
Core count	2	Console visible
Disk encryption	Off	IP Address
UUID	8f9f65a1950d47f667aa...	

**Network Adapters:**

NAME	IP	MAC ADD
Ethernet0		

**Actions**

- Disconnect From Network
- Fetch Logs
- Initiate Scan
- Move To Another Site
- Move To Another Site
- Reboot
- Remote Shell
- Show Applications
- Show Passphrase

The **APPLICATIONS** page shows all applications installed on the selected endpoint.

UUID: 8f9f65a1950d47f667aa...							
<input type="radio"/> Low (0) <input type="radio"/> Medium (5) <input type="radio"/> High (3) <input checked="" type="radio"/> Critical (2) <input type="radio"/> No risk (247,181)							
Type	Name	Endpoint	Risk	Installed Date	Version	Publisher	Size
App	Microsoft Project 2000	WIN-N5CR80LMUTN	Critical	08/05/2016 03:00:00	9.00.3821	Microsoft Corporation	1.00 B
App	Microsoft Office PowerPoint ...	WIN-N5CR80LMUTN	Critical	08/03/2016 02:00:00	11.0.8305.0	Microsoft Corporation	1.00 B
App	Microsoft Exchange Server 2...	WIN-N5CR80LMUTN	Critical	06/02/2017 02:00:00	15.1.225.42	Microsoft Corporation	1.00 B
App	Microsoft Digital Image Suite...	WIN-N5CR80LMUTN	Critical	14/01/2019 02:00:00	11.0.0422	Microsoft Corporation	1.00 B
App	Ethereal 0.99.0	WIN-N5CR80LMUTN	Critical	08/03/2016 02:00:00	0.99.0	The Ethereal developer comm...	1.00 B
App	Adobe PageMaker 7.0	WIN-N5CR80LMUTN	Critical	08/05/2016 03:00:00	7.0.2	Adobe Systems, Inc.	1.00 B
App	Adobe Acrobat 5.0	WIN-N5CR80LMUTN	Critical	08/03/2016 02:00:00	5.0	Adobe Systems, Inc.	1.00 B
App	2007 Microsoft Office system	WIN-N5CR80LMUTN	Critical	06/02/2017 02:00:00	12.0.6612.1000	Microsoft Corporation	1.00 B
App	Wireshark 2.0.3 (64-bit)	WIN-N5CR80LMUTN	High	14/01/2019 02:00:00	2.0.3	The Wireshark developer co...	1.00 B
App	Microsoft SharePoint Server ...	WIN-N5CR80LMUTN	High	08/03/2016 02:00:00	16.0.4351.1000	Microsoft Corporation	1.00 B

4. To filter the applications list by risk level, select the risk levels you want to see.

<input type="radio"/> Low (0)	<input type="radio"/> Medium (5)	<input type="radio"/> High (3)	<input checked="" type="radio"/> Critical (2)	<input type="radio"/> No known risk (247,181)
-------------------------------	----------------------------------	--------------------------------	---	---

- Low: CVSS score from 0.1 to 3.9
- Medium: CVSS score from 4.0 to 6.9
- High: CVSS score from 7.0 to 8.9
- Critical: CVSS score from 9.0 to 10.0
- No known risk: The application poses no risk to the endpoint.

## 21.3. Exporting Application Data

**Management:** Fuji, Grand Canyon, Houston

**Agents:** Windows 2.6+ | macOS 2.6+

**SKU:** Complete (not available with Core)

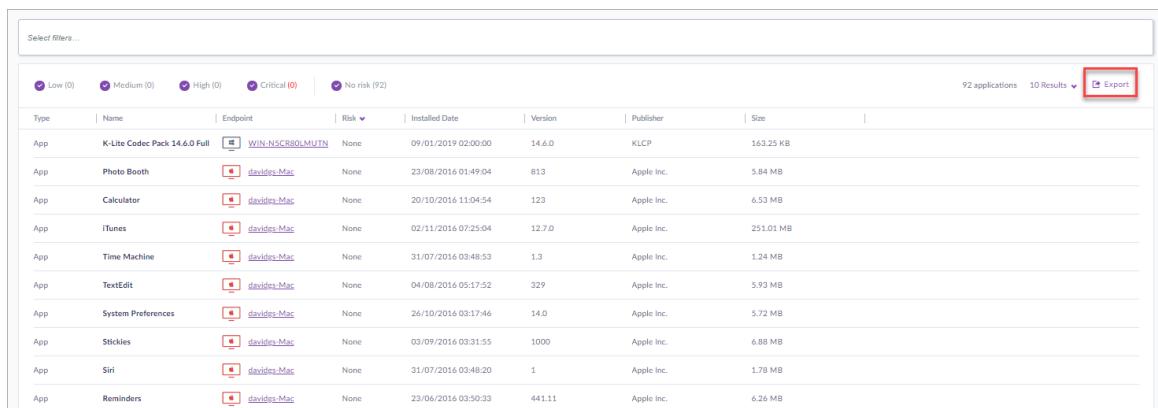
**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

This feature is currently in EA.

To export application data:

1. In the sidebar, click **Scope**  and select a scope.
2. In the sidebar, click **Applications** .
3. Click **Export**. A CSV file downloads containing the application data that appears on the screen.



The screenshot shows a table of applications. At the top, there are filters for Low (0), Medium (0), High (0), Critical (0), and No risk (92). On the right, it says 92 applications, 10 Results, and an **Export** button. The table has columns for Type, Name, Endpoint, Risk, Installed Date, Version, Publisher, and Size. The data includes:

Type	Name	Endpoint	Risk	Installed Date	Version	Publisher	Size
App	K-Lite Codec Pack 14.6.0 Full	WIN-NSCR80LMUTN	None	09/01/2019 02:00:00	14.6.0	KLCP	163.25 KB
App	Photo Booth	davides-Mac	None	23/08/2016 01:49:04	813	Apple Inc.	5.84 MB
App	Calculator	davides-Mac	None	20/10/2016 11:04:54	123	Apple Inc.	6.53 MB
App	iTunes	davides-Mac	None	02/11/2016 07:25:04	12.7.0	Apple Inc.	251.01 MB
App	Time Machine	davides-Mac	None	31/07/2016 03:48:53	1.3	Apple Inc.	1.24 MB
App	TextEdit	davides-Mac	None	04/08/2016 05:17:52	329	Apple Inc.	5.93 MB
App	System Preferences	davides-Mac	None	26/10/2016 03:17:46	14.0	Apple Inc.	5.72 MB
App	Stickies	davides-Mac	None	03/09/2016 03:31:55	1000	Apple Inc.	6.88 MB
App	Siri	davides-Mac	None	31/07/2016 03:48:20	1	Apple Inc.	1.78 MB
App	Reminders	davides-Mac	None	23/06/2016 03:50:33	441.11	Apple Inc.	6.26 MB

The data exported to the Application Risk CSV file: Application ID, Name, Version, Publisher, OS, Installed, Size, Signed, Risk, Machine Type, Agent UUID, Agent name, Agent version, and CVE IDs.

## 22. Location Aware Firewall

**Management:** Grand Canyon, Houston

**Agents:** Windows 3.2+ | macOS 3.2+

**SKU:** Complete (not available with Core)

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

Starting from version Grand Canyon, admins can configure customized sets of Agent Locations based on one or more endpoint network parameters. Agents detect which location they are in and act accordingly.

Agents can be in multiple locations at the same time.

In Grand Canyon the Agent location can affect which Firewall Control rules an Agent uses, as each Firewall rule can be configured for a specific location.

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.

Locations can be defined for a Site, Account, or Globally.

**Define a location with one or more of these network identifiers:**

- **IP Address** - Do the endpoint's IP addresses match the defined IP addresses?
- **DNS Server** - Do the endpoint's DNS servers match the defined DNS servers?
- **DNS Resolution** - Can the endpoint resolve the defined DNS hostnames?
- **Network Interface** - Is the endpoint's current internet connection wired or wireless?
- **SentinelOne Connection** - Is the endpoint currently connected to a SentinelOne server?
- **Registry Key** - Does the defined registry exist on the endpoint?

**Define how each location is determined:**

- All parameters are true
- At least one parameter is true
- No defined parameters are true

### 22.1. Configuring Locations

**Management:** Grand Canyon, Houston

**Agents:** Windows 3.2+ | macOS 3.2+

**SKU:** Complete (not available with Core)

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

See the locations for a scope and configure new locations in **Settings > Locations**.



For each location define one or more parameters, and the relationship between them: If all, one, or no parameters must be true for an endpoint to be in the location.

### To define a new location:

1. In the sidebar, click **Scope**  and select a scope.
2. In the sidebar, click **Settings** .
3. In the **Settings** toolbar, click **Locations**.
4. Click **New Location**.



5. In the **General** page of the new location, define:
  - **Location Name** - Name of the location that shows wherever the location is used in the Management Console.
  - **Description** - A more complete description that shows in the **Locations** page. Add here information about the location that is important for Admins to know.
  - **An endpoint is in this location if:** Select what is necessary for an endpoint to be considered in this location.
    - **At least one parameter is true** - The endpoint must match one or more of the network identifiers that you defined for this location.

For example: If you defined an IP Address range and a DNS server, the endpoint is in this location if the DNS Server matches the endpoint but the IP address does not.

- **All parameters are true** - The endpoint must match all of the network identifiers that you defined for this location.

For example: If you defined an IP Address range and a DNS server, the endpoint is in this location if its IP address is in the defined range AND the DNS server matches.

- **No parameters are true** - The endpoint must NOT match any network identifiers that you defined for this location.

For example: If you defined an IP Address range and a DNS server, the endpoint is in this location if its IP address is not in the range AND it does not have a matching DNS server.

- Select a parameter from the list and define it.

New Location

Define one or more parameters for this location

An endpoint is in this location if: At least one parameter is true [Change](#)

General	<a href="#">+</a> Add more
IP Address	<input checked="" type="radio"/> One of the endpoint's IP addresses matches a defined IP <input type="radio"/> All of the endpoint's IP addresses match a defined IP <input checked="" type="radio"/> None of the endpoint's IP addresses match a defined IP
DNS Server	
DNS Resolution	
Network Interface	
SentinelOne Connection	
Registry Key	

[Save](#) [Cancel](#)

See [Defining Specific Location Parameters \[392\]](#).

- Define more parameters, if necessary.
- Review the details of the defined location. Make sure that the **An endpoint is in this location if:** setting is correct. To edit it, click **Change** or go to the **General** page.

New Location

Define one or more parameters for this location

An endpoint is in this location if: At least one parameter is true [Change](#)

General	<a href="#">+</a> Add more
---------	----------------------------

- Click **Save**.

The defined location shows in the **Locations** list.

Locations						
New location		Actions	No Items Selected			
Name	Description	Creation Time	Created By	Last Update Time	Last Updated By	Scope Name
Fallback	The Fallback location contain...					
<input type="checkbox"/> Global Location A	A Global Location	Apr 28, 2019 10:28:06	Yonatan klein	Apr 28, 2019 10:28:06	Yonatan klein	Global

### To delete a location:

- You cannot delete a location if it is used in a Firewall rule.

If a location is used in one or more Firewall rules, the deletion fails.

- You can delete a location if Agents are in the location.

The Agents will move to a different defined location or to the Fallback location.

1. In the **Locations** list, select a location.
2. Click **Actions > Delete**.

## 22.2. Defining Specific Location Parameters

**Management:** Grand Canyon, Houston

**Agents:** Windows 3.2+ | macOS 3.2+

**SKU:** Complete (not available with Core)

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

You can define multiple parameters for each location.

### IP Address

Do the endpoint's IP addresses match the defined IP addresses?

The endpoint compares all of its active IP addresses to the IP addresses, Ranges, and CIDRs defined for the location.

For example, if the location's setting is, **All of the endpoint's IP addresses match the defined IPs**, every active IP address on the endpoint must be mapped to at least one of the IP addresses in the location's definition.

Addresses can be IPv4 or IPv6. You can add up to five address fields.

1. Click .
2. In **Type**, select **Address, CIDR, or Range**.

New Location

Define one or more parameters for this location

An endpoint is in this location if: At least one parameter is true [Change](#)

General	<input type="text"/> <input checked="" type="radio"/> All of the endpoint's IP addresses match a defined IP <input type="radio"/> One of the endpoint's IP addresses matches a defined IP <input type="radio"/> None of the endpoint's IP addresses match a defined IP	Delete
IP Address (1)	<input type="text"/> <div style="border: 1px solid #ccc; padding: 2px; display: inline-block;"> <span style="font-size: 1.5em;">+</span> Add more       </div>	
DNS Server		
DNS Resolution		
Network Interface		
SentinelOne Connection		
Registry Key		

**Save** **Cancel**

3. Enter the information in the field or fields shown.
4. To add another IP Address, CIDR, or Range, click + Add more.
5. Select if one, all, or none of the endpoint's IP addresses to match the defined addresses.

## DNS Server

Do the endpoint's DNS servers match the defined DNS servers?

The endpoint compares all of its configured DNS servers to those defined for the location.

Addresses can be IPv4 or IPv6. You can add up to five address fields.

1. Click + Add more.
2. In **Type**, select **Address**, **CIDR**, or **Range**.

New Location

Define one or more parameters for this location

An endpoint is in this location if: At least one parameter is true [Change](#)

General	<input type="text" value="Address"/> 	Delete
IP Address (1)	<input type="text" value="CIDR"/>	
DNS Server (1)	<input checked="" type="radio"/> One of the endpoint's DNS Servers matches the defined DNS server <input type="radio"/> All of the endpoint's DNS Servers match a defined DNS server <input type="radio"/> None of the endpoint's DNS Servers match a defined DNS server	
DNS Resolution		
Network Interface		
SentinelOne Connection		
Registry Key		

**Save** **Cancel**

3. Enter the information in the field or fields shown.
4. To add another IP Address, CIDR, or Range, click .
5. Select if one, all, or none of the endpoint's DNS Servers need to match the defined DNS Server or Servers.

## DNS Resolution

Can the endpoint resolve the defined DNS host names?

The endpoint checks if it can resolve the provided Host name, by doing a DNS query using OS services.

The Host name must be in FQDN format. The Resolved IP can be IPv4 or IPv6. You can add up to five Host name and IP pairs.

1. Click .
2. Enter a **Host name** and a **Resolved IP**, that the host name should resolve to.

New Location

Define one or more parameters for this location

An endpoint is in this location if: At least one parameter is true [Change](#)

General	<input type="text" value="Host name"/> Host name	<input type="text" value="Resolved IP"/> Resolved IP	<a href="#">Delete</a>
IP Address (1)	<a href="#">+ Add more</a>		
DNS Server (1)			
<b>DNS Resolution (1)</b>	<input type="radio"/> Endpoint can resolve at least one DNS hostname <input checked="" type="radio"/> Endpoint can resolve all DNS hostnames <input type="radio"/> Endpoint cannot resolve any DNS hostname		
Network Interface			
SentinelOne Connection			
Registry Key			

[Save](#) [Cancel](#)

3. To add another **Host name** and a **Resolved IP**, click [+ Add more](#).
4. Select if endpoints must be able to resolve one, all, or none of the defined DNS hostnames.

## Network Interface

Is the endpoint's current internet connection wired or wireless?

**Note:** If one of the connected interfaces is wireless, the endpoint is considered connected with wireless

A connection is considered **Wireless** if:

- **Windows Agents** - At least one NDIS Interface Type is one of: IF\_TYPE\_PROP\_WIRELESS\_P2, IF\_TYPE\_PROP\_DOCS\_WIRELESS\_MACLAYE, IF\_TYPE\_PROP\_DOCS\_WIRELESS\_DOWNSTREAM, IF\_TYPE\_PROP\_DOCS\_WIRELESS\_UPSTREA, IF\_TYPE\_IEEE80211, IF\_TYPE\_WWANPP, IF\_TYPE\_WWANPP2
- **macOS Agents** - At least one NDIS Interface Type is one of: kSCNetworkInterfaceTypeIEEE80211, kSCNetworkInterfaceTypeWWAN, kSCNetworkInterfaceTypeBluetooth

1. Move the toggle to turn on the Network Interface setting.

New Location

Define one or more parameters for this location

An endpoint is in this location if: At least one parameter is true [Change](#)

General	<input checked="" type="checkbox"/> Endpoint's current connection to the network: <input type="radio"/> Wireless <input checked="" type="radio"/> Wired
IP Address (2)	
DNS Server (1)	
DNS Resolution (1)	If one of the connected interfaces is wireless, the endpoint is considered connected with wireless
<b>Network Interface</b>	
SentinelOne Connection	
Registry Key	

**Save**   **Cancel**

## 2. Select **Wireless** or **Wired**.

**Note:** If one of the connected interfaces is wireless, the endpoint is considered connected with wireless

### SentinelOne Connection

Is the endpoint currently connected to a SentinelOne server?

## 1. Move the toggle to turn on the SentinelOne Management setting.

New Location

Define one or more parameters for this location

An endpoint is in this location if: At least one parameter is true [Change](#)

General	<input checked="" type="checkbox"/> Endpoint's current connection to the network: <input type="radio"/> Wireless <input checked="" type="radio"/> Wired
IP Address (1)	
DNS Server (1)	
DNS Resolution (1)	If one of the connected interfaces is wireless, the endpoint is considered connected with wireless
<b>Network Interface</b>	
SentinelOne Connection	
Registry Key	

**Save**   **Cancel**

## 2. Select Connected or Disconnected.

### Registry Key

Does the defined registry exist on the endpoint in HKEY\_LOCAL\_MACHINE\SOFTWARE?

If you enter a key that is in a different location, the location will not be saved.

1. In **Key name**, enter a Registry Key that must exist or not exist in the endpoint's registry, HKEY\_LOCAL\_MACHINE\SOFTWARE.

The screenshot shows the 'New Location' dialog box. On the left is a sidebar with tabs: General, IP Address (1), DNS Server (1), DNS Resolution (1), Network Interface, SentinelOne Connection, and Registry Key. The Registry Key tab is selected and highlighted in purple. The main area has a heading 'Define one or more parameters for this location' and a note 'An endpoint is in this location if: At least one parameter is true' with a 'Change' link. It contains fields for 'Key name' (with a placeholder 'I'), 'Value (optional)', and 'Data (optional)'. Below these fields is a note: 'The Registry Key condition is matched if the Key exists. If you enter a Value or Data, the Key must exist with the defined Value and/or Data.' A callout box states: 'This applies to Windows endpoints. macOS endpoints ignore this parameter.' At the bottom are 'Save' and 'Cancel' buttons.

2. Optional: In **Value name**, enter a value that the key must have.
3. Optional: In **Data**, enter data that the key must contain.

## 22.3. Using Locations in Firewall Rules

**Management:** Grand Canyon, Houston

**Agents:** Windows 3.2+ | macOS 3.2+

**SKU:** Complete (not available with Core)

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

From Management version Grand Canyon with 3.2 Windows and macOS Agents, you can create a Location aware Firewall policy. Define customized sets of Agent Locations [389], based on one or more endpoint network parameters, and use the Locations in Firewall rules.

By default, SentinelOne Firewall Control rules apply in **All** locations. To create a location aware Firewall policy, configure Agent Locations in **Settings >Locations** and create Firewall rules that apply for different locations.

**Important:** Agents earlier than version 3.2 do not support Locations in Firewall Rules. When Firewall Control is enabled, 3.1.x and earlier Windows and macOS Agents only apply Firewall rules that are set for **All** locations.

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.

See [SentinelOne Firewall Control](#) for complete Firewall information.

#### Notes:

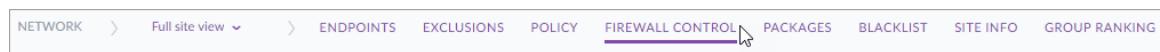
Agents use the Firewall Control rules for all the Locations that they match, based on the priority of the Firewall rules.

After you configure locations in Firewall rules, make sure the order of the rules still meets your needs.

Make sure to define some rules for the **Fallback** location, or for **All** locations.

#### To add locations to a Firewall rule:

1. In the sidebar, click **Network** .
2. In the sidebar, click **Scope**  and select a scope.
3. Click **Firewall Control**.



4. Click **New rule** or double-click an existing rule to edit it.
5. In the Rule parameters, click **+** next to **Locations** to expand it.

New Rule X

**Block File Share**

Os Type Windows  
Action Block  
Scope Site 260

**Rule parameters**  
Tip! You can press tab to move to the next parameter

---

Protocol +

---

Application Any +

---

Direction Any +

---

Local host Any +

---

Local port Any +

---

Remote host Any +

---

Remote port Any +

---

Locations All + 

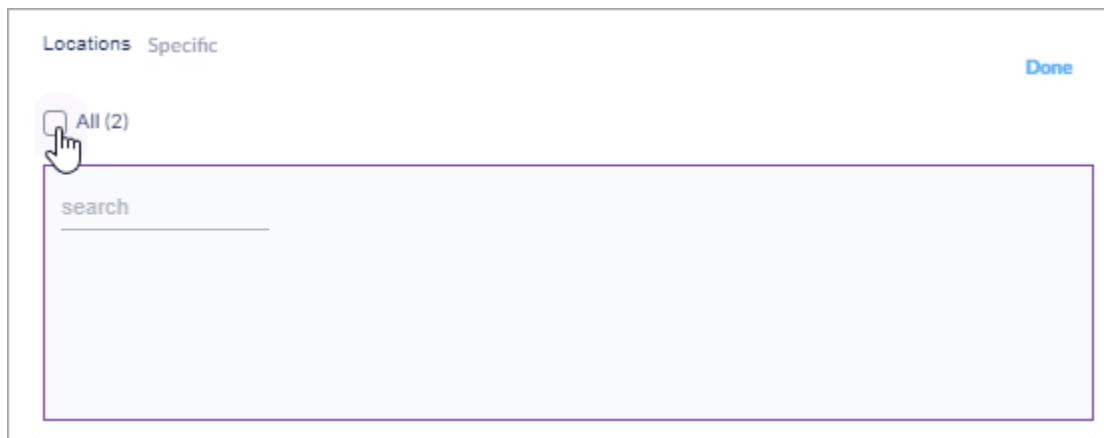
---

Enable rule immediately after saving

Save rule

Back | Quit

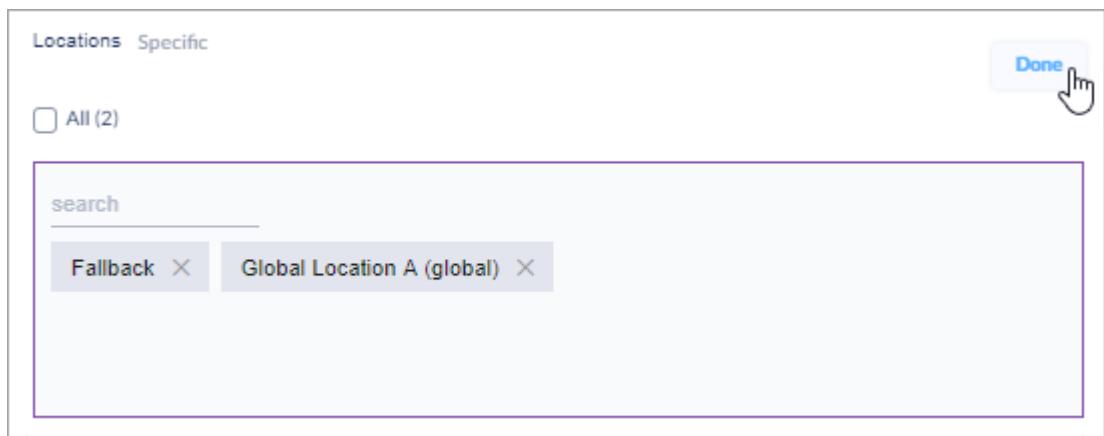
6. Uncheck the **All** option to select one or more specific Locations for the rule.



7. Start to type a Location name to see the defined locations that match. Select a Location.



8. Optional: Select more Locations.
9. After you add the desired Location or Locations, click **Done**.



10. Click **Save rule**.

## 22.4. Seeing an Endpoint's Location

**Management:** Grand Canyon, Houston

**Agents:** Windows 3.2+ | macOS 3.2+

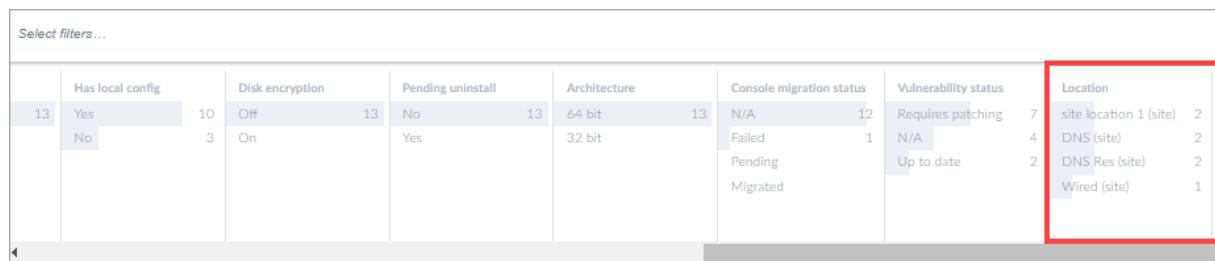
**SKU:** Complete (not available with Core)

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

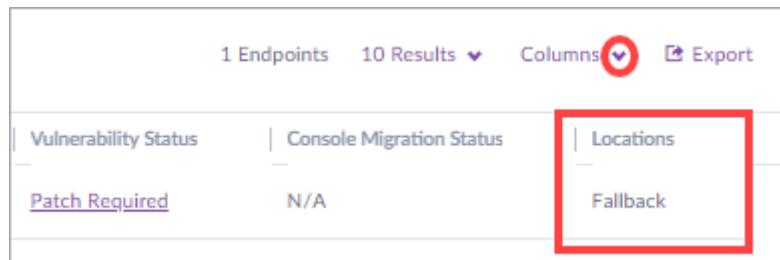
See the detected location of each endpoint in the **Network** view.

You can filter endpoints by location.



	Has local config	Disk encryption	Pending uninstall	Architecture	Console migration status	Vulnerability status	Location
13	Yes No	Off On	10 13	No Yes	13 32 bit	N/A Failed Pending Migrated	12 1 Up to date
							7 4 2 1 site location 1 (site) 2 DNS (site) 2 DNS Res (site) 2 Wired (site) 1

A **Locations** column is available. Scroll right to see it, or open the **Columns** list to select the columns to show in your **Network** view.



1 Endpoints 10 Results ▾ Columns  Export

Vulnerability Status	Console Migration Status	Locations
<a href="#">Patch Required</a>	N/A	Fallback

**Tip:** From version Grand Canyon, you can drag and drop the columns in the **Network** to change the order and customize your view.

Each endpoint's location shows in the Endpoint Details.

	Site name	Group name	
Agent version	3.2.1.17 <span style="color: green;">UPDATED</span>	Console connectivity	<span style="color: red;">Offline</span>
Scan status	In Progress ( May 02, 20...	Network status	<span style="color: green;">Enabled</span>
Memory	2.00 GB	Domain	WORKGROUP
CPU	2 X Intel(R) Xeon(R) CPU...	Subscribed on	May 02, 2019 11:13
Core count	2	Console visible IP	
Disk encryption	Off	IP Address	
UUID	3ee9c584ea8f4bf28156	Locations	<span style="color: red;">fallback</span>

Network Adapters:

NAME	IP	MAC ADDRESS
------	----	-------------

You can also use [Sentinelctl \[403\]](#) to see an endpoint's detected location.

## 22.5. Agent Calculation of its Location

**Management:** Grand Canyon, Houston

**Agents:** Windows 3.2+ | macOS 3.2+

**SKU:** Complete (not available with Core)

**Minimum Admin Scope:** Site Admin

**Scope:** Selected Site, Account, or Global

Each Agent gets the list of locations defined for its Site and Account and the Global locations.

Agents can be in multiple locations at the same time.

Agents use the Firewall Control rules for all the Locations that they match, based on the priority of the Firewall rules.

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.

**An Agent recalculates its location when:**

- A location is added or deleted from the **Locations** list in the Management.
- An Agent connects to or disconnects from the SentinelOne Management.
- The endpoint restarts.

- The Agent reloads.
- The endpoint's list of active network interfaces changes.
- One of the endpoint's IP addresses is updated.
- A Registry Key that is included in a location's definition changes (Windows only).

## 22.6. Sentinelctl commands for Locations

### Command for Windows

Also see [sentinelctl on Windows Agents](#).

#### 22.6.1. get\_current\_location

**Purpose** Shows the locations that the endpoint (version 3.2+) currently detects it is in, by ID. To see the Location names, use `-n`.

**Note:** From Agent version 3.3.x, a passphrase is not required for the command.

**Synopsis** `sentinelctl get_current_locations [-n] -k "passphrase"`

`-n` Shows the name of the location in addition to its ID number.

**Example**

```
In this example, the endpoint detects that it is in three
Locations:
>sentinelctl get_current_locations -n -k "LARK BIYF MALI SUCH STAG
HIM CAIN"
Agent Locations:
  611165040623490581      New York Office
  611189007128204829      Global location
  620034797837752430      Development Dept.

In this example, the endpoint does not detect that it is in a
configured Location:
>sentinelctl get_current_locations -n -k "LARK BIYF MALI SUCH STAG
HIM CAIN"
Agent Locations:
  Fallback
```

### Commands for macOS

Also see [sentinelctl on macOS Agents](#).

#### 22.6.2. locations current list

**Purpose** Shows the locations that the macOS endpoint (version 3.2+) currently detects it is in.

**Synopsis** `sentinelctl locations current list`

**Example**

```
In this example, the endpoint detects that it is in three
Locations:
>sudo sentinelctl locations current list
```

611165040623490581	New York Office
611189007128204829	Global location
620034797837752430	Development Dept.

In this example, the endpoint does not detect that it is in a configured Location:

```
>sudo sentinelctl locations current list  
Agent Locations:  
    Fallback
```

### 22.6.3. locations rules dump

**Purpose** Shows all possible locations available for the mac OS endpoint (version 3.2+) from the Management.

**Synopsis** `sentinelctl locations rules dump`

**Example** `sudo sentinelctl locations rules dump`

## 23. Getting Logs for Support [Multi-Site]

**Management:** Central Park, Denali, Eiffel, Fuji, Grand Canyon, Houston

**Agents:** All

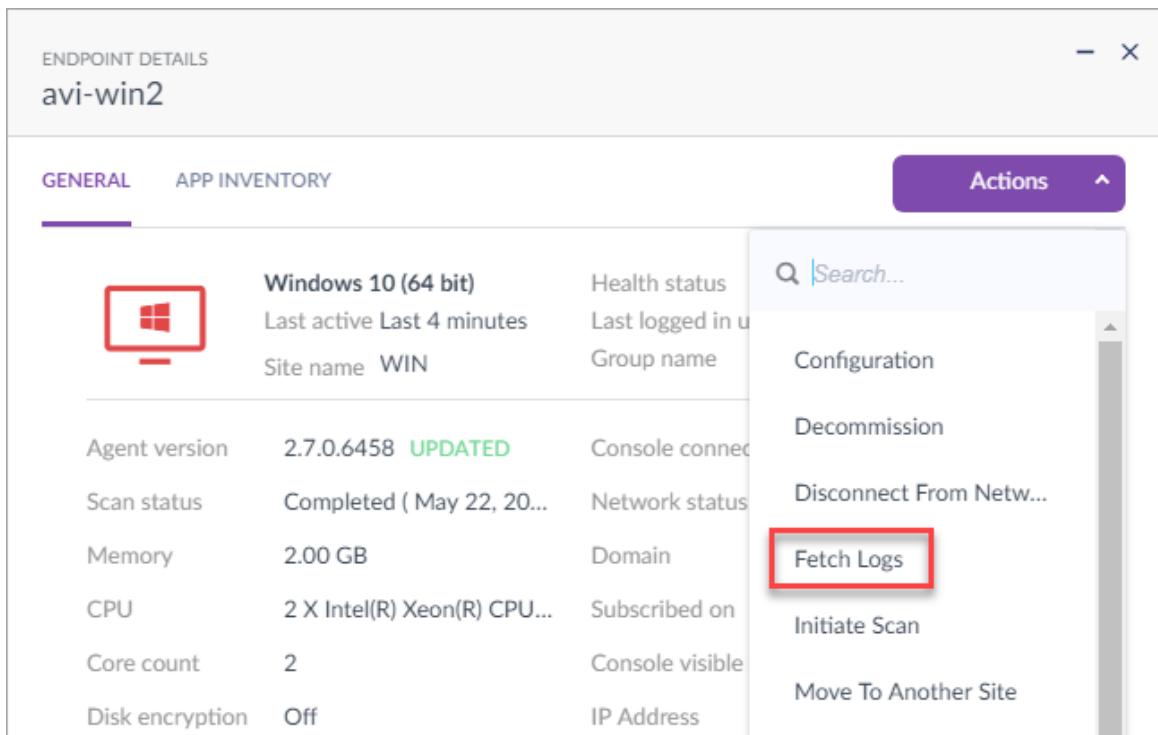
If SentinelOne Support asks for logs from Agents, use one of these procedures. The logs show Agent operations. The logs are encrypted and only Support can read them.

You can get logs from the Management Console or manually from an Agent.

[Watch: How to Get Logs for Support](#)

**To get logs for one Agent from the Management Console:**

1. In the sidebar, click **Network** .
  2. Click the Agent.
- Endpoint Details** loads.
3. Click **ACTIONS** and then click **Fetch Logs**.



The screenshot shows the 'ENDPOINT DETAILS' view for an agent named 'avi-win2'. The interface includes tabs for 'GENERAL' and 'APP INVENTORY'. On the right, there's a 'Actions' dropdown menu with the following options:

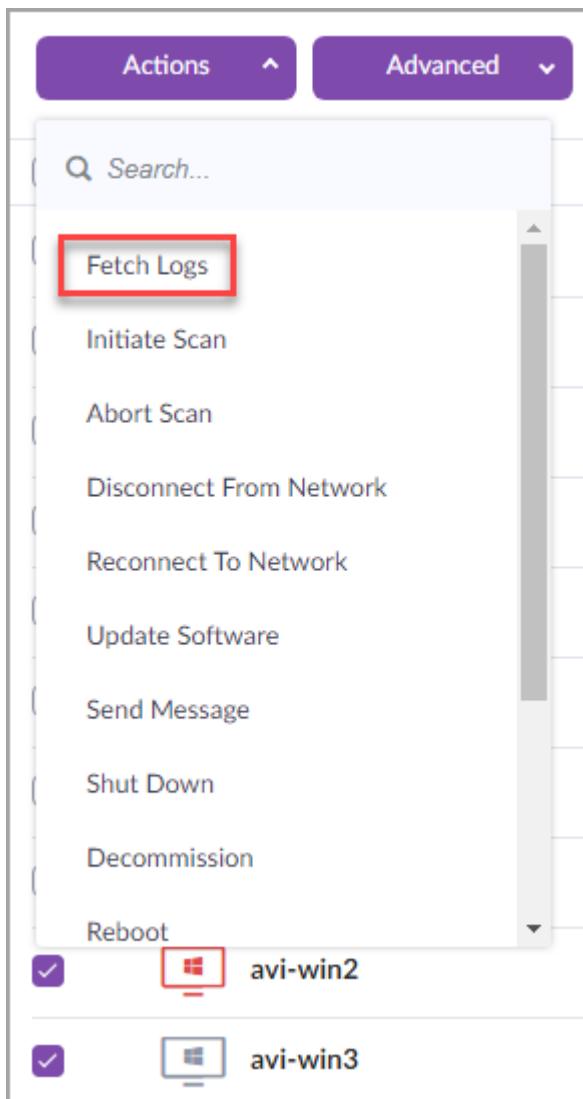
- Search...
- Configuration
- Decommission
- Disconnect From Network
- Fetch Logs** (highlighted with a red box)
- Initiate Scan
- Move To Another Site

Category	Value	Details
Operating System	Windows 10 (64 bit)	Health status: Last logged in user
Site name	WIN	Group name
Agent version	2.7.0.6458 <span>UPDATED</span>	Console connected
Scan status	Completed ( May 22, 20... )	Network status
Memory	2.00 GB	Domain
CPU	2 X Intel(R) Xeon(R) CPU...	Subscribed on
Core count	2	Console visible
Disk encryption	Off	IP Address

**To get logs for multiple Agents from the Management Console:**

1. In the sidebar, click **Network** .
2. Select the Agents.

3. Click **ACTIONS** and select **Fetch Logs**.



### To download the fetched logs:

If you have an On-Prem Management Console, download the log file and send it to Support. If you have a cloud-based Management Console, Support can get your fetched logs from the Cloud.

1. In the sidebar, click **Activity** .
2. In the **ACTIVITY** view, click **Administrative** and select **Log operations**.

The screenshot shows the 'Activity Log' section of the SentinelOne interface. At the top, there are filters for 'Malware', 'Exclusion', 'Operations', 'Mitigation', and 'Administrative'. A dropdown menu for 'Administrative' is open, showing five items: 'Administrative', 'Agent subscribed', 'Uninstall', 'Log operations' (which is selected, indicated by a checkmark and a hand cursor icon), 'Fetch files operations', and 'Agent decommissioned'. The main area displays a list of log entries, each with a timestamp, source, and a long log message. To the right of each entry is a small download icon, which is circled in red in several instances.

The results show entries with this syntax: Agent <name> successfully uploaded <file>.tar.gz

3. Select an entry and click the **Download** button.

This screenshot is similar to the one above, showing the 'Activity Log' section. The 'Log operations' filter is selected. The list of log entries includes download icons next to the log messages. Nine of these download icons are circled in red, indicating they are the targets for manual collection.

### Manual Log Collection

- **Windows Agents:** In C:\ProgramData\Sentinel\logs, zip the BINLOG files
- **macOS Agents logs:** Use [sentinelctl](#): sudo sentinelctl logreport and get the log files on the desktop.  
Or get the endpoint logs with the macOS Log Collection command.

- **Linux Agents:** Run `sudo /etc/init.d/sentineld fetch_logs` and see the location of the log files in the output.
- **Management logs:** Run `sudo /sentinel/webservice/scripts/sentinel.sh logreport` and see the location of the log files in the output.