



# ArcSight SOAR 3.11

Software Version: 3.11

## Integration Guides

Document Release Date: February 2024

Software Release Date: February 2024

## Legal Notices

Open Text Corporation  
275 Frank Tompa Drive, Waterloo, Ontario, Canada, N2L 0A1

## Copyright Notice

Copyright 2024 Open Text.

The only warranties for products and services of Open Text and its affiliates and licensors ("Open Text") are as may be set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Open Text shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

## Trademark Notices

"OpenText" and other Open Text trademarks and service marks are the property of Open Text or its affiliates. All other trademarks or service marks are the property of their respective owners.

## Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number
- Document Release Date, which changes each time the document is updated
- Software Release Date, which indicates the release date of this version of the software

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

<https://www.microfocus.com/support-and-services/documentation>

# Contents

Integration Guide for AbuselPDB .....	26
Integration Overview .....	26
Integration Capabilities .....	26
Prerequisites .....	26
Configuration .....	26
Configuring AbuselPDB .....	26
Configuring SOAR .....	26
Capabilities .....	27
Integration Guide for AlientVault OTX .....	29
Integration Overview .....	29
Integration Capabilities .....	29
Configuration .....	29
Configuring SOAR .....	30
Additional Notes .....	31
Integration Guide for Amazon AWS CloudTrail .....	32
Overview of the Plugin .....	32
Integration Capabilities .....	32
Prerequisites .....	33
Configuration .....	33
Configuring Amazon CloudTrail Logs .....	33
Configuring SOAR .....	34
Integration Capabilities: .....	34
Integration Guide for Amazon AWS Lambda .....	42
Integration Overview .....	42
Integration Capabilities .....	42
Prerequisites .....	42
Configuring Amazon AWS Lambda .....	42
Configuring SOAR .....	43
Capabilities .....	44
Integration Guide for Amazon EC2 .....	46
Integration Overview .....	46
Integration Capabilities .....	46
Configuration .....	46

Prerequisites .....	46
Configuring on Amazon AWS .....	46
Configuring on SOAR .....	51
Additional Notes .....	52
Integration Guide for Amazon GuardDuty .....	53
Integration Overview .....	53
Integration Capabilities .....	53
Prerequisites .....	54
Configuration .....	54
Configuring Amazon GuardDuty .....	54
Configuring SOAR .....	55
Capabilities .....	55
Integration Guide for Amazon IAM .....	71
Integration Overview .....	71
Integration Capabilities .....	71
Configuration .....	72
Configuring SOAR .....	72
Capabilities .....	73
Integration Guide for Amazon S3 .....	91
Integration Overview .....	91
Integration Capabilities .....	91
Prerequisites .....	91
Configuration .....	91
Configuring SOAR .....	91
Capabilities .....	92
Integration Guide for APIVoid .....	96
Integration Overview .....	96
Integration Capabilities .....	96
Prerequisites .....	96
Configuration .....	97
Configuring APIVoid .....	97
Configuring SOAR .....	97
Capabilities .....	97
Integration Guide for Anomali ThreatStream .....	109
Integration Overview .....	109
Integration Capabilities .....	109

Configuration .....	110
Prerequisites .....	110
Configuring Anomali ThreatStream .....	110
Configuring SOAR .....	110
Additioinal Notes .....	112
Integration Guide for Arbor Networks APS .....	114
Integration Overview .....	114
Integration Capabilities .....	114
Configuration .....	114
Prerequisites .....	114
Configuring Arbor Networks APS .....	114
Configuring SOAR .....	115
Integration Guide for AWS Network Firewall .....	116
Integration Overview .....	116
Integration Capabilities .....	116
Prerequisites .....	116
Configuration .....	117
Configuring AWS Network Firewall .....	117
Configuring SOAR .....	118
Capabilities .....	119
Integration Guide for Azure Network Security Groups .....	126
Integration Overview .....	126
Integration Capabilities .....	126
Prerequisites .....	126
Configuration .....	127
Configuring Microsoft Azure Network Security .....	127
Configuring SOAR .....	128
Capabilities .....	129
Integration Guide for Bind RPZ DNS .....	134
Integration Overview .....	134
Integration Capabilities .....	134
Configuration .....	134
Prerequisites .....	134
Configuring SOAR .....	134
Integration Guide for BMC Discovery .....	136
Integration Overview .....	136

Integration Capabilities .....	136
Prerequisites .....	136
Configuration .....	136
Configuring BMC Discovery .....	136
Configuring SOAR .....	137
Integration Capabilities: .....	137
Integration Guide for BMC Helix ITSM .....	140
Integration Overview .....	140
Integration Capabilities .....	140
Prerequisites .....	141
Configuration .....	141
Configuring BMC Helix ITSM .....	141
Configuring SOAR .....	141
Integration Capabilities: .....	142
Integration Guide for BMC Helix Remedyforce .....	147
Configuring BMC Helix Remedyforce .....	148
Configuring SOAR .....	148
Capabilities .....	149
Integration Guide for Carbon Black Response (EDR) .....	162
Integration Overview .....	162
Integration Capabilities .....	162
Prerequisites .....	163
Configuring Carbon Black Response(EDR) .....	163
Configuring SOAR .....	163
Additional Notes .....	165
Integration Guide for Cofense Triage .....	166
Integration Overview .....	166
Integration Capabilities .....	166
Prerequisites .....	167
Configuration .....	167
Configuring Cofense Triage .....	167
Configuring SOAR .....	167
Integration Capabilities .....	168
Integration Guide for Check Point R80 .....	177
Integration Overview .....	177
Integration Capabilities .....	177

Prerequisites .....	177
Configuration .....	177
Configuring Check Point R80 .....	177
Configuring SOAR .....	178
Capabilities .....	180
Integration Guide for Check Point SandBlast .....	183
Integration Overview .....	183
Integration Capabilities .....	183
Configuration .....	183
Prerequisites .....	183
Configuring Check Point SandBlast .....	183
Configuring SOAR .....	184
Integration Guide for CiscoASA Firewall .....	186
Integration Capabilities .....	186
Prerequisites .....	186
Configuration .....	186
Configuring Cisco ASA Firewall .....	186
Configuring SOAR .....	187
Capabilities .....	188
Integration Guide for Cisco Firepower Management Center .....	189
Integration Overview .....	189
Integration Capabilities .....	189
Prerequisites .....	189
Configuration .....	189
Configuring Cisco Firepower Management Center .....	189
Configuring SOAR .....	191
Capabilities .....	192
Integration Guide for Cisco Identity Service Engine .....	194
Integration Overview .....	194
Integration Capabilities .....	194
Configuration .....	194
Prerequisites .....	194
Configuring Cisco Identity Services Engine .....	194
Configuring SOAR .....	194
Integration Guide for Cisco Ironport Email Security .....	196
Integration Overview .....	196

Integration Capabilities .....	196
Configuration .....	196
Prerequisites .....	196
Configuring Cisco Ironport Email Security .....	196
Configuring SOAR .....	197
Additional Notes .....	197
Integration Guide for Cisco SecureX .....	198
Integration Overview .....	198
Supported Integration Capabilities .....	198
Prerequisites .....	199
Configuration .....	199
Configuring Cisco SecureX .....	199
Configuring SOAR .....	200
Integration Capabilities: .....	201
Integration Guide for Cisco Umbrella .....	207
Integration Overview .....	207
Integration Capabilities .....	207
Prerequisites .....	208
Configuration .....	208
Configuring Cisco Umbrella .....	208
Configuring SOAR .....	208
Integration Capabilities .....	209
Integration Guide for CrowdStrike Falcon .....	217
Integration Overview .....	217
Integration Capabilities .....	217
Prerequisites .....	218
Configuration .....	218
Configuring CrowdStrike .....	218
Configuring SOAR .....	218
Capabilities .....	219
Integration Guide for Cyberark Central Credential Provider .....	225
Integration Overview .....	225
Configuration .....	225
Prerequisites .....	225
Configuring CyberArk Application Identity Manager .....	225
Configuring SOAR .....	226
Additional Notes .....	227

Integration Guide for CYMRU Malware Hash Registry Query .....	228
Integration Overview .....	228
Integration Capabilities .....	228
Configuration .....	228
Configuring CYMRU Malware Hash Registry Query .....	228
Configuring SOAR .....	228
Integration Guide for Cymru Malware Hash Registry .....	229
Integration Overview .....	229
Integration Capabilities .....	230
Prerequisites .....	230
Configuration .....	230
Configuring Team Cymru Malware Hash Registry V2 .....	230
Configuring SOAR .....	230
Integration Capabilities: .....	231
CyberRes Galaxy Threat Accelerator .....	234
Integration Overview .....	234
Integration Capabilities .....	234
Prerequisites .....	234
Configuring CyberRes Galaxy Threat Accelerator .....	234
Configuring SOAR .....	234
Capabilities .....	235
Integration Guide for CyThreat Threat Intelligence .....	238
Integration Overview .....	238
Integration Capabilities .....	238
Alert Source Capability .....	238
Prerequisites .....	238
Configuration .....	239
Configuring SOAR .....	239
Configuring CyThreat as an Alert Source .....	240
Integration Capabilities .....	241
Integration Guide for DomainTools .....	242
Integration Overview .....	242
Integration Capabilities .....	242
Configuration .....	243
Configuring DomainTools .....	243
Configuring SOAR .....	243
Capabilities .....	244

Integration Guide for DNS Service .....	253
Integration Overview .....	253
Integration Capabilities .....	253
Configuration .....	253
Prerequisites .....	253
Configuring DNS Service .....	253
Configuring SOAR .....	253
Integration Guide for EmailRep .....	255
Integration Overview .....	255
Integration Capabilities .....	255
Prerequisite .....	255
Configuring SOAR .....	255
Capabilities .....	256
Integration Guide for EnCase Endpoint Security .....	258
Integration Overview .....	258
Integration Capabilities .....	258
Prerequisites .....	259
Configuration .....	259
Configuring SOAR .....	260
Integration Capabilities: .....	260
Integration Guide for ESB Karar .....	271
Integration Guide for F5 Big-IP Advanced Firewall Manager .....	273
Integration Overview .....	273
Integration Capabilities .....	273
Configuration .....	273
Configuring F5 Big-IP Advanced Firewall Manager .....	273
Integration Guide for FireEye HX .....	275
Integration Overview .....	275
Integration Capabilities .....	275
Enrichment .....	275
Action .....	275
Configuring FireEye HX .....	275
Configuring SOAR .....	275
Integration Guide for Forcepoint Cloud Services .....	278
Integration Overview .....	278
Integration Capabilities .....	278

Configuration .....	278
Configuring Forcepoint Cloud Services .....	278
Configuring SOAR .....	278
Integration Guide for Forcepoint Content Gateway .....	280
Integration Overview .....	280
Integration Capabilities .....	280
Configuration .....	280
Prerequisites .....	280
Configuring Facepoint Web Content Gateway .....	281
Configuring SOAR .....	281
Integration Guide for ForeScout CounterACT NAC .....	284
Integration Overview .....	284
Integration Capabilities .....	284
Configuration .....	284
Prerequisites .....	284
Configuring ForeScout CounterACT NAC .....	285
Configuring SOAR .....	287
Additional Notes .....	289
Integration Guide for Fortinet Forti Manager V2 .....	290
Integration Overview .....	290
Integration Capabilities .....	290
Prerequisites .....	290
Configuration .....	291
Configuring Forti Manager .....	291
Configuring SOAR .....	291
Capabilities .....	291
Integration Guide for Fortinet FortiAnalyzer .....	294
Integration Overview .....	294
Integration Capabilities .....	294
Configuring Fortinet FortiAnalyzer .....	294
Configuring SOAR .....	294
Integration Guide for Fortinet FortiDDoS .....	297
Integration Overview .....	297
Integration Capabilities .....	297
Configuration .....	297
Prerequisites .....	297

Configuring FortiDDoS .....	297
Configuring SOAR .....	298
Integration Guide for Fortinet FortiGate API .....	301
Integration Overview .....	301
Integration Capabilities .....	301
Configuration .....	301
Prerequisites .....	301
Configuring Fortinet FortiGate .....	301
Configuring SOAR .....	304
Additional Notes .....	305
Integration Guide for Fortinet FortiMail .....	306
Integration Overview .....	306
Integration Capabilities .....	306
Configuration .....	306
Prerequisites .....	306
Configuring FortiMail .....	306
Configuring SOAR .....	308
Additional Notes .....	310
Integration Guide for Fortinet FortiManager .....	311
Integration Overview .....	311
Integration Capabilities .....	311
Prerequisites .....	311
Configuring FortiManager .....	312
Configuring SOAR .....	313
Additional Notes .....	314
Integration Guide for Fortinet FortiSandbox .....	315
Integration Overview .....	315
Integration Capabilities .....	315
Configuration .....	315
Prerequisites .....	315
Configuring Fortinet Sandbox .....	315
Configuring SOAR .....	317
Integration Guide for FraudGuard .....	319
Integration Capabilities .....	319
Prerequisites .....	319
Configuring FraudGuard .....	319

Configuring SOAR .....	320
Capabilities .....	321
Integration Guide for FTP Server .....	325
Integration Overview .....	325
Integration Capabilities .....	325
Configuration .....	325
Prerequisites .....	325
Configuring SOAR .....	325
Integration Guide for Google Cloud Compute .....	327
Integration Overview .....	327
Integration Capabilities .....	327
Prerequisites .....	327
Configuration .....	327
Configuring Google Cloud Compute .....	327
Configuring SOAR .....	330
Integration Capabilities: .....	331
List Instance .....	331
Get Instance Details .....	332
Get IAM Policy .....	333
Get Screenshot .....	334
Start Instance .....	335
Stop Instance .....	335
Suspend Instance .....	336
Integration Guide for Have I Been Pwned .....	338
Integration Overview .....	338
Integration Capabilities .....	338
Prerequisites .....	338
Configuration .....	338
Configuring SOAR .....	338
Capabilities .....	339
Integration Guide for Generic HTTP SMS Gateway .....	342
Integration Overview .....	342
Integration Capabilities .....	342
Configuration .....	342
Configuring Generic HTTP SMS Gateway .....	342
Configuring SOAR .....	342

Integration Guide for HTTP Proxy .....	344
Integration Overview .....	344
Configuration .....	344
Prerequisites .....	344
Configuring HTTP Proxy .....	344
Configuring SOAR .....	344
Integration Guide for IBM Security X-Force .....	346
Integration Overview .....	346
Integration Capabilities .....	346
Configuration .....	346
Prerequisites .....	346
Configuring IBM X-Force Exchange .....	347
Configuring SOAR .....	347
Integration Guide for Infoblox DNS Firewall .....	350
Integration Overview .....	350
Integration Capabilities .....	350
Configuration .....	350
Prerequisites .....	350
Configuring Infoblox DNS Firewall .....	350
Configuring SOAR .....	351
Integration Guide for Intezer .....	353
Integration Overview .....	353
Integration Capabilities .....	354
Prerequisites .....	354
Configuration .....	354
Configuring Intezer .....	354
Configuring SOAR .....	354
Capabilities .....	355
Integration Guide for Invictus USTA ThreatIntelligence .....	359
Integration Overview .....	359
Integration Capabilities .....	359
Configuration .....	359
Prerequisites .....	359
Configuring Invictus USPA .....	360
Configuring SOAR .....	360
Configuring Invictus USTA as Alert Source .....	360

Configuring Invictus USTA as Integration .....	361
Additional Notes .....	362
Integration Guide for IPInfo .....	363
Integration Overview .....	363
Integration Capabilities .....	363
Configuration .....	363
Capabilities .....	364
Integration Guide for Jira .....	366
Integration Overview .....	366
Integration Capabilities .....	366
Prerequisites .....	366
Configuration .....	366
Configuring SOAR .....	366
Configuring Jira .....	368
Capabilities .....	368
Integration Guide for JDBC(Database) Server .....	371
Integration Capabilities .....	371
Configuration .....	371
Prerequisites .....	371
Configuring Database Server .....	371
Configuring SOAR .....	371
Integration Guides for Kannel SMS Gateway .....	374
Integration Overview .....	374
Integration Capabilities .....	374
Supported Action Capabilities .....	374
Configuring Kannel SMS Gateway .....	374
Configuring SOAR .....	374
Integration Guide for Kaspersky Security Center .....	376
Configuration on Kaspersky Security Center .....	376
Configuring SOAR .....	376
Optional configuration .....	377
Overriding built-in scripts .....	377
Get Task Names .....	378
Get Group Names .....	379
Get Tag Names .....	379
Host Information Enrichment .....	380

Block Hash Action Capability .....	382
Rollback of block hash capability .....	383
Add tag to host capability .....	384
Rollback of Add Tag to Host Capability .....	385
Move system to group capability .....	386
Run task capability .....	387
Integration Guide for MAY Siber Scop NET .....	389
Prerequisites .....	389
Configuring MAY Siber Scop NET .....	389
Configuring SOAR .....	389
Integration Guide for McAfee ePolicy Orchestrator .....	391
Prerequisites .....	391
Configuration on McAfee ePolicy Orchestrator .....	392
Configuring SOAR .....	392
Integration Guide for McAfee Network Security Platform (IPS) .....	394
Configuration .....	394
Configuration on McAfee Network Security Platform (IPS) .....	394
Configuring SOAR .....	395
Integration Guide for McAfee Web Gateway .....	397
Prerequisites .....	397
Configuration on McAfee Web Gateway .....	397
Configuration on SOAR .....	398
Integration Guide for McAfee Web Gateway v2 .....	399
Configuring McAfee Web Gateway v2 .....	399
Configuring SOAR .....	399
Capabilities .....	401
Integration Guide for Micro Focus ArcSight ESM .....	406
Integration Guide for ArcSight Intelligence .....	406
Integration Guide for Micro Focus ArcSight Logger .....	407
Configuration .....	407
Prerequisites .....	407
Configuration on Micro Focus ArcSight Logger .....	407
Configuring SOAR .....	408
Configuring SOAR .....	408
Integration Guide for Microsoft Active Directory .....	410

Configuration .....	410
Prerequisites .....	410
Configuration on Microsoft Active Directory .....	411
Configuring SOAR .....	411
Integration Guide for Microsoft Azure Active Directory .....	413
Integration Overview .....	413
Integration Capabilities .....	413
Prerequisites .....	413
Configuration .....	414
Configuring Microsoft Azure .....	414
Configuring SOAR .....	414
Capabilities .....	415
Integration Guide for Microsoft Defender for CloudApps .....	423
Integration Overview .....	423
Integration Capabilities .....	423
Prerequisites .....	424
Configuration .....	424
Configuring Microsoft Defender for CloudApps .....	424
Configuring SOAR .....	425
Capabilities .....	426
Integration Guide for Microsoft Defender Endpoint .....	439
Integration Overview .....	439
Integration Capabilities .....	439
Prerequisites .....	440
Configuring Microsoft Defender .....	440
Configuring SOAR .....	441
Capabilities .....	442
Integration Guide for OpenText IT Service Manager .....	453
Integration Overview .....	453
Integration Capabilities .....	453
Prerequisites .....	453
Configuration .....	453
Configuring OpenText IT Service Manager .....	453
Configuring SOAR .....	454
Capabilities .....	455
Integration Guide for OpenText UCMDDB .....	457

Integration Overview .....	457
Integration Capabilities .....	457
Prerequisites .....	457
Configuration .....	457
Configuring OpenText UCMDB .....	457
Configuring SOAR .....	458
Capabilities .....	459
Integration Guide for Microsoft Exchange .....	462
Prerequisites .....	462
Configuration on Microsoft Exchange .....	462
Configuration on SOAR .....	463
Additional Notes .....	464
Integration Guide for Microsoft Office365 Exchange EWS .....	465
Configuration on Microsoft Exchange .....	466
Using OAuth2 with Microsoft Exchange online Integrations .....	466
Configuring SOAR .....	467
Additional Notes .....	468
Integration Guide for Microsoft Teams .....	469
Integration Overview .....	469
Integration Capabilities .....	469
Prerequisites .....	470
Configuration .....	470
Configuring Microsoft Teams .....	470
Authentication Parameters .....	470
Configuring SOAR .....	471
Integration Capabilities .....	471
Integration Guide for Microsoft Windows DNS Server .....	485
Configuration on Microsoft Windows DNS Server .....	485
Configuring ATAR .....	485
Integration Guide for Microsoft Windows Services (WinRM) .....	487
Configuration on Microsoft Windows Services .....	487
Configuring SOAR .....	487
Integration Guide for Microsoft Graph Security .....	489
Integration Overview .....	489
Integration Capabilities .....	489
Prerequisites .....	489

Configuration .....	490
Configuring Microsoft Azure .....	490
Configuring SOAR .....	490
Capabilities .....	491
Integration Guide for MISP .....	501
Integration Overview .....	501
Integration Capabilities .....	501
Prerequisites .....	501
Integration Guide for MxToolBox .....	504
Integration Overview .....	504
Integration Capabilities .....	504
Prerequisites .....	504
Configuration .....	504
Configuring MxToolBox .....	504
Configuring SOAR .....	505
Capabilities .....	506
Integration Guide for Netskope v1 .....	507
Overview of the Plugin .....	507
Supported Integration Capabilities .....	507
Prerequisites .....	507
Configuration .....	508
Configuring Netskope .....	508
Configuring SOAR .....	508
Integration Capabilities: .....	509
Integration Guide for Netskope V2 .....	511
Integration Overview .....	511
Integration Capabilities .....	511
Prerequisites .....	512
Configuration .....	512
Configuring Netskope .....	512
Configuring SOAR .....	513
Integration Capabilities: .....	513
Integration Guide for Okta .....	518
Integration Overview .....	518
Integration Capabilities .....	518
Prerequisites .....	519

Configuration .....	520
Configuring SOAR .....	520
Capabilities .....	521
Integration Guide for Ones BioAffix .....	532
Integration Capabilities .....	532
Prerequisites .....	532
Configuration on Ones BioAffix .....	532
Configuring SOAR .....	532
Additional Notes .....	533
Integration Guide for OpenText Network Detection and Response .....	534
Integration Overview .....	534
Integration Capabilities .....	534
Prerequisites .....	534
Configuration .....	534
Configuring Opentext Network Detection and Response .....	534
Configuring SOAR .....	535
Capabilities .....	535
Integration Guide for Palo Alto Networks AutoFocus .....	540
Prerequisites .....	540
Configuration on Palo Alto Networks AutoFocus .....	541
Configuring SOAR .....	541
Integration Guide for Palo Alto Networks Firewall .....	542
Prerequisites .....	543
Configuration on Palo Alto Networks Firewall (API) .....	543
Configuring SOAR .....	543
Additional Notes .....	544
Integration Guide for Palo Alto Networks Panorama .....	545
Prerequisites .....	545
Configuration on Palo Alto Networks Panorama .....	545
Configuration on SOAR .....	546
Integration Guide for Qualys VM .....	547
Integration Overview .....	547
Integration Capabilities .....	547
Prerequisites .....	548
Configuration .....	548
Configuring Qualys VM .....	548

Configuring SOAR .....	549
Integration Capabilities: .....	549
Integration Guide for Recorded Future .....	562
Prerequisites .....	562
Configuration on Recorded Future .....	563
Configuring SOAR .....	563
Integration Guide for Robtex Lookup .....	565
Configuration on Robtex Lookup .....	565
Configuring SOAR .....	565
Integration Guide for Roksit DNS Firewall .....	567
Prerequisites .....	567
Configuration on Roksit DNS Firewall .....	567
Configuring SOAR .....	567
Integration Guide for RSA Security Analytics .....	569
Prerequisites .....	569
Configuration on RSA Security Analytics Suite .....	570
Configuring SOAR .....	570
Integration Guide for SailPoint .....	571
Integration Overview .....	571
Integration Capabilities .....	571
Configuration .....	571
Configuring on SailPoint .....	571
Configuring SOAR .....	572
Capabilities .....	573
Integration Guide for SentinelOne .....	577
Overview of the Plugin .....	577
Integration Capabilities .....	578
Prerequisites .....	578
Configuration .....	578
Configuring SentinelOne .....	578
Configuring SOAR .....	579
Integration Capabilities: .....	579
Integration Guide for ServiceNow .....	592
Integration Overview .....	592
Integration Capabilities .....	592
Prerequisites .....	592

Configuring ServiceNow .....	592
Configuring ServiceNow with OAuth2 .....	598
Configuring SOAR .....	598
Capabilities .....	599
Integration Guide for ServiceNow CMDB .....	601
Integration Overview .....	601
Integration Capabilities .....	601
Integration Configuration .....	601
Integration Capabilities: .....	603
Integration Guide for Slack .....	606
Integration Overview .....	606
Integration Capabilities .....	606
Prerequisites .....	606
Configuring Slack .....	607
Configuring SOAR .....	607
Capabilities .....	608
Integration Guide for SMTP Mail Server .....	612
Prerequisites .....	612
Configuration .....	612
Configuring SOAR Email Notification .....	612
Configuring SOAR .....	612
Additional Notes .....	614
Integration Guide for Sophos XG Firewall .....	615
Prerequisites .....	615
Configuration on Sophos XG Firewall .....	615
Integration Guide for SORBS Query .....	618
Configuration on SORBS Query .....	618
Configuring SOAR .....	618
folIntegration Guide for Symantec Advanced Threat Protection .....	620
Configuring Symantec Advanced Threat Protection .....	620
Configuring SOAR .....	620
Configuring SOAR .....	620
Integration Guide for Symantec Bluecoat Malware Analysis Appliance (MAA) .....	622
Prerequisites .....	622
Configuring SOAR .....	622
Integration Guide for Symantec BlueCoat Proxy SG .....	623

Prerequisites .....	624
Configuring SOAR .....	624
Configuring Symantec BlueCoat Proxy SG .....	627
Integration Guide for Symantec Bluecoat Site Review .....	629
Configuration on Bluecoat Site Review .....	629
Configuring SOAR .....	629
Integration Guide for Symantec Data Loss Prevention (DLP) .....	630
Integration Capabilities .....	630
Prerequisites .....	630
Configuring Symantec DLP .....	630
Configuring SOAR .....	631
Integration Guide for Symantec DeepSight Intelligence .....	633
Prerequisites .....	633
Configuring Symantec DeepSight Intelligence .....	634
Configuring SOAR .....	634
Configuring Symantec DeepSight Intelligence as Alert Source .....	635
Configuring Symantec DeepSight Intelligence as Integration .....	635
Integration Guide for Symantec Endpoint Protection Manager .....	637
Prerequisites .....	637
Configuring Symantec Endpoint Protection Manager .....	638
Configuring SOAR .....	638
Integration Guide for Symantec Managed Security Services (MSS) .....	641
Configuring Symantec MSS .....	642
Configuring SOAR .....	642
Configuring Credentials .....	642
Configuring Symantec MSS as Alert Source .....	643
Configuring Symantec MSS as an Integration .....	645
Additional Notes .....	645
Integration Guide for Symantec Messaging Gateway .....	647
Prerequisites .....	647
Configuring Symantec Messaging Gateway .....	647
Configuring SOAR .....	648
Integration Guide for Tenable Nessus .....	650
Configuring Tenable Nessus .....	650
Configuration on SOAR .....	650
Configuring SOAR .....	650

Integration Guide for Tenable Security Center .....	652
Prerequisites .....	652
Configuring Tenable Security Center .....	652
Configuring SOAR .....	653
Integration Guide for Trend Micro Apex Central .....	654
Integration Overview .....	654
Integration Capabilities .....	654
Prerequisites .....	654
Configuring Trend Micro Apex Central .....	654
Configuring SOAR .....	655
Capablities .....	656
Integration Guide for Trend Micro Vision One .....	657
Integration Overview .....	657
Integration Capabilities .....	657
Configuration .....	657
Configuring Trend Micro Vision One .....	657
Configuring SOAR .....	658
Capabilities .....	659
Integration Guide for Turkcell Threat Intelligence .....	665
Prerequisites .....	665
Configuration on Turkcell Threat Intelligence or Bozok .....	665
Configuring SOAR .....	666
Integration Guide for Udger .....	668
Integration Overview .....	668
Integration Capabilities .....	668
Prerequisites .....	668
Configuration .....	668
Configuring Udger .....	668
Configuring SOAR .....	668
Capabilities .....	669
Integration Guide for Urlscan .....	671
Integration Overview .....	671
Integration Capabilities .....	671
Configuration .....	671
Configuring SOAR .....	671
Capabilities .....	672

Integration Guide for VirusTotal .....	677
Prerequisites .....	677
Configuring VirusTotal .....	678
Configuring SOAR .....	678
Additional Notes .....	680
Integration Guide for VMware ESXi .....	681
Configuring VMware ESXi .....	681
Configuring SOAR .....	681
Integration Guide for VxStream Sandbox .....	683
Configuration on VxStream Sandbox .....	683
Configuring SOAR .....	683
Integration Guide for WinRM .....	685
Configuring SOAR .....	687
Configuring Domain-Controller for WinRM HTTPS Transport .....	687
Force Group Policy Update .....	689
Additional Notes .....	689
Send Documentation Feedback .....	690

# Integration Guide for AbuseIPDB

## Integration Overview

**Abuse Intelligence Production Data Base ( Abuse IPDB)** is a project dedicated to help combating the spread of hackers, spammers, and abusive activity on the internet.

## Integration Capabilities

ArcSight SOAR has the following integration capabilities with AbuseIPDB:

- Check IP
- Report IP

## Prerequisites

You must have access to HTTPS as the ArcSight SOAR connects to AbuseIPDB API through this service.

## Configuration

### Configuring AbuseIPDB

1. Navigate to [AbuseIPDB](#) create an account.
2. Click API tab and create an API key.

### Configuring SOAR

1. Click **Configuration > Credential > Create Credential**.
2. Specify the following parameter values in the **Credential Editor**:

Type	Name	Username	Password	Private Key
Internal credential	Display name of credential set (for example, AbuseIPDB Credential).			Create API key

3. Click **Configuration > Integrations > Create Integration**.

4. Specify the following parameter values in the **Configuration Form**.

Parameter	Value	
Name	Display name of the integration.	
Type	AbuseIPDB	
Address	<a href="https://api.abuseipdb.com">https://api.abuseipdb.com</a>	
Configuration	Specify the following configuration parameters:	
	<b>max.age.in.days</b>	The <b>max.age.in.days</b> parameter determines how far back in time go to fetch reports [1, 365]. For example, <b>max.age.in.days=30</b>
	<b>cache.reusing.duration</b>	configure how far (in minutes) into the past this enrichment will look. For example, <b>cache.reusing.duration=20</b>
	<b>proxy.id</b>	ID of the Proxy integration if you access AbuseIPDB through a web proxy device. For example, <b>proxy.id = 12345</b>
Credential	Credential that has been defined for this integration in the <b>Credentials</b> menu.	
Trust Invalid SSL Certificates	Select this option if web server's certificate is self-signed or is not recognized by browsers.	
Require Approval From	Select user(s) from list to ask the approval before executing actions on this integration.	
Notify	Select user(s) from the list to notify when SOAR performs an action on this integration.	

5. Click **Save** to save the integration definition.
6. Navigate to **Configuration>Customization Library** and edit **AbuseIPDB Advanced Action Script Default Template**.
7. Select the integration that you have added in **Integrations** menu.
8. Click **Save** to complete the integration.
9. Click **Test**, an **Integration Successful** message is displayed if the credential and address are valid.

## Capabilities

### 1. Check IP

Enrichment capability for getting details about the IP.

The following table presents the **Check IP** capability details:

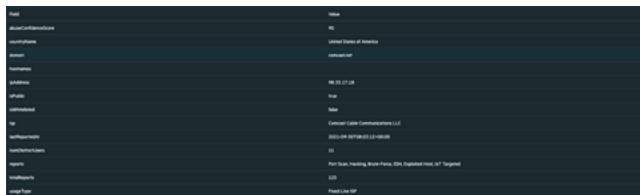
Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
Integration	Name of the third party integration.	Integration	No	Yes
Max Age in Days	The max.age.in.days parameter determines how far back in time go to fetch reports.	Text	No	No
IP	IP to be checked.	Network Address	Yes	Yes

**Output:**

Case Scope:

Action	Type	Category/ Value
Add	Scope Item	Keyword (Related)

Human Readable Output:

**2. Report IP**

Action capability for reporting an IP address:

Rollback : No

Duplicate Check: No

The following table provides the Report IP action capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
IP	IP to be reported.	Network Access	Yes	Yes
Category	Category of reported IP.	Enum	No	Yes
Comment	Comment for reported IP.	Text	No	No

**Output:**

Case Scope:

Action	Type	Category/ Value
Add	Scope Item	Keyword (Related)

Human Readable Output: N/A

# Integration Guide for AlienVault OTX

## Integration Overview

**AlienVault OTX** is an open threat exchange platform supported by AlienVault and the community.

## Integration Capabilities

ArcSight SOAR has the following integration capabilities with AlienVault OTX:

- IP Indicator
- Hash Indicator
- URL Indicator
- Domain Indicator
- Hostname Indicator

### **Use Case: Enrichment of artifacts detected in the organization**

SOAR, when integrated with AlienVault OTX, can search for an artifact and gather information such as related threats and recent detections. This information may lead the investigation into a different path, and analysts can investigate and root out malicious activities in their networks.

This integration can be performed automatically within a playbook or manually by an analyst.

## Configuration

### Prerequisites

- SOAR connects to AlienVault OTX API via HTTPS. Typically it runs on 443/tcp port. So access to this service is required.
- A user account is required for SOAR to connect to AlienVault OTX. It can be created from the following link:

<https://otx.alienvault.com>

## Configuring AlienVault OTX

- AlienVault OTX requires an API key for access. Users can retrieve it from <https://otx.alienvault.com/api> after logging in with a valid credential.

## Configuring SOAR

- Click Configuration > Credentials > Create Credential
- Fill in the Credential Editor form with the following information:

Type	Name	Username	Password	Private Key
Internal Credential	Display name of credential set (i.e., AlienVault OTX Credentials)	Empty	Empty	API Key retrieved from the AlienVault OTX

- Click Configuration > Integrations > Create Integration
- Fill in the configuration form with the following information:

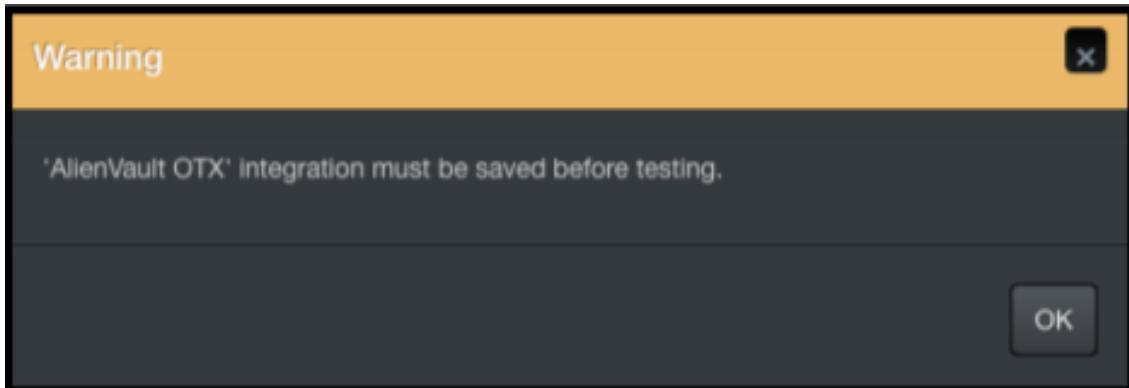
Parameter	Value
Name	Display name of AlienVault OTX integration on SOAR.
Type	AlienVault OTX.
Address	Address of the cloud service is standard: <a href="https://otx.alienvault.com">https://otx.alienvault.com</a> .

Parameter	Value
<b>Configuration</b>	<p>You need to specify the following configuration parameters:</p> <pre># Integration ID of the proxy integration to use when connecting to current # integration. # If not provided, SOAR will try to use a direct connection. #proxy.id=123 #Max count of fetching NIDS list for IP Indicator enrichment #If not provided, SOAR will fetch last 10 NIDS(s) #ip.indicator.nids.list.entry.count=10 #Max count of fetching URL list for IP Indicator enrichment #If not provided, SOAR will fetch last 50 URL(s) #ip.indicator.url.list.entry.count=50 #Max count of fetching URL list for Domain Indicator enrichment #If not provided, SOAR will fetch last 50 URL(s) #domain.indicator.url.list.entry.count=50 #Max count of fetching Malware list for Hostname Indicator enrichment #If not provided, SOAR will fetch last 50 Malware(s) #hostname.indicator.malware.list.entry.count=50 #Max count of fetching URL list for Hostname Indicator enrichment #If not provided, SOAR will fetch last 50 URL(s) #hostname.indicator.url.list.entry.count=50 # configure how far (in minutes) into the past this enrichment will look. #cache.reusing.duration=20</pre>
<b>Credential</b>	Name of the credential set you've just created on step 2. (i.e., AlienVault OTX Credentials).
<b>Trust Invalid SSL Certificates</b>	Select this if Engine's certificate is self-signed or not recognized by browsers. Not selected.
<b>Require Approval From</b>	Select user(s) from list to ask her/his approval before executing enrichments on this integration.
<b>Notify</b>	Select user(s) from the list to notify when SOAR performs an enrichment on this integration.

5. Click Save to complete integration.
6. When you click the Test button the following pop up should be displayed if your credentials and address are valid.

## Additional Notes

- AlienVault OTX integration on SOAR is an Advanced Action Script, and the content of the default script is accessible under Configuration > Customization Library.
- While defining the integration for the first time, you will encounter the following warning message, which is expected behavior for this type of integration.



# Integration Guide for Amazon AWS CloudTrail

## Overview of the Plugin

Amazon AWS CloudTrail is an AWS service that helps you enable operational and risk auditing, governance, and compliance of your AWS account. Actions taken by a user, role, or an AWS service are recorded as events in CloudTrail. CloudTrail is enabled on your AWS account when you create it. When activity occurs in an AWS account, that activity is recorded in a CloudTrail event. You can easily view recent events in the CloudTrail console by going to Event history. For an ongoing record of activity and events in your AWS account.

## Integration Capabilities

Amazon AWS CloudTrail Logs Features/Functionalities to be Integrated:

- List Trails
- Get Trail
- Create Trail
- Delete Trail
- Start Logging
- Stop Logging
- Get Trail Status
- Lookup Events
- List Queries

## Prerequisites

You must have access to HTTPS as the ArcSight SOAR connects to Amazon CloudTrail Logs API through this service

## Configuration

### Configuring Amazon CloudTrail Logs

1. Authentication: API requires **Access key** and **Secret Key** to generate the AWS signature.  
Follow these basic steps to generate the access key and secret key to access the Amazon AWS CloudTrail Logs Rest API.
  - a. Create your Amazon account.
  - b. Create a new user by navigating to the **Identity and Access Management (IAM)** section from your AWS Management Console.
  - c. Click **Add User** button to create a new user.
  - d. Choose your preferred username and make sure you select **Programmatic access**.
  - e. When it comes to permissions, you can add existing permission during this step. For most services, you can also do this from within the service configuration.

Add the below scope to the user.

Scope	Required
AWSCloudTrail_FullAccess	Yes
AmazonS3FullAccess	Yes

On the last page, you will see the access key id and the secret code. You will need to save them somewhere securely.

#### Authentication Parameters

- a. Request Headers:

Parameter	Data type	Description	Required
Access Key	String	Access key of the particular user.	Yes
Secret Key	String	Secret key of the particular user.	Yes

b. Additional Configuration:

Configuration Parameter	Description
proxy.id	Proxy device to be used while communicating with the remote system's API.
AWS Region	The region name to which the AWS server belongs too.
Cache.reusing.duration	Default cache-reuse parameter

## Configuring SOAR

1. Click Configuration > Credentials > Create Credentials.
2. Specify the following parameter values in the Credential Editor form.

Type	Name	Username	Password	Private Key
Internal credential	Display name for credential set (for example, AWS CloudWatch Logs Credentials).	N/A	The Access Key to authenticate the Amazon AWS CloudTrail Logs APIs.	The Secret Key.

3. Select your integration plugin zip file and click on Save.
4. Select the integration that you have added to the Integrationsmenu.
5. Click Save to complete the integration.
6. Click Test, and an Integration Successful message is displayed if the credential and address are valid.

## Integration Capabilities:

### 1. List Trails

Enrichment capability to list trails that are in the current account.

Input Parameters: N/A

Request Headers:

X-Amz-Target	CloudTrail_20131101.ListTrails
Content-Type	application/x-amz-json-1.1

Default Parameters:

Key	Description	Data Type	Scope Restricted	Required
NextToken	The token for the next set of items to return.	String	No	No

Output:

Case Scope: N/A

Human Readable Output:

The screenshot shows a table with two columns: 'Trail Name' and 'Trail Arn'. The table lists five trails: 'abhijeet\_123', 'mftrail', 'new-test-trail', 'test-trail', and 'test-trail-qa'. Each entry has its corresponding ARN listed next to it. At the bottom left, there is a pagination indicator 'Total 5 , items / page' and a page number '1'.

Trail Name	Trail Arn
abhijeet_123	arn:aws:cloudtrail:us-east-1:102716399460:trail/abhijeet_123
mftrail	arn:aws:cloudtrail:us-east-1:102716399460:trail/mftrail
new-test-trail	arn:aws:cloudtrail:us-east-1:102716399460:trail/new-test-trail
test-trail	arn:aws:cloudtrail:us-east-1:102716399460:trail/test-trail
test-trail-qa	arn:aws:cloudtrail:us-east-1:102716399460:trail/test-trail-qa

## 2. Get Trail

Enrichment capability to return settings information for a specified trail.

Input Parameters:

Path Parameter	Description	Type	Scope restricted (Yes/No)	Required (Yes/No)
Trail Name	The name or the Amazon Resource Name (ARN) of the trail for which you want to retrieve settings information.	UNKNOWN, KEYWORD	Yes	Yes

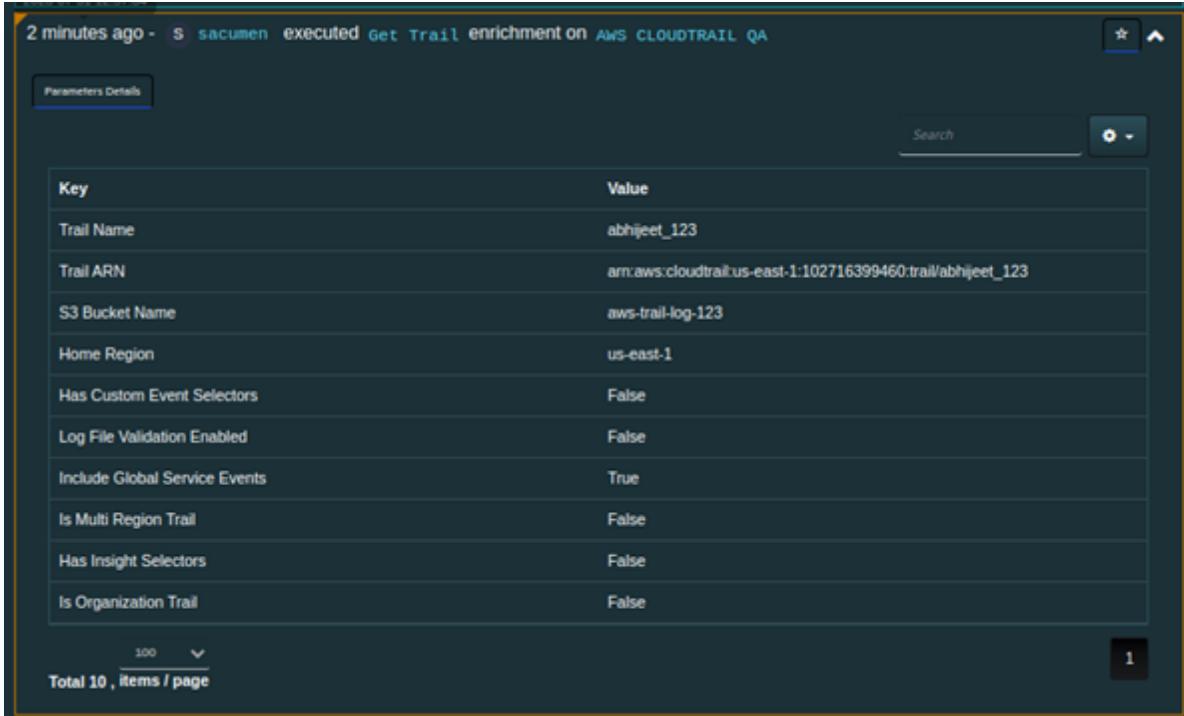
Request Headers:

X-Amz-Target	com.amazonaws.cloudtrail.v20131101.CloudTrail_20131101.GetTrail
Content-Type	application/x-amz-json-1.1

Output:

Case Scope: N/A

Human Readable Output:



The screenshot shows a table of parameters for a CloudTrail trail named 'abhijeet\_123'. The table has two columns: 'Key' and 'Value'. The parameters listed are:

Key	Value
Trail Name	abhijeet_123
Trail ARN	arn:aws:cloudtrail:us-east-1:102716399460:trail/abhijeet_123
S3 Bucket Name	aws-trail-log-123
Home Region	us-east-1
Has Custom Event Selectors	False
Log File Validation Enabled	False
Include Global Service Events	True
Is Multi Region Trail	False
Has Insight Selectors	False
Is Organization Trail	False

At the bottom left, it says 'Total 10 , items / page'. At the bottom right, there is a page number '1'.

### 3. Create Trail

Action capability to Create a trail that specifies the settings for delivery of log data to an Amazon S3 bucket.

Rollback: No

Duplicate Control: Yes

Input Parameters:

Key	Description	Type	Scope restricted	Required (Yes/No)
Trail Name	Specifies the name of the trail.	String	No	Yes
S3 Bucket Name	Specifies the name of the Amazon S3 bucket designated for publishing log files.	String	No	Yes
Start Logging	Specifies if logging needs to start on the newly created trail or not	Array of string	No	Yes

Request Headers:

X-Amz-Target	com.amazonaws.cloudtrail.v20131101.CloudTrail_20131101.CreateTrail
Content-Type	application/x-amz-json-1.1

Default Parameters:

Query Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
Enable Log File Validation	Specifies whether log file integrity validation is enabled. (Default: True)	Bool	No	No
Include Global Service Events	Specifies whether the trail is publishing events from global services such as IAM to the log files.(Default Value: True)	Bool	No	No

Output:

Case Scope: N/A

Human Readable Output: N/A

#### 4. Delete Trail

Action capability to delete a trail. This operation must be called from the Region in which the trail was created. DeleteTrail cannot be called on the shadow trails (replicated trails in other Regions) of a trail that is enabled in all Regions.

Rollback: No

Duplicate Control: No

Input Parameters:

Path Parameter	Description	Type	Scope restricted (Yes/No)	Required (Yes/No)
Trail Name	The name or the Amazon Resource Name (ARN) of the trail to be deleted.	UNKNOWN, KEYWORD	Yes	Yes

Request Headers:

X-Amz-Target	com.amazonaws.cloudtrail.v20131101.CloudTrail_20131101.DeleteTrail
Content-Type	application/x-amz-json-1.1

Output:

Case Scope: N/A

Human Readable Output: N/A

#### 5. Start Logging

Action capability to Start the recording of AWS API calls and log file delivery for a trail. For a trail that is enabled in all Regions, this operation must be called from the Region in which the trail was created. This operation cannot be called on the shadow trails (replicated trails in other Regions) of a trail that is enabled in all Regions.

Rollback: Yes

Duplicate Control: No

**Input Parameters:**

Path Parameter	Description	Type	Scope restricted (Yes/No)	Required (Yes/No)
Trail Name	Specifies the name or the CloudTrail ARN of the trail for which CloudTrail logs AWS API calls.	UNKNOWN, KEYWORD	Yes	Yes

**Request Headers:**

X-Amz-Target	com.amazonaws.cloudtrail.v20131101.CloudTrail_20131101.StartLogging
Content-Type	application/x-amz-json-1.1

**Output:**

Case Scope: N/A

Human Readable Output: N/A

**6. Stop Logging**

Action capability to suspend the recording of AWS API calls and log file delivery for the specified trail. Under most circumstances, there is no need to use this action. You can update a trail without stopping it first. This action is the only way to stop recording.

Rollback: Yes

Duplicate Control: No

**Input Parameters:**

Path Parameter	Description	Type	Scope restricted (Yes/No)	Required (Yes/No)
Trail Name	Specifies the name or the CloudTrail ARN of the trail for which CloudTrail logs AWS API calls.	UNKNOWN, KEYWORD	Yes	Yes

**Request Headers:**

X-Amz-Target	com.amazonaws.cloudtrail.v20131101.CloudTrail_20131101.StopLogging
Content-Type	application/x-amz-json-1.1

**Output:**

Case Scope: N/A

Human Readable Output: N/A

**7. Get Trail Status**

Enrichment capability which returns a JSON-formatted list of information about the specified trail. Fields include information on delivery errors, Amazon SNS and Amazon S3 errors, and start and stop logging times for each trail. This operation returns trail status

from a single Region. To return trail status from all Regions, you must call the operation on each Region.

**Input Parameters:**

Key	Description	Type	Scope restricted	Required (Yes/No)
Name	Specifies the name or the CloudTrail ARN of the trail for which you are requesting status.	String	Yes	Yes

**Request Headers:**

X-Amz-Target	com.amazonaws.cloudtrail.v20131101.CloudTrail_20131101.GetTrailStatus
Content-Type	application/x-amz-json-1.1

**Output:**

Case Scope: N/A

**Human Readable Output:**

The screenshot shows a web-based interface for viewing enrichment details. At the top, there's a timestamp: "a few seconds ago - S sacumen executed Get Trail Status enrichment on AWS CLOUDTRAIL QA". Below this is a "Parameters Details" button and a search bar. The main content is a table with columns "Key" and "Value". The table contains the following data:

Key	Value
Is Logging	True
Latest Delivery Attempt Succeeded	2023-08-01T08:44:03Z
Latest Delivery Attempt Time	2023-08-01T08:44:03Z
Latest Delivery Time	2023-08-01T08:44:03Z
Latest Notification Attempt Succeeded	N/A
Latest Notification Attempt Time	N/A
Start Logging Time	2023-07-31T08:59:24Z
Stop Logging Time	2023-07-31T08:54:13Z
Time Logging Started	2023-07-31T08:59:24Z
Time Logging Stopped	2023-07-31T08:54:13Z

At the bottom, there are pagination controls: "100" (dropdown), "Total 10 , items / page", and a page number "1".

## 8. Lookup Events

Enrichment capability to Look up management events or cloudTrail Insights events that are captured by CloudTrail. You can look up events that occurred in a Region within the last 90 days.

**Input Parameters:**

Key	Description	Data Type	Scope Restricted	Required
Time Range	Specifies that only events that occur before or at the specified time are returned.	Datetime Range	No	No
Event Category	Specifies the event category. (Default Value: Insight, Management )	Array	No	Yes

## Request Headers:

X-Amz-Target	com.amazonaws.cloudtrail.v20131101.CloudTrail_20131101.LookupEvents
Content-Type	application/x-amz-json-1.1

## Default Parameters:

Key	Description	Data Type	Scope Restricted	Required
NextToken	The token for the next set of items to return.	String	No	No
MaxResults	The number of events to return. Possible values are 1 through 50. The default is 50.	Integer	No	No

## Output:

Case Scope: N/A

## Human Readable Output:

## 9. List Queries

Enrichment capability to return a list of queries and query statuses for the past seven days.

**Input Parameters:**

Key	Description	Data Type	Scope Restricted	Required
Time Range	Specifies that only events that occur before or at the specified time are returned.	Datetime Range	No	No
Event Data Store ID	The ARN (or the ID suffix of the ARN) of an event data store on which queries were run.	String	No	Yes
Query Status	The status of queries that you want to return in results. Valid values for QueryStatus include "ALL", "CANCELLED", "FAILED", "FINISHED", "QUEUED", "RUNNING", "TIMED OUT"	Array	No	Yes

**Request Headers:**

X-Amz-Target	com.amazonaws.cloudtrail.v20131101.CloudTrail_20131101.ListQueries
Content-Type	application/x-amz-json-1.1

**Default Parameters:**

Key	Description	Data Type	Scope Restricted	Required
NextToken	The token for the next set of items to return.	String	No	No
MaxResults	The maximum number of queries to show on a page.	String	No	No

**Output:**

Case Scope: N/A

**Human Readable Output:**

Creation Time	Query Id	Query Status
2023-08-01T07:52:57Z	71c020f3-d39e-4941-b205-206194d9fca6	FINISHED
2023-08-01T07:24:25Z	9fdb0da6-adee-4e59-b98d-c29509090c9f	FINISHED
2023-07-31T12:22:21Z	e690387a-a095-46f5-8fb9-b8009baae921	FINISHED
2023-07-31T12:11:02Z	ca7a15b6-8115-4b67-896b-2790b525e260	FINISHED

Total 4 , items / page

# Integration Guide for Amazon AWS Lambda

## Integration Overview

AWS Lambda is an event-driven, server-less computing platform provided by Amazon as a part of Amazon Web Services. It is a computing service that runs code in response to events and automatically manages the computing resources required by that code.

## Integration Capabilities

- Get Function
- List Function
- Invoke Function

## Prerequisites

- ArcSight SOAR connects to lambda.region.api.aws APIs through HTTPS. Access to this service is required.
- **Access key ID** and **Secret Access key** are required for ArcSight SOAR to connect to Amazon AWS Lambda.

## Configuring Amazon AWS Lambda

1. Log in to <https://aws.amazon.com>.
2. Navigate to **My Security Credentials > Identity Access Management (IAM)**.
3. Click **Access Management > Users > Add Users**.
4. Select **Access Type as Programmatic Access**.
5. You can skip the next steps until **Access Key** and **Secret Access Key** are displayed.



Download the credentials as the Secret Access Key is not displayed post this step.

6. Add the following action permissions if you require admin permissions for this service or contact your AWS cloud support:

```
{  
    "Version": "2012-18-17",  
    "Statement": [
```

```
{
    "Sid": "VisualEditore0",
    "Effect": "Allow",
    "Action": [
        "lambda>ListFunctions",
        "lambda: InvokeFunction",
        "lambda: GetFunction"
    ],
    "Resource": "*"
}
]
```

## Configuring SOAR

1. Click **Configuration > Credential > Create Credential**.
2. Specify the following parameter values in the **Credential Editor**:

Type	Name	Username	Password	Private Key
Internal Credential	Display name of credential set ( for example, Amazon AWS Lambda Credentials).	Empty	Access Key	Secret Key

3. Click **Configuration > Integrations > Create Integration**.
4. Specify the following parameter values in the **Configuration Form**:

Parameter	Value		
Name	Display name of the integration		
Type	Amazon Lambda Integration		
Address	Address of the integration should follow the format <code>https://lambda.ap-southeast-1.api.aws</code> for specific region		
Configuration	<p>Specify the following configuration parameter values:</p> <table border="1"> <tr> <td>proxy.id</td> <td>Integration ID of the proxy to use current intergration. For example: Proxy.id=12345</td> </tr> </table>	proxy.id	Integration ID of the proxy to use current intergration. For example: Proxy.id=12345
proxy.id	Integration ID of the proxy to use current intergration. For example: Proxy.id=12345		

Parameter	Value
Credential	Credential that has been defined for this integration under the Credentials menu
Trust Invalid SSL Certificates	Select this option if the firewall's web certificate is self-signed or if it is not recognized by browsers
Require Approval From	Select user(s) from list who can provide approval before executing actions on this integration
Notify	Select user(s) from the list who can provide approval when SOAR performs an action on this integration

## Capabilities

### 1. Get Function

Enrichment capability for creating Lambda function.

Input Parameter	Description	Type	Scope Restricted(Yes/No)	Required (Yes/No)
Integration	Name of the third party integration	Integration	N/A	Yes
Region	Region to be specified for creating the Lambda function	String	No	Yes
Function name	Function Name, Function ARN, Partial ARN	String	No	Yes
Qualifier	Ex: \$LATEST	String	No	Yes

Output:

Case Scope

N/A

Human Readable Output

### 2. List Functions

Enrichment capability for retrieving list of Lambda Functions

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
Integrations	Name of the third party integrations	Integer	N/A	Yes
Region	Region to be specified for creating the Lambda function	String	No	Yes

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
Function All Versions	Version of the function, ex: ALL, LATEST	Boolean	No	No
Max Item	Maximum value of item must be fetched from range 1-1000	Integer	No	Yes

Case Scope

N/A

Human Readable Output

### 3. Invoke Action

Action capability for invoking Lambda function.

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
Integration	Name of the third party integration.	Integration	N/A	Yes
Rollback Mode	Time to rollback this action. Default is no rollback	N/A	N/A	No
Region	Region to be specified for creating the Lambda function	String	No	Yes
Function name	Function Name, Function ARN, Partial ARN	String	No	Yes
Qualifier	Ex: ALL \$LATEST	String	No	No
Invocation Type	Invocation Type Ex: RequestResponse, Event, DryRun	String	No	No
Payload	Json payload	Json	No	No

Output:

Case Scope

N/A

Human Readable Output

N/A

# Integration Guide for Amazon EC2

## Integration Overview

Amazon EC2 (Elastic Compute Cloud) forms a central part of Amazon.com's cloud-computing platform, Amazon Web Services, by allowing users to establish virtual networks and rent virtual computers on which they can run their own applications. Amazon EC2 REST-API supports the following Amazon Web Services:

- Amazon EC2
- Amazon EBS
- Amazon VPC
- AWS VPN

Please note that this integration is in Beta.

## Integration Capabilities

ArcSight SOAR has the following integration capabilities with Amazon EC2:

- Add Network ACL Entry (VPC)
- Delete Network ACL Entry (VPC)

### Use Case: Blocking Attackers

SOAR when integrated with Amazon EC2, blocks the attacker's IP addresses while responding to a cyber-attack. The blocking can be performed automatically within a playbook or manually by an analyst.

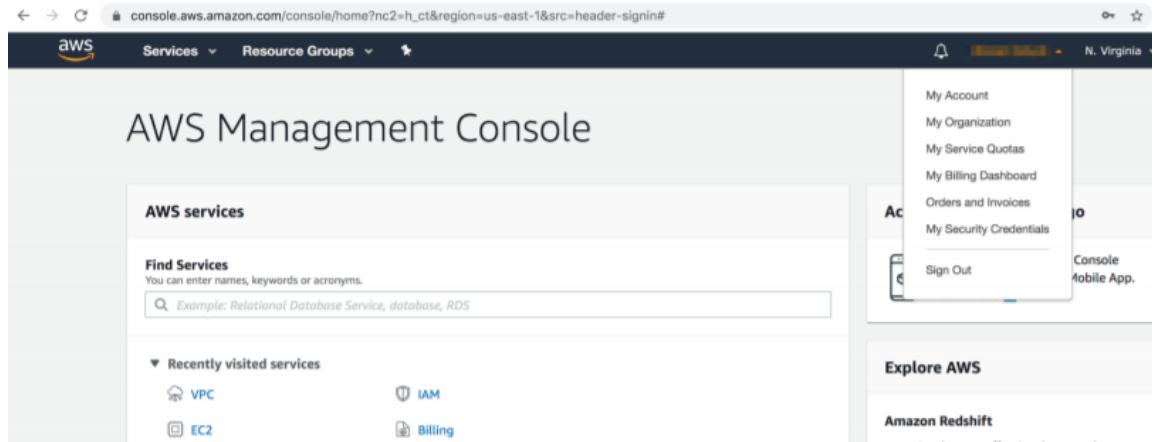
## Configuration

### Prerequisites

- SOAR connects to Amazon EC2 API via HTTPS. Access to <https://ec2.amazonaws.com> (443/tcp port) is required.
- AWS Access Key and AWS Access Key Secret are required for SOAR to connect Amazon Web Services.

### Configuring on Amazon AWS

1. Log in to Amazon Console (<https://aws.amazon.com>). Navigate to My Security Credentials, and select Identity Access Management (IAM) service:



2. To add an IAM(identity and access management) user, click Access Management > Users > Add User. While adding new user account, it is important to select Access Type as Programmatic Access.

The screenshot shows the AWS IAM 'Users' page. On the left, there's a navigation sidebar with options like 'Dashboard', 'Access management', 'Groups', 'Users' (which is selected), 'Roles', 'Policies', 'Identity providers', and 'Account settings'. The main area displays a table with columns: 'User name', 'Groups', 'Access key age', 'Password age', 'Last activity', and 'MFA'. There are two users listed: one with an access key age of 8 days and another with None.

The screenshot shows the 'Add user' wizard at step 1. The title is 'Set user details'. It says you can add multiple users at once. A 'User name\*' field contains 'aws-atar-poc'. Below it is a link to 'Add another user'.

**Select AWS access type**

Select how these users will access AWS. Access keys and autogenerated passwords are provided in the last step. [Learn more](#)

**Access type\***  **Programmatic access**  
Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.

**AWS Management Console access**  
Enables a **password** that allows users to sign-in to the AWS Management Console.

3. You can skip the next steps in the Add User process until Access Key and Access Key Secret are displayed.

**Note:** Download the credentials as the Access Key Secret is never displayed post this step.

The screenshot shows the 'Add user' wizard at step 5. A success message says: 'You successfully created the users shown below. You can view and download user security credentials. You can also email users instructions for signing in to the AWS Management Console. This is the last time these credentials will be available to download. However, you can create new credentials at any time.' Below this is a table with columns: 'User', 'Access key ID', and 'Secret access key'. One row is shown for 'aws-atar-poc' with a 'Show' link for the secret key.

4. To arrange access policy, click > Access Management > Policies, and search for the required policy in previously defined policies list.

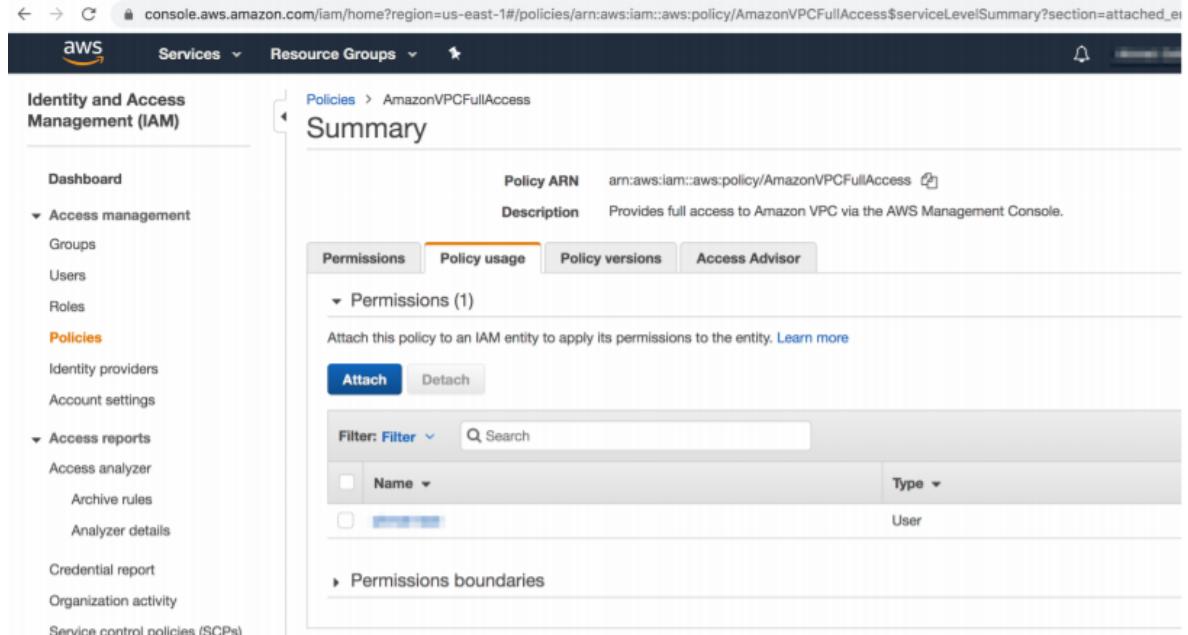
For example, the following image shows the policy AmazonVPCFullAccess.

The screenshot shows the AWS Identity and Access Management (IAM) Policies page. The left sidebar is collapsed. The main area displays a table of policies. A search bar at the top right is set to 'vpc'. The table has columns: Policy name, Type, Used as, and Description. One row is selected, highlighted with a blue dot: 'AmazonVPCFullAccess' (AWS managed, Permissions policy). Below the table, a note says 'Provides full access to Amazon VPC via the AWS Management Console.' At the bottom, there's a table for 'Policy summary' with columns: Service, Access level, Resource, and Request condition. It shows one entry: EC2, Full: Tagging Limited: List, Read, Write, Permissions management, All resources, and None.

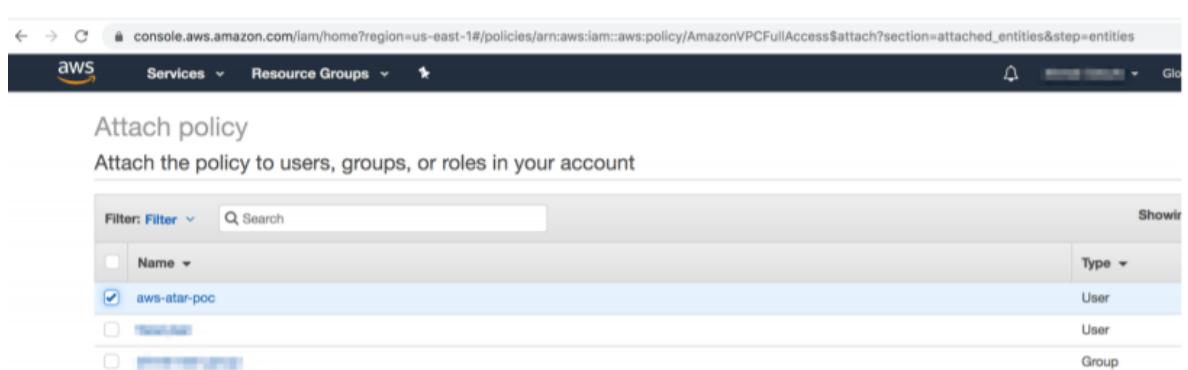
5. Select AmazonVPCFullAccess and open the Policy Summary.

a. **Click Policy Usage > Attach.**

b. In the Attach Policy menu, select the user that you have created in the previous steps, from the available users list in the system.



The screenshot shows the AWS IAM Policies Summary page for the 'AmazonVPCFullAccess' policy. The policy ARN is arn:aws:iam::aws:policy/AmazonVPCFullAccess. The description states: 'Provides full access to Amazon VPC via the AWS Management Console.' The 'Permissions' tab is selected, showing one permission entry: 'Attach'. Below this is a search bar and a table with columns for Name and Type. One row is visible, showing a user named 'aws-atar-poc'.

The screenshot shows the 'Attach policy' page. The heading is 'Attach the policy to users, groups, or roles in your account'. Below is a search bar and a table with columns for Name and Type. The 'aws-atar-poc' user is selected, indicated by a checked checkbox. Other entries include a user and a group, both with unchecked checkboxes.

6. You can verify if the permission is successful for the user account that you've created on the Policy Usage page.

The screenshot shows the AWS IAM Policies page. The left sidebar is titled 'Identity and Access Management (IAM)' and includes sections for Dashboard, Access management (Groups, Users, Roles, Policies), Access reports (Access analyzer, Archive rules, Analyzer details), Credential report, Organization activity, and Service control policies (SCPs). The main content area is titled 'Summary' for the 'AmazonVPCFullAccess' policy. It shows the Policy ARN (arn:aws:iam::aws:policy/AmazonVPCFullAccess) and a Description stating 'Provides full access to Amazon VPC via the AWS Management Console.' Below this, there are tabs for Permissions, Policy usage, Policy versions, and Access Advisor. The Permissions tab is selected, showing a list of attached permissions. One permission is listed for a user named 'aws-atar-poc'. There are also sections for 'Permissions boundaries' and 'Show more'.

## Configuring on SOAR

1. Click **Configuration > Credentials > Create Credential**.
2. Fill the Credential Editor form with the following information:

### a. Internal Credential:

Type	Name	Username:	Password	Private Key
Internal credential	Display name of credential set (i.e., Amazon AWS Credentials)	Access Key of IAM user you have created	Secret of Access Key of IAM user you have created	Empty

### b. Credential Store:

Type	Name
External credential	Name of the credential with full path of the safe on store

3. Click **Configuration > Integrations > Create Integration**. Fill the Configuration form with the following information:

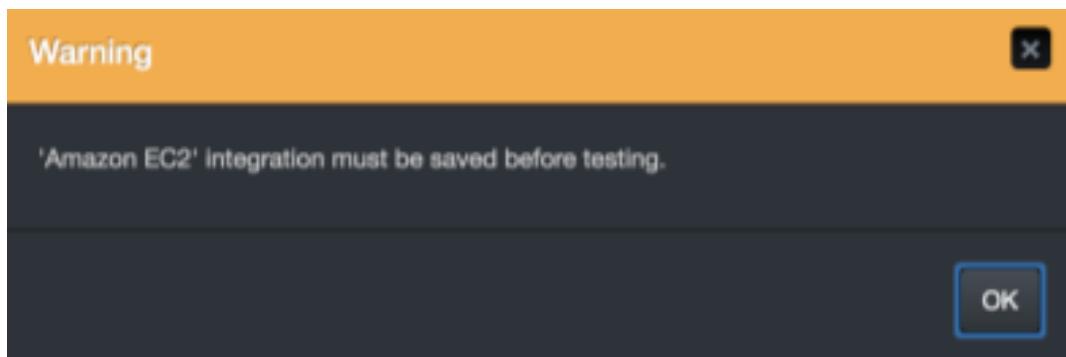
Parameter	Value
Type	Amazon EC2
Address	Address of the integration ( <a href="https://ec2.amazonaws.com">https://ec2.amazonaws.com</a> )

Parameter	Value
Configuration	You need to specify the following configuration parameters
Credential	Name of the credential set you have just created on step 2. (i.e., Amazon AWS Credentials)
Trust Invalid SSL Certificates	No need to select
Require Approval From	Select user(s) from list to ask her/his approval before executing actions on this integration
Notify	Select user(s) from the list to notify when SOAR performs an action on integration

4. Click Save to complete integration.
5. Click the Test button. The following pop up will be displayed if your credential and address are valid.

## Additional Notes

- Amazon EC2 integration on SOAR is an Advanced Script, and the content of the default script is accessible under **Configuration > Customization Library**.
- While defining the integration for the first time, you might encounter the following warning message, which is the expected behavior for this type of integration.



# Integration Guide for Amazon GuardDuty

## Integration Overview

Amazon GuardDuty is a security monitoring service that analyses and processes data sources, such as Amazon AWS CloudTrail data events for Amazon S3 logs, CloudTrail management event logs, DNS logs, Amazon EBS volume data, Kubernetes audit logs, Amazon VPC flow logs, and RDS login activity. It uses threat intelligence feeds, such as lists of malicious IP addresses and domains, and machine learning to identify unexpected, potentially unauthorized, and malicious activity within your AWS environment. This can include issues such as escalation of privileges, use of exposed credentials, or communication with malicious IP addresses, domains, presence of malware on your Amazon EC2 instances and container workloads, or discovery of unusual patterns of login events on your database.

## Integration Capabilities

ArcSight SOAR has the following integration capabilities with Amazon GuardDuty:

- List Detectors
- Get Detector Details
- Create Trusted IP List
- Delete Trusted IP List
- List Trusted IP List
- Get Trusted IP List Detail
- Add to trusted IP List
- Remove from trusted IP List
- Create Threat Intel List
- Delete Threat Intel List
- List Threat Intel List
- Get Threat Intel List Details
- Add to Threat Intel List
- Remove from Threat Intel List
- List Findings
- Get Finding Detail
- Archive Finding

- Unarchive Finding
- Update Finding Feedback

## Prerequisites

You must have access to HTTPS as the ArcSight SOAR connects to Amazon GuardDuty API through this service.

## Configuration

### Configuring Amazon GuardDuty

1. **Authentication:** API requires Access Key and Secret Key to generate the AWS signature. Complete the following basic steps to generate the access Key and secret Key to access the Amazon GuardDuty Rest API:
  - a. Create your amazon account.
  - b. Navigate to the Identity and Access Management (IAM) section from your AWS Management Console to create a new user.
  - c. Click Add User to create a user.
  - d. Specify your preferred Username and make sure you select Programmatic access.
  - e. For permissions, you can add existing permission during this step. For most services, you can also add it from within the service configuration.

Add the following scope to the user:

Scope	Required
AmazonGuardDutyFullAccess	Yes
IAMFullAccess	Yes
AmazonS3ReadOnlyAccess	Yes



On the last page, you will see the access key id and the secret code. You will need to save them somewhere securely.

#### Authentication parameters

##### Request Headers:

Parameters	Data Type	Description	Required
Access Key	String	Access Key of the particular user.	Yes

Secret Key	String	Secret Key	Yes
------------	--------	------------	-----

## 2. Additional Configuration:

Configuration Parameter	Description
proxy.id	Proxy device to be used while communicating with remote system's API.
AWS Region	The region name to which the AWS server belongs too.
Service Name	Name of the AWS service.
Cache.reusing.duration	Default cache-reuse parameter.

# Configuring SOAR

1. Click **Configuration > Credentials > Create Credentials**.
2. Specify the following parameter values in the **Credential Editor** form:

Type	Name	Username	Password	Private Key
Internal credential	Display name of credential set (for example, Amazon GuardDuty Credentials)	N/A	The Access Key to authenticate the Amazon GuardDuty APIs	Secret Key

3. Click **Configuration > Integrations > Upload plugin**.
4. Select your integration plugin zip file and click **Save**.
5. Select the integration that you have added to **Integrations** menu.
6. Click **Save** to complete the integration.
7. Click **Test**, If the credential and address are valid a success message is displayed.

# Capabilities

## 1. List Detectors

Lists detector IDs of all the existing Amazon GuardDuty detector resources.

### Request Headers:

Parameters	Datatype	Description	Required
Access Key	String	Access key of the particular user	Yes
Secret Key	String	Secret Key	Yes

### Default Parameter:

Query Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
MaxResults	You can use this parameter to indicate the maximum number of items that you want in the response. The default value is 50. The maximum value is 50.	Integer	No	No
NextToken	You can use this parameter when paginating results. Set the value of this parameter to null on your first call the list action. For subsequent calls to the action, fill nextToken in the request with the value of NextToken from the previous response to continue listing data.	String	No	No

**Output:**

Case Scope:

N/A

Human Readable Output:

Key	Value
Detector Ids	[ "48c264162c61bfa034abb98ca81a341c" ]

**2. Get Detector Detail**

Retrieves an Amazon GuardDuty detector specified by the detectorId.

**Request Headers:**

Parameters	Datatype	Description	Required
Access Key	String	Access key of the particular user	Yes
Secret Key	String	Secret Key	Yes

**Path Parameters:**

Path parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
detectorId	The unique ID of the detector that you want to get.	String	No	Yes

**Output:**

Case Scope: N/A

Human Readable Output

Key	Value
Status	ENABLED
Created At	2022-11-30T10:54:20.526Z
Update At	2022-11-30T10:54:20.526Z
Finding Publishing Frequency	SIX_HOURS
Data Sources	{"kubernetes": {"auditLogs": {"reason": null, "status": "ENABLED", "updatedAt": null}}, "dnsLogs": {"reason": null, "status": "ENABLED", "updatedAt": null}, "cloudTrail": {"reason": null, "status": "ENABLED", "updatedAt": null}, "malwareProtection": {"serviceRole": "arn:aws:iam::100420467922:role/aws-service-role/malware-protection.guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDutyMalwareProtection", "scanEc2InstanceWithFindings": {"ebsVolumes": {"reason": null, "status": "ENABLED", "updatedAt": null}}, "flowLogs": {"reason": null, "status": "ENABLED", "updatedAt": null}, "database": {"rds": {"databaseEvents": {"reason": null, "status": "ENABLED", "updatedAt": null}}, "s3Logs": {"reason": null, "status": "ENABLED", "updatedAt": null}}}}
Tags	N/A
Service Role	arn:aws:iam::100420467922:role/aws-service-role/guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty

### 3. Create Trusted IP List

Creates a new IPSet, which is called a trusted IP list in the console user interface. An IPSet is a list of IP addresses that are trusted for secure communication with AWS infrastructure and applications. GuardDuty does not generate findings for IP addresses that are included in IPSets. Only users from the administrator account can use this operation.

- **Rollback:** No
- **Duplicate Control:** No

#### Request Headers:

Parameters	Datatype	Description	Required
Access Key	String	Access key of the particular user	Yes
Secret Key	String	Secret Key	Yes

#### Path Parameters:

Path parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
<b>detectorId</b>	The unique ID of the detector that you want to get.	String	No	Yes

#### Request Body Parameters:

Request Body	Description	Type	Scope restricted (Yes/No)	Required (Yes/No)
<b>activate</b>	A Boolean value that indicates whether GuardDuty is to start using the uploaded IPSet. (Default is set to True always)	Bool	No	No
<b>clientToken</b>	The idempotency token for the create request.	String	No	No
<b>format</b>	The format of the file that contains the IPSet. Valid Values: TXT   STIX   OTX_CSV   ALIEN_VAULT   PROOF_POINT   FIRE_EYE	String	No	Yes
<b>location</b>	The URI of the file that contains the IPSet.	String	No	Yes
<b>name</b>	The user-friendly name to identify the IPSet.	String	No	Yes

**Output:**

Case Scope: N/A

Human Readable Output: N/A

**4. Delete Trusted IP List**

Deletes the IPSet specified by the ipSetId. IPSets are called trusted IP lists in the console user interface.

- Rollback: No
- Duplicate Control: No

**Request Headers:**

Parameters	Datatype	Description	Required
Access Key	String	Access key of the particular user	Yes
Secret Key	String	Secret Key	Yes

**Path Parameters:**

Path Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
<b>detectorId</b>	The unique ID of the detector associated with the IPSet.	String	No	Yes
<b>ipSetId</b>	The unique ID of the IPSet to delete.	String	No	Yes

**Output:**

Case Scope: N/A

Human Readable Output: N/A

**5. List Trusted IP List**

Enrichment capability to search for domain names that match your specific search string. Unlike Domain suggestions, Domain Search finds currently registered or previously registered domain names that are either currently registered or have been registered in the past under one of the major gTLDs (.com, .net, .org, .info, .us, or .biz). Many countries code TLDs, or the new gTLDs.

#### Request Headers:

Parameters	Datatype	Description	Required
Access Key	String	Access key of the particular user	Yes
Secret Key	String	Secret Key	Yes

#### Path Parameters:

Path parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
<b>detectorId</b>	The unique ID of the detector that you want to get.	String	No	Yes

#### Default Parameters:

Path Parameter	Description	Type	Scope restricted (Yes/No)	Required (Yes/No)
MaxResults	You can use this parameter to indicate the maximum number of items you want in the response. The default value is 50. The maximum value is 50.	Integer	No	No
NextToken	You can use this parameter when paginating results. Set the value of this parameter to null on your first call to the list action. For subsequent calls to the action, fill nextToken in the request with the value of NextToken from the previous response to continue listing data.	String	No	No

#### Output:

Case Scope: N/A

Human Readable Output

ID	Name	Location	Format	Status	Tags
eac31343892f254ad85 367c523ef59a0	testingFile7	s3://newone12345678/ sample.txt	TXT	INACTIVE	N/A

## 6. Get Trusted IP List Details

Retrieves the IPSet specified by the ipSetId.

#### Request Headers:

Parameters	Datatype	Description	Required
Access Key	String	Access key of the particular user	Yes
Secret Key	String	Secret Key	Yes

Path Parameters:

Path Parameter	Description	Type	Scope restricted (Yes/No)	Required (Yes/No)
<b>detectorId</b>	The unique ID of the detector that the IPSet is associated with.	String	No	Yes
<b>IpSetId</b>	The unique ID of the IPSet to retrieve.	String	No	Yes

Output:

Case Scope: N/A

Human Readable Output

Key	Value
Name	testingFile7
Location	s3://newone12345678/sample.txt
Format	TXT
Status	INACTIVE
Tags	N/A

## 7. Add to Trusted IP List

Add IP to the Trusted IP list detail.

- Rollback: Yes
- Duplicate Control: Yes

Request Headers

Parameters	Datatype	Description	Required
Access Key	String	Access key of the particular user	Yes
Secret Key	String	Secret Key	Yes

Path Parameters:

Path Parameter	Description	Type	Scope Restricted(Yes/No)	Required (Yes/No)
Bucket Name	The name of the S3 bucket	String	No	Yes
Key	The file path of S3 bucket file	String	No	Yes

Request Body Parameters:

Request Body	Description	Type	Scope restricted (Yes/No)	Required (Yes/No)
IPSET	The unique ID that specifies the IPSet that you want to update.	String	No	Yes

Output:

Case Scope: N/A

Human Readable Output: N/A

## 8. Remove from Trusted IP List

Remove the IP from Trusted IP list detail.

- Rollback: No
- Duplicate Control: No

Request Headers:

Parameters	Datatype	Description	Required	Parameters
Access Key	String	Access key of the particular user	Yes	Access Key
Secret Key	String	Secret Key	Yes	Secret Key

Path parameters:

Path Parameter	Description	Type	Scope Restricted(Yes/No)	Required (Yes/No)
Bucket Name	The name of the S3 bucket	String	No	Yes
Key	The file path of S3 bucket file	String	No	Yes

Request Body Parameters:

Request Body	Description	Type	Scope restricted (Yes/No)	Required (Yes/No)
IPSET	The unique ID that specifies the IPSet that you want to update.	String	No	Yes

Output:

Case Scope: N/A

Human Readable Output: N/A

## 9. Create Threat Intel List

Creates a new ThreatIntelSet. ThreatIntelSets consist of known malicious IP addresses. GuardDuty generates findings based on ThreatIntelSets. Only users of the administrator account can use this operation.

- Rollback: No
- Duplicate Control: No

## Request Headers

Parameters	Datatype	Description	Required
Access Key	string	Access key of the particular user	Yes
Secret Key	string	Secret Key	Yes

## Path Parameters:

Path Parameter	Description	Type	Scope restricted (Yes/No)	Required (Yes/No)
detectorId	The unique ID of the detector of the GuardDuty account that you want to create a threatIntelSet for.	String	No	Yes

## Request Body Parameters

Request Body	Description	Type	Scope restricted (Yes/No)	Required (Yes/No)
clinetToken	The idempotency token for the create request.	String	No	No
format	The format of the file that contains the ThreatIntelSet.  Valid Values: TXT   STIX   OTX_CSV   ALIEN_VAULT   PROOF_POINT   FIRE_EYE	String	No	Yes
location	The URI of the file that contains the ThreatIntelSet.	String	No	Yes
name	A user-friendly ThreatIntelSet name displayed in all findings that are generated by activity that involves IP addresses included in this ThreatIntelSet.	String	No	Yes

## Default Request Body Parameters:

Request Body	Description	Type	Scope restricted (Yes/No)	Required (Yes/No)
activate	A Boolean value that indicates whether GuardDuty is to start using the uploaded ThreatIntelSet.{Default Keep it as True}	Bool	No	No

## Output:

Case Scope: N/A

Human Readable Output: N/A

## 10. Delete Threat Intel List

Deletes the ThreatIntelSet specified by the ThreatIntelSet ID.

- Rollback: No
- Duplicate Control: No

Request Headers:

Parameters	Datatype	Description	Required
Access Key	string	Access key of the particular user	Yes
Secret Key	string	Secret Key	Yes

Path Parameters:

Path Parameter	Description	Type	Scope restricted (Yes/No)	Required (Yes/No)
detectorId	The unique ID of the detector that the threatIntelSet is associated with.	String	No	Yes
threatIntelSetId	The unique ID of the threatIntelSet that you want to delete.	HOST, UNKNOWN, KEYWORD	No	Yes

Output:

Case Scope: N/A

Human Readable Output

## 11. List Threat Intel List

Lists the ThreatIntelSets of the GuardDuty service specified by the detector ID. If you use this operation from a member account, the ThreatIntelSets associated with the administrator account are returned.

Request Headers:

Parameters	Datatype	Description	Required
Access Key	string	Access key of the particular user	Yes
Secret Key	string	Secret Key	Yes

Path Parameters:

Path Parameter	Description	Type	Scope restricted (Yes/No)	Required (Yes/No)
detectorId	The unique ID of the detector that the IPSet is associated with.	String	No	Yes

Default Parameters:

Path Parameter	Description	Type	Scope restricted (Yes/No)	Required (Yes/No)
MaxResults	You can use this parameter to indicate the maximum number of items you want in the response. The default value is 50. The maximum value is 50.	integer	No	No
NextToken	You can use this parameter when paginating results. Set the value of this parameter to null on your first call to the list action. For subsequent calls to the action, fill nextToken in the request with the value of NextToken from the previous response to continue listing data.	String	No	No

**Output:**

Case Scope: N/A

Human Readable Output

ID	Name	Location	Format	Status	Tags
80c3132469ac6b11781 c78464a24be7a	testingFile	s3://newone12345678/ sample.txt	TXT	ERROR	N/A
b4c3138a4a6879ca994 cc9a8b2fa6bf2	testB	s3://newone12345678/ sample.txt	TXT	ERROR	N/A
e8c30bcd345cd75b60 9ba9dae9ceb92	testD1	s3://newone12345678/ sample.txt	TXT	ERROR	N/A

**12. Get Threat Intel Details**

Retrieves the ThreatIntelSet that is specified by the ThreatIntelSet ID.

**Request Headers**

Parameters	Datatype	Description	Required
Access Key	string	Access key of the particular user	Yes
Secret Key	string	Secret Key	Yes

**Path Parameters:**

Path Parameter	Description	Type	Scope restricted (Yes/No)	Required (Yes/No)
detectorId	The unique ID of the detector that the IPSet is associated with.	String	No	Yes
Threat Intel ID	The unique ID of the threatIntelSet that you want to get.	HOST, UNKNOWN, KEYWORD	No	Yes

**Output:**

Case Scope: N/A

Human Readable Output

Key	Value
Name	testingFile
Location	s3://newone12345678/sample.txt
Format	TXT
Status	ERROR
Tags	N/A

### 13. Add To Threat Intel List

Add IP to the Threat intel List.

- Rollback: Yes
- Duplicate Control: Yes

#### Request Headers:

Parameters	Datatype	Description	Required
Access Key	string	Access key of the particular user	Yes
Secret Key	string	Secret Key	Yes

#### Path Parameters:

Path Parameter	Description	Type	Scope restricted (Yes/No)	Required (Yes/No)
Bucket Name	The name of the S3 bucket	String	No	Yes
Key	The file path of S3 bucket file	String	No	Yes

#### Request Body Parameters:

Request Body	Description	Type	Scope restricted (Yes/No)	Required (Yes/No)
IPSET	The unique ID that specifies the IPSet that you want to update.	String	No	Yes

#### Output:

Case Scope: N/A

Human Readable Output: N/A

### 14. Remove from Threat Intel List

Remove IP from the Threat Intel List.

**Rollback:** No

**Duplicate Control:** No

#### Request Headers:

Parameters	Datatype	Description	Required
Access Key	string	Access key of the particular user	Yes
Secret Key	string	Secret Key	Yes

**Path Parameters:**

Path Parameter	Description	Type	Scope restricted (Yes/No)	Required (Yes/No)
Bucket Name	The name of the S3 bucket	String	No	Yes
Key	The file path of S3 bucket file	String	No	Yes

**Request Body Parameters:**

Request Body	Description	Type	Scope restricted (Yes/No)	Required (Yes/No)
IPSET	The unique ID that specifies the IPSet that you want to update.	String	No	Yes

**Output:**

Case Scope: N/A

Human Readable Output: N/A

**15. List Findings**

Lists Amazon GuardDuty findings for the specified detector ID

**Request Headers:**

Parameters	Datatype	Description	Required
Access Key	string	Access key of the particular user	Yes
Secret Key	string	Secret Key	Yes

**Path Parameters:**

Path Parameter	Description	Type	Scope restricted (Yes/No)	Required (Yes/No)
detectorId	The unique ID of the detector that the threatIntelSet is associated with.	String	No	Yes

Case Scope: N/A

Human Readable Output:

Id	Title	Description	Createdat	Updatedat	Severity
32c30b84f405c03e810864077adbf8d7	API DescribeEventAggregates was invoked using root credentials.	API DescribeEventAggregates was invoked using root credentials from IP address 116.73.106.231.	2023-02-03T11:29:30.635Z	2023-02-06T08:53:42.528Z	2
bcc3083cf61c295f31a07534e046a113	API GetObject was invoked using root credentials.	API GetObject was invoked using root credentials from IP address 157.33.202.140.	2023-02-02T04:54:31.224Z	2023-02-03T10:01:06.783Z	2
1ac305e788705883a93ccb033#0133ee	API DescribeEventAggregates was invoked using root credentials.	API DescribeEventAggregates was invoked using root credentials from IP address 103.5.134.251.	2023-02-01T07:09:25.088Z	2023-02-01T14:50:24.239Z	2
cac300a05ef689fee5e8bd178baa97a4	API DescribeEventAggregates was invoked using root credentials.	API DescribeEventAggregates was invoked using root credentials from IP address	2023-01-30T05:57:45.581Z	2023-01-31T14:33:12.708Z	2

## 16. Get Finding Detail

Describes Amazon GuardDuty findings specified by finding IDs.

### Request Headers

Parameters	Datatype	Description	Required
Access Key	string	Access key of the particular user	Yes
Secret Key	string	Secret Key	Yes

### Path Parameters:

Path Parameter	Description	Type	Scope restricted (Yes/No)	Required (Yes/No)
detectorId	The unique ID of the detector that the threatIntelSet is associated with.	String	No	Yes

### Request Body Parameters:

Request Body	Description	Type	Scope restricted (Yes/No)	Required (Yes/No)
findingids	The IDs of the findings that you want to retrieve.	String	No	Yes

### Output:

Case Scope: N/A

Human Readable Output:

Key	Value
Schema Version	2.0
Account Id	100420467922
Region	us-east-1
Partition	aws
Id	bcc3083cf51c295f31a07534e046a113
Arn	arn:aws:guardduty:us-east-1:100420467922:detector:48c264162c51fa034ab99ca81a341c/finding/bcc3083cf51c295f31a07534e046a113
type	Policy.IAMUserRootCredentialUsage
Resource	[{"accessKeyDetails": {"accessKeyId": "ASIAJ0YMGXTJMXXDQAZK", "principalId": "100420467922", "userName": "Root", "userType": "Root"}, "s3BucketDetails": [{"owner": {"id": "4899ad69247852c6e39a706e01128de91bdac27fe02eb437fe7be538e18"}}, {"publicAccess": {"effectivePermission": "NOT_PUBLIC", "permissionConfiguration": {"bucketLevelPermissions": [{"accessControlList": {"allowPublicReadAccess": false, "allowPublicWriteAccess": false}, "blockPublicAccess": {"restrictPublicBuckets": false, "blockPublicAcls": false, "ignorePublicAcls": false}, "bucketPolicy": {"allowPublicReadAccess": false, "allowPublicWriteAccess": false}, "accountLevelPermissions": {"blockPublicAccess": {"restrictPublicBuckets": false, "blockPublicAcls": false, "blockPublicPolicy": false, "ignorePublicAcls": false}}, "blockPublicPolicy": false, "ignorePublicAcls": false}}}], "type": {"destination": {}, "tags": {}, "createdAt": 1670832977, "name": "newone12345678", "defaultServerSideEncryption": null}, "arn": "arn:aws:s3:::newone12345678"}, {"resourceType": "S3Bucket"}]
Service	[{"count": 456, "serviceName": "guardduty", "archived": false, "resourceRole": "TARGET", "detectorId": "48c264162c51fa034ab99ca81a341c", "eventFirstSeen": "2023-02-03T09:56:03.000Z", "additionalInfo": {"type": "default", "value": "0"}, "action": {"actionType": "AWS_API_CALL", "awsApiCallAction": {"errorCode": "NoSuchWebsiteConfiguration", "serviceName": "s3.amazonaws.com", "awsApiCallAction": {"errorCode": "NoSuchWebsiteConfiguration", "serviceName": "s3.amazonaws.com", "ipAddressV4": "157.33.202.140", "geoLocation": {"lon": 72.8856, "lat": 19.0748}, "organization": {"awsOrg": "Reliance Jio Infocomm Limited", "org": "Jio", "isp": "Jio", "asn": "55836"}}, "affectedResources": [{"callerType": "Remote IP", "api": "GetObject"}]}]
Severity	2
Created At	2023-02-02T04:54:31.224Z
Updated At	2023-02-03T10:01:06.783Z
Title	API GetObject was invoked using root credentials.
Description	API GetObject was invoked using root credentials from IP address 157.33.202.140.

## 17. Archive Findings

Archives GuardDuty findings that are specified by the list of finding IDs.

**Rollback:** Yes

**Duplicate Control:** No

**Request Headers:**

Parameters	Datatype	Description	Required
Access Key	string	Access key of the particular user	Yes
Secret Key	string	Secret Key	Yes

**Path Parameters:**

Path Parameter	Description	Type	Scope restricted (Yes/No)	Required (Yes/No)
detectorId	The unique ID of the detector that the IPSet is associated with.	String	No	Yes

**Request Body Parameters:**

Request Body	Description	Type	Scope restricted (Yes/No)	Required (Yes/No)
findingIds	The IDs of the findings that you want to archive.	String	No	Yes

**Output:**

Case Scope: N/A

Human Readable Output: N/A

**18. Unarchive Findings**

Unarchives GuardDuty findings specified by the findingIds.

- **Rollback:** Yes
- **Duplicate Control:** No

**Request Headers:**

Parameters	Datatype	Description	Required
Access Key	string	Access key of the particular user	Yes
Secret Key	string	Secret Key	Yes

**Path Parameters:**

Path Parameter	Description	Type	Scope restricted (Yes/No)	Required (Yes/No)
detectorId	The unique ID of the detector that the IPSet is associated with.	String	No	Yes

Request Body	Description	Type	Scope restricted (Yes/No)	Required (Yes/No)
findingIds	The IDs of the findings that you want to archive.	String	No	Yes

**Output:**

Case Scope: N/A

Human Readable Output: N/A

**19. Update Finding Feedback**

Marks the specified GuardDuty findings as useful or not useful.

- Rollback: No
- Duplicate Control: No

**Request Headers:**

Parameters	Datatype	Description	Required
Access Key	string	Access key of the particular user	Yes
Secret Key	string	Secret Key	Yes

**Path Parameters:**

Path Parameter	Description	Type	Scope restricted (Yes/No)	Required (Yes/No)
detectorId	The unique ID of the detector that the threatIntelSet is associated with.	String	No	Yes

**Request Body Parameters:**

Request Body	Description	Type	Scope restricted (Yes/No)	Required (Yes/No)
comments	Additional feedback about the GuardDuty findings.	String	No	Yes
Feedback	The feedback for the finding. Valid Values: USEFUL   NOT_USEFUL	String	No	Yes
findingIds	The IDs of the findings that you want to mark as useful or not useful.	String	Yes	Yes

**Output:**

Case Scope: N/A

Human Readable Output: N/A

# Integration Guide for Amazon IAM

## Integration Overview

**Amazon AWS Identity and Access Management (IAM)** enables you to manage access to AWS services and resources securely. Using IAM, you can create and manage AWS users and groups, and use permissions to allow and deny their access to AWS resources.

## Integration Capabilities

ArcSight SOAR has the following integration capabilities with amazon IAM:

- Add User to Group
- Create Group
- Deactivate MFA Device
- Delete Access Key
- Delete All Access Keys
- Delete All SSH Public Keys
- Delete All Service Specific Credentials
- Delete Group
- Delete Login Profile
- Delete SSH Public Key
- Delete Service Specific Credential
- Delete User Policy
- Delete Virtual MFA Device
- Detach User Policy
- Get Access Key Last Used
- Get Group (List Group Members)
- Get Policy
- Get User Policy
- Get User
- List Access Keys
- List Attached User Policies

- List Entities for Policy
- List Groups
- List Groups for User
- List MFA Devices
- List SSH Public Keys
- List Service Specific Credentials
- List User Policies
- List User Tags
- List Users
- Remove User from Group

## Configuration

### Prerequisites

- You must have access to HTTPS as the ArcSight SOAR connects to [amazon iam](#) API through this service.
- Access key is required to access this service.

## Configuring SOAR

1. Click **Configuration > Credential > Create Credential**.
2. Specify the following parameter values in the **Credential Editor** form:

Type	Name	Username	Password	Private Key
Internal credential	Display name of credential set (for example,Amazon IAM Credential).	Empty	Access Key	Secret Key

3. Click **Configuration > Integrations > Create Integration**.
4. Specify the following parameter values in the **Configuration** form.

Parameter	Value
Name	Display name of the integration.
Type	Amazon IAM
Address	Address of the integration (the format must be <a href="https://iam.amazonaws.com">https://iam.amazonaws.com</a> ).

Parameter	Value	
Configuration	Specify the following configuration parameters:	
	<b>proxy.id</b>	ID of the proxy integration if you access amazon web services through a web proxy device. For example: proxy.id = 12345 .
Credential	Credential that has been defined for this integration in the <b>Credentials</b> menu.	
Trust Invalid SSL Certificates	Select this if web server's certificate is self-signed or is not recognized by browsers.	
Require Approval From	Select user(s) from list to ask the approval before executing actions on this integration.	
Notify	Select user(s) from the list to notify when SOAR performs an action on this integration.	

5. Click **Save** to save the integration definition.
6. Navigate to **Configuration>Customization Library** and edit **Amazon IAM Advanced Action Script Default Template**.
7. Select the integration that you have added in the **Integrations** menu.
8. Click **Save** to complete the integration.
9. Click **Test**, an **Integration Successful** message is displayed if the credential and address are valid.

## Capabilities

### 1. Add User to Group

Action capability for adding a user to given group.

- Rollback: Yes
- Duplicate Control: No

The following table presents the **Add User to Group** action capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Integration</b>	Name of the third party integration.	Integration	N/A	Yes
<b>Rollback Mode</b>	Time to rollback this action. Default is <b>no-rollback</b> .	N/A	N/A	No

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
User	Username to be added to group	Username Keyword Unknown	Yes	Yes
Group Name	Target group Name	String	No	Yes

**Output:**

Case Scope: N/A

Human Readable Output: N/A

**2. Create Group**

Action capability for creating a user group.

- Rollback: No
- Duplicate Control: False

The following table presents the **Create Group** action capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
Integration	Name of the third party integration.	Integration	N/A	Yes
Path Prefix	Path where the group is created.	String	No	Yes
Group Name	Target group Name	String	No	Yes

**Output:**

Case Scope: N/A

Human Readable Output: N/A

**3. Deactivate MFA**

Action capability for deactivating user's multi factor authentication device.

- Rollback: No
- Duplicate Control: Yes

The following table presents the **Deactivate MFA** action capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Integration</b>	Name of the third party integration.	Integration	N/A	Yes
<b>User</b>	Username	Username Keyword Unknown	Yes	Yes
<b>Serial Number</b>	MFA Device's serial number	String	No	Yes

**Output:**

Case Scope: N/A

Human Readable Output: N/A

**4. Delete Access Key**

Action capability for deleting user's access key.

- Rollback: No
- Duplicate Control: Yes

The following table presents the **Delete Access Key** action capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Integration</b>	Name of the third party integration.	Integration	N/A	Yes
<b>User</b>	Username	Username Keyword Unknown	Yes	Yes
<b>Access Key ID</b>	Access Key ID	String	No	Yes

**Output:**

Case Scope: N/A

Human Readable Output: N/A

**5. Delete All Access Keys**

Action capability for deleting user's all access keys.

- Rollback: No
- Duplicate Control: No

The following table presents the **Delete All Access Keys** action capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Integration</b>	Name of the third party integration.	Integration	N/A	Yes
<b>User</b>	Username	Username Keyword Unknown	Yes	Yes

**Output:**

Case Scope: No

Human Readable Output: No

**6. Delete All Service Specific Credentials**

Action capability for deleting user's all service specific credentials.

- Rollback: No
- Duplicate Control: No

The following table presents the **Delete All Service Specific Credentials** action capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Integration</b>	Name of the third party integration.	Integration	N/A	Yes
<b>User</b>	Username	Username Keyword Unknown	Yes	Yes

**Output:**

Case Scope: N/A

Human Readable Output: N/A

**7. Delete All SSH Public Keys**

Action capability for deleting user's all SSH public keys.

- Rollback: No
- Duplicate Control: No

The following table presents the **Delete All SSH Public Keys** action capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Integration</b>	Name of the third party integration.	Integration	N/A	Yes
<b>User</b>		Username Keyword Unknown	Yes	Yes

**Output:**

Case Scope: N/A

Human Readable Output: N/A

**8. Delete Group**

Action capability for deleting group.

- Rollback: No
- Duplicate Control: No

The following table presents the **Delete Group** action capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Integration</b>	Name of the third party integration.	Integration	N/A	Yes
<b>Group Name</b>	Group name to be deleted	String	Yes	Yes

**Output:**

Case Scope: N/A

Human Readable Output: N/A

**9. Delete Login Profile**

Action capability for deleting user's login profile.

- Rollback: No
- Duplicate Control: No

The following table presents the **Delete Login Profile** action capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Integration</b>	Name of the third party integration.	Integration	N/A	Yes
<b>User</b>	Username	Username Keyword Unknown	Yes	Yes

**Output:**

Case Scope: N/A

Human Readable Output: N/A

**10. Delete Service Specific Credential**

Action capability for deleting user's service specific credential.

- Rollback: No
- Duplicate Control: Yes

The following table presents the **Delete Service Specific Credential** action capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Integration</b>	Name of the third party integration.	Integration	N/A	Yes
<b>User</b>	Username	Username Keyword Unknown	Yes	Yes
<b>Credential ID</b>	Service specific credential Id to be deleted	String	No	Yes

**Output:**

Case Scope: N/A

Human Readable Output: N/A

**11. Delete SSH Public Key**

Action capability for deleting user's SSH public key.

The following table presents the **Delete SSH Public Key** action capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Integration</b>	Name of the third party integration.	Integration	N/A	Yes
<b>User</b>	Username	Username Keyword Unknown	Yes	Yes
<b>SSH Public Key Id</b>	SSH Public Key Id to be deleted.	String	No	Yes

**Output:**

Case Scope: N/A

Human Readable Output: N/A

**12. Delete User Policy**

Action capability for deleting user policy.

- Rollback: No
- Duplicate Control: No

The following table presents the **Delete User Policy** action capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Integration</b>	Name of the third party integration.	Integration	N/A	Yes
<b>User</b>	Username	Username Keyword Unknown	Yes	Yes
<b>Policy Name</b>	Policy to be deleted.	String	No	Yes

**Output:**

Case Scope: N/A

Human Readable Output: No/A

**13. Delete Virtual MFA Device**

Action capability for deleting virtual multi factor authentication device.

- Rollback: No
- Duplicate Control: Yes

The following table presents the **Delete Virtual MFA Device** action capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Integration</b>	Name of the third party integration.	Integration	N/A	Yes
<b>Serial Number</b>	Serial number of MFA device to be deleted.	String	No	Yes

**Output:**

Case Scope: N/A

Human Readable Output: N/A

**14. Detach User Policy**

Action capability for detaching policy from user.

- Rollback: No
- Duplicate Control: No

The following table presents the **Detach User Policy** action capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Integration</b>	Name of the third party integration.	Integration	N/A	Yes
<b>User</b>	Username Keyword Unknown	Username Keyword Unknown	Yes	Yes
<b>Policy arn</b>	Policy to be detached.	String	No	Yes

**Output:**

Case Scope: N/A

Human Readable Output: N/A

**15. Get Access Key Last Used**

Enrichment capability for retrieving last used information for access key.

The following table presents **Get Access Key Last Used** action capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Integration</b>	Name of the third party integration.	Integration	N/A	Yes
<b>Access Key ID</b>	Key ID to be queried .	String	No	Yes

**Output:**

Case Scope:

Enrichment	Type	Category Value
None	N/A	N/A

Human Readable Output:

User Name	Service	Region	Last Used Date
matt-acg	iam	us-east-1	1634811000

**16. Get Group**

Enrichment capability for retrieving list of group members.

The following table presents the **Get Group** action capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Integration</b>	Name of the third party integration.	Integration	N/A	Yes
<b>Group Name</b>	Group Name	String	No	Yes

**Output:**

Case Scope:

Enrichment	Type	Category Value
None	N/A	N/A

Human Readable Output:

User Name	User Id	Arn	Path
iamdev	[REDACTED]	arn:aws:iam:462521641599:user/ia /mdev	
iamdev2	[REDACTED]	arn:aws:iam:462521641599:user/ia /mdev2	

**17. Get Policy**

Enrichment capability for retrieving policy information.

The following table presents the **Get Policy** action capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
Integration	Name of the third party integration.	Integration	N/A	Yes
Policy arn	Policy arn.	String	No	Yes

**Output:**

Case Scope:

Enrichment	Type	Category Value
None	N/A	N/A

Human Readable Output:

Policy Name	Description	Version	Policy Id	Policy Arn	Path	Attachment Count	Create Date	Update Date
Company-AllowAllPolicy	Allow all policy for Company users	v1	ANPAWXMDQFJ756D834TOQ	arn:aws:iam::462521641599:policy/Company-AllowAllPolicy	/	2	1622529672	1622529672

**18. Get User**

Enrichment capability for retrieving user details.

The following table presents the **Get User** action capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
Integration	Name of the third party integration.	Integration	N/A	Yes
User	Username	Username Keyword Unknown	Yes	Yes

**Output:**

Case Scope:

Enrichment	Type	Category Value
None	N/A	N/A

Human Readable Output:

User Name	User Id	Arn	Path	Tags	Create Date	Password Last Used
iamdev	AIDAWXMDQFJ73QA Y4Q6AB	arn:aws:iam::4625216 41599:user/iamdev	/	[{"Value": "Engineering", "Key": "Dept"}, {"Value": "UI Expert", "Key": "Role"}, {"Value": "Ahmet Ozturk", "Key": "Manager"}]	1622166862	

## 19. Get User Policy

Enrichment capability for adding a user to given group.

The following table presents the **Get User Policy** action capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Integration</b>	Name of the third party integration.	Integration	N/A	Yes
<b>User</b>	Username to be added to group	Username Keyword Unknown	Yes	Yes
<b>Policy Name</b>	Policy name	String	No	Yes

### Output:

Case Scope:

Enrichment	Type	Category Value
None	N/A	N/A

## 20. List Access Keys

Enrichment capability for listing user's access keys.

The following table presents the **List Access Keys** action capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Integration</b>	Name of the third party integration.	Integration	N/A	Yes
<b>User</b>	Username	Username Keyword Unknown	Yes	Yes

### Output:

Case Scope:

Enrichment	Type	Category Value
None	N/A	N/A

Human Readable Output:

User Name	Key Id	Status	Create Date
iamdev	AKIAWXMDQFJ736000000	Active	1634811053

## 21. List Attached User Policies

Enrichment capability for listing attached user policies.

The following table presents the **List Attached User Policies** action capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Integration</b>	Name of the third party integration.	Integration	N/A	Yes
<b>User</b>	Username	Username Keyword Unknown	Yes	Yes

**Output:**

Case Scope:

Enrichment	Type	Category Value
None	N/A	N/A

Human Readable Output: No

Policy Name	Arn
AmazonS3FullAccess	arn:aws:iam::aws:policy/AmazonS3FullAccess
IAMUserChangePassword	arn:aws:siam::aws:policy/IAMUserChangePassword

## 22. List Entities for User Policy

Enrichment capability for listing entities for given user policy.

The following table presents the **List Entities for User Policy** action capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Integration</b>	Name of the third party integration.	Integration	N/A	Yes
<b>Policy Arn</b>	Policy arn	String	No	Yes

**Output:**

Case Scope:

Enrichment	Type	Category Value
None	N/A	N/A

Human Readable Output:

Type	Entity
Policy User	iamdev
Policy User	iamdelete

## 23. List Groups

Enrichment capability for listing groups under given path prefix.

The following table presents the **List Groups** action capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Integration</b>	Name of the third party integration.	Integration	N/A	Yes
<b>Path Prefix</b>	Path Prefix under groups to be listed.	String	No	Yes

**Output:**

Case Scope:

Enrichment	Type	Category Value
None	N/A	N/A

Human Readable Output:

Group Name	Group Id	Arn	Path	Create Date
Red Team	AGPAWXMDQFJ74NU000000	arn:aws:iam::462521641599:group/Devs/RedTeam	/Devs/RedTeam	1622545035
Admins	AGPAWXMDQFJ7Y4I700000	arn:aws:iam::462521641599:group/Admins	/up/Admins	1634813556

## 24. List Groups for User

Enrichment capability for listing user's groups.

The following table presents the **List Groups for User** action capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Integration</b>	Name of the third party integration.	Integration	N/A	Yes
<b>User</b>	Username Keyword Unknown	Username Keyword Unknown	Yes	Yes

**Output:**

Case Scope:

Enrichment	Type	Category Value
None	N/A	N/A

## Human Readable Output:

Group Name	Group Id	Arn	Path
AdminGroup	AGPAWXMDQFJ7SXY000000	arn:aws:siam:462521641599:group/AdminGroup	/
BillingGroup	AGPAWXMDQFJ7XN2000000	arn:aws:siam:462521641599:group/BillingGroup	/

**25. List MFA Devices**

Enrichment capability for listing user's MFA devices.

The following table presents the **List MFA Devices** action capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Integration</b>	Name of the third party integration.	Integration	N/A	Yes
<b>User</b>	Username Keyword Unknown	Username Keyword Unknown	Yes	Yes

**Output:**

Case Scope:

Enrichment	Type	Category Value
None	N/A	N/A

## Human Readable Output: No

**26. List Service Specific Credentials**

Enrichment capability for listing user's service specific credentials.

The following table presents the **List Service Specific Credentials** action capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
Integration	Name of the third party integration.	Integration	N/A	Yes
User	Username Keyword Unknown	Username	Yes	Yes

#### Output:

Case Scope:

Enrichment	Type	Category Value
None	N/A	N/A

Human Readable Output:

Service Name	User Name	Service User Name	Credential Id	Status	Create Date
codecommit.amazonaws.com	iamdev	iamdev-at-462521640000	ACCAWXMDQFJ7YE2V00000	Active	1633008565
cassandra.amazonaws.com	iamdev	iamdev-at-462521640000	ACCAWXMDQFJ743IJ00000	Active	1633008570

## 27. List SSH Public Keys

Enrichment capability for listing user's SSH Public Keys..

The following table presents the **List SSH Public Keys** action capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
Integration	Name of the third party integration.	Integration	N/A	Yes
User	Username to be added to group	Username Keyword Unknown	Yes	Yes

#### Output:

Case Scope:

Enrichment	Type	Category Value
None	N/A	N/A

Human Readable Output:

User Name	Key Id	Status	Upload Date
iamdev	APKAWXMDQFJ7Z2000000	Active	1633008559

## 28. List Users

Enrichment capability for listing users under the given path.

The following table presents the **List Uesrs** action capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Integration</b>	Name of the third party integration.	Integration	N/A	Yes
<b>Path Prefix</b>	Path Prefix under users to be listed.	String	No	Yes

### Output:

Case Scope:

Enrichment	Type	Category Value
None	N/A	N/A

### Human Readable Output:

User Name	Id	Arn	Path	Tags	Create Date	Password Last Used
jackbauer	AIDAWXMDQFJ74AU500000	arn:aws:iam::46252164:0000:user/jack	/		1610491406	
matt	AIDAWXMDQFJ7YZ600000	arn:aws:iam::46252164:0000:user/matt	/	admin	1589167999	1634810211

## 29. List User Policies

Enrichment capability for listing user's policies.

The following table presents the **List User Policies** action capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Integration</b>	Name of the third party integration.	Integration	N/A	Yes
<b>User</b>		Username Keyword Unknown	Yes	Yes

### Output:

Case Scope:

Enrichment	Type	Category Value
None	N/A	N/A

### 30. List User Tags

Enrichment capability for listing user's tags.

The following table presents the **List User Tags** action capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Integration</b>	Name of the third party integration.	Integration	N/A	Yes
<b>User</b>	Username	Username Keyword Unknown	Yes	Yes

**Output:**

Case Scope:

Enrichment	Type	Category Value
None	N/A	N/A

Human Readable Output: No

Key	Value
Dept	Engineering
Role	UI Expert
Manager	Ahmet Ozturk

### 31. Remove User from Group

Action capability for adding a user to given group.

- Rollback: Yes
- Duplicate Control: No

The following table presents the **Add User to Group** action capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Integration</b>	Name of the third party integration.	Integration	N/A	Yes
<b>Rollback Mode</b>	Time to rollback this action. Default is no-rollback.	N/A	N/A	No

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
User	Username to be added to group	Username Keyword Unknown	Yes	Yes
Group Name	Target group Name	String	No	Yes

**Output:**

Case Scope: N/A

Human Readable Output: N/A

# Integration Guide for Amazon S3

## Integration Overview

**Amazon S3** service is offered by Amazon Web Services which provides object storage through a web service framework.

## Integration Capabilities

ArcSight SOAR has the following integration capabilities with Amazon S3:

- Create Bucket
- Delete Bucket
- Download File From Bucket
- List Bucket Objects
- List Buckets
- Get Bucket Location

These capabilities can be performed automatically within a playbook or manually by an analyst.

## Prerequisites

- You must have access to HTTPS as the ArcSight SOAR connects to [Amazon S3 API](#) through this service.
- Access Key ID and Secret Access Key is also required for integration.

## Configuration

### Configuring SOAR

1. Click **Configuration > Credential > Create Credential**.
2. Specify the following parameter values in the **Credential Editor** form.

Type	Name	Username	Password	Private Key
Internal credential	Display name of credential set (for example, Amazon S3 Credential).		Access Key ID should be filled in this field.	Secret key should be filled in this field.

3. Click **Configuration > Integrations > Create Integration**.
4. Specify the following parameter values in the **Configuration** form.

Parameter	Value	
Name	Display name of the integration.	
Type	Amazon S3	
Address	Address of the integration (the format must be https://s3.amazonaws.com).	
Configuration	Specify the following configuration parameters:	
	<b>proxy.id</b>	ID of the Proxy integration if you access Amazon S3 through a web proxy device. For example: proxy.id = 12345 .
	<b>region</b>	Default region name that has to be used while working on buckets. For example, proxy.id = 12345.
Credential	Credential that has been defined for this integration in the <b>Credentials</b> menu.	
Trust Invalid SSL Certificates	Select this if web server's certificate is self-signed or is not recognized by browsers.	
Require Approval From	Select user(s) from list to ask the approval before executing actions on this integration.	
Notify	Select user(s) from the list to notify when SOAR performs an action on this integration.	

5. Click **Save** to save the integration definition.
6. Navigate to **Configuration>Customization Library** and edit **Amazon S3 Advanced Action Script Default Template**.
7. Select the integration that you have added in the **Integrations** menu.
8. Click **Save** to complete the integration.
9. Click **Test**, an **Integration Successful** message is displayed if the credential and address are valid.

## Capabilities

### 1. Create Bucket

Action capability for creating a bucket in Amazon S3.

The following table presents the **Create Bucket** action capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Bucket Name</b>	Name of the Amazon S3 Bucket that would be created.	String	N/A	Yes
<b>Region</b>	Region name of the bucket that would be created	List	N/A	No

**Output:**

Case Scope: N/A

Human Readable Output: N/A

**2. Delete Bucket**

Action capability for deleting a bucket in Amazon S3.

The following table presents the **Delete Bucket** action capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Bucket Name</b>	Name of the Amazon S3 Bucket that would be deleted.	String	N/A	Yes

**Output:**

Case Scope: N/A

Human Readable Output: N/A

**3. Download File From Bucket**

Enrichment capability for downloading a file from bucket.

The following table presents the **Download File From Bucket** enrichment capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Integration</b>	Name of the third party integration.	Integration	N/A	Yes
<b>Bucket Name</b>	Name of the bucket that contains the file.	String	N/A	Yes
<b>Key</b>	Name of the file to be downloaded.	String	No	Yes
<b>Do not Use Cache</b>	SOAR does not use cached results if this box is checked.	Boolean	N/A	No
<b>Region</b>	Region name of the bucket that would be created	List	N/A	No

**Output:**

Case Scope:

Enrichment	Type	Category/ Value
Download File From Bucket	Any	File
Download File From Bucket	String	File Name
Download File From Bucket	MD5	#
Download File From Bucket	SHA1	#

Human Readable Output:

a few seconds ago - [REDACTED] downloaded AMAZON\_S3\_2//DOWNLOAD\_FILE\_FROM\_BUCKET-[REDACTED]

#### 4. List Bucket Objects

Enrichment capability for listing bucket objects in Amazon S3.

The following table presents the **List Bucket Objects** enrichment capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
Integration	Name of the third party integration.	Integration	N/A	Yes
Bucket Name	Name of the bucket that contains the file.	String	N/A	Yes
Do not Use Cache	SOAR does not use cached results if this box is checked.	Boolean	N/A	No
Region	Region name of the bucket that would be created	List	N/A	No

**Output:**

Case Scope: N/A

Human Readable Output:

Key	Last Modified	Etag	Size in Bytes	Storage Class
[REDACTED]	2021-09-28T10:08:11.000Z	[REDACTED]	31	STANDARD

#### 5. List Buckets

Enrichment capability for listing a buckets in Amazon S3.

The following table presents the **List Buckets** enrichment capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
Integration	Name of the third party integration.	Integration	N/A	Yes

**Output:**

Case Scope: N/A

### Human Readable Output:

Bucket Name	Bucket Creation Date
-ports	2020-10-01T11:12:19.000Z
-1-app-logs	2021-02-14T09:19:03.000Z
-1-elb-logs	2021-02-14T09:19:03.000Z
-1-s3-logs	2021-02-14T09:18:33.000Z
-1-vpc-flow-logs	2021-02-14T09:19:04.000Z
-app-logs	2020-10-01T11:12:57.000Z
-elb-logs	2020-10-01T11:12:57.000Z
-s3-logs	2020-10-01T11:12:18.000Z
-vpc-flow-logs	2020-10-01T11:12:57.000Z
soar-test	2021-09-28T07:45:29.000Z

### 6. Get Bucket Location

Enrichment capability of getting region of the bucket.

The following table presents the **List Buckets** enrichment capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
<b>Integration</b>	Name of the third party integration.	Integration	N/A	Yes
Bucket Name	Name of the Bucket	String	No	Yes

### Output:

Case Scope: N/A

### Human Readable Output:

Bucket	Location
-1-s3-logs	us-east-1

# Integration Guide for APIVoid

## Integration Overview

**APIVoid** is an API service for threat analysis and threat detection and prevention.

## Integration Capabilities

ArcSight SOAR has the following integration capabilities with APIVoid:

- IP Reputation
- ThreatLog Domain Query
- Domain Reputation
- URL Screenshot
- URL Reputation
- Domain Age
- Site Trustworthiness
- Parked Domain
- URL Status
- HTTP Tracker
- Email Verify
- DNS Lookup
- DNS Propagation
- SSL Info
- URL to HTML
- URL to PDF

## Prerequisites

- You must have the network access through [APIVoid](#)
- You must have the APIVoid API key.

# Configuration

## Configuring APIVoid

1. Register to **APIVoid**. After logging, the API key is available.
2. Click **My API Keys** and copy the API key.

## Configuring SOAR

1. Click **Configuration > Integration > Create Integration**.
  2. Click **Create**. In **Configuration Editor** specify following values to create a credential:
 

Type	Name	Username	Password	Private Key
Internal credential	Display name of credential set (for example, APIVoid Credential).			API Key that you copied from APIVoid portal.
  3. Click **Save** to save the integration definition.
  4. Navigate to **Configuration>Customization Library** and edit **APIVoid Advanced Action Script Default Template**.
  5. Select the integration that you have added in the **Integrations** menu.
  6. Click **Save** to complete the integration.
  7. Click **Test**, an **Integration Successful** message is displayed if the credential and address are valid.
1. **IP Reputation**  
 Enrichment capability for retrieving reputation value of given IP address.  
 Following table presents the **IP reputation** enrichment capability details:

## Capabilities

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
<b>Integration</b>	Name of the third party integration.	Integration	N/A	Yes
<b>IP</b>	IP address to retrieve reputation.	Network Address Host	Yes	Yes

### Output:

Case Scope: N/A

## Human Readable Output:

Parameters Details	
Field	Value
credits_Remained	19.46
data_Report_anonymity_is_hosting	false
data_Report_anonymity_is_proxy	false
data_Report_anonymity_is_tor	false
data_Report_anonymity_is_vpn	false
data_Report_anonymity_is_webproxy	false
data_Report_blacklists_detection_rate	0%
data_Report_blacklists_detections	0
data_Report_blacklists_engines_0_detected	false
data_Report_blacklists_engines_0_elapsed	0.03

## 2. ThreatLog Domain Query

Enrichment capability to query a domain for ThreatLog.

Following table presents the **ThreatLog Domian Query** enrichment capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
Integration	Name of the third party integration.	Integration	N/A	Yes
Domain	Host to query	HOST	Yes	Yes

**Output:**

Case Scope: N/A

Human Readable Output

Parameters Details	
Field	Value
elapsed_time	0.03
error	Host is not valid
Total 2 , 100 ▾ items / page	

### 3. Domain Reputation

Enrichment capability to retrieve Domain Reputation.

Following table presents the **Domain Reputation** enrichment capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
Integration	Name of the third party integration.	Integration	N/A	Yes
Domain	Host to query	HOST	Yes	Yes

#### Output:

Case Scope: N/A

Human Readable Output:

Parameters Details	
Field	Value
credits_Remained	19.38
data_report_blacklists_detection_rate	0%
data_report_blacklists_detections	0
data_report_blacklists_engines_0_confidence	low
data_report_blacklists_engines_0_detected	false
data_report_blacklists_engines_0_elapsed	0.00
data_report_blacklists_engines_0_engine	Phishing Test

### 4. URL Screenshot

Enrichment capability to take a screenshot for given URL by APIVoid.

Following table presents the **URL Screenshot** enrichment capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
Integration	Name of the third party integration.	Integration	N/A	Yes
URL	URL to take screenshot.	URL	Yes	Yes

#### Output:

Case Scope: N/A

Human Readable Output:

Parameters Details	
Field	Value
elapsed	2.95
file_md5_hash	828ce39cd28ac7e03f5
file_size_bytes	428154
file_size_readable	418.1KB
format	PNG
image_height	768
image_width	1024

## 5. URL Reputation

Enrichment capability to retrieve URL reputation.

Following table presents the **URL Reputation** enrichment capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
<b>Integration</b>	Name of the third party integration.	Integration	N/A	Yes
<b>URL</b>	URL to retrieve reputation.	URL	Yes	Yes

### Output:

Case Scope: N/A

Human Readable Output:

Parameters Details	
Field	Value
credits_reained	17.48
data_report_dns_records_mx_records	[{"ip": "68.65.120.250", "isp": "Namecheap Inc.", "target": "mail.gmifan.com", "country_code": "US", "country_name": "United States of America"}]
data_report_dns_records_ns_records	[{"ip": "156.154.132.200", "isp": "Neustar Inc.", "target": "dns1.namecheaphosting.com", "country_code": "US", "country_name": "United States of America"}, {"ip": "156.154.133.200", "isp": "Neustar Inc.", "target": "dns2.namecheaphosting.com", "country_code": "US", "country_name": "United States of America"}]

## 6. Domain Age

Enrichment capability to retrieve domain age information.

Following table presents the **Domain Age** enrichment details:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Integration</b>	Name of the third party integration.	Integration	N/A	Yes
<b>Domain</b>	Domain to retrieve age information.	HOST	Yes	Yes

**Output:**

Case Scope: N/A

Human Readable Output:

Parameters Details	
Field	Value
credits_Remained	16.98
data_Debug_Message	
data_Domain_Age_Found	true
data_Domain_Age_In_Days	26
data_Domain_Age_In_Months	0
data_Domain_Age_In_Years	0
data_Domain_Creation_Date	2021-09-05
data_Domain_Registered	yes

**7. Site Trustworthiness**

Enrichment capability to retrieve site trustworthiness score / information

Following table presents the **Site Trustworthiness** enrichment capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Integration</b>	Name of the third party integration.	Integration	N/A	Yes
<b>Host</b>	Host to retrieve site trustworthiness information.	HOST	Yes	Yes

**Output:**

Case Scope: N/A

Human Readable Output:

Parameters Details	
Field	Value
credits_Remained	16.13
data_report_dns_records_mx_records	[{"ip": "68.65.120.250", "isp": "Namecheap Inc.", "target": "mail.gmtloan.com", "country_code": "US", "country_name": "United States of America"}]
data_report_dns_records_ns_records	[{"ip": "156.154.132.200", "isp": "Neustar Inc.", "target": "dns1.namecheaphosting.com", "country_code": "US", "country_name": "United States of America"}, {"ip": "156.154.133.200", "isp": "Neustar Inc.", "target": "dns2.namecheaphosting.com", "country_code": "US", "country_name": "United States of America"}]
data_report_domain_age_domain_age_in_days	26

## 8. Parked Domain

Enrichment capability to retrieve information for parked domain.

Following table presents the **Parked Domain** enrichment capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
<b>Integration</b>	Name of the third party integration.	Integration	N/A	Yes
<b>Domain</b>	Domain to retrieve information.	HOST	Yes	Yes

### Output:

Case Scope: N/A

Human Readable Output:

Parameters Details	
Field	Value
credits_Remained	15.83
data_a_records_found	true
data_host	gmtloan.com
data_parked_domain	false
elapsed_time	1.00
estimated_queries	52
success	true

## 9. URL Status

Enrichment capability to retrieve URL Status information.

Following table presents the **URL Status** enrichment capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
<b>Integration</b>	Name of the third party integration.	Integration	N/A	Yes
<b>URL</b>	URL to retrieve status.	URL	Yes	Yes

**Output:**

Case Scope: N/A

Human Readable Output:

Parameters Details	
Field	Value
credits_Remained	15.43
data_report_analysis_http_client_error	false
data_report_analysis_http_server_error	true
data_report_analysis_http_status_code	0
data_report_analysis_sinkholed_domain	false
data_report_analysis_suspended_page	false
data_report_analysis_url_status	offline

**10. HTTP Tracker**

Enrichment capability for tracking http requests per URL.

Following table presents the **HTTP Tracker** enrichment capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
<b>Integration</b>	Name of the third party integration.	Integration	N/A	Yes
<b>URL</b>	URL to track http requests.	HOST	Yes	Yes

**Output:**

Case Scope: N/A

Human Readable Output:

Parameters Details		Search
Field	Value	
credits_remainded	17.98	
data_hosts_contacted	[ "fonts.googleapis.com", "fonts.gstatic.com", "gmtloan.com" ]	
data_hosts_total	3	
data_http_requests	[ "https://www.gmtloan.com/", "https://www.gmtloan.com/inc/assets/css/bootstrap.min.css", "https://www.gmtloan.com/inc/assets/css/animate.min.css", "https://www.gmtloan.com/inc/assets/css/mennmenu.css" ]	

## 11. Email Verify

Enrichment capability that verifies given E-mail address.

Following table presents the **Email Verify** enrichment capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Integration</b>	Name of the third party integration.	Integration	N/A	Yes
<b>Email Address</b>	Email Address to verify.	EMAIL_ADDRESS	Yes	Yes

### Output:

Case Scope: N/A

Human Readable Output:

Parameters Details	
Field	Value
credits_remainded	15.37
data_china_free_email	false
data_did_you_mean	false
data_dirty_words_domain	false
data_dirty_words_username	false
data_disposable	false
data_dmarc_configured	true

## 12. DNS Lookup

Enrichment capability to lookup for DNS per given host.

Following table presents the **DNS Lookup** enrichment capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Integration</b>	Name of the third party integration.	Integration	N/A	Yes
<b>HOST</b>	Host or domain to lookup.	HOST	Yes	Yes

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Lookup Type</b>	DNS Lookup type. Can be one of the following: "dns-a", "dns-aaaa", "dns-mx", "dns-ns", "dns-dmark", "dns-ptr", "dns-txt", "dns-any", "dns-cname", "dns-soa", "dns-srv", "dns-caa".	ENUM	No	Yes

**Output:**

Case Scope: N/A

Human Readable Output:

Parameters Details	
Field	Value
credits_Remained	15.31
data_host	gmtloan.com
data_records_count	1
data_records_found	true
data_records_items	[{"ip": "68.65.120.250", "type": "A", "ttl": 1200, "host": "gmtloan.com", "class": "IN"}]
elapsed_time	0.07
estimated_queries	255
success	true

**13. DNS Propagation**

Enrichment capability to check for DNS of the given host.

Following table presents the **DNS Propagation** enrichment capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Integration</b>	Name of the third party integration.	Integration	N/A	Yes
<b>Email Address</b>	Host or domain to lookup.	HOST	Yes	Yes
<b>Lookup Type</b>	DNS Lookup type. Can be one of the following: "A", "AAAA", "NS", "MX", "TXT", "SRV", "PTR", "SOA", "CNAME", "SPF", "CAA".	ENUM	No	Yes

**Output:**

Case Scope: N/A

Human Readable Output:

Parameters Details		Search
Field	Value	
credits_remainded	12.81	
data_dns_type	A	
data_host	gmfloan.com	
data_propagation	[{"country_code": "AU", "service": "Cloudflare", "response": "68.65.120.250\n"}, {"country_code": "US", "service": "Google", "response": "68.65.120.250\n"}, {"country_name": "United States", "country_code": "US", "service": "Comodo", "response": "68.65.120.250\n"}, {"country_name": "United States", "country_code": "US", "service": "OpenDNS", "response": "68.65.120.250\n"}, {"country_name": "Russia", "country_code": "RU", "service": "Fortinet Inc", "response": "68.65.120.250\n"}, {"country_name": "Russia", "country_code": "RU", "service": "Yandex", "response": "68.65.120.250\n"}]	

## 14. SSL Info

Enrichment capability to retrieve SSL information.

Following table presents the **SSL Info** enrichment capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
<b>Integration</b>	Name of the third party integration.	Integration	N/A	Yes
<b>HOST</b>	Host or domain to lookup.	HOST	Yes	Yes

### Output:

Case Scope: N/A

Human Readable Output:

Parameters Details		Search
Field	Value	
credits_remainded	12.74	
data_certificate_blacklisted	false	
data_certificate_debug_message		
data_certificate_deprecated_issuer	false	
data_certificate_details_extensions_authority_info_access	CA Issuers - URL: http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt OCSP - URL: http://ocsp.sectigo.com	
data_certificate_details_extensions_authority_key_identifier	keyId:BD:8C:5E:C4:S4:AD:8A:E1:77:E9:F9:9B:05:E1:BB:01:BD:61:E1	

## 15. URL to HTML

Following table presents the **URL to HTML** enrichment capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
<b>Integration</b>	Name of the third party integration.	Integration	N/A	Yes
<b>URL</b>	URL to retrieve HTML.	URL	Yes	Yes

### Output:

Case Scope: N/A

**Human Readable Output:**

The screenshot shows a 'Parameters Details' table with the following data:

Field	Value
elapsed	2.78
file_md5_hash	790a3c088434013fd4de2bc9eaea71e
file_size_bytes	38975
file_size_readable	38.1KB
format	HTML

Total 5, 100 items / page

A few seconds ago - gurkan aslan commented  
<https://www.gmtloan.com>

```

<!DOCTYPE html><html lang="en"><head>
<title>Home | GMT LOAN</title>
<meta charset="UTF-8">

<meta name="description" content="We help organizations across the private, public, and social sectors create Change that Matters.">
<meta name="keywords" content="Home, GMT LOAN">

<meta property="og:locale" content="en_US">
<meta property="og:type" content="website">
<meta property="og:title" content="GMT LOAN">
<meta property="og:description" content="We help organizations across the private, public, and social sectors create Change that Matters.">
<meta property="og:url" content="http://gmtloan.com">
<meta property="og:site_name" content="GMT LOAN">
<meta name="twitter:card" content="summary_large_image">
<meta name="twitter:description" content="We help organizations across the private, public, and social sectors create Change that Matters.">
<meta name="twitter:title" content="GMT LOAN">
```

**16. URL to PDF**

Enrichment capability to retrieve PDF file from URL.

Following table presents the **URL to PDF** enrichment capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
<b>Integration</b>	Name of the third party integration.	Integration	N/A	Yes
<b>URL</b>	URL to retrieve PDF.	URL	Yes	Yes

**Output:**

Case Scope: N/A

**Human Readable Output:**

Parameters Details

Field	Value
elapsed	1.95
file_md5_hash	ae5235c90cb5b93963c9e9474ccb7ae5
file_size_bytes	1626964
file_size_readable	1.6MB
format	PDF

Total 5,  items / page

a few seconds ago -  gurkan aslan commented  
<https://www.gmtloan.com>

 url.pdf (1589KB)

# Integration Guide for Anomali ThreatStream

## Integration Overview

**Anomali ThreatStream** is a Threat Intelligence Platform that enables businesses to integrate security products and leverage threat data to defend against cyber threats.

## Integration Capabilities

ArcSight SOAR has the following integration capabilities with Anomali ThreatStream:

- Domain Reputation
- Email Reputation
- File Reputation
- Get Incident Details
- Get Intelligence
- Get Investigation Details
- IP Reputation
- List Incidents
- List Investigations
- Report Indicator
- Create Investigation
- Close Investigation
- Update Investigation

### Use Case: Investigating Phishing Campaigns

SOAR, when integrated with Anomali ThreatStream, helps campaigns that investigate and mitigate phishing. When a phishing report email comes from a user, SOAR extracts the indicators such as IP address, URLs and attachments in the message and creates an incident on the Incident Management Service Desk. SOAR then checks with Anomali ThreatStream, to know if this is a known attack and whether these indicators were previously analyzed.

This investigation can be either performed automatically within a playbook or manually by an analyst.

# Configuration

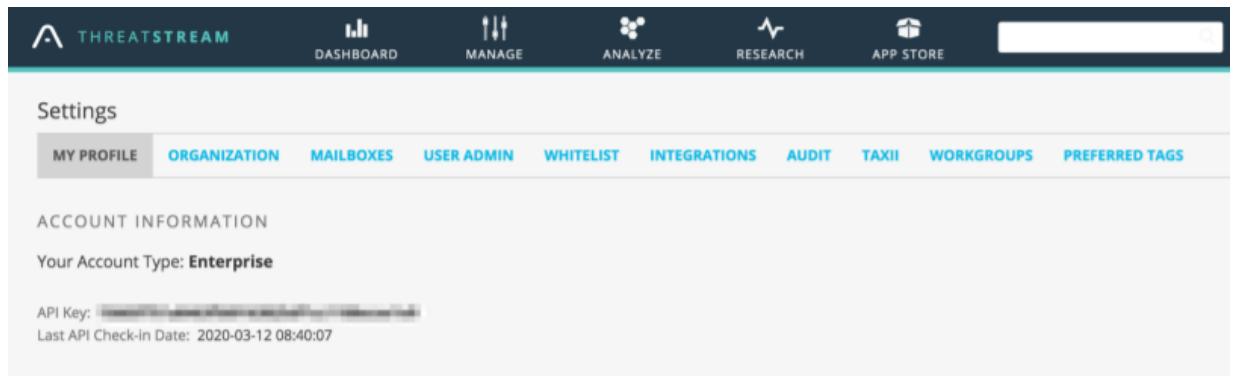
## Prerequisites

- SOAR connects to Anomali ThreatStream API via HTTPS. Access to <https://api.threatstream.com/>(443/tcp port) is required.
- An API key is required for SOAR to connect to Anomali ThreatStream Service.

## Configuring Anomali ThreatStream

1. Log in to <https://ui.threatstream.com/>.
2. Navigate to **Settings > My Profile** to get the API Key.

 **Note:** This key is required by SOAR to access the platform for queries.



The screenshot shows the Anomali ThreatStream user interface. At the top, there's a navigation bar with icons for ThreatStream, Dashboard, Manage, Analyze, Research, and App Store. Below the navigation bar, the title 'Settings' is displayed, followed by a horizontal menu with tabs: MY PROFILE (which is active and highlighted in blue), ORGANIZATION, MAILBOXES, USER ADMIN, WHITELIST, INTEGRATIONS, AUDIT, TAXII, WORKGROUPS, and PREFERRED TAGS. Under the 'MY PROFILE' tab, the 'ACCOUNT INFORMATION' section is visible, showing 'Your Account Type: Enterprise'. Below this, it shows 'API Key: [REDACTED]' and 'Last API Check-in Date: 2020-03-12 08:40:07'.

## Configuring SOAR

1. Configuration > Credentials > Create Credential.
2. Fill the **Credential Editor** form with the following details:
  - a. Internal Credential:

Parameter	Value
Type	Internal credential
Name	Display name of credential set (For example, Anomali ThreatStream Credentials)
Username	Your username on Anomali ThreatStream platform
Password	Empty
Private Key	API key you have obtained from Anamoli ThreatStream Platform

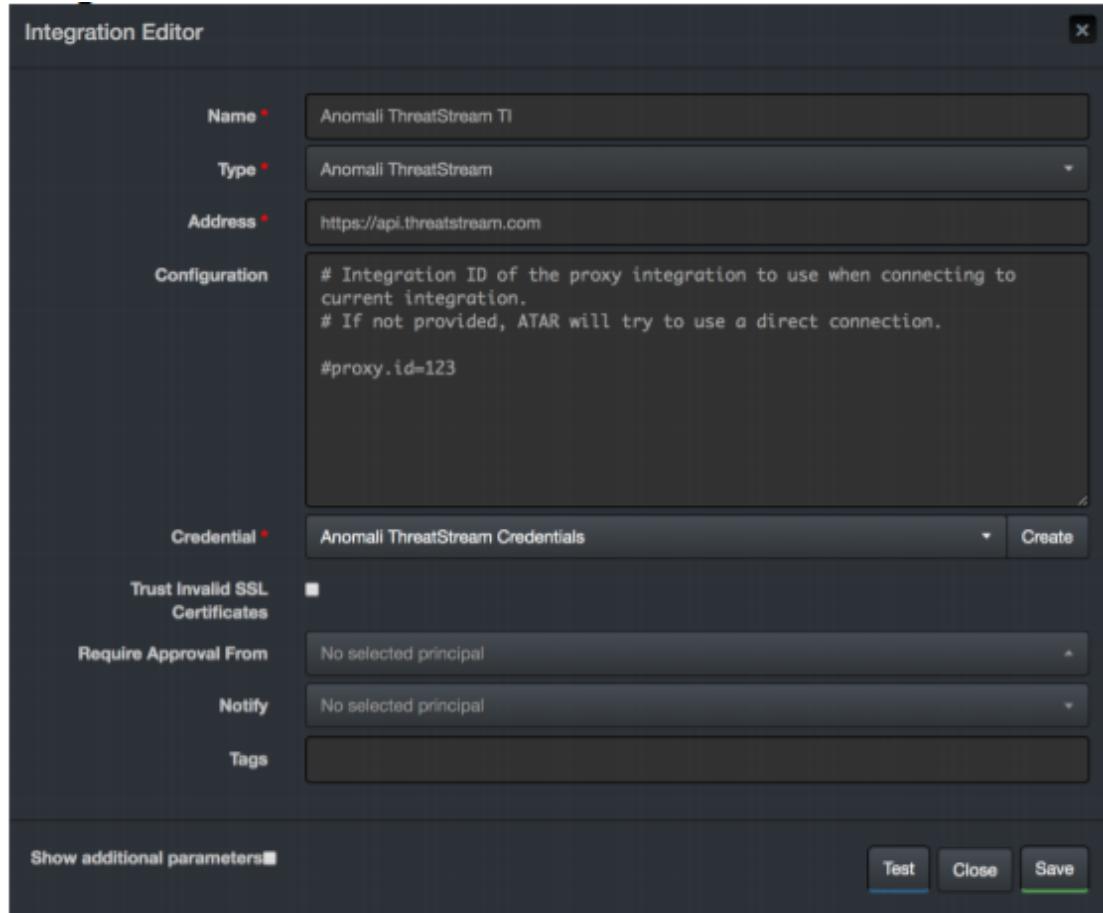
**b. Credential Store:**

Parameter	Value
Type	External credential
Name	Name of the credential with full path of the safe on store

**3. Configuration > Integrations > Create Integration.**

4. Fill the configuration form with the following parameter values:

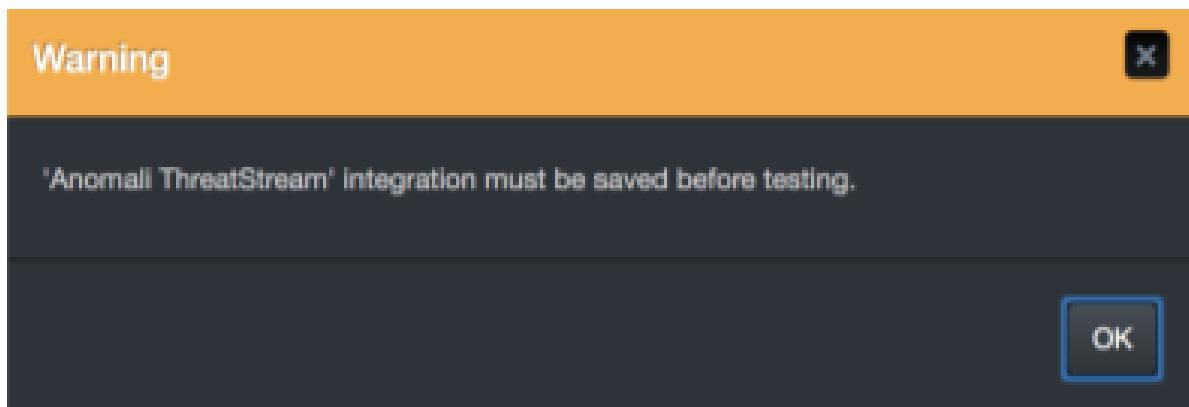
Parameter	Value
Name	Display name of Anomali ThreatStream integration on SOAR
Type	Anomali ThreatStream
Address	Address of the integration ( <a href="https://api.threatstream.com">https://api.threatstream.com</a> ).
Configuration	You need to specify the following configuration parameters: <pre># Integration ID of the proxy integration to use when connecting to # current integration. # If not provided, ATAR will try to use a direct connection. #proxy.id=123</pre>
Credential	Name of the credential set you have just created on step 2. (For example, Anomali ThreatStream Credentials)
Trust Invalid SSL Certificates	No selection required
Require Approval From	Select user(s) from list to ask her/his approval before executing actions on this integration.
Notify	Select user(s) from the list to notify when SOAR performs an action on this integration.



5. Click **Save** to complete integration.
6. Click **Test** to test the integration.

## Additioinal Notes

- Anomali ThreatStream integration on SOAR is an Advanced Script and content of the default script is accessible under **Configuration > Customization Library**.
- While defining the integration for the first time, you might encounter the following warning message, which is the expected behavior for this type of integration.



# Integration Guide for Arbor Networks APS

## Integration Overview

**Arbor Networks APS** is an in-line Distributed Denial of Service(DDoS) protection solution.

## Integration Capabilities

ArcSight has the following integration capabilities with Arbor Networks APS:

- Block IP
- Block access to IP

### Use Case: Blocking malicious IP on peripheral

ArcSight SOAR integrates with Arbor Networks APS to block malicious IP addresses detected while responding to an incident. SOAR can block both the incoming and outgoing traffic either automatically within a playbook or manually by an analyst.

## Configuration

### Prerequisites

- SOAR connects to Arbor Networks APS' API via HTTPS. By default, the API interface works on **443/tcp port**. So access permission to this port is required.
- An API access token needs to be created for SOAR to connect to Arbor Networks APS.

### Configuring Arbor Networks APS

1. Log in to Arbor Networks APS device.
2. Add a new API token.

```
admin@arbos: /# serv aaa local apitoken generate admin ATAR_INTEGRATION
Added token: jwP9JcmZYz4I9QH0LpkDA_n5nj_DNHifc6Iwsq0P
```



**Note:** SOAR uses the generated token as the credential password and user name as admin.

## Configuring SOAR

1. Click **Configuration > Credentials > Create Credential**.
2. Fill the **Credential Editor form** with the following parameter values:

a. **Internal Credential:**

Parameter	Value
Type	Internal credential
Name	Display name of the credential set (For example, Arbor APS Credential)
Username	admin
Password	API Token you have created for SOAR on Arbor Networks APS device
Private Key	Empty

b. **Credential Store:**

Parameter	Value
Type	External credential
Name	Name of the credential with pull path of the safe on store

3. **Configuration > Integrations > Create Integration**.
4. Fill the configuration form with the following parameter values:

Parameter	Value
Name	Display name of Arbor Networks APS integration on SOAR
Type	Arbor Networks APS
Address	Address of the integration (the format should be http(s)://1.1.1.1:1234 or http[s]://abc.example.com:1234)
Password	API Token you have created for SOAR on Arbor Networks APS device
Credential	Name of the credential set you have just created on step 2. (For example, Arbor APS Credential)
Trust Invalid SSL Certificates	Select this if device's certificate is self-signed or not recognized by browsers
Require Approval From	Select user(s) from list to ask her/his approval before executing actions on this integration
Notify	Select user(s) from the list to notify when ATAR performs an action on this integration

5. Click **Test**.The following pop up will be displayed if your credential and address are valid.
6. Click **Save** to complete integration.

# Integration Guide for AWS Network Firewall

## Integration Overview

AWS Network Firewall is a managed service that makes it easy to deploy essential network protections for all of your Amazon Virtual Private Clouds (VPCs). AWS Network Firewall's flexible rules engine allows you to define firewall rules that provide fine-grained control over network traffic, such as blocking outbound Server Message Block (SMB) requests to prevent the spread of malicious activity. AWS Network Firewall's stateful firewall can incorporate context from traffic flows, like tracking connections and protocol identification, to enforce policies such as preventing your VPCs from accessing domains using an unauthorized protocol.

## Integration Capabilities

ArcSight SOAR has the following integration capabilities with AWS Network Firewall:

- Create Stateful Rule Group
- Create Stateless Rule Group
- Add Stateful Rule
- Add Stateless Rule
- Delete Rule Group
- Delete Stateful Rule
- Delete Stateless Rule
- List Firewalls
- List Rule Groups
- List Firewall Policies
- Get Firewall Policies
- Get Firewall Rule Group

## Prerequisites

- ArcSight SOAR connects to AWS Network Firewall API using HTTPS. Access to <https://aws.amazon.com/network-firewall> is required.

- **Access key ID** and **Secret Access key** are required for ArcSight SOAR to connect to AWS Network Firewall.

## Configuration

### Configuring AWS Network Firewall

1. Log in to [Amazon AWS](#).
2. Navigate to **My Security Credentials** and select **Identity Access Management (IAM)** service.
3. Click **Access Management > Users > Add User** to add an IAM user.
4. Select **Access Type as Programmatic Access**.
5. You can skip the next steps until **Access Key** and **Secret Access Key** are displayed.



Download the credentials as the Secret Access Key is not displayed post this step.

6. Add the following action permissions if you require admin permissions for this service or contact your AWS cloud support:

```
[  
  "network-firewall>ListTagsForResource",  
  "network-firewall>DeleteRuleGroup",  
  "network-firewall>DescribeLoggingConfiguration",  
  "network-firewall>CreateRuleGroup",  
  "network-firewall>DescribeRuleGroupMetadata",  
  "network-firewall>DescribeFirewall",  
  "network-firewall>UpdateRuleGroup",  
  "network-firewall>ListRuleGroups",  
  "network-firewall>DescribeRuleGroup",  
  "network-firewall>DescribeFirewallPolicy",  
  "network-firewall>ListFirewalls",  
  "network-firewall>TagResource",  
  "network-firewall>DescribeResourcePolicy",  
  "network-firewall>DeleteFirewall",  
  "network-firewall>ListFirewallPolicies"  
]
```

# Configuring SOAR

1. Click **Configuration > Credential > Create Credential**.
2. Specify the following parameter values in the **Credential Editor**:

Type	Name	Username	Password	Private Key
Internal Credential	Display name of credential set ( for example, Amazon Network Firewall Credentials).	Empty	Access Key	Secret Key

3. Click **Configuration > Integrations > Create Integration**.
4. Specify the following parameter values in the **Configuration Form**:

Parameter	Value					
Name	Display name of the integration					
Type	Amazon Network Firewall					
Address	Address of the integration should follow the format <code>https://networkfirewall.amazonaws.com:443</code> For specific region, the integration should follow the format <code>https://network-firewall. region.amazonaws.com</code>					
Configuration	Specify the following configuration parameter values: <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 15%;">Region</td> <td>Region is required for retrieving the correct endpoint for current integration. For example: ap-southeast-1</td> </tr> <tr> <td>proxy.id</td> <td>Integration ID of the proxy to use current intergration. For example: Proxy.id=12345</td> </tr> </table>		Region	Region is required for retrieving the correct endpoint for current integration. For example: ap-southeast-1	proxy.id	Integration ID of the proxy to use current intergration. For example: Proxy.id=12345
Region	Region is required for retrieving the correct endpoint for current integration. For example: ap-southeast-1					
proxy.id	Integration ID of the proxy to use current intergration. For example: Proxy.id=12345					
Credential	Credential that has been defined for this integration under the Credentials menu					
Trust Invalid SSL Certificates	Select this option if the firewall's web certificate is self-signed or if it is not recognized by browsers					
Require Approval From	Select user(s) from list who can provide approval before executing actions on this integration					
Notify	Select user(s) from the list who can provide approval when SOAR performs an action on this integration					

5. Click **Save**.

6. Navigate to **Configuration > Customization Library** and edit **Amazon Network Firewall Advanced Action Script Default Script Template**.
7. Select the integration that you have created in step 4 from the **Integrations** drop-down menu and click **Save**.
8. Click **Test**, an **Integration Successful** message is displayed if the credential and address are valid.

## Capabilities

### 1. Create Stateful Rule Group

Action capability for creating a Stateful Rule Group for blocking IP address.

- Rollback: No
- Duplicate Control: No

The following table presents the **Create Stateful Rule Group** action capabilities details:

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
Integration	Name of the third party integration	Integration	N/A	Yes
Rollback Mode	Time to rollback this action. Default is no-rollback.	N/A	N/A	No
Rule Group Name	Name of the Rule Group	String	No	No
Action	Action to be taken (PASS,DROP,ALERT)	String	No	Yes
Header Protocol	Header Protocol (TCP,HTTP,ICMP and so on)	String	No	Yes
Capacity	Capacity	Integer	No	Yes
Header Source	IP Address	String	No	Yes
Header Source Port	Source Port	String	No	Yes
Header Destination	IP Address	String	No	Yes
Header Destination Port	Destination Port	String	No	Yes
Direction	Direction (FORWARD,ANY)	String	No	Yes
Rule Order	Rule Order to be executed	String	No	Yes

### Output:

N/A

Human Readable Output

N/A

## 2. Create Stateless Rule Group

Action capability for creating a Stateless Rule Group for blocking IP address.

- Rollback: No
- Duplicate Control: No

The following table presents the **Create Stateless Rule Group** action capabilities details:

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
Integration	Name of the third party integration	Integration	N/A	Yes
Roll Back mode	Time to rollback this action. Default is no-rollback	N/A	N/A	No
Rule Group Name	Rule Group Name	String	No	Yes
Rule Group Action	Action to be taken (aws:PASS,aws:DROP)	String	No	Yes
Source Address Definition	IP address,range of IP address	String	No	Yes
Destination Address Definition	IP address,range of IP address	String	No	Yes
Header Destination Port	Destination Port	String	No	Yes
Priority	Priority for execution	Integer	No	Yes
Capacity	Capacity	Integer	No	Yes

### Output:

Case Scope

N/A

Human Readable Output

N/A

## 3. Add Stateful Rule

Action capability for adding a Stateful rule to an existing Rule Group for blocking IP address.

- Rollback: Yes
- Duplicate Control: Yes

The following table presents the **Add Stateful Rule** action capabilities details:

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
Integraion	Name of the third party integration	Integration	N/A	Yes
Rollback Mode	Time to rollback this action. Default is no-rollback	String	N/A	No
Rule Group Name	Rule Group Name	String	No	Yes
Rule Group Action Name	Action to be taken (PASS,DROP,ALERT)	String	No	Yes
Header Protocol	Header Protocol(TCP, HTTP, ICMP and so on)	String	No	Yes
Header Source	IP Address	String	No	Yes
Header Source Port	Source Port	String	No	Yes
Header Destination	IP Address	String	No	Yes
Header Destination Port	Destination Port	String	No	Yes
Direction	Direction(FORWARD,ANY)	String	No	Yes
Rule Order	Rule Order to be executed	String	No	Yes

**Output:**

Case Scope

N/A

Human Readable Output

N/A

**4. Add Stateless Rule**

Action capability for adding a Stateless Rule to an existing Rule Group for blocking IP address.

- Rollback: Yes
- Duplicate Control: Yes

The following table presents the **Add Stateless Rule** action capabilities details:

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
Integration	Name of the third party integration	Integration	N/A	Yes
Rollback Mode	Time to rollback this action. Default is no-rollback	String	N/A	No
Rule Group Name	Rule Group Name	String	No	Yes
Action	Action to be taken (aws:PASS,aws:DROP)	String	No	Yes
Source Address Definition	IP Address, Range of IP Address	String	No	Yes
Destination Address Definition	IP Address, Range of IP Address	String	No	Yes
Priority	Priority for execution	String	No	Yes

**Output:**

Case Scope

N/A

Human Readable Output

N/A

**5. Delete Rule Group**

Action capability for deleting Rule Group from existing Rule Group.

- Rollback: No
- Duplicate Control: Yes

The following table presents the **Delete Rule Group** action capabilities details:

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
Integration	Name of the third party integration	Integration	N/A	Yes
Rollback Mode	Time to rollback this action. Default is no rollback.	N/A	N/A	No
Rule Group Name	Rule Group Name	String	No	Yes
Type	Type (STATEFUL or STATELESS)	String	No	Yes

**Output:**

Case Scope

N/A

Human Readable Output

N/A

**6. Delete Stateful Rule**

Action capability for deleting a Stateful Rule from an existing Rule Group .

- Rollback: No
- Duplicate Control: No

The following table presents the **Delete Stateful Group** action capabilities details:

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
Integration	Name of the third party integration	Integration	N/A	Yes
Rollback Mode	Time to rollback this action. Default is norollback.	N/A	N/A	No
Rule Group Name	Rule Group Name	String	No	Yes
Sid	Sid	Integer	No	Yes

**Output:**

Case Scope

N/A

Human Readable Output

N/A

**7. Delete Stateless Rule**

Action capability for deleting a Stateless Rule from an existing Rule Group.

- Rollback: No
- Duplicate Control: No

The following table presents the **Delete Stateless Group** action capabilities details:

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
Integration	Name of the third party integration	Integration	N/A	Yes
Rollback Mode	Time to rollback this action. Default is norollback.	N/A	N/A	No
Rule Group Name	Rule Group Name	String	No	Yes
Priority	Priority for execution	Integer	No	Yes

**Output:**

Case Scope

N/A

Human Readable Output

N/A

## 8. List Firewalls

Enrichment capability for retrieving a list of firewall for the specified VPC identifiers.

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
Integration	Name of the third party integration	Integration	N/A	Yes
Max result	Max result	Integration	N/A	Yes
VPC IDs	VPC identifiers	String	N/A	No

### Output:

Case Scope

N/A

Human Readable Output

## 9. List Rule Groups

Enrichment capability for retrieving a list of rule groups.

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
Integration	Name of the third party integration	Integration	N/A	Yes
Max result	Max result	Integration	N/A	Yes
Scope	Scope(ACCOUNT,MANAGED)	String	N/A	Yes

### Output:

Case Scope

N/A

Human Readable Output

N/A

## 10. List Firewall Policies

Enrichment capability for retrieving a list of firewall policies.

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
Integration	Name of the third party integration	Integration	N/A	Yes
Max result	Max result	Integration	N/A	Yes

**Output:**

Case Scope

N/A

Human Readable Output

N/A

**11. Get Firewall Policy**

Enrichment capability for retrieving the details of a firewall policy.

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
Integration	Name of the third party integration	Integration	N/A	Yes
Firewall Policy Name	Firewall Policy Name	String	N/A	Yes

**Output:**

Case Scope

N/A

Human Readable Output

N/A

**12. Get Firewall Rule Group**

Enrichment capability for retrieving the details of a firewall rule group.

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
Integration	Name of the third party integration	Integeration	N/A	Yes
Max Results	Max Results	Integer	N/A	Yes
Scope	Scope(ACCOUNT,MANAGED)	String	N/A	Yes

**Output:**

Case Scope

N/A

Human Readable Output

N/A

# Integration Guide for Azure Network Security Groups

## Integration Overview

Azure Network Security Groups is a service that is used to filter network traffic to and from Azure resources in an Azure virtual networks. A network security group contains security rules that allow or deny inbound network traffic to, or outbound network traffic from, several types of Azure resources. For each rule, you can specify source and destination, port, and protocol.

## Integration Capabilities

ArcSight SOAR has the following integration capabilities with Azure Network Security Groups:

- Get Network Security Group
- List All Network Security Group
- List Network Security Group in Resource Group
- Create Network Security Group
- Create Network Security Group Rule
- Add Network Security Group Tag
- Remove Network Security Group Tag

## Prerequisites

ArcSight SOAR connects to Microsoft Azure Network Security API using HTTPS. Access to Azure Portal (<https://login.live.com>) is required.

## Configuration

### Configuring Microsoft Azure Network Security

1. Log in to <https://portal.azure.com> and Navigate to **Azure Active Directory** service.
2. Click **App Registration > New Registration**. Complete the ArcSight SOAR application registration by specifying the following parameter values in the Register an application form:

Name	Supported Account types	Redirected URL
ArcSight SOAR	Accounts in this organizational directory only (Default Directory for single tenant only)	https://localhost/soar

3. Select your application and Click **Add a certificate or secret > New Client Secret**. Add a description and specify the expiry period as 24 months.

 Note down the **Secret Key** along with **Client ID** as you may need it later.

- a. Click **API Permissions > Add a Permission** and select **Azure Service Management API**.
- b. Add the **user\_impersonation** as a permission.
4. Navigate to **Home > Subscriptions** and note down the **subscription ID**.
5. Navigate to **Home > Resource groups > IAM > Add Role** to add role level permissions.
6. Grant following permissions to the users:

Permissions	Description
Microsoft.Network/networkSecurityGroups/read	Gets a network security group definitionAction
Microsoft.Network/networkSecurityGroups/write	Creates a network security group or updates an existing network security groupAction

Permissions	Description
Microsoft.Network/networkSecurityGroups/securityRules/read	Gets a security rule definition Action
Microsoft.Network/networkSecurityGroups/securityRules/write	Creates a security rule or updates an existing security rule Action

## Configuring SOAR

1. Click **Configuration > Credential > Create Credential**.
2. Specify the following parameter values in the **Credential Editor**:

Type	Name	Password	Private Key
Internal Credential	Display name of credential set (for example, Microsoft Azure Network Security).	Client ID of the user that you have created for SOAR on Microsoft Azure Network Security.	Client secret key of the users that you have created for SOAR on Microsoft Azure Network Security.

3. Click **Configuration > Integrations > Create Integration**
4. Specify the following parameter values in the **Configuration Form**:

Parameter	Value
Name	Display name of the integration
Type	Microsoft Azure Network Security
Address	Address of the integration (the format should be <a href="https://management.azure.com">https://management.azure.com</a> )

Parameter	Value	
Configuration	Specify the following configuration parameters:	
	tenant.id	Tenant Id on Microsoft Azure. For example: tenant.id = 57faef05-5f3f-4147-a5e1-5ecd93902c3a
	subscription	Subscription ID on Microsoft Azure. For example, subscription = 7ee609fd-4deb4156-826e-7d1796f6e3e7
	version	Microsoft Azure Network Security API version . For example: version= 2021-05-01
	proxy.id	ID of the proxy integration if you access Microsoft Azure through a web proxy device. Forexample: proxy.id = 12345
Credential	Credential that has been defined for this integration under <b>Credential</b> menu.	
Notify	Select user(s) from the list to notify when SOAR performs an action on this integration.	

5. Click **Save**.
6. Navigate to **Configuration > Customization Library** and edit **Amazon Network Firewall Advanced Action Script Default Script Template**.
7. Select the integration that you have created in step 4 from the **Integrations** drop-down menu and click **Save**.
8. Click **Test**, and **Integration Successful** message is displayed if the credential and address are valid.

## Capabilities

### 1. Get Network Security Group

Enrichment capability for retrieving a network security group in a resource group.

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
Integration	Name of the third party integration	Integration	N/A	Yes
Network Security Group Name	Name of the network security group	String	N/A	Yes
Resource Group Name	Resource group of the user that you have created in Microsoft Azure Network Security Group	String	N/A	Yes

**Output:**

Case Scope

N/A

Human Readable Output

N/A

## 2. List All Network Security Group

Enrichment capability for retrieving all network security groups from a resource group.

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
Integration	Name of the third party integration	Integration	N/A	Yes
Network Security Group Name	Name of the network security group	String	N/A	Yes
Resource Group Name	Resource group of the user in Microsoft Azure Network Security Group	String	N/A	Yes

### Output:

Case Scope

N/A

Human Readable Output

N/A

## 3. List Network Security Group in Resource Group

Enrichment capability for listing all network security group in a particular resource group.

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
Integration	Name of the third party integration	Integration	N/A	Yes
Network Security Group Name	Name of the network security group	String	N/A	Yes
Resource Group Name	Resource group of the user in Microsoft Azure Network Security Group	String	N/A	Yes

### Output:

Case Scope

N/A

Human Readable Output

#### 4. Create Network Security Group

Action capability for creating a network security group in a particular resource group.

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
inNetwork Security Group Name	Network Security Group Name	String	N/A	Yes
Resource groups Name	Resource group of the users in Microsoft Azure Network Security Group.	String	N/A	Yes
Location	Location of the user.	String	N/A	Yes

#### Output:

Case Scope

N/A

Human Readable Output

N/A

#### 5. Create Network Security Group Rule

Action capability for creating a network security group rule in resource group.

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
Network Security Group Name	Name of the network security group name	String	N/A	Yes
Resource Group Name	Resource group of the users in Microsoft Azure Network Security Group.	String	N/A	Yes
Name	Unique Rule Name	String	N/A	Yes
Protocol	TCP, UDP, ICMP, ESP, AH, or Any	String	N/A	Yes
Source Address Prefix	“*” for all default or 0.0.0.0/0 or AzureLoadBalancer	String	N/A	Yes
Destination Address Prefix	“*” for all default or 0.0.0.0/0 or AzureLoadBalancer	String	N/A	Yes
Source Port Range	0-65535	String	N/A	Yes
Destination Port Range	0-65535	String	N/A	Yes

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
Priority	A number in the range 100-4096 to assign a priority. Rules are processed in priority order, with lower numbers processed before higher numbers	String	N/A	Yes
Direction	Whether the rule applies to inbound, or outbound traffic	String	N/A	Yes
Access	Allow or deny.	String	N/A	Yes
Location	Location of the user	String	N/A	Yes

**Output:**

Case Scope

N/A

Human Readable Output

N/A

**6. Add Network Security Group Tags**

Action capability for updating a network security group tag in the specified resource group.

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
Network Security Group Name	Network Security Group Name	String	N/A	Yes
Resource group Name	Resource group of the user in Microsoft Azure Network Security Group.	String	N/A	Yes
Tag Name	Resource Tag Key	String	N/A	Yes
Tag Value	Resource Tag Value	String	N/A	Yes

**Output:**

Case Scope

N/A

Human Readable Output

N/A

**7. Remove Network Security Group Tags**

Action capability for Updating network security group tag in the specified resource group.

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
Network Security Group Name	Network Security Group Name	String	N/A	Yes
Resource group Name	Resource group of the user in Microsoft Azure Network Security Group.	String	N/A	Yes
Tag Name	Resource Tag Key	String	N/A	Yes
Tag Value	Resource Tag Value	String	N/A	Yes

**Output:**

Case Scope

N/A

Human Readable Output

N/A

# Integration Guide for Bind RPZ DNS

## Integration Overview

ArcSight SOAR uses BIND DNS servers to block malicious domains using incident scope.

## Integration Capabilities

### Action

- Block

## Configuration

### Prerequisites

- You must enable the DNS Zone Transfer on the server as SOAR uses DNS Zone Transfer Protocol to connect to the BIND DNS server.
- Remote Name Daemon Control (RNDC)

## Configuring SOAR

1. To create the integration, navigate to **Configuration > Integrations**.
2. Specify the following parameter values in the **Integration Editor window**:

Parameter	Value
Name	Display name of the integration
Type	BIND RPZ DNS
Address	Address of the integration (the format must be 1.1.1.1).
Configuration	You must specify the following configuration parameters: <ul style="list-style-type: none"><li>• <b>ZONE</b>: Name of the RPZ configured on the BIND server</li><li>• <b>BLOCK_IP</b>: IP address to which malicious domains need to be redirected</li><li>• <b>TTL</b>: Time-to-live for the DNS record</li><li>• <b>KEY_NAME</b>: Name of the RNDC key</li></ul>

Parameter	Value
Credential	Specify the Credential that was defined for this integration under the <b>Credentials</b> menu
Trust Invalid SSL Certificates	Select this if Engine's certificate is self-signed or is not recognized by browsers.
Require Approval From	Select users from list who can provide approval before executing action on this integration
Notify	Select user(s) from the list to notify when SOAR performs an action on this integration

Integration Editor

Name *	Bind RPZ DNS
Type *	Bind RPZ DNS
Address *	192.168.1.1
Configuration	<pre>#Zone name in fully qualified domain name (FQDN) format - default is . #ZONE= #The address of the host record - default is 1.2.3.4 #BLOCK_IP= #(Time To Live) expresses the duration (in seconds) of the information contained in the Resource Records - default is 86400 #TTL= #Security key name - default is rndc-key #KEY_NAME=</pre>
Credential *	Bind RPZ DNS <span style="float: right;">Create</span>
Trust Invalid SSL Certificates	<input checked="" type="checkbox"/>
Require Approval From	T Timothy Dalton
Notify	J Jennifer Lee
Tags	
<a href="#">Show additional parameters</a> <span style="float: right;"><b>Test</b> <b>Close</b> <b>Save</b></span>	

3. Click **Test**. The following pop up will be displayed if your credential and address are valid.
4. Click **Save** to complete integration.

# Integration Guide for BMC Discovery

## Integration Overview

BMC Discovery products automate the process of populating BMC Discovery CMDB. When these products discover IT hardware and software, they create Configuration Items and relationships from the discovered data.

## Integration Capabilities

ArcSight SOAR has the following integration capabilities with BMC Discovery:

- Get CI Details
- Get Installed Software

## Prerequisites

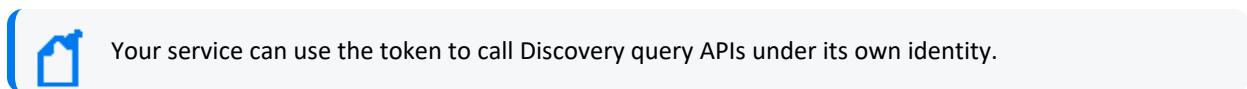
You must have access to HTTPS as ArcSight SOAR connects to BMC Discovery API through this service.

## Configuration

### Configuring BMC Discovery

Basic Authentication:

To configure a service and fetch a token from the BMC Discovery endpoint, follow these steps :



1. Log in to create an authorization key which will be used in all subsequent calls In the login page, specify the following details:

#### Authentication Parameters

Parameters	Description
Username	Username of the BMC Discovery
Password	Password of the BMC Discovery

Client creates a POST call and passes the username, password, and the Request headers using the /x-www-form-urlencoded content type.

Additional Configuration:

Configuration Parameter	Description
proxy.id	Proxy device to be used while communicating with the remote system's API
cache.reusing.duration	Default cache-reuse parameter

## Configuring SOAR

1. Click Configuration > Credentials > Create Credentials.
2. Specify the following parameters values in the Credential Editor form.

Type	Name	Username	Password	Private Key
Internal credential	Display name of credential set (for example, BMC Discovery Credentials).	Username of the BMC Discovery	Password of the BMC Discovery	N/A

3. Select your integration plugin zip file and click on Save.
4. Select the integration that you have added to the Integrations menu.
5. Click Save to complete the integration.
6. Click Test, If the credential and address are valid a success message is displayed.

## Integration Capabilities:

### 1. Get CI Details

Enrichment capability to retrieve the CI details from the BMC discovery search by hostname.

**Request headers:**

Header	Value	Required
Authorization	Bearer <token generated>	Yes

**Input Parameters:**

Parameter	Description	Type	Scope restricted (Yes/No)	Required (Yes/No)
Host Name	Host name to be provide	String	Yes	Yes

**Output:**

Case Scope: N/A

Human Readable Output:

4 minutes ago - S sacumen executed [Get CI Details](#) enrichment on BMC\_DISCOVERY\_QA

Parameters Details	
Key	Value
Host Name	agent-id-pcfdev-0
Type	UNIX Server
Hardware Vendor	innotek GmbH
Virtual	true
DNS Domain	N/A
Local FQDN	localhost
Business Owner	julie.mayer
Role	Manager Application Owner
Phone	+44 (0) 2079 460 882
Employee ID	N/A
Description	N/A
Business Continuity Critical	N/A
OS	Ubuntu 14.04.5 LTS

OS Class	UNIX
OS Type	Ubuntu Linux
OS Version	14.04
OS Architecture	x86_64
OS Build	Trusty Tahr
OS Vendor	Canonical
Kernel	4.2.0-42-generic
Model	VirtualBox
Host Running on Environment	[ "Node.js", "Java Virtual Machine", "Java Virtual Machine", "Java Virtual Machine" ]
Network Interface Names	[ "silk-vtep on agent-id-pcfdev-0, IPv4: 10.255.6.0, IPv6: fe80:a44b:37ff:fe5c:5a5, MAC Addr: ee:ee:0a:ff:06:00", "eth1 on agent-id-pcfdev-0, IPv4: 10.204.11.11, IPv6: fe80::a00:27ff:fe43:1c48, MAC Addr: 08:00:27:43:1c:48", "eth0 on agent-id-pcfdev-0, IPv4: 10.0.2.15, IPv6: fe80:a00:27ff:fe5a:a0cd, MAC Addr: 08:00:27:5a:a0:cd" ]
Software Instance Names	[ "Nginx Webserver on agent-id-pcfdev-0 Ports:None", "Cloud Foundry MySQL Broker 35 on agent-id-pcfdev-0 Ports:None", "Apache Tomcat Application Server 8.0 listening on 8085, 8443, 8989 on agent-id-pcfdev-0 Ports:[8085, 8443, 8989]", "etcd on agent-id-pcfdev-0 Ports:[2379, 2380]", "Cloud Foundry Diego Database 1.16 on agent-id-pcfdev-0 Ports:None", "Nginx Webserver 1.11 on agent-id-pcfdev-0 Ports:None", "Cloud Foundry Diego Cell on agent-id-pcfdev-0 Ports:None", "Cloud Foundry Cloud Controller 1.28 on agent-id-pcfdev-0 Ports:None" ]

Software Instance Names	[ "Nginx Webserver on agent-id-pcfdev-0 Ports:None", "Cloud Foundry MySQL Broker 35 on agent-id-pcfdev-0 Ports:None", "Apache Tomcat Application Server 8.0 listening on 8085, 8443, 8989 on agent-id-pcfdev-0 Ports:[8085, 8443, 8989]", "etcd on agent-id-pcfdev-0 Ports:[2379, 2380]", "Cloud Foundry Diego Database 1.16 on agent-id-pcfdev-0 Ports:None", "Nginx Webserver 1.11 on agent-id-pcfdev-0 Ports:None", "Cloud Foundry Diego Cell on agent-id-pcfdev-0 Ports:None", "Cloud Foundry Cloud Controller 1.28 on agent-id-pcfdev-0 Ports:None", "Cloud Foundry Redis Broker 429.3 on agent-id-pcfdev-0 Ports:None", "Redis Server listening on 35877 on agent-id-pcfdev-0 Ports:[35877]", "Nginx Webserver 1.11 on agent-id-pcfdev-0 Ports:None", "Cloud Foundry Diego Brain 1.16 on agent-id-pcfdev-0 Ports:None", "Cloud Foundry Diego Access 1.16 on agent-id-pcfdev-0 Ports:None", "Cloud Foundry CC-Bridge 1.28 on agent-id-pcfdev-0 Ports:None", "Cloud Foundry Networking 0.25 on agent-id-pcfdev-0 Ports:None", "HAProxy 1.5 on agent-id-pcfdev-0 Ports:None", "MariaDB Database Server 10.1 on agent-id-pcfdev-0 Ports:[3306]", "Cloud Foundry Diego Metron on agent-id-pcfdev-0 Ports:None", "Cloud Foundry Loggregator 87 on agent-id-pcfdev-0 Ports:None", "Cloud Foundry Messaging 16 on agent-id-pcfdev-0 Ports:None", "Cloud Foundry Garden 1.6 on agent-id-pcfdev-0 Ports:None", "HashiCorp Consul Agent on agent-id-pcfdev-0 Ports:[], "Cloud Foundry GORouter 0.154 on agent-id-pcfdev-0 Ports:None", "Nginx Webserver 1.8 on agent-id-pcfdev-0 Ports:None", "Cloud Foundry RabbitMQ Broker 226.7 on agent-id-pcfdev-0 Ports:None", "Pivotal RabbitMQ Server rabbit on agent-id-pcfdev-0 Ports:[], "Cloud Foundry Diego Emitter on agent-id-pcfdev-0 Ports:None" ]
Virtual Machine Names	N/A
Total 25 , items / page	1

## 2. Get Installed Software

Enrichment capability to retrieve the information for the installed application on the server.

### Request headers:

Header	Value	Required
Authorization	Bearer {token}	Yes

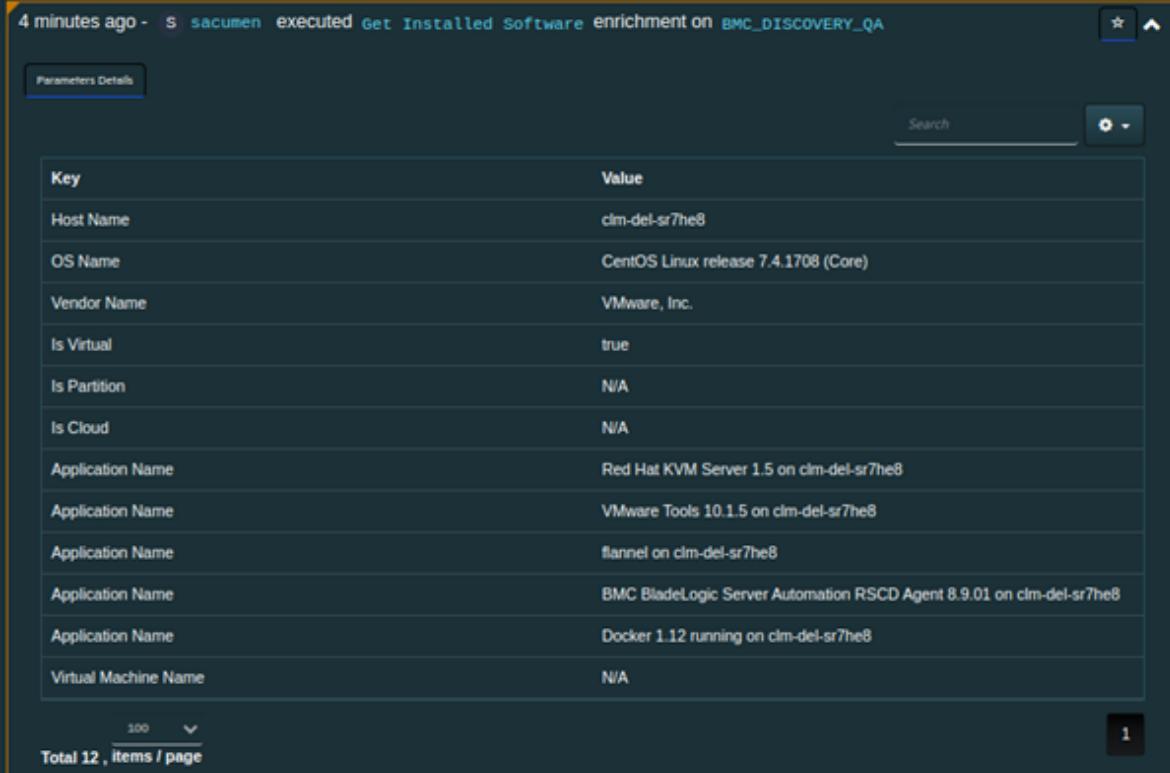
### Input Parameters:

Parameter	Description	Type	Scope restricted (Yes/No)	Required (Yes/No)
Host Name	Host name to be provide	String	Yes	Yes

### Output:

Case Scope: N/A

Human Readable Output:



Key	Value
Host Name	clm-del-sr7he8
OS Name	CentOS Linux release 7.4.1708 (Core)
Vendor Name	VMware, Inc.
Is Virtual	true
Is Partition	N/A
Is Cloud	N/A
Application Name	Red Hat KVM Server 1.5 on clm-del-sr7he8
Application Name	VMware Tools 10.1.5 on clm-del-sr7he8
Application Name	flannel on clm-del-sr7he8
Application Name	BMC BladeLogic Server Automation RSCD Agent 8.9.01 on clm-del-sr7he8
Application Name	Docker 1.12 running on clm-del-sr7he8
Virtual Machine Name	N/A

## Integration Guide for BMC Helix ITSM

### Integration Overview

BMC Helix ITSM is a comprehensive Cognitive Service Management cloud offering, that consists of robust cognitive capabilities such as intelligent chatbots and predictive capabilities.

### Integration Capabilities

ArcSight SOAR has the following integration capabilities with BMC Helix ITSM:

- Create Incident
- Update Incident
- Get an Incident
- Close Incident
- Add Work Note to Incident

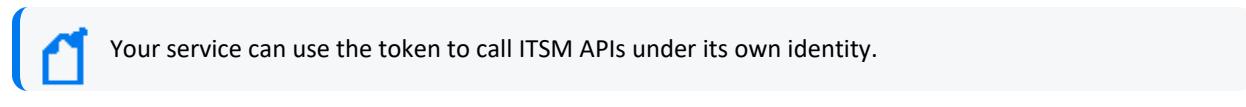
## Prerequisites

You must have HTTPS access as ArcSight SOAR connects to BMC Helix API through this service.

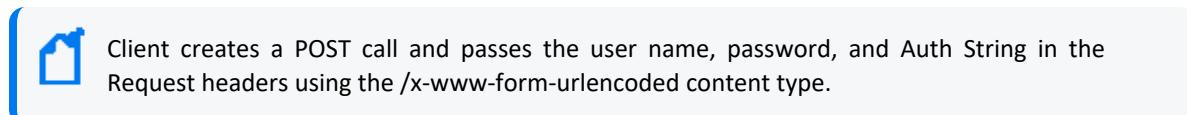
## Configuration

### Configuring BMC Helix ITSM

To configure a service and get a jwt token from the BMC Helix platform endpoint, complete the following steps:



1. Login to create an authorization key used in all subsequent calls.
2. In the login page, specify the following details:



Body Parameters for the JWT (JSON Web Tokens) Token generation:

Parameter	Description	Data Type	Required
Username	<username>	String	Yes
Password	<password>	String	Yes

#### Additional Configurations:

Configuration Parameters	Description
proxy.id	Proxy device to be used while communicating with the remote system's API
cache.reusing.duration	Default cache-reuse parameter
list.name	List name that is used for mapping ArcSight SOAR cases to MC Helix ITSM incidents. For example, list.name=bmcMapList

### Configuring SOAR

1. Click Configuration > Credentials > Create Credentials.
2. Specify the following parameters values in the Credential Editor form.

Type	Name	Username	Password	Private Key
Internal credential	Display name of credential set (for example, BMC Helix Credentials).	Your username from BMC Helic	Your password from BMC Helic	Empty

3. Click **Configuration > Integrations > Upload plugin**
4. Select your integration plugin zip file and click **Save**.
5. Select the integration that you have added to the Integrations menu.
6. Click **Save** to complete the integration.
7. Click **Test**. A successful message is displayed if the credential and address are valid.

## Integration Capabilities:

### 1. Create Incident

Action capability to create incident records with severity, priority, descriptions etc.

- Rollback: No
- Duplicate Control: No

#### Request headers:

Parameter	Value	Required
Authorization	AR-JWT <token generated>	Yes

#### Input Parameters:

Parameter	Description	Type	Scope restricted (Yes/No)	Required (Yes/No)
Urgency	The level of incident. The level, for example, can be critical, low or high.	Array	No	Yes
Impact	The type of issue.	Array	No	Yes
Service Type	The type of service incident. The type, for example, can be 'User Service Restoration'.	Array	No	Yes
Description	Description of the incident.	String	No	Yes

#### Output:

Case Scope: N/A

Human Readable Output: N/A

### 2. Update Incident

Action capability to update the incident.

- Rollback: No
- Duplicate Control: No

**Request headers:**

Parameter	Value	Required
Authorization	AR-JWT <token generated>	Yes

**Input Parameters:**

Parameter	Description	Type	Scope restricted (Yes/No)	Required (Yes/No)
<b>Request ID</b>	RequestID Of An IncidentOn HPD:IncidentInterface	String	No	Yes
<b>Status</b>	The status of the incident (Ex Status:"Resolved" <ul style="list-style-type: none"> <li>• Closed</li> <li>• In Progress</li> <li>• Assigned</li> <li>• Canceled</li> </ul> )	Array	No	Yes
<b>Urgency</b>	The level if incident. The level, for example, can be critical, low or high.	Array	No	Yes
<b>Impact</b>	The type of issue.	Array	No	Yes
<b>Status Reason</b>	The status of the reason.	Array	No	Yes
<b>Description</b>	Description of the incident.	String	No	No

**Output:**

Case Scope: N/A

Human Readable Output: N/A

**3. Get an Incident**

Enrichment capability to fetch the incident details for a given incident ID.

**Request headers:**

Parameter	Value	Required
Authorization	AR-JWT <token generated>	Yes

**Input Parameters:**

Parameter	Description	Type	Scope restricted (Yes/No)	Required (Yes/No)
Incident Number	Incident number Of An IncidentOn HPD:IncidentInterface	String	No	Yes

**Output:**

Case Scope: N/A

Human Readable Output:

Key	Value
Request ID	INC000000005318 INC000000005318
Incident Number	INC000000005587
Submitter	Sam_Agent
Submit Date	2023-03-03T11:32:12.000+0000
Assignee Login ID	Arthur Agent
Reported Date	2023-03-03T11:32:12.000+0000
Responded Date	2023-03-03T11:32:12.000+0000
Last Modified By	Sam_Agent
Last Modified Date	2023-03-03T12:24:32.000+0000
Last Resolved Date	2023-03-03T12:16:36.000+0000
Close Date	2023-03-03T12:16:36.000+0000
Status	Closed

Status	Closed
Status History	N/A
Assignee Groups	15032;'Sam_Agent';
Department	BMCOpsMonitoring Dept
Site Group	United States
Region	Americas
Entry ID	INC000000005318
Customer Login ID	Sam_Agent
Description	Changed Status
Company	BMCOpsMonitoring
Country	United States
State Province	Texas
City	Houston
Last Name	Agent
First Name	Sam
Contact Client Type	Office-Based Employee
VIP	No

VIP	No
Contact Sensitivity	Standard
Street	2103 CityWest Blvd.
Zip/Postal Code	77042-2828
Internet E-mail	N/A
Corporate ID	N/A
Phone Number	###
Service Type	Infrastructure Restoration
Status Reason	Automated Resolution Reported
Detailed Description	N/A
Resolution	Closed Incident
Urgency	4-Low
Impact	2-Significant/Large
Priority	Low
Reported Source	Systems Management

#### 4. Close Incident

Action capability to update existing incident.

- Rollback: No
- Duplicate Control: No

#### Request headers:

Parameter	Value	Required
Authorization	AR-JWT <token generated>	Yes

#### Input Parameters:

Parameter	Description	Type	Scope restricted (Yes/No)	Required (Yes/No)
Request ID	RequestID Of An IncidentOn HPD:IncidentInterface	String	No	Yes
Resolution Note	Detailed note of the updating incident	String	No	Yes

#### Output:

Case Scope: N/A

Human Readable Output: N/A

## 5. Add Work note to Incident

Action capability to create a work note to existing incident.

- Rollback: No
- Duplicate Control: No

### Request headers:

Parameter	Value	Required
Authorization	AR-JWT <token generated>	Yes

### Input Parameters:

Parameter	Description	Type	Scope restricted (Yes/No)	Required (Yes/No)
Incident Number	Incident number of work note	String	No	Yes
Work Note	Work note for the Incident	String	No	Yes

### Output:

Case Scope: N/A

Human Readable Output: N/A

# Integration Guide for BMC Helix Remedyforce

## Integration Overview

BMC Helix Remedyforce is a cloud service management solution on Salesforce for IT service operations. It improves service delivery with incident and asset management capabilities.

## Integration Capabilities

SOAR has the following integration capabilities with BMC Helix Remedyforce:

- Add Client Note to Incident
- Add Client Note to Service Request
- Close Incident
- Close Service Request
- Create Incident
- Create Service Request
- Update Incident
- Update Service Request

- Get Incident Details
- Get Service Request Details
- List Request Definition Questions
- List Request Definitions

## Configuration

### Configuring BMC Helix Remedyforce

- You must have access to HTTPS as the ArcSight SOAR connects to <https://na1.salesforce.com> API through this service.
- BMC Helix Remedyforce requires a **Username**, **Password**, and **Security Token** for access.
- Users must have API access enabled.

### Configuring SOAR

1. Click **Configuration > Credentials > Create Credential**.
2. Specify the following parameter values in the **Credential Editor**:

Parameter	Value
Type	Internal Credential
Name	Display name of credential set (For example, BMC Helix Remedyforce Credentials)
Username	<Username>
Password	<password>
Private Key	<security token>

3. Click **Configuration > Integrations > Create Integration**.
4. Specify the following parameter values in the **Configuration** form:

Parameter	Value
Name	Display name of BMC Helix Remedyforce Integration on SOAR
Type	Advanced Scriptable Device
Address	Address of the Integration (address should be in the format <a href="https://na1.salesforce.com">https://na1.salesforce.com</a> )

Parameter	Value
Configuration	<p>Specify the following configuration parameters:</p> <pre># Integration ID of the proxy integration to use when connecting to current integration.  # If not provided, ArcSight SOAR will try to use a direct connection.  #proxy.id=123  # Name of the list mapping SOAR Case IDs to Salesforce IDs of incidents and service requests  list.name=SOAR_to_Remedyforce_List</pre>
Credential	Name of the credential set created in step 2 (For example, BMC Helix Remedyforce Credentials)
Trust Invalid SSL Certificates	Select this if the certificate of the engine is self-signed or is not recognized by browsers
Require Approval From	Select users from the list who can provide approval before executing actions on this integration
Notify	Select users from the list to notify when SOAR performs an enrichment on this integration

5. Click **Test** to test whether the configuration and credentials used can successfully authenticate.
6. Click **Save** to complete the integration.
7. Click **Configuration > Lists > Create List.**

Parameter	Value
List Name	Name of list corresponding to list.name in configuration (ie. SOAR_to_Remedyforce_List)

8. Specify the following in the **List Editor** form:

Type	Column Name
Keyword	Key
Keyword	Salesforce ID

## Capabilities

1. **Add Client note to Incident**

Action capability for adding a client note to an incident.

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
Summary	Summary of the note	String	No	Yes
Notes	Note to add to the incident	String	No	Yes

**Output:**

Case Scope

N/A

Human Readable Output

N/A

**2. Add Client Note to Service Request**

Action capability for adding a client note to a service request.

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
Summary	Summary of the note	String	No	Yes
Notes	Note to add to the incident	String	No	Yes

**Output:**

Case Scope

N/A

Human Readable Output

N/A

**3. Close Incident**

Action capability to close an incident given its status.

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
Status	Status of the incident	Dropdown menu with the following options: CLOSED, CLOSED/NO CONTACT, COMPLETED, REJECTED	No	Yes

**Output:**

Case Scope

N/A

Human Readable Output

N/A

**4. Close Service Request**

Action capability to create a service request.

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
Status	Status of the incident	Dropdown menu with the following options: <ul style="list-style-type: none"> <li>• CLOSED</li> <li>• CLOSED/NO CONTACT</li> <li>• COMPLETED</li> <li>• REJECTED</li> </ul>	No	Yes

**Output:**

Case Scope

N/A

Human Readable Output

N/A

**5. Create Incident**

Action capability to create a new incident.

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
Client Username	Username of the client for which the incident is created	Email Address	No	Yes
Account	Name of the account for the incident	Dropdown menu with options: <ul style="list-style-type: none"> <li>• Account A</li> <li>• Account B</li> <li>• Account C</li> </ul>	No	No
Status	Status of the incident	Dropdown menu with options: <ul style="list-style-type: none"> <li>• IN PROGRESS</li> <li>• PENDING</li> <li>• ACCEPTED</li> <li>• ASSIGNED</li> <li>• OPENED</li> </ul>	No	No

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Category</b>	Category of the incident	Dropdown menu with the options: <ul style="list-style-type: none"><li>• HR-Separation - Disable Systems Access</li><li>• Email Distribution</li><li>• Human Resource Inquiries</li><li>• Building Access</li></ul>	No	No
<b>Impact</b>	Impact of the incident	Dropdown menu with the options: HIGH, MEDIUM, LOW	No	No
<b>Urgency</b>	Urgency of the incident	Dropdown menu with the options: <ul style="list-style-type: none"><li>• HIGH</li><li>• MEDIUM</li><li>• LOW</li></ul>	No	No
<b>Queue</b>	Name of the queue to assign the incident to	Dropdown menu with the options: <ul style="list-style-type: none"><li>• Change Management</li><li>• Client Services</li><li>• Application Development</li><li>• Desk Side Support</li></ul>	No	No
<b>Staff Username</b>	Username of the staff to assign the incident to.	Email Address	No	No
<b>Description</b>	Description of the incident	String	No	No
<b>Due Date Time</b>	Date time when the incident is due, can be static (format yyyy-mm-dd HH:MM:SS) or relative (ex: 1d, 2h, 3m)	String	No	No

**Output:**

Case Scope

N/A

Human Readable Output

N/A

**6. Create Service Request**

Action capability to create a service request.

<b>Input Parameter</b>	<b>Description</b>	<b>Type</b>	<b>Scope Restricted (Yes/ No)</b>	<b>Required (Yes/ No)</b>
<b>Request Definition ID</b>	Salesforce ID of the request definition.	String	No	Yes
<b>Request Definition Questions</b>	Questions and answers for the request definition in the format questionID1=value1;questionID2=value2	String	No	No
<b>Client Username</b>	Username of the client for which the service request is created	Email Address	No	Yes
<b>Account</b>	Name of the account for the service requested	Dropdown menu with options: <ul style="list-style-type: none"><li>• Account A</li><li>• Account B</li><li>• Account C</li></ul>	No	No
<b>Status</b>	Status of the service requested	Dropdown menu with options: <ul style="list-style-type: none"><li>• IN PROGRESS</li><li>• PENDING</li><li>• ACCEPTED</li><li>• ASSIGNED</li><li>• OPENED</li></ul>	No	No

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Category</b>	Category of the service requested	Dropdown menu with the options: <ul style="list-style-type: none"><li>• HR-Separation - Disable Systems Access</li><li>• Email Distribution</li><li>• Human Resource Inquiries</li><li>• Building Access</li></ul>	No	No
<b>Impact</b>	Impact of the service request	Dropdown menu with the options: <ul style="list-style-type: none"><li>• HIGH</li><li>• MEDIUM</li><li>• LOW</li></ul>	No	No
<b>Urgency</b>	Urgency of the service request	Dropdown menu with the options: <ul style="list-style-type: none"><li>• HIGH</li><li>• MEDIUM</li><li>• LOW</li></ul>	No	No
<b>Queue</b>	Name of the queue to which the service request is assigned	Dropdown menu with the options: <ul style="list-style-type: none"><li>• Change Management,</li><li>• Client Services,</li><li>• Application Development,</li><li>• Desk Side Support</li></ul>	No	No
<b>Staff Username</b>	Username of the staff to which the service request is assigned	Email Address	No	No
<b>Description</b>	Description of the service request	String	No	No
<b>Due Date Time</b>	Date time when the service request is due, can be static (format yyyy-mm-dd HH:MM:SS) or relative (ex: 1d, 2h, 3m)	String	No	No

**Output:**

Case Scope

N/A

Human Readable Output

N/A

## 7. Update Incident

Action capability to acquire the client username, account, status, category, impact, urgency, queue, staff username, description, and due date time and updates the incident. At least one of the following parameter must be updated:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Client Username</b>	(Optional) Username of the client for which the service request is created	Email Address	No	Yes
<b>Account</b>	Name of the account	Dropdown menu with options: <ul style="list-style-type: none"> <li>• Account A</li> <li>• Account B</li> <li>• Account C</li> </ul>	No	No
<b>Status</b>	Status of the incident	Dropdown menu with options: <ul style="list-style-type: none"> <li>• IN PROGRESS</li> <li>• PENDING</li> <li>• ACCEPTED</li> <li>• ASSIGNED</li> <li>• OPENED</li> </ul>	No	No
<b>Category</b>	Category of the incident	Dropdown menu with the options: <ul style="list-style-type: none"> <li>• HR-Separation - Disable Systems Access</li> <li>• Email Distribution</li> <li>• Human Resource Inquiries</li> <li>• Building Access</li> </ul>	No	No
<b>Impact</b>	Impact of the incident	Dropdown menu with the options: <ul style="list-style-type: none"> <li>• HIGH</li> <li>• MEDIUM</li> <li>• LOW</li> </ul>	No	No

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Urgency</b>	Urgency of the incident	Dropdown menu with the options: <ul style="list-style-type: none"> <li>• HIGH</li> <li>• MEDIUM</li> <li>• LOW</li> </ul>	No	No
<b>Queue</b>	Name of the queue to which the service request is assigned	Dropdown menu with the options: <ul style="list-style-type: none"> <li>• Change Management</li> <li>• Client Services</li> <li>• Application Development</li> <li>• Desk Side Support</li> </ul>	No	No
<b>Staff Username</b>	Username of the staff to which the incident is assigned	Email Address	No	No
<b>Description</b>	Description of the incident	String	No	No
<b>Due Date Time</b>	Date time when the service request is due, can be static (format yyyy-mm-dd HH:MM:SS) or relative (ex: 1d, 2h, 3m)	String	No	No

**Output:**

Case Scope

N/A

Human Readable Output

N/A

**8. Update Service Request**

Action capability that takes the client email address, status, category, impact, urgency, queue, staff username, description, and due date time and updates the service request. At least one of the following parameters must be updated:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Client Username</b>	(Optional) Username of the client to which the service request is created	Email Address	No	Yes
<b>Account</b>	Name of the account for the service requested	Dropdown menu with options: <ul style="list-style-type: none"><li>• Account A</li><li>• Account B</li><li>• Account C</li></ul>	No	No
<b>Status</b>	Status of the service request	Dropdown menu with options: <ul style="list-style-type: none"><li>• IN PROGRESS</li><li>• PENDING</li><li>• ACCEPTED</li><li>• ASSIGNED</li><li>• OPENED</li></ul>	No	No
<b>Category</b>	Category of the service request	Dropdown menu with the options: <ul style="list-style-type: none"><li>• HR-Separation - Disable Systems Access</li><li>• Email Distribution</li><li>• Human Resource Inquiries</li><li>• Building Access</li></ul>	No	No
<b>Impact</b>	Impact of the service request	Dropdown menu with the options: <ul style="list-style-type: none"><li>• HIGH</li><li>• MEDIUM</li><li>• LOW</li></ul>	No	No
<b>Urgency</b>	Urgency of the service request	Dropdown menu with the options: <ul style="list-style-type: none"><li>• HIGH</li><li>• MEDIUM</li><li>• LOW</li></ul>	No	No

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Queue</b>	Name of the queue to which the service request is assigned	Dropdown menu with the options: <ul style="list-style-type: none"> <li>• Change Management</li> <li>• Client Services</li> <li>• Application Development</li> <li>• Desk Side Support</li> </ul>	No	No
<b>Staff Username</b>	Username of the staff to which the incident is assigned	Email Address	No	No
<b>Description</b>	Description of the service request	String	No	No
<b>Due Date Time</b>	Date time when the service request is due, can be static (format yyyy-mm-dd HH:MM:SS) or relative (ex: 1d, 2h, 3m)	String	No	No

## 9. Get Incident Details

Enrichment capability to retrieve incident details given by the Salesforce ID. Salesforce ID will be retrieved from the list on the SOAR.

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Integration</b>	BMC Helix Remedyforce	Integration	N/A	Yes

### Output:

Case Scope

Action	Type	Category/Value
N/A	N/A	N/A

Human Readable Output:

Field	Value
Incident ID	00000021
Salesforce ID	[REDACTED]
Description	AutoCAD is not responding. Computer appears to be frozen.
Client Name	[REDACTED]
Client Email	[REDACTED]
Client Username	[REDACTED]
Account	Universal Systems LLC
Status	CLOSED
Category	Autocad
Priority	4
Impact	LOW
Urgency	MEDIUM
Staff Name	[REDACTED]
Staff Email	[REDACTED]
Staff Username	[REDACTED]
Open Date Time	2022-10-07 09:07:11
Due Date Time	2022-10-09 01:07:11

## 10. Get Service Request Details

Enrichment capability to retrieves service request details given the Salesforce ID. Salesforce ID will be retrieved from the list on the SOAR.

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
Integration	BMC Helix Remedyforce	Integration	N/A	Yes

Output:

Case Scope:

Action	Type	Category/value
N/A	N/A	N/A

Human Readable Output

Field	Value
Service Request ID	00000039
Salesforce ID	[REDACTED]
Request Definition	I need a server for a project
Request Details	# of CPU's needed: Allocate 1 CPU to new system, Memory required: Allocate 512 MB memory to new system, Operating System Requested: Install Windows 7 on new system, Other details: None
Description	220825 test service request
Client Name	[REDACTED]
Client Email	[REDACTED]
Client Username	[REDACTED]
Account	Account C
Status	ASSIGNED
Category	Building Access
Priority	S
Impact	LOW
Urgency	LOW
Queue	Desk Side Support
Staff Name	[REDACTED]
Staff Email	[REDACTED]
Staff Username	[REDACTED]
Open Date Time	2022-08-25 02:54:38
Due Date Time	2022-12-20 18:33:00

## 11. List Request Definition Questions

Enrichment capability to list the questions associated with a request definition.

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
Integration	BMC Helix Remedyforce	Integration	N/A	Yes
Request Definition ID	Salesforce ID of the request definition	String	No	Yes

### Output:

Case Scope:

Action	Type	Category/Value
N/A	N/A	N/A

Human Readable Output:

Question Id	Question Prompt	Required	Input Values
[REDACTED]	# of CPU's needed	true	Option: Allocate 1 CPU to new system, Value: 1, Default: true   Option: Allocate 2 CPUs to new system, Value: 2, Default: false   Option: Allocate 4 CPUs to new system, Value: 4, Default: false
[REDACTED]	Memory required	true	Option: Allocate 512 MB memory to new system, Value: 512, Default: true   Option: Allocate 1 GB memory to new system, Value: 1024, Default: false   Option: Allocate 2 GB memory to new system, Value: 2048, Default: false   Option: Allocate 4 GB memory to new system, Value: 4096, Default: false
[REDACTED]	Operating System Requested	true	Option: Install Windows 7 on new system, Value: WIN7, Default: true   Option: Install Linux Redhat on new system, Value: Linux, Default: false
[REDACTED]	Other details:	false	Enter text

## 12. List Request Definitions

Enrichment capability to list all available request definitions that can be used for service request creation.

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
Integration	BMC Helix Remedyforce	Integration	N/A	Yes

### Output:

Case Scope

Action	Type	Category/Value
N/A	N/A	N/A

### Human Readable Output:

Name	Id	Description
I need a server for a project	[REDACTED]	Request for a new project server
Request a Copy/License of AutoCAD 2015	[REDACTED]	Use this to request a copy of Autodesk AutoCAD 2015 to be installed on your computer. You will be charged for the cost of the license associated with the software install.
Cannot Access Imagine	[REDACTED]	N/A
Request Employee Separation (Off-boarding / Termination)	[REDACTED]	Starts the separation process as an employee leaves the organization.
Client Services: Request for Change	[REDACTED]	Need a report? Marketing materials? An enhancement request for one of our solutions?

# Integration Guide for Carbon Black Response (EDR)

## Integration Overview

Carbon Black Response (EDR) is a next-generation antivirus and end point detection response application. Its sophisticated detection combines custom and cloud-delivered threat intel, automated watchlists, and integrations with other platforms to efficiently scale hunt across the enterprise. It consolidates threat intelligence for your environment to automatically detect suspicious behavior.

## Integration Capabilities

- Block Hash
- Unblock Hash
- Quarantine
- Unquarantine
- Computer Info
- Download Binary
- Get Binary Metadata
- List Process Connections
- Process Event Details
- Search Binaries
- Search Processes

### Use Case: Investigating and Blocking Malware Spread

ArcSight SOAR integrates with Carbon Black Response (EDR), to help investigation and mitigation of malware attacks. When a suspicious file or malware is detected, SOAR lets you to search malware across endpoints, isolates PCs from network, and blocks relevant hashes. This investigation can either be performed automatically within a playbook or manually by an analyst.

# Configuration

## Prerequisites

- Access to port 443/tcp as SOAR connects to Carbon Black Response(EDR) API through HTTPS.
- An API key is required for SOAR to connect to Carbon Black Response(EDR).

## Configuring Carbon Black Response(EDR)

1. Log in to Carbon Black Server.
2. Navigate to **User Profile > API Token** and make a note of the API key.

## Configuring SOAR

1. Click **Configuration > Credentials > Create Credential**.
2. Specify the **Credential Editor** form with the following parameter values:
  - a. **Internal credential:**

Parameter	Value
Type	Internal credential
Name	Display name of the credential set (For example, Carbon Black Credential)
Username	Empty
Password	Empty
Private Key	API Key obtained from Carbon Black Response (EDR)

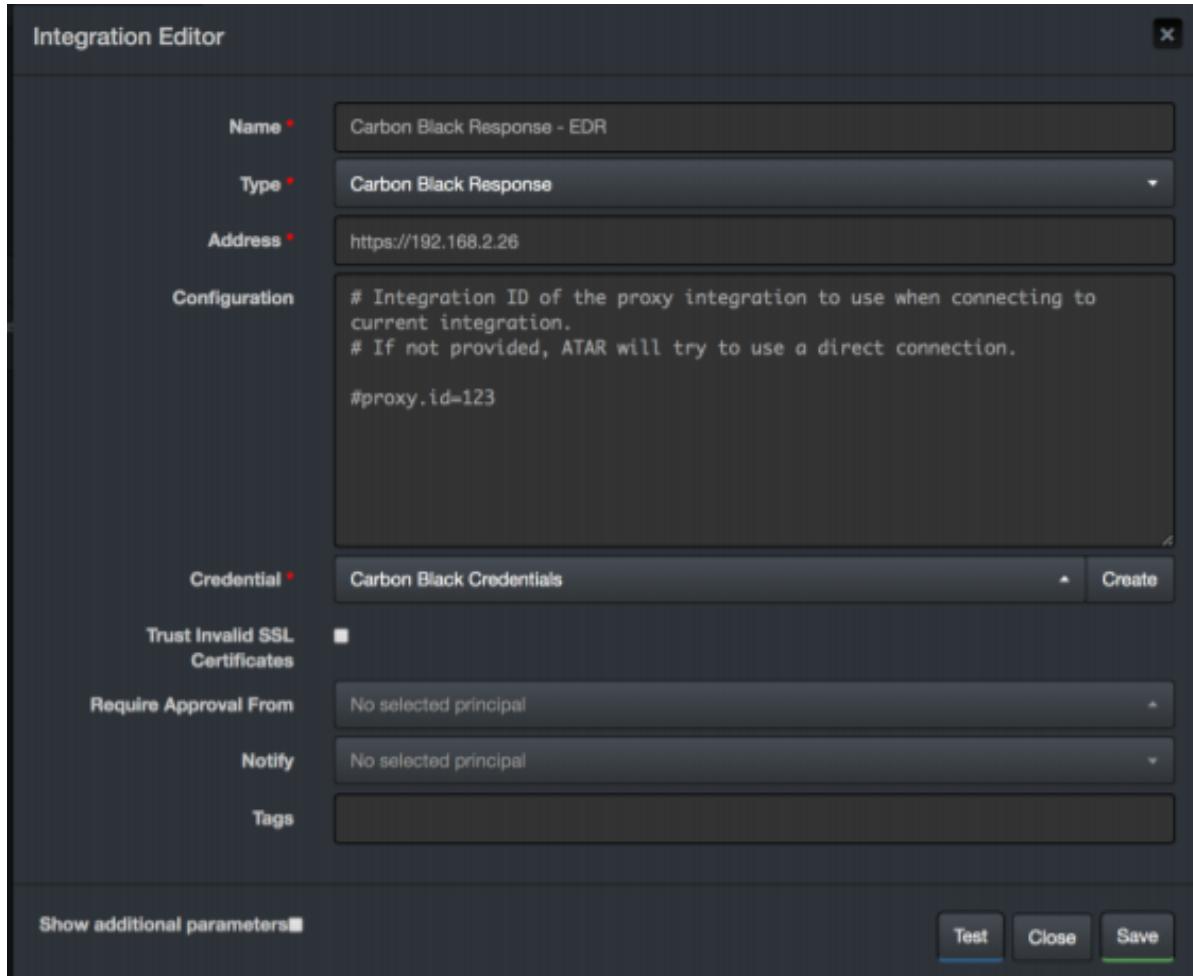
- b. **Credential Store:**

Parameter	Value
Type	External credential
Name	Name of the credential with full path of the safe on store.

3. Click **Configuration > Integrations > Create Migration**.

4. Specify the **Configuration form** with the following parameter values:

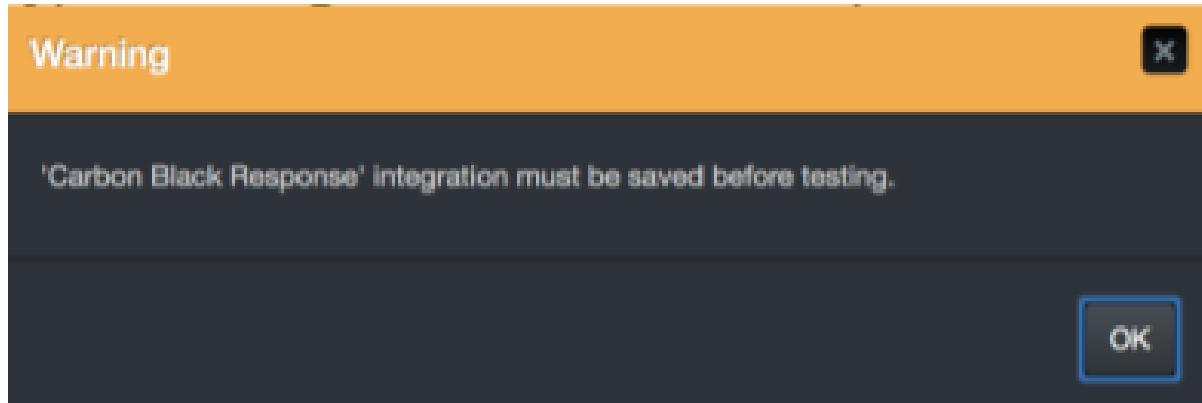
Parameter	Value
Name	Display name of Carbon Black Response (EDR) integration on SOAR
Type	Carbon Black Response
Address	Address of the integration (in the format: https://192.168.2.26)
Configuration	<p>Specify the following configuration parameters:</p> <pre># Integration ID of the proxy integration to use when connecting to # current integration. # If not provided, SOAR will try to use a direct connection. #proxy.id=123</pre>
Credential	Name of the credential set created on step 2. (For example, Carbon Black Credentials)
Trust Invalid SSL Certificates	Not Applicable
Require Approval From	Select users from list who can provide approval before executing actions on this integration.
Notify	Select users from the list to notify when SOAR performs an action on this integration



5. Navigate to **Configuration > Customization Library** and edit **Carbon Black Response Advanced Action Script Default Template**.
6. Select the integration that you have added to **Integrations** menu.
7. Click **Save** to complete the integration.
8. Click **Test**, an **Integration Successful** message is displayed if the credential and address are valid.

## Additional Notes

- Carbon Black Response integration on SOAR is an Advanced Script, and the content of default script is accessible under **Configuration > Customization Library**.
- While defining the integration for the first time, you will encounter the following warning message, which is expected behavior for this type of integration.



# Integration Guide for Cofense Triage

## Integration Overview

Cofense Triage is an automated malware analysis platform that enables security teams to quickly identify and respond to threats. It uses advanced machine learning algorithms and behavioral analysis to automatically detect and classify malware, phishing scams, and other malicious activities. It also enables security teams to prioritize and classify threats based on severity, allowing them to focus on the most critical security issues. With its user-friendly interface, Cofense Triage provides valuable insights into the nature and scope of a security breach, making it an indispensable tool for security teams looking to bolster their defenses against cyber threats.

## Integration Capabilities

ArcSight SOAR has the following integration capabilities with Cofense Triage:

1. Get URL Details
2. Get Domain Details
3. Get Report Details
4. List Report Attachments
5. Download Attachment Payload
6. Get Reporter Details
7. Update Report Category
8. List Threat Indicators
9. Get Threat Indicator Details

## Prerequisites

You must have access to HTTPS as ArcSight SOAR connects to the Cofense Triage API through this service.

All the APIs documentation links can only be accessible from the whitelisted IP address.

## Configuration

### Configuring Cofense Triage

1. Authentication: Cofense Triage API Version 2 uses Open Authentication (OAuth) to allow access to the API. All resource requests, unless otherwise stated, require authorization to access them. You supply this authorization by adding a bearer access token to an Authorization header in each request.
2. To get an access token, a superuser must first create an API application. Doing so will generate a Client ID and Secret for the API application. You must exchange these credentials for your access token.

#### Authentication Parameters:

Parameters	Description	Data Type	Required
client_id	Client ID of the API application	String	Yes
client_secret	Client secret of the API application	String	Yes
grant_type	Grant type of the API application. For Client Credentials, this must be client_credentials	String	Yes

#### Additional Configuration:

Configuration Parameter	Description
proxy.id	Proxy device to be used while communicating with the remote system's API.
Cache.reusing.duration	Default cache-reuse parameter

## Configuring SOAR

1. Click Configuration > Credentials > Create Credentials.
2. Specify the following parameters values in the Credential Editor form.

Type	Name	Username	Password	Private Key
Internal credential	Display name of credential set (for example, Cofense Triage Credentials).	Client id has to be enter in this field	Client secret has to be enter in this field	N/A

4. Select your integration plugin zip file and click on Save.
5. Select the integration that you have added to the Integrations menu.
6. Click Save to complete the integration.
7. Click Test, an Integration Successful message is displayed if the credential and address are valid.

## Integration Capabilities

### 1. Get URL Details

Enrichment capability to get URL details, relations and risk score.

Request headers:

Header	Value	Required
Authorization	Bearer {token}	Yes

Input Parameters:

Parameter	Description	Data Type	Scope Restricted	Required
ID	ID of the url	String	Yes	Yes

Output:

Case Scope:

Action	Type	Category/ Value
Set	Scope Item Property	Cofense Triage URL Risk Score

Human Readable Output:

Key	Value
URL	<a href="https://exchange.xforce.ibmcloud.com/#/collection/31a53084cb721d165721d2c92ec0c0d2">https://exchange.xforce.ibmcloud.com/#/collection/31a53084cb721d165721d2c92ec0c0d2</a>
Risk Score	N/A
Created At	2020-10-21T20:54:24.330Z
Updated At	2020-10-21T20:54:24.330Z
Relationship Reports	<a href="https://reltest6.phishmecloud.com/api/public/v2/urls/22/relationships/reports">https://reltest6.phishmecloud.com/api/public/v2/urls/22/relationships/reports</a>
Relationship Hostname	<a href="https://reltest6.phishmecloud.com/api/public/v2/urls/22/relationships/hostname">https://reltest6.phishmecloud.com/api/public/v2/urls/22/relationships/hostname</a>
Relationship Domain	<a href="https://reltest6.phishmecloud.com/api/public/v2/urls/22/relationships/domain">https://reltest6.phishmecloud.com/api/public/v2/urls/22/relationships/domain</a>
Relationship Clusters	<a href="https://reltest6.phishmecloud.com/api/public/v2/urls/22/relationships/clusters">https://reltest6.phishmecloud.com/api/public/v2/urls/22/relationships/clusters</a>
Relationship Integration Submissions	<a href="https://reltest6.phishmecloud.com/api/public/v2/urls/22/relationships/integration_submissions">https://reltest6.phishmecloud.com/api/public/v2/urls/22/relationships/integration_submissions</a>

Total 9 , items / page 1

## 2. Get Domain Details

Enrichment capability to get Domain details and relations.

Request headers

Header	Value	Required
Authorization	Bearer{token}	Yes

Input Parameters

Parameter	Description	Data Type	Scope Restricted	Required
Domain name	Name of the domain to enter	USERNAME, KEYWORD, UNKNOWN	Yes	Yes

Output:

Case Scope: N/A

Human Readable Output:

Parameters Details	
Key	Value
ID	5
Type	domains
Domain	mkt7665.com
Created At	2020-10-21T20:54:24.167Z
Updated At	2020-10-21T20:54:24.167Z
Relationship Reports	<a href="https://reltest6.phishmecloud.com/api/public/v2/domains/5/relationships/reports">https://reltest6.phishmecloud.com/api/public/v2/domains/5/relationships/reports</a>
Relationship Hostnames	<a href="https://reltest6.phishmecloud.com/api/public/v2/domains/5/relationships/hostnames">https://reltest6.phishmecloud.com/api/public/v2/domains/5/relationships/hostnames</a>
Relationship Urls	<a href="https://reltest6.phishmecloud.com/api/public/v2/domains/5/relationships/urls">https://reltest6.phishmecloud.com/api/public/v2/domains/5/relationships/urls</a>
Relationship Clusters	<a href="https://reltest6.phishmecloud.com/api/public/v2/domains/5/relationships/clusters">https://reltest6.phishmecloud.com/api/public/v2/domains/5/relationships/clusters</a>

Total 9 items / page      1

### 3. Get Report Details

Enrichment capability to get report details, relations.

Request headers

Header	Value	Required
Authorization	Bearer{token}	Yes

Input Parameters

Parameter	Description	Data Type	Scope Restricted	Required
Report ID	Id of the report	KEYWORD, UNKNOWN	Yes	Yes

Output:

Case Scope:

Action	Type	Category/ Value
Set	Scope Item Property	Cofense Triage Report Risk Score

Parameters Details	
Key	Value
Location	Processed
Risk Score	2
From Address	N/A
Subject	Palo Alto Networks Content Update
Received At	2019-11-12T01:33:28.000Z
Reported At	2019-11-12T01:31:59.000Z
MD5	ffe8cd33280d9f948988e325127cf089
Sha256	38d74aa6f0b54cf875a821ac749349121fe32a127032edbb2ccc0bd67d7629 4
Match Priority	0
URLs Count	4
Tags	[ "xcvbn", "asdflg", "12345" ]
Integrations	2

Human Readable Output:

#### 4. List Report Attachments

Enrichment capability to list the report attachments.

Request headers

Header	Value	Required
Authorization	Bearer{token}	Yes

Input Parameters

Parameter	Description	Data Type	Scope Restricted	Required
Report ID	Id of the report	KEYWORD, UNKNOWN	Yes	Yes

Default Parameters

Parameter	Description	Data Type	Required
Page[size]	This page will get the 200 latest data. but internally we set it page size as 200	String	No
Sort	The sort keyword used to get the latest data so internally we set it sort as latest.	String	No

Output:

Case Scope: N/A

Human Readable Output:

a few seconds ago - S sacumen executed List Report Attachments enrichment on COFENSE_TRIAGE					
Parameters Details					
Search <span style="float: right;">⚙️</span>					
<b>Id</b>	<b>File Name</b>	<b>Size</b>	<b>Is Child</b>	<b>Created At</b>	<b>Updated At</b>
8	image001.png	1391	false	2020-10-21T20:54:36.485Z	2020-10-21T20:54:36.485Z
9	image002.png	1424	false	2020-10-21T20:54:36.549Z	2020-10-21T20:54:36.549Z
10	image003.png	1695	false	2020-10-21T20:54:36.592Z	2020-10-21T20:54:36.592Z
11	image004.png	1551	false	2020-10-21T20:54:36.644Z	2020-10-21T20:54:36.644Z
12	image005.png	1603	false	2020-10-21T20:54:36.693Z	2020-10-21T20:54:36.693Z
13	image006.png	1988	false	2020-10-21T20:54:36.744Z	2020-10-21T20:54:36.744Z

Total 6 items / page 1

## 5. Download Attachment Payload

Enrichment capability to download attachment payload.

Request headers

Header	Value	Required
Authorization	Bearer{token}	Yes

Input Parameters

Parameter	Description	Data Type	Scope Restricted	Required
Attachment ID	attachment Id needs to be provide	String	No	Yes

Output:

Case Scope:

Action	Type	Category/Value
Automatically Set	Scope Item Property	Hash Algorithm
Automatically Set	Scope Item Property	Hash Algorithm
Automatically Set	Scope Item Property	
Automatically Set	Scope Item Property	

**Human Readable Output:****6. Get Reporter Details**

Enrichment capabilities to get details of a reporter user

Request headers

Header	Value	Required
Authorization	Bearer{token}	Yes

Input Parameters

Parameter	Description	Data Type	Scope Restricted	Required
Email ID	Email id of the reporter	EMAIL_ADDRESSUNKNOWN, USERNAME, KEYWORD,	Yes	Yes

Output:

Case Scope:

Action	Type	Category/Value
Set	Scope Item Property	Cofense Triage Reporter Reputation Score
Set	Scope Item Property	Cofense Triage Reporter VIP

Human Readable Output:

Key	Value
ID	4
Email	no-reply@xforce.ibmcloud.com
Reports Count	10
VIP	false
Reputation Score	11
Last Reported At	2020-12-11T05:46:39.000Z
Created At	2020-10-21T20:54:23.383Z
Updated At	2021-05-30T11:51:00.170Z
Relationship Reports	<a href="https://reitest6.phishmecloud.com/api/public/v2/reporters/4/relationships/reports">https://reitest6.phishmecloud.com/api/public/v2/reporters/4/relationships/reports</a>
Relationship Clusters	<a href="https://reitest6.phishmecloud.com/api/public/v2/reporters/4/relationships/clusters">https://reitest6.phishmecloud.com/api/public/v2/reporters/4/relationships/clusters</a>

Total 10 , items / page      1

## 7. Update Report Category

Action capability to update the category of a report.

Rollback: No

Duplicate Control: No

Request headers

Header	Value	Required
Authorization	Bearer{token}	Yes

Input Parameters

Parameter	Description	Data Type	Scope Restricted	Required
Tags	Email id of the reporter	EMAIL_ADDRESSUNKNOWN, USERNAME, KEYWORD,	Yes	Yes
Report ID	ID of the resource	UNKNOWN, KEYWORD	Yes	Yes

Output:

Case Scope: N/A

Human Readable Output: N/A

## 8. List Threat Indicators

Enrichment capability to list all threat indicators.

## Request headers

Header	Value	Required
Authorization	Bearer{token}	Yes

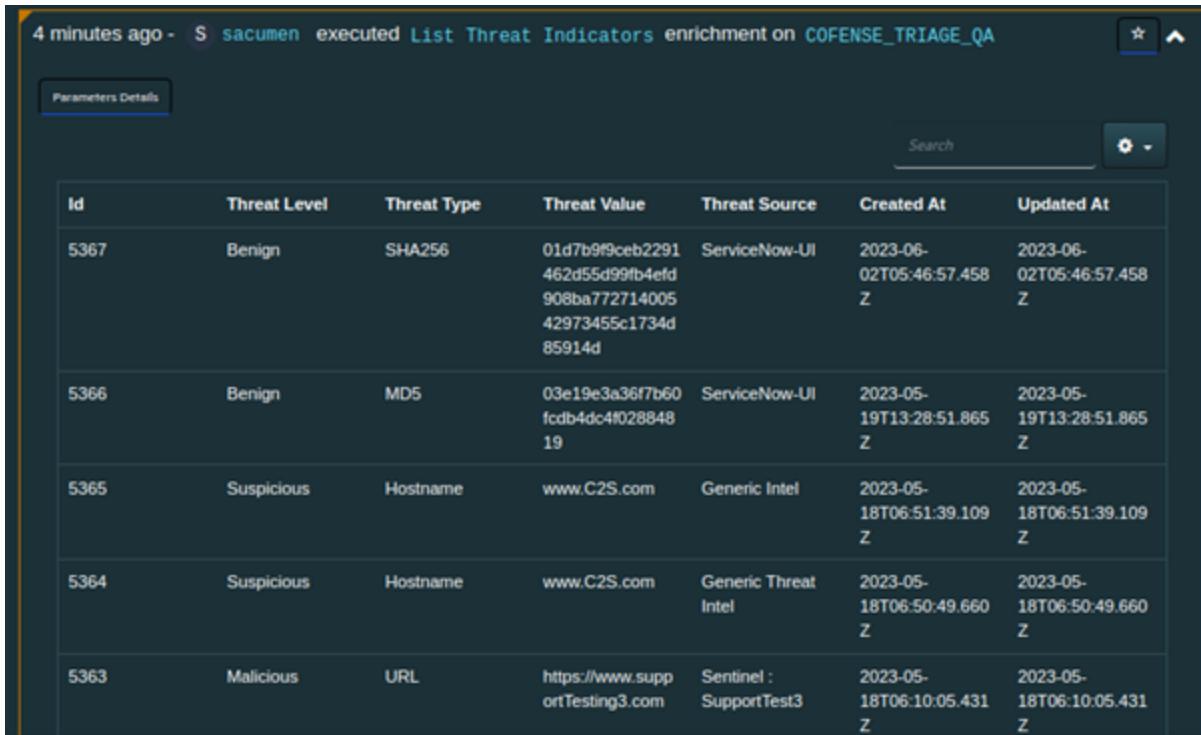
Default Parameters:

Parameter	Description	Data Type	Required
Page[size]	This page will get the 200 latest data. but internally we set it page size as 200	String	No
Sort	The sort keyword used to get the latest data so internally we set it sort as latest.	String	No

Output:

Case Scope: N/A

Human Readable Output:



A screenshot of a log entry from a security platform. The log message is: "4 minutes ago - S sacumen executed List Threat Indicators enrichment on COFENSE\_TRIAGE\_QA". Below the log message is a table titled "Parameters Details" showing threat indicator data. The table has columns: Id, Threat Level, Threat Type, Threat Value, Threat Source, Created At, and Updated At. There are five rows of data:

Parameters Details						
Id	Threat Level	Threat Type	Threat Value	Threat Source	Created At	Updated At
5367	Benign	SHA256	01d7b9f9ceb2291 462d55d99fb4efd 908ba772714005 42973455c1734d 85914d	ServiceNow-UI	2023-06-02T05:46:57.458Z	2023-06-02T05:46:57.458Z
5366	Benign	MD5	03e19e3a36f7b60 fcd84dc4f028848 19	ServiceNow-UI	2023-05-19T13:28:51.865Z	2023-05-19T13:28:51.865Z
5365	Suspicious	Hostname	www.C2S.com	Generic Intel	2023-05-18T06:51:39.109Z	2023-05-18T06:51:39.109Z
5364	Suspicious	Hostname	www.C2S.com	Generic Threat Intel	2023-05-18T06:50:49.660Z	2023-05-18T06:50:49.660Z
5363	Malicious	URL	https://www.sup ortTesting3.com	Sentinel : SupportTest3	2023-05-18T06:10:05.431Z	2023-05-18T06:10:05.431Z

## 9. Get Threat Indicator Details

Enrichment capability to get details of a given threat indicator (email, url, domain, hash).

Request headers

Header	Value	Required
Authorization	Bearer{token}	Yes

Input Parameters:

Parameter	Description	Data Type	Scope Restricted	Required
Threat Indicator	Threat value name to be proved it can (URL name,Hostname,email,hash)	KEYWORD, USERNAME, UNKNOWN, HOST	Yes	Yes

Output:

Case Scope:

Action	Type	Category/Value
Set	Scope Item Property	Cofense Triage Threat Level
Set	Scope Item Property	Cofense Triage Threat Type

Human Readable Output:

Key	Value
ID	46
Threat Level	Malicious
Threat Type	Hostname
Threat Value	www.btc.co.uk
Threat Source	Triage-UI
Created At	2020-11-17T14:03:00.066Z
Updated At	2020-11-17T14:03:00.071Z
Relationship Owner	<a href="https://retest6.phishmecloud.com/api/public/v2/threat_indicators/46/relationships/owner">https://retest6.phishmecloud.com/api/public/v2/threat_indicators/46/relationships/owner</a>
Relationship Reports	<a href="https://retest6.phishmecloud.com/api/public/v2/threat_indicators/46/relationships/reports">https://retest6.phishmecloud.com/api/public/v2/threat_indicators/46/relationships/reports</a>
Relationship Comments	<a href="https://retest6.phishmecloud.com/api/public/v2/threat_indicators/46/relationships/comments">https://retest6.phishmecloud.com/api/public/v2/threat_indicators/46/relationships/comments</a>

# Integration Guide for Check Point R80

## Integration Overview

**Check Point R80** is an integrated solution for advanced threat prevention and security management.

This integration was tested with Check Point R80.20.

## Integration Capabilities

- Block Email Sender
- Block Hash
- Block Host
- Block IP
- Block URL

## Prerequisites

You must have access to HTTPS as the ArcSight SOAR connects to Check Point Smart Console API through this service.

## Configuration

### Configuring Check Point R80

1. Login to **Management Console** and navigate to **Manage & Settings > Blades > Management API Advanced Settings** and select **All IP addresses that can be used for GUI clients** in the Access Settings section.
2. Restart the API service by executing the following command in the command prompt:  
`api restart`
3. SOAR requires standard read/write access for the necessary policy and objects. To install policy automatically, the user must have the rights in its permission profile. You must

configure the required access rights for SOAR user as follows:

Type	Permission
Access Control	<ul style="list-style-type: none"> <li>• Policy</li> <li>• Data Loss Prevention</li> <li>• Access Control Objects and Settings</li> <li>• Install Policy</li> </ul>
Threat Prevention	<ul style="list-style-type: none"> <li>• Policy Layers</li> <li>• Policy Exceptions</li> <li>• Profiles</li> <li>• Protections</li> <li>• Install Policy</li> </ul>
Management	Management API Login
Others	Common Objects

4. Create an **Object Group** to be used by SOAR. The ArcSight SOAR adds the objects that you want to block in the Object Group.

## Configuring SOAR

1. Click **Configuration > Credential > Create Credential**.
2. Specify the following values in the **Credential Editor**:

Parameter	Value
Type	Internal Credential
Name	Display name of credential set, for example, Check Point R80 Credentials.
Username	User that you have created for SOAR on Check Point R80
Password	Password of the user you have created for SOAR on Check Point R80
Private Key	Empty

3. Click **Configuration > Integrations > Create Integration**.
4. Specify the following values in the **Configuration Form**:

Parameter	Value
Name	Display name of the integration.
Type	Check Point R80 Next Generation Firewall.
Address	Address of the integration (the format must be 10.0.0.1 or abc.example.com)

Parameter	Value	
Configuration	Specify the following configuration parameters:	
	group.name	Object Group's name created in Check Point configuration steps. For example: <code>group.name = SOAR</code>
	products	Possible values are AV (Anti Virus) for external threats and AB (Anti Bot) for internal threats. Please put " " separator for more than one product. For example: <code>Product = AV AB</code>
	install.policy	If you would like to install policy automatically, set this variable true: <code>install.policy = true</code>
	policy.package	Policy which SOAR installs on target systems. Required if install.policy is true. For example: <code>policy.package = standard</code>
	targets	Name of the target gateways. Required if install.policy is true. Please use " " as separator if you have more than one target. For example: <code>targets = CP_Cluster</code>
	access	Required for blocking IP addresses on access policy. Required if install.policy is true. <code>access = true</code>
	threat.prevention	Required for blocking indicators on Threat Prevention policy (Domain, Email, Hash, URL). Required if install.policy is true. <code>threat.prevention = true</code>
	proxy.id	ID of the Proxy integration if you access Check Point R80 through a web proxy device. For example: <code>proxy.id = 12345</code>
Credentials	Credential that has been defined for this integration under the Credentials menu.	
Trust Invalid SSL Certificates	Select this if Engine's certificate is self-signed or is not recognized by browsers.	
Require Approval From	Select user(s) from list to ask her/his approval before executing actions on this integration	
Notify	Select user(s) from the list to notify when SOAR performs an action on this integration	

5. Click **Show Additional Parameters** checkbox and select the frequency of policy install in **Maintenance** dropdown.



As the firewall might get overloaded, in case of frequent attacks or misconfiguration, thus, SOAR does not install the policy after every action. Instead, you can define the frequency of the policy install in **Maintenance** menu by either selecting pre-defined values or by defining a custom Cron expression for scheduling. The ArcSight SOAR uses spring-framework's Cron expression format. For the format and similar example, refer to the [Spring Framework-Cron Expression](#)

6. Click **Test**. An **Integration Successful** message is displayed if your credential and address are valid.
7. Click **Save** to complete the integration.

## Capabilities

### 1. Block Email Sender

Action capability for blocking malicious email addresses.

- Rollback: Yes
- Duplicate Control: Yes



Only supported on AV product. AB product doesn't support this capability.

Input Parameter	Description	Type	Scope Restricted	Required
Integration	Name of the third party integration	Integration	N/A	Yes
Rollback	Time to rollback this action. Default is no-rollback.	N/A	N/A	No
Email Address	Email address to be blocked	Email Address	Yes	Yes

Output:

Case Scope: N/A

Human Readable Output: N/A

### 2. Block Hash

Action capability for blocking hash values of malicious files.

- Rollback: Yes
- Duplicate Control: Yes



Only supported on AV product. AB product doesn't support this capability.

Input Parameter	Description	Type	Scope Restricted	Required Yes/No
<b>Integration</b>	Name of the third party integration	Integration	N/A	Yes
<b>Rollback</b>	Time to rollback this action. Default is no-rollback.	N/A	N/A	No
<b>Hash</b>	Hash to be blocked	Hash	Yes	Yes

**Output:**

Case Scope: N/A

Human Readable Output: N/A

### 3. Block Host

Action capability for blocking malicious hosts.

- Rollback: Yes
- Duplicate Control: Yes



Only supported on AV product. AB product doesn't support this capability.

Input Parameter	Description	Type	Scope Restricted	Required Yes/No
<b>Integration</b>	Name of the third party integration	Integration	N/A	Yes
<b>Rollback</b>	Time to rollback this action. Default is no-rollback.	N/A	N/A	No
<b>Host</b>	Host to be blocked	Host  (It is mentioned as domain object on Check Point)	Yes	Yes

**Output:**

Case Scope: N/A

Human Readable Output: N/A

### 4. Block IP

Action capability for blocking malicious IP addresses.

- Rollback: Yes
- Duplicate Control: Yes



Only supported on AV product. AB product doesn't support this capability.

Input Parameter	Description	Type	Scope Restricted	Required
Integration	Name of the third party integration	Integration	N/A	Yes
Rollback	Time to rollback this action. Default is no-rollback.	N/A	N/A	No
IP Address	IP address to be blocked	Network Address	Yes	Yes

Output:

Case Scope: N/A

Human Readable Output: N/A

## 5. Block URL

Action capability for blocking URLs.

- Rollback: Yes
- Duplicate Control: Yes



Only supported on AV product. AB product doesn't support this capability.

Input Parameter	Description	Type	Scope Restricted	Required
Integration	Name of the third party integration	Integration	N/A	Yes
Rollback	Time to rollback this action. Default is no-rollback.	N/A	N/A	No
URL	URL to be blocked	URL	Yes	Yes

Output:

Case Scope: N/A

Human Readable Output: N/A

# Integration Guide for Check Point SandBlast

## Integration Overview

**Check Point SandBlast** provides advanced threat protection against known threats, zero-day malware, and sophisticated attacks.

## Integration Capabilities

Threat Emulation capability prevents infections from undiscovered exploits, zero-day and targeted attacks by inspecting files, and running them in a virtual sandbox to discover malicious behavior.

ArcSight SOAR has the following integration capabilities with Check Point SandBlast:

- Threat Emulation & AV Scan

### Use Case: Investigating suspicious file

With Check Point SandBlast integration, during the investigation of an incident, SOAR can send a suspicious file to Check Point SandBlast to emulate threats and run an anti virus scan for the file. This investigation can either be performed automatically within a playbook or manually by an analyst.

## Configuration

### Prerequisites

- Make sure you have access to 443/tcp port as SOAR connects to Check Point SandBlast's API through HTTPS. If cloud-based threat emulation service is used, the API interface works on <https://te.checkpoint.com/api/bla/bla>
- If a local gateway is used, typically access permission to 18194/tcp port is required.
- An API key is required for SOAR to connect to Check Point SandBlast.

### Configuring Check Point SandBlast

1. If you are using cloud-based threat emulation service, contact Check Point to get the API key.

2. If you are using local gateway, the following link provides you with the document for creating API key:

<http://supportcontent.checkpoint.com/solutions?id=sk113599>

## Configuring SOAR

1. **Configuration > Integrations > Create Integration.**
2. Fill the **Credential Editor** form with the following parameter values:

a. **Internal Credential:**

Parameter	Value
Type	Internal Credential
Name	Display name of credential set (For example, Check Point SandBlast Credential)
Username	Empty
Password	Empty
Private Key	API key you have created for SOAR on local gateway or you have obtained from Check Point.

b. **Credential Store:**

Parameter	Value
Type	External credential
Name	Name of the credential with full path of the safe on store

3. **Configuration > Integrations > Create Integration.**
4. Fill the configuration form with the following parameter values:

Parameter	Value
Name	Display name of Check Point SandBlast integration on SOAR
Address	Address of the integration (the format must be <a href="https://192.168.1.1:18194">https://192.168.1.1:18194</a> or <a href="https://te.checkpoint.com">https://te.checkpoint.com</a> )
Credential	Name of the credential set you <b>have</b> just created on step 2. (For example, Check Point SandBlast Credential).
Trust Invalid SSL Certificates	Select this if Engine's certificate is self-signed or is not recognized by browsers.

Parameter	Value
Configuration	<p>Specify the following configuration parameters:</p> <pre># Set local_instance true if you use local gateway. local_instance=false# configure how far (in minutes) into the past this enrichment will look. cache.reusing.duration=60 # Set proxy id if necessary for SOAR to reach the SandBlast instance. proxy.id=123</pre>
Require Approval Form	Select user(s) from list to ask her/his approval before executing actions on this s.
Notify	Select user(s) from the list to notify when SOAR performs an action on this integration.

Integration Editor

Name *	Check Point SandBlast
Type *	Check Point SandBlast
Address *	https://te.checkpoint.com
Configuration	<pre>local_instance=false  # configure how far (in minutes) into the past this enrichment will look. #cache.reusing.duration=60  #proxy.id=123</pre>
Credential *	Check Point SandBlast <span style="float: right;">Create</span>
Trust Invalid SSL Certificates	<input checked="" type="checkbox"/>
Require Approval From	T Timothy Dalton
Notify	T Tim Lee
Tags	
<a href="#">Show additional parameters</a> <span style="float: right;"><b>Test</b> <b>Close</b> <b>Save</b></span>	

5. Click **Test**. The following pop up will be displayed if your credential and address are valid.
6. Click **Save** to complete integration.

# Integration Guide for CiscoASA Firewall

Cisco ASA is a security technology that combines firewall, antivirus , intrusion prevention and virtual private network (VPN) capabilities. It provides proactive threat defence and stops attacks before they spread in the network.

## Integration Capabilities

- Block Host
- Block IP

## Prerequisites

- You must have access to 443/tcp port for HTTPS as the ArcSight SOAR connects to Cisco ASA Firewall REST-API interface through this service.
- SOAR must have a user account to connect to Cisco ASA Firewall.

## Configuration

### Configuring Cisco ASA Firewall

1. Log in to **Cisco ASA Firewall** device command line console.
2. Create a user account with privilege level 15 as follows:

```
# configure terminal  
# username soar password choose_a_complex_password privilege 15
```

3. Enable the **REST API** services by running the following commands:

```
# rest-api image  
# rest-api agent
```

# Configuring SOAR

1. Click **Configuration > Credential > Create Credential**.
2. Specify the following parameter values in the **Credential Editor** form.

Type	Name	Username	Password	Private Key
Internal credential	Display name of credential set (for example, Cisco ASA Firewall Credential).	User you have created for SOAR on Cisco ASA Firewall.	Password of the user you have created for SOAR on Cisco ASA Firewall.	Empty.

3. Click **Configuration > Integrations > Create Integration**.
4. Specify the following parameter values in the **Configuration** form.

Parameter	Value						
Name	Display name of the integration.						
Type	Cisco ASA Firewall						
Address	Address of the integration (the format should be https://10.0.0.1)						
Configuration	<p>Specify the following configuration parameters:</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="padding: 5px;">NETWORK_OBJECT_GROUP_NAME_FOR_IP</td> <td style="padding: 5px;">IP Object Group name used by SOAR. For example: NETWORK_OBJECT_GROUP_NAME_FOR_IP=SOAR_IP_LIST .</td> </tr> <tr> <td style="padding: 5px;">NETWORK_OBJECT_GROUP_NAME_FOR_DOMAIN</td> <td style="padding: 5px;">FQDN Object Group name used by SOAR. For example: NETWORK_OBJECT_GROUP_NAME_FOR_DOMAIN=SOAR_DOMAIN_LIST.</td> </tr> <tr> <td style="padding: 5px;">proxy.id</td> <td style="padding: 5px;">ID of the Proxy integration if you access Cisco ASA Firewall through a web proxy device. For example: proxy.id = 12345</td> </tr> </table>	NETWORK_OBJECT_GROUP_NAME_FOR_IP	IP Object Group name used by SOAR. For example: NETWORK_OBJECT_GROUP_NAME_FOR_IP=SOAR_IP_LIST .	NETWORK_OBJECT_GROUP_NAME_FOR_DOMAIN	FQDN Object Group name used by SOAR. For example: NETWORK_OBJECT_GROUP_NAME_FOR_DOMAIN=SOAR_DOMAIN_LIST.	proxy.id	ID of the Proxy integration if you access Cisco ASA Firewall through a web proxy device. For example: proxy.id = 12345
NETWORK_OBJECT_GROUP_NAME_FOR_IP	IP Object Group name used by SOAR. For example: NETWORK_OBJECT_GROUP_NAME_FOR_IP=SOAR_IP_LIST .						
NETWORK_OBJECT_GROUP_NAME_FOR_DOMAIN	FQDN Object Group name used by SOAR. For example: NETWORK_OBJECT_GROUP_NAME_FOR_DOMAIN=SOAR_DOMAIN_LIST.						
proxy.id	ID of the Proxy integration if you access Cisco ASA Firewall through a web proxy device. For example: proxy.id = 12345						
Credential	Credential that has been defined for this integration in the <b>Credentials</b> menu.						
Trust Invalid SSL Certificates	Select this if firewall's web certificate is self-signed or is not recognized by browsers.						
Require Approval From	Select user(s) from list to ask the approval before executing actions on this integration.						
Notify	Select user(s) from the list to notify when SOAR performs an action on this integration.						

5. Click **Save** to save the integration definition.
6. Navigate to **Configuration>Customization Library** and edit **Cisco ASA Firewall Advanced Action Script Default Template**.

7. Select the integration that you have added in the **Integrations** menu.
8. Click **Save** to complete the integration.

## Capabilities

### 1. Block Host

Action capability for blocking malicious host.

- Rollback: Yes
- Duplicate Control: Yes

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Integration</b>	Name of the 3rd party integration	Integration	N/A	Yes
<b>Rollback Mode</b>	Time to rollback this action. Default is no-rollback	N/A	N/A	No
<b>FQDN</b>	Host to be blocked	Host (It is written as domain object on Cisco ASA Firewall)	Yes	Yes

#### Output:

Case Scope: N/A

Human Readable Output: N/A

### 2. Block IP

Action capability for blocking malicious IP addresses.

- Rollback: Yes
- Duplicate Control: Yes

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Integration</b>	Name of the 3rd party integration.	Integration	N/A	Yes
<b>Rollback Mode</b>	Time to rollback this action. Default is no-rollback.	N/A	N/A	No
<b>IP Address</b>	IP address to be blocked	Network Address	Yes	Yes

#### Output:

Case Scope: N/A

Human Readable Output: N/A

# Integration Guide for Cisco Firepower Management Center

## Integration Overview

Cisco Firepower Management Center (formerly Sourcefire Firepower Management Center) is an administrative center node of the Firepower Threat Defense systems and manages critical Cisco network security solutions. It provides complete and unified management over firewalls, application control, intrusion prevention, URL filtering, and advanced malware protection.

This integration is tested with Cisco Firepower Management Center version 6.3.0 (build83).

## Integration Capabilities

ArcSight SOAR has the following integration capabilities with Cisco Firepower Management Center:

- Block IP
- Block URL

## Prerequisites

You must have access to HTTPS as the ArcSight SOAR connects to Cisco Firepower Management Center REST API through this service.

## Configuration

### Configuring Cisco Firepower Management Center

1. Login to **Management Center** and navigate to **System > Configuration > REST API Preferences** and enable **REST API**.
2. Navigate to **System > Users > User Roles** and create a new role with the following permissions:

- Object Manager>Modify Object Manager
- Deploy Configuration to Devices

Name: SOAR API Role

Description:

**Menu-Based Permissions**

- Overview
- Analysis
- Policies
- Devices
- Object Manager
- Rule Editor
- Modify Object Manager
- Cisco AMP
- Intelligence
- Deploy Configuration to Devices
- System

**System Permissions**

External Database Access

Save Cancel

3. Navigate to **System > Users > Users** and create a new user account with user role that you have created in the previous step.

User Configuration

User Name: soar

Authentication:  Use External Authentication Method

Password:

Confirm Password:

Maximum Number of Failed Logins: 5 (0 = Unlimited)

Minimum Password Length: 8

Days Until Password Expiration: 0 (0 = Unlimited)

Days Before Password Expiration Warning: 0

Options:

- Force Password Reset on Login
- Check Password Strength
- Exempt from Browser Session Timeout

User Role Configuration

Default User Roles:

- Administrator
- External Database User
- Security Analyst
- Security Analyst (Read Only)
- Security Approver
- Intrusion Admin
- Access Admin
- Network Admin
- Maintenance User
- Discovery Admin
- Threat Intelligence Director (TID) User

Custom User Roles:

- SOAR API Role

Save Cancel

4. Navigate to **Objects > Object Management** and create two object groups with the following configurations.

Name	Description	Allow Overrides
SOAR_BLOCK_IP	Object Group for IPs blocked by ArcSight SOAR.	True
SOAR_BLOCK_URL	Object Group for URLs blocked by ArcSight SOAR.	True



**Note:** You can use these object groups in required rules.

## Configuring SOAR

1. Click **Configuration > Credential > Create Credential**.
2. Specify the following parameter values in the **Credential Editor** form.

Type	Name	Username	Password	Private Key
Internal credential	Display name of credential set (for example, Cisco FMC Credential).	User you have created for SOAR on Cisco Firepower Management Center.	Password of the user that you have created for SOAR on Cisco Firepower Management Center.	

3. Click **Configuration > Integrations > Create Integration**.
4. Specify the following parameter values in the **Configuration** form.

Parameter	Value	
<b>Name</b>	Display name of the integration.	
<b>Type</b>	Cisco Firepower Management Center.	
<b>Address</b>	Address of the integration (the format must be https://10.10.20.40).	
<b>Configuration</b>	Specify the following configuration parameters:	
	<b>proxy.id</b>	ID of the Proxy integration if you access Cisco Firepower Management Center through a web proxy device. For example: proxy.id = 12345 .
	<b>network.object.group.name</b>	Name of the object group SOAR adds IP addresses into. network.object.group.name = SOAR_BLOCK_IP
	<b>url.object.group.name</b>	Name of the object group SOAR adds IP addresses into. url.object.group.name=SOAR_BLOCK_URL.
<b>Credential</b>	Credential that has been defined for this integration under the <b>Credentials</b> menu.	

Parameter	Value
<b>Trust Invalid SSL Certificates</b>	Select this if web server's certificate is self-signed or is not recognized by browsers.
<b>Require Approval From</b>	Select user(s) from list to ask the approval before executing actions on this integration.
<b>Notify</b>	Select user(s) from the list to notify when SOAR performs an action on this integration.

5. Click **Show Additional Parameters** checkbox and select the frequency of policy install in **Maintenance** dropdown.



As the devices managed by Cisco Firepower Management Center might get overloaded, in case of frequent attacks or misconfiguration, thus, SOAR does not deploy the changes after every action. Instead, you can define the frequency of the deployments in Maintenance menu by either selecting pre-defined values or by defining a custom Cron expression for scheduling.

The ArcSight SOAR uses spring-framework's Cron expression format. For the format and similar example, refer to the [Spring Framework-Cron Expression](#).

6. Click **Save** to save the integration definition.
7. Navigate to **Configuration>Customization Library** and edit **Cisco Firepower Management Center Advanced Action Script Default Template**.
8. Select the integration that you have added to **Integrations** menu.
9. Click **Save** to complete the integration.
10. Click **Test**, an **Integration Successful** message is displayed if the credential and address are valid.

## Capabilities

### 1. Block IP

Action capability for adding an IP to given object group.

- Rollback: Yes
- Duplicate Control: No

This table presents the **Block IP** action capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Integration</b>	Name of the third party integration	Integration	N/A	Yes
<b>Rollback Mode</b>	Time to rollback this action. Default is no-rollback	N/A	N/A	No
<b>IP</b>	IP address to be added to object group	Network Address	Yes	Yes

**Output:**

Case Scope: N/A

Human Readable Output: N/A

**2. Block URL**

Action capability for adding an URL to given object group.

- Rollback: Yes
- Duplicate Control: No

This table presents the **Block URL** action capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Integration</b>	Name of the third party integration	Integration	N/A	Yes
<b>Rollback Mode</b>	Time to rollback this action. Default is no-rollback	N/A	N/A	No
<b>URL</b>	URL to be added to object group	URL	Yes	Yes

**Output:**

Case Scope: N/A

Human Readable Output: N/A

# Integration Guide for Cisco Identity Service Engine

## Integration Overview

The Cisco Identity Services Engine (ISE) offers a network-based approach for adaptable, trusted access everywhere, based on the context. It provides intelligent, integrated protection through intent-based policy and compliance solutions. This integration has been tested with Cisco Identity Services Engine 2.3.0.238 version.

## Integration Capabilities

ArcSight SOAR has the following integration capability with Cisco Identity Services Engine:

### Action:

- Block MAC Address

## Configuration

### Prerequisites

Make sure to check the following prerequisites:

- Access to 443/tcpport as SOAR connects to Identity Services Engine API through HTTPS.
- An user account for SOAR to connect to Identity Services Engine

## Configuring Cisco Identity Services Engine

1. Create a user account and the user must be a member of MnT Admin.

## Configuring SOAR

1. Click **Configuration > Credentials > Create Credential**
2. Fill the **Credential Editor** form with following parameter values:

**a. Internal Credential:**

Parameter	Value
Type	Internal Credential
Name	Display name of credential set (For example, Cisco ISE credentials)
Username	User you have created for SOAR on Cisco Identity Services Engine
Password	Password of the user that you have created for SOAR on Cisco Identity Services Engine.
Private Key	Empty

**b. Credential Store:**

Parameter	Value
Type	External Credential
Name	Name of the credential with full path of the safe on store.

3. Click **Configuration > Integrations > Create Integration**.

4. Fill the configuration form with the following parameter values:

Parameter	Value
Name	Display name of Cisco Identity Services Engine integration on SOAR
Type	Cisco Identity Services Engine
Address	Address of the integration (the format must be https://192.168.2.3)
Credential	Name of the credential set you have just created on step 2 (For example, Cisco ISE Credentials)
Trust Invalid SSL Certificates	Select this if Firewall's certificate is self-signed or is not recognized by browsers
Configuration	You must specify the following configuration parameters.  <code>serverHost =</code>
Require Approval From	Select user(s) from list to ask her/his approval before executing actions on this integration
Notify	Select user(s) from the list to notify when SOAR performs an action on this integration.

5. Click **Test**. The following pop up will be displayed if your credential and address are valid.

6. Click **Save** to complete integration.

# Integration Guide for Cisco Ironport Email Security

## Integration Overview

Cisco Ironport Email Security is one of Cisco Ironport products to prevent phishing, business email compromise, ransomware and spam. This integration has been tested with Cisco Ironport Email Security 11.0.0-264 version.

## Integration Capabilities

ArcSight SOAR has the following integration capabilities with Cisco Ironport Email Security:

- Block sender IP/Host
- Block email that includes a keyword
- Block sender email

### Use Case: Stopping phishing campaigns

With this integration, SOAR can block emails based on sender, IP address or a keyword while responding to cyber-attacks. Blocking can be either performed automatically within a playbook or manually by an analyst.

## Configuration

### Prerequisites

Make sure to check the following prerequisites:.

- Access to 22/tcp port as SOAR connects to Cisco Ironport Email Security via SSH.
- A user account for SOAR to connect to Cisco Ironport Email Security.

### Configuring Cisco Ironport Email Security

1. To access the **Cisco Ironport Email Security resources**, create a user account with minimum **operator** role.

## Configuring SOAR

1. Click **Configuration > Credentials > Create Credential**.
2. Fill the Credential Editor form with the following parameter values:

a. **Internal Credential:**

Parameter	Value
Type	Internal Credential
Name	Display name of credential set (For example, Cisco Firepower Management Credentials)
Username	User you have created for SOAR on Cisco Firepower Management Center
Password	Password of the user that you have created for SOAR on Cisco Firepower Management Center.
Private Key	Empty

b. **Credential Store:**

Parameter	Value
Type	External Credential
Name	Name of the credential with pull path of the safe on store.

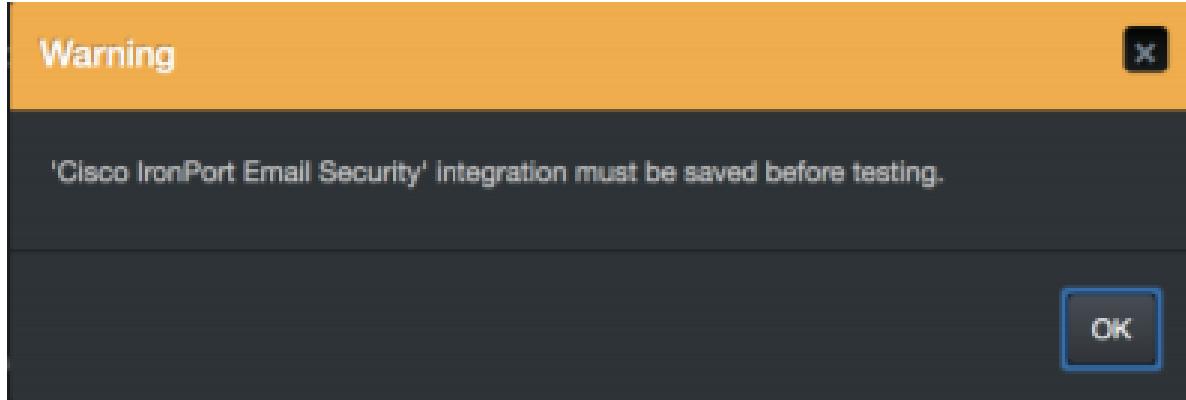
3. Click **Configuration > Integrations > Create Integration**.
4. Fill the configuration form with the following parameter values:

Parameter	Value
Name	Display name of Cisco Ironport Email Security integration on SOAR
Type	Cisco Ironport Email Security
Address	Address of the integration (the format must be 192.168.200.43)
Credential	Name of the credential set you have just created on step 2 (For example, Cisco Ironport Credentials)
Require Approval From	Select user(s) from list to ask her/his approval before executing actions on this integration
Notify	Select user(s) from the list to notify when SOAR performs an action on this integration.

5. Click **Save** to complete integration.
6. Click **Test** to test the integration.

## Additional Notes

- Cisco Ironport Email Security integration on SOAR is an Advanced Action Script, and you can access the content of the default script under **Configuration > Customization Library**.
- While defining integration for the first time, you might encounter the following warning message, which is the expected behavior for this type of integration.



## Integration Guide for Cisco SecureX

### Integration Overview

Cisco SecureX is designed to provide visibility, threat detection, and response capabilities across the entire security infrastructure of an organization. Cisco SecureX integrates various security products and services, both from Cisco and third-party vendors, into a unified platform. It aims to simplify security operations by bringing together different security tools and technologies, allowing security teams to manage and monitor them from a single interface.

### Supported Integration Capabilities

ArcSight SOAR has the following integration capabilities with Cisco SecureX:

- Get Observable Details
- Get Observable Score
- Get Event Details
- Get Threat Context (Targets)
- Respond observable

## Prerequisites

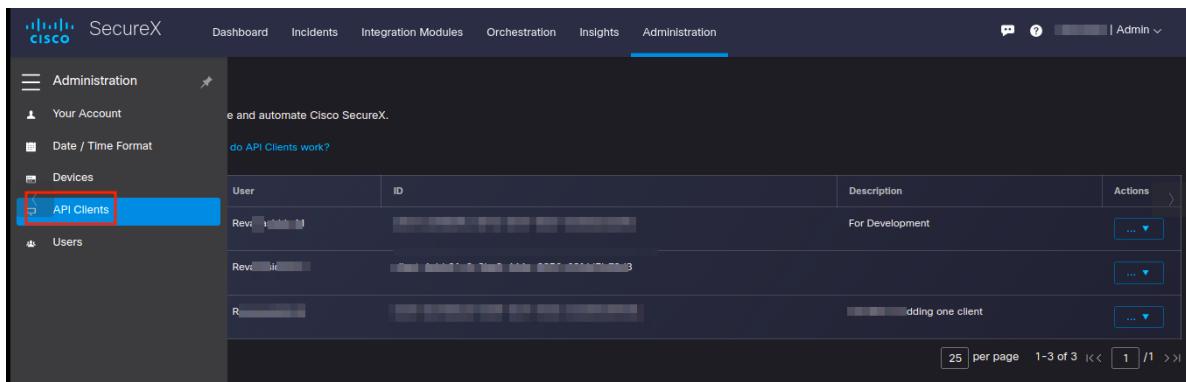
You must have access to HTTPS as the ArcSight SOAR connects to Cisco SecureX API through this service.

## Configuration

### Configuring Cisco SecureX

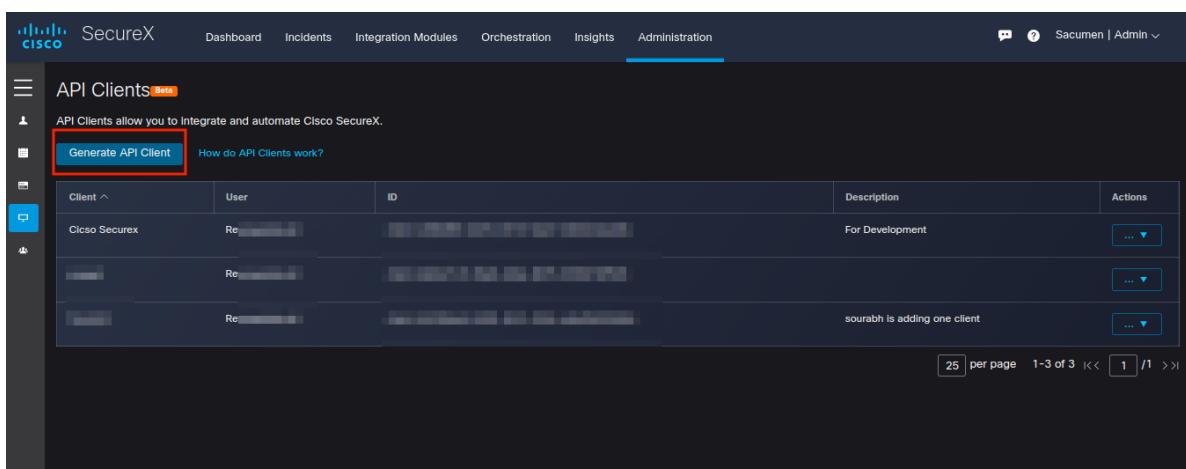
**Authentication:** Access the Cisco SecureX REST API basic auth. To begin, a user must obtain a client ID and client password from Cisco secureX Administrator. Following the basic steps shown below.

1. Click the Administration tab and choose API Clients in the navigation pane (“API Clients - Cisco”) as shown.



The screenshot shows the Cisco SecureX administration interface. The top navigation bar includes links for Dashboard, Incidents, Integration Modules, Orchestration, Insights, and Administration. The Administration tab is currently selected. On the left, a sidebar titled 'Administration' contains options like Your Account, Date / Time Format, Devices, and API Clients, with the 'API Clients' option highlighted by a red box. The main content area displays a table of API clients with columns for User, ID, Description, and Actions. There are three entries in the table, each with a '...' button under Actions. At the bottom, there are pagination controls showing 25 per page, 1-3 of 3, and a page number 1/1.

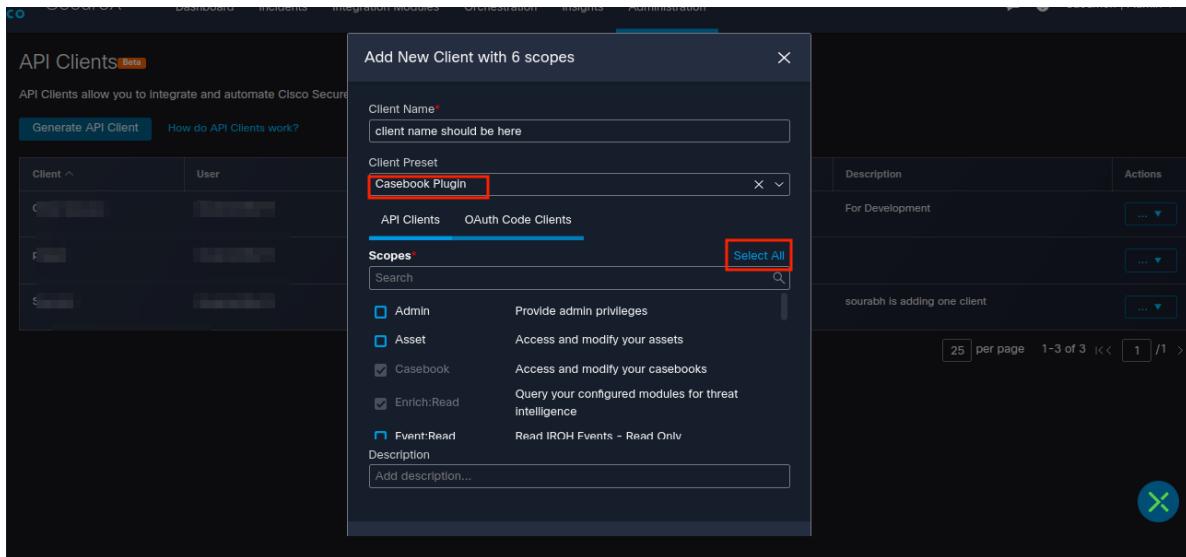
2. Click Generate API Client to create a new API client and client password for access token.



This screenshot shows the 'API Clients' page within the Cisco SecureX administration interface. The left sidebar shows the 'API Clients' section with a 'Generate API Client' button highlighted by a red box. The main content area displays a table of API clients with columns for Client, User, ID, Description, and Actions. There are three entries in the table, each with a '...' button under Actions. At the bottom, there are pagination controls showing 25 per page, 1-3 of 3, and a page number 1/1.

3. Enter a Client Name and optionally, choose a Client Preset from the drop-down list.

4. While creating the client id and client password, make sure to click on Select All for Scopes.



5. If you did not choose a Client Preset, check the check boxes for the scopes for which you want to grant privileges to the client. You can also click Select All to grant all scopes to the client.
6. Optionally, enter a Description and click Add New Client.

 On the last page, you will see the access key id and the secret code. You will need to save them somewhere securely.

## Configuring SOAR

1. Click Configuration > Credentials > Create Credentials.
2. Specify the following parameters values in the Credential Editor form.

Type	Name	Username	Password	Private Key
Internal credential	Display name of credential set (for example, Cisco SecureX Credentials).	The client ID obtained from the API administrator client.	The client password obtained from the API administrator for Reset client.	N/A

3. Select your integration plugin zip file and click **Save**.
4. Select the integration that you have added to **Integrations** menu.
5. Click **Save** to complete the integration.
6. Click **Test**, If the credential and address are valid a success message is displayed.
7. Parameters for the Token generation:

Parameters	Datatype	Description	Required
client_id	String	The client ID that's assigned to the user while generating an api client.	Yes
client_password	String	The Client secret that was generated for the user while generating an API client.	Yes
grant_type	String	The client_credentials will be passed internally	No

## Integration Capabilities:

### 1. Get Observable Details

Enrichment capability to get all enabled modules supporting the enrichment protocol with the supplied Observables to get any related Threat Context.

Request headers:

Header	Value	Required
Authorization	Bearer {token}	Yes
Content-type	application/json	No

Input Parameters:

Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
Observable Name	An Observable name and if user wants give multiple names with comma(,) example (google.com,example@domain.com)	HOST, KEYWORD, USERNAME, COMPUTER_NAME, MAC_ADDRESS, NETWORK_ADDRESS, UNKNOWN, EMAIL_ADDRESS, HASH	Yes	Yes

Output:

Case Scope: N/A

Limitation: N/A

Human Readable output:

a few seconds ago - S sacumen executed Get Observable Details enrichment on Cisco\_SecureX

Parameters Details

Key	Value
Module	SecureX Global Threat Intelligence
Attack Patterns	[ "Indirect Command Execution : https://intel.amp.cisco.com:443/ctia/attack-pattern/attack-pattern-78765354-33c1-4b72-8619-9b7901147327", "System Binary Proxy Execution : https://intel.amp.cisco.com:443/ctia/attack-pattern/attack-pattern-9492443a-0ebc-4c5c-a0da-e981e2e3739d", "Obfuscated Files or Information : https://intel.amp.cisco.com:443/ctia/attack-pattern/attack-pattern-204f3365-3c2b-4d7f-90f8-16c37ab6b2fa", "Command and Scripting Interpreter : https://intel.amp.cisco.com:443/ctia/attack-pattern/attack-pattern-441a28b5-6f84-4b84-913c-df7a2fb95931" ]
Sightings	[ "Talos Threat Advisory Blog : https://blog.talosintelligence.com/following-the-Lnk-metadata-trail" ]
Indicators	[ "Threat Spotlight: Following the LNK metadata trail : https://intel.amp.cisco.com:443/ctia/indicator/indicator-dd5baa69-ba69-4c9c-9635-617276336292" ]
Actors	[ "Gamaredon Group, IRON TILDEN, Primitive Bear, ACTINIUM, Armageddon, Shuckworm, DEV-0157 : https://intel.amp.cisco.com:443/ctia/actor/actor-6be0ce84-af78-461a-a649-1e75abedfb7a" ]

Judgements	[ "Talos Threat Advisory Blog : https://blog.talosintelligence.com/following-the-Lnk-metadata-trail" ]
Malwares	[ "IcedID : https://intel.amp.cisco.com:443/ctia/malware/malware-09cc7e83-9cd5-4b1d-9fa2-bad49ef74253", "QakBot : https://intel.amp.cisco.com:443/ctia/malware/malware-9bb3550d-a45e-4a44-81aa-62753c9cb086" ]
Module	AMP File Reputation
Verdicts	Malicious
Judgements	[ "AMP Protect DB : N/A" ]

100 ▾  
Total 10 , items / page 1

## 2. Get Observable Score

Enrichment capability to get fast Verdicts from all your integrations.

Request headers:

Header	Value	Required
Authorization	Bearer {token}	Yes
Content-type	application/json	No

Input Parameters:

Parameter	Description	Type	Scope	Restricted (Yes/No)	Required (Yes/No)
Observable Name	An Observable names with comma(,) example (google.com,example@domain.com)	HOST, KEYWORD, USERNAME, COMPUTER_NAME, MAC_ADDRESS, NETWORK_ADDRESS, UNKNOWN, EMAIL_ADDRESS, HASH	Yes	Yes	

Output:

Case Scope:

Action	Type	Category/ Value
Set	Scope Item Property	Cisco SecureX Observable DispositionScore
Set	Scope Item Property	Cisco SecureX Observable DispositionName

Case Scope Property Output:

The screenshot shows a dark-themed interface for managing scope items. At the top, there's a button labeled '+ Add New Scope Item' and a small orange tag icon. Below this, a list of scope items is shown, with the first item highlighted. The details for this item are displayed in a table:

Source	Alert
Role	Related
Other Roles	Related
CISCO SECUREX OBSERVABLE DISPOSITION NAME	Unknown
CISCO SECUREX OBSERVABLE DISPOSITION SCORE	5
Alerts	Show alerts with this scope item

Limitation: None

Human Readable Output:

a few seconds ago - S sacumen executed Get Observable Score enrichment on Cisco_SecureX				
<a href="#">Parameters Details</a> <span style="float: right;">Search</span> <span style="float: right;">⚙️</span>				
Module Name	Disposition Score	Disposition Name	Started Time	Ended Time
SecureX Global Threat Intelligence	1	Clean	2023-08-14T09:42:02.778Z	2023-08-21T09:42:02.778Z
AMP File Reputation	N/A	N/A	N/A	N/A
Talos Intelligence	1	Clean	2023-08-21T07:56:38.056Z	2023-09-20T07:56:38.056Z
Talos Intelligence	5	Unknown	2023-08-21T07:56:38.084Z	2023-09-20T07:56:38.084Z

Total 4 , items / page 1

### 3. Get Event Details

Enrichment capability to get event details.

Request headers:

Header	Value	Required
Authorization	Bearer {token}	Yes
Content-type	application/json	No

Input Parameters:

Parameter	Description	Type	Scope Restricted(Yes/No)	Required (Yes/No)
Event ID	Event Id need to be entered	String	No	Yes

Output:

Case Scope: N/A

Limitation: None

## Human Readable Output:

Key	Value
Event ID	722e19bd-20b5-413a-b5af-90aa4b25d905
Created At	2023-07-23T06:15:38.309Z
Event Type	module-instance/created
Module Instance ID	0ddeb1bd-acf5-45f4-a347-320cdf5cc709
Module Type ID	188d70f7-29d5-5069-9098-d83a3ec8e797
Module Instance Visibility	org
Issuer	IROH
User ID	2abee746-c90f-5e71-a1fb-1119a89cat65
Org ID	7cf4abc5-d82d-5433-bce9-a0d9e993cdff8

Total 9 , items / page      1

## 4. Get Threat Context (Targets)

Enrichment capability to This route queries all enabled modules supporting the enrichment protocol with the supplied Observables to get any related Threat Context

Request headers:

Header	Value	Required
Authorization	Bearer {token}	Yes
Content-type	application/json	No

Input Parameters:

Parameter	Description	Type	Scope	Restricted (Yes/No)	Required (Yes/No)
Observable Name	An Observable names with comma(,) example (google.com,example@domain.com)	HOST, KEYWORD, USERNAME, COMPUTER_NAME, MAC_ADDRESS, NETWORK_ADDRESS, UNKNOWN, EMAIL_ADDRESS, HASH	Yes		Yes

Output:

Case Scope: N/A

Limitation: N/A

Human Readable Output:

The screenshot shows a web-based interface for threat context enrichment. At the top, there's a header bar with the text "a few seconds ago - S sacumen executed Get Threat Context (Targets) enrichment on Cisco\_SecureX". Below the header are two tables of data.

Key	Value
Module	SecureX Global Threat Intelligence
Source	ZeroDot1_CoinBlockerLists
Description	N/A
Source URI	<a href="https://zerodot1.gitlab.io/CoinBlockerLists/white_list.txt">https://zerodot1.gitlab.io/CoinBlockerLists/white_list.txt</a>
Target Observable	N/A
Module	Talos Intelligence
Observable threat context (Targets)	Talos Intelligence module does not contains targets and threat contexts
Module	Secure Endpoint - Sourabh
Source	AMP Event
Description	NFM iOS Sighting
Source URI	<a href="https://console.amp.cisco.com/computers/0271fd89-3dc3-4e9a-84ee-13bdea412080/trajectory?q=google.com">https://console.amp.cisco.com/computers/0271fd89-3dc3-4e9a-84ee-13bdea412080/trajectory?q=google.com</a>
Targeted Observable Hostname	Demo_iOS_1
Targeted Observable Amp Computer Guid	0271fd89-3dc3-4e9a-84ee-13bdea412080

Targeted Observable Ip	232.183.35.180
Targeted Observable Mac Address	cc:5e:5b:e7:10:4f
Targeted OS	iOS 17.0 (iPhone14,6)
Observable Relations Hosted By	[{"Source Value": "http://benhomelandefit.com/rssnews.php", "Related Value": "75.102.25.76"}]
Observable Relations File Name Of	[{"Source Value": "iexplore.exe", "Related Value": "b4e5c2775de098946b4e11aba138b89d42b88c1dbd4d5ec879ef6919bf018132"}, {"Source Value": "iexplore.exe", "Related Value": "814a37d89a79aa3975308e723bc1a3a67360323b7e3584de00896fe7c59bbb8e"}]
Observable Relations Connected To	[{"Source Value": "192.168.1.3", "Related Value": "75.102.25.76"}, {"Source Value": "b4e5c2775de098946b4e11aba138b89d42b88c1dbd4d5ec879ef6919bf018132", "Related Value": "75.102.25.76"}, {"Source Value": "814a37d89a79aa3975308e723bc1a3a67360323b7e3584de00896fe7c59bbb8e", "Related Value": "http://benhomelandefit.com/rssnews.php"}, {"Source Value": "9.43.56.65", "Related Value": "75.102.25.76"}, {"Source Value": "814a37d89a79aa3975308e723bc1a3a67360323b7e3584de00896fe7c59bbb8e", "Related Value": "75.102.25.76"}]

At the bottom of the interface, there are pagination controls: "Total 19 , items / page" and a page number "1".

## 5. Respond Observable

Action capability to Respond Observables helps security teams to apply necessary response actions, such as containment, blocking, or isolation of affected entities.

Rollback: Yes

Duplicate Control: No

Request headers:

Header	Value	Required
Authorization	Bearer {token}	Yes
Content-type	application/json	No

Input Parameters:

Parameter	Description	Type	Scope	
			Restricted (Yes/No)	Required (Yes/No)
Observable Hash Value	An observable hash	KEYWORD UNKNOWN, HASH	Yes	Yes

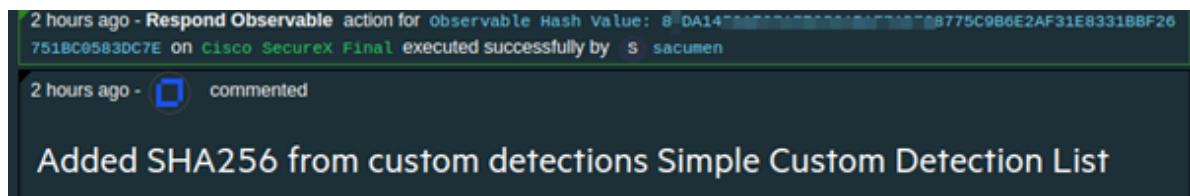
API Method Documentation:

Output:

Case Scope: N/A

Limitation: N/A

Human Readable Output:



## Integration Guide for Cisco Umbrella

### Integration Overview

Cisco Umbrella provides resolution of threats to cloud protection. Cisco paragliding provides flexible cloud protection when and how you ask for it. It combines various security features into one solution, helping you to optimize your data on incident response and rapidly improve safety across devices and locations.

### Integration Capabilities

ArcSight SOAR has the following integration capabilities with Cisco Umbrella:

- Get Domain Status
- Get Security Score Information
- Get Risk Score
- Get WHOIS Domain
- Get Related Domain
- Get Co-occurrences
- Get Passive DNS Record

## Prerequisites

You must have HTTPS access as ArcSight SOAR connects to Cisco Umbrella API through this service.

## Configuration

### Configuring Cisco Umbrella

API requires Token authentication which can be extracted from the dashboard.

1. Navigate to Investigate > API Keys > Create New Token.
2. Enter a token name and click Create.



The generated token includes the email address of the person who created it and the token creation date. To revoke the token, click the delete icon.



You can use any number of valid Investigate API access tokens to authorize and Investigate API requests.

### Configuring SOAR

1. Click Configuration > Credential > Create Credential.
2. Specify the following parameter values in the Credential Editor form:

Type	Name	Username	Password	Private Key
Internal credential	Display name of credential set (for example, Cisco Umbrella Credentials)	N/A	N/A	Bearer {token}

3. Click Configuration > Integrations > Upload plugin.
4. Select your integration plugin zip file and click Save.
5. Select the integration that you have added to the Integrations menu.
6. Click Save to complete the integration.
7. Click Test. A successful message is displayed if the credential and address are valid.

## Integration Capabilities

### 1. Get Domain Status

Enrichment capability to look up the status, and security and content category IDs for the domain.

#### **Input Parameters:**

Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
Domain	A domain name. For example, 'opentext.com'.	HOST, UNKNOWN, KEYWORD	Yes	Yes

#### **Default Parameters:**

Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
showLabels	Include the showLabels query parameter to display the human-readable or named category labels in the response.	Boolean	No	No

#### **Output:**

Case Scope:

N/A

Human Readable :

Key	Value
Status	safe
Security Categories	N/A
Content Categories	[ "Software/Technology", "Business Services", "Computers and Internet" ]

### 2. Get Security Score Information

Enrichment capability to list multiple scores or security features of a domain

#### **Input Parameters:**

Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
Domain	A domain name. For example, 'opentext.com'.	HOST, UNKNOWN, KEYWORD	Yes	Yes

## Output:

## Case Scope:

N/A

## Human Readable :

Geo Diversity Normalized	[["BM", 0.13011612150372967], ["SO", 0.11521633561296357], [0.0842140453065806], ["GQ", 0.05567870764071444], ["MP", 0.0520982290866921], ["LC", 0.032035374802228], ["ES", 0.02952773440772515], ["JP", 0.023524272467427578], ["TC", 0.021394843534347736], ["MW", 0.017920390433431684], ["ZA", 0.014851502650070581], ["AW", 0.013596616800255193], ["KY", 0.01297097347810252], ["DM", 0.01224931568095718], ["IM", 0.011488543247711588], ["NE", 0.011056866966053598], ["AU", 0.009798426438900514], ["MG", 0.00959776178046056], ["VG", 0.009584825822987834], ["IL", 0.009141606774933225], ["GY", 0.008960822461743262], ["ZW", 0.008939545280117502], ["SN", 0.008871394335435753], ["BF", 0.00861466780173649], ["AG", 0.008352169441863663], ["BB", 0.008264808165418549], ["MZ", 0.008199951882771372], ["SG", 0.008120174546811855], ["LY", 0.006467856544186878], ["NA", 0.0061355197654221596], ["GU", 0.005408372015633028], ["QA", 0.00524999380141098], ["ML", 0.005142222667657675], ["ME", 0.005084621603416188], ["UG", 0.004894667668476694], ["HK", 0.00483500014047142], ["CR", 0.00478015381242424], ["KW", 0.004766951098562619], ["SA", 0.004593967339309916], ["KE", 0.0044616934907907605], ["MT", 0.004321803901818206], ["TZ", 0.004296490748363795], ["SV", 0.0041368780436617115], ["AT", 0.0038336635338383175], ["AE", 0.0038186740599361678], ["US", 0.003733933274307489], ["IS", 0.003697652922352606], ["NZ", 0.0036094169997616743], ["MO", 0.003583777055434305], ["NL", 0.0034305116364346283], ["DE", 0.0034218437493523652], ["GE", 0.003405756255580751], ["MX", 0.0033483481415477402], ["KG", 0.0032631117789844633], ["KR", 0.003218883719315073], ["BO", 0.0032164303018460826], ["OM", 0.0031478015213574945], ["IN", 0.002994147713194139], ["PA", 0.002894171552371821], ["MV", 0.0028179493421244366], ["CI", 0.0028008697401864804], ["ET", 0.0027981146056791154], ["CA", 0.002761827333617075], ["CH", 0.0027321918010848804], ["CZ", 0.002724923152767187], ["HU", 0.002688966745369394], ["GT", 0.0026827291618498846], ["UY", 0.002648103455134159], ["KH", 0.0025466606093029307], ["HT", 0.00254009105976907], ["GB", 0.0024529187826529525], ["BH", 0.002395399320071906], ["PT", 0.0023671244271030573], ["FR", 0.0023280408625176376], ["LU", 0.002317482055943173], ["GH", 0.0022450973659093143], ["GE", 0.0022339502419695726], ["JO", 0.00221648103455134159]
--------------------------	---

TLD Geo Diversity	N/A
Geo Score	0
KS Test	0
Attack	N/A
Threat Type	N/A
Found	true

### 3. Get Risk Score

Enrichment capability to get the risk score for a domain. The risk score is scaled from 0 to 100, with 100 being the highest risk and 0 being no risk at all.

Input Parameters:

Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
Domain	A domain name. For example, 'opentext.com'.	HOST, UNKNOWN, KEYWORD	Yes	Yes

**Output:**

Case Scope:

Action	Type	Category / Value
Domain	Scope Item Property	Cisco Umbrella Risk Score

Human Readable Output:

Key	Value
Indicators	[{"Indicator": "Geo Popularity Score", "normalized_score": 50, "score": 0, "indicator_id": "Geo Popularity Score"}, {"Indicator": "Keyword Score", "normalized_score": 50, "score": 0.5, "indicator_id": "Keyword Score"}, {"Indicator": "Lexical", "normalized_score": 100, "score": 1, "indicator_id": "Lexical"}, {"Indicator": "Popularity 1 Day", "normalized_score": null, "score": null, "indicator_id": "Popularity 1 Day"}, {"Indicator": "Popularity 30 Day", "normalized_score": null, "score": null, "indicator_id": "Popularity 30 Day"}, {"Indicator": "Popularity 7 Day", "normalized_score": null, "score": null, "indicator_id": "Popularity 7 Day"}, {"Indicator": "Popularity 90 Day", "normalized_score": null, "score": null, "indicator_id": "Popularity 90 Day"}, {"Indicator": "TLD Rank Score", "normalized_score": 0, "score": 0, "indicator_id": "TLD Rank Score"}, {"Indicator": "Umbrella Block Status", "normalized_score": 0, "score": false, "indicator_id": "Umbrella Block Status"}]
Risk Score	79

**4. Get WHOIS Domain**

Enrichment capability to fetch WHOIS information for the specified domain

Input Parameters:

Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
Domain	A domain name without wildcard and including top-level domain (TLD)	HOST, UNKNOWN, KEYWORD	Yes	Yes

**Output:**

Case Scope:

N/A

Human Readable Output:

Key	Value
Whois Servers	whois.markmonitor.com
Addresses	[ "170 w. tasman dr." ]
Administrative Contact Name	Domain Administrator
Administrative Contact Email	infosec@cisco.com
Technical Contact Email	infosec@cisco.com
Technical Contact Fax	14085264575
Name Servers	[ "ns1.cisco.com", "ns2.cisco.com", "ns3.cisco.com" ]
Administrative Contact City	San Jose
Registrant Name	MarkMonitor, Inc.
Domain Name	cisco.com
Technical Contact Country	UNITED STATES
RegistrarIANAID	292
Updated	2022-04-13
Status	[ "clientDeleteProhibited clientTransferProhibited clientUpdateProhibited serverDeleteProhibited serverTransferProhibited serverUpdateProhibited" ]
Registrar Name	MarkMonitor, Inc.
Technical Contact Organization	Cisco Technology Inc.
Emails	[ "infosec@cisco.com" ]
Audit Updated Date	2023-03-06 00:19:37 UTC
Record Expired	false

## 5. Get Related Domain

Enrichment capability to get a list of domain names that have been frequently requested around the same time (up to 60 seconds before or after) as the given domain name, but that are not frequently associated with other domain names.

Input Parameters:

Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
Domain	A domain name. For example, 'opentext.com'.	HOST, UNKNOWN, KEYWORD	Yes	Yes

**Output:**

Case Scope:

N/A

Human Readable Output:

Domain	Number Of Client Ip Requests
site.com	447
google.com	375
sfdcopens.com	328
salesforcecr.com	265
trailblazer.me	248
salesforce-sitesa.com	247
yahoo.com	239
salesforce.com	224
meraki.com	223
sfdc.sh	219
salesforce-cr.com	202
trailhead.com	187
salesforce-hub.com	131

## 6. Get Co-occurrences

Enrichment capability to list the co-occurrences for the specified domain.

Input Parameters:

Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
Domain	A domain name. For example. 'cisco.com'	HOST, UNKNOWN, KEYWORD	Yes	Yes

**Output:**

Case Scope:

N/A

Human Readable Output:

Domain	Value
visualforce.com	0.1395325910962083
trailhead.com	0.12338393401066777
sfdc.sh	0.0940698919293961
sfdcopens.com	0.085611968091635
site.com	0.0765182794794976
salesforce-sitesa.com	0.07137240765308193
salesforce-cr.com	0.06880765715826874
salesforce-hub.com	0.0674292465481571
salesforce-experience.com	0.05971431124816412
salesforce-communities.com	0.05116082433262011
salesforcecr.com	0.03937267908814215
salesforce.com	0.028666262043139404
lightning.com	0.027756049323472236
force-user-content.com	0.019588643799334343
forceusercontent.com	0.016911967447479512
trailblazer.me	0.012054556521978586

## 7. Get Passive DNS Record

Enrichment capability returns the Resource Record (RR) data for DNS responses, and categorization data, where the answer (or data) is the domain(s).

Input Parameters:

Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
Domain	A domain name. For example, 'cisco.com'.	HOST, UNKNOWN, KEYWORD	Yes	Yes

Query Parameters:

Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
limit	The number of records to return in the collection. The default limit is 500 records. The maximum number of records returned for all requests to the endpoint is 10,000.	integer	No	Yes
offset	A number that represents an index into the collection. By default, the offset is 0 (the first record).	integer	No	No
sortorder	Sort records by ascending (asc) or descending (desc) order. By default, the records are returned in descending order.	string	No	No
sortby	Sort records by one of the following fields: minTtl, maxTtl, firstSeen, or lastSeen.	string	No	No
recordType	The type of records. For example: 'A', 'CNAME', 'NS', 'MX'. Use commas to separate multiple types of record.	string	No	No
includefeatures	Specify 'true' to add feature sections to the response. The default value is 'false'.	boolean	No	No
minFirstSeen	Returns only records with firstSeen >= minFirstSeen.	integer	No	No
maxFirstSeen	Returns only records with firstSeen <= maxFirstSeen.	integer	No	No
minLastSeen	Returns only records with lastSeen >= minLastSeen.	integer	No	No

Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
maxLastSeen	Returns only records with lastSeen <= maxLastSeen.	integer	No	No
sortCategories	Comma-separated list of security categories or 'All'. 'All' stands for all security categories. Records which have at least one of these security categories will be first in the ordering. The rest of the sorting parameters are applied within the records with and without any of the security categories.	string	No	No
requiredCategories	Filter for records with security categories. The case-sensitive security category strings are Drive-by Downloads/Exploits, Mobile Threats, Dynamic DNS, High Risk Sites and Locations, Command and Control, Malware, Phishing, Newly Seen Domains, Potentially Harmful, DNS Tunneling VPN, and Cryptomining. Use commas to separate multiple security category strings.	string	No	No

**Output:**

Case Scope:

N/A

Human Readable Output:

Name	Type	First Seen	Last Seen	Min Ttl	Max Ttl	Rr	Security Categories	Content Categories
cisco.com	CNAME	2017-11-23T07:29Z	2023-03-08T05:40Z	23	600	master.cisco.com.	N/A	[ "Software/Techology", "Business Services", "Computers and Internet" ]
cisco.com	CNAME	2022-10-11T11:13Z	2023-03-05T20:23Z	1799	1799	uncle.cisco.com.	N/A	-
cisco.com	CNAME	2017-11-21T16:51Z	2023-03-04T11:29Z	300	300	www.slcsec.com.	N/A	[ "Software/Techology", "Computers and Internet" ]
cisco.com	CNAME	2022-05-05T12:25Z	2023-03-04T10:37Z	300	300	cisco.gladstonefamily.net.	N/A	[ "Forums/Message boards", "Online Communities" ]
cisco.com	CNAME	2023-03-03T17:17Z	2023-03-03T17:17Z	300	300	test.animeshjordan.com.	N/A	N/A
cisco.com	CNAME	2020-05-04T20:30Z	2023-02-27T12:49Z	86400	86400	tomwisehere.net.rubbermaid.com.	N/A	[ "Business Services", "Business and Industry" ]
cisco.com	CNAME	2023-02-05T14:40Z	2023-02-05T15:46Z	300	300	www.cotech.com.ar.	N/A	[ "Business Services", "Business and Industry" ]

# Integration Guide for CrowdStrike Falcon

## Integration Overview

CrowdStrike is a cloud based cybersecurity tool that allows organizations to leverage its lightweight agent. The agent is an all-encompassing EDR and antivirus software.

## Integration Capabilities

- Isolate Machine
- Unisolate Machine
- Add Comment to Detection
- Update Detection Status
- Assign Detection
- Get IOC Details
- Get Hosts by IOC
- Get Process by IOC

- List Host Vulnerabilities
- Get Host Details

## Prerequisites

- ArcSight SOAR connects to <https://falcon.crowdstrike.com/login/> APIs through HTTPS. Access to this service is required.
- CrowdStrike requires an API key for access.

## Configuration

### Configuring CrowdStrike

- CrowdStrike requires a Client ID and Client secret for access.
- Users with the Falcon Administrator role can create a Client ID and Client secret from <https://falcon.crowdstrike.com/> after logging in with valid credentials.

### Configuring SOAR

1. Click **Configuration > Credential > Create Credential**.
2. Specify the following parameter values in the **Credential Editor**:

Type	Name	Username	Password	Private Key
Internal credential	Display name of credential set (for example, CrowdStrike Falcon).	Empty	Client ID created on CrowdStrike Falcon	Client Secret for the Client ID created on CrowdStrike Falcon

3. Click **Configuration > Integrations > Create Integration**.
4. Specify the following parameter values in the **Configuration Form**:

Parameter	Value
Name	Display name of the integration
Type	Advanced Scriptable Device
Address	Address of the integration (the format should be https://api.crowdstrike.com/)

Parameter	Value
Configuration	<p>Specify the following configuration parameters:</p> <pre>Specify the following configuration parameters: # Integration ID of the proxy integration to use when connecting to current integration. # If not provided, ArcSight SOAR will try to use a direct connection. #proxy.id=123 # Maximum number of results to return from the API # If not provided, the integration will gather all results #max.result.count = 100</pre>
Credential	Credential that has been defined for this integration under <b>Credential</b> menu.
Trust Invalid SSL Certificates	Select this if Engine's certificate is self-signed or not recognized by browsers. Not selected.
Require Approval From	Select user(s) from the list to ask their approval before executing enrichments on this integration.
Notify	Select user(s) from the list to notify when SOAR performs an action on this integration.

5. Select the integration that you have added in the **Integrations** menu.
6. Click **Save** to complete the integration.
7. Click **Test**, an **Integration Successful** message is displayed if the credential and address are valid.

## Capabilities

### 1. Isolate Machine

Action capability for isolating a machine.

- Rollback: Yes
- Duplicate Control: Yes

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
Host	Network address, hostname or agent ID of the machine.	Network Address Computer Name Keyword Unknown	Yes	Yes

### Output:

Case Scope

N/A

Human Readable Output

N/A

**2. Unisolate Machine**

Action capability to unisolate a machine.

- Rollback: Yes
- Duplicate Control: Yes

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
Host	Network address, hostname or agent ID of the machine.	Network Address Computer Name Keyword Unknown	Yes	Yes

**Output:**

Case Scope

N/A

Human Readable Output

N/A

**3. Add Comment to Detection**

Action capability for adding a comment to a detection.

- Rollback: No
- Duplicate Control: No

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
Detection ID	CrowdStrike Detection ID.	Unknown	Yes	Yes
Comment	Comment added to the detection.	String	No	Yes

**Output:**

Case Scope

N/A

Human Readable Output

N/A

**4. Update Detection Status**

Action capability for updating detection status.

- Rollback: No

- Duplicate Control: No

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
<b>Detection ID</b>	CrowdStrike Detection ID.	Unknown	Yes	Yes
<b>Status</b>	Status from the following drop down menu options: New, In Progress, Closed, True Positive, False Positive, Ignored.	String	No	Yes

**Output:**

Case Scope

N/A

Human Readable Output

N/A

**5. Assign Detection**

Action capability for assigning a detection to a user.

- Rollback: No
- Duplicate Control: No

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required(Yes/No)
<b>Detection ID</b>	CrowdStrike Detection ID.	Unknown	Yes	Yes
<b>Email Address</b>	User email	String	No	Yes

**Output:**

Case Scope

N/A

Human Readable Output

N/A

**6. Get IOC Details**

Enrichment capability used to get the details of an IOC.

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
<b>Integration</b>	Name of the 3rd party integration.	Integration	N/A	Yes
<b>IOC</b>	SHA256 or MD5 hash value, network address or domain.	Hash Network Address Host URL	Yes	Yes
<b>Do not Use Cache</b>	SOAR does not use cached results if this box is checked.	Boolean	N/A	No

**Output:**

Case Scope

Action	Type	Category/Value
Set	Scope Item Property	CrowdStrike Severity

Human Readable Output

N/A

**7. Get Hosts by IOC**

Enrichment capability used to retrieve hosts where the IOC has been observed.

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
<b>Integration</b>	Name of the 3rd party integration.	Integration	N/A	Yes
<b>IOC</b>	SHA256 or MD5 hash value, network address or domain.	Hash Network Address Host URL	Yes	Yes
<b>Do not Use Cache</b>	SOAR does not use cached results if this box is checked.	Boolean	N/A	No

**Output:**

Case Scope

Action	Type	Category/Value
Set	Scope Item/Related	Hostname (Computer Name)

Human Readable Output

N/A

## 8. Get Process by IOC

Enrichment capability used to retrieve the process name of the IOC on the devices where the IOC has triggered a detection.

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
<b>Integration</b>	Name of the 3rd party integration.	Integration	N/A	Yes
<b>Hash</b>	SHA256 or MD5 hash value, network address or domain.	Hash	Yes	Yes
<b>Host</b>	Network address, hostname or agent ID of the machine.	Network Address Computer Name Keyword Unknown	Yes	No
<b>Do not Use Cache</b>	SOAR does not use cached results if this box is checked.	Boolean	N/A	No

### Output:

Case Scope

Action	Type	Category/Value
Set	Scope Item Property	CrowdStrike Process Name

Human Readable Output

N/A

## 9. List Host Vulnerabilities

Enrichment capability used to list the vulnerabilities on a host.

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
<b>Integration</b>	Name of the 3rd party integration.	Integration	N/A	Yes
<b>Status</b>	Status from the following options: All, Open, Closed, Reopen, Expired	String	No	Yes

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
Host	Network address, hostname or agent ID of the machine.	Network Address Computer Name Keyword Unknown	Yes	No
Do not Use Cache	SOAR does not use cached results if this box is checked.	Boolean	N/A	No

**Output:**

Case Scope

Action	Type	Category/Value
None	None	None

Human Readable Output

N/A

**10. Get Host Details**

Enrichment capability used to get the details of a host.

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
Integration	Name of the 3rd party integration.	Integration	N/A	Yes
Host	Network address, hostname or agent ID of the machine.	Network Address Computer Name Keyword Unknown	Yes	No
Do not use cache	SOAR does not use cached results if this box is checked.	Boolean	N/A	No

**Output:**

Case Scope

Action	Type	Category/Value
Set	Scope Item/Related	Hostname (Computer Name)

Human Readable Output

N/A

# Integration Guide for Cyberark Central Credential Provider

## Integration Overview

CyberArk Application Identity Manager is a central credential provider that stores passwords and other credentials used by systems, applications, and scripts by eliminating embedded credentials. SOAR might use encrypted credentials stored on its database and CyberArk AIM vault to connect to other systems and applications while investigating and responding to an incident.

## Configuration

### Prerequisites

- Make sure to check the access to CyberArk Application Identity Manager API as SOAR connects to it through HTTPS.
- Define a new application for SOAR on CyberArk's PVWA (Password Vault Web Access) Interface.

### Configuring CyberArk Application Identity Manager

1. Log in to **Password Vault Web Access** interface as a user with **Manage Users** authorization permission.
2. Navigate to **Applications** and click **Add Application**.
3. Fill the Add Application form with the following parameter values:

Parameter	Value
Name	Specify SOAR as the unique name (ID) of the application.
Description	Specify a short description of the application (For example, Application for Automated Threat Analysis&Response)
Business Owner	Specify contact information about the application's Business owner
Location	Specify the location of the application in the Vault hierarchy.  <b>Note:</b> If the location is not selected, the application gets added to the user location who creates it.

4. To specify unlimited number of machines and Windows OS users for a single application, select **Allow extended authentication restrictions**.
5. Navigate to **Allowed Machines** and specify the application's Allowed Machines.



**Note:** This information enables the Credential Provider to check only applications that run from specified machines can access their passwords.

## Configuring SOAR

1. Click **Configuration > Credentials > Create Credential**.
2. Fill the **Credential Editor** form with the following parameter values:
  - a. **Internal Credential:**

Parameter	Value
Type	Internal Credential
Name	Display name of credential set (For example, CyberArk AIM Credential)
Username	Application Name you have created on CyberArk Password Vault Web Access
Password	Empty
Private Key	Empty

3. Click **Configurations > Integrations > Create Integration**.
4. Fill the **Configuration** form with the following details:

Parameter	Value
Name	Display name of CyberArk AIM integration on SOAR
Type	CyberArk Central Credential Provider
Address	Address of the integration (the format must be https://192.168.1.1:1234 or https://abc.example.com:1234)
Credential	Name of the credential set you have just created on step 2 (For example, CyberArk AIM Credential).
Trust Invalid SSL Certificates	Select this if device's certificate is self-signed or is not recognized by browsers
Require Approval From	Select user(s) from list to ask her/his approval before executing actions on this integration
Notify	Select user(s) from the list to notify when SOAR performs an action on this integration

5. Click **Save** to complete integration.

6. Click **Test** to test the integration.

## Additional Notes

Following are the steps to use CyberArk AIM as central credential store:

1. Navigate to **Configuraiton > Parameters**.
2. Modify the **ExternalCredentialStoreIntegrationID** parameter value to ID of the CyberArk AIM integration that you have defined in the above procedure.
3. To define the new name for a credential:
  - a. Navigate to **Configuration > Credentials**.
  - b. Select **External Credential** from the drop down and it automatically uses CyberArk AIM integration.



**Note:** The name of the credential must be the same as the account name defined in CyberArk. Make sure to follow the naming convention of SOAR as Safe and Folder separated by | character. Else, SOAR automatically searches all Safes for the given credential name.

# Integration Guide for CYMRU Malware Hash Registry Query

## Integration Overview

CYMRU is a look-up service that checks if the hash code is malware. If the hashcode belongs to malware, then the latest timestamp of the malware and the rough antivirus package detection rate is returned. ArcSight SOAR uses CYMRU Malware Hash Registry Query to query computed MD5 or SHA-1 hash of a file to check for malware.

## Integration Capabilities

### Action

- Hash registry query

## Configuration

### Configuring CYMRU Malware Hash Registry Query

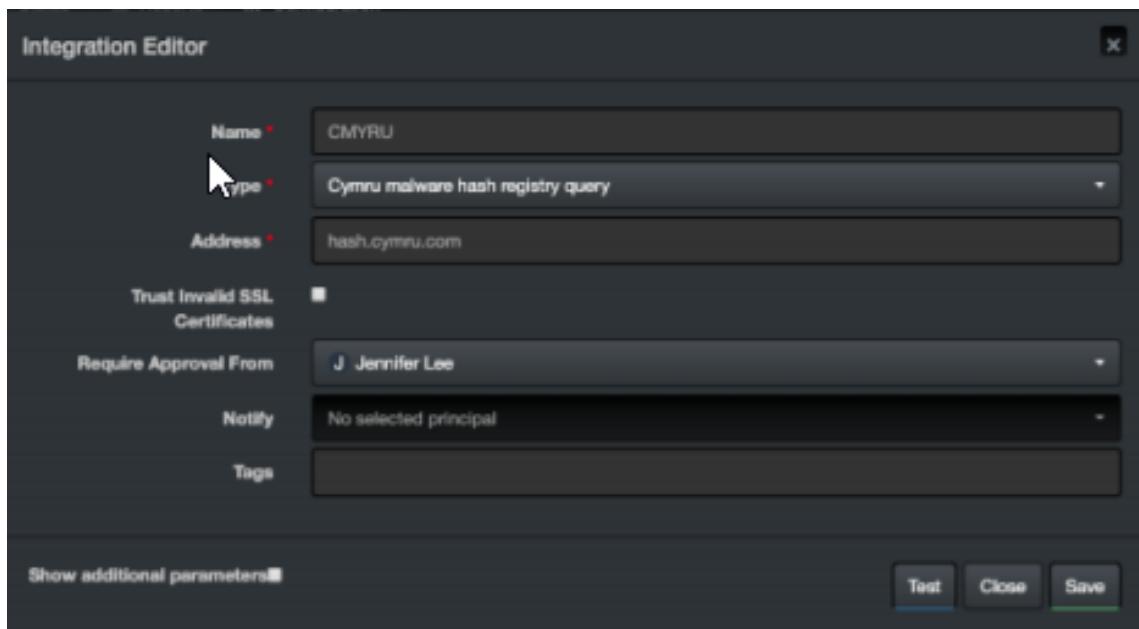
1. Make sure SOAR has access to CYMRU Malware Hash Registry Query integration's API as it connects to it through HTTPS.

### Configuring SOAR

1. To create the integration, navigate to **Configuration > Integrations**.
2. Specify the following parameter values in the **Integrations Editor**:

Parameter	Value
Name	Display name of the integration
Type	CYMRU malware hash registry query
Address	Address of the integration (in the following format http[s]://malware.cymru.hash.com)

Parameter	Value
Trust Invalid SSL Certificates	Select this if Engine's certificate is self-signed or is not recognized by browsers.
Require Approval From	Select users from the list who can provide approval before executing actions on this integration
Notify	Select users from the list to notify when SOAR performs an action on this integration.



3. Click **Test** to test the integration.
4. Click **Save** to complete the integration.

## Integration Guide for Cymru Malware Hash Registry

### Integration Overview

CYMRU MHR is a malware validation tool that searches against 30+ antivirus databases and malware databases to serve as a force multiplier for malware detection and validation. Researchers and analysts can submit their malware hashes via the MHR portal to get near-real-

time results that tell them the percentage of malware databases containing signature matches. Developers and networks security teams can integrate MHR into existing workflows to augment malware detection.

## Integration Capabilities

ArcSight SOAR has the following integration capabilities with Team Cymru Malware Hash Registry V2:

- Single Lookup Hash Query
- Bulk Lookup Hash Query

## Prerequisites

You must have access to HTTPS as the ArcSight SOAR connects to CYMRU MHR API through this service.

## Configuration

### Configuring Team Cymru Malware Hash Registry V2

Authentication: API requires Basic Authentication as username and password.

1. Create an account in Cymru MHR platform. Create Account.
2. The mail received to your registered mail address contains login credentials to MHR account.

Basic Authentication Parameters:

Parameter Name	Data type	Description	Required (Yes/No)
UserName	String	Username of the CYMRU account	Yes

Additional Configuration:

Configuration Parameter	Description
proxy.id	Proxy device to be used while communicating with the remote system's API.
Cache.reusing.duration	Default cache-reuse parameter

## Configuring SOAR

1. Click Configuration > Credentials > Create Credentials.

2. Specify the following parameters values in the Credential Editor form.

Type	Name	Username	Password	Private Key
Internal credential	Display name of credential set (for example, Cymru Malware Hash Registry v2 Credentials).	Username of the CYMRU account	Password of the CYMRU account	N/A

3. Click Configuration > Integrations > Upload plugin.
4. Select your integration plugin zip file and click on Save.
5. Select the integration that you have added to the Integrations menu.
6. Click Save to complete the integration.
7. Click Test, an Integration Successful message is displayed if the credential and address are valid.

## Integration Capabilities:

### 1. Single Lookup Hash Query

Enrichment capability to lookup for one hash at a time, by providing the hash value.

#### Request headers:

Header	Value	Required
Authorization	Basic {Credentials}	Yes
Content-type	application/json	No

#### Input Parameters:

Parameter	Description	Type	Scope	Required (Yes/No)
			Restricted (Yes/No)	
Hash Value	Provide hash value which supports md5, sha1, sha256	HASH	Yes	Yes

#### Output:

#### Case Scope:

Action	Type	Category/ Value
Create Scope Item	Scope Item	MD5 Hash Algorithm
Create Scope Item	Scope Item	SHA1 Hash Algorithm
Create Scope Item	Scope Item	Scope Item SHA256 Hash Algorithm
Action	Type	Category/ Value
Add Scope Item Property	Scope Item Property	Cymru Antivirus Detection Rate

Limitation: N/A

Human Readable output:

Key	Value
MD5	13433c643ae47750d4ba2a3793874f7a
SHA1	36127f11432f4e6cc0df0080da271a1b6060d553
SHA256	N/A
Antivirus Detection Rate	53
Last Run Date	2022-01-01T11:53:02Z
Error	N/A

Total 6 items / page

## 2. Bulk Lookup Hash Query

Enrichment capability for multiple hashes in a single request by submitting hashes

Request headers:

Header	Value	Required
Authorization	Basic {Credentials}	Yes
Content-type	text/plain; charset=utf-8	No

Input Parameters:

Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
Hash Values	Provide a list of multiple hash values which supports md5, sha1, sha256	HASH	Yes	Yes

## API Method Reference

[https://hash.cymru.com/docs\\_](https://hash.cymru.com/docs_)

Output:

Case Scope:

Action	Type	Category/ Value
Create Scope Item	Scope Item	MD5 Hash Algorithm
Create Scope Item	Scope Item	Scope Item SHA1 Hash Algorithm
Create Scope Item	Scope Item	Scope Item SHA1 Hash Algorithm

Action	Type	Category/Value
Add Scope Item Property	Scope Item Property	Cymru Antivirus Detection Rate

Limitation: N/A

Human Readable output:

a few seconds ago - S sacumen executed Bulk Lookup Hash Query enrichment on TEAM_CYMRU_MALWARE_HASH_REGISTRY_V2_FINAL					
Parameters Details		Search			
Md5	Sha1	Sha256	Antivirus Detection Rate	Last Run Date	Error
8ec544ff2f660913de87aed cb4b0b1df	a6a1a5871a680a244f24bb8d 7961ff5ae8b334131	1b3e94bb5fccd9ef534e895 ba94aa5aa6ac933ab9010 1a133f195256dbe1d13	31	2023-04-29T07:40:35Z	N/A
c0202cf6aaeb8437c638533 d14563d35	5767653494d05b3f3f8f166 2a63335d09ae6489	8d3f66b16f0710f858d8c1d2 c699260e643161a5510abb 0e7ba567bd72c965b	28	2018-08-19T09:16:10Z	N/A
N/A	N/A	a105f75e51dbbb19ecc1b 0cebdb5e624c8ea17767a6 aafb962a23079b86d32	0	N/A	N/A
8ec544ff2f660913de87aed cb4b0b1df	a6a1a5871a680a244f24bb8d 7961ff5ae8b334131	1b3e94bb5fccd9ef534e895 ba94aa5aa6ac933ab9010 1a133f195256dbe1d13	31	2023-04-29T07:40:35Z	N/A
N/A	N/A	17334006417f01c87ee8731 d4f14cce06ad7ac20e34781 a99bf542e52cce6275	0	N/A	N/A

# CyberRes Galaxy Threat Accelerator

## Integration Overview

CyberRes Galaxy Threat Accelerator Program (GTAP) Plus is a Threat Intelligence feed, available as a subscription service from Micro Focus CyberRes. Please talk to your Sales Representative to request a 60-day evaluation license or purchase an annual subscription. The license key provided will be the MISP API key that will be used in the CyberRes Galaxy Threat Accelerator (GTAP) Plus integration.

## Integration Capabilities

- Domain Reputation
- File Reputation
- IP Reputation
- URL Reputation

## Prerequisites

ArcSight SOAR connects to “<https://threatfeed.cyberres.com>” APIs through HTTPS. Access to this service is required.

## Configuring CyberRes Galaxy Threat Accelerator

You need to get the API key from CyberRes.

## Configuring SOAR

1. Click **Configuration > Integration > Upload Plugin** and upload the plugin zip file.
2. Edit the configuration to modify the name in the Configuration Form.
3. Click **Configuration > Credentials** and edit the credential .

Type	Internal credential
Name	Display name of credential set (i.e CyberRes Galaxy Threat Accelerator Credentials)
Username	Empty

Type	Internal credential
Password	Empty
Private Key	API key

4. Click **Configuration > Scope Item Property** and Create 2 new scope item property definitions with the following properties:

Property Visible Name	Data Type
CyberRes Galaxy Domain Reputation	TEXT
CyberRes Galaxy File Reputation	TEXT
CyberRes Galaxy IP Reputation	TEXT
CyberRes Galaxy URL Reputation	TEXT

## Capabilities

### 1. Domain Reputation

Enrichment capability for retrieving details of domain reputation.

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
Integration	Name of the third party integration	Integration	N/A	Yes
Domain	Domain to be queried from CyberRes Galaxy Threat Accelerator	Host	Yes	Yes
Do not use cache	SOAR does not use cached results if this box is checked.	Boolean	N/A	No

#### Output:

Case Scope

Action	Type	Category/value
Set	Scope Item Property	CyberRes Galaxy Domain Reputation

Human Readable Output

### 2. File Reputation

Enrichment capability for retrieving details of file hash and reputation.

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
<b>Integration</b>	Name of the third party integration	Integration	N/A	Yes
<b>Hash</b>	Hash to be queried from CyberRes Galaxy Threat Accelerator	Host	Yes	Yes
<b>Do not use cache</b>	SOAR does not use cached results if this box is checked.	Boolean	N/A	No

**Output:**

Case Scope:

Action	Type	Category/value
Set	Scope Item Property	CyberRes Galaxy File Reputation

Human Readable Output

**3. IP Reputation**

Enrichment capability for retrieving IP Address details and reputation.

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
<b>Integration</b>	Name of the third party integration	Integration	N/A	Yes
<b>IP Address</b>	IP Address to be queried from CyberRes Galaxy Threat Accelerator	Network Address	Yes	Yes
<b>Do not use cache</b>	SOAR does not use cached results if this box is checked.	Boolean	N/A	No

**Output:**

Case Scope

Action	Type	Category/value
Set	Scope Item Property	CyberRes Galaxy IP Reputation

Human Readable Output

**4. URL Reputation**

Enrichment capability for retrieving URL details and reputation.

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
<b>Integration</b>	Name of the third party integration	Integration	N/A	Yes
<b>URL</b>	URL to be queried from CyberRes Galaxy Threat Accelerator	URL	Yes	Yes

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
Do not use cache	SOAR does not use cached results if this box is checked.	Boolean	N/A	No

**Output:**

Case Scope

Action	Type	Category/value
Set	Scope Item Property	CyberRes Galaxy URL Reputation

Human Readable Output

# Integration Guide for CyThreat Threat Intelligence

## Integration Overview

**CyThreat** provides cyber threat intelligence data. These data feeds are enriched with subject and event-based reports as compiled by STM analysts.

CyThreat collects data from various open and commercial sources (deep/dark web, social media, blogs, forums, etc.) automatically. This allows the detection of the activities of the threat actors, proactive prevention of cyber-attacks before they occur and also allows applications to take preventive measures.

SOAR can seek benefit from CyThreat intelligence from both Integration and as Alert Source.

## Integration Capabilities

ArcSight SOAR has the following integration capabilities with CyThreat Threat Intelligence:

- Domain Query
- Hash Query
- IP Query

## Alert Source Capability

ArcSight SOAR has the following alert source capability with CyThreat Threat Intelligence:

- Consume Threat Intelligence feeds from CyThreat(default)

## Prerequisites

- You must have access to HTTPS as the ArcSight SOAR connects to CyThreat API through this service.
- API token and password to connect to CyThreat Threat Intelligence API.

# Configuration

## Configuring SOAR

1. Click **Configuration > Credential > Create Credential**.
2. Specify the following parameters in the **Credential Editor** form:

Type	Name	Username	Password	Private Key
<b>Internal credential</b>	Display name of credential set (for example, CyThreat Credentials).	Empty	API password that you have received from CyThreat service.	API token that you have received from the CyThreat service.

3. Click **Configuration > Integrations > Create Integration**.
4. Specify the following parameter values in the **Configuration Form**.

Parameter	Value		
<b>Name</b>	Display name of the CyThreat integration.		
<b>Type</b>	CyThreat		
<b>Address</b>	Address of the integration (the format should be https://cti.stm.com.tr).		
<b>Configuration</b>	Specify the following configuration parameters:  <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="padding: 2px;">proxy.id</td> <td style="padding: 2px;">ID of the Proxy integration if you access <a href="https://cti.stm.com.tr">https://cti.stm.com.tr</a> through a web proxy device. For example: proxy.id = 12345 .</td> </tr> </table>	proxy.id	ID of the Proxy integration if you access <a href="https://cti.stm.com.tr">https://cti.stm.com.tr</a> through a web proxy device. For example: proxy.id = 12345 .
proxy.id	ID of the Proxy integration if you access <a href="https://cti.stm.com.tr">https://cti.stm.com.tr</a> through a web proxy device. For example: proxy.id = 12345 .		
<b>Credential</b>	Credential that has been defined for this integration under the <b>Credentials</b> menu.		
<b>Trust Invalid SSL Certificates</b>	Select this if web server's certificate is self-signed or is not recognized by browsers. The SSL certificate of CyThreat service is going to known by SOAR, so you do not need to check this box.		
<b>Require Approval From</b>	Select user(s) from list to ask the approval before executing actions on this integration.		
<b>Notify</b>	Select user(s) from the list to notify when SOAR performs an action on this integration.		

5. Click **Save** to save the integration definition.
6. Navigate to **Configuration>Customization Library** and edit **CyThreat Advanced Action Script Default Script Template**.
7. Select the integration that you have added to **Integrations** menu.
8. Click **Save** to complete the integration.



**Note:** Steps 7-9 are required only for Advanced Action Script Default Templates.

9. Navigate to **Configuration > Integrations > CyThreat integration**.
10. Click **Test**. **Integration Successful** message is displayed if the credential and address are valid.

## Configuring CyThreat as an Alert Source

1. Navigate to **Configuration > Alert Source > Create Alert Source Configuration**.
2. Select **CyThreat Threat Intelligence** and specify the following parameters in the **Alert Source Configuration Editor**:

Parameter	Value
<b>Name</b>	Display name of the CyThreat alert source.
<b>Type</b>	CyThreat Threat Intelligence
<b>Address</b>	<a href="https://cti.stm.com.tr/api/">https://cti.stm.com.tr/api/</a>
<b>Alert Severities</b>	Arrangement table of severity mapping.
<b>enable.ip.risk.source</b>	Uncomment and change to true to consume IP Source.
<b>enable.domain.risk.source</b>	Uncomment and change to true to consume Domain Source.
<b>enable.hash.risk.source</b>	Uncomment and change to true to consume Hash Source.
<b>enable.usom.blacklist.source</b>	Uncomment and change to true to consume Usom Blacklist Source.
<b>ip.min.risk</b>	SOAR is not going to create case if risk level of the incoming alarm is below of the value.
<b>domain.min.risk</b>	SOAR is not going to create case if risk level of the incoming alarm is below of the value.
<b>hash.min.risk</b>	SOAR is not going to create case if risk level of the incoming alarm is below of the value.
<b>proxy.id</b>	ID of the Proxy integration if you access <a href="https://cti.stm.com.tr">https://cti.stm.com.tr</a> through a web proxy device. For Example: proxy.id = 12345.
<b>days.to.look.back.at.initial.sync</b>	How far (in days) into the past SOAR will look for remote incidents at the initial sync task.
<b>Credential</b>	Name of the credential set created on step 2 Configuring SOAR part (For example, CyThreat Credentials).
<b>Visible Alert Fields</b>	Field names from the alert if you want to show them on case.
<b>Trust Invalid SSL Certificates</b>	The SSL certificate of CyThreat service is going to be known by SOAR, so you do not need to check this box.

3. Click **Test**. The **Alert Source tested successfully** message is displayed if your credentials are valid.
4. Click **Save**.

## Integration Capabilities

### 1. Domain Query

Enrichment capability for retrieving domain information.

The following table presents the **Domain Query** action capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Integration</b>	Name of the third party integration.	Integration	N/A	Yes
<b>Domain</b>	Domain that you want to query.	Host	Yes	No

#### **Output:**

Case Scope: N/A

Human Readable Output: Yes

### 2. Hash Query

Enrichment capability for retrieving hash information.

The following table presents the **Hash Query** action capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Integration</b>	Name of the third party integration.	Integration	N/A	Yes
<b>Hash</b>	Hash value that you want to query.	Hash	Yes	Yes

#### **Output:**

Case Scope: N/A

Human Readable Output: Yes

### 3. IP Query

Enrichment capability for retrieving domain information.

The following table presents the **IP Query** action capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Integration</b>	Name of the third party integration.	Integration	N/A	Yes
<b>IP</b>	Ip that you want to query.	Host	Network Address	Yes

**Output:**

Case Scope: N/A

Human Readable Output: Yes

# Integration Guide for DomainTools

## Integration Overview

**DomainTools** is a leading provider of Whois and other DNS profile data for threat intelligence enrichment. It is a part of Datacenter Group (DCL and SA). DomainTools data helps security analysts investigate malicious activity on their networks.

## Integration Capabilities

- Get Domain Profile
- Get Domain Reputation
- Get Domain Risk
- Domain Hosting History
- Recent Domain
- Reverse IP Lookup
- Reverse IP Whois
- Whois Lookup
- Iris Investigate

# Configuration

## Configuring DomainTools

- You must have access to HTTPS as the ArcSight SOAR connects to DomainTools API through this service.

## Configuring SOAR

1. Click **Configuration > Credential > Create Credential**.
2. Specify the following parameter values in the **Credential Editor**:

Type	Name	Username	Password	Private Key
Internal Credential	Display name of credential set (for example, DomainTools Credentials)	Valid API username	Valid API Key to authenticate the DomainTools APIs	N/A

3. Click **Configuration > Integrations > Create Integration**.
4. Specify the following parameter values in the **Configuration Form**:

Parameter	Value		
Name	Display name of the integration		
Type	DomainTools		
Address	Address of the integration ( <a href="https://api.domaintools.com">https://api.domaintools.com</a> )		
Configuration	<p>Specify the following configuration parameter values:</p> <table border="1"> <tr> <td>proxy.id</td> <td>ID of the Proxy integration if you access DomainTools through a web proxy device. For example, proxy.id = 12345</td> </tr> </table>	proxy.id	ID of the Proxy integration if you access DomainTools through a web proxy device. For example, proxy.id = 12345
proxy.id	ID of the Proxy integration if you access DomainTools through a web proxy device. For example, proxy.id = 12345		
Credential	Credential that has been defined for this integration under the Credential menu		
Trust Invalid SSL Certificates	Select this option if the web server's certificate is self-signed or if it is not recognized by browsers		
Require Approval From	Select user(s) from list who can provide approval before executing actions on this integration		
Notify	Select user(s) from the list who can provide approval when SOAR performs an action on this integration		

5. Click **Save** to save the integration definition.
6. Navigate to **Configuration > Customization Library** and edit **DomainTools Advanced Action Script Default Template**.
7. Select the integration that you have added to **Integrations** menu.
8. Click **Save** to complete the integration
9. Click **Test**, an **Integration Successful** message is displayed if the credential and address are valid.

## Capabilities

### 1. Get Domain Profile

Enrichment capability for retrieving the basic domain name registration details and a preview of additional data available from DomainTools membership and report products.

Input Parameter	Description	Type	Scope Restricted(Yes/No)	Required (Yes/No)
<b>Integration</b>	Name of the third-party integration	Integration	N/A	Yes
<b>Domain</b>	Domain name to be queried	HOST UNKNOWN KEYWORD	Yes	Yes

#### Output:

Case Scope

N/A

Human Readable Output:

Key	Value
Registrant Name	REDACTED FOR PRIVACY
Registrant Domains	36356545
Registrant Product Url	<a href="https://reversewhois.domaintools.com/?all[]&amp;REDACTED+FOR+PRIVACY&amp;none[]">https://reversewhois.domaintools.com/?all[]&amp;REDACTED+FOR+PRIVACY&amp;none[]</a>
Server IP Address	141.193.213.20
Server Other Domains	41968
Server Product Url	<a href="https://reversesip.domaintools.com/search/?q=domaintools.com">https://reversesip.domaintools.com/search/?q=domaintools.com</a>
Registration Created	1998-08-02
Registration Expires	2027-08-01
Registration Updated	2020-01-09
Registration Registrar	eNom, LLC
Registration Statuses	[ "clientTransferProhibited" ]
Name Servers	[ "Server: DNS1.P04.NSONE.NET, Product URL: <a href="https://reversens.domaintools.com/search/?q=DNS1.P04.NSONE.NET">https://reversens.domaintools.com/search/?q=DNS1.P04.NSONE.NET</a> ", "Server: DNS2.P04.NSONE.NET, Product URL: <a href="https://reversens.domaintools.com/search/?q=DNS2.P04.NSONE.NET">https://reversens.domaintools.com/search/?q=DNS2.P04.NSONE.NET</a> ", "Server: DNS3.P04.NSONE.NET, Product URL: <a href="https://reversens.domaintools.com/search/?q=DNS3.P04.NSONE.NET">https://reversens.domaintools.com/search/?q=DNS3.P04.NSONE.NET</a> ", "Server: DNS4.P04.NSONE.NET, Product URL: <a href="https://reversens.domaintools.com/search/?q=DNS4.P04.NSONE.NET">https://reversens.domaintools.com/search/?q=DNS4.P04.NSONE.NET</a> " ]
History	[ "Registrar - Earliest_Event: 2002-04-12, Events: 4, Product_URL: <a href="https://research.domaintools.com/research/hosting-history?q=domaintools.com">https://research.domaintools.com/research/hosting-history?q=domaintools.com</a> ", "IP Address - Events: 91, Years: 11, Product_URL: <a href="https://research.domaintools.com/research/hosting-history?q=domaintools.com">https://research.domaintools.com/research/hosting-history?q=domaintools.com</a> ", "Name Server - Events: 7, Years: 18, Product_URL: <a href="https://research.domaintools.com/research/hosting-history?q=domaintools.com">https://research.domaintools.com/research/hosting-history?q=domaintools.com</a> ", "Whois - Records: 6139, Earliest_Event: 2001-10-26, Product_URL: <a href="https://research.domaintools.com/research/whois-history/search/?q=domaintools.com">https://research.domaintools.com/research/whois-history/search/?q=domaintools.com</a> " ]
SEO Score	N/A
SEO Product Url	<a href="https://research.domaintools.com/seo-browser?domain=domaintools.com">https://research.domaintools.com/seo-browser?domain=domaintools.com</a>
Website Response Code	N/A
Website Title	N/A
Website Server	N/A
Website Meta	N/A
Website Product Url	<a href="https://whois.domaintools.com/domaintools.com">https://whois.domaintools.com/domaintools.com</a>

## 2. Get Domain Reputation

Enrichment capability for retrieving domain details and reputation.

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
Integration	Name of the third-party integration	Integration	N/A	Yes
Domain	Domain name to be queried for which the risk score is desired	HOST, UNKNOWN, KEYWORD	Yes	Yes

### Output:

Case Scope:

Action	Type	Category/Value
Set	Scope item Property	Risk Score

Human Readable Output:

Key	Value
Domain	domaintools.com
Risk Score	0
Reasons	[ "zerolist" ]

### 3. Get Domain Risk

Enrichment capability for deeper investigation of individual domains and to retrieve the risk score.

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
Integration	Name of the third-party integration	Integration	N/A	Yes
Domain	Domain name to be queried for which the risk score is desired	HOST, UNKNOWN, KEYWORD	Yes	Yes

**Output:**

Case Scope

Action	Type	Category/Value
Set	Scope item Property	Risk Score

Human Readable Output:

Key	Value
Risk (overall)	0
Risk (zerolist)	0

### 4. Domain Hosting History

Enrichment capability for retrieving a list of changes that have occurred in a Domain Name's registrar, IP address, and name servers. IP and name server's events include the value before and after the change and indicate the type of action that triggered the event.

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
<b>Integration</b>	Name of the third-party integration	Integration	N/A	Yes
<b>Domain</b>	Domain name to be queried to get hosting history	HOST, UNKNOWN, KEYWORD	Yes	Yes

**Output:**

Case Scope

N/A

Human Readable Output:

Date	Type	Action	Details
2002-10-03	Registrar	N/A	Registrar: Alldomains, Registrar Tag: Alldomains
2006-04-10	Registrar	N/A	Registrar: MarkMonitor, Registrar Tag: eMarkMonitor
2004-04-24	IP	New	Previous: N/A, New: 216.239.57.99
2004-05-08	IP	Change	Previous: 216.239.57.99, New: 66.102.7.99
2004-05-15	IP	Change	Previous: 66.102.7.99, New: 216.239.57.99
2004-05-22	IP	Change	Previous: 216.239.57.99, New: 216.239.51.99
2004-05-29	IP	Change	Previous: 216.239.51.99, New: 216.239.53.99
2004-06-19	IP	Change	Previous: 216.239.53.99, New: 216.239.57.99
2004-07-17	IP	Change	Previous: 216.239.57.99, New: 66.102.7.99
2004-07-24	IP	Change	Previous: 66.102.7.99, New: 216.239.57.99
2004-08-29	IP	Change	Previous: 216.239.57.99, New: 66.102.7.99

**5. Recent Domain**

Enrichment capability to search for domain names that match your specific search string. Unlike Domain suggestions, Domain Search finds currently registered or previously registered domain names that are either currently registered or have been registered in the past under one of the major gTLDs (.com, .net, .org, .info, .us, or .biz) many countries code TLDs, or the new gTLDs.

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
Integration	Name of the third-party integration	Integration	N/A	Yes
Query	Query string for the search	Host Unknown Keyword	Yes	Yes

**Output:**

Case Scope

N/A

Human Readable Output:

Sid	Tids	Hashad Tids	Tids Count	Has Deleted	Has Active
domaintools	[ "app", "asia", "ar", "au", "be", "ca", "cc", "cf", "cn", "cloud", "club", "cm", "cn", "co", "co.il", "co.in", "co.nz", "co.uk", "co.za", "com", "com.au", "com.cn", "com.pl", "com.tr", "cz", "de", "dev", "directory", "dk", "domains", "email", "es", "eu", "fail", "fr", "ga", "gg", "gr", "horse", "hu", "in", "info", "io", "is", "it", "jp", "link", "ma", "me", "ml", "mobi", "monster", "net", "met.cm", "minja", "nl", "no", "nu", "one", "online", "org", "pro", "pw", "report", "ru", "se", "services", "site", "solutions", "support", "sx", "tech", "technology", "tel", "top", "tv", "tw", "uk", "us", "website", "work", "xxx", "xyz" ]	[ "app", "asia", "ar", "au", "be", "best", "biz", "bz", "ca", "cc", "cf", "ch", "chat", "cf", "click", "cloud", "club", "cn", "co", "co.ba", "co.il", "co.in", "co.kr", "co.ni", "co.nz", "co.uk", "co.za", "com", "com.ar", "com.au", "com.bd", "com.bn", "com.br", "com.cn", "com.dn", "com.jf", "com.jo", "com.kw", "com.pf", "com.ru", "com.tr", "com.ua", "com.vc", "cz", "de", "dev", "directory", "dk", "domains", "email", "es", "eu", "fail", "fm", "fr", "ga", "gg", "gr", "horse", "host", "hu", "id", "in", "info", "io", "is", "it", "jp", "kew", "kr", "la", "link", "lt", "lu", "ma", "me", "ml", "mobi", "monster", "ms", "mx", "name", "net", "net.au", "met.cm", "minja", "nl", "no", "nu", "one", "online", "ooo", "org", "org.uk", "ovn", "page", "pk", "pf", "pro", "pt", "pub", "pv", "report", "ro", "ru", "science", "se", "services", "site", "sk", "solutions", "space", "store", "su", "support", "sx", "tech", "technology", "tel", "tips", "tk", "tools", "top", "tv", "tw", "uk", "us", "wdc", "website", "work", "world", "ws", "xn-kpwn3d", "xn--mgbayh7gpa", "xxx", "xyz" ]	84	1	1
domain-tools	[ "ch", "co", "co.uk", "com", "de", "in.it", "it", "me", "net", "org", "nu", "site", "tk", "xyz" ]	[ "app", "asia", "biz", "ca", "ch", "cn", "co", "co.uk", "com", "com.au", "com.br", "com.cn", "de", "eu", "in", "in.it", "info", "id", "it", "me", "ml", "net", "net.au", "org", "pw", "ru", "site", "sk", "tk", "uk", "us", "xyz" ]	14	1	1
freedomaintools	[ "co", "co.il", "com", "in", "net", "online", "tk", "xyz" ]	[ "co", "co.il", "com", "eu", "in", "info", "net", "online", "org", "tk", "xyz" ]	8	1	1

**6. Reverse IP Lookup**

Enrichment capability to retrieve a list of domain names that share the same Internet host (I.e., the same IP address).



The users can request an IP address or a domain name. It is recommended to provide a domain name, and if a domain name is provided the system would return a list of all domains that share the same IP address.

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
<b>Integration</b>	Name of the third-party integration	Integration	N/A	Yes
<b>Domain</b>	Domain name to be queried for which the risk score is desired	HOST UNKNOWN KEYWORD	Yes	Yes

### Output:

Case Scope

N/A

Human Readable Output:

Ip Address	Domain Count	Domain Names
141.193.213.20	41968	[ "WMHENDERSON.COM", "VETSUCCESSINC.COM", "FIRST15WORSHIP.ORG", "DFDF.VC", "CUBBYCARE.COM.AU", "PRUEBADEVIH.COM.MX", "LIFEBALANCECOACHINH.COM", "GALLORODENTALGROUP.COM", "SYNERGI.SO", "RESET101COACHING.COM", "SETTYDENTALGROUP.COM", "HAVENEARLYLEARNING.COM.AU", "COLYANDROPUBLICAFFAIRS.COM", "TREEOFLIFESEEDS.COM", "DISAPPEARINGINC.COM", "PET-BLISS.IE", "BVCAREERS.DEV", "ANGELAWSTILLWELL.COM", "SNOWINCLUDED.COM", "PATHWAYSMEDICALCARE.CA", "ROSEBERRYHOUSE.COM.AU", "CARLTONPRODUCTS.COM", "OK.ORG", "BUFFETING.COM", "ETWELLNESS.ORG", "TURBOLUTION.COM", "NEWBERLINGRADING.COM", "THEBUSINESSYOGI.COM", "JAMILAHMED.COM", "GRACEFULWAYCOUNSELING.COM", "WELLANDGOODBAKERY.COM.AU", "RESUME-RESCUE.COM.AU", "PUREMECHANICAL.CA", "ATREALTYPROPERTYSALES.GIPPSLAND.COM.AU", "BOLDMEDIAGROUP.COM.AU", "GENER8.DIGITAL", "JANDJRESTORATION.COM.AU", "TONYCULLINAN.COM.AU", "MOTUSHYDRAULICS.COM", "NEUROSCIENCEGROUP.ORG", "SASMABV.COM", "EFNS.CA", "NSEGG.S.CA", "ARC-AZ.COM", "1-833-DEBT-FREE.COM", "1000MUNI.CO.IL", "100XCOIN.COM", "10100ATA.COM", "1045ROSE.COM", "1072STANNAGE.COM", "1072WESTPEACHTREE.COM", "10DEGREES.CO.UK", "10DEGREES.UK", "10EDISON.COM", "10GYM.COM", "10PASTEISNENHUMVEGANO.COM.BR", "10THPLANETEL PASO.COM", "10XTRAVEL.COM", "110PARKAVE.COM", "11305MICHIGAN.COM", "11601WILSHIRE.COM", "1166FCU.ORG", ]

## 7. Reverse IP Whois

Enrichment capability to retrieve a list of IP ranges that are owned by an organization.

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
Integration	Name of the third-party integration	Integration	N/A	Yes
Query	Name of the organization to be queried	String	Yes	Yes

**Output:**

Case Scope

N/A

Human Readable Output:

Range	Record Ip	Record Date	Organization	Country	Server
199.30.228.0/22	199.30.228.13	2022-11-16	DomainTools, LLC	US	whois.arin.net
64.246.187.40/30	64.246.187.40	2022-10-13	DomainTools, LLC	US	whois.arin.net
64.246.165.48/30	64.246.165.50	2022-11-10	DomainTools, LLC	US	whois.arin.net
66.249.16.0/23	66.249.16.0	2022-10-05	Name Intelligence, Inc.	US	whois.arin.net
216.145.14.140/30	216.145.14.140	2022-10-08	DomainTools, LLC	US	whois.arin.net
64.246.165.8/30	64.246.165.8	2022-10-15	DomainTools, LLC	US	whois.arin.net
67.135.38.72/29	67.135.38.72	2022-10-12	DomainTools, LLC	US	whois.arin.net
63.150.103.144/29	63.150.103.147	2022-10-26	DomainTools, LLC	US	whois.arin.net

**8. Whois Lookup**

Enrichment capability to retrieve the ownership record for a domain name or IP address with basic registration details.

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
Integration	Name of the third-party integration	Integration	N/A	Yes
Domain	Domain name to be queried.	HOST UNKNOWN KEYWORD	Yes	Yes

**Output:**

Case Scope

N/A

Human Readable Output:

Key	Value
Registrant	REDACTED FOR PRIVACY
Registration Created	1998-08-02
Registration Expires	2027-08-01
Registration Updated	2020-01-09
Registration Registrar	eNom, LLC
Registration Statuses	[ "clientTransferProhibited" ]
Name Servers	[ "DNS1.P04.NSONE.NET", "DNS2.P04.NSONE.NET", "DNS3.P04.NSONE.NET", "DNS4.P04.NSONE.NET" ]
Whois Date	2022-11-16
Whois Record	Domain Name: domaintools.com Registry Domain ID: 1697312_DOMAIN_COM-VRSN Registrar WHOIS Server: WHOIS.ENOM.COM Registrar URL: WWW.ENOM.COM Updated Date: 2020-01-09T23:06:29.00Z Creation Date: 1998-08-02T04:00:00.00Z Registrar Registration Expiration Date: 2027-08-01T04:00:00.00Z Registrar: ENOM, INC. Registrar IANA ID: 48 Domain Status: clientTransferProhibited https://www.icann.org/eppclientTransferProhibited Registrant Name: REDACTED FOR PRIVACY Registrant Organization: REDACTED FOR PRIVACY Registrant Street: REDACTED FOR PRIVACY Registrant Street: Registrant City: REDACTED FOR PRIVACY Registrant State/Province: WA Registrant Postal Code: REDACTED FOR PRIVACY Registrant Country: US Registrant Phone: REDACTED FOR PRIVACY Registrant Phone Ext: Registrant Fax: REDACTED FOR PRIVACY Registrant Email: https://tieredaccess.com/contact/e4e03487-86e0-4e34-bc3d-723c615024e9 Admin Name: REDACTED FOR PRIVACY Admin Organization: REDACTED FOR PRIVACY Admin Street: REDACTED FOR PRIVACY Admin Street: Admin City: REDACTED FOR PRIVACY Admin State/Province: REDACTED FOR PRIVACY Admin Postal Code: REDACTED FOR PRIVACY Admin Country: REDACTED FOR PRIVACY Admin Phone: REDACTED FOR PRIVACY Admin Phone Ext: Admin Fax: REDACTED FOR PRIVACY Admin Email: REDACTED FOR PRIVACY Tech Name: REDACTED FOR PRIVACY Tech Organization: REDACTED FOR PRIVACY Tech Street: REDACTED FOR PRIVACY Tech Street: Tech City: REDACTED FOR PRIVACY Tech State/Province: REDACTED FOR PRIVACY Tech Postal Code: REDACTED FOR PRIVACY Tech Country: REDACTED FOR PRIVACY Tech Phone: REDACTED FOR PRIVACY Tech Phone Ext: Tech Fax: REDACTED FOR PRIVACY Tech Email: REDACTED FOR PRIVACY Name Server: DNS1.P04.NSONE.NET, Name Server: DNS2.P04.NSONE.NET, Name Server: DNS3.P04.NSONE.NET, Name Server: DNS4.P04.NSONE.NET, DNSSEC: unsigned Registrar Abuse Contact Email: ABUSE@ENOM.COM Registrar Abuse Contact Phone: +1.4259744689 URL of the ICANN WHOIS Data Problem Reporting System: HTTP://WDPRS.INTERNIC.NET/
Record Source	domaintools.com

## 9. Iris Investigate

Enrichment capability is ideally suited for investigating and orchestrating use cases at a human scale.

These are typically triggered on-demand by an analyst seeking additional context on a single indicator, with the best result available for investigations.

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
Integration	Name of the third-party integration	Integration	N/A	Yes
Domain	Domain name to be queried.	HOST UNKNOWN KEYWORD	Yes	Yes

### Output:

Case Scope

N/A

## Human Readable Output:

Key	Value
Domain	domaintools.com
Domain Risk	[ "zerolist: 0", "OverAll Risk Score: 0" ]
Whois Url	<a href="https://whois.domaintools.com/domaintools.com">https://whois.domaintools.com/domaintools.com</a>
Adsense	N/A
Alexa	3954
Popularity Rank	3763
Active	true
Google Analytics	N/A
Admin Contact	country: REDACTED FOR PRIVACY, org: REDACTED FOR PRIVACY, city: REDACTED FOR PRIVACY, phone: N/A, street: REDACTED FOR PRIVACY, name: REDACTED FOR PRIVACY, state: REDACTED FOR PRIVACY, postal: REDACTED FOR PRIVACY, fax: N/A, email: N/A
Billing Contact	country: N/A, org: N/A, city: N/A, phone: N/A, street: N/A, name: N/A, state: N/A, postal: N/A, fax: N/A, email: N/A
Registrant Contact	country: us, org: REDACTED FOR PRIVACY, city: REDACTED FOR PRIVACY, phone: N/A, street: REDACTED FOR PRIVACY, name: REDACTED FOR PRIVACY, state: WA, postal: REDACTED FOR PRIVACY, fax: N/A, email: N/A
Technical Contact	country: REDACTED FOR PRIVACY, org: REDACTED FOR PRIVACY, city: REDACTED FOR PRIVACY, phone: N/A, street: REDACTED FOR PRIVACY, name: REDACTED FOR PRIVACY, state: REDACTED FOR PRIVACY, postal: REDACTED FOR PRIVACY, fax: N/A, email: N/A
Create Date	1998-08-02
Expiration Date	2027-08-01
Email Domain	[ "nsone.net", "enom.com" ]
SOA Email	[ "hostmaster@nsone.net" ]
SSL EMAIL	N/A
Additional Whois Email	[ "abuse@enom.com" ]
IP	[ "address: 141.193.213.21, isp: WPEngine Inc., country_code: us, asn: [209242]", "address: 141.193.213.20, isp: WPEngine Inc., country_code: us, asn: [209242]" ]

# Integration Guide for DNS Service

## Integration Overview

DNS Server is used to resolve and translate the IP addresses, host names and queries to various DNS records.

## Integration Capabilities

SOAR has the following integration capabilities with DNS Server.

- DNS Lookup

## Configuration

### Prerequisites

- Make sure SOAR has access to DNS Server through 53/udp port

### Configuring DNS Service

- No specific configuration is needed on DNS Server.

### Configuring SOAR

1. Click **Configuration > Integrations > Create Integrations**.
2. Specify the following parameter values in the **Configuration** form:

Parameter	Value
Name	Display name of DNS Server integration on SOAR.
Type	DNS Service
Address	Address of the integration (in the format: 192.168.2.53)

Parameter	Value
<b>Trust Invalid SSL Certificates</b>	Not applicable
<b>Require Approval From</b>	Select users from the list who can provide approval before executing actions on this integration. As SOAR only executes enrichment on DNS Server, leave it empty
<b>Notify</b>	Select users from the list to notify when SOAR performs an action on this integration. As SOAR only executes enrichment on DNS Server, leave it empty

**Integration Editor**

Name *	Company DNS Server
Type *	DNS Service
Address *	192.168.2.53
Trust Invalid SSL Certificates	<input checked="" type="checkbox"/>
Require Approval From	No selected principal
Notify	No selected principal
Tags	

Show additional parameters

**Test** **Close** **Save**

3. Click **Test**. The following pop up will be displayed if your credential and address are valid.
4. Click **Save** to complete integration.

# Integration Guide for EmailRep

## Integration Overview

**EmailRep** consists of crawlers, scanners and enrichment services that collect data from email addresses, domains, and internet personas.

EmailRep uses hundreds of data points from social media profiles, professional networking sites, dark web credential leaks, data breaches, phishing kits, phishing emails, spam lists, open mail relays, domain age and reputation, and deliverability to predict the risk on an email address.

This integration enables ArcSight SOAR to report and query an email address.

## Integration Capabilities

ArcSight SOAR has the following integration capabilities with EmailRep:

- Email Query
- Report Email

## Prerequisite

- An API key is required for accessing EmailRep.

## Configuring SOAR

1. Click **Configuration > Credential > Create Credential**.
2. Specify the following parameter values in the **Credential Editor** form:

Type	Name	Username	Password	Private Key
Internal credential	Display name of credential set (for example, EmailRep Credentials).			API Key

3. Click **Configuration > Integration > Create Integrations** Specify the following parameter values in the **Configuration** form:

Parameter	Value	
<b>Name</b>	Display name of the integration.	
<b>Type</b>	EmailRep	
<b>Address</b>	Address of the integration ( <a href="https://emailrep.io">https://emailrep.io</a> ).	
<b>Configuration</b>	Specify the following configuration parameters:	
	<b>proxy.id</b>	ID of the Proxy integration if you access EmailRep through a web proxy device. For example, proxy.id = 12345 .
<b>Credential</b>	Credential that has been defined for this integration under the <b>Credentials</b> menu.	
<b>Trust Invalid SSL Certificates</b>	Select this if web server's certificate is self-signed or is not recognized by browsers.	
<b>Require Approval From</b>	Select user(s) from list to ask the approval before executing actions on this integration.	
<b>Notify</b>	Select user(s) from the list to notify when SOAR performs an action on this integration.	

4. Click **Save** to save the integration definition.
5. Navigate to **Configuration>Customization Library** and edit **Emailrep Advanced Action Script Default Template**.
6. Select the integration that you have added to **Integrations** menu.
7. Click **Save** to complete the integration.
8. Click **Test**, an **Integration Successful** message is displayed if the credential and address are valid.

## Capabilities

### 1. Email Query

Enrichment capability for getting reputation of email addresses.

The following table presents the **Email Query** enrichment capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Integration</b>	Name of the third party integration.	Integration	N/A	Yes
<b>Email Address</b>	Email address to be queried.	Email Address	Yes	Yes
<b>Do not Use Cache</b>	SOAR does not use cached results if this box is checked.	Checkbox	N/A	No

**Output:**

**Case Scope:**

Action	Type	Category/ Value
Set	Scope item value	EmailRep Suspicious
Set	Scope item value	EmailRep Reputation

**Human Readable Output:**

Key	Value
Reputation	high
Suspicious	false
Domain Reputation	low
Primary MX Server	i2seng-com01.mail.protection.outlook.com

2. Report Email
3. Action capability for reporting malicious email addresses.
  - Rollback: No
  - Duplicate Control: Yes



**Note:** This capability requires Professional or Enterprise API membership to EmailRep.

The following table presents **Report Email** action capability details:

**Output:**

	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Integration</b>	Name of the third party integration.	Integration	N/A	Yes
<b>Rollback Mode</b>	Time to rollback this action. Default is no-rollback.	N/A	N/A	No
<b>Email Address</b>	Email address to be reported.	Email Address	Yes	Yes
<b>Tag</b>	Report tag.	String	N/A	No
<b>Description</b>	Description/ reason to report.	String	No	Yes

Case Scope: N/A

Human Readable Output: N/A

# Integration Guide for EnCase Endpoint Security

## Integration Overview

EnCase Endpoint Security detects, validates and prioritizes unknown threats, assess the scope and impact of a compromise, and returns devices to a trusted state. With EnCase Endpoint Security, you can:

- Collect, aggregate and baseline all endpoint activity
- Proactively address the gaps in your security framework
- Detect unknown risks or threats even before data exfiltration has begun
- Respond to any events for validation and triage
- Perform manual or automated incident response with forensic-level investigations of endpoints
- Automate the recovery of endpoints to a trusted state through remediation

## Integration Capabilities

ArcSight SOAR has the following integration capabilities with EnCase Endpoint Security:

- List Investigations
- Find Hosts with IOCs
- Standard Agent Timeline (Snapshot)
- Collect Memory
- Create Snapshot
- Find Hosts with Items of Interest
- Get Investigation Job Status
- Get Event Status
- Collect Data - Pre Defined Filter
- Collect Data -Custom Filter
- Isolate
- Reconnect
- Create Event
- Remediate

## Prerequisites

You must have access to HTTPS as the ArcSight SOAR connects to Encase API through this service.

## Configuration

### Configuring EnCase Endpoint Security

- Authentication: Encase REST APIs supports authentication using an Integration Key.
- Integration Key Authentication**
- To authenticate using an Integration Key, a new Integration Account needs to be created in the Account Management page of the web application.
  - The Integration Key can be viewed or regenerated from the Manage Integration Key action.
  - The Base URL for Integration Key APIs is: `http(s)://server:port/integration`. The Integration Key should be passed in a Request Parameter called `Key`.

#### Authentication Parameters

##### Request Headers:

Parameters	Datatype	Description	Required
Key	string	The Encase REST API Key	Yes

Configuration Parameter	Description
proxy.id	Proxy device to be used while communicating with the remote system's API
cache.reusing.duration	Default cache-reuse parameter
investigation.name	Default case name we want to create in Encase. For Example: SOAR

#### Additional Configuration:



In the Address configuration, replace the server-port with your server-port.  
 For example: `https://<server_name>:<server_port>`  
 where,  
 <server\_name>: Name of the server  
 <server\_port>: Port number of the server

## Configuring SOAR

1. Click Configuration > Credentials > Create Credentials.
2. Specify the following parameters values in the Credential Editor form.

Type	Name	Username	Password	Private Key
Internal credential	Display name of credential set (for example, Encase v1 Credentials).	N/A	N/A	The Encase REST API v1 Key

3. Click Configuration > Integrations > Upload plugin
4. Select your integration plugin zip file and click Save.
5. Select the integration that you have added to Integrations menu.
6. Click Save to complete the integration.
7. Click Test. an Integration Successful message is displayed if the credential and address are valid.

## Integration Capabilities:

### 1. List Investigations:

Enrichment capability to get the list of Investigations.

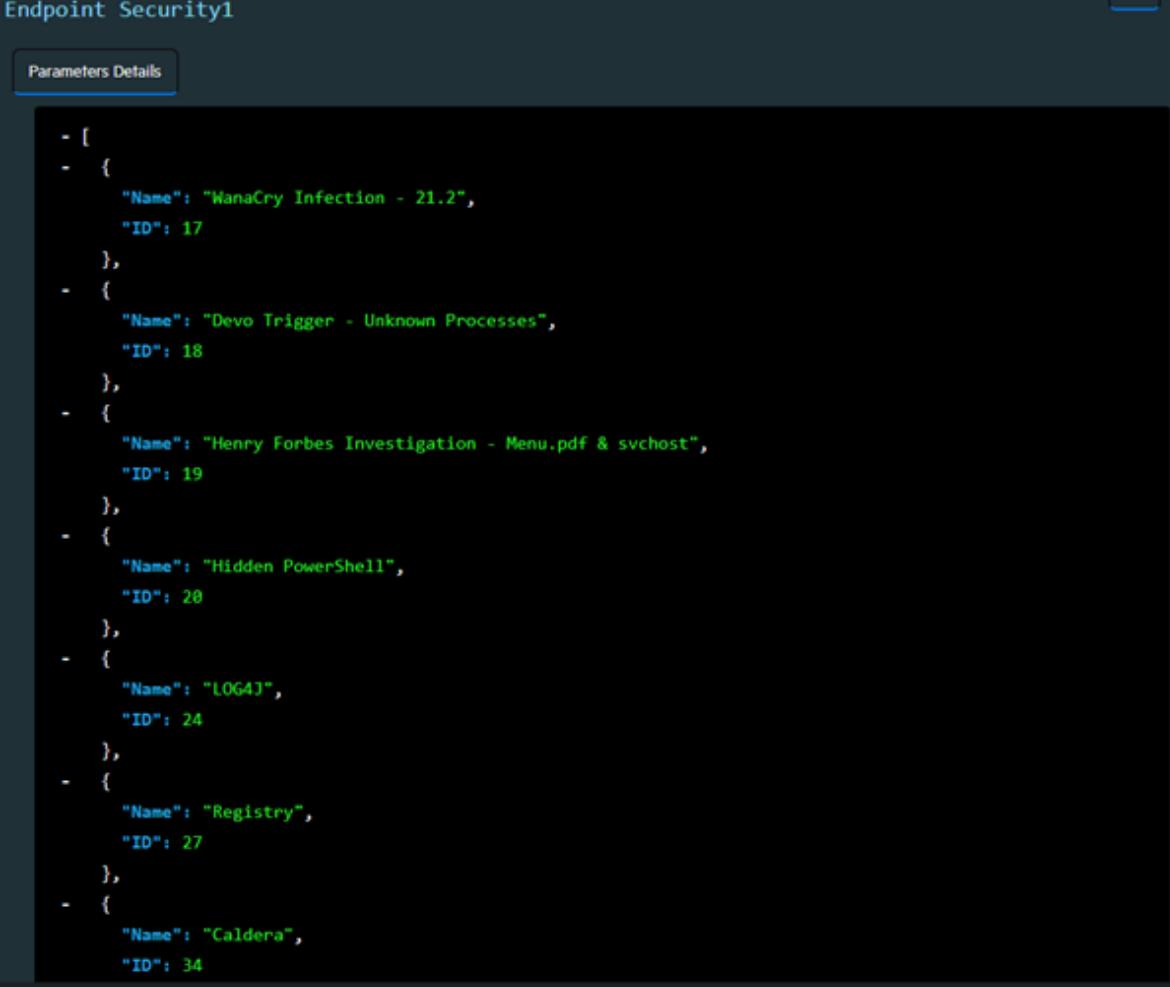
#### **Input Parameters:**

N/A

#### **Output:**

Case Scope:

N/A

**Human Readable Output:**


The screenshot shows a mobile application interface titled "Endpoint Security1". Below the title is a button labeled "Parameters Details". The main content area displays a JSON-like list of findings:

```

[{"Name": "WanaCry Infection - 21.2", "ID": 17}, {"Name": "Devo Trigger - Unknown Processes", "ID": 18}, {"Name": "Henry Forbes Investigation - Menu.pdf & svchost", "ID": 19}, {"Name": "Hidden PowerShell", "ID": 20}, {"Name": "LOG4J", "ID": 24}, {"Name": "Registry", "ID": 27}, {"Name": "Caldera", "ID": 34}

```

**2. Find Hosts with IOCs**

The Enrichment capability queues a search for file-based indicators of compromise.

**Input Parameters:**

Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
Target IP addresses, FQDNs or hostnames	The name of the target address, FQDNs or hostnames	["COMPUTER_NAME", "HOST", "NETWORK_ADDRESS"]	Yes	No
Target IP ranges, IP addresses, FQDNs or hostnames	The range of IP address, FQDNs or hostnames	String	No	No

Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
Name of existing filter	Filter name for search	String	Yes	Yes
Stop the search after the first hit	Whether to stop or not after the first search	Boolean	Yes	Yes

**Output:**

Case Scope:

N/A

Human Readable Output

**3. Standard Agent Timeline (Snapshot)**

The enrichment capability triggers a collection of automatic snapshots which are then stitched together to create a timeline.

**Input Parameters:**

Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
Target IP addresses, FQDNs or hostnames	The name of the target address, FQDNs or hostnames	[ "COMPUTER_NAME", "HOST", "NETWORK_ADDRESS" ]	Yes	No
Target IP ranges, IP addresses, FQDNs or hostnames	The range of IP address, FQDNs or hostnames	String	No	No

**Output:**

Case Scope:

N/A

Human Readable Output

**4. Collect Memory**

The enrichment capability triggers a collection of physical memory to an evidence file (.E01 or .RAW) which can later be analysed in a memory forensics tool such as Volatility.

**Input Parameter**

Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
Memory Output Format	Memory Out put format like "RAW", "E01"	String	No	Yes
Target IP addresses, FQDNs or hostnames	The name of the target address, FQDNs or hostnames	[ "COMPUTER_NAME", "HOST", "NETWORK_ADDRESS" ]	Yes	No
Target IP ranges, IP addresses, FQDNs or hostnames	The rage of IP address, FQDNs or hostnames	String	No	No

**Output:**

Case Scope: N/A

Human Readable Output

**5. Create Snapshot**

The enrichment capability is used to queue a new snapshot of the specified targets within a specified investigation. A snapshot captures the state of a machine at a given time, including the running processes, open ports, network cards, and logon information.

**Input Parameter**

Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
Target IP addresses, FQDNs or hostnames	The name of the target address, FQDNs or hostnames	[ "COMPUTER_NAME", "HOST", "NETWORK_ADDRESS" ]	Yes	No
Target IP ranges, IP addresses, FQDNs or hostnames	The rage of IP address, FQDNs or hostnames	String	No	No

Case Scope: N/A

Human Readable Output

**6. Find Hosts with Items of Interest**

The Enrichment capability queues a scan of your network for indicators including running processes, loaded DLLs, network connections, DNS cache entries, and more. This search relies only on live snapshots, as opposed to forensically searching filesystems. This search can efficiently sweep large IP ranges.

**Input Parameter**

Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
Target IP addresses, FQDNs or hostnames	The name of the target address, FQDNs or hostnames	["COMPUTER_NAME", "HOST", "NETWORK_ADDRESS"]	Yes	No
Target IP ranges, IP addresses, FQDNs or hostnames	The range of IP address, FQDNs or hostnames	String	No	No
MD5 and SHA1 Hashes of Interest	MD5 and SHA1 Hashes of Interest	Hash	Yes	No
IP Addresses of Interest	IP Address	["NETWORK_ADDRESS"]	Yes	No
Domains of Interest	Domains of Interest	["HOST"]	Yes	No
URLs of Interest will derive Domain Name	List of URLs	["URL"]	Yes	No

**Output:**

Case Scope: N/A

Human Readable Output

**7. Get Investigation Job Status**

The enrichment capability I is used to get the status of an investigation job.

**Input Parameter**

Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
Valid Job Type	Valid Job Type to get the status	String	No	Yes
Job ID	Job ID to get the status	String	No	Yes

**Output:**

Case Scope: N/A

Human Readable Output

**8. Get Event Status**

The Enrichment Capability I is used to get the status of an event created using the CreateEvent API

**Input Parameter**

Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
Job ID	Job ID to get the status	String	No	Yes

**Output:**

Case Scope: N/A

Human Readable Output:

a few seconds ago - S swarna dash executed Get Event Status enrichment on EnCase End point Security1	
Parameters Details	
Field	Value
JobId	68625
JobName	Snapshot Test-527
JobStatus	Pending
TargetStatus	[ { "Status": "Pending", "Target": "IR518W-WIN10" } ]

## 9. Collect Data - Pre Defined Filter

The enrichment capability queues a file collection using any existing web or desktop filter.

### Input Parameter

Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
Target IP addresses, FQDNs or hostnames	The name of the target address, FQDNs or hostnames	["COMPUTER_NAME", "HOST", "NETWORK_ADDRESS"]	Yes	No
Target IP ranges, IP addresses, FQDNs or hostnames	The range of IP address, FQDNs or hostnames	String	No	No
Name of existing filter	Name of existing filter	String	No	Yes
Endpoint Investigator Case Collection	Endpoint Investigator Case Collection value need to select	Boolean	No	Yes
Endpoint Investigator Case Name	Case Name	String	No	No
Endpoint Investigator Base Case Folder	Base Case Folder Name	String	No	No
Endpoint Investigator Case Backup Location	Endpoint Investigator Case Backup Location path	String	No	No
Endpoint Investigator Case Maximum Backup Size (GB)	Endpoint Investigator Case Maximum Backup Size (GB)	Number	No	No

Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
Endpoint Investigator Case Backup Every Interval	Endpoint Investigator Case Backup Every Interval	String	No	Yes
Endpoint Investigator Case Number. Use SOAR Case Number?	Endpoint Investigator Case Number. Use SOAR Case Number?	Number	No	Yes
Endpoint Investigator User Defined Case Number	If SOAR Case Number not used specify a case number	Number	No	No
Endpoint Investigator Case Examiner Name	Name of person doing the investigation.	String	No	No
Endpoint Investigator Case Description	Endpoint Investigator Case Description	String	No	No

**Output:**

Case Scope: N/A

Human Readable Output

**10. Collect Data -Custom Filter**

The enrichment capability queues a file collection using user-supplied EnDef filter

Input Parameter

Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
Target IP addresses, FQDNs or hostnames	The name of the target address, FQDNs or hostnames	["COMPUTER_NAME", "HOST", "NETWORK_ADDRESS"]	Yes	No
Target IP ranges, IP addresses, FQDNs or hostnames	The range of IP address, FQDNs or hostnames	String	No	No
EnDefFilter	Name of existing filter	Is supported only for application/json	No	Yes
Endpoint Investigator Case Collection	Endpoint Investigator Case Collection value need to select	Boolean	No	Yes
Endpoint Investigator Case Name	Case Name	String	No	No

Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
Endpoint Investigator Base Case Folder	Base Case Folder Name	String	No	No
Endpoint Investigator Case Backup Location	Endpoint Investigator Case Backup Location path	String	No	No
Endpoint Investigator Case Maximum Backup Size (GB)	Endpoint Investigator Case Maximum Backup Size (GB)	Number	No	No
Endpoint Investigator Case Backup Every Interval	Endpoint Investigator Case Backup Every Interval	String	No	Yes
Endpoint Investigator Case Number. Use SOAR Case Number?	Endpoint Investigator Case Number. Use SOAR Case Number?	Number	No	Yes
Endpoint Investigator User Defined Case Number	If SOAR Case Number not used specify a case number.	Number	No	No
Endpoint Investigator Case Examiner Name	Name of person doing the investigation.	String	No	No
Endpoint Investigator Case Description	Endpoint Investigator Case Description	String	No	No

**Output:**

Case Scope: N/A

Human Readable Output

**11. Isolate**

The Action capability used to isolate an endpoint, which prevents an endpoint from communicating across the network

**Input Parameter**

Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
A single target name that can be: HostName, IP Address, or FQDN	A single target name that can be: HostName, IP Address, or FQDN	[ "COMPUTER_NAME", "HOST", "NETWORK_ADDRESS" ]	Yes	Yes

**Output**

Case Scope: N/A

Human Readable Output:

```
a few seconds ago - Isolate action for A single target name that can be: HostName, IP Address, or FQDN: ir518w-win10 on EnCase Endpoint Security1 executed successfully by S swarna dash
a few seconds ago - [REDACTED] commented
JobId:68640, JobType :isolate, InvestigationId:79, InvestigationUrl:https://vm-ehutnyk.eastus.cloudapp.azure.com:4421/#/investigation/79?view=7,Targets:ir518w-win10
```

## 12. Reconnect

The Action capability is used to reconnect a previously isolated endpoint (using Isolate) back to the network.

Input Parameter

Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
A single target name that can be: HostName, IP Address, or FQDN	A single target name that can be: HostName, IP Address, or FQDN	["COMPUTER_NAME", "HOST", "NETWORK_ADDRESS"]	Yes	Yes

Output

Case Scope: N/A

Human Readable Output:

```
2 hours ago - Reconnect action for A single target name that can be: HostName, IP Address, or FQDN: ir518w-win10 on EnCase Endpoint Security1 executed successfully by S swarna dash
2 hours ago - Reconnect action for A single target name that can be: HostName, IP Address, or FQDN: ir518w-win10 on EnCase Endpoint Security1 created by S swarna dash (waiting for execution)
2 hours ago - [REDACTED] commented
JobId:68641, JobType :reconnect, InvestigationId:79, InvestigationUrl:https://vm-ehutnyk.eastus.cloudapp.azure.com:4421/#/investigation/79?view=7,Targets:ir518w-win10
```

## 13. Create Event

The Action capability is used by SIEMs or other security software to queue a new snapshot of the specified target, and it subsequently create a new event to be triaged within EnCaseEndpoint Security. A snapshot captures the state of a machine at a given time, including the running processes, open ports, network cards, and logon information.

Input Parameter

Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
Source	Source	String	No	Yes
Comment	Comment	String	No	No
Id	Id	String	No	Yes
Score Enter a value between 1 and 100. 1-30 = assess, 31-69 = suspicious, 70-100 = malicious	Sore value	Number	No	Yes
A single target name that can be: HostName, IP Address, or FQDN	A single target name that can be: HostName, IP Address, or FQDN	["COMPUTER_NAME", "HOST", "NETWORK_ADDRESS"]	Yes	Yes

## Output

Case Scope: N/A

Human Readable Output:

```
a few seconds ago -  commented
JobId:68663, Source:Swarna Source, Comment:Test CommentId:Score:36 ,Targets:ir518w-win10

a few seconds ago - Create Event action for Score Enter a value between 1 and 100. 1-30 = asses
s, 31-69 = suspicious, 70-100 = malicious: 36, Target IP addresses, FQDNs or hostnames: ir518
w-win10, Source: Swarna Source, Id: Test Id, Comment: Test Comment on EnCase Endpoint Securit
y1 created by S swarna dash (waiting for execution)
```

## 14. Remediate

The action capability queues a remediation of processes and files using a combination of hash and size.

Input Parameter

Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
Remediation Option	Remediation Option	String	No	Yes
Target IP ranges, IP addresses, FQDNs or hostnames	Target IP ranges, IP addresses, FQDNs or hostnames	String	No	No
A single target name that can be: HostName, IP Address, or FQDN	A single target name that can be: HostName, IP Address, or FQDN	["COMPUTER_NAME", "HOST", "NETWORK_ADDRESS"]	Yes	Yes
MD5 Hashes		["HASH"], ["MD5"]	Yes	Yes

## Output

Case Scope: N/A

Human Readable Output:

```
a few seconds ago - Remediate action for Remediation Option: Kill running processes only (optimized for IP ranges), Target IP addresses, FQDNs or hostnames: ir518w-win10, MD5 Hashes: 07411F169FBCE7CC3C3E4830779EAFDD on EnCase Endpoint Security1 executed successfully by S swarna dash
```

```
a few seconds ago - Remediate action for Remediation Option: Kill running processes only (optimized for IP ranges), Target IP addresses, FQDNs or hostnames: ir518w-win10, MD5 Hashes: 07411F169FBCE7CC3C3E4830779EAFDD on EnCase Endpoint Security1 created by S swarna dash (waiting for execution)
```

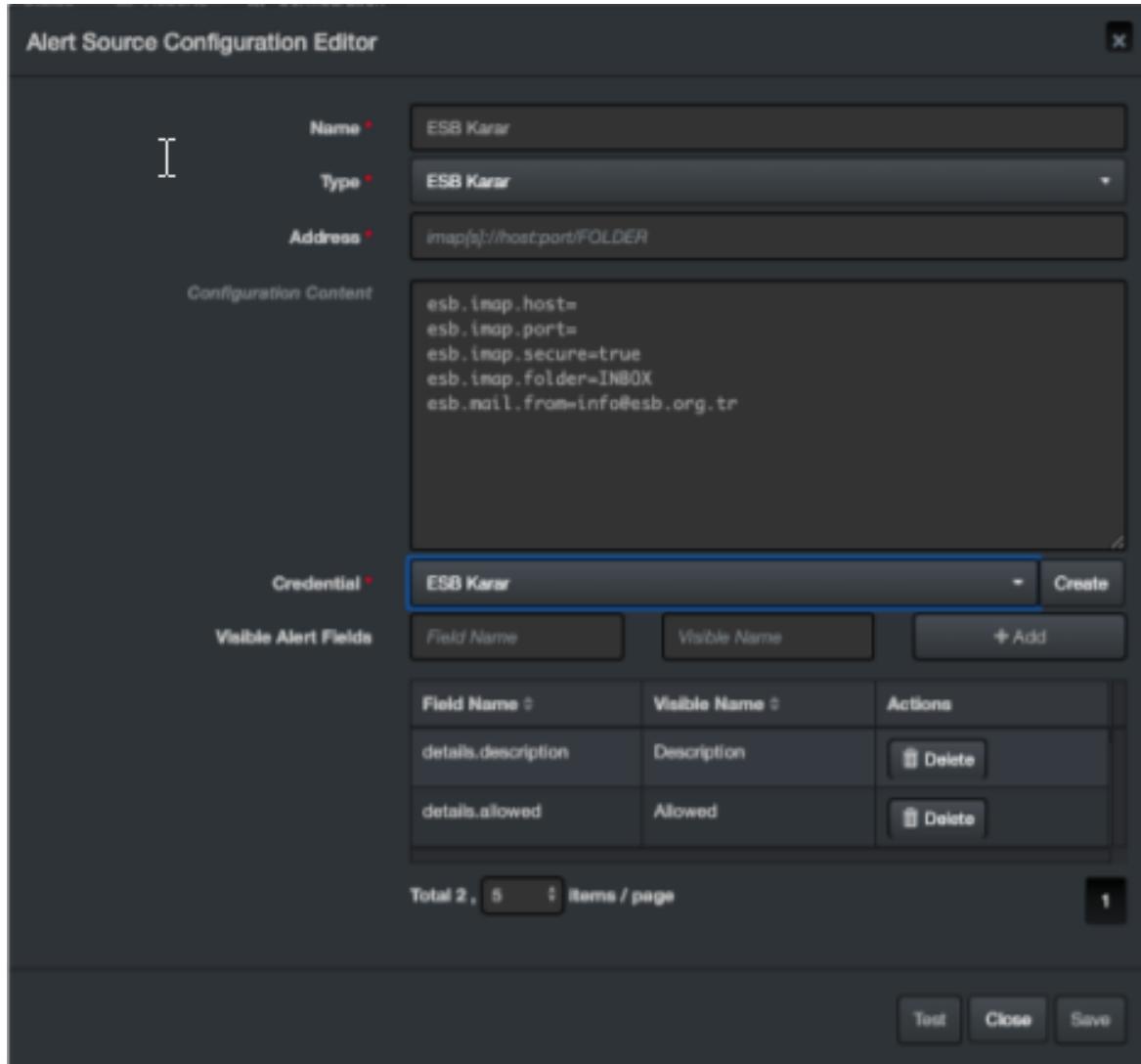
a few seconds ago -  commented

JobId:68668, InvestigationId:79, InvestigationUrl:<https://vm-ehutnyk.eastus.cloudapp.azure.com:4421/#/investigation/79?view=6>, Remediation Option ID:1, Remediation Option Level:Kill running processes only (optimized for IP ranges) ,Hashes:{'Md5': u'07411F169FBCE7CC3C3E4830779EAFDD'}, Targets:ir518w-win10

# Integration Guide for ESB Karar

1. To create the alert source, click **Configuration > Alert Source**.
2. Specify the following parameter values in the **Configuration Editor**:

Parameter	Value
Name	Display name of the alert source
Type	ESB Karar
Address	Address of the alert source. (in the format imap[s]://host:port/FOLDER).
Configuration Content	<code>esb imap host=</code> <code>esb imap port=</code> <code>esb imap secure=true</code> <code>esb imap folder=INBOX</code> <code>esb mail from=info@esb.org.tr</code>
Credential	Credential defined for this alert source under the Credentials menu
Visible Alert Field	- details.description - details.allowed



3. Click **Test**. The following pop up will be displayed if your credential and address are valid.
4. Click **Save** to complete integration.

# Integration Guide for F5 Big-IP Advanced Firewall Manager

## Integration Overview

Big IP AFM protects the network against incoming threats, even the most massive and complex DDoS attacks.

Big IP AFM keeps bad traffic away from some specific network addresses and protects the data center against DDoS attacks, and other network or application attacks. It also brings visibility and control to SSH, and SSL connections, providing against back door threats that use the SSH channel for data breaches and app attacks.

## Integration Capabilities

### Action

- Add address to specific address list

## Configuration

### Configuring F5 Big-IP Advanced Firewall Manager

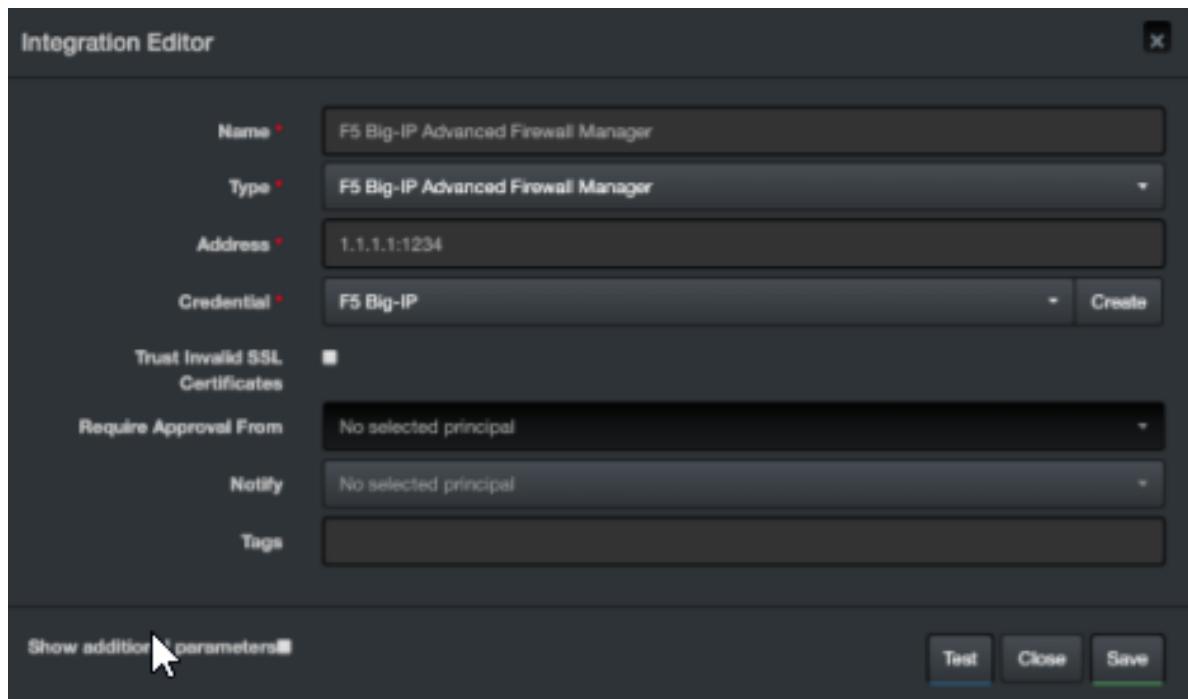
- Make sure SOAR has access to F5 Big-IP Advanced Firewall Manager integration's API as it connects to it using HTTPS.

### Configuring SOAR

1. To create the integration, navigate to **Configuration > Integrations**.
2. Specify the following parameter values in the **Integrations Editor** form.

Parameter	Value
Name	Display name of integration
Type	F5 Big-IP Advanced Firewall Manager

Parameter	Value
Address	Address of the integration (in the format 1.1.1.1:1234 or abc.example.com:1234)
Credential	Credential that was defined for this integration under the <b>Credentials</b> menu
Trust Invalid SSL Certificates	Select this if device's certificate is self-signed or is not recognized by browsers
Require Approval From	Select users from the list who can provide approval before executing actions on this integration
Notify	Select user(s) from the list to notify when SOAR performs an action on this integration



3. Click **Test**. The following pop up will be displayed if your credential and address are valid.
4. Click **Save** to complete integration.

# Integration Guide for FireEye HX

## Integration Overview

FireEye HX is an endpoint threat detection and prevention solution. ArcSight SOAR integrates with FireEye HX through REST API to give enrichment and action capabilities to the users.

## Integration Capabilities

### Enrichment

- **IoC Scan:** HX can scan a given scope item in a target system and return information.
- **Detailed System Information:** HX can gather a target system information.
- **Script Execution:** HX supports different forensic data gathering scripts. These are XML formatted files that exist on HX installation. If customer wishes, they can import these script like files into Customization Library and then execute them through SOAR.

### Action

**Quarantine:** HX quarantines a target system and reverts the quarantine if required.

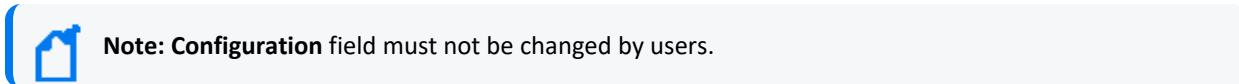
## Configuration

### Configuring FireEye HX

- Make sure API services are enabled and create a api\_admin user. To enable the service, please see product documentation
- Access to the port number defined in the HX during installation as SOAR connects to FireEye HX.
- Define required access control rules if SOAR and FireEye HX are segregated.

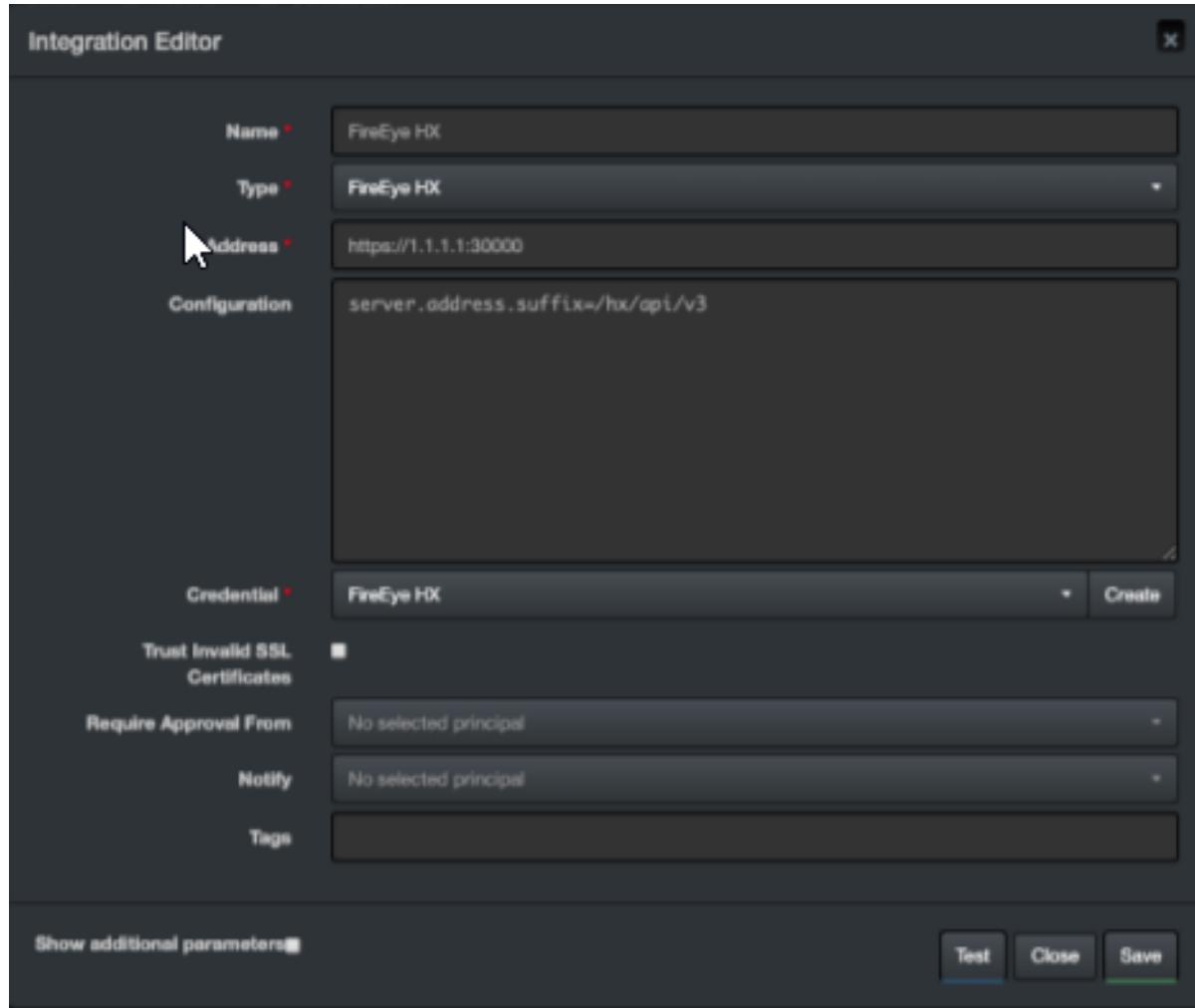
### Configuring SOAR

SOAR configuration is standard and users need to specify **Name**, **Address** and **Credential fields**. Rest of the fields can be changed as required.



1. To create the integration, navigate to **Configuration > Integrations**.
2. Specify the following parameter values in the **Integration Editor** form:

Parameter	Value
Name	Display name of the integration
Type	FireEye HX
Address	Address of the alert source (in the format http[s]://1.1.1.1:3000 or http[s]://abc.example.com:3000)
Configuration	Specify the following configuration parameter: <code>server.address.suffix=/hx/api/v3</code>
Credential	Credential defined under the <b>Credentials menu</b>
Trust Invalid SSL Certificates	Select this if device's certificate is self-signed or is not recognized by browsers
Require Approval From	Select users from the list who can provide approval before executing actions on this integration
Notify	Select users from the list to notify when SOAR performs an action on this integration



3. Click **Test** to test the integration.
4. Click **Save** to complete integration.

# Integration Guide for Forcepoint Cloud Services

## Integration Overview

SOAR works with Forcepoint Cloud Services to report uncategorized sites.

## Integration Capabilities

### Action

- Report

## Configuration

### Configuring Forcepoint Cloud Services

- Make sure SOAR has access to HTTPS as it connects to Forcepoint Cloud Services URL (<https://www.websense.com>).
- A user account on Forcepoint/WebSense to use the **Sitelookup** tool.

### Configuring SOAR

1. To create the integration, navigate to **Configuration > Integrations**.
2. Specify the following parameter values in the **Integrations Editor**.

Parameter	Value
Name	Display name of the integration
Type	Forcepoint Cloud Services
Address	Address of the integration (in the format http[s]://abc.example.com:3000)
Credential	Credential defined for this integration under the <b>Credentials</b> menu.

Parameter	Value
Trust Invalid SSL Certificates	Select this if device's certificate is self-signed or is not recognized by browsers
Require Approval From	Select users from the list who can provide approval before executing actions on this integration
Notify	Select users from the list to notify when SOAR performs an action on this integration

Integration Editor

The screenshot shows the 'Integration Editor' dialog box with the following configuration:

- Name:** ForcePoint Cloud Services
- Type:** Forcepoint Cloud Services
- Address:** https://www.websense.com
- Credential:** Forcepoint (selected)
- Trust Invalid SSL Certificates:**
- Require Approval From:** No selected principal
- Notify:** No selected principal
- Tags:** (empty)

At the bottom right are three buttons: **Test**, **Close**, and **Save**.

3. Click **Test** to test the integration.
4. Click **Save** to complete the integration.

# Integration Guide for Forcepoint Content Gateway

## Integration Overview

Forcepoint Web Content Gateway is a web proxy and cache that analyzes HTTP(S) requests in real-time and passes the traffic to Filtering Service for policy enforcement.

## Integration Capabilities

ArcSight SOAR has the following integration capability with Forcepoint Web Content Gateway:

- Block Access to IP Addresses, URLs and Hostnames

### **Use Case: Blocking Phishing Domains**

SOAR checks the inbox of user's email, for phishing reports and automatically creates an incident record on the service desk. During the investigation, SOAR extracts the malicious IP addresses, domains, and URLs in the message body and blocks access to Forcepoint Web Content Gateway. This can either be performed automatically within a playbook or manually by an analyst.

Also, SOAR uses threat intelligence (TI) feeds as an Alert Source and automatically blocks malicious domains/IP addresses reported by TI source on Forcepoint Web Content Gateway before any attack occurs.

## Configuration

### Prerequisites

- Current version of Forcepoint Web Content Gateway.
- Access to HTTPS as SOAR connects to Forcepoint Web Content Gateway Policy API
- Access to 15873/tcp port

## Configuring Facepoint Web Content Gateway

1. Forcepoint Management API does not get installed by default. To complete the integration, install this service on the server or appliance. Also, the configuration steps differ with the usage of the server. For the complete instructions, see [Management API Installation Guide](#).
2. After installing Management API components, use the Forcepoint Security Manager to configure the account used for authentication. To enable the communication, see ***Enabling communication between Management API clients and servers*** in the [Management API Installation Guide](#).

## Configuring SOAR

1. Click **Configuration > Credentials > Create Credential**.
2. Specify the following parameter values in the **Credential Editor** form:
  - a. **Internal credential:**

Parameter	Value
Type	Internal credential
Name	Display name of the credential set (For example, Forcepoint WCG Credentials)
Username	Username configured on Forcepoint Management API
Password	Password for the user configured on Forcepoint Management API.
Private Key	Empty

- b. **Credential Store:**

Parameter	Value
Type	External credential
Name	Name of the credential with pull path of the safe on store.

3. Click **Configuration > integrations > Create Integration**.
4. Specify the following configuration parameter values in the **Configuration form**:

Parameter	Value
Name	Display name of Forcepoint Web Content Gateway integration on SOAR
Type	Forcepoint Web Content Gateway
Address	Address of the integration (in the format <code>https://192.168.2.99:15:15873</code> ).

Parameter	Value
Configuration	Specify the following configuration parameters: <pre># The Category name cannot include any of the following characters: # * &lt; &gt; { } ~ ! \$ % &amp; @ # . "   \ &amp; + = ? / ; : , # SOAR is going to automatically add new category name if it doesn't exist categoryName=SOAR_BLOCK</pre>
Credential	Name of the credential set created on step 2. (For example, Forcepoint WCG Credentials)
Trust Invalid SSL Certificates	Select this if Engine's certificate is self-signed or is not recognized by browsers.
Require Approval From	Select users from the list who can provide approval before executing actions on this integration.
Notify	Select users from the list to notify when SOAR performs an action on this integration

Integration Editor

Name *	Forcepoint Content Gateway
Type *	Forcepoint Content Gateway
Address *	https://1.1.1.1:1234
Configuration	<pre># The Category name cannot include any of the following characters: # * &lt; &gt; { } ~ ! \$ % &amp; @ # . "   \ &amp; + = ? / ; : , # ATAR is going to automatically add new category name if it doesn't exist #categoryName=</pre>
Credential *	Forcepoint <span style="float: right;">Create</span>
Trust Invalid SSL Certificates	<input checked="" type="checkbox"/>
Require Approval From	No selected principal
Notify	No selected principal
Tags	
<a href="#">Show additional parameters</a> <span style="float: right;"><b>Test</b> <b>Close</b> <b>Save</b></span>	

5. Click **Test**. The following pop up will be displayed if your credentials and address are valid.
6. Click **Save** to complete integration.

## Additional Notes

- The **categoryName** you provide in the Configuration section is API-Managed but not managed by UI. If the category does not exist on the device, SOAR creates it automatically.

# Integration Guide for ForeScout CounterACT NAC

## Integration Overview

ForeScout CounterACT NAC provides virtual insight into any device connected across the enterprise and gives a single-pane-of-glass perspective. ForeScout discovers devices in real-time, then classifies, assesses, and monitors these devices. Also, this platform provides agent-less control and continuous monitoring across heterogeneous environments. Enables to trigger actions to notify, monitor, and remediation.

## Integration Capabilities

SOAR has the following integration capability with ForeScout CounterACT NAC:

### Action Capabilities

- Assign Policy to Host

### Enrichment Capabilities

- Host information query by Network Address
- Host information query by Username
- Host information query by MAC Address
- Host information query by Computer Name

### Use Case: Isolating Mal-behaving PC

SOAR integrates with ForeScout CounterACT NAC, while responding to an incident it applies a policy to mal-behaving computers and prevents further spread of the attack. A policy to the host can either be applied automatically within a playbook or manually by an analyst.

## Configuration

### Prerequisites

- Current version of ForeScout CounterACT NAC
- Access to SSH protocol(22/tcp port) as SOAR connects to ForeScout CounterACT NAC using SSH protocol.
- Access to 443/tcp port as enrichment plugin connects to ForeScout CounterACT NAC server
- A shell user account needs to be created for SOAR to connect to ForeScout

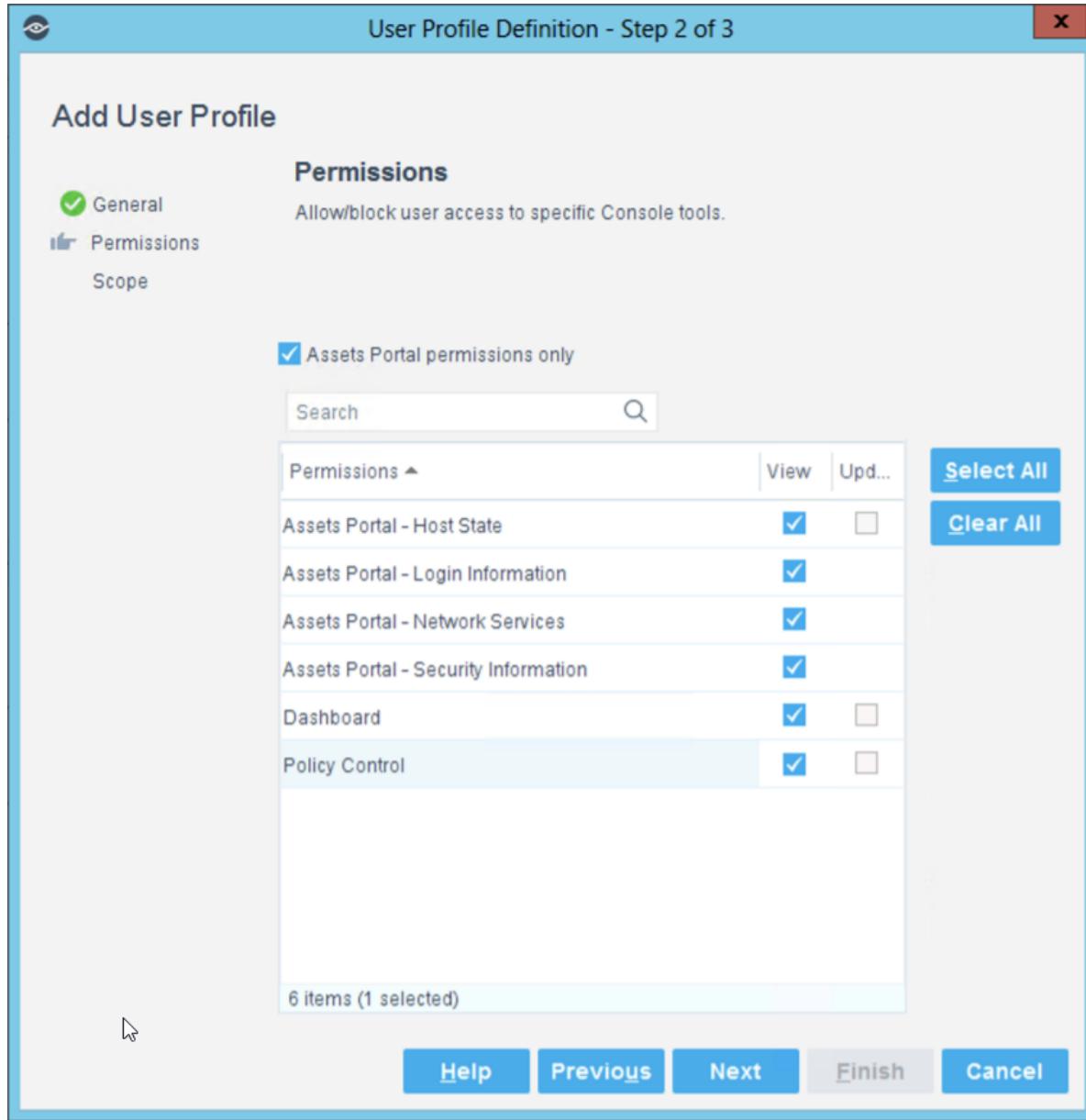
## CounterACT NAC

### Configuring ForeScout CounterACT NAC

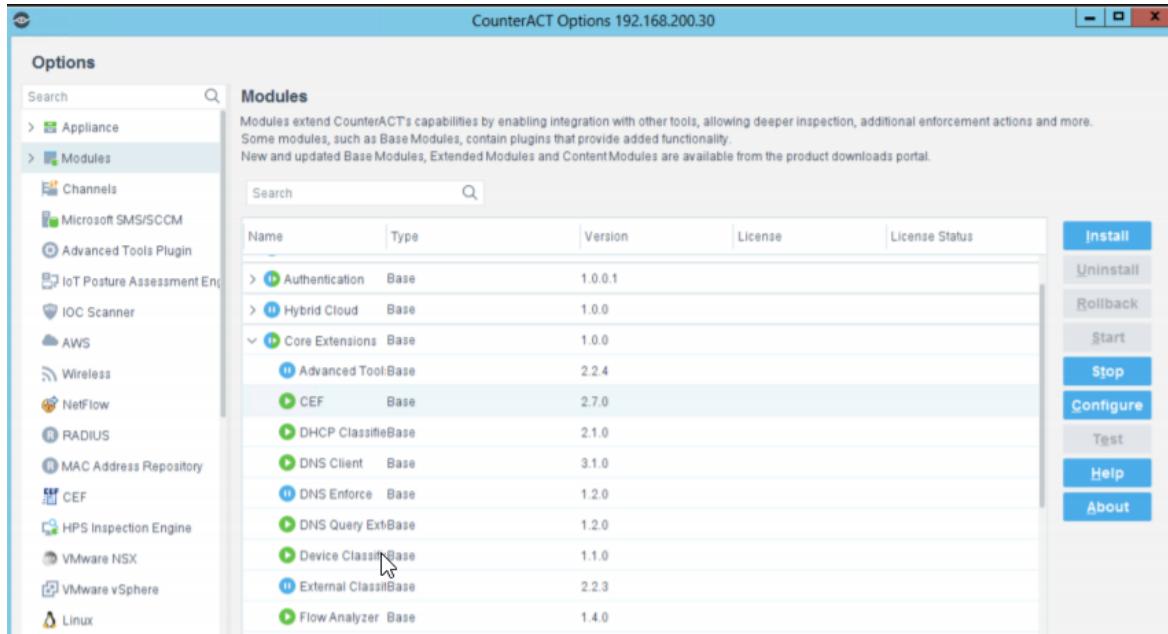
1. Login to ForeScout CounterACT NAC appliance.
2. Create a shell account by executing the following command in the command prompt:

```
$ useradd -s /bin/bash -m -d /home/soar soar  
$ passwd soar
```
3. To allow new user to execute fstool command without the need to enter the password, add the following line to sudo configuration (/etc/sudoers)  

```
soar ALL=(root) NOPASSWD: /usr/local/forescout/bin/fstool
```
4. To use enrichment capabilities, add or use an existing web management user with the following permission:



5. Login to Forescout **Management Interface**.
6. Enable **CEF service**.



7. Navigate to **Policy** and edit one of the existing policies or create a new one.
8. To edit condition of a rule, add “SIEM Message” as Criteria and select desired action.



**Note:** Make a note or save the SIEM message to use while configuring SOAR.

## Configuring SOAR

1. Click **Configuration > Credentials > Create Credential**.
2. Specify the following parameter values in the **Credential Editor** form:
  - a. **Internal Credential**

Parameter	Value
Type	Internal Credential
Name	Display name of credential set (For example, ForeScout CounterACT NAC Credential)
Username	Username created for SOAR on ForeScout CounterACT NAC
Password	Password of the user that was created for SOAR on ForeScout CounterACT NAC
Private Key	Empty

- b. **Internal Credential**

Parameter	Value
Type	Internal Credential
Name	Display name of credential set (For example, ForeScout CounterACT NAC Credential)
Username	Username created for SOAR on ForeScout CounterACT NAC for web management user (2.2.3).
Password	Password of the user you have created for SOAR on ForeScout for web management user (2.2.3).
Private Key	Empty



**Note:** Make a note or save the credential ID to use it in device configuration (2.3.4).

#### c. Credential Store:

Parameter	Value
Type	External Credential
Name	Name of the credential with pull path of the safe on store.

### 3. Click Configuration > Integrations > Create Integration.

Specify the following parameter values in the **Configuraiton** form:

Parameter	Value
Name	Display name of Database Server integration on SOAR
Type	ForeScout CounterACT NAC
Address	Address of the integration (in the format 192.168.1.1)
Configurati on	<p>Specify the following configuration parameters.</p> <pre># Supported versions are: v1 (for version 8.0) and v2 (for version 8.1.3). Default version is v1 #version= # Siem messages should be separate with comma # For Example: # policy.siem.messages=MSG1,MSG2,MSG3 policy.siem.messages= # please provide the credential id if the ForeScout query page has a # different username &amp; password webui_credential_id=(Credential id that you made a note in step 2.3.4)</pre>
Credential	Name of the credential set created on step 2. (For example, ForeScout CounterACT NAC Credential)

Parameter	Value
Trust Invalid SSL Certificates	Select this if device's certificate is self-signed or is not recognized by browsers
Require Approval from	Select users from the list who can provide approval before executing actions on this integration
Notify	Select users from the list to notify when SOAR performs an action on this integration.

Integration Editor

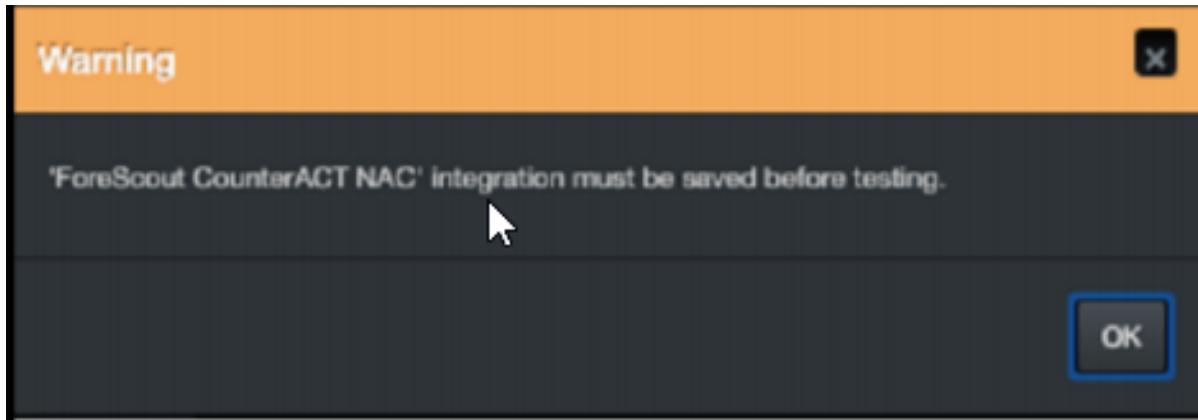
Name *	ForeScout CounterACT NAC
Type *	ForeScout CounterACT NAC
Address *	1.1.1.1
Configuration	<pre># Siem messages should be separate with comma. # For Example: # policy.siem.messages=MSG1,MSG2,MSG3  policy.siem.messages=  #please provide the credential id if the ForeScout query page has a different username &amp; password #webui_credential_id=</pre>
Credential *	Forescout
Trust Invalid SSL Certificates	<input checked="" type="checkbox"/>
Require Approval From	No selected principal
Notify	No selected principal
Tags	
<a href="#">Show additional parameters</a>	
<input type="button" value="Test"/> <input type="button" value="Close"/> <input type="button" value="Save"/>	

4. Click **Save** to complete integration.
5. Click **Test** to test the integration.

## Additional Notes

- ForeScout CounterACT NAC integration is an Advanced Script, and the content of the default script is accessible under **Configuration > Customization Library**.

- While defining the integration for the first time, you might encounter the following warning message, which is the expected behavior for this type of integration.



## Integration Guide for Fortinet Forti Manager V2

### Integration Overview

**FortiManager** is a management tool for Fortify Firewalls. It can manage multiple firewalls in a row from its central user interface.

### Integration Capabilities

ArcSight SOAR has the following integration capabilities with Forti Manager:

- Add to Address Group
- List Devices
- List Firewall Address Groups
- List Firewall Addresses

### Prerequisites

- You must have access to HTTPS as the ArcSight SOAR connects to [Forti Manager IP](#) through this service.
- You must have a super user credentials.

# Configuration

## Configuring Forti Manager

SSH to FortigateManager with admin user credential and execute the following command on ssh terminal:

```
FW # config system admin user
(user)# edit admin
(admin)# set rpc-permit read-write
```

## Configuring SOAR

1. Click **Configuration > Integration > Create Integration**.
2. In **Configuration Editor**, select **FortiManager** in the **Type** list.
3. Click **Create** to create a new credential and specify the following parameters in the **Credential Editor** form:
 

Type	Name	Username	Password	Private Key
Internal credential	Display name of credential set (for example, Fortin Manager Credentials).	FortiManager Username	FortiManager Password	Empty
4. Check the **Clear Text Access** checkbox .
5. Click **Save** to save the integration definition.
6. Navigate to **Configuration>Customization Library** and edit **FortiManager Advanced Action Script Default Template**.
7. Select the integration that you have added to **Integrations** menu.
8. Click **Save** to complete the integration.
9. Click **Test**. **Integration Successful** message is displayed if the credential and address are valid.

## Capabilities

1. **Add To Address Group**
2. Adds Ip address to given group for specified ADOM.

The following table presents the **Add To Address Group** action capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>IP</b>	A valid IP Address to retrieve data.	Network Address Host	Yes	Yes
<b>ADOM</b>	Administrative Domain.	String	No	Yes

**Output:**

Case Scope: N/A

Human Readable Output: N/A

3. List Firewall Address Groups
4. List of firewall address groups on FortiManager.

The following table presents the **List Firewall Address Groups** action capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>ADOM</b>	Administrative Domain.	String	No	Yes

**Output:**

Case Scope: N/A

Human Readable Output:



5. List Firewall Addresses
6. List of Firewall Addresses on FortiManager.

The following table presents the **List Firewall Addresses** action capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>ADOM</b>	Administrative Domain.	String	No	Yes

**Output:**

Case Scope: N/A

Human Readable Output:

a few seconds ago - gurkan aslan executed List Firewall Addresses enrichment on FortiManager v2\_5

Parameters Details

Name	Associated-interface	End-ip	Fqdn	List	Start-ip	Subnet
FIREWALL_AUTH_PORTAL_A_DORESS	["any"]	-	-	-	-	["0.0.0.0", "0.0.0.0"]
SOAR-1.1.1.1	["any"]	-	-	-	-	["1.1.1.1", "255.255.255.255"]
SOAR-185.14.31.9	["any"]	-	-	-	-	["185.14.31.9", "255.255.255.255"]
SSLVPN_TUNNEL_ADDR1	["sslvpn_tun_intf"]	10.212.134.210	-	10.212.134.200	-	-
all	["any"]	-	-	-	-	["0.0.0.0", "0.0.0.0"]
autoupdate.opera.com	["any"]	-	autoupdate.opera.com	-	-	-
google-play	["any"]	-	play.google.com	-	-	-
none	["any"]	-	-	-	-	["0.0.0.0", "255.255.255.255"]
swscan.apple.com	["any"]	-	swscan.apple.com	-	-	-
update.microsoft.com	["any"]	-	update.microsoft.com	-	-	-

Total 10, 100 Items / page

# Integration Guide for Fortinet FortiAnalyzer

## Integration Overview

Fortinet FortiAnalyzer is a central log collection and analysis tool for Fortinet products. SOAR can query FortiAnalyzer (FAZ) for scope items to enrich incident data and to search the past events for emerging threats.

## Integration Capabilities

ArcSight SOAR has the following enrichment capabilities with Fortinet FortiAnalyzer:

- Accepted Traffic Logs : This query returns accepted traffic logs to or from the selected scope item and the time frame might be between 1 hour to 12 hours.
- URL Access Logs : This query returns the events that record access to the selected URL and the time frame might be between 1 hour to 12 hours.

## Configuring Fortinet FortiAnalyzer

Web services must be enabled on the network interface to which the client connects.

1. To enable web services for an interface, navigate to **System Settings > Network > Interface**.
2. Select **Edit** for the interface for which you need to enable the web services.
3. In the **Administrative Access** section, select **Web Service**.
4. Select **OK** to apply the changes.
5. Create a user with a custom profile.



**Note:** This user profile requires access to **Log View/FortiView/NOC - SOC** component and **ADOM's SOAR**.

## Configuring SOAR

1. Click **Configuration > Credentials > Create Credential**.
2. Specify the following parameter values in the **Credential Editor** form:

**a. Internal credential:**

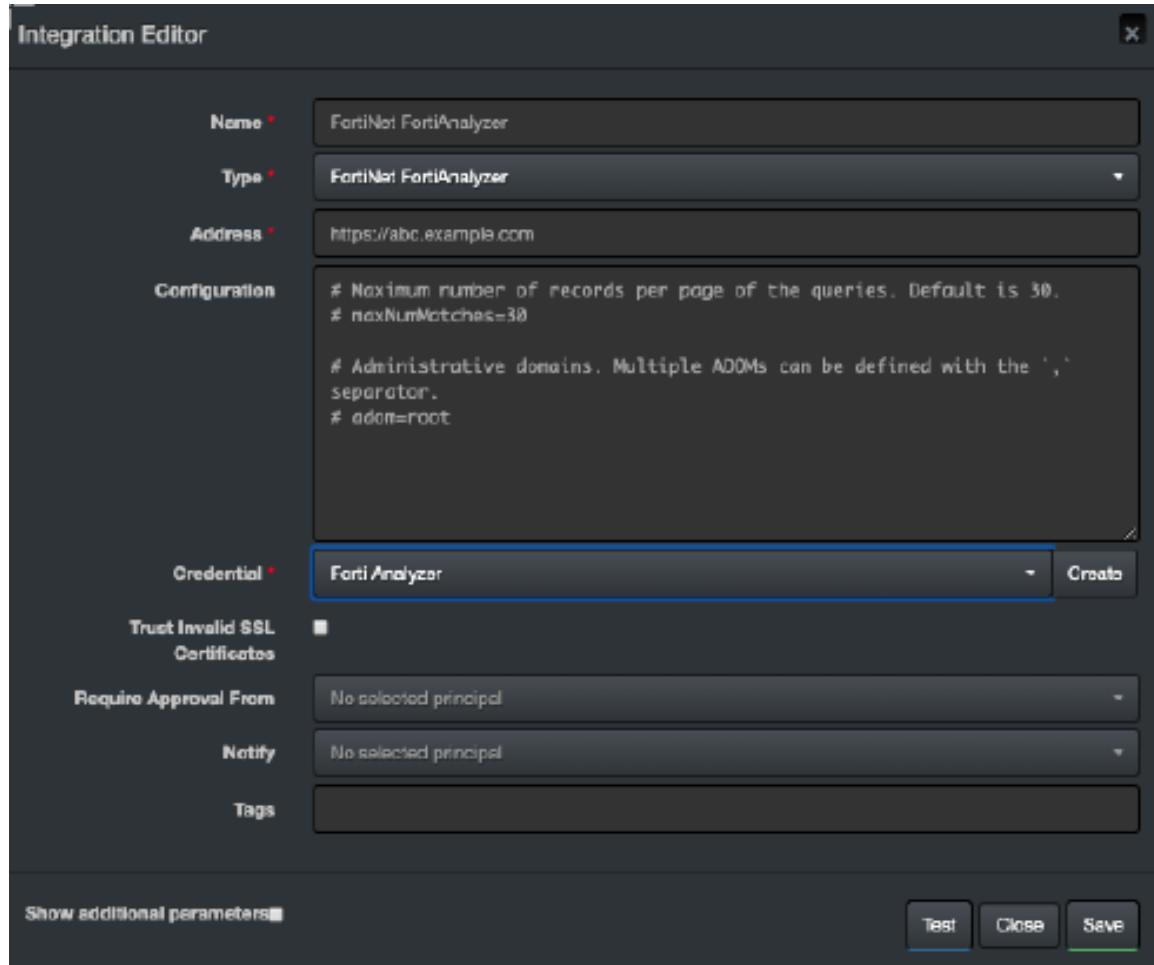
Parameter	Value
Type	Internal credential
Name	Display name of the credential set (For example, Fortinet FortiAnalyzer)
Username	API Key created on Fortinet FortiAnalyzer
Password	API Password for the key created on Fortinet FortiAnalyzer
Private Key	Empty

**b. Credential Store:**

Parameter	Value
Type	External credential
Name	Name of the credential with pull path of the safe on store

3. Click **Configuration > integrations > Create Integration**.
4. Specify the following configuration parameter values in the **Configuration form**:

Parameter	Value
Name	Display name of Fortinet FortiAnalyzer integration on SOAR
Type	Fortinet FortiAnalyzer
Address	Address of the integration (in the following format: 1.1.1.1 or http[s]://abc.example.com)
Credential	Name of the credential set created on step 2 (for example, Fortinet FortiAnalyzer Credentials)
Configuration	Specify the following configuration parameters:  maxNumMatches : Define the number of results SOAR shows per page of query adom: ADOM's SOAR query to get logs from
Require Approval From	Select users from the list who can provide approval before executing actions on this integration
Notify	Select users from the list to notify when SOAR performs an action on this integration



5. Click **Test** to test the integration.
6. Click **Save** to save the integration.

# Integration Guide for Fortinet FortiDDoS

## Integration Overview

FortiDDoS is a network behavior anomaly (NBA) prevention system that detects and blocks attacks that intend to disrupt network service (distributed denial of service (DDoS) attacks) by over utilizing server resources.

## Integration Capabilities

ArcSight SOAR has the following integration capabilities with FortiDDoS:

- Block IP and Hostname

### Use Case: Blocking malicious IP on peripheral

SOAR integrates with FortiDDoS to block malicious IP addresses detected while responding to an incident. Blocking can be performed automatically within a playbook or manually by an analyst.

## Configuration

### Prerequisites

- FortiDDoS version 4.7 and 5.1
- Access to tcp port 443 as SOAR connects to FortiDDoS' API using HTTPS
- An administrator user account for SOAR to connect to FortiDDoS

### Configuring FortiDDoS

1. To add a new SOAR user with the required access profile permissions, navigate to **System > Admin > Access Profile**.
2. In the Access profile form, select **Global Settings** and **Protection profiles** with **Read & Write** permissions.
3. Navigate to **System > Admin > Administrator**.
4. To add an administrator with the profile created in the previous step, select **Enable** for **Allow API Access**.

5. (Optional) To specify **Remote Authentication** and **Idle timeout** values, navigate to **Centralized Management > Admin**.

The screenshot shows the 'Admin' settings page in FortiDDoS-CM. It includes sections for Web Administration Ports (HTTP, HTTPS, SSH, Telnet ports), Web Administration (Language, Idle Timeout), and Remote Authentication Timeout (Remote Authentication Timeout). The 'Idle Timeout' field in the Web Administration section and the 'Remote Authentication Timeout' field in the Remote Authentication section are highlighted with red boxes.

6. Click **Save** to save the changes.

## Configuring SOAR

1. Click **Configuration > Credentials > Create Credential**.
2. Specify the **Credential Editor** with the following parameter values:

a. **Internal Credential**

Parameter	Value
Type	Internal Credential
Name	Display name of credential set (For example, FortiDDoS Credentials)
Username	User created on FortiMail for SOAR
Password	Password of the user that was created for SOAR on FortiMail
Private Key	Empty

b. **Credential Store:**

Parameter	Value
Type	External Credential
Name	Name of the credential with pull path of the safe on store

3. Click **Configuration > Integrations > Create Integration**.

4. Specify the following parameter values in the **Configuration** form:

Parameter	Value
Name	Display name of FortiDDoS integration on SOAR
Type	FortiDDoS
Address	Address of the integration ( in the following format: https://192.168.3.99)
Configuration	Specify the following configuration parameters: <pre># Supported API versions are: v1 (for 4.x versions) and v2 (for 5.x versions). Default api.version=v2 #proxy.id=123</pre>
Credential	Name of the credential set created on step 2 (For example, FortiDDoS Credentials)
Trust Invalid SSL Certificates	Select this if Integrations's certificate is self-signed or is not recognized by browsers.
Require Approval From	Select users from the list who can provide approval before executing actions on this integration
Notify	Select users from the list to notify when SOAR performs an action on this integration

Integration Editor

Name *	Fortinet FortiDDoS
Type *	FortiDDoS
Address *	https://192.168.3.99
Configuration	# Supported API versions are: v1 (for 4.x versions) and v2 (for 5.x versions). Default API version is v1 api.version=v2  #proxy.id=123
Credential *	FortiDDoS Credentials <span style="float: right;">Create</span>
Trust Invalid SSL Certificates	<input checked="" type="checkbox"/>
Require Approval From	J Jennifer McGratt
Notify	J Jennifer McGratt
Tags	

Show additional parameters

Test Close Save

5. Click **Test** to test the integration.
6. Click **Save** to complete the integration.

# Integration Guide for Fortinet FortiGate API

## Integration Overview

Fortinet FortiGate is an industry leading next generation security platform.

## Integration Capabilities

ArcSight SOAR has the following integration capabilities with Fortinet FortiGate API:

- Action
- Block IP
- Block FQDN
- Block URL

### **Use Case: Blocking malicious artifacts detected through alerts**

SOAR automatically executes playbooks and blocks malicious artifacts on FortiGate platform. The artifacts IP, Domain and URL can be blocked using SOAR.

## Configuration

### Prerequisites

- Access to tcp port 443 as SOAR connects to Fortinet FortiGate API using HTTPS
- A user account with necessary permissions on the FortiGate platform

## Configuring Fortinet FortiGate

1. To create a user, navigate to **System > Administrators**.
2. Click **Create New** and select **REST API Admin**.
3. Specify the following values in the **New REST API Admin** form:

**Username:** <SOAR user name>

**Administrator Profile:** <profile name>

**Trusted Hosts:** A subnet that covers SOAR's API address

New REST API Admin

Username	atar_api
Comments	0/255
Administrator Profile	API_Profile
PKI Group	<input type="radio"/>
CORS Allow Origin	<input type="radio"/>
Restrict login to trusted hosts	
Trusted Hosts	192.168.1.1/32
	<input type="button" value="+"/>

**OK** **Cancel**



**Note:** Use the IP address that SOAR uses and **0.0.0.0/0** must not be used as an IP address.

4. To create a profile, click **+** in the **Admin Profile** window.
5. Select **Read/Write** permissions for the following groups:  
**Firewall > Address**  
**Security > Web Filter**

Edit Admin Profile

### Access Permissions

Access Control	Permissions	Set All ▾
Security Fabric	<input type="radio"/> None <input checked="" type="radio"/> Read <input checked="" type="radio"/> Read/Write	
FortiView	<input type="radio"/> None <input checked="" type="radio"/> Read <input checked="" type="radio"/> Read/Write	
User & Device	<input type="radio"/> None <input checked="" type="radio"/> Read <input checked="" type="radio"/> Read/Write	
Firewall	<input type="radio"/> None <input checked="" type="radio"/> Read <input checked="" type="radio"/> Read/Write <input checked="" type="radio"/> Custom	
Policy	<input type="radio"/> None <input checked="" type="radio"/> Read <input checked="" type="radio"/> Read/Write	
Address	<input type="radio"/> None <input checked="" type="radio"/> Read <input checked="" type="radio"/> Read/Write	
Service	<input type="radio"/> None <input checked="" type="radio"/> Read <input checked="" type="radio"/> Read/Write	
Schedule	<input type="radio"/> None <input checked="" type="radio"/> Read <input checked="" type="radio"/> Read/Write	
Log & Report	<input type="radio"/> None <input checked="" type="radio"/> Read <input checked="" type="radio"/> Read/Write <input checked="" type="radio"/> Custom	
Network	<input type="radio"/> None <input checked="" type="radio"/> Read <input checked="" type="radio"/> Read/Write <input checked="" type="radio"/> Custom	
System	<input type="radio"/> None <input checked="" type="radio"/> Read <input checked="" type="radio"/> Read/Write <input checked="" type="radio"/> Custom	
Security Profile	<input type="radio"/> None <input checked="" type="radio"/> Read <input checked="" type="radio"/> Read/Write <input checked="" type="radio"/> Custom	
Antivirus	<input type="radio"/> None <input checked="" type="radio"/> Read <input checked="" type="radio"/> Read/Write	
IPS	<input type="radio"/> None <input checked="" type="radio"/> Read <input checked="" type="radio"/> Read/Write	
Web Filter	<input type="radio"/> None <input checked="" type="radio"/> Read <input checked="" type="radio"/> Read/Write	
Antispam Filter	<input type="radio"/> None <input checked="" type="radio"/> Read <input checked="" type="radio"/> Read/Write	
<input type="button" value="OK"/> <input type="button" value="Cancel"/>		

6. Click **OK** to save the profile and save the API key.

## Configuring SOAR

1. Click **Configuration > Credentials > Create Credential**.
2. Specify the **Credential Editor** with the following parameter values:
  - a. **Internal Credential**

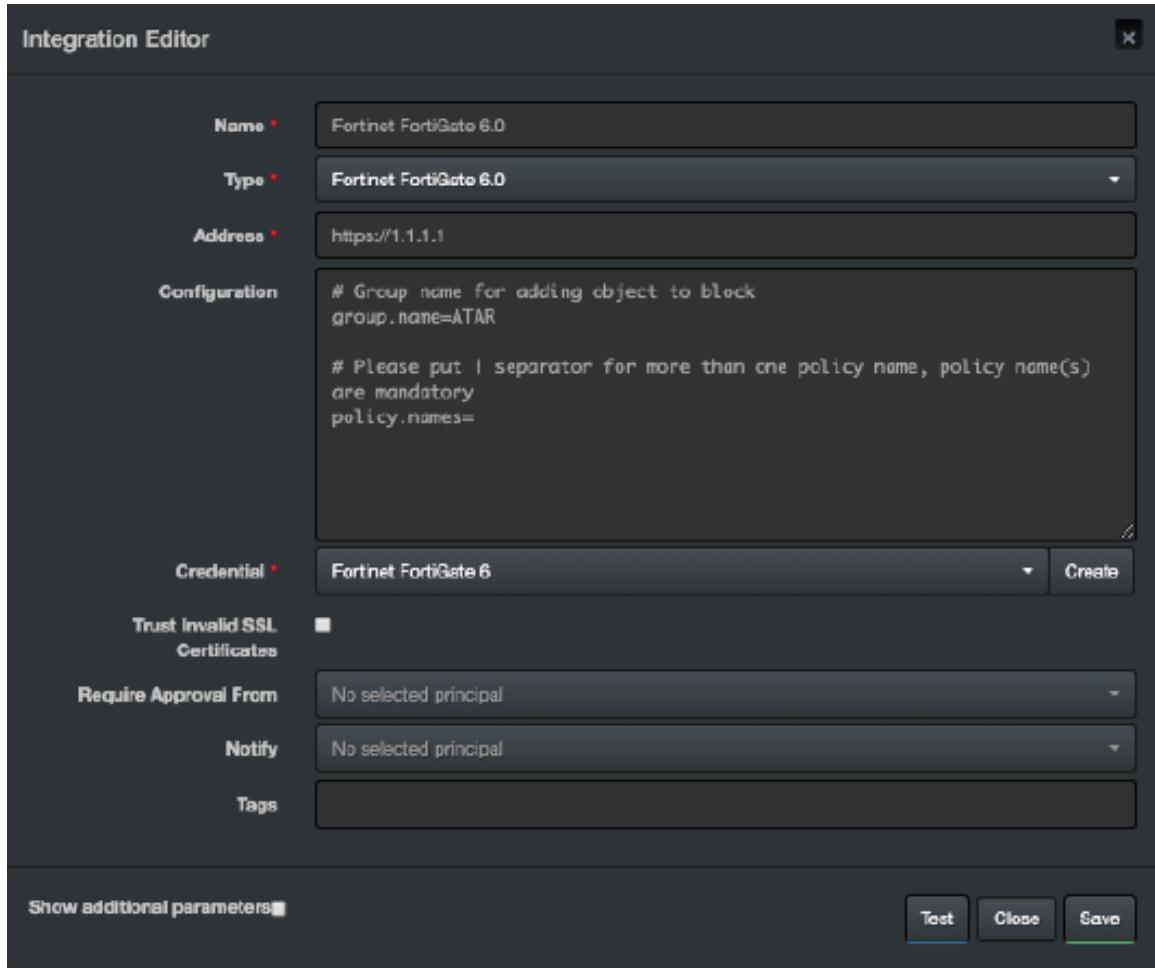
Parameter	Value
Type	Internal Credential
Name	Display name of credential set (For example, Fortinet FortiGate Credentials)
Username	Empty
Password	Empty
Private Key	Enter the API Key generated by FortiGate



**Note:**Fortinet FortiGate requires private key and External Credential is not used.

3. Click **Configuration > Integrations > Create Integration**.
4. Specify the following parameter values in the **Configuration** form:

Parameter	Value
Name	Display name of Fortinet FortiGate integration on SOAR
Type	Fortinet FortiGate 6.0
Address	Address of the firewall
Configuration	Specify the following configuration parameters: group.name: Group name for adding objects to be blocked. This Address Group will be created on FortiGate and then can be used in policies as the admin see fit policy.names: Policy names to be used to block URL. ‘ ’ is used as separator for policies and SOAR writes the URL to all the policies defined
Credential	Name of the credential set that was created on step 2 (For example, Fortinet FortiGate Credentials)
Trust Invalid SSL Certificates	Select this if Integrations’s certificate is self-signed or is not recognized by browsers
Require Approval From	Select users from the list who can provide approval before executing actions on this integration



- Click **Save** to complete the integration.

## Additional Notes

- The API Key to work properly requires access to HTTPS and for security reasons as well.

 **Note:** By default, HTTP access is enabled in FortiGate. However, in production environment, it is recommended to disable the HTTP access.

- If you have multiple policies on the integration configuration and if one of the policy's URL filter is disabled, SOAR with Fortinet integration displays no specific error message. In such case, you might encounter the following error message:

***None of policy names in the configuration are present in the Fortinet FortiGate server.***

# Integration Guide for Fortinet FortiMail

## Integration Overview

Fortinet FortiMail secure email gateway utilizes the latest technologies and security services from FortiGuard Labs to protect from common and advanced threats while integrating robust data protection capabilities to avoid data loss.

## Integration Capabilities

ArcSight SOAR has the following integration capabilities with FortiMail:

- Add to Block List
- Block

### **Use Case: Blocking malicious sender**

SOAR integrates with FortiMail to block malicious email addresses detected while responding to an incident. The blocking can either be performed automatically within a playbook or manually by an analyst.

## Configuration

### Prerequisites

- FortiMail version 6.2.2(GA) and later
- Access to tcp port 443 as SOAR connects to FortiMail API using it
- An administrator user account for SOAR to connect to FortiMail

### Configuring FortiMail

1. By default, REST-API service is disabled on FortiMail. To enable it, use the following CLI command:

```
config system global
    set rest-api enable
end
```

2. Navigate to **System > Administrator > Admin Profile**.
3. Select **Policy, Block/Safe List** with **Read-Write** support and create an admin profile in the **Admin Profile** form.

Admin Profile

Profile name: atar\_profile

Access Control	None	Read Only	Read-Write
-!Select All--	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
System	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Policy	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Block/Safe List	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Greylist	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
System Quarantine [All folders]	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Personal Quarantine	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Archive	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Mail Queue	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Others	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

**OK** **Cancel**

4. Navigate to **System > Administrator > Administrator**.
5. Create a new administrator account with the profile that you have created in the previous step.

The screenshot shows the 'Administrator' configuration page. It includes fields for 'Enable' (checkbox), 'Administrator' (text input: atarapi), 'Domain' (dropdown: --System--), 'Admin profile' (dropdown: atar\_profile), 'Access mode' (radio buttons: CLI, GUI, REST API - REST API is selected), 'Authentication type' (dropdown: Local), 'Trusted hosts' (IP range input: 0.0.0.0 / 0.0.0.0), 'Language' (dropdown: English), 'Theme' (dropdown: Green), and a 'Change Password' link. At the bottom are 'OK' and 'Cancel' buttons.

## Configuring SOAR

1. Click **Configuration > Credentials > Create Credential**.
2. Specify the **Credential Editor** with the following parameter values:
  - a. **Internal Credential**

Parameter	Value
Type	Internal Credential
Name	Display name of credential set (For example, FortiMail Credentials)
Username	User created on FortiMail for SOAR
Password	Password of the user created on FortiMail for SOAR
Private Key	Empty

- b. **Credential Store:**

Parameter	Value
Type	External Credential
Name	Name of the credential with pull path of the safe on store

3. Click **Configuration > Integrations > Create Integration**.
4. Specify the following parameter values in the **Configuration** form:

Parameter	Value
Name	Display name of FortiMail integration on SOAR
Type	FortiMail
Address	Address of the integration ( in the following format: https://192.168.3.100)
Configuration	Specify the following configuration parameters: #proxy.id=5433
Credential	Name of the credential set created on step 2 (For example, FortiMail Credentials)
Trust Invalid SSL Certificates	Select this if Integrations's certificate is self-signed or is not recognized by browsers.
Require Approval From	Select users from the list who can provide approval before executing actions on this integration
Notify	Select users from the list to notify when SOAR performs an action on this integration

### Integration Editor

**Fortinet FortiMail**

Name *	Fortinet FortiMail
Type *	FortiMail
Address *	https://192.168.3.100
Configuration	#proxy.id=5433
Credential *	Fortimail Credentials
Trust Invalid SSL Certificates	<input checked="" type="checkbox"/>
Require Approval From	Jennifer McGratt
Notify	Jennifer McGratt
Tags	

Show additional parameters 

**Test** **Close** **Save**

5. Click **Test** to test the integration.

6. Click **Save** to complete the integration.

## Additional Notes

**Add to Block List** capability uses the **Security > System > Blocklist**, whereas **Block** capability uses the **Policy > Access Control**.

# Integration Guide for Fortinet FortiManager

## Integration Overview

Fortinet FortiManager is a centralized management unit for Fortinet family devices. It provides best compliance practices and workflow automation. This integration has been tested with Fortinet FortiManager v5.6.2-build1631 180124 (GA) firmware version.

## Integration Capabilities

ArcSight SOAR has the following integration capabilities with FortiManager:

- Block file on an connected Fortinet family device (For example, Fortinet NGFW, Fortinet FortiMail, etc)
- Block IP address on an connected Fortinet family device (For example, Fortinet NGFW, Fortinet FortiMail, etc)
- Block username on an connected Fortinet family device (For example, Fortinet NGFW)
- Block email on an connected Fortinet family device (For example, Fortinet FortiMail)

### Use case: Mitigating Compromised Account Cases

SIEM, with the help of intelligence sources, creates an alarm. It compromises the suspected email accounts of the employees. SOAR integrates with Fortinet FortiManager and automatically blocks the outgoing emails and the incoming and outgoing traffic. This blocking can either be performed automatically within a playbook or manually by an analyst.

## Prerequisites

- Access to tcp port 443 as SOAR connects to Fortinet FortiManager using HTTPS
- A user account for SOAR to connect to Forti Manager

# Configuration

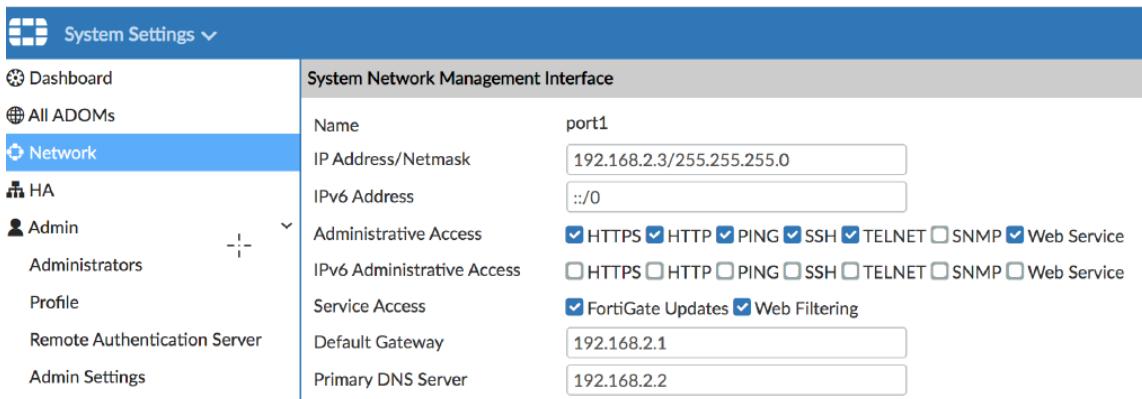
## Configuring FortiManager

1. Navigate to **System Settings > Admin > Administrators**.
2. To create a profile with Super\_User account, specify the following values in the **New Administrator** form:
  - **Username:** <SOAR username>
  - **Admin Type:** Local
  - **New Password:** <Specify the password>
  - **Confirm Password:** <Confirm the password entered in the **Password** field>
  - **Admin Profile:** Super\_User

The screenshot shows the 'New Administrator' configuration page. The form fields are as follows:

New Administrator	
User Name	ataruser
Avatar	A (Profile icon) + Change Photo - Remove Photo
Comments	0/127
Admin Type	LOCAL
New Password	*****
Confirm Password	*****
Admin Profile	!Super_User
Administrative Domain	All ADOMs All ADOMs except specified ones Specify
Policy Package Access	All Packages Specify
Trusted Hosts	OFF
Meta Fields >	

3. Navigate to **System Settings > Network**.
4. Enable the **Web Service** in the **Administrative Access**.



## Configuring SOAR

1. Click **Configuration > Credentials > Create Credential**.
2. Specify the following parameter values in the **Credential Editor**:
  - a. **Internal Credential**

Parameter	Value
Type	Internal Credential
Name	Display name of credential set (For example, Forti Manager Credentials)
Username	User that was created for SOAR on Forti Manager
Password	Password of the user that was created for SOAR on Forti Manager
Private Key	Empty

- b. **Credential Store:**

Parameter	Value
Type	External Credential
Name	Name of the credential with pull path of the safe on store

3. Click **Configuration > Integrations > Create Integration**.
4. Specify the following parameter values in the **Configuration** form:

Parameter	Value
Name	Display name of FortiMail integration on SOAR
Type	Forti Manager
Address	Address of the integration ( in the following format: https://192.168.2.2:8080)

Parameter	Value
Credential	Name of the credential set created on step 2 (For example, Forti Manager Credentials)
Trust Invalid SSL Certificates	Select this if Forti Manager's certificate is self signed or is not recognized by browsers
Require Approval From	Select users from the list who can provide approval before executing actions on this integration
Notify	Select users from the list to notify when SOAR performs an action on this integration

Integration Editor

The screenshot shows the 'Integration Editor' dialog box with the following fields filled in:

- Name**: Forti Manager
- Type**: Forti Manager
- Address**: 192.168.200.3:8080
- Credential**: Forti Manager Credentials (with a 'Create' button)
- Trust Invalid SSL Certificates**: Checked
- Require Approval From**: Jennifer McGratt
- Notify**: Jennifer McGratt
- Tags**: (empty)

At the bottom, there are buttons for **Show additional parameters**, **Test**, **Close**, and **Save**.

5. Click **Test** to test the integration.
6. Click **Save** to complete the integration.

## Additional Notes

Commands to be run on Forti Gate firewall devices are defined as Advanced Action Script. To access the default scripts navigate to **Configuration > Customization Library**.

# Integration Guide for Fortinet FortiSandbox

## Integration Overview

Fortinet Sandbox is a zero-day malware behavior analysis system. It enables organizations to defend against advanced threats such as ransomware by integrating various Fortinet technologies and other security products. Or is used as an extension to their on-premise security architectures to leverage complete control. This integration has been tested with Fortinet FortiSandbox 3.1.0 version.

## Integration Capabilities

ArcSight SOAR has the following integration capabilities with Fortinet Sandbox:

- Query File Hash
- Analyze File
- Analyze URL

### Use Case: Investigating Suspicious Files

During the investigation of a suspicious endpoint behavior, SOAR integrated with Fortinet Sandbox analyzes the behavior of potential malware and hashes and URLs detected on suspicious network traffic. This investigation can either be performed automatically within a playbook or manually by an analyst.

## Configuration

### Prerequisites

- Access to tcp port 443 as SOAR connects to Fortinet Sandbox API using HTTPS
- A user account is required for SOAR to connect to Fortinet Sandbox

### Configuring Fortinet Sandbox

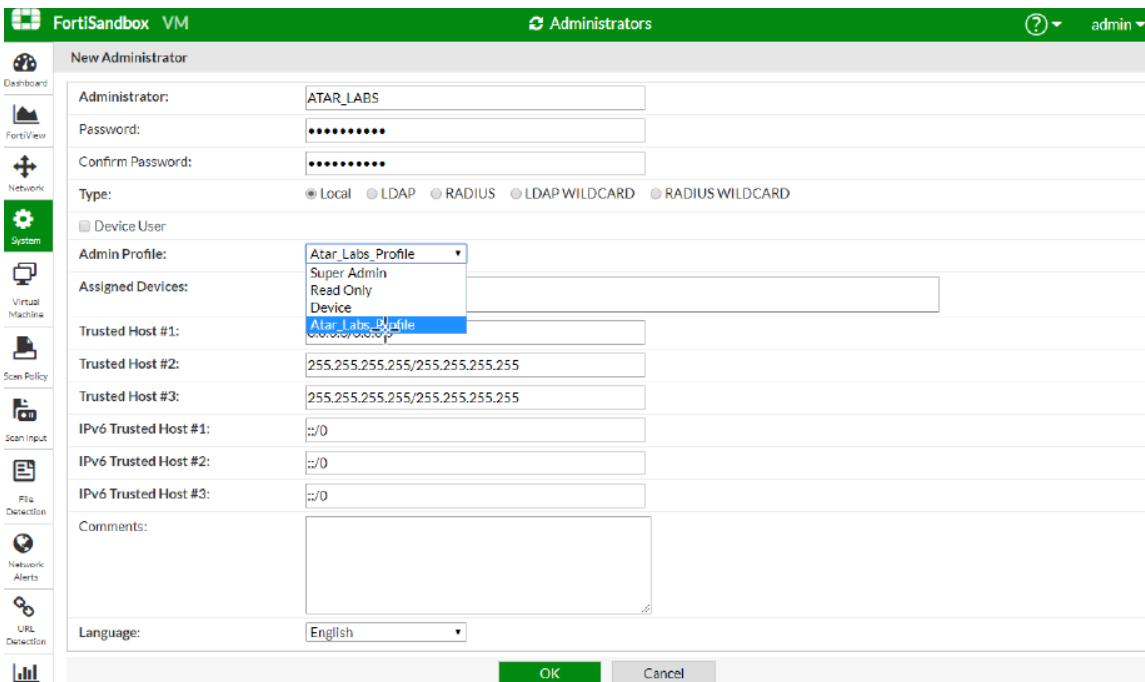
1. Navigate to **System > Admin Profiles**.
2. Create an Admin Profile with **Read/Write permission** for **SCAN INPUT** and select **Enable** for **JSON API**.

Menu Access			
	None	Read Only	ReadWrite
Dashboard	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
FortiView	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
Network	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
System	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
Virtual Machine	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
Scan Policy	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
Scan Input	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
HA Cluster	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
File Detection	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
Network Alerts	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
URL Detections	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
Logs & Reports	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>

Control Access		
	Disable	Enable
Mark FPN	<input type="radio"/>	<input checked="" type="radio"/>
Download Original File	<input type="radio"/>	<input checked="" type="radio"/>
JSON API	<input type="radio"/>	<input checked="" type="radio"/>

3. Navigate to **System > Administrators**.
4. Create an **Administrator** account with the profile that is created in the previous step and specify the following values:
  - **Administrator:** SOAR\_LABS
  - **Password:** <Specify the password>
  - **Confirm Password:** <Confirm the password specified in the Password field>
  - **Type:** Select **Local**
  - **Admin Profile:** <Specify the profile name>



## Configuring SOAR

1. Click **Configuration > Credentials > Create Credential**.
2. Specify the following parameter values in the **Credential Editor**:

a. **Internal Credential**

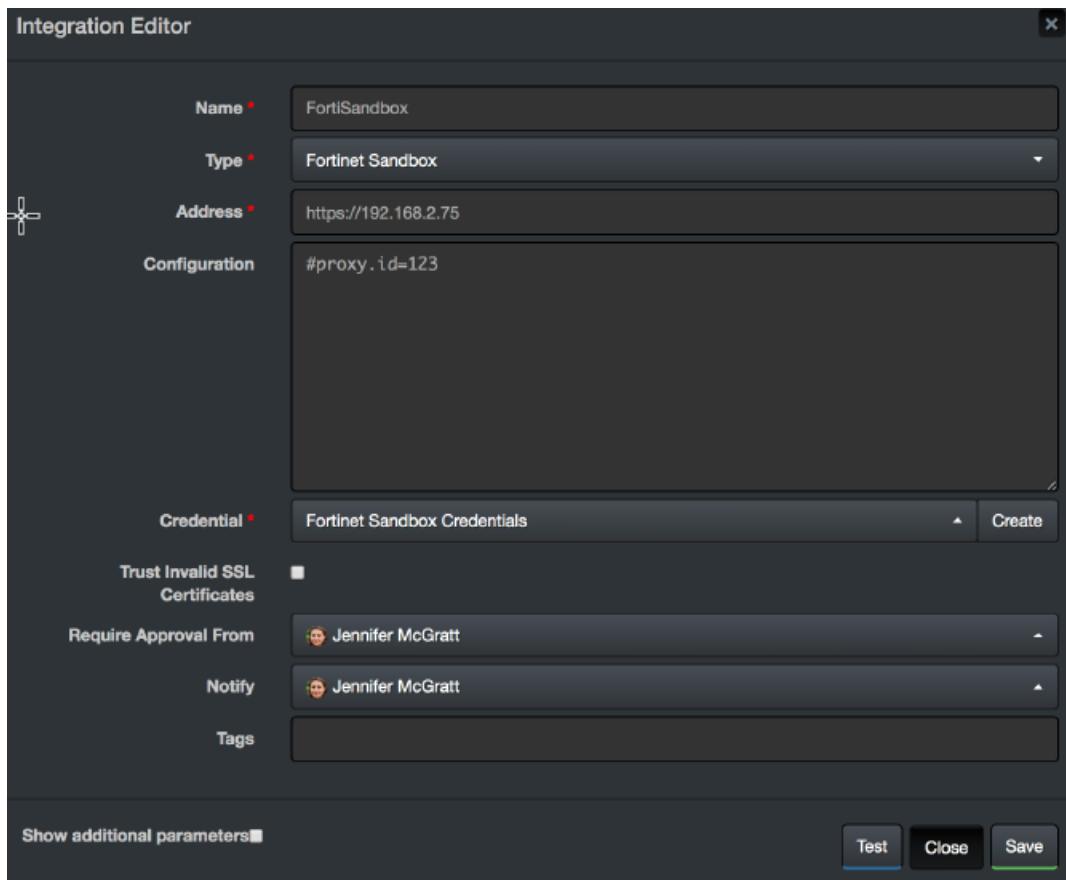
Parameter	Value
Type	Internal Credential
Name	Display name of credential set (For example, Fortinet Sandbox Credentials)
Username	User that was created on Fortinet Sandbox for SOAR
Password	Password of the user that was created for SOAR on Fortinet Sandbox
Private Key	Empty

b. **Credential Store:**

Parameter	Value
Type	External Credential
Name	Name of the credential with pull path of the safe on store

3. Click **Configuration > Integrations > Create Integration**.
4. Specify the following parameter values in the **Configuration** form:

Parameter	Value
Name	Display name of Fortinet Sandbox integration on SOAR
Type	Fortinet Sandbox
Address	Address of the integration ( in the following format: https://192.168.2.75)
Configuration	Specify the following configuration parameters: #proxy.id=5442
Credential	Name of the credential set created on step 2 (For example, Fortinet Sandbox Credentials)
Trust Invalid SSL Certificates	Select this if Web UI's certificate certificate is self-signed or is not recognized by browsers
Require Approval From	Select users from the list who can provide approval before executing actions on this integration
Notify	Not Applicable



5. Click **Test** to test the integration.
6. Click **Save** to complete the integration.

## Additional Notes

Fortinet Sandbox supports the following compressed file types:

.tar, .z, .xz, .gz, .tar.gz, .tgz, .zip, .bz2, .tar.bz2, .tar.Z, .7z, .rar, .lzh, .ace

## Integration Guide for FraudGuard

FraudGuard is a service designed to provide an easy way to validate usage by continuously collecting and analyzing real-time internet traffic. Utilizing just a few simple API endpoints we make integration as simple as possible and return data such as: Risk Level, Threat Type, Geo Location

## Integration Capabilities

- Geo Lookup
- Get Host Reputation
- Get IP Reputation
- Add to Custom Blacklist
- Add to Custom Whitelist
- Delete From Custom Blacklist
- Delete From Custom Whitelist

## Prerequisites

You must have access to HTTPS as the ArcSight SOAR connects to FraudGuard API through this service.

## Configuring FraudGuard

1. Navigate to <https://api.fraudguard.io>.
2. Create a user account by setting your username and password.

# Configuring SOAR

1. Click **Configurations > Credentials > Create credentials**.
2. Specify the following parameter values in the **Credential Editor**:
  - Internal Credential

Parameter	Value
Type	Internal credential
Name	Display name of credential set(i.e, FraudGuard credentials)
Username	Username that you have noted from the service
Password	Password that you have noted from the service
Private Key	Empty

3. Click **Configuration > Integrations > Create Integration**.
4. Specify the following parameter values in the **Configuration** form:

Parameter	Value				
Name	Display name of FraudGuard integration on SOAR.				
Type	FraudGuard				
Address	<a href="https://api.fraudguard.io">https://api.fraudguard.io</a>				
Configuration	Specify the following configuration parameters: <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="padding: 5px;">proxy.id</td> <td style="padding: 5px;">ID of the Proxy integration if you access Fraudguard through a web proxy device. For example: proxy.id = 12345</td> </tr> <tr> <td style="padding: 5px;">cache.reusing.duration</td> <td style="padding: 5px;">configure how far (in minutes) into the past this enrichment will look.</td> </tr> </table>	proxy.id	ID of the Proxy integration if you access Fraudguard through a web proxy device. For example: proxy.id = 12345	cache.reusing.duration	configure how far (in minutes) into the past this enrichment will look.
proxy.id	ID of the Proxy integration if you access Fraudguard through a web proxy device. For example: proxy.id = 12345				
cache.reusing.duration	configure how far (in minutes) into the past this enrichment will look.				
Credential	Credential that has been defined for this integration under the credentials menu.				
Notify	Select user(s) from the list to notify when SOAR performs an action on this integration				

5. Click **Save** to save the integration definition.
6. Navigate to **Configuration > Customization Library**” and edit **Fraudguard Action Script Default Template**.
7. Select the integration you have added to **Integrations** dropdown menu.
8. Click **Save** to complete the integration.

# Capabilities

## 1. Geo Lookup

Enrichment capability for lookup of IP address.

Input Parameter	Description	Type	Scope Restricted(Yes/No)	Required (Yes/No)
<b>Integration</b>	Name of the 3rd party integration	Integration	N/A	Yes
<b>IP Address</b>	Scoped variable to store IP address	String	N/A	Yes

### Output:

Case Scope

N/A

Human Readable Output

Yes

## 2. Get Host Reputation

Enrichment capability for get host reputation and details.

Input Parameter	Description	Type	Scope Restricted(Yes/No)	Required (Yes/No)
<b>Integration</b>	Name of the 3rd party integration	Integration	N/A	Yes
<b>Hostname</b>	Scoped Parameter to store host address.	String	N/A	Yes

### Output:

Case Scope

N/A

Human Readable Output

Yes

## 3. Get IP Reputation

Enrichment capability for Getting IP details from fraudguard.

Input Parameter	Description	Type	Scope Restricted(Yes/No)	Required (Yes/No)
<b>Integration</b>	Name of the 3rd party integration	Integration	N/A	Yes
<b>IP Address</b>	Scoped Parameter IP Address.	String	N/A	Yes

**Output:**

Case Scope

N/A

Human Readable Output

Yes

**4. Add to Custom Blacklist**

Action capability for Adding an IP to blacklist.

- Rollback: Yes

Input Parameter	Description	Type	Scope Restricted(Yes/No)	Required (Yes/No)
<b>Rollback Mode</b>	Time to rollback this action. Default is no-rollback.	N/A	N/A	No
<b>IP Address</b>	IP Address to be added to the blacklist eg: 0.0.0.0/0	String	N/A	Yes

**Output:**

Case Scope

N/A

Human Readable Output

N/A

**5. Add to Custom Whitelist**

Action capability for Adding an IP to whitelist.

- Rollback: Yes

Input Parameter	Description	Type	Scope Restricted(Yes/No)	Required (Yes/No)
<b>Rollback Mode</b>	Time to rollback this action. Default is no-rollback.	N/A	N/A	No
<b>IP Address</b>	IP Address to be added to the whitelist eg: 0.0.0.0/0	String	N/A	Yes

**Output:**

Case Scope

N/A

Human Readable Output

N/A

**6. Delete From Custom Blacklist**

Action capability for Deleting an IP from blacklist.

- Rollback: Yes

Input Parameter	Description	Type	Scope Restricted(Yes/No)	Required (Yes/No)
<b>Rollback Mode</b>	Time to rollback this action. Default is no-rollback.	N/A	N/A	No
<b>IP Address</b>	IP Address to be removed from the blacklist eg: 0.0.0.0/0	String	N/A	Yes

**Output:**

Case Scope

N/A

Human Readable Output

N/A

**7. Delete From Custom Whitelist**

a. Action capability for Deleting an IP from whitelist.

- Rollback: Yes

<b>Input Parameter</b>	<b>Description</b>	<b>Type</b>	<b>Scope Restricted(Yes/No)</b>	<b>Required (Yes/No)</b>
<b>Rollback Mode</b>	Time to rollback this action. Default is no-rollback.	N/A	N/A	No
<b>IP Address</b>	IP Address to be removed from the whitelist eg: 0.0.0.0/0	String	N/A	Yes

**Output:**

Case Scope

N/A

Human Readable Output

N/A

# Integration Guide for FTP Server

## Integration Overview

ArcSight SOAR uses FTP Servers to put or transfer files to remote machines using incident scope.

## Integration Capabilities

### Action

- Put File

## Configuration

### Prerequisites

- Access to File Transfer Protocol or SFTP as SOAR connects to FTP Server using it
- A user's credential

## Configuring SOAR

1. To create the integration, navigate to **Configuration > Integrations**.
2. Specify the following parameter values in the **Integrations Editor** form.

Parameter	Value
Name	Display name of the integration
Type	FTP Server
Address	Address of the integration (in the format: 1.1.1.1 or abc.example.com)

Parameter	Value
Configuration	<p>Specify the following configuration parameters:</p> <pre>connection.port is the listening port of the FTP/SFTP service running. connection.protocol could be FTP or SFTP. remote.file.filename.appenduuid specifies whether the UUID will be appended to the filename. It can be either "true" or "false". remote.folder is the folder relative to the FTP home directory.</pre>
Credential	Credential that was defined for this integration under the <b>Credentials</b> menu
Trust Invalid SSL Certificates	Select this if device's certificate is self-signed or is not recognized by browsers
Require Approval From	Select users from the list who can provide approval before executing actions on this integration
Notify	Select users from the list to notify when SOAR performs an action on this integration

**Integration Editor**

Name *	FTP Server
Type *	FTP Server
Address *	abc.example.com
Configuration	<pre>connection.port=21 connection.protocol=FTP remote.file.filename.appenduuid=false remote.folder=/</pre>
Credential *	FTP Server <span style="float: right;">Create</span>
Trust Invalid SSL Certificates	<input checked="" type="checkbox"/>
Require Approval From	No selected principal
Notify	No selected principal
Tags	
<a href="#">Show additional parameters</a> <span style="float: right;"><b>Test</b> <b>Close</b> <b>Save</b></span>	

3. Click **Test** to test the integration.
4. Click **Save** to complete integration.

# Integration Guide for Google Cloud Compute

## Integration Overview

Google Cloud Compute, also known as Google Compute Engine (GCE), is a part of the Google Cloud Platform (GCP) that provides scalable and flexible virtual machine (VM) instances in the cloud. It enables users to run their applications and workloads on virtual machines hosted on Google's infrastructure.

## Integration Capabilities

ArcSight SOAR has the following integration capabilities with Google Cloud Compute:

- List Instance
- Get Instance Details
- Get IAM Policy
- Get Screenshot
- Start Instance
- Stop Instance
- Suspend Instance

## Prerequisites

- You must have access to HTTPS as the ArcSight SOAR connects to Google Cloud Compute API through this service.

## Configuration

### Configuring Google Cloud Compute

**Authentication:** This integration includes OAuth 2.0 flow. OAuth 2.0 flow is specifically for user authorization. It is designed for applications that can store confidential information and maintain state.

A properly authorized web server application can access an API while the user interacts with the application.

Any application that uses OAuth 2.0 to access Google APIs must have authorization credentials that identify the application to Google's OAuth 2.0 server.

To create credentials perform the following steps:

1. Click [Credentials page](#).
2. Click Create credentials > OAuth client ID.
3. Select Web application.
4. Fill in the form and click Create. Applications that use languages and frameworks like PHP, Java, Python, Ruby, and .NET must specify authorized redirect URIs. The redirect URIs are the endpoints to which the OAuth 2.0 server can send responses. These endpoints must adhere to [Google's validation rules](#).

For testing, you can specify URIs that refer to the local machine, such as <https://localhost/arcsightsoar>. With that in mind, please note that all the examples in this document use <https://localhost/arcsightsoar> as the redirect URI.

5. After creating your credentials, download the client\_secret.json file from the API Console. Securely store the file in a location that only your application can access.

Authorization Parameters:

Parameters	Description	DataType	Required
client_id	The client ID for your application. You can find this value in the API Console <a href="#">Credentials page</a> .	String	Yes
scope	A space-delimited list of scopes that identify the resources that your application could access on the user's behalf. These values inform the consent screen that Google displays to the user.	String	No
redirect_uri	Determines where the API server redirects the user after the user completes the authorization flow. The value must exactly match one of the authorized redirect URIs for the OAuth 2.0 client, which you configured in your client's API Console <a href="#">Credentials page</a> . If this value doesn't match an authorized redirect URI for the provided client_id you will get a redirect_uri_mismatch error.  Note that the http or https scheme, case, and trailing slash ('/') must all match.	String	Yes
response_type	Determines whether the Google OAuth 2.0 endpoint returns an code. Set the parameter value to code for web server applications.	Yes	No

Parameters	Description	DataType	Required
grant_type	Must be set to client credentials.	String	Yes
access_type	Indicates whether your application can refresh access tokens when the user is not present at the browser. Valid parameter values are online, which is the default value, and offline.	String	No
prompt	consent Prompt the user for consent.	String	No

On the last page, you will see the access key id and the secret code. You will need to save them somewhere securely.

1. To Obtain refresh token follow the below steps:
  - a. This plugin has an Oauth 2.0 mechanism.
  - b. The users should get Authorization Code obtaining Authorization Code User must follow these below steps.
  - c. The Authorization Code is needed to get the Refresh Token. For this the below URL can be used.
  - d. Copy the below command URL and update your <client\_id>.



It is advisable to copy the URL to a text editor and the modifications made. After making the changes, copy and paste the URL to a browser.

```
https://accounts.google.com/o/oauth2/auth?response_type=code&client_id=<client_id>&scope=https://www.googleapis.com/auth/compute
https://www.googleapis.com/auth/compute.readonly https://www.googleapis.com/auth/cloud-platform
https://www.googleapis.com/auth/iam&redirect_uri=https://localhost/arcsightsoar&access_type=offline&prompt=consent
```

- e. The browser would redirect to the redirect\_uri with a code in the address bar. Refer to the below image
- f. Exchange authorization code for refresh token and access tokens:



Authorization code is short lived. Typically, they expire after about 10 minutes or one time use.

Parameters	Description	DataType	Required
client_id	The client ID obtained from the API Console <a href="#">Credentials page</a> .	Yes	Yes
client_secret	The client secret obtained from the API Console <a href="#">Credentials page</a> .	Yes	Yes

code	The authorization code returned from the initial request. (brower) Note: - Authorization codes are short lived. Typically, they expire after about 10 minutes or one time use.	Yes	Yes
grant_type	This field's value must be set to authorization_code.	Yes	No
redirect_uri	One of the redirect URIs listed for your project in the API Console <a href="#">Credentials page</a> for the given inside OAuth 2.0 Client ID and you must to create this redirect uri <a href="https://localhost/arcsightsoar">https://localhost/arcsightsoar</a> and Internally we are kept the redirect uri static	Yes	No

- g. Download the [Curl\\_command](#)file and provide below mentioned key values.
- h. Provide the values client\_id,client\_secret and Authorization code based on the organization specific configurations. It would be better than the CURL command file. Download and provide key values (client\_id,client\_secret and Authorization code). After making the changes, copy and paste the command to the terminal.
- i. Check for the key word refresh\_token in the command response and copy the values of the refresh token.
- j. After copying refresh token values from the command, paste the refresh token values to the ArcSight SOAR configuration in the credential section. Now you can see your plugin name credential. This is done on the private key section under the credentials section. Refer to the screen image given below.
- k. Save the Credential Editor

Additional Configuration:

Configuration Parameter	Description
proxy.id	Proxy device to be used while communicating with the remote system's API
cache.reusing.duration	Default cache-reuse parameter

## Configuring SOAR

1. Click Configuration > Credentials > Create Credentials.
2. Specify the following parameters values in the Credential Editor form.

Type	Name	Username	Password	Private Key
Internal credential	Display name of credential set (for example, Google Cloud Compute Credentials).	The client ID obtained from the API Console <a href="#">Credentials page</a> .	The client secret obtained from the API Console <a href="#">Credentials page</a> .	Refresh token here generating from Curl

3. Select your integration plugin zip file and click on Save.
4. Select the integration that you have added to the Integrations menu.
5. Click Save to complete the integration.
6. Click Test, an Integration Successful message is displayed if the credential and address are valid.

## Integration Capabilities:

### 1. List Instance

Enrichment capability to retrieve the list of instances contained within the specified zone.

**Input Parameters:**

Parameter	Description	Data Type	Scope Restricted	Required
Zone	The name of the zone for this request.	String	No	Yes
Project	Project ID for this request.id will get it from Google cloud compute plugin integration configuration section	String	No	Yes

**Query Parameters:**

Parameter	Description	Data Type	Scope Restricted	Required
maxResults	The maximum number of results per page that should be returned.	Integer	No	No
pageToken	Specifies a page token to use. Set pageToken to the nextPageToken returned by a previous list request to get the next page of results.	String	No	No

**Request headers:**

Header	Value	Required
Authorization	Bearer {token}	Yes

**Output:**

Case Scope: N/A

## Human Readable Output:

a few seconds ago - S sacumen executed List Instance enrichment on Google Cloud Compute							
Parameters Details		Search					
Name	Created	Labels	Status	Tags	Last Started	Last Stopped	Last Suspended
instance-1	2023-06-28T22:53:14.1 37-07:00	N/A	TERMINATED	[ "http-server" ]	2023-07-06T05:43:04.0 56-07:00	2023-07-07T00:23:44.8 18-07:00	N/A
instance-2	2023-06-28T23:04:07.3 29-07:00	N/A	TERMINATED	[ "http-server" ]	2023-07-05T04:46:31.0 61-07:00	2023-07-05T04:47:47.8 26-07:00	2023-07-04T00:28:40.3 53-07:00
Total 2 , items / page		1					

## 2. Get Instance Details

Enrichment capability to return the specified Instance resource.

Input Parameters:

Parameter	Description	Data Type	Scope Restricted	Required
Instance Name	Name of the instance scoping this request.	COMPUTERNAME,KEYWORD,UNKNOWN	Yes	Yes
Zone	The name of the zone for this request.	String	No	Yes
Project	Project ID for this request.id will get it from integration configuration	String	No	Yes

Request headers

Header	Value	Required
Authorization	Bearer {token}	Yes

Output:

Case Scope: N/A

## Human Readable Output:

Parameters Details	
Key	Value
Kind	compute#instance
Name	instance-1
ID	5892723175077225127
Created	2023-06-28T22:53:14.137-07:00
Description	N/A
Tags	[ "http-server" ]
Machine Type	<a href="https://www.googleapis.com/compute/v1/projects/sacumen-vm-01/zones/us-central1-a/machineTypes/n2d-standard-2">https://www.googleapis.com/compute/v1/projects/sacumen-vm-01/zones/us-central1-a/machineTypes/n2d-standard-2</a>
Status	TERMINATED
Zone	<a href="https://www.googleapis.com/compute/v1/projects/sacumen-vm-01/zones/us-central1-a">https://www.googleapis.com/compute/v1/projects/sacumen-vm-01/zones/us-central1-a</a>
Can Ip Forward	false
Network Interfaces	[ [ "Interface Name:nic0", "Interface Network IP:10.128.0.2" ] ]

## 3. Get IAM Policy

Enrichment Capability Gets the access control policy for a resource. May be empty if no such policy or resource exists.

Input Parameters:

Parameter	Description	Data Type	Scope Restricted	Required
Instance Name	Name of the instance scoping this request.	COMPUTERNAME,KEYWORD,UNKNOWN	Yes	Yes
Zone	The name of the zone for this request.	String	No	Yes
Project	Project ID for this request.id will get it from integration configuration	String	No	Yes

Request headers

Header	Value	Required
Authorization	Bearer {token}	Yes

Output:

Case Scope: N/A

### Human Readable Output:

Parameters Details		
Roles	Members	Condition
roles/compute.admin	[ "user:abdu.shuaib@sacumen.com", "user:revanasidda.m@sacumen.com" ]	N/A
roles/compute.instanceAdmin.v1	[ "user:revanasidda.m@sacumen.com" ]	N/A
roles/owner	[ "user:abdu.shuaib@sacumen.com", "user:revanasidda.m@sacumen.com" ]	N/A
roles/resourcemanager.tagUser	[ "user:abdu.shuaib@sacumen.com" ]	N/A

Total 4 , Items / page 1

### 4. Get Screenshot

Enrichment capability to get the screenshot from the specified instance.



Obtain the instance screenshot only if the Display Device is enabled and the instance is running.

#### Input Parameters:

Parameter	Description	Data Type	Scope Restricted	Required
Instance Name	Name of the instance scoping this request.	COMPUTERNAME,KEYWORD,UNKNOWN	Yes	Yes
Zone	The name of the zone for this request.	String	No	Yes
Project	Project ID for this request.id will get it from integration configuration	String	No	Yes

#### Request headers:

Header	Value	Required
Authorization	Bearer {token}	Yes

#### Output:

Case Scope: N/A

Human Readable Output:



## 5. Start Instance

Action Capability to start the specified instance.

Rollback: Yes

Duplicate Control: No

Input Parameters:

Parameter	Description	Data Type	Scope Restricted	Required
Instance Name	Name of the instance scoping this request.	COMPUTERNAME,KEYWORD,UNKNOWN	Yes	Yes
Zone	The name of the zone for this request.	String	No	Yes
Project	Project ID for this request.id will get it from integration configuration	String	No	Yes

Request headers:

Header	Value	Required
Authorization	Bearer {token}	Yes

Output:

Case Scope: N/A

Human Readable Output: N/A

## 6. Stop Instance

Action Capability to stop the specified instance.

Rollback: Yes

Duplicate Control: No

Input Parameters:

Parameter	Description	Data Type	Scope Restricted	Required
Instance Name	Name of the instance scoping this request.	COMPUTERNAME,KEYWORD,UNKNOWN	Yes	Yes
Zone	The name of the zone for this request.	String	No	Yes
Project	Project ID for this request.id will get it from integration configuration	String	No	Yes

Request headers

Header	Value	Required
Authorization	Bearer {token}	Yes

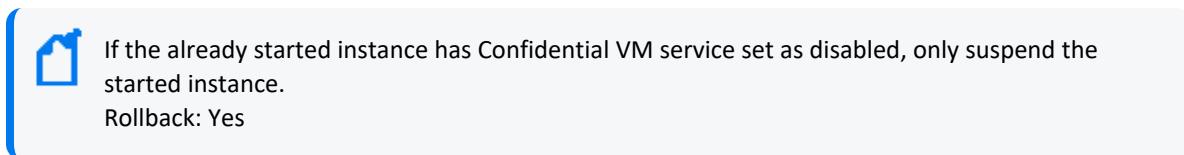
Output:

Case Scope: N/A

Human Readable Output: N/A

## 7. Suspend Instance

Action Capability to Suspend the specified instance.



Duplicate Control: No

Input Parameters:

Parameter	Description	Data Type	Scope Restricted	Required
Instance Name	Name of the instance scoping this request.	COMPUTERNAME,KEYWORD,UNKNOWN	Yes	Yes
Zone	The name of the zone for this request.	String	No	Yes
Project	Project ID for this request.id will get it from integration configuration	String	No	Yes

### Request headers

Header	Value	Required
Authorization	Bearer {token}	Yes

Output:

Case Scope: N/A

Human Readable Output: N/A

# Integration Guide for Have I Been Pwned

## Integration Overview

**Have I Been Pwned** is a web service that allows to check if the emails/usernames are exposed as part of previous data breaches.

This integration supports Have I Been Pwned API v3.

## Integration Capabilities

ArcSight SOAR has the following integration capabilities with Have I Been Pwned:

- Check Pwned Accounts
- Check Pwned Pastes
- Check Pwned Domains

## Prerequisites

Have I Been Pwned requires an API key for access.

## Configuration

### Configuring SOAR

1. Click **Configuration > Credential > Create Credential**.
2. Specify the following parameter values in the **Credential Editor** form:

Type	Name	Username	Password	Private Key
Internal credential	Display name of credential set (i.e., Have I Been Pwned Credentials)			API Key

3. Click **Configuration > Integrations > Create Integration**.

4. Specify the following parameter values in the **Configuration Form**:

Parameter	Value	
Name	Display name of the integration	
Type	Have I Been Pwned	
Address	Address of the integration ( <a href="https://haveibeenpwned.com/">https://haveibeenpwned.com/</a> )	
Configuration	Specify the following configuration parameters:	
	proxy.id	Access the ID of the Proxy integration <a href="#">Have I Been Pwned</a> through a web proxy device. For example: proxy.id = 12345
Credential	Credential that has been defined for this integration under the Credentials menu.	
Trust Invalid SSL Certificates	Select this if web server's certificate is self-signed or is not recognized by browsers.	
Require Approval From	Since there is no action capability in this plugin, please leave it empty.	
Notify	Since there is no action capability in this plugin, please leave it empty.	

5. Click **Save** to save the integration definition.
6. Navigate to **Configuration>Customization Library** and edit **Have I Been Pwned Advanced Action Script Default Template**.
7. Select the integration you have added to **Integrations** menu.
8. Click **Save** to complete the integration.
9. Click **Test**. **Integration Successful** message is displayed if your credential and address are valid.

## Capabilities

### 1. Check Pwned Accounts

Enrichment capability for gathering pwned account details.

The following table presents the **Check Pwned Accounts** action capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Integration</b>	Name of the third party integration	Integration	N/A	Yes
<b>Email Address</b>	Email address to be queried	Email Address Username Keyword Unknown	Yes	Yes
<b>Do not Use Cache</b>	SOAR does not use cached results if this box is checked	Checkbox	N/A	No

**Output:**

Case Scope: N/A

**Human Readable Output:**

Breach	Date	Description
Anti Public Combo List	2016-12-16	In December 2016, a huge list of email address and password pairs appeared in a "combo list" referred to as "Anti Public". The list contained 458 million unique email addresses, many with multiple different passwords hacked from various online systems. The list was broadly circulated and used for credential stuffing, that is attackers employ it in an attempt to identify other online systems where the account owner had reused their password. For detailed background on this incident, read <a href="https://www.troyhunt.com/password-reuse-credential-stuffing-and-another-1-billion-records-in-have-i-been-pwned" rel="noopener" target="_blank">Password reuse, credential stuffing and another billion records in Have I Been Pwned</a> .
Apollo	2018-07-23	In July 2018, the sales engagement startup <a href="https://www.wired.com/story/apollo-breach-linkedin-salesforce-data/" rel="noopener" target="_blank">Apollo</a> left a database containing billions of data points publicly exposed without a password. The data was discovered by security researcher <a href="http://www.vinnytrola.com/" rel="noopener" target="_blank">Vinny Troia</a> who subsequently sent a subset of the data containing 126 million unique email addresses to Have I Been Pwned. The data left exposed by Apollo was used in their "revenue acceleration platform" and included personal information such as names and email addresses as well as professional information including places of employment, the roles people hold and where they're located. Apollo stressed that the exposed data did not include sensitive information such as passwords, social security numbers or financial data. <a href="https://www.apollo.io/contact" rel="noopener" target="_blank">The Apollo website has a contact form</a> for those looking to get in touch with the organisation.

**2. Check Pwned Domains**

Enrichment capability for gathering pwned domain details.

Following is the **Check Pwned Domains** enrichment capability details.

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Integration</b>	Name of the third party integration	Integration	N/A	Yes
<b>Domain</b>	Domain to be queried	Domain Keyword Unknown	Yes	Yes
<b>Do not Use Cache</b>	SOAR does not use cached results if this box is checked	Checkbox	N/A	No

**Output:**

Case Scope: N/A

Human Readable Output:

Breach	Domain	Date	Description
Acne.org	acne.org	2014-11-25	In November 2014, the acne website <a href="http://www.acne.org/" target="_blank" rel="noopener">acne.org</a> suffered a data breach that exposed over 430k forum members' accounts. The data was being actively traded on underground forums and included email addresses, birth dates and passwords.

### 3. Check Pwned Pastes

Enrichment capability for listing the paste sites that pwned account is mentioned.

Following is the **Check Pwned Pastes** enrichment capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
Integration	Name of the third party integration	Integration	N/A	Yes
Email Address	Email address to be queried	Email Address Username Keyword Unknown	Yes	Yes
Do not Use Cache	SOAR does not use cached results if this box is checked	Checkbox	N/A	No

### Output:

Human Readable Output:

Source	Paste Title	Id	Date
AdHocUrl	www.pemiblanc.com	http://www.pemiblanc.com/test.txt	
Pastebin	Braydoon	SvZR2M9L	2014-05-12T22:05:00Z
Pastebin	alibudgoadgb	jdDgA26z	2014-07-04T22:07:00Z
Pastebin	something	z6fMvVdt	2014-07-12T21:07:00Z
Pastebin	WARZ ACCOUNTS	4jy1VNct	2014-12-05T01:12:00Z
Pastebin	Funny Passwords	mUKY4AL5	2014-12-30T19:15:00Z
Pastebin		1a33mzkW	2015-01-06T08:56:00Z
Pastebin	//3x0// R  =3G5	5FCp5Dxc	2015-02-12T19:02:00Z
Pastebin	//3x0// R  =3G5.	WKpdpyEM	2015-02-12T19:03:00Z
Pastebin	10k+ US Combolist	Qm1yQmVb	2015-07-12T03:33:10Z
Pastebin		1v22W7TG	2018-08-12T15:19:16Z

# Integration Guide for Generic HTTP SMS Gateway

## Integration Overview

ArcSight SOAR uses Generic HTTP SMS (Short Message Service) Gateway to send SMS.

## Integration Capabilities

- None

## Configuration

### Configuring Generic HTTP SMS Gateway

- Access to **File HTTPS** service as SOAR uses it to connect to Generic HTTP SMS Gateway
- A SOAR user account

### Configuring SOAR

1. To create the integration, navigate to **Configuration > Integrations**.
2. Specify the following parameter values in the **Integrations Editor** form.

Parameter	Value
Name	Display name of the integration
Type	Generic HTTP SMS Gateway
Address	Address of the integration (in the following format: 1.1.1.1 or abc.example.com)
Configuration	Specify the following configuration parameters: <pre>http.method = POST http.auth.enabled = false params.jobID = \${credential.privateKey} params.url = http://dev.swh.soarlabs.io/atar/ params.username = \${credential.username} params.text = \${text} params.gsmNumber = \${recipient} http.header.User-Agent = SOAR http.header.Content-Type = application/x-www-form-urlencoded sms.stripCountryCode = +90</pre>

Parameter	Value
Credential	Credential that was defined for this integration under the <b>Credentials</b> menu
Trust Invalid SSL Certificates	Select this if device's certificate is self-signed or is not recognized by browsers
Require Approval From	Select users from the list who can provide approval before executing actions on this integration
Notify	Select users from the list to notify when SOAR performs an action on this integration

3. Click **Test** to test the integration.
4. Click **Save** to complete integration.

# Integration Guide for HTTP Proxy

## Integration Overview

ArcSight SOAR uses HTTP proxies to access HTTP services. Some integration plugins are capable of accessing resources on the Internet or other networks through a proxy device configuration. See the respective integration guides for configuring the proxy.

## Configuration

### Prerequisites

- Access to proxy service for SOAR
- A user account to connect to proxy if proxy authentication enabled

## Configuring HTTP Proxy

HTTP Proxy software must be configured to get the access to SOAR. You can consult the system to know the HTTP Proxy used in the network.

## Configuring SOAR

1. Click **Configuration > Credentials > Create Credential**.
2. Specify the following parameter values in the **Credential Editor**:

#### Internal Credential

Parameter	Value
Type	Internal Credential
Name	Display name of credential set (for example, HTTP Proxy Credentials)
Username	User that was created on HTTP proxy software for SOAR
Password	Password of the user that was created on HTTP proxy software for SOAR
Private Key	Empty

3. Click **Configuration > Integrations > Create Integration**.
4. Specify the following parameter values in the **Configuration** form:

Parameter	Value
Name	Display name of HTTP Proxy integration on SOAR
Type	HTTP Proxy
Address	Address of the integration (in the following format: https://192.168.1.3:8081)
Configuration	<p>Specify the following configuration parameters:</p> <pre># Supported values: basic, ntlm, none # For NTLM, username in credential should be specified like: username@domain authentication.type=basic # URL to use when testing availability of this proxy integration. # Defaults to the value of HttpProxyCheckURL configuration parameter.</pre>
Credential	Name of the credential set created on step 2 (For example, HTTP Proxy Credentials)
Trust Invalid SSL Certificates	Select this if Web UI's certificate certificate is self-signed or is not recognized by browsers
Require Approval From	Select users from the list who can provide approval before executing actions on this integration
Notify	Select users from the list to notify when SOAR performs an action on this integration

5. Click **Test** to test the integration.
6. Click **Save** to complete the integration.

## Additional Notes

For SOAR to perform Automatic Update Checks, navigate to **Configuration > Parameters** and set `ProxyIntegrationIdForAutomaticUpdateCheck`.

# Integration Guide for IBM Security X-Force

## Integration Overview

IBM X-Force Exchange is a cloud-based threat intelligence platform that enables users to research security threats, search attack indicators, aggregate actionable intelligence, and collaborate with peers.

## Integration Capabilities

ArcSight SOAR has the following integration capabilities with IBM X-Force Exchange:

- DNS Records
- IP Report
- Malware for File Hash
- Send File for Analysis
- URL Report

### Use Case: Investigating Phishing Campaigns

SOAR follows the user's email inbox for phishing reports and automatically creates an incident record on its service desk. While investigating the attack, SOAR extracts the sender address, IP address, URLs in the message body, files in the attachment, and checks with IBM X-Force Exchange if these attacks are previously analyzed. This investigation can either be performed automatically within a playbook or manually by an analyst.

## Configuration

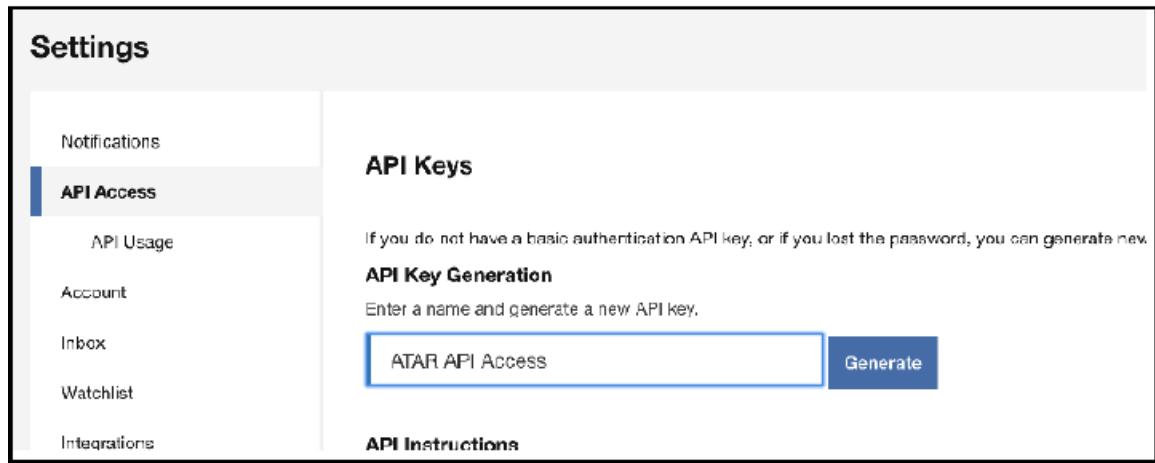
### Prerequisites

- Access to <https://api.xforce.ibmcloud.com> (443/tcp port) for SOAR to connect to IBM X-Force Exchange API
- An API key for SOAR to connect to IBM X-Force Exchange

## Configuring IBM X-Force Exchange

1. Log in to <https://exchange.xforce.ibmcloud.com>.
2. To create a new API key, navigate to **Settings > API Access**.

 Note: Save the generated API key and the password.



The screenshot shows the 'Settings' page with the 'API Access' tab selected. On the left, there's a sidebar with links for Notifications, API Usage, Account, Inbox, Watchlist, and Integrations. The main area is titled 'API Keys' and contains instructions for generating a basic authentication API key. It has a text input field labeled 'ATAR API Access' and a blue 'Generate' button. Below the input field, there's a link 'API Instructions'.

## Configuring SOAR

1. Click **Configuration > Credentials > Create Credential**.
2. Specify the following parameter values in the **Credential Editor**:

### a. Internal Credential

Parameter	Value
Type	Internal Credential
Name	Display name of credential set (For example, IBM X-Force Exchange Credentials)
Username	API Key created on IBM X-Force Exchange
Password	API Password for the key created on IBM X-Force Exchange
Private Key	Empty

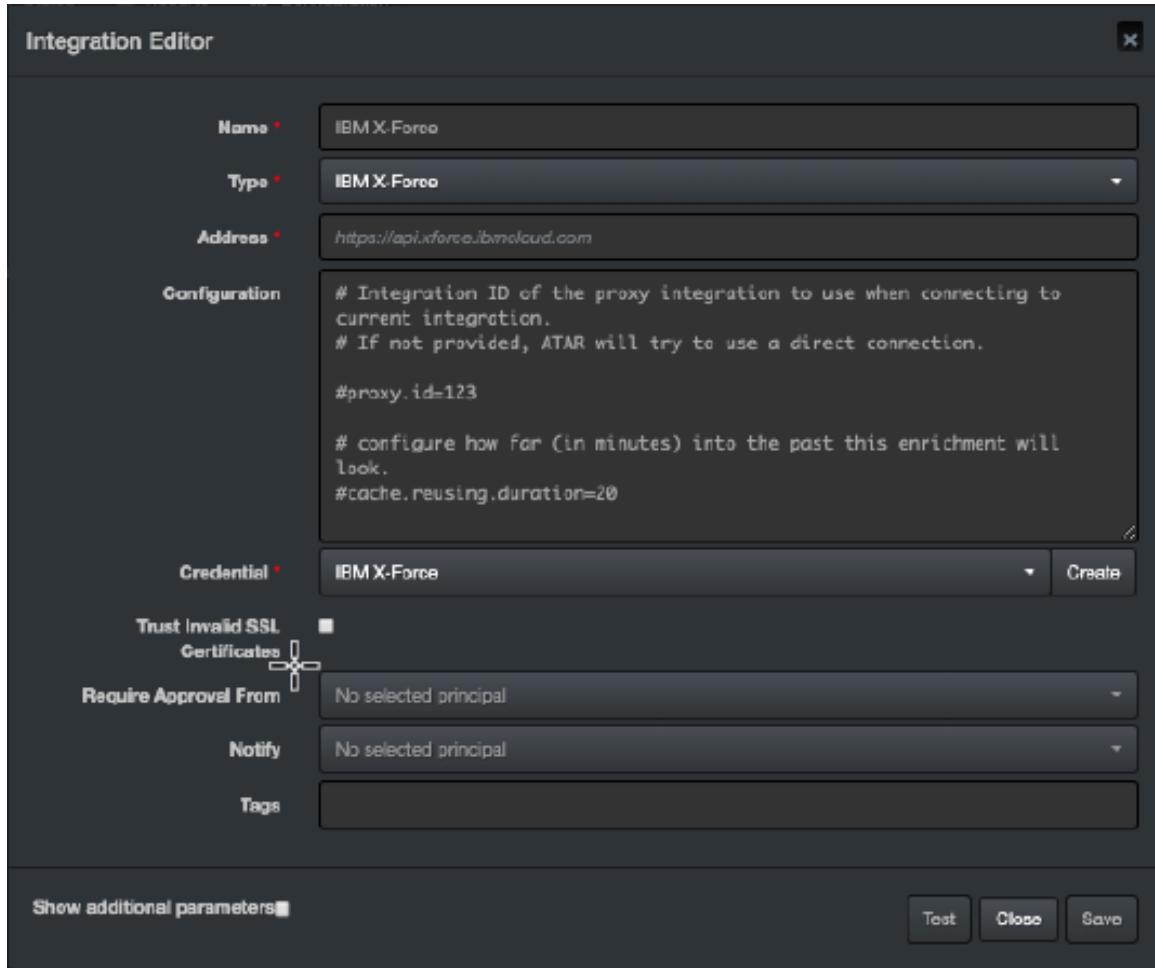
### b. Credential Store:

Parameter	Value
Type	External Credential
Name	Name of the credential with pull path of the safe on store

3. Click **Configuration > Integrations > Create Integration**.

4. Specify the following parameter values in the **Configuration** form:

Parameter	Value
Name	Display name of IBM X-Force Exchange integration on SOAR
Type	IBM X-Force Exchange
Address	Address of the integration ( <a href="https://api.xforce.ibmcloud.com">https://api.xforce.ibmcloud.com</a> )
Configuration	<p>Specify the following configuration parameters:</p> <pre># Integration ID of the proxy integration # to use when connecting # to current integration. # If not provided, SOAR will try to use # a direct connection. #proxy.id=123 # configure how far (in minutes) into the # past this enrichment will look. cache.reusing.duration=60</pre>
Credential	Name of the credential set created on step 2 (For example, IBM XForce Exchange Credentials)
Trust Invalid SSL Certificates	Select this if Web UI's certificate is self-signed or is not recognized by browsers
Require Approval From	Select users from the list who can provide approval before executing actions on this integration
Notify	Select users from the list to notify when SOAR performs an action on this integration



5. Click **Test** to test the integration.
6. Click **Save** to complete the integration.

# Integration Guide for Infoblox DNS Firewall

## Integration Overview

Infoblox DNS Firewall defends DNS servers from the comprehensive range of DNS-based attacks while maintaining service availability and business continuity. The Grid Manager web interface provides access to the appliance for network and IP address management.

## Integration Capabilities

ArcSight SOAR has the following integration capabilities with Infoblox DNS Firewall:

- Block IP address (No Data)
- Block IP Address (No Such Domain)
- Block Host (No Data)
- Block Host (No Such Domain)
- Substitute DNS A Record

### Use Case: Blocking malicious IP addresses on DNS

SOAR integrates with Infoblox DNS firewall to block malicious IP addresses and hosts on DNS firewall to stop malware attacks and protect users. These actions can either be performed automatically within a playbook or manually by an analyst.

## Configuration

### Prerequisites

- Infoblox NIOS 8.4 version
- Access to tcp port 443 as SOAR connects to Infoblox DNS Firewall API
- A SOAR user account to connect Infoblox DNS Firewall

## Configuring Infoblox DNS Firewall

1. Navigate to **Administration > Administrators > Admins**.
2. To add an account, specify the following values in the **Add Administrator Wizard**:  
**Authentication Type:** Local

**Login:** <Specify the username>

**Password:** <Specify the password>

**Confirm Password:** <confirm the password specified in **Password** field>

**Admin Group:** Select *admin-group*

3. To create a new Response Policy Zone, navigate to **Data Management > DNS > Response Policy Zones.**

## Configuring SOAR

1. Click **Configuration > Credentials > Create Credential.**
2. Specify the following parameter values in the **Credential Editor:**
  - a. **Internal Credential**

Parameter	Value
Type	Internal Credential
Name	Display name of credential set (For example, Infoblox DNS FW Credentials)
Username	User created for SOAR on Infoblox DNS FW
Password	API Password for the key created for SOAR on Infoblox DNS FW
Private Key	Empty

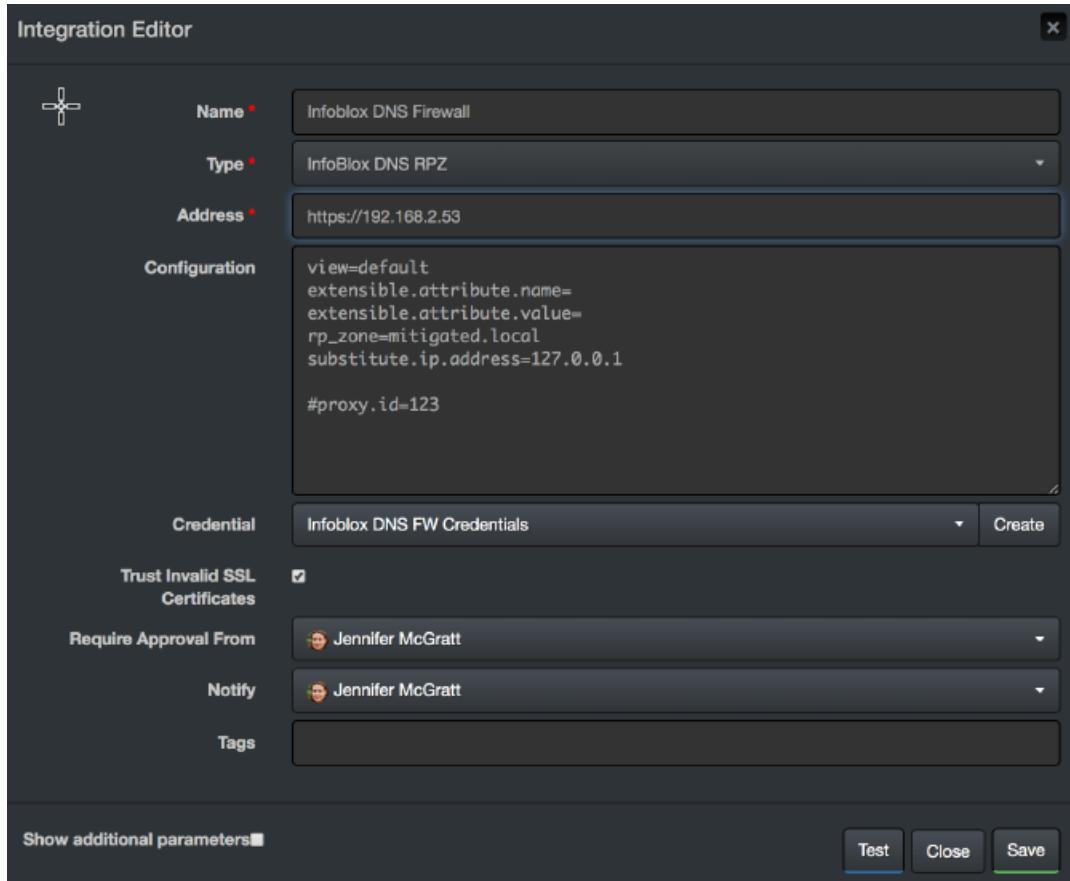
- b. **Credential Store:**

Parameter	Value
Type	External Credential
Name	Name of the credential with pull path of the safe on store

3. Click **Configuration > Integrations > Create Integration.**

4. Specify the following parameter values in the **Configuration** form:

Parameter	Value
Name	Display name of Infoblox DNS Firewall integration on SOAR
Type	Infoblox DNS Firewall
Address	Address of the integration (in the following format: https://192.168.2.53)
Configuration	<p>Specify the following configuration parameters:</p> <pre># Name of View under which rp_zone is located. view=default # Name of Response Policy Zone that SOAR will write block rules rp_zone=mitigated.local # Default name and value of extensible attribute which SOAR uses to write comment for block extensible.attribute.name= extensible.attribute.value= # IP address that SOAR uses to substitute in DNS A records. substitute.ip.address=127.0.0.1 #proxy.id=5442</pre>
Credential	Name of the credential set created on step 2 (For example, Infoblox DNS FW Credentials)
Trust Invalid SSL Certificates	Select this if Web UI's certificate is self-signed or is not recognized by browsers
Require Approval From	Select users from the list who can provide approval before executing actions on this integration
Notify	Select users from the list to notify when SOAR performs an action on this integration.



5. Click **Test** to test the integration.
6. Click **Save** to complete the integration.

## Additional Notes

Infoblox DNS Firewall allows blocking IP and host with only one rule type (either No Data or No Such Domain). If you try to block an IP or host that already got blocked with another rule type, you might get an error.

# Integration Guide for Intezer

## Integration Overview

Intezer is a malware analysis tool that automates alert triage, incident response and threat hunting.

# Integration Capabilities

ArcSight SOAR has the following integration capabilities with Intezer:

- Analyze Hash
- Get Sub-Analyses
- Get File Metadata
- Code Reuse Families
- Get Related Files

## Prerequisites

- ArcSight SOAR connects to the <https://analyze.intezer.com/> API through HTTPS. Access to this service is required.
- Intezer requires an API key for access.

## Configuration

### Configuring Intezer

- Intezer requires an API key for access.
- Users can obtain an API key from [intezer.com](https://intezer.com) after logging in with valid credentials.

### Configuring SOAR

1. Click **Configuration > Credential > Create Credential**.
2. Specify the following parameter values in the **Credential Editor**:

Type	Name	Username	Password	Private Key
Internal Credential	Display name of credential set ( for example Intezer).	Empty	Empty	API Key created on Intezer

3. Click **Configuration > Integrations > Create Integration**

**4. Specify the following parameter values in the Configuration Form:**

Parameter	Value
Name	Display name of the integration.
Type	Intezer.
Address	Address of the integration (the format must be https://s3.amazonaws.com).
Configuration	<p>Specify the following configuration parameters:</p> <pre># Integration ID of the proxy integration to use when connecting to current integration. # If not provided, ArcSight SOAR will try to use a direct connection. #proxy.id=123 # configure how far (in minutes) into the past this enrichment will look. #cache.reusing.duration=20</pre>
Credential	Name of the credential set created in step 2. (i.e. Intezer Credentials).
Trust Invalid SSL Certificates	Select this if Engine's certificate is self-signed or not recognized by browsers. Not selected.
Require Approval From	Select user(s) from list to ask the approval before executing actions on this integration.
Notify	Select user(s) from the list to notify when SOAR performs an action on this integration.

5. Click **Save**.
6. Navigate to **Configuration > Customization Library** and edit **Intezer Advanced Action Script Default Script Template**.
7. Select the integration that you have created in step 4 from the **Integrations** drop-down menu and click **Save**.
8. Click **Test**, an **Integration Successful** message is displayed if the credential and address are valid.

## Capabilities

### 1. Analyze Hash

Enrichment capability for retrieving details of a file hash.

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
Integration	Name of the 3rd party integration.	Integration	N/A	Yes
Hash	SHA256, SHA1, or MD5 hash value.	Hash	Yes	Yes
Do not Use Cache	SOAR does not use cached results if this box is checked.	Boolean	N/A	No

**Output:**

Case Scope

Action	Type	Category/Value
Add	Scope Item	Intezer Hash Value (SHA1, SHA256, MD5)
Set	Scope Item Property	Intezer Verdict
Set	Scope Item Property	Intezer Malware Family

Human Readable Output

**2. Get Sub-Analyses**

Enrichment capability for retrieving all sub-analyses of an Intezer analysis ID.

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
Integration	Name of the 3rd party integration.	Integration	N/A	Yes
Analysis ID	Intezer analysis ID. Can be retrieved from the human readable output of the 'Analyze Hash' enrichment.	String	No	Yes
Do not Use Cache	SOAR does not use cached results if this box is checked.	Boolean	N/A	No

**Output:**

Case Scope

N/A

Human Readable Output

**3. Get File Metadata**

Enrichment capability for retrieving the file metadata for an Intezer analysis ID and sub-analysis ID.

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
Integration	Name of the 3rd party integration.	Integration	N/A	Yes
Analysis ID	Intezer analysis ID. Can be retrieved from the human readable output of the 'Analyze Hash' enrichment.	String	No	Yes

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
Sub-Analysis ID	Intezer sub-analysis ID. Can be retrieved from the human readable output of the 'Get Sub-Analyses' enrichment.	String	No	Yes
Do not Use Cache	SOAR does not use cached results if this box is checked.	Boolean	N/A	No

**Output:**

Case Scope

Action	Type	Category/Value
None	N/A	N/A

Human Readable Output

**4. Code Reuse Families**

Enrichment capability for retrieving the malware family code reuse data for an Intezer analysis ID and sub-analysis ID.

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
Integration	Name of the 3rd party integration.	Integration	N/A	Yes
Analysis ID	Intezer analysis ID. Can be retrieved from the human readable output of the 'Analyze Hash' enrichment.	String	No	Yes
Sub-Analysis ID	Intezer sub-analysis ID. Can be retrieved from the human readable output of the 'Get Sub-Analyses' enrichment.	String	No	Yes

**Output:**

Case Scope

Action	Type	Category/Value
None	N/A	N/A

Human Readable Output

**5. Get Related Files**

<b>Input Parameter</b>	<b>Description</b>	<b>Type</b>	<b>Scope Restricted (Yes/No)</b>	<b>Required (Yes/No)</b>
Integration	Name of the 3rd party integration.	Integration	N/A	Yes
Analysis ID	Intezer analysis ID. Can be retrieved from the human readable output of the 'Analyze Hash' enrichment.	String	No	Yes
Sub-Analysis ID	Intezer sub-analysis ID. Can be retrieved from the human readable output of the 'Get Sub-Analyses' enrichment.	String	No	Yes
Family ID	Intezer family ID. Can be retrieved from the human readable output of the 'Code Reuse Families' enrichment.	String	No	Yes

**Output:**

Case Scope

N/A

Human Readable Output

# Integration Guide for Invictus USTA ThreatIntelligence

## Integration Overview

Invictus USTA is a threat intelligence service which delivers cyber-threat insights in real time.

## Integration Capabilities

- Ingest Threat Intelligence Feed as Alert
- Check Identity Leak
- Check Stolen Client Account
- Check Domain Info
- Check Hash Info
- Check IP Info
- Check URL Info
- Submit Bad Sender
- Submit Referer URL

### **Use Case: Blocking malicious URLs and IPs before they harm**

ArcSight SOAR integrates with USTA intelligence feed to block malicious entities on your perimeter protection before they harm.

### **Use Case #2: Investigating Fraud and ID Theft**

SOAR integrates with USTA Threat Intelligence to investigate fraud cases, possible ID theft, and cases of client account compromises.

## Configuration

### Prerequisites

- Access to <https://usta01.invictuseurope.com/api/> (443/tcp port) for SOAR to connect to USTA API
- An API Key for SOAR to connect to Invictus USTA API

## Configuring Invictus USPA

Invictus USTA requires no specific configuration.

## Configuring SOAR

1. Click **Configuration > Credentials > Create Credential**.
2. Specify the following parameter values in the **Credential Editor**:

### a. Internal Credential

Parameter	Value
Type	Internal Credential
Name	Display name of credential set (For example, Invictus USTA Credentials)
Username	Empty
Password	Empty
Private Key	API Key obtained from Invictus USTA platform

### b. Credential Store:

Parameter	Value
Type	External Credential
Name	Name of the credential with pull path of the safe on store

## Configuring Invictus USTA as Alert Source

1. Click **Configuration > Alert Source > Create Alert Source Configuration**.
2. Specify the following parameter values in the **Configuration** form:

Parameter	Value
Name	Display name of Invictus USTA Alert Source on SOAR
Type	USTA
Address	Address of the Invictus USTA Threat Intelligence Service ( <a href="https://usta01.invictuseurope.com/api/">https://usta01.invictuseurope.com/api/</a> )
Alert Severities	Mapping of alert severity values to SOAR incident severities

Parameter	Value
<b>Configuration</b>	<p>Specify the following configuration parameters:</p> <pre># Ignore events older than specified date. If empty, date based filtering is disabled. # Example: filterOlderThanDate=2017-01-01 filterOlderThanDate=2020-01-10 # Integration ID of the proxy integration to use when connecting to current source. # If not provided, SOAR will try to use a direct connection. #proxy.id=5523</pre>
<b>Credential</b>	Name of the credential set just created. (For example, Invictus USTA Credentials)
<b>Trust Invalid SSL Certificates</b>	Select this if Web UI's certificate is self-signed or is not recognized by browsers
<b>Visible Alert Fields</b>	Define the alarm fields to be displayed on Incident Management Service Desk

3. Click **Test** to test the integration.
4. Click **Save** to complete the integration.

## Configuring Invictus USTA as Integration

1. Click **Configuration > Integrations > Create Integration**.
2. Specify the following parameter values in the **Configuration** form:

Parameter	Value
<b>Name</b>	Display name of Invictus USTA integration on SOAR
<b>Type</b>	USTA
<b>Address</b>	Address of the Invictus USTA Threat Intelligence Service ( <a href="https://usta01.invictuseurope.com">https://usta01.invictuseurope.com</a> )
<b>Configuration</b>	<p>Specify the following configuration parameters:</p> <pre># Integration ID of the proxy integration to use when connecting to current source. # If not provided, SOAR will try to use a direct connection. #proxy.id=5523#proxy.id=5523</pre>
<b>Credential</b>	Name of the credential set created on step 2 (For example, Invictus USTA Credentials)
<b>Trust Invalid SSL Certificates</b>	Select this if Web UI's certificate is self-signed or is not recognized by browsers
<b>Require Approval From</b>	Select users from the list who can provide approval before executing actions on this integration
<b>Notify</b>	Select users from the list to notify when SOAR performs an action on this integration.

3. Click **Test** to test the integration.
4. Click **Save** to complete the integration.

## Additional Notes

USTA permits connection requests from specific network addresses for each customer. Hence, make sure to check the access permission by USTA before integration.

# Integration Guide for IPInfo

## Integration Overview

**IPInfo** is a solution for IP data which offers both free and paid API tokens to put IP geolocation, ASN, IP to company, mobile carrier, and many more.

## Integration Capabilities

ArcSight SOAR has the following integration capabilities with IPInfo:

- IP Query

## Configuration

### Prerequisites

- You must have access to HTTPS as ArcSight SOAR connects to **IPInfo** through this service.
- IPInfo requires an API key for access.

### Configuring SOAR

1. Click **Configuration > Credential > Create Credential**.
2. Specify the following parameter values in the **Credential Editor** form:

Type	Name	Username	Password	Private Key
Internal credential	Display name of credential set (for example, IPInfo Credential).			Access token

- a. Click **Configuration > Integrations > Create Integration**.
- b. Specify the following parameter values in the **Configuration** form:

Parameter	Value
Name	Display name of the integration.
Type	IPInfo.io
Address	Address of the integration (the format should be https://ipinfo.io).

Parameter	Value		
<b>Configuration</b>	Specify the following configuration parameters:  <table border="1" style="margin-left: 20px;"> <tr> <td><b>proxy.id</b></td> <td>ID of the Proxy integration if you access ipinfo.io through a web proxy device. For example: proxy.id = 12345 .</td> </tr> </table>	<b>proxy.id</b>	ID of the Proxy integration if you access ipinfo.io through a web proxy device. For example: proxy.id = 12345 .
<b>proxy.id</b>	ID of the Proxy integration if you access ipinfo.io through a web proxy device. For example: proxy.id = 12345 .		
<b>Credential</b>	Credential that has been defined for this integration under the <b>Credentials</b> menu.		
<b>Trust Invalid SSL Certificates</b>	Select this if web server's certificate is self-signed or is not recognized by browsers.		
<b>Require Approval From</b>	Select user(s) from list to ask the approval before executing actions on this integration.		
<b>Notify</b>	Select user(s) from the list to notify when SOAR performs an action on this integration.		

- c. Click **Save** to save the integration definition.
- d. Navigate to **Configuration>Customization Library** and edit **IPinfo Advanced Action Script Default Template**.
- e. Select the integration that you have added to **Integrations** menu.
- f. Click **Save** to complete the integration.
- g. Click **Test**, an **Integration Successful** message is displayed if the credential and address are valid.

## Capabilities

### a. IP Query

Enrichment capability for retrieving information regarding an IP.

The following table presents the **IP Query** enrichment capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Integration</b>	Name of the third party integration.	Integration	N/A	Yes
<b>IP</b>	Network address to be queried from IPInfo .	Network Address	Yes	Yes
<b>Do not Use Cache</b>	SOAR does not use cached results if this box is checked.	Boolean	N/A	No

### Output:

Case Scope:

Enrichment	Type	Category/ Value
None	N/A	N/A

Human Readable Output:

Field	Value
anycast	true
city	Mountain View
country	US
hostname	dns.google
ip	8.8.8.8
loc	37.4056,-122.0775
org	AS15169 Google LLC
postal	94043
region	California
timezone	America/Los_Angeles

# Integration Guide for Jira

## Integration Overview

Jira is an ITSM service that provides issue management to users.

Unlike our other plugins, this plugin consists of two modules. One was developed as a custom script in SOAR to perform actions on Jira, and the other as an add-on in Jira to perform actions on the SOAR product. We aimed that both products keep each other informed of certain changes on each other. SOAR is using Jira API to perform operations on Jira, and Jira is using our newly developed SOAR API to perform operations on SOAR through the add-on we developed. Issue creation must be initiated with SOAR, so we can mark the issue and track it both sides.

## Integration Capabilities

ArcSight SOAR has the following integration capabilities with Jira:

- Create Issue
- Send Comment
- Update Issue
- Update Issue Status

## Prerequisites

You must have access to HTTPS as the ArcSight SOAR connects to Jira API through this service and Jira connects to SOAR through this service.

## Configuration

### Configuring SOAR

1. Navigate to **ITOM Management** and click the **Three dots** button for deployment and select **Reconfigure**.
2. Click **SOAR** tab. On the **REST API** fields, specify values for one of them and keep a note of it, as shown in the following figure:

The screenshot shows the Jira Plugins page. Under the heading "User-installed apps", there is a list of installed plugins. One plugin, "ArcSight SOAR Plugin", is highlighted. Below the list, a note states: "This plugin implements a simple issue event listener for JIRA using atlassian-event." There are three buttons for this plugin: "Configure", "Uninstall", and "Disable". To the right of the plugin list, it says "Version: 1.0-SNAPSHOT", "Vendor: Micro Focus", and "App key: com.plugins.soar.listener-plugin". A progress bar indicates "2 of 2 modules enabled".



**Note:** You can note down the **Client Id Suffix** and **Client Secret** values to be used later.

3. Click **Save**
4. Navigate to **SOAR** application and click **Configuration > Credentials > Create Credential**.
5. Specify the following parameter values in the **Credential Editor**:

Parameter	Value
<b>Type</b>	Internal credential.
<b>Name</b>	Display name of credential set (for example, Jira Credentials)
<b>Username</b>	Jira User Username.
<b>Password</b>	Jira User Password.
<b>Private Key</b>	

6. Click **Save**.
7. Click **Configuration > Lists > Create List**. Give the list a name (for example, jiraLookup).



**Note:** SOAR is going to map SOAR cases and Jira issues on this list for both sides.

8. Click **Save**
9. Click **Configuration > Integration > Create Integration**
10. Specify the following parameter values in the **Configuration Form**:

Parameter	Value
<b>Name</b>	Display name of Jira integration on SOAR.
<b>Type</b>	Jira
<b>Address</b>	Address of the integration (for example, <a href="https://192.168.200.231:8080">https://192.168.200.231:8080</a> ).
<b>proxy.id</b>	ID of the Proxy integration if accessing the jira service through a web proxy device. For Example: proxy.id = 12345.
<b>list.name</b>	Parameter must be equal to list name that is given at step 8. (for example, list.name=jiraLookup).

Parameter	Value
<b>Credential</b>	Name of the credential set created on step 5(for example, Jira Credentials).
<b>Trust Invalid SSL Certificates</b>	Select this if service's certificate is self-signed or is not recognized by browsers.
<b>Required Approval From</b>	Select users from the list who can provide approval before executing actions on this integration.
<b>Notify</b>	Select user(s) from the list to notify when SOAR performs an action on this integration.

11. Click **Save**.
12. Navigate to **Configuration > Customization Library > Open Jira Script**.
13. Select integration that is newly created in the **Integrations** field.
14. Click **Save** to complete the integration.
15. Click **Test**, an **Integration Successful** message is displayed if the address and credential are valid.

## Configuring Jira

1. Navigate to **Jira Administration<Manage apps**.
  2. Click **Upload app** and choose the Jira add-on jar file that is provided. After the installation completion, the plugin is visible in the **User-installed** apps.
-  **Note:** You can also download the [Jira add-on jar file](#) from Marketplace.
3. Click **Configure**. Specify the values for **Base URL**, **Client ID**, **Client Secret** (as noted during creating an API user in **Configuring SOAR** part) and SOAR username (SOAR needs a JIRA user to access Jira service).
  4. Click **Save**.
-  **Note:** Now you can start creating issue on Jira by **Create Issue** capability on SOAR.

## Capabilities

1. **Create Issue**  
Action capability for creating issue on Jira.  
The following table presents the **Create Issue** action capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Project Key</b>	Key of the project that you want to create issue in it.	Text	No	Yes
<b>Issue Type</b>	Type of the issue.	Text	No	Yes
<b>Summary</b>	Summary of the issue.	Text	No	Yes
<b>Description</b>	Description of the issue.	Text	No	Yes

**Output:**

Case Scope: N/A

Human Readable Output: N/A

**2. Send Comment**

Action capability for sending comment to related issue.

The following table presents the **Send Comment** action capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Comment</b>	Comment that you want to add to the issue.	Text	No	Yes

**Output:**

Case Scope: N/A

Human Readable Output: N/A

**3. Update Issue**

Action capability for updating attributes of the issue

The following table presents the **Update Issue** action capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Summary</b>	Summary of the issue.	Text	No	No
<b>Description</b>	Description of the issue.	Text	No	No
<b>Assignee</b>	Assignee of the issue.	Text	No	No
<b>Priority</b>	Priority of the issue.	Text	No	No

**Output:**

Case Scope: N/A

Human Readable Output: N/A

**4. Update Issue Status**

Action capability for updating status of the issue.

The following table presents the **Update Issue Status** action capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
Status	Status of the issue	ComboBox (Elements of the combobox are changeable by the script code)	No	Yes

**Output:**

Case Scope: N/A

Human Readable Output: N/A



**Note:** We are supporting **Update Status**, **Update Severity**, **Update Description**, **Update Subject** and **Add Comment** capabilities through SOAR application. If the Jira user changes any of the related items in the Jira issue, and if that issue description contains SoarCaseId then the prepared API requests are sent to SOAR.

SOAR then adds the SOAR CaseId into description-field during the creation of the Jira Issue. The Add-On uses this SoarCaseId for SOAR API requests.

# Integration Guide for JDBC(Database) Server

## Integration Capabilities

ArcSight SOAR has the following integration capability with database servers:

- JDBC Query

### Use Case: Querying HR Database

With this integration, while investigating an incident SOAR can run a query on HR database to see if they are logged on the user on a suspicious endpoint. This can either be performed automatically within a playbook or manually by an analyst.

## Configuration

### Prerequisites

- A database listener or service for SOAR to access.
- Create a DB user account for SOAR to run the SQL queries.

### Configuring Database Server

Please contact database administrator for user account and access permissions.

### Configuring SOAR

1. Click **Configuration > Credentials > Create Credential**.
2. Specify the following parameter values in the **Credential Editor**:

### a. Internal Credential

Parameter	Value
Type	Internal Credential
Name	Display name of credential set (For example, JDBC Credentials)
Username	User account that was configured on database server
Password	Password for user account that was configured on database server
Private Key	Empty

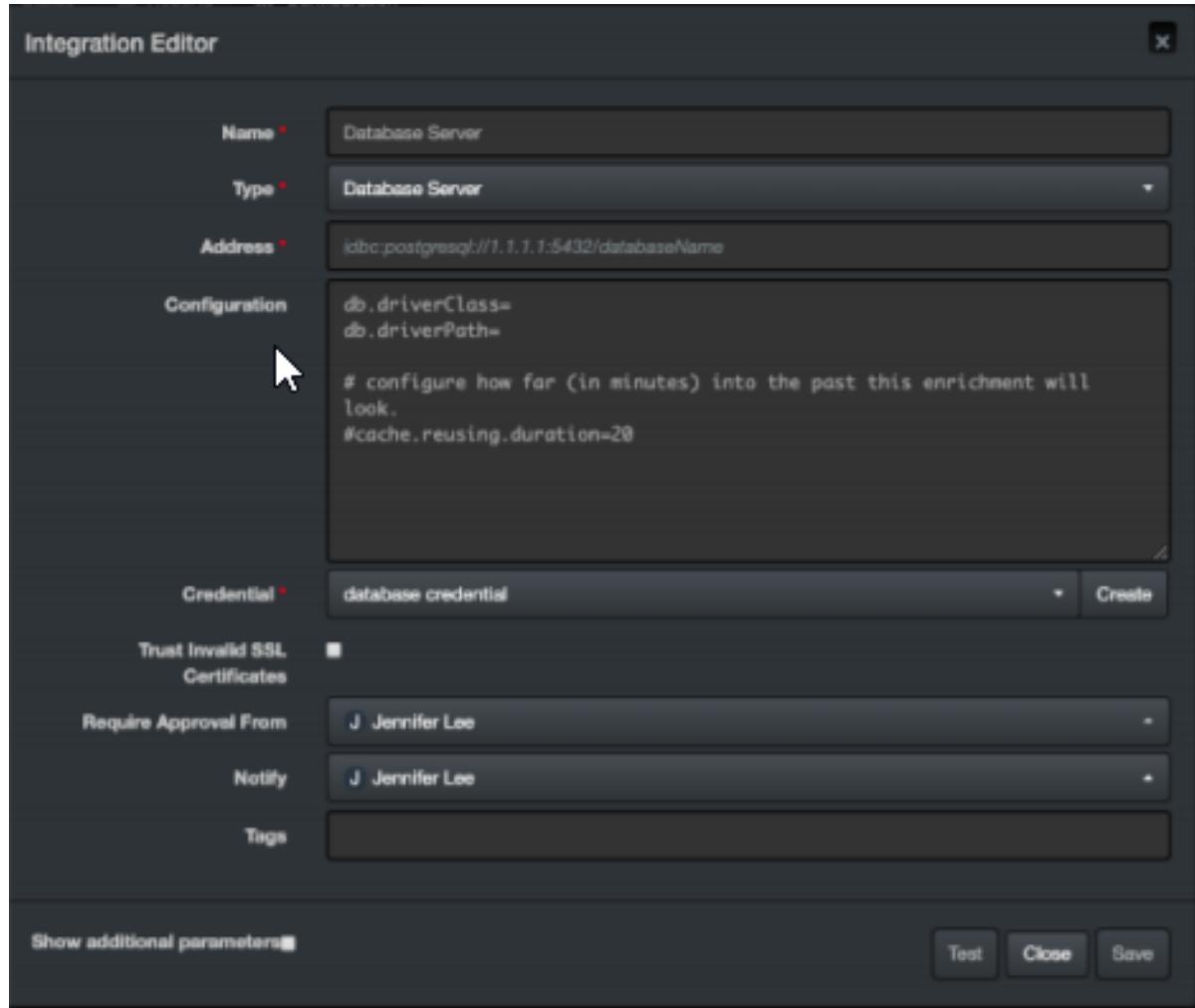
### b. Credential Store

Parameter	Value
Type	External Credential
Name	Name of the credential with full path of the safe on store.

3. Click **Configuration > Integrations > Create Integration**.

4. Specify the following parameter values in the **Configuration** form:

Parameter	Value
Name	Display name of Database Server integration on SOAR
Type	Database Server
Address	Address of the integration ( in the format jdbc:driverName://192.168.3.10:5432/databaseName).
Configuration	Specify the following configuration parameters: <pre># For MySQL: db.driverClass=com.mysql.jdbc.Driver # For Oracle: db.driverClass=oracle.jdbc.OracleDriver # For PostgreSQL: db.driverClass=org.postgresql.Driver # For MSSQL Server: db.driverClass=com.microsoft.sqlserver.jdbc.SQLServerDriver db.driverClass=db.driverClass=org.postgresql.Driver # Absolute path where you put the JDBC driver's JAR file. db.driverPath= # configure how far (in minutes) into the past this enrichment will look. cache.reusing.duration=30</pre>
Credential	Name of the credential set created on step 2. (For example, Database Server Credentials).
Trust Invalid SSL Certificates	Select this if device's certificate is self-signed or is not recognized by browsers
Require Approval from	Select users from the list who can provide approval before executing actions on this integration
Notify	Select users from the list to notify when SOAR performs an action on this integration.



5. Click **Test**. The following pop up will be displayed if your credential and address are valid.
6. Click **Save** to complete integration.

# Integration Guides for Kannel SMS Gateway

## Integration Overview

Kannel is an open source SMS Gateway which is used widely for sending in either single or bulk SMS(Short Message Service). Kannel links HTTP based services to various SMS centers using various protocols.

## Integration Capabilities

### Supported Action Capabilities

Kannel SMS Gateway allows user notifications using SMS messages which was set when creating the Playbook involving this integration.

## Configuration

### Configuring Kannel SMS Gateway

- Configure the integration to send SMS messages.

### Configuring SOAR

Following are the steps to create the integration:

1. Navigate to **Configuration > Parameters**.
2. Configure **SMS Device** to be used as the ID of Kannel SMS Gateway integration.
3. To configure the integration, navigate to **Configuration > Integrations**.
4. Specify the following parameter values in the **Integration Editor**:

Parameter	Value
Name	Display name of Kannel SMS Gateway integration on SOAR
Type	Kannel SMS Gateway
Address	Address of the integration (in the following format: 1.1.1.1:1234)

Parameter	Value
Configuration	sms.sender=<Specify the value configured in the SMS Device field>
Credential	Name of the credential set created on step 2
Trust Invalid SSL Certificates	Select this if Integrations's certificate is self-signed or is not recognized by browsers.
Require Approval From	Select users from the list who can provide approval before executing actions on this integration
Notify	Select users from the list to notify when SOAR performs an action on this integration

**Integration Editor**

Name *	Kannel SMS Gateway
Type *	Kannel SMS Gateway
Address *	1.1.1.1:1234
Configuration	sms.sender=
Credential *	Kannel SMS Gateway
Trust Invalid SSL, Certificates	<input checked="" type="checkbox"/>
Require Approval From	No selected principal
Notify	No selected principal
Tags	
<a href="#">Show additional parameters</a>	
<input type="button" value="Test"/> <input type="button" value="Close"/> <input type="button" value="Save"/>	

5. Click **Test** to test the integration.
6. Click **Save** to complete the integration.

# Integration Guide for Kaspersky Security Center

## Integration Overview

ArcSight SOAR is capable of communicating with Kaspersky Security Center through WinRM and Powershell to block hashes, add tags to hosts, run tasks, move hosts to groups and retrieve information about various management objects.

## Integration Capabilities

- Block (blacklist) SHA-256 or MD5 hash, with rollback support
- Add tag to host, with rollback support
- Move host to group
- Run task
- Retrieve host information

## Configuration

### Configuration on Kaspersky Security Center

- To define a Kaspersky Security Center installation as an integration on your SOAR, following integration specific configuration should be performed.
- SOAR should be able to access the server with Kaspersky Security Center through WinRM on the network; usually with TCP port 5985 or 5986 (if SSL is enabled on WinRM). See WinRM Integration Guide for details on how to configure WinRM access.
- A local or domain administrator user account is required execute various capabilities.
- 32-bit version of Windows Scripting Host (which is available on a default Windows installation) is required to execute built-in scripts, which is usually located at C:\Windows\SYSWOW64\cscript.exe.

### Configuring SOAR

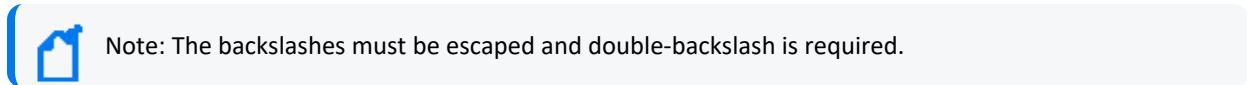
- While creating this integration via Integrations tab of Configuration menu:
- Name: Display name of the integration.

- Address: Address of the integration. Format of the address should be IP, IP:port, dns.hostname.localnet, or dns.hostname.localnet:port for HTTP; or prefixed with https:// if HTTPS/SSL listener was enabled on WinRM.
- Credential: Credential that has been defined for this integration under the Credentials menu.

## Optional configuration

- `blockhash.categoryname`: Category name to add block hashes into; if unspecified defaults to SOAR. If specified category name doesn't exist, it will be automatically created.
- `path.cscriptexe`: Location of the 32-bits version of the cscript.exe on server.

If unspecified, defaults to "C:\\Windows\\SysWOW64\\cscript.exe".



## Overriding built-in scripts

SOAR allows overriding built-in scripts using Customization Library. Create a new customization of **Basic plugin script**, take note of its ID, and set the value of the script you'd like to override in the integration configuration by specifying its identifier as specified below:

Parameter Name	Description
<code>enrichment.gettasknames</code>	Retrieve names of tasks available for Run task capability
<code>enrichment.getgroupnames</code>	Retrieve names of groups available for Move host to group capability
<code>enrichment.gettagnames</code>	Retrieve names of tags available for Add tag to host capability
<code>enrichment.hostinfo</code>	Retrieve host information enrichment script
<code>execute.blockhash</code>	Block hash capability
<code>rollback.blockhash</code>	Rollback block hash capability
<code>execute.addtag</code>	Add tag capability
<code>rollback.addtag</code>	Rollback add tag capability
<code>execute.movesystem</code>	Move host to group capability
<code>execute.runtask</code>	Run task capability

## Important points

- When these parameters are specified, built-in scripts will be ignored and the customization with specified ID will be used instead as the script. All scripts should target Windows Scripting Host with Javascript language, unless a different/compatible interpreter is specified in path.cscriptexe parameter in integration configuration. See [https://support.kaspersky.com/9291](Kaspersky Enterprise Security Administration Kit Automation10) for reference on using its COM/ActiveX API.
- SOAR's implementation is sensitive to the expected output of these scripts; overriding a capability with a script that doesn't write expected output to stdout may break existing functionality.
- Scripts are automatically evaluated as StringTemplate and various parameters are injected into the template for block hash, run task, move host into group, add tag and host information capabilities. See built-in scripts below for example usage and [http://www.stringtemplate.org](String Template Website) for more details on how to make use of the ST engine.

**Example:**

# 4214 is the ID of the customization to override this capability.

execute.runtask=4214

## Built-in Tasks

### Get Task Names

```
function obj(name) {
    return new ActiveXObject("klakaut.KlAk" + name);
}
try {
    var oConnectProps = obj("Params"), oAdmServer = obj("Proxy"),
        oSrvView = obj("SrvView"),
        oTasks = obj("Tasks2"), item, enumObj;
    oConnectProps.Add("Address", "127.0.0.1:13291");
    oAdmServer.Connect(oConnectProps);
    oTasks.AdmServer = oSrvView.AdmServer = oAdmServer;
    enumObj = new Enumerator(oTasks.EnumTasks(-1));
    WScript.Echo('[OK] [BEGIN]');
    for (; !enumObj.atEnd(); enumObj.moveNext()) {
        item = enumObj.item();
        WScript.Echo(item.item('TASK_UNIQUE_ID') + '=' + item.item('DisplayName'));
    }
    WScript.Echo('[END]');
}
```

```

} catch (e) {
WScript.Echo("[Error] " + e.number + " occurred !!! " + e.description);
}

```

## Get Group Names

```

function obj(name) {
return new ActiveXObject("klakaut.KlAk" + name);
}
function EnumerateGroups(oSubgroupsEnum) {
var enumObj = new Enumerator(oSubgroupsEnum);
for (; !enumObj.atEnd(); enumObj.moveNext()) {
var oObj = enumObj.item();
WScript.Echo(oObj.Item("id") + '=' + oObj.Item("name"));
if (oObj.Check("groups")) {
EnumerateGroups(oObj.Item("groups"));
}
}
}
try {
var oConnectProps = obj("Params"), oAdmServer = obj("Proxy"),
oGroups = obj("Groups");
oConnectProps.Add("Address", "127.0.0.1:13291");
oAdmServer.Connect(oConnectProps);
oGroups.AdmServer = oAdmServer;
WScript.Echo('[OK] [BEGIN]');
EnumerateGroups(oGroups.GetSubgroups(oGroups.GroupIdGroups, 0));
WScript.Echo('[END]');
} catch (e) {
WScript.Echo("[Error] " + e.number + " occurred !!! " + e.description);
}

```

## Get Tag Names

```

function obj(name) {
return new ActiveXObject("klakaut.KlAk" + name);
}
try {
var oConnectProps = obj("Params"), oAdmServer = obj("Proxy"),
oTagsControl = obj("TagsControl"), oProps = obj("Params"), oTags,
enumObj;
oConnectProps.Add("Address", "127.0.0.1:13291");

```

```

oAdmServer.Connect(oConnectProps);
oTagsControl.AdmServer = oAdmServer;
oTagsControl.Prop("ListName") = "HostsTags";
oTags = oTagsControl.GetAllTags(oProps);
WScript.Echo('[OK] [BEGIN]');
if (oTags != null) {
enumObj = new Enumerator(oTags);
for (; !enumObj.atEnd(); enumObj.moveNext()) {
WScript.Echo(enumObj.item() + "=" + enumObj.item());
}
}
WScript.Echo('[END]');
} catch (e) {
WScript.Echo("[Error] " + e.number + " occurred !!! " + e.description);
}

```

## Host Information Enrichment

```

function obj(name) {
return new ActiveXObject("klakaut.KlAk" + name);
}
function ip2long(IPAddress) {
var ip = IPAddress.match(/^\d+\.\d+\.\d+\.\d+$/);
return ip ? (+ip[1] << 24) + (+ip[2] << 16) + (+ip[3] << 8) + (+ip[4]) : null;
}
function long2ip(l) {
return ((l >> 24) & 255) + "." + ((l >> 16) & 255) + "." + ((l >> 8) & 255) +
"." + (l & 255);
}
function coll() {
var ret = obj("Collection"), len = arguments.length, args = arguments;
if (len == 1) {
args = arguments[0].split('|');
len = args.length;
}
ret.SetSize(len);
for (var i=0; i<len; i++) {
ret.SetAt(i, (arguments.length == 1 ? "KLHST_WKS_" : "") + args[i]);
}
return ret;
}
function g(a, e) {
var r = e.item('KLHST_WKS_' + a);
if (r === undefined) {
r = '';
}
return r;
}

```

```

}

var rtpState = ["Unknown", "Stopped", "Suspended", "Starting", "Running",
"Running (Maximum protection)", "Running (Maximum speed)",
"Running (Recommended settings)", "Running (Custom settings)",
"Failure"];
function getStatus(v) {
var r = [];
if ((v & 1) == 1) {
r.push("Visible");
}
if ((v & 4) == 4) {
r.push("Agent:Installed");
}
if ((v & 8) == 8) {
r.push("Agent:Alive");
}
if ((v & 16) == 16) {
r.push("Real-Time-Protection:Installed");
return r.join(",");
}
try {
var oConnectProps = obj("Params"), oAdmServer = obj("Proxy"),
oHosts = obj("Hosts"), c=0;
oConnectProps.Add("Address", "127.0.0.1:13291");
oAdmServer.Connect(oConnectProps);
oHosts.AdmServer = oAdmServer;
var fieldsToReturn = "LAST_VISIBLE|STATUS|RTP_STATE|LAST_UPDATE|LAST_FULLSCAN|
WINHOSTNAME|WINDOMAIN|OS_NAME|OS_VER_MAJOR|OS_VER_MINOR|IP_LONG|PRODUCT_TAG_
NAME";
var ftr = fieldsToReturn.split('|');
var enumObj = new Enumerator(oHosts.FindHosts("(KLHST_WKS_IP_LONG=" +
ip2long('%host%') + ")", coll(fieldsToReturn), coll()));
WScript.Echo('[OK]');
for (; !enumObj.atEnd(); enumObj.moveNext()) {
var e = enumObj.item();
WScript.Echo('[' + c++ + ']' +
'LAST_VISIBLE=' + Date.parse(g('LAST_VISIBLE', e)) +
'|LAST_UPDATE=' + Date.parse(g('LAST_UPDATE', e)) +
'|LAST_FULLSCAN=' + Date.parse(g('LAST_FULLSCAN', e)) +
'|WINHOSTNAME=' + g('WINHOSTNAME', e) +
'|WINDOMAIN=' + g('WINDOMAIN', e) +
'|OS=' + g('OS_NAME', e) + ' (' + g('OS_VER_MAJOR', e) + '.' +
g('OS_VER_MINOR', e) + ')' +
'|IP=' + long2ip(g('IP_LONG', e)) +
'|RTP_STATE=' + rtpState[g('RTP_STATE', e)] +
'|STATUS=' + getStatus(g('STATUS', e)) +
'|PRODUCT_TAG_NAME=' + g('PRODUCT_TAG_NAME', e)
}
}

```

```

);
}
WScript.Echo("[END] Retrieved information for " + c + " hosts.");
} catch (e) {
WScript.Echo("[Error] " + e.number + " occurred !!! " + e.description);
}

```

## Block Hash Action Capability

```

var hashes = [%hashes: {h | "%h%"}; separator=", "%];
function obj(name) {
return new ActiveXObject("klakaut.KlAk" + name);
}
try {
var oConnectProps = obj("Params"), oAdmServer = obj("Proxy"),
oCategory = obj("FileCategorizer"), oFields2Return = obj("Collection"),
oSrvView = obj("SrvView");
oConnectProps.Add("Address", "127.0.0.1:13291");
oAdmServer.Connect(oConnectProps);
oCategory.AdmServer = oSrvView.AdmServer = oAdmServer;
oFields2Return.SetSize(2);
oFields2Return.SetAt(0, "id");
oFields2Return.SetAt(1, "name");
var enumObj = new Enumerator(oSrvView.GetChunkAccessor
('customcategories',
'(name = "*")', oFields2Return, obj("Collection"))), catFound = null;
for (; !enumObj.atEnd(); enumObj.moveNext()) {
var item = enumObj.item();
if (item.item('name') === '%categoryname%') {
catFound = item.item('id');
}
// dump("", "", item, false);
// dump("", "", oCategory.GetCategory(item.item('id')), false);
}
var oCatToAdd, oInclProps, i, oCatProps = obj("Params"), oCatData = catFound ?
oCategory.getCategory(catFound) : null, oInclusions = catFound ?
oCatData.Item('inclusions') : obj("Collection");
for (i=0; i<hashes.length; i++) {
oInclProps = obj("Params");
oInclProps.Add('ex_type', 3);
oInclProps.Add(hashes[i].length == 32 ? 'str' : 'str2', hashes[i]);
oInclProps.Add('str_op', 0);
oInclusions.SetSize(oInclusions.Count + 1);
oInclusions.setAt(oInclusions.Count - 1, oInclProps);
}
if (!catFound) {
oCatProps.Add('name', '%categoryname%');
}

```

```

oCatProps.Add('CategoryType', 0);
oCatProps.Add('inclusions', oInclusions);
oCatToAdd = oCategory.CreateCategory(oCatProps);
WScript.Echo("[OK] [CREATED] Added " + hashes.length +
' hashes to newly created category: %categoryname%');
} else {
oCategory.UpdateCategory(catFound, oCatData);
WScript.Echo("[OK] [UPDATED] Added " + hashes.length +
' hashes to existing category: %categoryname% its current size is: ' +
+ oInclusions.Count);
}
} catch (e) {
WScript.Echo("[Error] " + e.number + " occurred !!! " + e.description);
}

```

## Rollback of block hash capability

```

var hashes = [%hashes: {h | "%h%"}; separator=, "%"];
function obj(name) {
return new ActiveXObject("klakaut.KlAk" + name);
}
try {
var oConnectProps = obj("Params"), oAdmServer = obj("Proxy"),
oCategory = obj("FileCategorizer"), oFields2Return = obj("Collection"),
oSrvView = obj("SrvView");
oConnectProps.Add("Address", "127.0.0.1:13291");
oAdmServer.Connect(oConnectProps);
oCategory.AdmServer = oSrvView.AdmServer = oAdmServer;
oFields2Return.SetSize(2);
oFields2Return.SetAt(0, "id");
oFields2Return.SetAt(1, "name");
var enumObj = new Enumerator(oSrvView.GetChunkAccessor('customcategories',
'(name = "*')', oFields2Return, obj("Collection"))), catFound = null;
for (; !enumObj.atEnd(); enumObj.moveNext()) {
var item = enumObj.item();
if (item.item('name') === '%categoryname%') {
catFound = item.item('id');
}
}
if (!catFound) {
WScript.Echo("[OK] [DOESNTEXIST] Category %categoryname% doesn't exist,
no need to remove anything.");
} else {
var oCatData = oCategory.getCategory(catFound),
oInclusions = oCatData.Item('inclusions'),
oNewInclusions = obj("Collection"), i, j, k=0;
for (j=0; j<oInclusions.Count; j++) {

```

```

for (i=0; i<hashes.length; i++) {
var incl = oInclusions.Item(j);
if (incl.Item('str') !== hashes[i] && incl.Item('str2') !== hashes[i]) {
oNewInclusions.SetSize(oNewInclusions.Count + 1);
oNewInclusions.setAt(oNewInclusions.Count - 1, incl);
} else {
k++;
}
}
}
}
oCatData.Item('inclusions') = oNewInclusions;
oCategory.UpdateCategory(catFound, oCatData);
WScript.Echo("[OK] [UPDATED] Removed " + k + " of " + hashes.length +
' hashes from category: %categoryname% its current size is: ' +
oNewInclusions.Count);
}
} catch (e) {
WScript.Echo("[Error] " + e.number + " occurred !!! " + e.description);
}

```

## Add tag to host capability

```

function obj(name) {
return new ActiveXObject("klakaut.KlAk" + name);
}
function ip2long(IPAddress) {
var ip = IPAddress.match(/^\d+\.\d+\.\d+\.\d+$/);
return ip ? (+ip[1] << 24) + (+ip[2] << 16) + (+ip[3] << 8) + (+ip[4]) : null;
}
try {
var oConnectProps = obj("Params"), oAdmServer = obj("Proxy"),
oTagsControl = obj("TagsControl"), oHosts = obj("Hosts"),
oFields2Return = obj("Collection"), enumObj, taggedHosts = 0;
oConnectProps.Add("Address", "127.0.0.1:13291");
oAdmServer.Connect(oConnectProps);
oTagsControl.Prop("ListName") = "HostsTags";
oTagsControl.AdmServer = oHosts.AdmServer = oAdmServer;
oFields2Return.SetSize(1);
oFields2Return.SetAt(0, "KLHST_WKS_HOSTNAME");
enumObj = new Enumerator(oHosts.FindHosts("(KLHST_WKS_IP_LONG=" +
ip2long('%host%') +
")", oFields2Return, obj("Collection")));
for (; !enumObj.atEnd(); enumObj.moveNext()) {
var oTagArrayItem = obj("Params");
oTagArrayItem.Add("KLTAGS_VALUE", "%tag%");
oTagArrayItem.Add("KLTAGS_SET", true);
var oTagArray = obj("Collection");

```

```

oTagArray.SetSize(1);
oTagArray.SetAt(0, oTagArrayItem);
var oHostsArrayItem = obj("Params");
oHostsArrayItem.Add("KLTAGS_ITEM_ID", enumObj.item().item('KLHST_WKS_HOSTNAME'));
oHostsArrayItem.Add("KLTAGS_TAGS", oTagArray);
var oHostsArray = obj("Collection");
oHostsArray.SetSize(1);
oHostsArray.SetAt(0, oHostsArrayItem);
var oSetTagsCallProps = obj("Params");
oSetTagsCallProps.Add("KLTAGS_FULL_REPLACE", false);
oTagsControl.SetTags(oHostsArray, oSetTagsCallProps);
taggedHosts++;
}
WScript.Echo("[OK] Added '%tag%' to " + taggedHosts + " hosts.");
} catch (e) {
WScript.Echo("[Error] " + e.number + " occurred !!! " + e.description);
}

```

## Rollback of Add Tag to Host Capability

```

function obj(name) {
return new ActiveXObject("klakaut.KlAk" + name);
}
function ip2long(IPAddress) {
var ip = IPAddress.match(/^(\d+)\.(\d+)\.(\d+)\.(\d+)$/);
return ip ? (+ip[1] << 24) + (+ip[2] << 16) + (+ip[3] << 8) + (+ip[4]) : null;
}
try {
var oConnectProps = obj("Params"), oAdmServer = obj("Proxy"),
oTagsControl = obj("TagsControl"), oHosts = obj("Hosts"),
oFields2Return = obj("Collection"), enumObj, tagRemovedHosts = 0,
removedTagCount;
oConnectProps.Add("Address", "127.0.0.1:13291");
oAdmServer.Connect(oConnectProps);
oTagsControl.Prop("ListName") = "HostsTags";
oTagsControl.AdmServer = oHosts.AdmServer = oAdmServer;
oFields2Return.SetSize(1);
oFields2Return.SetAt(0, "KLHST_WKS_HOSTNAME");
enumObj = new Enumerator(oHosts.FindHosts("(KLHST_WKS_IP_LONG=" +
ip2long('%host%') + ")", oFields2Return, obj("Collection")));
for (; !enumObj.atEnd(); enumObj.moveNext()) {
var hostId = enumObj.item().item('KLHST_WKS_HOSTNAME');
var oHostIds = obj("Collection");
oHostIds.setSize(1);
oHostIds.SetAt(0, hostId);
var oExistingTagArray = oTagsControl.GetTags(oHostIds, obj("Params"));

```

```

var oTagArray = obj("Collection");
removedTagCount = 0;
for (var i = 0; i < oExistingTagArray.Count; i++) {
    var oTagEntry = oExistingTagArray.Item(i);
    var oTagValues = oTagEntry.Item("KLTAGS_TAGS");
    for (var j = 0; j < oTagValues.Count; j++) {
        var tag = oTagValues.Item(j);
        if (tag != '%tag%') {
            oTagArray.SetSize(oTagArray.Count + 1);
            var oTagArrayItem = obj("Params");
            oTagArrayItem.Add("KLTAGS_VALUE", tag);
            oTagArrayItem.Add("KLTAGS_SET", true);
            oTagArray.SetAt(oTagArray.Count - 1, oTagArrayItem);
        } else {
            removedTagCount++;
        }
    }
}
var oHostsArrayItem = obj("Params");
oHostsArrayItem.Add("KLTAGS_ITEM_ID", hostId);
oHostsArrayItem.Add("KLTAGS_TAGS", oTagArray);
var oHostsArray = obj("Collection");
oHostsArray.SetSize(1);
oHostsArray.SetAt(0, oHostsArrayItem);
var oSetTagsCallProps = obj("Params");
oSetTagsCallProps.Add("KLTAGS_FULL_REPLACE", true);
oTagsControl.SetTags(oHostsArray, oSetTagsCallProps);
if (removedTagCount > 0) {
    tagRemovedHosts++;
}
}
WScript.Echo("[OK] Removed '%tag%' from " + tagRemovedHosts + " hosts.");
} catch (e) {
    WScript.Echo("[Error] " + e.number + " occurred !!! " + e.description);
}

```

## Move system to group capability

```

function obj(name) {
    return new ActiveXObject("klakaut.KlAk" + name);
}
function ip2long(IPAddress) {
    var ip = IPAddress.match(/^\d+\.\d+\.\d+\.\d+$/);
    return ip ? (+ip[1] << 24) + (+ip[2] << 16) + (+ip[3] << 8) + (+ip[4]) : null;
}
try {

```

```

var oConnectProps = obj("Params"), oAdmServer = obj("Proxy"),
oHosts = obj("Hosts"), oFields2Return = obj("Collection"), enumObj,
hostsToMove = obj("Collection");
oConnectProps.Add("Address", "127.0.0.1:13291");
oAdmServer.Connect(oConnectProps);
oHosts.AdmServer = oAdmServer;
oFields2Return.SetSize(1);
oFields2Return.SetAt(0, "KLHST_WKS_HOSTNAME");
enumObj = new Enumerator(oHosts.FindHosts("(KLHST_WKS_IP_LONG=" +
ip2long('%host%') + ")", oFields2Return, obj("Collection")));
for (; !enumObj.atEnd(); enumObj.moveNext()) {
hostsToMove.SetSize(hostsToMove.Count + 1);
hostsToMove.SetAt(hostsToMove.Count - 1,
enumObj.item().item('KLHST_WKS_HOSTNAME'));
}
oHosts.MoveHostsToGroup(parseInt('%group%'), hostsToMove);
WScript.Echo("[OK] " + hostsToMove.Count + " hosts moved to group
#%group%");
} catch (e) {
WScript.Echo("[Error] " + e.number + " occurred !!! " + e.description);
}

```

## Run task capability

```

function obj(name) {
return new ActiveXObject("klakaut.KlAk" + name);
}
try {
var oConnectProps = obj("Params"), oAdmServer = obj("Proxy"),
oTasks = obj("Tasks2"), item, enumObj, taskFound=false;
oConnectProps.Add("Address", "127.0.0.1:13291");
oAdmServer.Connect(oConnectProps);
oTasks.AdmServer = oAdmServer;
enumObj = new Enumerator(oTasks.EnumTasks(-1));
for (; !enumObj.atEnd(); enumObj.moveNext()) {
item = enumObj.item();
if (item.item('TASK_UNIQUE_ID') == '%task%') {
oTask = oTasks.GetTask(parseInt('%task%'));
oTasks.RunTask(parseInt('%task%'));
taskFound = oTask;
}
}
WScript.Echo(taskFound ? '[OK] Task #%task%:' + taskFound.item
('DisplayName') +
' successfully started.' : '[ERROR] Specified task #%task% was not found.');
} catch (e) {

```

```
WScript.Echo("[Error] " + e.number + " occurred !!! " + e.description);  
}
```

# Integration Guide for MAY Siber Scop NET

## Integration Overview

MAY Siber Scop NET is a NAC platform that provides visibility to any connected device across the network by integrating switches, routers and firewalls. This integration has been tested with MAY Siber Scop NET 7.1.17 version.

## Integration Capabilities

ArcSight SOAR has the following integration capability with MAY Siber Scop NET:

Block

### Use Case: Isolating Mal-behaving PC

With MAY Siber Scop NET integration, while responding an incident ATAR may block malbehaving computers' network access in order to contain the attack and prevent further spread of the attack. Blocking the host can be performed automatically within a playbook or manually by an analyst.

## Configuration

### Prerequisites

- SOAR connects to MAY Siber Scop NET API via HTTPS. Typically it runs on 443/tcp port. So access to this service is required.
- An API key is required for SOAR to connect to MAY Siber Scop NET.

### Configuring MAY Siber Scop NET

Login to MAY Siber Scop NET and create Web service key under **Settings > Global Settings > Web Service Key** menu.

### Configuring SOAR

1. Navigate to **Configuration > Credentials** and click **Create Credential**.
2. Fill the Credential Editor form as follows:

**a. Internal Credential:**

Type	Name	Username	Password	Private Key
Internal credential.	Display name of credential set (i.e., MAY Siber Scop NET Credential).	Empty.	Web Service Key you have created for ATAR on MAY Siber Scop NET.	Empty.

**b. Credential Store:**

Type	Name
External credential.	Name of the credential with pull path of the safe on store.

3. Navigate to **Configuration > Integrations** and click **Create Integration**.

4. Fill the configuration form as follows:

Parameter	Value
<b>Name:</b>	Display name of MAY Siber Scop NET integration on SOAR.
<b>Type:</b>	MAY Siber Scop NET.
<b>Address:</b>	Address of the integration (the format should be https://1.1.1.1 or https://abc.example.com).
<b>Configuration:</b>	You need to specify the following configuration parameters: <pre># Blocked by message customization # \$incident. for incident, \$rule. for rule ,\$alert. for alert # \$incident. for incident, \$rule. for rule ,\$alert. for alert # \$incident. for incident, \$rule. for rule ,\$alert. for alert # \$incident.serial\$ for incident serial, \$incident.subject\$ for incident # subject # \$rule.id\$ for rule id, \$rule.name\$ for rule name # for customize reasons followings can be uncomment #block.reason=Blocked by ATAR - \$incident.serial\$ \$incident.subject\$ #rollback.reason=Rollbacked by ATAR - \$incident.serial\$ \$incident.subject\$</pre>
<b>Credential:</b>	Name of the credential set you've just created on step 2. (i.e., MAY Siber Scop NET Credential).
<b>Trust Invalid SSL Certificates:</b>	Select this if Engine's certificate is self-signed or not recognized by browsers. Not selected.
<b>Require Approval From:</b>	Select user(s) from list to ask her/his approval before executing actions on this integration.
<b>Notify:</b>	Select user(s) from the list to notify when ATAR performs an action on this integration.

5. When you click the **Test** button a success message is displayed.

6. Click **Save** to complete integration.

# Integration Guide for McAfee ePolicy Orchestrator

## Integration Overview

McAfee ePolicy Orchestrator (ePO) is a management server for McAfee products which are used to protect endpoints from malware and network threats. It provides a centralized management console to simplify and accelerate the security effectiveness with visibility and control from device to cloud. This integration has been tested with McAfee ePolicy Orchestrator NET 5.10 version.

## Integration Capabilities

- SOAR has the following integration capabilities with McAfee ePolicy Orchestrator:
- Assign Policy
- Apply Tag
- Host Information
- Move Host
- Run Task
- Set TIE Reputation

### Use Case: Examining suspicious endpoint

With this integration, during the investigation of an incident SOAR may start an on-demand scan on a suspicious endpoint and may force new policy or move host to other place in system tree regarding scan result. This can be performed automatically within a playbook or manually by an analyst.

## Configuration

### Prerequisites

- SOAR connects to McAfee ePolicy Orchestrator API through HTTPS. Typically it runs on 8443/tcp port. So access to this service is required.
- An user account is required for SOAR to connect McAfee ePolicy Orchestrator.

## Configuration on McAfee ePolicy Orchestrator

1. Navigate to **User Management > Permission Sets** and create a permission set for SOAR with the following permissions:

<b>Endpoint Security Threat Prevention</b>	View and change task settings
<b>McAfee Agent</b>	View and change policy settings
<b>McAfee TIE Reputations</b>	View and change reputations
<b>Queries and Reports</b>	Use public groups.
<b>Systems</b>	Edit System Tree groups and systems & Apply, exclude, and clear tags
<b>System Tree access</b>	Can search on the following nodes and portions of the System
<b>Tree</b>	My Organization & Can access the following nodes and portions of the System

2. View and change policy settings for the products that you want SOAR to change policies for (for example: Endpoint Security Threat Prevention, Endpoint Security Firewall, Active Response, etc.)
3. Navigate **User Management > Users** and create a user with permission set you in previous step.

## Configuring SOAR

1. Navigate to **Configuration > Credentials** and click **Create Credential**.
2. Fill the Credential Editor form as follows:

### a. Internal Credential:

Type	Name:	Username:	Password:	Private Key:
Internal credential.	Display name of credential set (i.e., McAfee ePO Credentials).	Username you have configured on McAfee ePolicy Orchestrator.	Password for the user you have configured on McAfee ePolicy Orchestrator.	Empty.

### b. Credential Store:

Type:	Name:
External credential.	Name of the credential with pull path of the safe on store.

3. Navigate to **Configuration > Integrations** and click **Create Integration**.
4. Fill the configuration form as follows:

Parameter	Value
<b>Name</b>	Display name of McAfee ePolicy Orchestrator integration on ATAR.
<b>Type</b>	McAfee ePolicy Orchestrator.
<b>Address</b>	Address of the integration (the format should be <a href="https://192.168.2.100:8443">https://192.168.2.100:8443</a> ).
<b>Configuration</b>	You need to specify the following configuration parameters. For the first integration these values can be left as is:  <pre>system.move.autoSort=false clienttask.run.retryAttempts = clienttask.run.retryIntervalInSeconds = clienttask.run.abortAfterMinutes = clienttask.run.useAllAgentHandlers = clienttask.run.stopAfterMinutes= clienttask.run.randomizationInterval = policy.assignToSystem.resetInheritance=</pre>
<b>Credential</b>	Name of the credential set you've just created on step 2. (i.e., McAfeePO Credentials).
<b>Trust Invalid SSL Certificates</b>	Select this if Engine's certificate is self-signed or not recognized by browsers.
<b>Require Approval From</b>	Select user(s) from list to ask her/his approval before executing actions on this integration.
<b>Notify</b>	Select user(s) from the list to notify when SOAR performs an action on this integration.

5. When you click the **Test** button a success message is displayed.

6. Click **Save** to complete integration.

# Integration Guide for McAfee Network Security Platform (IPS)

## Integration Overview

McAfee Network Security Platform is an intrusion prevention system (IPS) to identify malicious network traffic and stops never-before-seen attacks for which no signatures exist. This integration has been tested with McAfee Network Security Platform 9.2.7.22 version.

## Integration Capabilities

SOAR has the following integration capabilities with McAfee Network Security Platform:

- Blacklist MD5 Hash
- Quarantine IP address

## Configuration

### Prerequisites

- SOAR connects to McAfee Network Security Platform's API via HTTPS. By default McAfee Network Security Platform REST-API interface works on 443/tcp port. So access permission to this port is required.
- A user account is required for SOAR to connect McAfee Network Security Platform.

## Configuration on McAfee Network Security Platform (IPS)

1. Navigate to **Manager > Users and Roles > Users** and create a user account with Super User role. In order to access API, Super User role is needed.
2. Navigate to **Devices** and note the device/sensor names.

# Configuring SOAR

1. Navigate **Configuration > Credentials** and click **Create Credential**.

2. Fill the Credential Editor form as follows:

**a. Internal Credential:**

Type	Name	Username	Password	Private Key
Internal credential.	Display name of credential set (i.e., McAfee NSP Credentials).	User you have created for SOAR on McAfee Network Security Platform.	Password of the user you have created for SOAR on McAfee Network Security Platform.	Empty.

**b. Credential Store:**

Type	Name
External credential.	Name of the credential with full path of the safe on store.

3. Navigate to **Configuration > Integrations** and click **Create Integration**.

4. Fill the configuration form as follows:

Parameter	Value
<b>Name</b>	Display name of McAfee Network Security Platform integration on SOAR.
<b>Type</b>	McAfee Network Security Platform.
<b>Address</b>	Address of the integration (the format should be <a href="https://192.168.2.2">https://192.168.2.2</a> ).
<b>Credential</b>	Name of the credential set you've just created on step 2. (i.e., McAfee NSP Credentials).
<b>Trust Invalid SSL Certificates</b>	Select this if Platform's certificate is self-signed or not recognized by browsers.
<b>Configuration</b>	You need to specify the following configuration parameters.  <pre># Name of ISP Devices/Sensors. SENSOR_NAME=SENSOR #proxy.id=5442</pre>
<b>Require Approval From</b>	Select user(s) from list to ask her/his approval before executing actions on this integration.
<b>Notify</b>	Select user(s) from the list to notify when SOAR performs an action on this integration.

5. When you click on the **Test** button a success message is displayed.
6. Click **Save** to complete integration.

# Integration Guide for McAfee Web Gateway

## Integration Overview

McAfee Web Gateway is a web filtering solution which utilizes both reputation and categorybased filtering and protection against zero-day malware as well. This integration has been tested with McAfee Web Gateway 7.7.2.8.0 version.

## Integration Capabilities

SOAR has the following integration capability with McAfee Web Gateway:

- Block URL

### Use Case: Blocking access to malicious URL

SOAR can integrate with McAfee Web Gateway to block malicious URLs detected while responding an incident. Blocking can be performed automatically within a playbook or manually by an analyst.

## Configuration

### Prerequisites

- SOAR connects to McAfee Web Gateway's API through HTTPS. By default McAfee Web Gateway REST-API interface works on 4712/tcp port. So access permission to this port is required.
- A user account for SOAR to connect to McAfee Web Gateway.

### Configuration on McAfee Web Gateway

1. Navigate to **Accounts** menu and add a new Role to be used for SOAR user. The new role should have at least “Rest-Interface Accessible” permission.
2. Navigate through Accounts menu and add an Internal Administrator Account with the role you have created in previous step.
3. Create a Wildcard Expression List under **Policy > Lists**.
4. Create a new rule and enable it under **Policy > Rule Sets > URL Filtering** menu to use list created in previous step. Rule criteria should be:

URL.Host matches in list ATARBlock

5. Save changes.

## Configuration on SOAR

1. Navigate **Configuration > Credentials** and click **Create Credential**.

2. Fill the Credential Editor form as follows:

### a. Internal Credential:

Type	Name	Username	Password	Private Key
Internal credential.	Display name of credential set (i.e., McAfee Web GW Credential).	User you have created for SOAR on McAfee Web Gateway.	Password of the user you have created for SOAR on McAfee Web Gateway.	Empty.

### b. Credential Store:

Type	Name
External credential.	Name of the credential with full path of the safe on store.

3. Navigate **Configuration > Integrations** and click **Create Integration**.

4. Fill the configuration form as follows:

Parameter	Value
Name	Display name of McAfee Web Gateway integration on SOAR
Type	McAfee Web Gateway
Address	Address of the integration (the format should be 192.168.1.1:4712)
Configuration	You need to specify the following configuration parameters:  <pre># Use the McAfee Web Gateway management interface to create the # list in Policy -&gt; Rule set -&gt; URL filtering section. SOAR will use # specified list name when adding blocked items. block.list.name=ATARBlock</pre>
Credential	Name of the credential set you've just created on step 2. (i.e., McAfeeWeb GW Credential)
Trust Invalid SSL Certificates	Select this if the certificate of the engine is self-signed or is not recognized by browsers
Require Approval From	Select users from the list who can provide approval before executing actions on this integration
Notify	Select users from the list to notify when SOAR performs an enrichment on this integration

5. On Integration editor, click **Show Additional Parameters** checkbox and set **ConnectionLimit** to “1” . Because of a limitation of McAfee Web Gateway, this value should never be greater than “1”.
6. When you click the **Test** button the following popup should be displayed if your credential and address is valid.
7. Click **Save** to complete integration.

## Integration Guide for McAfee Web Gateway v2

### Integration Overview

McAfee Web Gateway is a web filtering solution which utilizes both reputation and category-based filtering and protection against zero-day malware as well.

### Integration Capabilities

SOAR has the following integration capability with McAfee Web Gateway v2:

- Add Entry to List
- Remove Entry from List
- Get List Entries
- Get List Entry Details
- Get Lists

### Configuration

### Configuring McAfee Web Gateway v2

- Configure the **Username** and **Password** for McAfee Web Gateway v2.
- Enable **REST-Interface accessible** permission for the administrator role.

### Configuring SOAR

1. Navigate **Configuration > Credentials** and click **Create Credential**.
2. Specify the following parameter values in the Credential Editor form:

Parameter	Value
Type	Internal Credential
Name	Display name of credential set (For example, McAfee Web Gateway v2 Credential)
Username	<Username>
Password	<password>
Private Key	Empty

3. Click **Configuration > Integrations > Create Integration**.
4. Specify the following parameter values in the Configuration form:

Parameter	Value
Name	Display name of McAfee Web Gateway v2 integration on SOAR
Type	Advanced Scriptable Device
Address	https://{{base_url:port}}
Configuration	<p>Specify the following configuration parameters:</p> <pre>## Please use the McAfee Web Gateway management interface to create the list.</pre> <pre># ArcSight SOAR will use the specified list name when no List parameter is specified</pre> <pre># for the enrichment and action capabilities.</pre> <pre>default.list.name=ATARBlockList</pre> <pre># Integration ID of the proxy integration to use when connecting to current integration.</pre> <pre># If not provided, ArcSight SOAR will try to use a direct connection.</pre> <pre>#proxy.id=123</pre> <pre># Maximum number of results to return from the API.</pre> <pre># If not provided, the integration will gather all results.</pre> <pre>#max.result.count=100</pre>
Credential	Name of the credential set that you just created in step 2. (i.e., McAfeeWebGateway v2 Credentials)
Trust Invalid SSL Certificates	Select this if the certificate of the engine is self-signed or is not recognized by browsers
Require Approval From	Select users from the list who can provide approval before executing actions on this integration
Notify	Select users from the list to notify when SOAR performs an enrichment on this integration

- Click **Show Additional Parameters** and specify the following parameters in the Configuration form.

Parameter	Value
Batch Size	1
Connection Limit	1

- Click **Test**, an **Integration Successful** message is displayed if the credential and address are valid.
- Click **Save** to complete the integration.

## Capabilities

### 1. Add Entry to List

Action capability to take the List name/ID to be added, Value to be added, and Description of the entry being added, and adds entry to the list. An asterisk can be added to the beginning and/or end of the value.

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Value</b>	Entry value to add to the list	Network Address, Host, URL, Keyword, Unknown	Yes	Yes
<b>List</b>	Name or ID of the list. If not specified, the default list in the configuration will be used.	String	No	No
<b>Description</b>	Description of the list entry	String	No	No
<b>Prefix Asterix</b>	Add asterisk to the beginning of the 'Value' input	Checkbox	No	No
<b>Suffix Asterix</b>	Add asterisk should be added to the end of the 'Value' input	Checkbox	No	No

#### **Output:**

Case Scope

N/A

Human Readable Input

N/A

- Remove Entry from list

Action capability that takes the List name/ID and the Value of the entry to remove, then removes the entry from the list. An asterisk can be added to the beginning and/or end of the value.

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Value</b>	Entry value to remove from the list	Network Address, Host, URL, Keyword, Unknown	Yes	Yes
<b>List</b>	Name or ID of the list. If not specified, the default list in the configuration will be used.	String	No	No
<b>Prefix Asterix</b>	Add asterisk to the beginning of the <b>Value</b> input	Checkbox	No	No
<b>Suffix Asterix</b>	Add asterisk to the end of the <b>Value</b> input	Checkbox	No	No



Note: Suffix Asterix parameter is optional.

### Output:

Case Scope:

N/A

Human Readable Output

N/A

### 3. Get List Entries

Takes the List name and returns the entries.

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
Integration	McAfee Web Gateway v2	N/A	No	Yes
List	Name or ID of the list  If not specified, the default list in the configuration will be used	String	No	No

**Output:**

Case Scope

Action	Type	Category/Value
N/A	N/A	N/A

Human Readable Output:

Entry	Description
217.94.215.154	Potentially malicious IP from Germany (source: Abuse IPDB)
43.155.113.200	Potentially malicious IP from Hong Kong (source: Abuse IPDB)
173.231.197.16	Potentially malicious IP from United States (source: Abuse IPDB)
20.19.121.168	Potentially malicious IP from France (source: Abuse IPDB)
41.57.134.48	Potentially malicious IP from South Africa (source: Abuse IPDB)

**4. Get List Entry Details**

Takes the entry Value and List and retrieves the entry details.

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
Integration	McAfee Web Gateway v2	N/A	No	Yes
Value	Entry value to fetch details	Network Address, Host, URL, Keyword, Unknown	Yes	Yes
List	Name or ID of the list  If not specified, the default list in the configuration will be used	String	No	No

**Output:**

Case Scope

Action	Type	Category/Value
N/A	N/A	N/A

Human Readable Output:

Field	Value
List ID	com.scur.type.ip.4552
List Title	Allowed Clients
List Type	ip
Entry Value	8.8.8.8
Entry Description	Google IP

**5. Get Lists**

Enrichment capability that takes the list types and retrieves all available lists for the list type specified.

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
Integration	McAfee Web Gateway v2	N/A	No	Yes
Type	Type of the list	Type of the list such as All, IP, IP Range, Number, Regex, String	No	Yes

**Output:**

Case Scope:

Action	Type	Category/Value
N/A	N/A	N/A

Human Readable Output:

Id	Title	Type
com.scur.type.regex.272	ATARBlockList	regex
com.scur.type.string.263	ATARBlock	string
com.scur.list.applcntrl.data_analytics	Data Analytics	applcontrol
5145	Category Blocklist	category
5146	Upload Media Type Blocklist	mediatype

## Integration Guide for Micro Focus ArcSight ESM

See [Integrating SOAR with ESM](#)

## Integration Guide for ArcSight Intelligence

See [Integrating SOAR with Intelligence](#).

# Integration Guide for Micro Focus ArcSight Logger

## Integration Overview

ArcSight Logger is a log management solution for compliance, efficient log search, and secure storage.

## Integration Capabilities

ArcSight SOAR has the following integration capability with Micro Focus ArcSight Logger:

- Search Query

### Use Case: Investigating Cyber-attacks

Integrated with Micro Focus ArcSight Logger, ATAR requires logs collected from various enterprise systems to enrich incident ticket, and improve analyst's understanding of incident.

## Configuration

### Prerequisites

- Currently SOAR supports Micro Focus ArcSight Logger version 6.3.1.7874.0 and later. SOAR connects to Micro Focus ArcSight Logger API using HTTPS. By default REST-API interface works on 443/tcp port. So access permission to this port is required.
- A user account is required for ATAR to connect Micro Focus ArcSight Logger.

### Configuration on Micro Focus ArcSight Logger

- Click **System Admin > Users/Groups > User Management** and add a user account with **Default Logger Search Group**.

## Configuring SOAR

### Configuring SOAR

1. Click **Configuration > Credentials > Create Credential**.
2. Specify the following parameter values in the **Credential Editor**:
  - a. **Internal Credential**

Parameter	Value
Type	Internal Credential
Name	Display name of credential set (For example, ArcSight Logger Credentials)
Username	User you have created for ATAR on Micro Focus ArcSight Logger.
Password	Password of the user you have created for ATAR on Micro Focus ArcSight Logger.
Private Key	Empty

- b. **Credential Store:**

Parameter	Value
Type	External Credential
Name	Name of the credential with pull path of the safe on store

3. Click **Configuration > Integrations > Create Integration**.
4. Specify the following parameter values in the **Configuration** form:

Parameter	Value
Name	Display name of Micro Focus ArcSight Logger integration on SOAR
Type	Micro Focus ArcSight Logger
Address	Address of the integration (the format must be https://192.168.12.6)

Parameter	Value
Configuration	<p>Specify the following configuration parameters:</p> <pre>events.pageLength=10000 # configure how far (in minutes) into the past this enrichment will look. #cache.reusing.duration=20 # local search enabling parameter for Search Query capability. # If this is set false, ATAR will perform searches on all nodes. #local.search.enabled=false # use master session while fetching events from peers for Search Query. # If this is set true, ATAR will use the same session ID while performing # searches on the other nodes. #reuse.master.session=false # peers credential list (if master session won't be shared) # peer address and credential ID values must be separated with : # additional peer-credential pairs must be separated with   #peer.credential.list=1.1.1.1:CredentialId 2.2.2.2:CredentialId</pre>
Credential	Name of the credential set created on step 2 (For example, ArcSight Logger Credentials)
Trust Invalid SSL Certificates	Select this if Engine's certificate is self-signed or is not recognized by browsers

5. Click **Test** to test the integration.
6. Click **Save** to complete the integration.

## Additional Notes

- In order to execute queries on Micro Focus ArcSight Logger, you should create query scripts with **ArcSight Logger Query** type under **Configuration -> Customization Library**.
- SOAR extracts scope items on columns defined as Artifact in the query script. For example,  
`// Artifact: deviceCustomNumber1Label | KEYWORD | RELATED`

# Integration Guide for Microsoft Active Directory

## Integration Overview

**Microsoft Active Directory** is an umbrella title for directory-based identity related services that Microsoft developed for the Windows domain networks.

ArcSight SOAR has the following integration capabilities with Microsoft Active Directory:

- Add user to a group
- Remove user from a group
- Lock user account
- Get user information
- Get user's groups
- Get group list
- Get group information
- Get computer information
- List computers on domain
- Fetch a domain object

### Use Case: Compromised user account

During the investigation of the attack SOAR can ask Microsoft Active Directory the details of the user account suspicious to be compromised, check the groups account belongs to, locks the account, fetches her/his manager's information and send a notification e-mail to manager if needed.

This can be performed automatically within a playbook or manually by an analyst.

## Configuration

### Prerequisites

- SOAR connects to Microsoft Active Directory using LDAPS protocols. Access to 636/tcp
- port is required.
- A domain user account is required for SOAR to connect Microsoft Active Directory.

## Configuration on Microsoft Active Directory

- Create a user account on Domain Controller with no password expiry.
- Add this user into “Account Operators” group. Members of this group can manage groups and accounts on domain except domain admins.

## Configuring SOAR

1. Navigate **Configuration > Credentials** and click **Create Credential**.
2. Fill the Credential Editor form as follows:

**a. Internal Credential:**

Type	Name:	Username	Password	Private Key
Internal credential.	Display name of credential set (i.e., Microsoft AD Credentials).	User you have created for SOAR on Microsoft Active Directory (the format should be username@domain).	Password of the user you have created for SOAR on Microsoft ActiveDirectory.	Empty.

**b. Credential Store:**

Type	Name
External credential.	Name of the credential with pull path of the safe on store.

3. Navigate to **Configuration > Integrations** and click **Create Integration**.
4. Fill the configuration form as follows:

Parameter	Value
Name	Display name of Microsoft Active Directory integration on SOAR.
Type	Microsoft Active Directory.
Address	Address of the integration (the format should be 192.168.2.2:636).

Parameter	Value
Configuration	<p>You need to specify the following configuration parameters.</p> <pre># SOAR will search objects under LDAP searchbase specified. # Format should be "DC=EXAMPLE,DC=COM" ldap.searchbase=DC=EXAMPLE,DC=COM # LDAP domain should be like "example.com" ldap.domain=example.com # LDAP NT domain name should be like "EXAMPLE" ldap.ntdomain=EXAMPLE # Username for LDAP service availability check. # SOAR will try to bind LDAP service as this user. ldap.checkavailabilityuser=testuser01@example.com # configure how far (in minutes) into the past this enrichment will look.  cache.reusing.duration=30</pre>
Credential	Name of the credential set you've just created on step 2. (i.e., Microsoft AD Credentials).
Trust Invalid SSL Certificates	Select this if Engine's certificate is self-signed or not recognized by browsers.
Require Approval From	Select user(s) from list to ask her/his approval before executing actions on this integration.
Notify	Select user(s) from the list to notify when SOAR performs an action on this integration.

5. Click on the **Test** button.
6. Click **Save** to complete integration.

# Integration Guide for Microsoft Azure Active Directory

## Integration Overview

**Azure Active Directory (Azure AD)** is Microsoft's cloud-based identity and access management service. It helps users to sign-in and access both external and internal resources, for example Microsoft 365, Azure portal, SaaS applications and many more.

## Integration Capabilities

ArcSight SOAR has the following integration capabilities with Azure Active Directory:

- Add User to Group
- Disable User
- Enable User
- Get User Details
- Get User's Manager
- List Groups
- List User's Groups
- List Users
- Remove User from Group
- Revoke Sessions
- Create Group
- Delete Group
- List Delegated Permissions

## Prerequisites

You must have access to HTTPS as the ArcSight SOAR connects to Azure Active Directory API through this service.

# Configuration

## Configuring Microsoft Azure

1. Log in to [Azure Portal](#) and navigate to **Azure Active Directory** service.
2. Click **App Registrations** tab to create a new registration with the following values:

Name	Supported Account Types	Redirect URL
ArcSight SOAR	Accounts in the organizational directory (Default Directory only - Single tenant)	(Web) <a href="https://localhost/soar">https://localhost/soar</a>

3. Navigate to **Add a certificate or secret > Client secret** to create a client secret. Add ArcSight SOAR as description and specify the expiry period as 24 months.
4. Note down the **Secret Key** value and **Client ID**.
5. Navigate to **API Permissions** and add the following permissions:

Permission Type	Permission	Description
Delegated	Directory Access as user All	Access directory as the signed in user
Application	Directory Read write All	Read and write directory data
Application	User Read write All	Read and write all users' full profiles.

6. Click **Yes** to grant admin consent for **Default Directory**.

## Configuring SOAR

1. Click **Configuration > Credential > Create Credential**.
2. Specify the following parameter values in the **Credential Editor** form:

Type	Name	Username	Password	Private Key
Internal credential	Display name of credential set (for example, Azure AD Credentials).		Client ID of the application (for example, ArcSight SOAR) that you registered on Azure portal.	Secret Key

3. Click **Configuration > Integrations > Create Integration**.

4. Specify the following parameter values in the **Configuration** form:

Parameter	Value				
<b>Name</b>	Display name of the integration.				
<b>Type</b>	Microsoft Azure Active Directory.				
<b>Address</b>	Address of the integration (for example, <a href="https://graph.microsoft.com/v1.0">https://graph.microsoft.com/v1.0</a> ).				
<b>Configuration</b>	<p>Specify the following configuration parameters:</p> <table border="1"> <tr> <td><b>list.name</b></td><td>Tenant ID on Microsoft Azure tenant.id = ff1f0000-c600-4500-0038-9d4000000000</td></tr> <tr> <td><b>proxy.id</b></td><td>ID of the Proxy integration if you access Microsoft Azure Active Directory through a web proxy device. For example, proxy.id = 12345 .</td></tr> </table>	<b>list.name</b>	Tenant ID on Microsoft Azure tenant.id = ff1f0000-c600-4500-0038-9d4000000000	<b>proxy.id</b>	ID of the Proxy integration if you access Microsoft Azure Active Directory through a web proxy device. For example, proxy.id = 12345 .
<b>list.name</b>	Tenant ID on Microsoft Azure tenant.id = ff1f0000-c600-4500-0038-9d4000000000				
<b>proxy.id</b>	ID of the Proxy integration if you access Microsoft Azure Active Directory through a web proxy device. For example, proxy.id = 12345 .				
<b>Credential</b>	Credential that has been defined for this integration under the <b>Credentials</b> menu.				
<b>Trust Invalid SSL Certificates</b>	Select this if web server's certificate is self-signed or is not recognized by browsers.				
<b>Require Approval From</b>	Select users from the list who can provide approval before executing actions on this integration				
<b>Notify</b>	Select users from the list to notify when SOAR performs an enrichment on this integration				

5. Click **Save** to save the integration definition.
6. Navigate to **Configuration>Customization Library** and edit **Microsoft Azure Active Directory Advanced Action Script Default Template**.
7. Select the integration that you have added to **Integrations** menu.
8. Click **Save** to complete the integration
9. Click **Test**, an **Integration Successful** message is displayed if the credential and address are valid.

## Capabilities

### 1. Add User to Group

Action capability for adding a user to given AD group.

- Rollback: Yes
- Duplicate Control: No

The following table provides the **Add User to Group** action capability details:

Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Integration</b>	Name of the third-party integration.	Integration	N/A	Yes
<b>Rollback Mode</b>	Time to rollback this action. Default is no-rollback.	N/A	N/A	No
<b>User</b>	Username to be added to group	Username Email Address Keyword Unknown	Yes	Yes
<b>Group ID</b>	Target group ID	String	No	Yes

**Output:**

Case Scope: N/A

Human Readable Output: N/A

**2. Disable User**

Action capability for disabling user account by blocking the sign-in procedure.

- Rollback: Yes
- Duplicate Control: No

The following table provides the **Disable User** action capability details:

Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Integration</b>	Name of the third-party integration.	Integration	N/A	Yes
<b>Rollback Mode</b>	Time to rollback this action. Default is no-rollback.	N/A	N/A	No
<b>User</b>	Username to be disabled.	Username Email Address Keyword Unknown	Yes	Yes

**Output:**

Case Scope: N/A

Human Readable Output: N/A

**3. Enable User**

Action capability for enabling user account by removing sign-in block.

- Rollback: Yes
- Duplicate Control: No

The following table provides the **Enable User** action capability details:

Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Integration</b>	Name of the third-party integration.	Integration	N/A	Yes
<b>Rollback Mode</b>	Time to rollback this action. Default is no-rollback.	N/A	N/A	No
<b>User</b>	Username to be enabled	Username Email Address Keyword Unknown	Yes	Yes

#### **Output:**

Case Scope: N/A

Human Readable Output: N/A

#### **4. Get User Details**

Enrichment capability for retrieving user details.

The following table provides the **Get User Details** enrichment capability details:

Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Integration</b>	Name of the third-party integration.	Integration	N/A	Yes
<b>User</b>	User to be queried from Active Directory	Username Email Address Keyword Unknown	Yes	Yes

#### **Output:**

Case Scope:

Action	Type	Category/ Value
<b>None</b>	N/A	N/A

Human Readable Output:

Key	Value
Name	Neil Philip
Login	neil@ <a href="https://contoso.onmicrosoft.com">contoso.onmicrosoft.com</a>
Job Title	QA & Test Engineer
Mail	neil@ <a href="https://contoso.onmicrosoft.com">contoso.onmicrosoft.com</a>
Mobile	+61 555 555 555
Office	
User ID	c6eced54-bda4-41f2-948f-55f1a31b30e4

## 5. Get User's Manager

Enrichment capability for retrieving user's manager.

The following table provides the **Get User's Manager** enrichment capability details:

Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Integration</b>	Name of the third-party integration.	Integration	N/A	Yes
<b>User</b>	User to be queried for manager's information.	Username Email Address Keyword Unknown	Yes	Yes

### Output:

Case Scope:

Action	Type	Category/ Value
<b>None</b>	N/A	N/A

### Human Readable Output:

Key	Value
Name	Ursula Carmine
Login	ursula@ <a href="https://contoso.onmicrosoft.com">contoso.onmicrosoft.com</a>
Job Title	QA Manager
Mail	ursula@ <a href="https://contoso.onmicrosoft.com">contoso.onmicrosoft.com</a>
Mobile	+61 999 999 999
Office	+61 999 999 999
User ID	3c0b44b8-3305-4d63-864b-01bf915abe

## 6. List Groups

Enrichment capability for retrieving AD group list.

The following table provides the **List Groups** enrichment capability details:

Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Integration</b>	Name of the third-party integration.	Integration	N/A	Yes

### Output:

**Case Scope:**

Action	Type	Category/ Value
None	N/A	N/A

**Human Readable Output:**

Name	Description	Group Mail	Created Time	Group Id
QATeam	QA & Test Team		2021-07-23T08:46:54Z	79444ee61-6459-4d7d-9fb5-25923ed0d43
DevTeam	Development Team		2021-07-23T08:46:32Z	9c581fcf-6d25-47b3-be65-31b6257b2ea2
Red Team	Red Team		2021-08-06T13:27:19Z	c94b4b18-f661-441e-9b01-eaa695c800b4
Blue Team	Blue Team		2021-08-06T13:26:49Z	d2b52062-852c-4a77-eac4-9be91423c255

**7. List User's Groups**

Enrichment capability for retrieving the list of groups for a specified username.

The following table provides the **List User's Group** enrichment capability details:

Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Integration</b>	Name of the third-party integration.	Integration	N/A	Yes
<b>User</b>	User to be queried for group memberships.	Username Email Address Keyword Unknown	Yes	Yes

**Output:****Case Scope:**

Action	Type	Category/ Value
None	N/A	N/A

**Human Readable Output:**

Name	Description	Group Mail	Created Time	Group Id
DevTeam	Development Team		2021-07-23T08:46:32Z	9c581fcf-6d25-47b3-be65-31b6257b2ea2
Purple Team	Purple Team		2021-08-06T13:29:48Z	d553b299-17e2-407c-98f9-4dcbff9eb992

**8. List Users**

Enrichment capability for retrieving list of users.

The following table provides the **List Users** enrichment capability details:

Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Integration</b>	Name of the third-party integration.	Integration	N/A	Yes

**Output:**

Case Scope:

Action	Type	Category/ Value
<b>None</b>	N/A	N/A

## Human Readable Output:

Name	Job Title	Principal Name	User Id
Carl Sagan	Senior Developer	carl@*****.onmicrosoft.com	b1a4eb78-d005-451c-96d8-b0a5379d0b9f
John M. Green	SW Engineer	john@*****.onmicrosoft.com	fe3c39ab-c5f0-4b1f-99f3-8707bd7a4d4c
Ahmet Ozturk		matt@*****.onmicrosoft.com	69de5fe1-bfa1-44dd-82fb-8ac37dd9ad44
Neil Philip	QA & Test Engineer	neil@*****.onmicrosoft.com	cbeecd54-bda4-41f2-948f-55f1a31b30e4
Ursula Carmine	QA Manager	ursula@*****.onmicrosoft.com	3c0b44b8-3305-4d63-864b-01fbef915abe

**9. Remove User from Group**

Action capability for removing a user from given AD group.

- Rollback: Yes
- Duplicate Control: No

The following table provides the **Remove Users Group action** capability details:

Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Integration</b>	Name of the third-party integration.	Integration	N/A	Yes
<b>Rollback Mode</b>	Time to rollback this action. Default is no-rollback.	N/A	N/A	No
<b>User</b>	Username to be removed from group	Username Email Address Keyword Unknown	Yes	Yes
<b>Group ID</b>	Target group ID	String	No	Yes

**Output:**

Case Scope: N/A

Human Readable Output: N/A

## 10. Revoke Sessions

Action capability to revoke all the refresh action of the user and session tokens issued to applications, by resetting the **signInSessionsValidFromDateTime** user property to the current date.

This forces the user to sign in to those applications again.

- Rollback: No
- Duplicate Control: Yes

The following table presents the **Revoke Sessions** enrichment capabilities details:

Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Integration</b>	Name of the third-party integration.	Integration	N/A	Yes
<b>Rollback Mode</b>	Time to rollback this action. Default is no-rollback.	N/A	N/A	No
<b>User</b>	Username to be forced to revoke (terminate) sign-in sessions.	Username Email Address Keyword Unknown	Yes	Yes

### Output:

Case Scope: N/A

Human Readable Output: N/A

## 11. Create Group

Action capability for creating a new group from a given AD.

- Rollback: No
- Duplicate Control: No

The following table provides the **Create Group** action capability details:

Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Integration</b>	Name of third-party integration	Integration	N/A	Yes
<b>Group Nickname</b>	The mail alias for the group, unique for Microsoft 365 groups in the organization.  Maximum length is 64 characters.  This property can contain only characters in the ASCII character set 0 - 127 except the following: @ () \ [] " ; : . <> , SPACE.	String	No	Yes

Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Group Name</b>	The name to display in the address book for the group.  Maximum length: 256 characters	String	No	Yes
<b>Description</b>	A brief description about the group	String	No	Yes

**Output:**

Case Scope: N/A

Human Readable Output: N/A

**12. Delete Group**

Action capability to delete a group from a given AD.

- Rollback: No
- Duplicate Control: Yes

The following table provides the **Delete Group** action capability details:

Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
Integration	Name of the third-party integration	Integration	N/A	Yes
Group Nickname	Nickname of the group to be queried from Active Directory	String	No	Yes

**Output:**

Case Scope:

N/A

Human Readable Output:

N/A

**13. List Delegated Permissions**

Enrichment capability to list delegated permissions.

The following table represents the **List Delegated Permissions** enrichment capabilities details:

Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
Integration	Name of the third-party integration	Integration	N/A	Yes
User	User to be queried from Active Directory	Username Email Address Keyword Unknown	Yes	Yes

**Output:**

Case Scope: N/A

Human Readable Output:

Client Id	Consent Type	Principal Name	Resource Name	Scope
346054c8-18cf-419a-9414-917c1b6a14a0	Principal	hirenpatel@sacuman.onmicrosoft.com	Microsoft Graph	Directory.AccessAsUser.All openid profile offline_access

# Integration Guide for Microsoft Defender for CloudApps

## Integration Overview

Microsoft Defender for Cloud Apps is a Cloud Access Security Broker (CASB) that supports various deployment modes including log collection, API connectors, and reverse proxy. It provides visibility, control over data travel, and sophisticated analytics to identify and combat cyber threats across all your Microsoft and third-party cloud services.

## Integration Capabilities

- Close Alert as Benign
- Close Alert as False Positive
- Close Alert as True Positive
- Get Alert by ID
- Get Entity Details
- List Activities

- List Activities by IP
- List Activities by User
- List Activities by User Domain
- List Alerts
- List Alerts by IP
- List Alerts by Severity
- List Alerts by Status
- List Entities
- List IP Ranges
- Mark Alert as Read
- Mark Alert as Unread

## Prerequisites

ArcSight SOAR connects to login.microsoft.com and \*.portal.cloudappsecurity.com APIs through HTTPS. Access to these services is required.

## Configuration

### Configuring Microsoft Defender for CloudApps

1. Log in to portal.azure.com.
2. Navigate to **Azure Active Directory service > App Registrations** to create a New Registration with the following values:

Name	Supported Account Types	Redirected URL
ArcSight SOAR	Accounts in this organizational directory only (Default Directory only - Single tenant)	https://localhost/soar (web)



If you have already defined an application for other integrations and want to use it, you can skip steps 1-4.

3. Click Add a certificate or secret to create a new Client Secret for the application you have registered and specify the following fields:

Description	Expiry
ArcSight SOAR	24 months

4. Note down the **Secret Key** along with **Client ID**.

5. Navigate to **API Permissions** and add the following permissions from Microsoft Cloud App Security:

Permission Type	Permission	Description
Application	Investigation.manage	Manage alerts, activities, policies, and other investigation-related information
Application	Investigation.read	View alerts, activities and policies

6. Grant admin consent for Default Directory.
7. Log in to **Defender for cloudsApps** portal and click on ? icon. Under **About**, please note the portal URL value (for example, `https://<tenant_id><tenant_region>.portal.cloudappsecurity.com`). This will be used as Integration address.

## Configuring SOAR

1. Click **Configuration > Credential > Create Credential**.
2. Fill the **Crdential Editor** form with following parameter values:

Type	Internal credential
Name	Display name of credential set ( i.e, Microsoft Defender for Cloud Apps Credentials)
Username	<Empty>
Password	Client ID of the application (i.e., ArcSight SOAR) you've registered on Azure Portal.
Private Key	Secret Key

3. Click **Configuration > Integrations > Create Integration**.
4. Fill the configuration form with the following parameter values:

Parameter	Value
Name	Display name of the Integration
Type	Microsoft Defender for CloudApps
Address	Address of the integration ( <code>https://&lt;tenant_id&gt;&lt;tenant_region&gt;.portal.cloudappsecurity.com</code> )

Parameter	Value	
Configuration	Specify the following configuration parameter:	
	tenant.id	Tenant ID on Microsoft Azure tenant.id = ff1f0000-c600-4500-0038-9d4000000000
	proxy.id	ID of the Proxy integration if you access Cisco Firepower Management Center through a web proxy device. For example: proxy.id = 12345
	cache.reusing.duration	Configure how far (in minutes) into the past this enrichment will look. cache.reusing.duration=20
Credential	Credential that has been defined for this integration under the Credentials menu.	
Trust Invalid SSL Certificates	Select this if web server's certificate is self-signed or is not recognized by browsers	
Require Approval From	Select user(s) from list to ask her/his approval before executing actions on this integration	
Notify	Select user(s) from the list to notify when SOAR performs an action on this integration	

5. Click **Save** to save the integration definition.
6. Navigate to **Configuration > Customization Library** and edit **Microsoft Defender for Cloud Apps Advanced Action Script Default Template**.
7. Select the integration you have added to **Integrations** dropdown menu.
8. Click **Save** to complete the integration
9. Edit the integration under **Configuration > Integrations** and Click **Test**. A Integration Successfull message will be displayed if your credential and address are valid.



Steps 6-8 are required only for Advanced Action Script Default Templates.

## Capabilities

### 1. Close Alert as Benign

Action capability for closing security alert as benign on Microsoft Defender for Cloud Apps portal.

- Rollback: No
- Duplicate Control: No

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
Alert ID	Alert ID on Defender for Cloud Apps portal.	String	No	Yes
Comment	Comment added to the alert on Defender for Cloud Apps portal	String	No	Yes
Reason	Closing reason added to the alert on Defender for Cloud Apps portal	String  Actual severity is lower  Confirmed with end user  Triggered by test Other	No	Yes

**Output:**

Case Scope

N/A

Human Readable Output

N/A

**2. Close Alert as False Positive**

Action capability for closing security alert as false positive on Microsoft Defender for Cloud Apps portal

- Rollback: No
- Duplicate Control: No

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
Alert ID	Alert ID on Defender for Cloud Apps portal.	String	No	Yes
Comment	Comment added to the alert on Defender for Cloud Apps portal	String	No	Yes
Reason	Closing reason added to the alert on Defender for Cloud Apps portal	String  Alert is not accurate  Not of interest  Too many similar alerts  Other	No	Yes

**Output:**

Case Scope

N/A

Human Readable Output

N/A

### 3. Close Alert as True Positive

Action capability for closing security alert as true positive on Microsoft Defender for Cloud Apps portal

- Rollback: No
- Duplicate Control: No

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
Alert ID	Alert ID on Defender for Cloud Apps portal.	String	No	Yes
Comment	Comment added to the alert on Defender for Cloud Apps portal	String	No	Yes

#### Output:

Case Scope

N/A

Human Readable Output

N/A

### 4. Mark Alert as Read

Action capability for marking the security alert as read.

- Rollback: No
- Duplicate Control: No

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
Integration	Name of the third party integration	Integration	N/A	Yes
Alert ID	Alert ID on Defender for Cloud Apps portal	String	No	Yes

#### Output:

Case Scope

N/A

Human Readable Output

N/A

### 5. Mark Alert as Unread

Action capability for marking the security as unread.

- Rollback: No

- Duplicate Control: No

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
Integration	Name of the third party integration	Integration	N/A	Yes
Alert ID	Alert ID on Defender for Cloud Apps portal	String	No	Yes

#### Output:

Case Scope

N/A

Human Readable Output

N/A

## 6. Get Alert by ID

Enrichment capability for querying & retrieving security alert details by alert ID.

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
Integration	Name of the third party integration	Integration	N/A	Yes
Alert ID	Alert ID on Defender for Cloud Apps portal.	String	No	Yes

#### Output:

Case Scope

Action	Type	Category/Value
None	N/A	N/A

Human Readable Output

Key	Value
Title	Logon from a risky IP address
Description	Activity policy 'Logon from a risky IP address' was triggered by 'Ahmet Ozturk ( [REDACTED] .onmicrosoft.com)'.
Severity	High
Status	Read
Resolution Status	Open
Stories	[ "Threat Detection" ]
Evidence	N/A
Intent	[ "Unknown" ]
Entities	[ { "label": "Logon from a risky IP address", "type": "policyRule", "policyType": "AUDIT", "id": "62b850c45e6c2f7bd12af2" }, { "entityType": 2, "em": "[REDACTED].onmicrosoft.com", "label": "Ahmet Ozturk", "type": "account", "pa": "[REDACTED].onmicrosoft.com", "saas": 11161, "inst": 0, "id": "d9ace34f-e0ce-4a3a-9921-2680f11169a0" }, { "label": "[REDACTED].onmicrosoft.com", "type": "user", "id": "9921-2680f11169a0" }, { "label": "Microsoft Defender for Cloud Apps", "type": "service", "id": 20595 }, { "label": "AU", "type": "country", "id": "AU" } ]
Threat Score	40
Alert Id	63046032c48dd33f77278a2
Alert Time	2022-08-23T05:05:51.0Z
Alert Timestamp	1661231151874

## 7. List IP Ranges

Enrichment capability for getting list of IP Ranges defined. Query returns maximum 100 items.

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
Integration	Name of the third party integration	Integration	N/A	Yes

### Output:

Case Scope

Action	Type	Category/Value
None	N/A	N/A

### Human Readable Output

ID	Name	Category	Subnets	Location	Tags	Last Modified
62fb849edf907614b4a52a16	Sydney-HQ	VPN	[ "192.168.1.100/24" ]	{ "latitude": -25.72810364, "countryCode": "AU", "name": "Australia", "countryName": "Australia", "longitude": 134.4901886 }	[ "Custom_tag1", "Custom_tag2" ]	2022-08-18T13:16:38.0Z
62fe31e6199de67916075ae8	Risky IP Ranges	Risky	[ "192.168.1.100/24", "192.168.1.101/24" ]		N/A	2022-08-18T12:34:46.0Z

## 8. Get Entity Details

Enrichment capability for retrieving entity details.

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
Integration	Name of the third party integration	Integration	N/A	Yes
Entity	Entity queried on Defender for Cloud Apps portal. It is represented as a dictionary with the entity ID, SaaS, and instance details. For example:  {"id":"3fa9f28b-eb0e-463a-ba7b-8089fe9991e2","saas":11161,"inst":0}	Username Keyword Unknown	Yes	Yes

### Output:

Case Scope

Action	Type	Category/Value
None	N/A	N/A

### Human Readable Output

Key	Value
Name	Neil Young
Email	neil.young@████████.com
Role	User
Groups	[ "External users" ]
Domain	████████.com
Organization	N/A
Threat Score	N/A
App. Name	Okta Dev-14556012
Status	Active

## 9. List Activities

Enrichment capability for getting list of activities in given time range. Results are ordered by create time from newest to oldest. Query returns maximum 100 items.

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Integration</b>	Name of the third party integration	Integration	N/A	Yes
<b>Time Range</b>	Time range filter for query  Relative: e.g. Last 5 days  Absolute: e.g. 2022-08-14 15:10 – 2022-08-14 15:32	Time range.	N/A	Yes

### Output:

Case Scope

Action	Type	Category/Value
None	N/A	N/A

### Human Readable Output:

Activity Date	App. Name	Description	User	Client Ip	Device Type	Id
2022-09-07T02:55:56.0Z	Microsoft Azure	Write Settings: resource <!--myusage--> - <--Succeeded-->	████████.onmicrosoft.com	49.████████.████████.████	N/A	224c1af7881131fea2b6863faa362ef5a418e367a183f7d0ee648f2662175265
2022-09-07T02:55:54.0Z	Microsoft Azure	Write Settings: resource <!--myusage--> - <--Started-->	████████.onmicrosoft.com	49.████████.████████.████	N/A	0753b2c0leaf16fc8c649a33f9db92e1a6d9e30a20065e503559ae741d5ba78
2022-09-07T02:55:36.0Z	Microsoft Azure	GetEntities Microsoft.Management: resource <!--/providers/Microsoft.Management--> - <--Succeeded-->	████████.onmicrosoft.com	49.████████.████████.████	N/A	cbd1bee164f3b89a5a01bee11ead9862ef0fa7d9de4b68ee914a8e989550df
2022-09-07T02:55:35.0Z	Microsoft Azure	GetEntities Microsoft.Management: resource <!--/providers/Microsoft.Management--> - <--Started-->	████████.onmicrosoft.com	49.████████.████████.████	N/A	e7d46a1fce9810cbc9f8f54ddd60e7a82648ba6e61270994d928c66b8753b71
2022-09-07T02:33:38.0Z	Microsoft Azure	GetEntities Microsoft.Management: resource <!--/providers/Microsoft.Management--> - <--Succeeded-->	509e4652-da8d-478d-a730-e9d4a1996ca4	52.████████.████████.████	N/A	b9fa206917ca3284f584e291686e8ab53cc9c0373fc9db1b928f1b02ee4e3

## 10. List Activities by IP

Enrichment capability for getting list of activities by IP address in given time range. Results are ordered by create time from newest to oldest. Query returns maximum 100 items.

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
Integration	Name of the third party integration	Integration	N/A	Yes
IP Address	Client IP address to filter activities	Network Address	Yes	Yes
Time Range	Time range filter for query	Time range. Relative: e.g. Last 5 days Absolute: e.g. 2022-08-14 15:10 – 2022-08-14 15:32	N/A	Yes

Output:

Action	Type	Category/Value
None	N/A	N/A

Human Readable Output:

Activity Date	App. Name	Description	User	Client Ip	Device Type	Id
2022-09-07T02:33:38.0Z	Microsoft Azure	GetEntities Microsoft.Management:resource <!-->/providers/Microsoft.Management:resource <!-->-><b>Succeeded</b>	509e4652-da8d-478d-a730-e9d4a1996ca4	52. [REDACTED]	N/A	b9fa206917fc3284f584e291686e8ab53bc9c0373f1c9db1b9281fb02ee4e3
2022-09-07T02:33:38.0Z	Microsoft Azure	GetEntities Microsoft.Management:resource <!-->/providers/Microsoft.Management:resource <!-->-><b>Started</b>	509e4652-da8d-478d-a730-e9d4a1996ca4	52. [REDACTED]	N/A	4cf8491d4934c8a77c070312c4017db4eaceea615b6f42b89e8ed5423d442f62
2022-09-06T14:33:37.0Z	Microsoft Azure	GetEntities Microsoft.Management:resource <!-->/providers/Microsoft.Management:resource <!-->-><b>Succeeded</b>	509e4652-da8d-478d-a730-e9d4a1996ca4	52. [REDACTED]	N/A	f7776964be7af0ff01a11b167824c15ef10ac735b1a52ae0a1d9ddda2132e2bb
2022-09-06T14:33:37.0Z	Microsoft Azure	GetEntities Microsoft.Management:resource <!-->/providers/Microsoft.Management:resource <!-->-><b>Started</b>	509e4652-da8d-478d-a730-e9d4a1996ca4	52. [REDACTED]	N/A	df614fe388a02bd3dc3d77f3764c1e5dbab4a34d99f680b074239de6a8a5d79d
2022-09-06T02:33:38.0Z	Microsoft Azure	GetEntities Microsoft.Management:resource <!-->/providers/Microsoft.Management:resource <!-->-><b>Succeeded</b>	509e4652-da8d-478d-a730-e9d4a1996ca4	52. [REDACTED]	N/A	8f730d550d44de6ce2cffb128dad22426592e990c02ed5a4346169bc18972015

## 11. List Activities by User

Enrichment capability for getting list of activities for a username in given time range. Results are ordered by create time from newest to oldest. Query returns maximum 100 items.

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
Integration	Name of the third party integration	Integration	N/A	Yes
Username	Username to filter activities.	Username Email Address Keyword Unknown	Yes	Yes
Time Range	Time range filter for query	Time range. Relative: e.g. Last 5 days Absolute: e.g. 2022-08-14 15:10 – 2022-08-14 15:32	N/A	Yes

**Output:**

Action	Type	Category/Value
None	N/A	N/A

**Human Readable Output**

Activity Date	App. Name	Description	User	Client Ip	Device Type	Id
2022-08-16T13:53:39.0Z	Okta Dev-14556012	Log out	ursula.ross@████████.com	49.████████	DESKTOP	106670475_10980_d5295d1f-1d5a-11ed-ba66-75033b9afa52
2022-08-16T11:57:13.0Z	Okta Dev-14556012	Single sign-on log on	ursula.ross@████████.com	49.████████	DESKTOP	106670475_10980_90e3492c-1d5a-11ed-b281-01b31e94283
2022-08-16T11:57:09.0Z	Okta Dev-14556012	Log on	ursula.ross@████████.com	49.████████	DESKTOP	106670475_10980_8ed7e8fc-1d5a-11ed-ac90-af9ccad2bf0e
2022-08-16T11:57:09.0Z	Okta Dev-14556012	Change password: user <b>ursula.ross@████████.com</b>	ursula.ross@████████.com	N/A	N/A	106670475_10980_8ed095fb-1d5a-11ed-ac90-af9ccad2bf0e
2022-08-16T11:57:03.0Z	Okta Dev-14556012	user.authentication.verify	ursula.ross@████████.com	49.████████	DESKTOP	106670475_10980_8ae4dc81-1d5a-11ed-b651-5db44a4edaac
2022-08-16T11:57:03.0Z	Okta Dev-14556012	policy.evaluate_sign_on	ursula.ross@████████.com	49.████████	DESKTOP	106670475_10980_8ae3f220-1d5a-11ed-b651-5db44a4edaac
2022-08-16T11:56:48.0Z	Okta Dev-14556012	user.authentication.verify	ursula.ross@████████.com	49.████████	OTHER	106670475_10980_821eeb99-1d5a-11ed-a282-17dd4534b6f4

**12. List Activities by User Domain**

Enrichment capability for getting list of activities for a user domain in given time range. Results are ordered by create time from newest to oldest. Query returns maximum 100 items.

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
Integration	Name of the third party integration	Integration	N/A	Yes
User Domaiin	User domain to filter activities.	Host Keyword Unknown	Yes	Yes
Time Range	Time range filter for query  Relative: e.g. Last 5 days  Absolute: e.g. 2022-08-14 15:10 – 2022-08-14 15:32	Time range.	N/A	Yes

Output:

Case Scope

Action	Type	Category/Value
None	N/A	N/A

Human Readable Output

Activity Date	App. Name	Description	User	Client Ip	Device Type	Id
2022-08-16T13:53:40.0Z	Okta Dev-14556012	Log out	ahmet.ozturk@████████.com	49.████████.████████.████	DESKTOP	106670475_10980_d558aa80-1d6a-11ed-bfdc-874e587366a8
2022-08-16T13:53:39.0Z	Okta Dev-14556012	Log out	ursula.ross@████████.com	49.████████.████████.████	DESKTOP	106670475_10980_d5295d1f-1d6a-11ed-ba66-7503369fa652
2022-08-16T11:57:13.0Z	Okta Dev-14556012	Single sign-on log on	ursula.ross@████████.com	49.████████.████████.████	DESKTOP	106670475_10980_90e3492c-1d5a-11ed-b281-01b31e9a4283
2022-08-16T11:57:09.0Z	Okta Dev-14556012	Log on	ursula.ross@████████.com	49.████████.████████.████	DESKTOP	106670475_10980_8ed7e8fc-1d5a-11ed-ac90-af9ccad2bf0e
2022-08-16T11:57:09.0Z	Okta Dev-14556012	Change password: user ursula.ross@████████.com</br>	ursula.ross@████████.com	N/A	N/A	106670475_10980_8ed095fb-1d5a-11ed-ac90-af9ccad2bf0e
2022-08-16T11:57:03.0Z	Okta Dev-14556012	user.authentication.verify	ursula.ross@████████.com	49.████████.████████.████	DESKTOP	106670475_10980_8ae4dc81-1d5a-11ed-b961-5db44a4edaac

### 13. List Alerts

Enrichment capability for getting list of security alerts created in given time range. Results are ordered by create time from newest to oldest. Query returns maximum 100 items.

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
Integration	Name of the third party integration	Integration	N/A	Yes
Time Range	Time range filter for query  Relative: e.g. Last 5 days  Absolute: e.g. 2022-08-14 15:10 – 2022-08-14 15:32	Time range.	N/A	Yes

**Output:****Case Scope**

Action	Type	Category/Value
None	N/A	N/A

**Human Readable output**

Alert Date	Title	Description	Severity	Status	Risk Category	Intent	Id
2022-08-26T12:57:13.0Z	System alert: Okta (Okta Dev-14556012) App connector error	The Okta (Okta Dev-14556012) App connector has not been working properly for more than 72 hours. This may be due to a timeout in the connection test or a connection problem with the app.	High	Open	N/A	[ "Unknown" ]	6308c32cab79f53e82b7a8df
2022-08-24T00:57:05.0Z	System alert: Okta (Okta Dev-14556012) App connector error	The Okta (Okta Dev-14556012) App connector has not been working properly for more than 12 hours. This may be due to a timeout in the connection test or a connection problem with the app.	High	Open	N/A	[ "Unknown" ]	63057763bb527f38df6cb7f4
2022-08-23T05:05:51.0Z	Logon from a risky IP address	Activity policy 'Logon from a risky IP address' was triggered by 'Ahmet Ozturk (mailto:[REDACTED].onmicrosoft.com)'	High	Open	[ "Threat Detection" ]	[ "Unknown" ]	63046032c48dd33f77278e2
2022-08-23T03:45:20.0Z	Logon from a risky IP address	Activity policy 'Logon from a risky IP address' was triggered by 'Ahmet Ozturk (mailto:[REDACTED].onmicrosoft.com)'	High	Open	[ "Threat Detection" ]	[ "Unknown" ]	63044d51092d0a774ca4122c

**14. List Alerts by IP**

Enrichment capability for getting list of security alerts with the specified IP field, created in given time range. Results are ordered by create time from newest to oldest. Query returns maximum 100 items.

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
Integration	Name of the third party integration	Integration	N/A	Yes
IP Address	IP Address to filter alerts	Network Address	Yes	Yes
Time Range	Time range filter for query  Relative: e.g. Last 5 days  Absolute: e.g. 2022-08-14 15:10 – 2022-08-14 15:32	Time range.	N/A	Yes

## Output:

### Case Scope

Action	Type	Category/Value
None	N/A	N/A

### Human Readable output

Alert Date	Title	Description	Severity	Status	Risk Category	Intent	Id
2022-09-08T08:09:55.0Z	Logon from a risky IP address	Activity policy 'Logon from a risky IP address' was triggered by 'Ahmet Ozturk (mailto:[REDACTED]@onmicrosoft.com)'	High	Open	[ "Threat Detection" ]	[ "Unknown" ]	6319a356bb28275c55bda8a9
2022-09-08T06:49:30.0Z	Logon from a risky IP address	Activity policy 'Logon from a risky IP address' was triggered by 'Ahmet Ozturk (mailto:[REDACTED]@onmicrosoft.com)'	High	Open	[ "Threat Detection" ]	[ "Unknown" ]	6319907cef0d93ba6a1a847
2022-09-08T01:17:58.0Z	Logon from a risky IP address	Activity policy 'Logon from a risky IP address' was triggered by 'Ahmet Ozturk (mailto:[REDACTED]@onmicrosoft.com)'	High	Open	[ "Threat Detection" ]	[ "Unknown" ]	631942c81ef9c55bbe34a751
2022-09-07T15:49:29.0Z	Logon from a risky IP address	Activity policy 'Logon from a risky IP address' was triggered by 'Ahmet Ozturk (mailto:[REDACTED]@onmicrosoft.com)'	High	Open	[ "Threat Detection" ]	[ "Unknown" ]	6318bd8aaaff392edc75306
2022-09-07T14:47:58.0Z	Logon from a risky IP address	Activity policy 'Logon from a risky IP address' was triggered by 'Ahmet Ozturk (mailto:[REDACTED]@onmicrosoft.com)'	High	Open	[ "Threat Detection" ]	[ "Unknown" ]	6318af1e9335c0397f399784

## 15. List Alerts by Severity

Enrichment capability for getting list of security alerts with the specified severity value, created in given time range. Results are ordered by create time from newest to oldest. Query returns maximum 100 items.

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
Integration	Name of the third party integration	Integration	N/A	Yes
Alert Severity	Alert severity set by vendor/provider	String High Medium Low Informational	No	Yes
Time Range	Time range filter for query	Time range. Relative: e.g. Last 5 days Absolute: e.g. 2022-08-14 15:10 – 2022-08-14 15:32	N/A	Yes

**Output:****Case Scope**

Action	Type	Category/Value
None	N/A	N/A

**Human Readable Output**

Alert Date	Title	Description	Severity	Status	Risk Category	Intent	Id
2022-08-22T04:45:02.0Z	Logon from a risky IP address	Activity policy 'Logon from a risky IP address' was triggered by 'Ahmet Ozturk (<mailto:ahmet.ozturk.onmicrosoft.com>)'.	High	Open	[ "Threat Detection" ]	[ "Unknown" ]	630309d07b8da932bcd4a961
2022-08-22T03:24:26.0Z	Logon from a risky IP address	Activity policy 'Logon from a risky IP address' was triggered by 'Ahmet Ozturk (<mailto:ahmet.ozturk.onmicrosoft.com>)'.	High	Open	[ "Threat Detection" ]	[ "Unknown" ]	630f6ec8afe46488b0b358d
2022-08-22T02:03:54.0Z	Logon from a risky IP address	Activity policy 'Logon from a risky IP address' was triggered by 'Ahmet Ozturk (<mailto:ahmet.ozturk.onmicrosoft.com>)'.	High	Open	[ "Threat Detection" ]	[ "Unknown" ]	6302e40b824aab20473cf072
2022-08-22T00:43:13.0Z	Logon from a risky IP address	Activity policy 'Logon from a risky IP address' was triggered by 'Ahmet Ozturk (<mailto:ahmet.ozturk.onmicrosoft.com>)'.	High	Open	[ "Threat Detection" ]	[ "Unknown" ]	6302d12384381753eb19d204
2022-08-21T11:12:19.0Z	Logon from a risky IP address	Activity policy 'Logon from a risky IP address' was triggered by 'Ahmet Ozturk (<mailto:ahmet.ozturk.onmicrosoft.com>)'.	High	Open	[ "Threat Detection" ]	[ "Unknown" ]	630213148e36546156e44ad1

**16. List Alerts by Status**

Enrichment capability for getting list of security alerts with the specified status value, created in given time range. Results are ordered by create time from newest to oldest. Query returns maximum 100 items.

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
Integration	Name of the third party integration	Integration	N/A	Yes
Alert Status	Alert resolution status	String Benign Dismissed False Positive Open Resolved True Positive	No	Yes
Time Range	Time range filter for query	Time range. Relative: e.g. Last 5 days Absolute: e.g. 2022-08-14 15:10 – 2022-08-14 15:32	N/A	Yes

## Output:

### Case Scope

Action	Type	Category/Value
None	N/A	N/A

### Human Readable Output

Alert Date	Title	Description	Severity	Status	Risk Category	Intent	Id
2022-08-18T05:49:51.0Z	Logon from a risky IP address	Activity policy 'Logon from a risky IP address' was triggered by 'Ahmet Ozturk ( <a href="#">[REDACTED].onmicrosoft.com</a> )'	High	Benign	[ "Threat Detection" ]	[ "Unknown" ]	62fd300ec29c6666eac1b00
2022-08-17T06:23:24.0Z	Logon from a risky IP address	Activity policy 'Logon from a risky IP address' was triggered by 'Ahmet Ozturk ( <a href="#">[REDACTED].onmicrosoft.com</a> )'	High	Benign	[ "Threat Detection" ]	[ "Unknown" ]	62fc895ccb37140ef4b5e88e
2022-08-17T01:08:23.0Z	Logon from a risky IP address	Activity policy 'Logon from a risky IP address' was triggered by 'Ahmet Ozturk ( <a href="#">[REDACTED].onmicrosoft.com</a> )'	High	Benign	[ "Threat Detection" ]	[ "Unknown" ]	62fc3f8a82f917098c792842

## 17. List Entities

Enrichment capability for getting list of entities. Query returns maximum 100 items.

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
Integration	Name of the third party integration	Integration	N/A	Yes

**Output:**

Case Scope

Action	Type	Category/Value
None	N/A	N/A

**Human Readable Output**

Name	Email	App. Name	Groups	Role	Threat Score	Username
Ahmet Ozturk	[REDACTED]@onmicrosoft.com	Office 365	[ "Office 365 administrator" ]	Global Administrator	400	{"id": "d9ace34f-e0ce-4a3a-9921-2680f11169a0", "saas": 11161, "inst": 0}
Nestor Wilke	[REDACTED]@onmicrosoft.com	Office 365	[]	User		{"id": "f660f7c2-c9f9-4905-a022-e0b59a9a34bb", "saas": 11161, "inst": 0}
Alex Wilber	[REDACTED]@onmicrosoft.com	Office 365	[]	User		{"id": "173ac479-70e0-474d-b292-8c2110dde3e3", "saas": 11161, "inst": 0}
Martin Heidegger	[REDACTED]@onmicrosoft.com	Office 365	[]	User		{"id": "0269474e-bde3-4430-8f5b-bf06cd5900e6", "saas": 11161, "inst": 0}
Ursula Ross	[REDACTED]@com	Okta Dev-14556012	[ "External users" ]	User		{"id": "00u21vzQ0uW3gkBl5d7", "saas": 10980, "inst": 0}
Martin Heidegger	[REDACTED]@com	Okta Dev-14556012	[ "External users" ]	User		{"id": "00u21zwf66kaOeEl45d7", "saas": 10980, "inst": 0}

# Integration Guide for Microsoft Defender Endpoint

## Integration Overview

Microsoft Defender for Endpoint is an enterprise endpoint security platform designed to help enterprise networks prevent, detect, investigate, and respond to advanced threats.

## Integration Capabilities

ArcSight SOAR has the following integration capabilities with Micro Focus ArcSight Intelligence:

- Get Alert by ID
- Get Domain Statistics
- Get File Information
- Get File Related Machines

- Get File Statistics
- Get Installed Software
- Get IP Statistics
- Get Logon Users
- Get Machine Details
- List Alerts
- List Alerts by Severity
- List Alerts by Status
- List File Related Alerts
- List Machines
- List User Related Alerts
- Add Machine Tag
- Assign Alert
- Isolate Machine
- Remove Machine Tag
- Restrict Code Execution
- Stop & Quarantine File
- Integrate Machine
- Unrestrict Code Execution
- Update Alert Classification
- Update Alert Comment
- Update Alert Determination
- Update Alert Status

## Prerequisites

ArcSight SOAR connects to Microsoft Defender API using HTTPS. Access to Microsoft portal [login.microsoft.com](https://login.microsoft.com) is required.

## Configuring Microsoft Defender

1. Log in to <https://portal.azure.com> and Navigate to **Azure Active Directory** service.



If an application is defined for other integrations, skip steps 1-3 to use it.

- Click **App Registration > New Registration**. Complete the ArcSight SOAR application registration by specifying the following parameter values in the Register an application form:

Name	Supported Account Types	Redirected URL
ArcSight SOAR	Accounts in this organizational directory only (Default Directory for single tenant only)	https://localhost/soar

- Select your application and Click **Add a certificate or secret > New Client Secret**. Add a description and specify the expiry period as 24 months.

 Note down the Secret Key value along with Client ID and tenant ID.

- Click **API Permissions > Add a Permission** and select **Windows Defender API**. Add the following permissions from WindowsDefender ATP:

Permission Type	Permission	Description
Application	Alert.Read.All, File.Read.All, Machine.Isolate, Machine.Read.All, Machine.RestrictEx, User.Read.All, Alert.ReadWrite.All, Ip.Read.All, Url.Read.All, Machine.StopAndQuarantine, Machine.Scan	Read and update your organisation's security events.

- Click **Yes** to grant admin consent for Default Directory.

## Configuring SOAR

- Click **Configuration > Credential > Create Credential**.
- Specify the following parameter values in the **Configuration Form**:

Parameter	Value
Name	Display name of the credential set
Type	Internal credential
Username	Empty
Password	client_id of the application created above for SOAR on Azure portal.
Private Key	Secret key of the application created above for SOAR on Azure portal.

- Click **Configuration > Integrations > Create Integration**.
- Specify the following parameter values in the **Configuration Form**:

Parameter	Value
Name	Display name of the integration
Type	Microsoft Defender for Endpoint
Address	Address of the integration ((the format should be https://api.securitycenter.microsoft.com)

Parameter	Value	
Configuration	Specify the following configuration parameters:	
	proxy.id	ID of the Proxy integration if you access Microsoft Azure through a web proxy device. For example: proxy.id = 12345
	tenant.id	Global Unique Identifier (GUID) for your Microsoft 365 Tenant.
	cache.reusing.duration	Configure how far (in minutes) into the past this enrichment will look.
Credential	Credential that has been defined for this integration under the Credentials menu	
Notify	Select user(s) from the list to notify when SOAR performs an action on this integration	

5. Click **Save**.
6. Navigate to **Configuration > Customization Library** and edit **Microsoft Defender for Endpoint Advanced Action Script Default Template**
7. Select the integration that you have created in step 4 from the **Integrations** drop-down menu and click **Save**.
8. Click **Test**, and **Integration Successful** message is displayed if the credential and address are valid.

## Capabilities

### 1. Get Alert by ID

Enrichment capability for getting details of an alert by Alert ID.

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
Integration	Name of the third party integration	Integration	N/A	Yes
Alert ID	Alert ID that has been created by the User.	String	N/A	Yes

#### Output:

Case Scope

N/A

Human Readable Output

N/A

### 2. Get Domain Statistics

Enrichment capability for retrieving statistics on a domain.

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
<b>Integration</b>	Name of the third party integration	Integration	N/A	Yes
<b>Domain</b>	Host that you have created from case scope	String	Yes	Yes

**Output:**

Case Scope

N/A

Human Readable Output

N/A

**3. Get File Information**

Enrichment Capability for getting file details

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
<b>Integration</b>	Name of the third party integration	Integration	N/A	Yes
<b>File Hash</b>	SHA1 & SHA256 file hash from case scope	String	Yes	Yes

**Output:**

Case Scope

Human Readable Output

**4. Get File Related Machines**

Enrichment capability for Retrieving a collection of machines related to a given file hash

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
<b>Integration</b>	Name of the third party integration	Integration	N/A	Yes
<b>File Hash</b>	SHA1 file hash from case scope	String	Yes	Yes

**Output:**

Case Scope

Human Readable Output

N/A

**5. Get File Statistics**

Enrichment capability for Retrieving the statistics for given file.

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
<b>Integration</b>	Name of the third party integration	Integration	N/A	Yes
<b>File Hash</b>	SHA1 file hash from case scope	String	Yes	Yes

**Output:**

Case Scope

Human Readable Output

N/A

**6. Get Installed Software**

Enrichment capability for Retrieving a collection of installed software related to a given device ID.

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
<b>Integration</b>	Name of the third party integration	Integration	N/A	Yes
<b>IP Address</b>	Network Address from case scope	String	Yes	Yes

**Output:**

Case Scope

Human Readable Output

N/A

**7. Get IP Statistics**

Enrichment capability for Retrieving the statistics for given IP.

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
<b>Integration</b>	Name of the third party integration	Integration	N/A	Yes
<b>IP Address</b>	Network Address from case scope	String	Yes	Yes

**Output:**

Case Scope

Human Readable Output

N/A

**8. Get Logon Users**

Enrichment capability for Retrieving collection of logged on users on a specific device

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
Integration	Name of the third party integration	Integration	N/A	Yes
IP Address	Network Address from case scope	String	Yes	Yes

**Output:**

Case Scope

Human Readable Output

N/A

**9. Get Machine Details**

Enrichment capability for retrieving machine details for given IP address.

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
Integration	Name of the third party integration	Integration	N/A	Yes
IP Address	Network Address from case scope	String	Yes	Yes

**Output:**

Case Scope

Human Readable Output

N/A

**10. List Alerts**

Enrichment capability for retrieving a collection of alerts in a given time-range.

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
Integration	Name of the third party integration	Integration	N/A	Yes
Time range	Time range	String	No	Yes

**Output:**

Case Scope

N/A

Human Readable Output

N/A

**11. List Alerts by Severity**

Enrichment Capability for retrieving a collection of alerts for a given severity value in a given time-range.

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
Integration	Name of the third party integration	Integration	N/A	Yes
Time range	Time range	String	No	Yes
Severity	Severity of the alert	String	No	Yes

**Output:**

Case Scope

N/A

Human Readable Output

N/A

**12. List Alerts by Status**

Enrichment Capability for retrieving a collection of alerts for a given status value in a given time-range.

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
Integration	Name of the third party integration	Integration	N/A	Yes
Time range	Time range	String	No	Yes
Alert Status	Alert Status	String	No	Yes

**Output:**

Case Scope

N/A

Human Readable Output

N/A

**13. List File Related Alerts**

Enrichment capability for retrieving a collection of alerts related to a given file hash.

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
<b>Integration</b>	Name of the third party integration	Integration	N/A	Yes
<b>Domain</b>	Domain host from case scope	String	Yes	Yes

**Output:**

Case Scope

Human Readable Output

N/A

**14. List Machines**

Enrichment capability for retrieving a list of machines that have communicated with Microsoft

Defender for Endpoint cloud.

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
<b>Integration</b>	Name of the third party integration	Integration	N/A	Yes

**Output:**

Case Scope

N/A

Human Readable Output

N/A

**15. List User Related Alerts**

Enrichment capability for retrieving a collection of alerts related to a given username.

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
Integration	Name of the third party integration	Integration	N/A	Yes
Username	Username from case scope	String	Yes	Yes

**Output:**

Case Scope

Human Readable Output

N/A

**16. List Machines By Tag**

Enrichment capability for finding machines by a given tag.

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
Integration	Name of the third party integration	Integration	N/A	Yes
Tag	Input Tag	String	Yes	Yes

**Output:**

Case Scope

Human Readable Output

N/A

**17. Add Machine Tag**

Action capability for adding a tag to specific machine.

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
IP Address	Network address from case scope	Network Address	Yes	Yes
Tag	Input Tag	String	Yes	Yes

**Output:**

Case Scope

Human Readable Output

N/A

**18. Assign Alert**

Action capability for assigning an alert.

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
Alert ID	Alert ID	String	No	Yes
Assignee	Assignee	String	No	Yes

**Output:**

Case Scope

N/A

Human Readable Output

N/A

**19. Isolate Machine**

Action capability for isolating device from accessing external network.

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
IP Address	Network address from case scope	Network Address	Yes	Yes
Comment	Comment	String	No	Yes

**Output:**

Case Scope

Human Readable Output

N/A

**20. Remove Machine Tag**

Action capability for removing a tag from a specific machine.

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
IP Address	Network address from case scope	Network Address	Yes	Yes
Tag	Input Tag	String	No	Yes

**Output:**

Case Scope

Human Readable Output

N/A

**21. Restrict Code Execution**

Action capability for restricting execution of all applications on the device except a

predefined set.

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
IP Address	Network address from case scope	Network Address	Yes	Yes

#### Output:

Case Scope

Human Readable Output

N/A

### 22. Stop & Quarantine File

Action capability for stopping execution of a file on a device and deleting it.

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
IP Address	Network address from case scope	Network Address	Yes	Yes
File Hash (SHA1)	File Hash (SHA1) from case scope	String	Yes	Yes

#### Output:

Case Scope

N/A

Human Readable Output

N/A

### 23. Unisolate Machine

Action capability for releasing machine from isolation.

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
IP Address	Network address from case scope	Network Address	Yes	Yes

#### Output:

Case Scope

N/A

Human Readable Output

N/A

**24. Unrestrict Code Execution**

Action capability for removing app restrictions on a device.

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
IP Address	Network address from case scope	Network Address	Yes	Yes

**Output:**

Case Scope

N/A

Human Readable Output

N/A

**25. Update Alert Classification**

Action capability for updating alert classification.

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
Alert ID	Alert ID	String	No	Yes
Alert Classification	Alert classification	String	No	Yes

**Output:**

Case Scope

Human Readable Output

N/A

**26. Update Alert Comment**

Action capability for adding comment to an alert.

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
Alert ID	Alert ID	String	No	Yes
Alert Comments	Alert comment	String	No	Yes

**Output:**

Case Scope

N/A

Human Readable Output

N/A

**27. Update Alert Determination**

Action capability for updating an alert determination.

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
Alert ID	Alert ID	String	No	Yes
Alert Determination	Alert determination	String	No	Yes

**Output:**

Case Scope

N/A

Human Readable Output

N/A

**28. Update Alert Status**

Action capability for updating alert status.

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
Alert ID	Alert ID	String	No	Yes
Alert Status	Alert status	String	No	Yes

**Output:**

Case Scope

N/A

Human Readable Output

N/A

# Integration Guide for OpenText IT Service Manager

## Integration Overview

**OpenText Service Manager** is an IT Service Management (ITSM) Tool that uses the Information Technology Infrastructure Library (ITIL) framework to provide a web interface for corporate changes, releases and interactions (request fulfillment) that is supported by a service catalog and Configuration Management Database (CMDB).

## Integration Capabilities

ArcSight SOAR has the following integration capabilities with OpenText IT Service Manager:

- Close Incident
- Create Incident
- Update Incident

## Prerequisites

You must have access to HTTPS as the ArcSight SOAR connects to OpenText IT Service Manager API through this service.

## Configuration

### Configuring OpenText IT Service Manager

1. Create a user on IT Service Manager with admin role. This user must be able to and consume the rest APIs of the IT Service Manager.

# Configuring SOAR

1. Click **Configuration > Credential > Create Credential**.
2. Specify the following parameter values in the **Credential Editor** form.

Type	Name	Username	Password	Private Key
Internal credential	Display name of credential set (for example, OpenText IT Service Manager Credentials).	Username of the created user on OpenText IT Service Manager.	Password of the created user on OpenText IT Service Manager.	

3. Click **Configuration > Lists > Create List**. The list must have two columns with the type keyword. Add a name to the list and save it. The name of the list is used during integration configuration.
4. Click **Configuration > Integrations > Create Integration**.
5. Specify the following parameter values in the **Configuration** form.

Parameter	Value				
<b>Name</b>	Display name of the integration.				
<b>Type</b>	OpenText IT Service Manager				
<b>Address</b>	URL of the OpenText IT Service Manager integration (for example, <a href="http://15.113.165.82:13080">http://15.113.165.82:13080</a> ).				
<b>Configuration</b>	<p>Specify the following configuration parameters:</p> <table border="1"> <tr> <td>list.name</td> <td>List name that is used for mapping ArcSight SOAR cases to OpenText IT Service Manager incidents. For example, list.name=mfitsmMapList</td> </tr> <tr> <td>proxy.id</td> <td>ID of the Proxy integration if you access OpenText IT Service Manager through a web proxy device. For example, proxy.id = 12345 .</td> </tr> </table>	list.name	List name that is used for mapping ArcSight SOAR cases to OpenText IT Service Manager incidents. For example, list.name=mfitsmMapList	proxy.id	ID of the Proxy integration if you access OpenText IT Service Manager through a web proxy device. For example, proxy.id = 12345 .
list.name	List name that is used for mapping ArcSight SOAR cases to OpenText IT Service Manager incidents. For example, list.name=mfitsmMapList				
proxy.id	ID of the Proxy integration if you access OpenText IT Service Manager through a web proxy device. For example, proxy.id = 12345 .				
<b>Credential</b>	Credential that has been defined for this integration under the <b>Credentials</b> menu.				
<b>Trust Invalid SSL Certificates</b>	Select this if web server's certificate is self-signed or is not recognized by browsers.				
<b>Require Approval From</b>	Select user(s) from list to ask the approval before executing actions on this integration.				
<b>Notify</b>	Select user(s) from the list to notify when SOAR performs an action on this integration.				

6. Click **Save** to save the integration definition.
7. Navigate to **Configuration>Customization Library** and edit **OpenText IT Service Manager Advanced Action Script Default Template**.
8. Select the integration that you have added to **Integrations** menu.

9. Click **Save** to complete the integration.
10. Click **Test**, an **Integration Successful** message is displayed if the credential and address are valid.

## Capabilities

### 1. Create Incident

Action capability for creating incident on OpenText IT Service Manager

Rollback : No

Duplicate Check: Yes

The following table presents the **Create Incident** action capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
<b>Category</b>	Category information of created incident.	Enum	No	Yes
<b>Description</b>	MF ITSM Incident Description.	Text	No	Yes
<b>Title</b>	Incident Title	Text	No	Yes
<b>Service</b>	Service Type	Enum	No	Yes
<b>Impact</b>	Incident Impact	Enum	No	Yes
<b>Urgency</b>	Incident Urgency	Enum	No	Yes
<b>Status</b>	Incident Status	Enum	No	No
<b>Alert Status</b>	Incident Alert Status	Text	No	No
<b>Area</b>	Incident Area	Text	No	No
<b>Subarea</b>	Incident Subarea	Text	No	No
<b>Assignment Group</b>	Incident Assignee	Text	No	No
<b>Affected CI</b>	Incident Affected CI	Text	No	No
<b>Company</b>	Incident Company	Text	No	No
<b>Phase</b>	Incident Phase	Text	No	No

### 2. Close Incident

Action capability for closing incident on OpenText IT Service Manager.

Rollback : No

Duplicate Check: Yes

The following table presents the **Close Incident** action capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Solution</b>	Solution Note	Text	No	Yes

### 3. Update Incident

Action capability for updating incident on OpenText IT Service Manager.

Rollback : No

Duplicate Check: No

The following table presents the update incident action capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Description</b>	MF ITSM Incident Description.	Text	No	Yes
<b>Title</b>	Incident Title	Text	No	Yes
<b>Service</b>	Service Type	Enum	No	Yes
<b>Impact</b>	Incident Impact	Enum	No	Yes
<b>Urgency</b>	Incident Urgency	Enum	No	Yes
<b>Status</b>	Incident Status	Enum	No	No
<b>Alert Status</b>	Incident Alert Status	Text	No	No
<b>Area</b>	Incident Area	Text	No	No
<b>Subarea</b>	Incident Subarea	Text	No	No
<b>Assignment Group</b>	Incident Assignee	Text	No	No
<b>Affected CI</b>	Incident Affected CI	Text	No	No
<b>Company</b>	Incident Company	Text	No	No
<b>Phase</b>	Incident Phase	Text	No	No

# Integration Guide for OpenText UCMDB

## Integration Overview

**OpenText Universal Configuration Management Database (UCMDB)** generates and maintains a Configuration Management Database of information technology items. It includes a mechanism for automated discovery of IT infrastructure components, such as computers and network devices.

## Integration Capabilities

ArcSight SOAR has the following integration capabilities with OpenText UCMDB:

- Expose CI Information
- Get CI
- Get Related CIs

## Prerequisites

You must have access to HTTPS as the ArcSight SOAR connects to OpenText UCMDB API through this service.

## Configuration

## Configuring OpenText UCMDB

Create a user with privileges to use REST API. The username and password of the user is used as credential in the ArcSight SOAR.

# Configuring SOAR

1. Click **Configuration > Credential > Create Credential**
2. Specify the following parameter values in the **Credential Editor** form:

Type	Name	Username	Password	Private Key
Internal credential	Display name of credential set (for example, OpenText UCMDB Credentials).	Username	Password	

3. Click **Configuration > Integrations > Create Integration**.
4. Specify the following parameter values in the **Configuration** form:

Parameter	Value						
<b>Name</b>	Display name of the integration.						
<b>Type</b>	OpenText UCMDB						
<b>Address</b>	URL of UCMDB (ie. <a href="https://cms.smax.swdemos.net:8443">https://cms.smax.swdemos.net:8443</a> )						
<b>Configuration</b>	Specify the following configuration parameters: <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="padding: 5px;"><code>cache.reusing.duration</code></td> <td style="padding: 5px;">Configure how far (in minutes) into the past this enrichment will look. For example, <code>cache.reusing.duration=20</code> .</td> </tr> <tr> <td style="padding: 5px;"><code>max.result.count</code></td> <td style="padding: 5px;">Maximum result count for Get Observed Attack Techniques capability. For example: <code>max.result.count=200</code></td> </tr> <tr> <td style="padding: 5px;"><code>proxy.id</code></td> <td style="padding: 5px;">ID of the Proxy integration if you access OpenText UCMDB through a web proxy device. For example, <code>proxy.id = 12345</code></td> </tr> </table>	<code>cache.reusing.duration</code>	Configure how far (in minutes) into the past this enrichment will look. For example, <code>cache.reusing.duration=20</code> .	<code>max.result.count</code>	Maximum result count for Get Observed Attack Techniques capability. For example: <code>max.result.count=200</code>	<code>proxy.id</code>	ID of the Proxy integration if you access OpenText UCMDB through a web proxy device. For example, <code>proxy.id = 12345</code>
<code>cache.reusing.duration</code>	Configure how far (in minutes) into the past this enrichment will look. For example, <code>cache.reusing.duration=20</code> .						
<code>max.result.count</code>	Maximum result count for Get Observed Attack Techniques capability. For example: <code>max.result.count=200</code>						
<code>proxy.id</code>	ID of the Proxy integration if you access OpenText UCMDB through a web proxy device. For example, <code>proxy.id = 12345</code>						
<b>Credential</b>	Credential that has been defined for this integration under the <b>Credentials</b> menu.						
<b>Trust Invalid SSL Certificates</b>	Select this if web server's certificate is self-signed or is not recognized by browsers.						
<b>Require Approval From</b>	Select user(s) from list to ask the approval before executing actions on this integration.						
<b>Notify</b>	Select user(s) from the list to notify when SOAR performs an action on this integration.						

5. Click **Save** to save the integration definition.
6. Navigate to **Configuration>Customization Library** and edit **OpenText UCMDB Advanced Action Script Default Template**.
7. Select the integration that you have added to **Integrations** menu.
8. Click **Save** to complete the integration.

- Click **Test**, an **Integration Successful** message is displayed if the credential and address are valid.

## Capabilities

### 1. Expose CI Information

Enrichment capability for information related to the CIs of a certain type.

The following table presents the **CI Enrichment** capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Integration</b>	Name of the third party integration.	Integration	No	Yes
<b>Layout</b>	The comma seperated columns that are displayed in the output, for example, display_label, name, description, node_role	Text	No	Yes
<b>Type</b>	The CI Type. For example, node, sqlserver, unix.	Text	No	Yes
<b>Column</b>	The value of this column is checked against the value you provided,for example, application_ip or name	Text	No	No
<b>Value</b>	Value, that is going to used during filtering.	Scopeltem	Yes	No

### Output:

Case Scope:

Action	Type	Category/ Value
<b>Add</b>	Scope Item	Keyword(Related)

Human Readable Output:

Displaylabel	Properties_name	GlobalId	Type	UomId	Attributequalifiers
vmamq285			unix	6361a6ed37c0bda3d0a781cc55d10e ff	
nancy-linux			unix	4570c42fb3labcd92ec2b625711b b7	
e02ea8f0-bastion			unix	43549f671508c3dab703aa149dd22 3	
bba4bcdf-db			unix	47719295242b63ad5641ecf5ee6b 8	
			unix	4f67998d2b65d5aa9bb6a5a79c27bd b7	
			unix	40a367e69c28e4930c223ea2e4e43fb c3	
			unix	4500b4a7100065a4a53c8d9eb080c 92	
			unix	4fa0511ad54c37a5988573be2286d 88	
			unix	405b40e5d7386c7780cf79d861784b e0	
labm3amnn53			unix	db0fa1ac36031fbde6a3b1670e35606 4d	
acswet1			unix	4744687202229860b05291c8a027 88	
labm1tg16			unix	5375bca19c1f789ea1a953ed989 96	

### 2. Get CI

Enrichment capability for returning details of a CI.

The following table presents the **Get CI** enrichment capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Integration</b>	Name of the third party integration.	Integration	No	Yes
<b>ID</b>	CI id. If provided this value will be used regardless of the IP and Type values.	Keyword	Yes	No

### Output:

Case Scope:

Action	Type	Category/ Value
<b>None</b>	N/A	N/A

Human Readable Output:

Field	Value
attributesQualifiers	
displayLabel	labm2sun20
globalId	
properties_bit_position	115
properties_bitmap_id	93
properties_contextmenu	[ "ICls" ]
properties_create_time	2021-06-06T10:02:30.061Z
properties_data_administrate	0 Managed
properties_data_slow_auto_discovery	true
properties_data_changeonstate	0 No Change
properties_data_changeinnew	false
properties_data_changestate	0 No Change
properties_data_operationonstate	0 Normal
properties_data_operatoreinew	false
properties_data_operationstate	0 Normal
properties_data_source	UCMDB: JMX
properties_data_testonstate	0 Normal
properties_data_testinnew	false
properties_data_teststate	0 Normal
properties_data_updated_by	UCMDB: JMX
properties_default_gateway_ip_address	16.55.248.1

### 3. Get Related CIs

Enrichment capability for returning the details of the CIs related to the specified CI.

The following table presents the **Get Related CI** enrichment capability details:

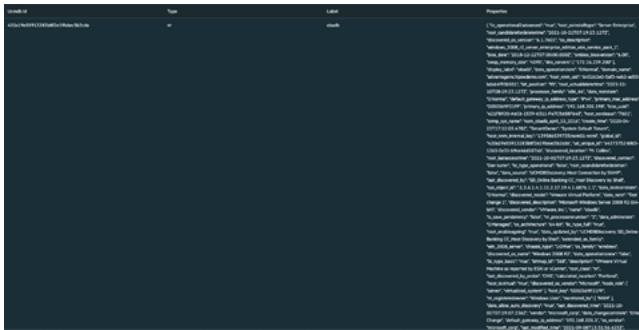
Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Integration</b>	Name of the third party integration.	Integration	No	Yes
<b>ID</b>	CI id. If provided this value will be used no matter type or ip provided or not.	Keyword	Yes	Yes
<b>Type</b>	The string that represents the name of a valid configuration item type from the UCMDB. The name of the CI Type can be found inside the CI Type Manager.	Text	No	Yes

### Output:

## Case Scope:

Action	Type	Category/ Value
<b>None</b>	N/A	N/A

## Human Readable Output:



# Integration Guide for Microsoft Exchange

## Integration Overview

Exchange Server is a mail server developed by Microsoft.

SOAR has the following integration capabilities with Microsoft Exchange Server :

- Delete email
- Mark email
- Quarantine email

### **Use Case: Deleting already delivered phishing emails**

SOAR can follow email inboxes for user's phishing reports and automatically creates an incident record on its service desk. During the investigation of the attack SOAR can extract the sender address and subject and using these values performs a search on Microsoft Exchange Server to mark or delete already delivered malicious messages. This can be performed automatically within a playbook or manually by an analyst.

## Configuration

### Prerequisites

- SOAR connects to Microsoft Exchange Web Service API via HTTPS. So access to 443/tcp port is required.
- A user account with impersonation role is required for SOAR to connect Microsoft Exchange.

### Configuration on Microsoft Exchange

1. Login to Microsoft Exchange admin center and add a user mailbox for SOAR.
2. Open Exchange Management Shell and give the user Application Impersonation role using the following command:

```
New-ManagementRoleAssignment \  
    -Name:<impersonation Assignment Name> \  
    -Role:ApplicationImpersonation \  
    -User:<account name>
```

## Configuration on SOAR

1. Navigate **Configuration > Credentials** and click **Create Credential**.
2. Specify the parameter values in the **Credential Editor** form as follows:

**a. Internal Credential:**

Type	Name	Username	Password	Private Key
Internal credential	Display name of credential set (i.e., Microsoft Exchange Credentials).	User you have configured SOAR on Microsoft Exchange (the format should be username@domain).	Password of the user you have configured for SOAR on Microsoft Exchange.	Empty

**b. Credential Store:**

**Type:** External credential.

**Name:** Name of the credential with pull path of the safe on store.

3. Navigate to**Configuration -> Integrations** and click **Create Integration**.
4. Specify the parameter values in the **Configuration** form as follows:

Address	Configuration	Credentials	Trust Invalid SSL Certificates	Require Approval from	Notify	Require Approval from	Notify
Display name of Microsoft Exchange integration on SOAR.	Microsoft Exchange	Address of the integration (the format should be 192.168.2.8).	You need to specify the following configuration parameters  requests.impersonation.disable=false  requests.cookies.enable=true  mail.store.protocol=exchange  mail.incoming.pollerperiod=10000  mail.incoming.folder=Inbox	Name of the credential set you've just created on step 2. (i.e., Microsoft Exchange Credentials).	Select this if certificate used on Exchange Server is self-signed or not recognized by browsers.	Select user(s) from list to ask her/his approval before executing actions on this integration.	Select user(s) from the list to notify when SOAR performs an action on this integration.

5. Click **Test** to test the integration.
6. Click **Save** to complete integration.

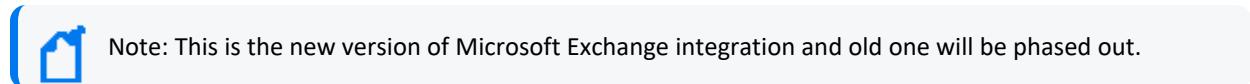
## Additional Notes

- To customize warning messages for Quarantine and Mark actions, edit the following parameters under **Configuration > Parameters**:
  - MSExchangeMarkWarningText
  - MSExchangeQuarantineWarningText
- To customize the mail folder to be used for Quarantine actions, edit the following parameter under **Configuration > Parameters**:
  - MSExchangeQuarantineEMailBox
- In some environments with multiple CAS deployments Exchange uses a request cookie to track the environment. The requests.cookies.enable configuration can help track the cookie so that SOAR won't have any mismatch and Subscription was not found error. It is by default true and should stay that way in most environments.

# Integration Guide for Microsoft Office365 Exchange EWS

## Integration Overview

Exchange Server EWS provide access to mailbox data stored in Exchange Online, Exchange Online as part of Office 365, and on-premises versions of Exchange starting with Exchange Server 2007, and enable you to manage that information according to the requirements of your organization.



Note: This is the new version of Microsoft Exchange integration and old one will be phased out.

Users are encouraged to use this integration.

ArcSight SOAR has the following integration capabilities with Microsoft Exchange EWS :

- Block Email Sender
- Delete Email
- Delete Attachment
- Get Attachments
- Get Emails
- Search Emails

### Use Case: Deleting already delivered phishing emails

SOAR follows email inboxes for user's phishing reports and automatically creates an incident record on its service desk. During the investigation of the attack ATAR can extract the sender address and subject and using these values performs a search on Microsoft Exchange Server to delete already delivered malicious messages and block malicious senders. This can be performed automatically within a playbook or manually by an analyst.

## Configuration

## Prerequisites

- SOAR connects to Microsoft Exchange Web Service API using HTTPS. So access to 443/tcp port is required.

- A user account with the following permissions is required for SOAR to connect MS Exchange EWS Server:
  - ApplicationImpersonation (Authorized to make operations for other users' accounts)
  - MailboxSearch (Authorized to search all mailboxes).

## Configuration on Microsoft Exchange

1. Login to Microsoft Exchange Admin Center (For example, <https://exchangeserver/ecp>) and add a user mailbox for SOAR.
2. Navigate to **Permissions > Cloud Migrator Impersonation**, edit and add user account you have created in first step to “Members” to give Account Impersonation permission.
3. Navigate to **Permissions > Discovery Management**, edit and add user account you have created in first step to “Members” to give Mailbox Search permission

## Using OAuth2 with Microsoft Exchange online Integrations

You can use the OAuth authentication service provided by Azure Active Directory to enable your EWS Managed API applications to access Exchange Online in Office 365. To use OAuth with your application complete the following:

1. Register the application for OAuth2. For more information see [Microsoft Documentation](#). After the application registered, it appears in the Application list. Click the application to view details.
2. Copy the values for Application(client) ID, Directory(tenant) ID and Client Credentials fields to create credentials in SOAR.

Essentials	Client credentials
Display name : SOAR Dev	Client ID : 0_certificate_1_secret
Application (client) ID	Redirect URIs : 0_web_0_sp_1_public_client
Object ID	Application ID URI : Add an Application ID URI
Directory (tenant) ID	Managed application in I... : SOAR Dev
Supported account types : My organization only	

### 3. Configure the following permissions for registered Application:

Microsoft Graph (5)					
Mail.Read	Application	Read mail in all mailboxes	Yes	Granted for gordioncyb...	...
Mail.ReadWrite	Application	Read and write mail in all mailboxes	Yes	Granted for gordioncyb...	...
Mail.Send	Application	Send mail as any user	Yes	Granted for gordioncyb...	...
User.Read	Delegated	Sign in and read user profile	No	Granted for gordioncyb...	...
User.Read.All	Application	Read all users' full profiles	Yes	Granted for gordioncyb...	...

Office 365 Exchange Online (1)					
full_access_as_app	Application	Use Exchange Web Services with full access to all mailboxes	Yes	Granted for gordioncyb...	For EWS Capabilities

## Configuring SOAR

### 1. Navigate **Configuration > Credentials** and click **Create Credential**.

Fill the Credential Editor form as follows:

#### a. Internal Credential:

Type	Internal credential.
Name	Display name of credential set (i.e., MS Exchange EWS Credentials).
Username	Application(client) ID value that has been copied from the application.
Password	Client Credentials value that has been copied from the application.
Private Key:	Directory(tenant) ID value that has been copied from the application.

#### b. Credential Store:

Type	External credential.
Name	Name of the credential with pull path of the safe on store.

### 2. Navigate **Configuration > Integrations** and click **Create Integration**.

### 3. Fill the configuration form as follows:

Name:	Display name of Microsoft Exchange EWS integration on ATAR.
Type:	Microsoft Exchange EWS.
Address:	Address of the integration (the format should be outlook.office365.com or 192.168.2.7).

<b>Configuration :</b>	You need to specify the following configuration parameters: <pre># Maximum record number per paginated response. Default value is 1000 page.size=200 # Connect time out in seconds. Default value is 200 connect.timeout=7200 # Request time out in seconds. Default value is 200 request.timeout=7200 # Trash folder name. Default value is Deleted Items #trash.folder= # Junk folder name. Default value is Junk Email #junk.folder= # Maximum record number per paginated attachment detail response. Default value is 10 #attachment.page.size= # Microsoft Exchange Server enrichment API timezone, if not specified GMT will be used as default #timezone= # Maximum number of email id list per request. Default value is 5 #email.id.size= # Maximum record number per paginated item detail response. Default value is 10 #email.page.size= # Maximum email item limit for each enrichment. Default value is 1000 #email.limit= # Maximum attachment item limit for each enrichment. Default value is 100 #attachment.limit= # Authentication methods for the integration. Supported options: Basic, OAuth2, default is Basic #auth.type=</pre>
	 Set <b>auth.type=OAuth2</b> in integration configurations to enable OAuth2.
<b>Credential</b>	Select newly created OAuth2 credential for credential field. (i.e., Microsoft Exchange Credentials).
<b>Trust Invalid SSL Certificates</b>	Select this if certificate used on Exchange Server is self-signed or not recognized by browsers.
<b>Require Approval From:</b>	Select user(s) from list to ask approval before executing actions on this integration
<b>Notify</b>	Select user(s) from the list to notify when ATAR performs an action on this integration.

4. Click the Test button.
5. Click **Save** to complete integration.

## Additional Notes

For Delete capability, at least one of the following parameters should be given:

- Email From
- Email Subject
- Email ID
- Attachment ID

And there are 3 deletion methods:

- **Hard Delete:** Deletes permanently (default)
- **Move To Trash:** Moves to trash folder (such as Deleted Items folder)
- **Soft Delete:** Moves to dumpster if it is enabled.

## Integration Guide for Microsoft Teams

### Integration Overview

Microsoft Teams is a messaging and collaboration app for organizations. It allows users to communicate and collaborate in real-time. It also allows users to conduct online meetings and share files among other features for business communications.

### Integration Capabilities

ArcSight SOAR has the following integration capabilities with Microsoft Teams:

- List Teams
- List Channels
- Create Team
- Create Channel
- List Team Members
- Add Team Member
- Delete Member
- Send Message
- Retrieve Message
- Archive Team
- Unarchive Team

## Prerequisites

You must have HTTP access as ArcSight SOAR connects to Microsoft Team API through this service.

## Configuration

### Configuring Microsoft Teams

To authenticate to Microsoft Teams, you must get a token from the Microsoft identity platform endpoint. Your service can use the token to call Microsoft Graph under its own identity.

1. Register your app.
2. Add redirect\_uri (for send message channel)
3. Configure permissions for Microsoft Graph on your app.
4. Get administrator consent.
5. Get an access token.
6. Use the access token to call Microsoft Graph.

Parameters	Description
client_id	The application ID that's assigned to your app. You can find this information in the portal where you registered your app.
client_secret	The client secret that you generated for your app in the app registration portal. The client secret must be URL-encoded before being sent. The Basic auth pattern of instead providing credentials in the Authorization header, per RFC 6749 is also supported.
grant_type	Must be set to client credentials.

7. On the last page, you will see the access key ID and the secret code. Save the details in a secure place.

## Authentication Parameters

### Request Headers:

Parameters	Datatype	Description	Required
Access Key	string	Access key of the user	Yes
Secret Key	string	Secret Key	Yes

### Additional Configuration:

Configuration Parameter	Description
proxy.id	Proxy device to be used while communicating with the remote system's API
cache.reusing.duration	Default cache-reuse parameter
tenant_id	The directory tenant against which the application plans to operate, in GUID or domain-name format.
owner_email.id	The email of a user who has owner access.
redirect.uri	The redirect_uri of your app, where authentication responses can be sent and received by your app. It must exactly match one of the redirect_uris you registered in the portal, but it must be URL-encoded.

## Configuring SOAR

1. Click **Configuration > Credentials > Create Credential**.
2. Specify the following parameters values in the Credential Editor form:

Type	Name	Username	Password	Private Key
Internal credential	Display name of credential set (for example, Microsoft Teams credentials)	The application ID (Client_id) that is assigned to your app. You can find this information in the portal where you have registered the app.		

3. Click **Configuration > Integrations > Upload plugin**.
4. Select your integration plugin zip file and click **Save**.
5. Select the integration that you have added to the **Integrations** menu.
6. Click **Save** to complete the integration.
7. Click **Test**. A successful message is displayed if the credential and address are valid.

## Integration Capabilities

### 1. List Teams

Enrichment capability to fetch the list of teams in an organization (tenant). To get a list of all groups in the organization that has Teams, get a list of all groups, and then in code find the ones that have a resourceProvisioningOptions property that contains Team.

### Required Permissions

Permission Type	Permissions (from least to most privileged)
Application	GroupMember.Read.All, Group.Read.All, Directory.Read.All, Group.ReadWrite.All, Directory.ReadWrite.All

## Request headers

Header	Value	Required
Authorization	Bearer{Token}	Yes
Content-type	application/json	No

## Default Parameters

Parameter	Description	Data Type	Scope Restricted	Required
\$top	This parameter is internally used to get the group item per page (default set it to 999) Eg: /users? \$top=999	Integer	No	No
\$filter	Filters results (rows). (Default is set to 'Team'). E.g.: /groups? \$filter=resourceProvisioningOptions/Any(x:x eq 'Team')	String	No	No

## Output:

Case Scope

N/A

## Human Readable Output

ID	Display Name	Description	Visibility	Mail Enabled	Mail Nickname	Security Enabled
024b4ef1-d630-4932-84fb-a280602c7185	Microfocus	final test	Public	true	Microfocus	false
03993312-b1b5-466f-83c6-69c08a318069	Architecture Team	The team for those in architecture design.	Public	true	ArchitectureTeam	false
0809e34c-dcae-49d8-b2c2-c918c3985cf7	MicroFocus	team	Public	true	MicroFocus784	false

## 2. List Channels

Enrichment capability to get the list of channels either in this team or shared with this team (incoming channels).

### Required Permissions:

Permission type	Permissions (from least to most privileged)
Application	Channel.ReadBasic.All, ChannelSettings.Read.All, ChannelSettings.ReadWrite.All

**Path Parameters:**

Path Parameter	Description	Type	Scope restricted (Yes/No)	Required (Yes/No)
Team Display Name	The name of the Team. (Team ID will be fetched internally by using the given team's name).	String	No	Yes

**Request headers:**

Header	Value	Required
Authorization	Bearer{token}	Yes
Content-type	application/json	No

**Output:**

Case Scope: N/A

**Human Readable Output**

Channel Id	Created Date Time	Dispaly Name	Description	Membership Type
19:088e199a9062477 b9afc2b3e42c50964 @thread.tacv2	2022-12-20T12:21:00.842Z	Microsoft Postman collection	This channel is where we have to collect all microsoft apis endpoints in potsman	standard
19:c616503f76a403 08c1b24dd1adb209e @thread.tacv2	2022-12-25T00:28:18.08Z	My Private Channel	This is my first private channels	private
19:2fb57f001ede44e3 b12f4954fea62457@t hread.tacv2	2022-12-29T09:44:25.411Z	My Channel	This is my first private channels	standard
19:c26838ce37a04d3 a8db56ea146ea44d1 @thread.tacv2	2023-01-19T12:23:41.352Z	Demo channel	demo channel	standard
19:d000ec51f6ece4ac 2a1b70c7f3788691e @thread.tacv2	2023-01-24T11:44:44.174Z	Sacumen Microfocus Channel	Only Microfocus realted discussion	standard

**3. Create Team**

Action capability to create a new team.

- **Rollback:** No
- **Duplicate Control:** Yes

**Required Permissions:**

Permission type	Permissions (from least to most privileged)
Application	Team.Create, Teamwork.Migrate.All, Group.ReadWrite.All**, Directory.ReadWrite.All**



Permissions marked with \*\* are supported only for backward compatibility. It is recommend that you update your solutions to use an alternative permission listed in the previous table and avoid using these permissions going forward.

**Path Parameters:**

Path Parameter	Description	Type	Scope restricted (Yes/No)	Required (Yes/No)
Display Name	The name of the team.	String	No	Yes
Description	A description for the team.	String	No	Yes

**Output:**

Case Scope: N/A

Human Readable Output: N/A

**4. Create Channel**

Create a new channel in a team, as specified in the request body.

**Rollback:** No

**Duplicate Control:** Yes



You can add a maximum of 200 members when you create a private channel.

**Required Permissions**

Permission type	Permissions (from least to most privileged)
Application	Channel.Create.Group*, Channel.Create, Teamwork.Migrate.All, Group.ReadWrite.All**, Directory.ReadWrite.All**



Permissions marked with \*\* are supported only for backward compatibility. It is recommend that you update your solutions to use an alternative permission listed in the previous table and avoid using these permissions going forward.

**Request headers**

Header	Value	Required
Authorization	Bearer {token}	Yes
Content-type	application/json	No

**Path Parameters:**

Path Parameter	Description	Type	Scope restricted (Yes/No)	Required (Yes/No)
Team Display Name	The name of the Team. (Team Id will be identified internally)	String	Yes	Yes
Channel Display Name	Channel name as it will appear to the user in Microsoft Teams. The maximum length is 50 characters.	String	No	Yes
Description	Textual description for the channel.	String	No	Yes

**Default Parameters**

Parameter	Description	DataType	Scope Restricted	Required
membershipType	The type of channel. Can be set during creation and can't be changed. The possible values are standard, private, unknownFutureValue, shared. The default value is standard. Note that you must use the Prefer: include-unknown-enum-members request header to get the following value in this evolvable enum: shared.  (Default is set to 'private').	String	No	No

**Output:**

Case Scope: N/A

Human Readable Output: N/A

**5. List Team Members**

Enrichment Capability to list given team members.

**Required Permissions**

Permission type	Permissions (from least to most privileged)
Application	TeamMember.Read.Group*, TeamMember.Read.All, TeamMember.ReadWrite.All



Permissions marked with \*\* are supported only for backward compatibility. It is recommended that you update your solutions to use an alternative permission listed in the previous table and avoid using these permissions going forward.

## Request headers

Header	Value	Required
Authorization	Bearer {token}	Yes
Content-type	application/json	No

## Path Parameters:

Path Parameter	Description	Type	Scope restricted (Yes/No)	Required (Yes/No)
Team Display Name	The name of the team	String	Yes	Yes

## Default Parameters:

Path Parameter	Description	Type	Scope restricted (Yes/No)	Required (Yes/No)
MaxResults	You can use this parameter to indicate the maximum number of items you want in the response. The default value is 50. The maximum value is 50.	integer	No	No
NextToken	You can use this parameter when paginating results. Set the value of this parameter to null on your first call to the list action. For subsequent calls to the action, fill nextToken in the request with the value of NextToken from the previous response to continue listing data.	String	No	No

## Output:

Case Scope: N/A

Human Readable Output

User Id	Name	Email	Team Membership	
			Id	Role
aacb40a-16e2-4aad-9457-0785f45abe3a	deepak.b	deepak.b@microsoft.com	MCMjMSMjMWQ4YjVmM2UtMWlwMy00Zjk4LWEyNTQtZWM4OGM1ZGZINTZllyM5ZDlyOGFiZC04OTViLTRkYTMtOTJjMi0wOTM2MWFmZDMYWW EjI2FhY2NINDBhLTE2ZTltNGFhZC05NDU3LTA3ODVmNDVhYmUzYQ==	N/A
3b37f154-67f5-4019-a8f0-a9fa54bdb9f2	Aakash		MCMjMSMjMWQ4YjVmM2UtMWlwMy00Zjk4LWEyNTQtZWM4OGM1ZGZINTZllyM5ZDlyOGFiZC04OTViLTRkYTMtOTJjMi0wOTM2MWFmZDMYWW EjIzNiMzdmMTU0LTY3ZjUtNDAxOS1hO	N/A

## 6. Add Team Member

Action capability to add a member to a given team.



The roles property will be empty by default for all members. This property only contains additional qualifiers when relevant - for example, if the member has owner privileges, the roles property contains owner as one of the values. Similarly, if the member is a guest, the roles property contains a guest as one of the values. A basic member should not have any values specified in the roles property.

**Rollback:** No

**Duplicate Control:** Yes

**Required Permissions:**

Permission type	Permissions (from least to most privileged)
Application	TeamMember.ReadWrite.All

**Request headers:**

Header	Value	Required
Authorization	Bearer {token}	Yes
Content-type	application/json	No

**Default Parameters:**

Parameter	Description	DataType	Scope Restricted	Required
@odata.type	It's value should be: `#microsoft.graph.aadUserConversationMember`	String	No	No



Do not add any guest to the team using this action capability as the name only suggests adding a member to the team. If you are trying to add guests, you will get an access denied error.

### Path Parameters:

Path Parameter	Description	Type	Scope restricted (Yes/No)	Required (Yes/No)
Team Display Name	The name of the team	USERNAME, UNKNOWN, KEYWORD	Yes	Yes
Member Mail	<p>The user object that needs to be added. Eg: `<a 147="" 218="" 563="" 581"="" data-label="Section-Header" href="https://graph.microsoft.com/v1.0/users('8b081ef6-4792-4def-b2c9-c363a1bf41d5')`&lt;/a&gt;&lt;/p&gt; &lt;p&gt;Internally member id will generate&lt;/p&gt; &lt;/td&gt;&lt;td&gt; String.&lt;br/&gt;EMAIL_ADDRESS &lt;/td&gt;&lt;td&gt;No&lt;/td&gt;&lt;td&gt;Yes&lt;/td&gt;&lt;/tr&gt; &lt;/tbody&gt; &lt;/table&gt; &lt;/div&gt; &lt;div data-bbox="> <h3>Output:</h3> </a></p>			

Case Scope: N/A

Human Readable Output: N/A

## 7. Delete Member

Action Capability to delete team members.

**Rollback:** No

**Duplicate Control:** No

### Required Permissions

Permission type	Permissions (from least to most privileged)
Application	TeamMember.ReadWrite.All

### Request headers

Header	Value	Required
Authorization	Bearer {token}	Yes
Content-type	application/json	No

**Path Parameters:**

Path Parameter	Description	Type	Scope restricted (Yes/No)	Required (Yes/No)
Team Display Name	The name of the team	USERNAME, UNKNOWN, KEYWORD	Yes	Yes
Member Display Name	The name of the team member. (The team membership Id will be identified internally).	USERNAME, UNKNOWN, KEYWORD	Yes	Yes

**Output:**

Case Scope: N/A

Human Readable Output: N/A

**8. Send Message**Action Capability to Send a message in the specified [channel](#).**Rollback:** No**Duplicate Control:** No

Application permissions are supported for [migration](#) only. In the future, Microsoft may require an additional fees to be paid based on the amount of data imported.

Therefore, for the above note, a different authentication mechanism called auth\_code flow has been added. Here, the user must perform several steps.

To get auth code url, perform the following:

- The user must call the Get Auth Code URL enrichment capability.

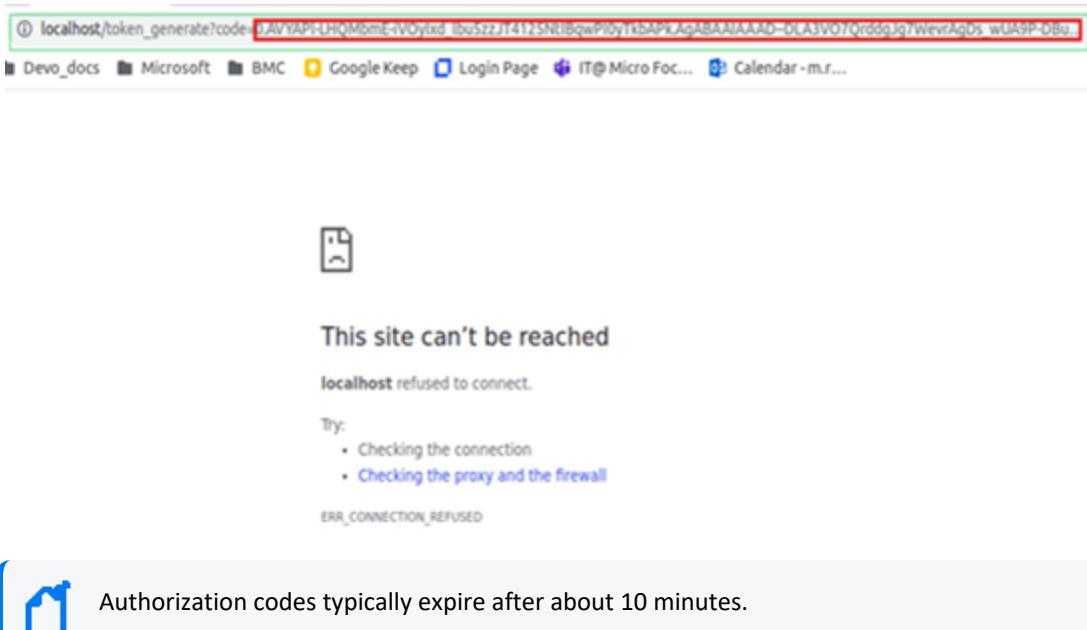


The Auth URL is present in ArcSight SOAR case timeline.



This has to be done before performing **send message in channel** action capability.

- Copy the **Auth URL** from ArcSight SOAR case timeline and paste it into a web browser. On pasting this URL, the browser would be redirected to the Permissions page. **Check the Consent on behalf of your organization** checkbox and click **Accept**.
- After accepting the permissions, the browser will redirect to the **redirect\_uri** with a code in the address bar.



- d. Use the following CURL command to get the **Auth Code**, which is required to get the **Refresh Token**.

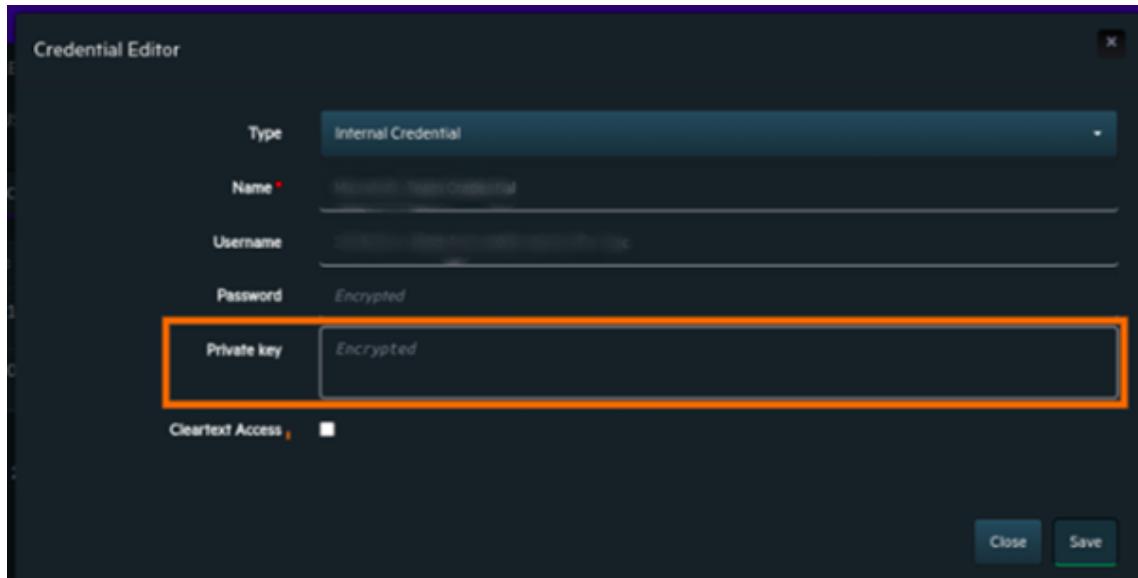
```
curl --location --request POST
'https://login.microsoftonline.com/common/oauth2/v2.0/token' \
--header 'Content-Type: application/x-www-form-urlencoded' \
--data-urlencode 'client_id=<client id>' \
--data-urlencode 'scope=https://graph.microsoft.com/mail.read' \
--data-urlencode 'redirect_uri=<redirect_uri>' \
--data-urlencode 'grant_type=authorization_code' \
--data-urlencode 'client_secret=<client secret>' \
--data-urlencode 'code=<auth_code>' \
curl -'
```

#### Parameters for the refresh token generation

Parameters	Description	DataType	Required
client_id	The application ID that is assigned to your app. You can find this information in the portal where you registered your app.	String	Yes
scope	Default set as:- <code>https://graph.microsoft.com/mail.read</code>	String	Yes
client_secret	The client secret that you generated for your app in the app registration portal. The client secret must be URL-encoded before being sent. instead of providing credentials in the Authorization header, per <a href="#">RFC 6749</a> providing basic auth pattern is also supported.	String	Yes

Parameters	Description	DataType	Required
grant_type	Must be authorization_code for the authorization code flow. Default set it as: Authorization_code	String	Yes
redirect_uri	The redirect_uri of your app, where authentication responses can be sent and received by your app. It must exactly match one of the redirect URIs you registered in the portal .	String	Yes
code	The authorization_code that the app requested. The app can use the authorization code to request an access token for the target resource. Authorization codes are short lived. Typically, they expire after about 10 minutes.	String	Yes

- e. Click Credential Editor > Private Key and paste the refresh token value.



 This step is only required if and only if the user gets the unauthorized code message while performing **Send message in channel** action capability.

### Required Permissions:

Permission type	Permissions (from least to most privileged)
Delegated	Required permissions already added in authorized code URLs.

### Request headers

Header	Value	Required
Authorization	Bearer {token}	Yes
Content-type	application/json	No

### Path Parameters:

Path Parameter	Description	Type	Scope restricted (Yes/No)	Required (Yes/No)
Team Display Name	The name of the team	String	No	Yes
Content	The text message to send to channel	String	No	Yes
Channel Display Name	The name of the channel	String	Yes	Yes

**Output:**

Case Scope: N/A

Human Readable Output: N/A

**9. Retrieve Message**Enrichment Capability to retrieve messages from a given [channel](#).**Permissions for channel:**

Permission type	Permissions (from least to most privileged)
Application	ChannelMessage.Read.Group, ChannelMessage.Read.All, Group.Read.All**, Group.ReadWrite.All**



Permissions marked with \*\* are supported only for backward compatibility. It is recommended that you update your solutions to use an alternative permission listed in the previous table and avoid using these permissions going forward.

**Request headers**

Header	Value	Required
Authorization	Bearer {token}	Yes
Content-type	application/json	No

**Default Request Body Parameters:**

Request Body	Description	Type	Scope restricted (Yes/No)	Required (Yes/No)
Team Display Name	The name of the team	String	No	Yes
Channel Display Name	Name of the channel	HOST, UNKNOWN, KEYWORD	Yes	Yes

**Limitations:** Retrieve Message is a Protected API



Microsoft Teams APIs in Microsoft Graph that access sensitive data are considered protected APIs. These APIs require that you have additional validation, beyond permissions and consent, before you can use them. For more information see, [Protected APIs](#). To request access to these protected APIs, fill the [request form](#) to connect with the Microsoft support team.

## Output:

Case Scope: N/A

Human Readable Output:

<b>Id</b>	<b>Created Date Time</b>	<b>Sender Name</b>	<b>Content</b>	<b>Content Type</b>
1676533857278	2023-02-16T07:50:57.278Z	Abdul Shuaib	MS Team Auth code required only	text
1674981579526	2023-01-29T08:39:39.526Z	Abdul Shuaib	yep	text
1674981576704	2023-01-29T08:39:36.704Z	Abdul Shuaib	See you	text
1674981571583	2023-01-29T08:39:31.583Z	Abdul Shuaib	thank you bye	text
1674981565070	2023-01-29T08:39:25.07Z	Abdul Shuaib	Nice to talk with you!!	text
1674981548578	2023-01-29T08:39:08.578Z	Abdul Shuaib	okay	text

## 10. Archive Team

Action capability to archive a given team.

**Rollback:** Yes

**Duplicate Control:** No

**Required Permissions**

<b>Permission type</b>	<b>Permissions (from least to most privileged)</b>
Application	TeamSettings.ReadWrite.Group*, TeamSettings.ReadWrite.All, Group.ReadWrite.All**, Directory.ReadWrite.All**



Permissions marked with \*\* are supported only for backward compatibility. It is recommended that you update your solutions to use an alternative permission listed in the previous table and avoid using these permissions going forward.

## Request headers

Header	Value	Required
Authorization	Bearer {token}	Yes
Content-type	application/json	No

**Path Parameters:**

Path Parameter	Description	Type	Scope restricted (Yes/No)	Required (Yes/No)
Team Display Name	The name of the team	String	No	Yes

**Output:**

Case Scope: N/A

Human Readable Output: N/A

**11. Unarchive Team**

Action capability to archive a given team.

**Rollback:** Yes**Duplicate Control:** No**Required Permissions**

Permission type	Permissions (from least to most privileged)
Application	TeamSettings.ReadWrite.Group*, TeamSettings.ReadWrite.All, Group.ReadWrite.All**, Directory.ReadWrite.All**



Permissions marked with \*\* are supported only for backward compatibility. It is recommended that you update your solutions to use an alternative permission listed in the previous table and avoid using these permissions going forward.

**Path Parameters:**

Path Parameter	Description	Type	Scope restricted (Yes/No)	Required (Yes/No)
Display Name	The name of the team.	String	No	Yes
Description	A description for the team.	String	No	Yes

**Output:**

Case Scope: N/A

Human Readable Output: N/A

# Integration Guide for Microsoft Windows DNS Server

## Integration Overview

ArcSight SOAR uses Microsoft Windows DNS Server to redirect IP address to another IP address.

SOAR checks connection.secure parameter to connect via WinRM over http or https protocol.

## Integration Capabilities

- Action
- Block

## Configuration

### Configuration on Microsoft Windows DNS Server

- SOAR connects to Microsoft Windows DNS Server's integration API via WinRM services. Therefore SOAR should be able to connect this service.
- WinRM credential is required.

### Configuring ATAR

1. While creating this integration via Integrations tab of Configuration menu:

**Name:** Display name of the integration.

**Type:** Microsoft Windows DNS Server.

**Address:** Address of the integration (the format should be http[s]://1.1.1.1:1234).

**Credential:** WinRM credential is required. Credential that has been defined for this integration under the **Credentials** menu.

**Configuration:** You need to specify the following configuration parameters.

```
dns.zone.name: Redirected DNS server zone name  
dns.block.ip: Redirection address
```

```
dns.server.name: DNS server name  
#Use https:// instead of http:// on WinRM connection  
connection.secure=true : For secure connections, otherwise set to false.  
#Parameters:
```

**WindowsDNSCommandExecPath:** Windows DNS command execution path.

**Trust Invalid SSL Certificates:** Select this if Engine's certificate used for the service is self-signed or not recognized by browsers.

**Require Approval From:** Select user(s) from list to ask her/his approval before executing actions on this integration.

**Notify:** Select user(s) from the list to notify when ATAR performs an action on this integration.

2. Click the **Test** button.
3. Click **Save** to complete integration.

# Integration Guide for Microsoft Windows Services (WinRM)

## Integration Overview

### Integration Capabilities

- Action
- None

## Configuration

### Configuration on Microsoft Windows Services

- SOAR connects to Microsoft Windows Service's integration API via WinRM services.
- Therefore SOAR should be able to connect this service.
- WinRM credential is required.

## Configuring SOAR

1. While creating this integration via Integrations tab of Configuration menu:

**Name:** Display name of the integration.

**Type:** Microsoft Windows Services.

**Address:** Address of the integration (the format should be 1.1.1.1 or abc.example.com).

**Configuration:** You need to specify the following configuration parameters.

putfile.generateuuid =

putfile.defaultfolder =

connection.secure = true

**Credential:** Credential that has been defined for this integration under the Credentials menu.

**Trust Invalid SSL Certificates:** Select this if certificate used for the service is selfsigned or not recognized by browsers.

**Require Approval From:** Select user(s) from list to ask her/his approval before executing actions on this integration.

**Notify:** Select user(s) from the list to notify when SOAR performs an action on this integration.

2. Click the **Test** button.
3. Click **Save** to complete integration.

# Integration Guide for Microsoft Graph Security

## Integration Overview

**Microsoft Graph Security** is an intermediary service (or broker) that provides a single programmatic interface to connect multiple Microsoft Graph Security providers such as Azure Security Center, Microsoft Defender APT, Microsoft Cloud App. Security, etc. Microsoft Graph Security integration lets you to search and manage security alerts created by those providers. This integration supports Microsoft Graph API v1.0.

## Integration Capabilities

- Assign Alert
- Get Alert by ID
- List Alerts
- List Alerts by Category
- List Alerts by Destination
- List Alerts by Provider
- List Alerts by Severity
- List Alerts by Source IP
- List Alerts by Status
- Update Alert Comment
- Update Alert Feedback
- Update Alert Status

## Prerequisites

ArcSight SOAR connects to “[login.microsoft.com](https://login.microsoft.com)” and “[graph.microsoft.com](https://graph.microsoft.com)” APIs through HTTPS. Access to these services is required

.

# Configuration

## Configuring Microsoft Azure

1. Login to <https://portal.azure.com> and navigate to **Azure Active Directory** service.
2. Create a new registration in **App Registrations** menu following values.



Note: If an application is defined for other integrations, skip steps 1-3 to use it.

Name	Supported Account Types	Redirect URI
ArcSight SOAR	Accounts in this organizational directory only (Default Directory only - Single tenant)	(Web) <a href="https://localhost/soar">https://localhost/soar</a>

3. Click **Add a certificate or secret link** and create a new client secret. Specify the description and expiry period as 24 months.
4. Note the created **Secret Key** value along with Client ID.
5. Navigate to **API Permissions** and add the following permissions from Microsoft Graph:

Permission Type	Permission	Description
Application	SecurityEvents, ReadWrite, All.	Read and update your organization's security events.

6. Click **Yes** to grant admin consent for Default Directory.

## Configuring SOAR

1. Click **Configuration > Credential > Create Credential**.
2. Specify the following parameter values in the **Credential Editor** form:

Type	Name	Username	Password	Private Key
Internal credential	Display name of credential set (for example, Azure AD Credential).		Client ID of the application (for example, ArcSight SOAR) that is registered on Azure Portal.	Secret Key

3. Click **Configuration > Integrations > Create Integration**.
4. Specify the following parameter values in the **Configuration** form:

Parameter	Value
Name	Display name of the integration.
Type	Microsoft Graph Security

Parameter	Value	
<b>Address</b>	Address of the integration ( <a href="https://graph.microsoft.com/v1.0/security">https://graph.microsoft.com/v1.0/security</a> ).	
<b>Configuration</b>	Specify the following configuration parameters:	
	<b>tenant.id</b>	Tenant ID on Microsoft Azure tenant.id = ff1f0000-c600-4500-0038-9d4000000000
	<b>proxy.id</b>	ID of the Proxy integration if you access Microsoft Graph Security through a web proxy device. For example, proxy.id = 12345 .
<b>Credential</b>	Credential that has been defined for this integration under the <b>Credentials</b> menu.	
<b>Trust Invalid SSL Certificates</b>	Select this if web server's certificate is self-signed or is not recognized by browsers.	
<b>Require Approval From</b>	Select user(s) from list to ask the approval before executing actions on this integration.	
<b>Notify</b>	Select user(s) from the list to notify when SOAR performs an action on this integration.	

5. Click **Save** to save the integration definition.
6. Navigate to **Configuration>Customization Library** and edit **Microsoft Graph Security Advanced Action Script Default Template**.
7. Select the integration that you have added to **Integrations** menu.
8. Click **Save** to complete the integration.
9. Click **Test**, an **Integration Successful** message is displayed if the credential and address are valid.

## Capabilities

### 1. Assign Alert

Action capability for assigning security alert to a person on Azure Security Center.

- Rollback: No
- Duplicate Control: No

The following table presents the assign alert action capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
<b>Integration</b>	Name of the third party integration.	Integration	N/A	Yes
<b>Assign to</b>	Person this alert to be assigned to.	String	No	Yes

**Output:**

Case Scope: N/A

Human Readable Output: N/A

## 2. Get Alert by ID

Enrichment capability for querying & retrieving security alert details by alert ID.

The following table presents the get alert ID enrichment capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
<b>Integration</b>	Name of the third party integration.	Integration	N/A	Yes
<b>Alert ID</b>	Alert ID on Azure Security Center.	String	No	Yes

**Output:**

Case Scope:

Action	Type	Category/ Value
<b>None</b>	N/A	N/A

Human Readable Output:

Following image provides the **Human Readable Output**:

Key	Value
Title	[SAMPLE ALERT] Suspicious WordPress theme invocation detected
Description	THIS IS A SAMPLE ALERT: The Azure App Service activity log indicates a possible code injection activity on your App Service resource. The suspicious activity detected resembles that of a manipulation of WordPress theme to support server side execution of code, followed by a direct web request to invoke the manipulated theme file. This type of activity was seen in the past as part of an attack campaign over WordPress.
Severity	high
Category	SIMULATED_APPS_WpThemeInjection
Security Resources	[{"resource": "/SUBSCRIPTIONS/9ad0a547-a8dc-4f84-bc79-87b9d5603212/RESOURCEGROUPS/Sample-RG/providers/Microsoft.Web/sites/Sample-App", "resourceType": "attacked"}]
Created Time	2021-08-20T04:42:24.873571Z
ID	2517728662571264282_1b0dea7-1bc2-40c7-a1ca-16775853eed5
Raw	{"eventDateTime": "2021-08-20T04:42:22.873571Z", "lastModifiedDateTime": "2021-08-20T12:31:01.850352Z", "malwareStates": [], "networkConnections": [], "fileStates": [], "registryKeyStates": [], "createdDateTime": "2021-08-20T04:42:24.873571Z", "description": "THIS IS A SAMPLE ALERT: The Azure App Service activity log indicates a possible code injection activity on your App Service resource.\n\nThe suspicious activity detected resembles that of a manipulation of WordPress theme to support server side execution of code, followed by a direct web request to invoke the manipulated theme file.\n\nThis type of activity was seen in the past as part of an attack campaign over WordPress.", "title": "[SAMPLE ALERT] Suspicious WordPress theme invocation detected", "assignedTo": "Ahmet Ozturk", "alertDetections": [], "feedback": ""}

## 3. List Alerts

Enrichment capability for getting list of security alerts created in given time range. Results are based on the alerts creation time, displayed in newest to oldest manner..

The following table presents the list alerts enrichment capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Integration</b>	Name of the third party integration.	Integration	N/A	Yes
<b>Time Range</b>	Time range filter for query.	Time range. Relative: e.g. Last 5 days Absolute: For example, 2021-08-14 15:10 – 2021-08-14 15:32	N/A	Yes

**Output:**

**Case Scope:**

Action	Type	Category/ Value
<b>None</b>	N/A	N/A

**Human Readable Output:**

Following image provides the **Human Readable Output**:

Created Time	Title	Severity	Status	Id
2021-08-20T04:42:24.8891406Z	[SAMPLE ALERT] Potential SQL Injection	high	newAlert	2517728663351108593_e028a31a-2d7a-437a-aa0b-ab4f824ce7c3
2021-08-20T04:42:24.8891406Z	[SAMPLE ALERT] Possible data exfiltration via DNS tunnel (Preview)	low	newAlert	2517728663151108593_7ad517e3-558b-4407-8d2d-7c3f401f65a1
2021-08-20T04:42:24.8891406Z	[SAMPLE ALERT] MicroBurst exploitation toolkit used to extract keys to your storage accounts (Preview)	high	inProgress	2517728663071108593_73692524-d021-43f6-8f9a-e23af4380fb5
2021-08-20T04:42:24.8891406Z	[SAMPLE ALERT] Suspected successful brute force attack	high	inProgress	2517728663331108593_791d8c46-46ac-4adb-9cad-6f3aa5b496c41
2021-08-20T04:42:24.8891406Z	[SAMPLE ALERT] Executable found running from a suspicious location	medium	newAlert	2517728662951264282_a9f1b21a-03ad-4b80-837d-3cb2aec27c70

#### 4. List Alerts by Category

Enrichment capability for getting list of security alerts of a certain category created in given time range. Results are based on the alerts creation time, displayed in newest to oldest manner.

The following table presents the list alert by category enrichment capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Integration</b>	Name of the third party integration.	Integration	N/A	Yes
<b>Alert Category</b>	Category name	String	No	Yes

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Time Range</b>	Time range filter for query.	Time range. Relative: e.g. Last 5 days Absolute: For example, 2021-08-14 15:10 – 2021-08-14 15:32	N/A	Yes

Output:

Case Scope:

Action	Type	Category/ Value
<b>None</b>	N/A	N/A

Human Readable Output:

Following image provides the **Human Readable Output**:

Created Time	Title	Severity	Status	Id
2021-08-20T04:42:24.8891406Z	[SAMPLE ALERT] Digital currency mining related behavior detected	high	newAlert	2517728662971264282_52d66d86-089d-4efb-8ba0-a9f0524f39a6
2021-08-13T10:38:16.2749644Z	[SAMPLE ALERT] Digital currency mining related behavior detected	high	newAlert	2517734497457406600_8d18f7ca-98d6-42ad-9de2-7e500b40b865

## 5. List Alerts by Destination

Enrichment capability for getting list of security alerts with the specified destination field, created in given time range. Results are based on the alerts creation time, displayed in newest to oldest manner.

The following table presents the list alerts by destination enrichment capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Integration</b>	Name of the third party integration.	Integration	N/A	Yes
<b>Destination</b>	Destination Address.	Host Network Address URL .	Yes	Yes
<b>Time Range</b>	Time range filter for query.	Time range. Relative: e.g. Last 5 days Absolute: For example, 2021-08-14 15:10 – 2021-08-14 15:32	N/A	Yes

Output:

Case Scope:

Action	Type	Category/ Value
<b>None</b>	N/A	N/A

Human Readable Output:

Following image provides the **Human Readable Output**:

Created Time	Title	Severity	Status	Id
2021-08-20T04:42:24.8891406Z	[SAMPLE ALERT] Potential SQL Injection	high	newAlert	2517728663351108593_e028a31a-2d7a-437a-aa0b-ab4fb24ce7c3
2021-08-20T04:42:24.8891406Z	[SAMPLE ALERT] Possible data exfiltration via DNS tunnel (Preview)	low	newAlert	2517728663151108593_7ad617e3-558b-4407-8dd7-7cf401f65a1
2021-08-20T04:42:24.8891406Z	[SAMPLE ALERT] MicroBurst exploitation toolkit used to extract keys to your storage accounts (Preview)	high	inProgress	2517728663071108593_73692524-d021-43f6-8f9a-e23af4380fb5
2021-08-20T04:42:24.8891406Z	[SAMPLE ALERT] Suspected successful brute force attack	high	inProgress	2517728663331108593_791d8c46-46ac-4adb-9cad-6f3aab496c41
2021-08-20T04:42:24.8891406Z	[SAMPLE ALERT] Executable found running from a suspicious location	medium	newAlert	2517728662951264282_a9f1b21a-03ad-4b80-837d-3cb2aec27c70

## 6. List Alerts by Provider

Enrichment capability for getting list of security alerts originated from the specified security provider, created in given time range. Results are based on the alerts creation time, displayed in newest to oldest manner.

The following table presents the list alerts by provider enrichment capability:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Integration</b>	Name of the third party integration.	Integration	N/A	Yes
<b>Provider</b>	One of the Microsoft Security Providers.	String Azure Active Directory Identity Protection Azure Advanced Threat Protection Azure Security Center Azure Sentinel Microsoft Cloud App Security Microsoft Defender Advanced Threat Protection	No	Yes
<b>Time Range</b>	Time range filter for query.	Time range. Relative: For example, Last 5 days Absolute: For example, 2021-08-14 15:10 – 2021-08-14 15:32	N/A	Yes

Output:

Case Scope:

Action	Type	Category/ Value
<b>None</b>	N/A	N/A

Human Readable Output:

Following image provides the **Human Readable Output**:

Created Time	Title	Severity	Status	Id
2021-08-20T04:42:24.8891406Z	[SAMPLE ALERT] Potential SQL Injection	high	newAlert	2517728663351108593_e028a31a-2d7a-437a-aa0b-ab4f824ce7c3
2021-08-20T04:42:24.8891406Z	[SAMPLE ALERT] Possible data exfiltration via DNS tunnel (Preview)	low	newAlert	2517728663151108593_7adb17e-3-558b-4407-8d2d-7c3f40165a1
2021-08-20T04:42:24.8891406Z	[SAMPLE ALERT] MicroBurst exploitation toolkit used to extract keys to your storage accounts (Preview)	high	inProgress	2517728663071108593_7369252-4-d021-43f6-8f9a-e23af4380fb5
2021-08-20T04:42:24.8891406Z	[SAMPLE ALERT] Suspected successful brute force attack	high	inProgress	2517728663331108593_791d8c4-6-46ac-4adb-9cad-6f3aab496c41
2021-08-20T04:42:24.8891406Z	[SAMPLE ALERT] Executable found running from a suspicious location	medium	newAlert	2517728662951264282_a91b21a-03ad-4b80-837d-5cb2aec27c70

## 7. List Alerts by Severity

Enrichment capability for getting list of security alerts with the specified severity value, created in given time range. Results are based on the alerts creation time, displayed in newest to oldest manner.

The following table presents the list alerts by severity enrichment capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Integration</b>	Name of the third party integration.	Integration	N/A	Yes
<b>Alert Severity</b>	Alert severity set by vendor/provider.	String High Medium Low Informational Unknown	No	Yes
<b>Time Range</b>	Time range filter for query.	Time range. Relative: For example, Last 5 days Absolute: For example, 2021-08-14 15:10 – 2021-08-14 15:32	N/A	Yes

Output:

Case Scope:

Action	Type	Category/ Value
None	N/A	N/A

Human Readable Output:

Following image provides the **Human Readable Output**:

Created Time	Title	Severity	Status	Id
2021-08-20T04:42:24.8735717Z	[SAMPLE ALERT] Exposed Kubernetes service detected	medium	newAlert	2517728662731264282_6fad8e3-cc13-4633-988f-1bf342f9af94
2021-08-20T04:42:24.8735717Z	[SAMPLE ALERT] Logon from an unusual location	medium	newAlert	2517728662831264282_4a0555a-b-14fe-4db8-97be-f368f0825b35
2021-08-20T04:42:24.8735717Z	[SAMPLE ALERT] Kubernetes events deleted (Preview)	medium	newAlert	2517728663271264282_e4190ac7-2754-4ea-beb5-5d3e24e1ae2d
2021-08-20T04:42:24.8735717Z	[SAMPLE ALERT] High volume of operations in a Key Vault	medium	newAlert	2517728662631264282_32ecc7af-91be-4b28-9ac5-511a271073d2
2021-08-20T04:42:24.8735717Z	[SAMPLE ALERT] Suspicious policy change and secret query in a Key Vault	medium	newAlert	2517728662671264282_e5953fb-640c-41d1-a685-ec5bd18f05a7

## 8. List Alerts by Source IP

Enrichment capability for getting list of security alerts with the specified source IP field, created in given time range. Results are based on the alerts creation time, displayed in newest to oldest manner.

The following table presents the list alerts by source IP enrichment capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Integration</b>	Name of the third party integration.	Integration	N/A	Yes
<b>Source IP</b>	Source IP Address.	Network Address	Yes	Yes
<b>Time Range</b>	Time range filter for query.	Time range. Relative: For example, Last 5 days Absolute: For example, 2021-08-14 15:10 – 2021-08-14 15:32	N/A	Yes

Output:

Case Scope:

Action	Type	Category/ Value
<b>None</b>	N/A	N/A

Human Readable Output:

Following image provides the **Human Readable Output**:

Created Time	Title	Severity	Status	Id
2021-08-20T04:42:24.8891406Z	[SAMPLE ALERT] Potential SQL Injection	high	newAlert	2517728663351108593_e028a31a-2d7a-437a-aa0b-ab4f824ce7c3
2021-08-20T04:42:24.8891406Z	[SAMPLE ALERT] Possible data exfiltration via DNS tunnel (Preview)	low	newAlert	25177286631108593_7ad617e-3-558b-4407-8d2d-7c3f401f65a1
2021-08-20T04:42:24.8891406Z	[SAMPLE ALERT] MicroBurst exploitation toolkit used to extract keys to your storage accounts (Preview)	high	inProgress	2517728663071108593_7369252-4-d021-43f6-8f9a-e23af4380fb5
2021-08-20T04:42:24.8891406Z	[SAMPLE ALERT] Suspected successful brute force attack	high	inProgress	2517728663331108593_791d8c4-6-4ac-4adb-9cad-6f3aab496c41
2021-08-20T04:42:24.8891406Z	[SAMPLE ALERT] Executable found running from a suspicious location	medium	newAlert	2517728662951264282_a9f1b21a-03ad-4b80-837d-3cb2ae27c70

## 9. List Alerts by Status

Enrichment capability for getting list of security alerts with the specified status value, created in given time range. Results are based on the alerts creation time, displayed in newest to oldest manner.

The following table presents the list alerts by source enrichment capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Integration</b>	Name of the third party integration.	Integration	N/A	Yes
<b>Alert Status</b>	Alert lifecycle status (stage).	String NewAlert InProgress Resolved Unknown	No	Yes
<b>Time Range</b>	Time range filter for query.	Time range. Relative: For example, Last 5 days Absolute: For example, 2021-08-14 15:10 – 2021-08-14 15:32	N/A	Yes

Output:

Case Scope:

Action	Type	Category/ Value
None	N/A	N/A

Human Readable Output:

Following image provides the **Human Readable Output**:

Created Time	Title	Severity	Status	Id
2021-08-20T04:42:24.873571Z	[SAMPLE ALERT] Exposed Kubernetes service detected	medium	newAlert	2517728662731264282_6fad8e3-cc13-4633-988f-1bf342f9af94
2021-08-20T04:42:24.873571Z	[SAMPLE ALERT] Logon from an unusual location	medium	newAlert	2517728662831264282_4a0555a-b14fe-4d8c-97be-f368f0825b35
2021-08-20T04:42:24.873571Z	[SAMPLE ALERT] Kubernetes events deleted (Preview)	medium	newAlert	251772863271264282_e4190ac7-2754-4ea-beb5-5d3e24e1ae2d
2021-08-20T04:42:24.873571Z	[SAMPLE ALERT] High volume of operations in a Key Vault	medium	newAlert	2517728662631264282_32ec7af-91be-4b28-9ac5-511a271073d2
2021-08-20T04:42:24.873571Z	[SAMPLE ALERT] Suspicious policy change and secret query in a Key Vault	medium	newAlert	2517728662671264282_e5953fc6-640c-41d1-a685-ec5bd18f05a7

## 10. Update Alert Comment

Action capability for adding/updating comment field of the security alert.

- Rollback: No
- Duplicate Control: No

The following table presents the update alert comments action capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Integration</b>	Name of the third party integration.	Integration	N/A	Yes
<b>Alert ID</b>	Alert ID on Azure Security Center.	String	No	Yes
<b>Alert Comment</b>	Comment to be added to security alert.	String Closed in IPC Closed in MCAS	No	Yes

Output:

Case Scope: N/A

Human Readable Output: N/A

## 11. Update Alert Feedback

Action capability for adding/updating feedback field of the security alert.

- Rollback: No
- Duplicate Control: No

The following table presents the update alert feedback action capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Integration</b>	Name of the third party integration.	Integration	N/A	Yes
<b>Alert ID</b>	Alert ID on Azure Security Center.	String	No	Yes
<b>Alert Feedback</b>	Comment to be added to security alert.	String Benign Positive False Positive True Positive Unknown	No	Yes

Output:

Case Scope: N/A

Human Readable Output: N/A

## 12. Update Alert Status

Action capability for updating status of the security alert.

- Rollback: No
- Duplicate Control: No

The following table presents the update alert status action capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
<b>Integration</b>	Name of the third party integration.	Integration	N/A	Yes
<b>Alert ID</b>	Alert ID on Azure Security Center.	String	No	Yes
<b>Alert Status</b>	Comment to be added to security alert.	String In Progress New Alert Resolved Unknown	No	Yes

Output:

Case Scope: N/A

Human Readable Output: N/A

# Integration Guide for MISP

## Integration Overview

The MISP threat sharing platform is a free and open source software helping information sharing of threat intelligence including cyber security indicators.

## Integration Capabilities

ArcSight SOAR has the following integration capabilities with MISP.

- File Reputation
- IP Reputation
- URL Reputation
- Get Event
- Add Attribute to Event
- Add Tag to Event
- Create Event
- Create Event with Attribute
- Remove Attribute from Event
- Remove Tag from Event

ArcSight SOAR integrates with MISP to gather, store threat information and can query to IoCs. The capabilities can either be performed automatically within a playbook or manually by an analyst.

## Configuration

### Prerequisites

- Access to tcp port 443 as SOAR connects to MISP using HTTPS
- An API key for SOAR to connect to MISP



**Note:** To gather the API key for SOAR, navigate to **MISP Interface > Event Actions > Automation**.

The screenshot shows the MISP web interface with the 'Automation' page selected. The left sidebar has a 'Automation' section highlighted. The main content area is titled 'Automation' and contains the following text:

Automation functionality is designed to automatically feed other tools and systems with the data in your MISP repository. To make this functionality available for automated tools an authentication key is used.

You can use the REST client to test your API queries against your MISP and export the resulting tuned queries as curl or python scripts. Make sure you keep your API key secret as it gives access to the all of the data that you normally have access to in MISP. To view the old MISP automation page, click here.

Your current key is: `Vm6r#Fkrg66Tmj4rCdV77btRebsvuSdSznCuU1`. You can [reset](#) this key.

**Search**

It is possible to search the database for attributes based on a list of criteria. To return an event or a list of events in a desired format, use the following syntax. Whilst a list of parameters is provided below, it isn't necessarily exhaustive, specific export formats could have additional parameters.

```
https://192.168.200.54/attributes/restSearch
https://192.168.200.54/events/restSearch
```

**returnFormat:** Set the return format of the search (Currently supported: json, xml, openioc, suricata, snort - more formats are being moved to restSearch with the goal being that all searches happen through this API). Can be passed as the first parameter after restSearch or via the JSON payload.

## Configuring SOAR

1. Click **Configuration > Credentials > Create Credential**.
2. Specify the following parameter values in the **Credential Editor** form:
  - a. **Internal Credential**

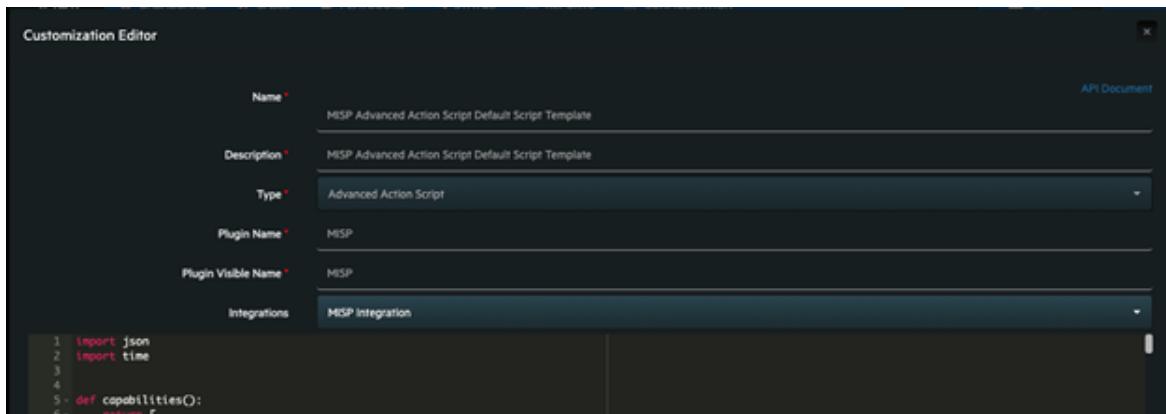
Parameter	Value
Type	Internal Credential
Name	Display name of credential set (For example, MISP Credentials)
Username	Empty
Password	Empty
Private Key	API Key retrieved from the MISP

3. Click **Configuration > Integrations > Create Integration**.
4. Specify the following parameter values in the **Configuration** form:

Parameter	Value
Name	Display name of MISP integration on ArcSight SOAR
Type	MISP
Address	Address of the cloud service, in the following format: <code>https://&lt;misp_environement_ip&gt;</code>
Credential	Name of the credential set created in the previous step(For example, MISP Credentials)

Parameter	Value
Trust Invalid SSL Certificates	Not Applicable
Require Approval From	Select users from the list who can provide approval before executing enrichments on the integration
Notify	Select users from the list to notify when SOAR performs an enrichment on the integration

5. Click **Save** to complete the integration.
6. Navigate to **Configuration > Customization Library**.
7. In the **Customization Editor**, Edit **MISP Advanced Action Script Default Script Template** and for the **Integrations** field select the integration you saved (for example, MISP Integration).



8. Navigate to **Configuration > Integrations**.
9. Click **Edit** for the MISP integration you created.
10. Click **Test** to test the integration.

# Integration Guide for MxToolBox

## Integration Overview

**MxToolBox** is a service that helps customers to make a query for domains and run the lookups.

## Integration Capabilities

ArcSight SOAR has the following integration capabilities with MxToolBox:

- Domain Blacklist Check
- Domain MX Check

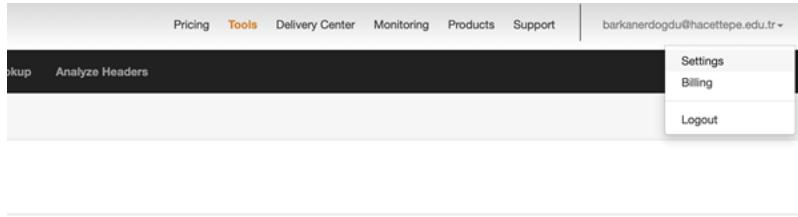
## Prerequisites

You must have access to HTTPS as the ArcSight SOAR connects to MxToolBox API through this service.

## Configuration

### Configuring MxToolBox

1. Login to MxToolBox and navigate to **Settings**, as shown in the following figure:



2. Click **Automation API Access Settings** in the Setting and add a new application.

3. Click **API Tab** and note the **API Key** to use on SOAR as shown in the following figure:

The screenshot shows the 'API' tab selected in the top navigation bar of the MxToolBox website. Below the navigation, there's a section titled 'ABOUT MXTOOLBOX API' with a brief description. A red box highlights the 'API Key' field, which contains the value '4f72d1c1-8e53-4'. To the right of the key is a 'Revoke API Key' button. Below this, there's a 'Api Usage' section with two status indicators: 'Dns Requests Remaining Today: 64 of 64' and 'Network Requests Remaining Today: 0 of 0'. A 'Request an increase to API limits' button is also present. At the bottom, there's a section titled 'MxToolbox API Available Methods' listing four items: 'Lookup', 'Monitor', 'Monitor Tags', and 'Usage', each with a '+' sign to expand.

## Configuring SOAR

1. Click **Configuration > Credentials > Create Credential**.
2. Specify the following parameter values in the **Credential Editor**

Type	Name	Username	Password	Private Key
Internal credential	Display name of credential set (for example, MxToolBox Credential).			API Key that is noted from the service

3. Click **Configuration > Integrations > Create Integration**.
4. Specify the following parameter values in the **Configuration Form**.

Parameter	Value
<b>Name</b>	Display name of MxToolBox integration on SOAR.
<b>Type</b>	MxToolBox
<b>Address</b>	<a href="https://mxtoolbox.com">https://mxtoolbox.com</a>
<b>proxy.id</b>	ID of the Proxy integration if you access mxtoolbox.com through a web proxy device. For Example: proxy.id = 12345.
<b>Credential</b>	Name of the credential set created on step 2(For example, MxToolBox Credentials).

Parameter	Value
<b>Trust Invalid SSL Certificates</b>	The SSL certificate of MxToolBox service is going to known by SOAR, so you do not need to check this box.
<b>Required Approval From</b>	Select users from the list who can provide approval before executing actions on this integration.
<b>Notify</b>	Select users from the list to notify when SOAR performs an action on this integration.

5. Click **Save** to save the integration definition.
6. Navigate to **Configuration > Customization Library > Open MxToolBox Script**
7. Select integration that is created at step 4 for **Integrations** field.
8. Click **Save** to complete the integration.
9. Click **Test**, an **Integration Successful** message is displayed if the credential and address are valid.

## Capabilities

### 1. Domain Blacklist Check

Enrichment capability for retrieving blacklist domain information.

The following table provides the **Domain Blacklist Check** enrichment capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
<b>Domain</b>	Domain that you want to query.	Host	Yes	Yes
<b>Integration</b>	Name of the integration.	Integration	N/A	Yes

#### Output:

Case Scope: N/A

Human Readable Output: Yes

### 2. Domain MX Check

Enrichment capability for retrieving MX record information.

The following table provides the **Domain MX Check** enrichment capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
<b>Domain</b>	Domain that you want to query.	Host	Yes	Yes
<b>Integration</b>	Name of the integration.	Integration	N/A	Yes

#### Output:

Case Scope: N/A

Human Readable Output:

Parameters Details	
Attribute	Info
DMARC Record Published	No DMARC Record found
DNS Record Published	DNS Record not found
Total 2 , 100 items / page	1

# Integration Guide for Netskope v1

## Overview of the Plugin

Netskope is a Cloud Security/Security Service Edge (SSE) platform which secures access to the web, cloud services. Netskope provides solutions to help organizations discover, understand, and secure cloud usage across all their users, devices, apps, and data. Their offerings include cloud security posture management, cloud access security broker (CASB), data loss prevention, and threat protection to help organizations safely embrace cloud services and meet compliance requirements.

## Supported Integration Capabilities

ArcSight SOAR has the following integration capabilities with Netskope V1:

- List Quarantined Files
- Allow Quarantined File
- Block Quarantined File

## Prerequisites

You must have access to HTTPS, as the ArcSight SOAR connects to Netskope API through HTTPS service.

# Configuration

## Configuring Netskope

### 1. Authentication:

Netskope REST APIs use an auth token to make authorized calls to the API.

Netskope REST APIs provide access to resources via URI paths. The auth token must be used in every REST API call for the tenant. Click Settings > Tools > Rest API v1 to generate or revoke a token in the Netskope UI.

- Click Generate New Token and note down the token generated.
- To set the token expiration, click the pencil icon next to the expiration date.
- From the dropdown list, select the number of hours, days, weeks or months to keep the token valid, or to never expire it, and then click Save.

#### Authentication Parameters

##### Request Headers:

Parameters	Datatype	Description	Required
Access Key	string	The Netskope REST API v1 token	Yes

### 2. Additional Configuration:

Configuration Parameter	Description
proxy.id	Proxy device to be used while communicating with the remote system's API
cache.reusing.duration	Default cache-reuse parameter



In the Address configuration, replace the tenant-name with your tenant name.  
Eg:<https://alliances.goskope.com>

## Configuring SOAR

- Click Configuration > Credentials > Create Credentials.
- Specify the following parameter values in the Credential Editor form.

Type	Name	Username	Password	Private Key
Internal credential	Display name of credential set (for example, Netskope v1 Credentials).	N/A	N/A	The Netskope REST API v1 token

3. Click Configuration > Integrations > Upload plugin.
4. Select your integration plugin zip file and click Save.
5. Select the integration that you have added to the Integrations menu.
6. Click Save to complete the integration.
7. Click Test, an Integration Successful message is displayed if the credential and address are valid.

## Integration Capabilities:

### 1. List Quarantined Files

Enrichment capability to get the list of quarantined files.

**Input Parameters:**

N/A

**Default Parameters:**

Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
op	The operation to be performed. Allowed values: get-files   download-url   take-action Default value: get-files (Will get list of quarantined files.)	String	No	Yes

**Output:**

Case Scope:

N/A

Human Readable Output:

### 2. Block Quarantined File

The action capability to block a quarantined file. This capability deletes the quarantined file.

**Rollback:** No

**Duplicate Control:** Yes

**Input Parameters:**

Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
Quarantine Profile Name	The profile name of the quarantined file.	String	No	Yes
File Name	The name of the quarantined file.	[FILE NAME, UNKNOWN, KEYWORD]	Yes	Yes

**Default Parameters:**

Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
op	The operation to be performed.  <b>Allowed values:</b> get-files   download-url   take-action Default value: `take-action` (Action to be taken on a SINGLE quarantined file.)	String	No	Yes
action	Action to be performed on a quarantined file.  <b>Allowed values:</b> block   allow Default value: `block`	String	No	Yes

**Output:**

Case Scope: N/A

Human Readable Output: N/A

**3. Allow Quarantined File**

The action capability to allow a quarantined file. This capability restores the quarantined file.

**Rollback:** No**Duplicate Control:** Yes**Input Parameters:**

Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
Quarantine Profile Name	The profile name of the quarantined file.	String	No	Yes
File Name	The name of the quarantined file.	[FILE NAME, UNKNOWN, KEYWORD]	Yes	Yes

**Default Parameter:**

Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
op	The operation to be performed.  <b>Allowed values:</b> get-files   download-url   take-action <b>Default value:</b> `take-action` (Action to be taken on a SINGLE quarantined file.)	String	No	Yes
action	Action to be performed on a quarantined file.  <b>Allowed values:</b> block   allow <b>Default value:</b> `allow`	[FILE NAME, UNKNOWN, KEYWORD]	No	Yes

**Output:**

Case Scope: N/A

Human Readable Output: N/A

# Integration Guide for Netskope V2

## Integration Overview

Netskope is a Cloud Security/Security Service Edge (SSE) platform which secures access to the web and cloud services. Netskope provides solutions to help organizations discover, understand, and secure cloud usage across all their users, devices, apps, and data. The offerings include cloud security posture management, cloud access security broker (CASB), data loss prevention, and threat protection to help organizations safely embrace cloud services and meet compliance requirements.

## Integration Capabilities

ArcSight SOAR has the following integration capabilities with Netskope V2:

- Search Alerts
- List URL Lists
- Get URL List Details
- Add to URL List
- Remove from URL List

## Prerequisites

You must have access to HTTPS as the ArcSight SOAR connects to Netskope API through HTTPS service.

## Configuration

### Configuring Netskope

#### 1. Authentication:

Netskope REST APIs use an auth token to make authorized calls to the API. Click Settings > Tools > Rest API v2 to create the token for specific APIs.

2. Click New Token to create a new token on the REST API v2.
3. Enter a token name and the token expiration time, and then click Add Endpoint to select the API endpoints to use with the token.
4. Specify the privileges for each of the endpoints added.  
Read privileges include GET, and Read+Write privileges include GET, PUT, POST, PATCH, and DELETE.
5. Click Save.
6. A confirmation box appears showing whether the token creation was successful. If yes, click Copy Token to save it for later use in your API requests.



Add the token to the Netskope-Api-Token header.

### Authentication Parameters

#### Request Headers:

Parameters	Datatype	Description	Required
Access Key	string	The Netskope REST API v2 token	Yes

#### 2. Additional Configuration:

Configuration Parameter	Description
proxy.id	Proxy device to be used while communicating with the remote system's API
cache.reusing.duration	Default cache-reuse parameter
url_list_name	Name of the URL list



**Note:** Replace tenant-name with your tenant name in the Address configuration  
For example: <https://alliances.goskope.com>

## Configuring SOAR

1. Click Configuration > Credentials > Create Credentials.
2. Specify the following parameters values in the Credential Editor form.

Type	Name	Username	Password	Private Key
Internal credential	Display name of credential set (for example, Netskope v2 Credentials).	N/A	N/A	The Netskope REST API v2 token

3. Click Configuration > Integrations > Upload plugin.
4. Select your integration plugin zip file and click Save.
5. Select the integration that you have added to Integrations menu.
6. Click Save to complete the integration
7. Click Test, an Integration Successful message is displayed if the credential and address are valid.

## Integration Capabilities:

### 1. Search Alerts

Enrichment capability to a list of alerts generated by Netskope. You can filter Search Alerts based on the time period.

#### Required Scopes

Endpoint Name	Required Privilege
/api/v2/events/data/alert	Read



These privileges are specified while creating the REST API Token.

#### Input Parameters:

Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
Time Range	The relative or absolute time range for the alerts to retrieve.  The required starttime and endtime will be calculated internally based on the given Time range.	Integer/ Datetime	No	Yes
Username/User IP Address	Filter alerts by the username or user IP address.	["USERNAME", "NETWORK ADDRESS", "UNKNOWN", "KEYWORD"]	Yes	Yes
Severity	Filter alerts by severity.	String	No	Yes

**Default Parameters:**

Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
limit	Maximum number of records to retrieve.  Default value is 5000	Integer	No	No
offset	Used to shift the window of alerts if limit is reached.  Default value is 0	Integer	No	No

**Output:****Case Scope:**

N/A

**Human Readable Output:**

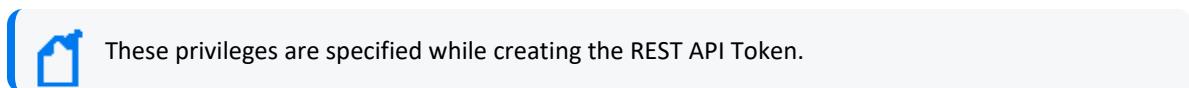
Id	Action	Alert Name	Alert Type	Attack Severity	Timestamp	User	User Ip
a3eae4273b9a87e49daa148e	anomaly_detection	Suspicious Data Movement	uba	high	2023-01-03T06:00:04.0Z	Aaron.Etheridge (@kkrlgistics.com)	172.31.11.215
762edcccd5478eb2228dfaee2	anomaly_detection	Suspicious Data Movement	uba	high	2022-12-27T06:00:04.0Z	Aaron.Etheridge (@kkrlgistics.com)	172.31.11.215
74da621548b5995f33933d63	anomaly_detection	Suspicious Data Movement	uba	high	2023-01-19T06:00:05.0Z	Aaron.Etheridge (@kkrlgistics.com)	172.31.11.215
45c20e35d2337c51d16de877	anomaly_detection	Suspicious Data Movement	uba	high	2023-02-22T06:00:05.0Z	Aaron.Etheridge (@kkrlgistics.com)	172.31.11.215
8dc2a1fc1cadcc379f70004	anomaly_detection	Suspicious Data Movement	uba	high	2023-01-10T06:00:04.0Z	Aaron.Etheridge (@kkrlgistics.com)	172.31.11.215
cecede3faa7d08d9c25295ab	anomaly_detection	Suspicious Data Movement	uba	high	2023-02-06T06:00:05.0Z	Aaron.Etheridge (@kkrlgistics.com)	172.31.11.215
ac014e154b8121e6b3bb1ad	anomaly_detection	Suspicious Data Movement	uba	high	2023-02-12T06:00:04.0Z	Aaron.Etheridge (@kkrlgistics.com)	172.31.11.215
9eeb273f977da1de2febfbad	anomaly_detection	Suspicious Data Movement	uba	high	2023-02-07T06:00:06.0Z	Aaron.Etheridge (@kkrlgistics.com)	172.31.11.215
b2addf31d256f97c99a775d5	anomaly_detection	Suspicious Data Movement	uba	high	2023-01-20T06:00:05.0Z	Aaron.Etheridge (@kkrlgistics.com)	172.31.11.215

## 2. List URL Lists

Enrichment capability to get all applied and pending URL lists.

Required Scopes

Endpoint Name	Required Privilege
/api/v2/policy/urllist	Read



Input parameters:

N/A

Output:

Case Scope:

N/A

**Human Readable Output:**

<b>Id</b>	<b>Name</b>	<b>Urls Count</b>	<b>Type</b>	<b>Modified By</b>	<b>Modified Time</b>	<b>Modified Type</b>	<b>Pending</b>
2	Allowed URLs	1	exact	aarguelles@lum-u.io	2023-02-13T20:02:11.000Z	Edited	0
5	bannedUrlList1w er	2	exact	darshit.trivedi@c restdatasys.com	2022-12-22T00:00:00.000Z	Edited	0
18	CE Fireeye	1	exact	aarguelles@lum-u.io	2023-02-13T20:02:11.000Z	Edited	0
25	testing	1	exact	darshit.trivedi@c restdatasys.com	2022-01-12T00:00:00.000Z	Edited	0
27	root	1	exact	aarguelles@lum-u.io	2023-02-13T20:02:12.000Z	Edited	0
30	Teting resilient	1	exact	aarguelles@lum-u.io	2023-02-13T20:02:12.000Z	Edited	0
31	Teting resilient1	1	exact	aarguelles@lum-u.io	2023-02-13T20:02:12.000Z	Edited	0
32	Resilient URL Lists	1	exact	aarguelles@lum-u.io	2023-02-13T19:51:46.000Z	Edited	0
37	string111	1	exact	aarguelles@lum-u.io	2023-02-13T20:02:13.000Z	Edited	0

**3. Get URL List Details**

Enrichment capability to get details of the given URL list by name.

**Input Parameters:**

<b>Name</b>	<b>Description</b>	<b>Type</b>	<b>Scope restricted (Yes/No)</b>	<b>Required (Yes/No)</b>
URL List Name	Name of the URL List.	String	No	Yes

**Output:**

Case Scope: N/A

**Human Readable Output:**

<b>Key</b>	<b>Value</b>
Id	1
Name	test01
URLs	[ "www.test.com", "www.testing.co.in", "1.2.3.4", "www.test-new.com" ]
Type	exact
Modified by	API
Modified time	2023-02-25T07:48:25.000Z
Modified type	Edited
Pending	1

#### 4. Add to URL List

Action capability to add a new URL to an existing URL list by updating it.

**Rollback:** Yes

**Duplicate Control:** No



Update URL List API is used to implement this feature and it does not support Duplicate Control.

##### Required Scopes

Endpoint Name	Required Privilege
/api/v2/policy/urllist	ReadWrite



These privileges are specified while creating the REST API Token.

##### Input Parameters:

Parameter	Description	Type	Scope restricted (Yes/No)	Required (Yes/No)
URL / HOST / IP	The url to be added. Eg: 'www.example.com'	[ "URL", "HOST", "NETWORK ADDRESS", "UNKNOWN", "KEYWORD" ]	Yes	Yes

##### Default Parameters:

Parameter	Description	Type	Scope restricted (Yes/No)	Required (Yes/No)
action	The action to be performed on URL list.  Default value: append	String	No	Yes

##### Output:

Case Scope: N/A

Human Readable Output: N/A

#### 5. Remove from URL List

Action capability to remove a specific URL from an existing URL list by updating it.

**Rollback:** Yes

**Duplicate Control:** No



Update URL List API is used to implement this feature and it does not support Duplicate Control.

### Required Scopes

Endpoint Name	Required Privilege
/api/v2/policy/urllist	Read+Write



These privileges are specified while creating the REST API Token.

### Input Parameters:

Parameter	Description	Type	Scope restricted (Yes/No)	Required (Yes/No)
URL / HOST / IP	The URL to be removed. Eg: 'www.example.com'	[ "URL", "HOST", "NETWORK ADDRESS", "UNKNOWN", "KEYWORD" ]	Yes	Yes

### Default Parameters:

Parameter	Description	Type	Scope restricted (Yes/No)	Required (Yes/No)
action	The action to be performed on URL list.  Default value: replace	String	No	Yes

### Output:

Case Scope: N/A

Human Readable Output: N/A

## Integration Guide for Okta

### Integration Overview

**Okta** provides cloud software that helps organizations to manage and secure user authentication into applications.

This integration supports Okta API v1.0.

### Integration Capabilities

ArcSight SOAR has the following integration capabilities with Okta:

- Activate User
- Add User Into Group
- Clear User Sessions
- Deactivate User
- Expire Password
- Get Group Members
- Get Groups For User
- Get User Details
- Get User Logs
- List Groups
- Remove User From Group
- Reset Password
- Set Temporary Password
- Suspend User
- Unlock User
- Unsuspend User
- List Devices
- Get Device Details
- Suspend Device
- Unsuspend Device

## Prerequisites

- You must have access to HTTPS as the ArcSight SOAR connects to Okta API through this service.
- API Token is needed to access Okta REST API.

# Configuration

## Configuring SOAR

1. Click **Configuration > Credential > Create Credential**.
2. Specify the following parameters in the **Credential Editor** form:

Type	Name	Username	Password	Private Key
Internal credential	Display name of credential set (for example, Okta API Credentials).			SSWS<space>API token

 **Note:** The API token must be specified in the Private Key field by adding SSWS term (SSWS<space><apitoken>).

3. Click **Configuration > Integrations > Create Integration**.
4. Specify the following parameter values in the **Configuration Form**.

Parameter	Value		
<b>Name</b>	Display name of the integration.		
<b>Type</b>	Okta		
<b>Address</b>	Address of the integration (the format should be https://dev-1423.okta.com/).		
<b>Configuration</b>	Specify the following configuration parameters:  <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <td style="padding: 2px;">proxy.id</td> <td style="padding: 2px;">ID of the Proxy integration if you access Okta through a web proxy device. For example: proxy.id = 12345 .</td> </tr> </table>	proxy.id	ID of the Proxy integration if you access Okta through a web proxy device. For example: proxy.id = 12345 .
proxy.id	ID of the Proxy integration if you access Okta through a web proxy device. For example: proxy.id = 12345 .		
<b>Credential</b>	Credential that has been defined for this integration under the <b>Credentials</b> menu.		
<b>Trust Invalid SSL Certificates</b>	Select this if web server's certificate is self-signed or is not recognized by browsers.		
<b>Require Approval From</b>	Select user(s) from list to ask the approval before executing actions on this integration.		
<b>Notify</b>	Select user(s) from the list to notify when SOAR performs an action on this integration.		

5. Click **Save** to save the integration definition.
6. Navigate to **Configuration>Customization Library** and edit **Okta Advanced Action Script Default Template**.
7. Select the integration that you have added to **Integrations** menu.
8. Click **Save** to complete the integration.

- Click **Test**. **Integration Successful** message is displayed if the credential and address are valid.

## Capabilities

### 1. Activate User

Action capability for activating an inactive user account.

- Rollback: Yes
- Duplicate Control: Yes

The following table presents the **Activate User** action capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Rollback Mode</b>	Time to rollback this action. Default is no-rollback.	N/A	N/A	No
<b>Username</b>	Username to be added to group.	Username Email Address	Yes	Yes

#### Output:

Case Scope: N/A

Human Readable Output: N/A

### 2. Add User into Group

Action capability for adding user account into a group.

- Rollback: Yes
- Duplicate Control: Yes

The following table presents the **Add User into Group** action capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Rollback Mode</b>	Time to rollback this action. Default is no-rollback.	N/A	N/A	No
<b>Username</b>	Username to be added to group.	Username Email Address	Yes	Yes
<b>Group</b>	Name of the group.	String	No	Yes

#### Output:

Case Scope: N/A

Human Readable Output: N/A

### 3. Clear User Session

Action capability for clearing user's active sessions.

- Rollback: No
- Duplicate Control: No

The following table presents the **Clear User Session** action capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Username</b>	User whose sessions will be cleared.	Username Email Address	Yes	Yes

#### Output:

Case Scope: N/A

Human Readable Output: N/A

### 4. Deactivate User

Action capability for deactivating a user account.

- Rollback: Yes
- Duplicate Control: Yes

The following table presents the **Deactivate User** action capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Rollback Mode</b>	Time to rollback this action. Default is no-rollback.	N/A	N/A	No
<b>Username</b>	Username to be deactivated.	Username Email Address	Yes	Yes

#### Output:

Case Scope: N/A

Human Readable Output: N/A

### 5. Expire Password

Action capability for expiring user's password.

- Rollback: No
- Duplicate Control: No

The following table presents the **Expire Password** action capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Username</b>	User whose password will be set expired.	Username Email Address	Yes	Yes

**Output:**

Case Scope: N/A

Human Readable Output: N/A

**6. Get Groups Members**

Enrichment capability for retrieving list of users belong to a group.

The following table presents the **Get Groups Members** action capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Integration</b>	Name of the third party integration.	Integration	N/A	Yes
<b>Group</b>	Group name to be queried for group memberships.	String	No	Yes

**Output:**

Case Scope

Action	Type	Category/ Value
<b>Add</b>	Scope Item	Username [Related]

**Human Readable Output:**

Login	Email	Status	Id	Last Updated
john.wood@example.com	john.wood@example.com	ACTIVE	00u21zxw78hplQIZ65d7	2021-09-30T01:24:16.000Z
neil.young@example.com	neil.young@example.com	ACTIVE	00u22001rx4asNNnh5d7	2021-09-30T01:08:36.000Z
martin.sagan@example.com	martin.sagan@example.com	ACTIVE	00u646b0WrYzSfry5d6	2021-03-24T12:22:14.000Z

**7. Get Groups for User**

Enrichment capability for retrieving list of groups which user is member of.

The following table presents the **Get Groups for User** enrichment capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Integration</b>	Name of the third party integration.	Integration	N/A	Yes
<b>User</b>	User to be queried for group memberships.	Username Email Address	Yes	Yes

**Output:**

Case Scope:

Action	Type	Category/ Value
<b>None</b>	N/A	N/A

Human Readable Output:

<b>Id</b>	<b>Display Name</b>	<b>Status</b>	<b>Registered</b>	<b>Created</b>	<b>Last Updated</b>
guo26deyy0uP UOQep697	Iphone	ACTIVE	TRUE	2022-09-12T05:13:39.00 0Z	2022-09-12T08:53:24.00 0Z
guo26dura5ey5 3Fmr697	Nokia 6.1 Plus	SUSPENDED	TRUE	2022-09-12T07:33:13.00 0Z	2022-09-19T09:31:45.00 0Z

Total 2 , items / page

**8. Get User Details**

Enrichment capability for retrieving user account details.

The following table presents the **Get User Details** enrichment capability details:**Output:**

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Integration</b>	Name of the third party integration.	Integration	N/A	Yes
<b>User</b>	User to be queried.	Username Email Address	Yes	Yes

Case Scope

Action	Type	Category/ Value
<b>None</b>	N/A	N/A

Human Readable Output:

Key	Value
Full Name	John Wood
Login	john.wood@example.com
Email	john.wood@example.com
Mobile	
ID	00u21zxw78hpIQz65d7
Status	ACTIVE
Last Login	
Created	2021-09-30T01:09:17.000Z
Last Updated	2021-09-30T01:24:16.000Z

## 9. Get User Logs

Enrichment capability for retrieving log records for user account.

The following table presents the **Get User Logs** enrichment capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
<b>Integration</b>	Name of the third party integration.	Integration	N/A	Yes
<b>User</b>	User to be queried.	Username Email Address	Yes	Yes

### Output:

Case Scope:

Action	Type	Category/ Value
<b>None</b>	N/A	N/A

### Human Readable Output:

Date	Severity	Event Type	Actor	Log
2021-09-30T01:09:17.409Z	INFO	user.lifecycle.create	martin.northcutt@example.com (User)	{"severity": "INFO", "request": { "ipChain": [ { "ip": "49.189.232.112", "source": null, "geographicalContext": { "country": "Australia", "city": "Lindfield", "postalCode": "2070", "state": "New South Wales", "geolocation": { "lon": 151.1619, "lat": -33.7834 } }, "version": "V4" } ], "authenticationContext": { "externalSessionId": "102Hr4nSmW9SxyNT21DerAqA", "interface": null, "authenticationStep": 0, "issuer": null, "credentialType": null, "authenticationProvider": null, "credentialProvider": null }, "eventType": "user.lifecycle.create", "published": "2021-09-30T01:09:17.409Z" }}

## 10. List Groups

Enrichment capability for retrieving list of user groups.

The following table presents the **List Groups** enrichment capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Integration</b>	Name of the third party integration.	Integration	N/A	Yes

**Output:**

Case Scope:

Action	Type	Category/ Value
<b>None</b>	N/A	N/A

Human Readable Output:

Group Name	Description	Type	Id	Last Membership Updated
Administrators	Administrators	OKTA_GROUP	00g2201onBzv6Db575d7	2021-09-30T01:20:13.000Z
Development	Dev Team	OKTA_GROUP	00g64fj3mUjZ2OrCz5d6	2021-09-30T01:18:33.000Z
Everyone	All users in your organization	BUILT_IN	00g64bb6JhNDw9Uy5d6	2021-09-30T01:11:05.000Z
Quarantine	Quarantined Users	OKTA_GROUP	00g64boyh2R2bPvHE5d6	2021-05-04T15:22:13.000Z
Test	Test and QA Team	OKTA_GROUP	00g64g49r27DoJaE05d6	2021-09-30T01:19:00.000Z

**11. Remove User from Group**

Action capability for removing user account from a group.

- Rollback: Yes
- Duplicate Control: Yes

The following table presents the **Remove User from Group** enrichment capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Rollback Mode</b>	Time to rollback this action. Default is no-rollback.	N/A	N/A	No
<b>User</b>	User to be queried.	Username Email Address	Yes	Yes
<b>Group</b>	Name of the group	String	No	Yes

**Output:**

Case Scope: N/A

Human Readable Output: N/A

**12. Reset Password**

Action capability for resetting user's password. A password reset mail is sent to user by Okta.

- Rollback: No
- Duplicate Control: No

The following table presents the **Reset Password** action capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Username</b>	User whose password will be reset	Username Email Address	Yes	Yes

**Output:**

Case Scope: N/A

Human Readable Output: N/A

**13. Set Temporary Password**

Action capability for expiring user's password. This capability sets **tempPassword** value of the user as **true**.

- Rollback: No
- Duplicate Control: No

The following table presents the **Set Temporary Password** enrichment capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Username</b>	User whose password will be expired and "tempPassword" will be set to "True".	Username Email Address	Yes	Yes

**Output:**

Case Scope: N/A

Human Readable Output: N/A

**14. Suspend User**

Action capability for suspending user account.

- Rollback: Yes
- Duplicate Control: Yes

The following table presents the **Suspend User** enrichment capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Rollback Mode</b>	Time to rollback this action. Default is no-rollback.	N/A	N/A	No
<b>Username</b>	User account to be suspended.	Username Email Address	Yes	Yes

**Output:**

Case Scope: N/A

Human Readable Output: N/A

## 15. **Unlock User**

Action capability for unlocking user account.

- Rollback: No
- Duplicate Control: No

The following table presents the **Unlock User** enrichment capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Username</b>	User account to be unlocked.	Username Email Address	Yes	Yes

### **Output:**

Case Scope: N/A

Human Readable Output: N/A

## 16. **Unsuspended User**

Action capability for unsuspending user account.

- Rollback: Yes
- Duplicate Control: Yes

The following table presents the **Unlock User** enrichment capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Rollback Mode</b>	Time to rollback this action. Default is no-rollback.	N/A	N/A	No
<b>Username</b>	User account to be suspended.	Username Email Address	Yes	Yes

### **Output:**

Case Scope: N/A

Human Readable Output: N/A

## 17. **List Devices**

Action capability for listing devices.

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Integration</b>	Name of the third party integration.	Integration	N/A	Yes
<b>Status</b>	Status from the following options: ALL, CREATED, ACTIVE, SUSPENDED, DEACTIVATED OR DELETED	String	No	No
<b>Last Updated From</b>	Starting date to filter the device's last updated date. It can be absolute (format yyyy-mm-dd HH:MM:SS) or relative (ex: 1d, 2h, 3m)	String	No	No
<b>Last Updated To</b>	Starting date to filter the device's last updated date. It can be absolute (format yyyy-mm-dd HH:MM:SS) or relative (ex: 1d, 2h, 3m)	String	No	No

Output:

Case Scope: N/A

Human Readable Output:

ID	Display Name	Status	Registered	Created	Last Updated
guo26deyy0uP UOQep697	Iphone	ACTIVE	TRUE	2022-09-12T05:13:39.00 0Z	2022-09-12T08:53:24.00 0Z
guo26dura5ey5 3Fmr697	Nokia 6.1 Plus	SUSPENDED	TRUE	2022-09-12T07:33:13.00 0Z	2022-09-19T09:31:45.00 0Z

Total 2 , items / page

## 18. Get Device Details

Action capability to get device details.

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Integration</b>	Name of the third party integration.	Integration	N/A	Yes
<b>Device</b>	Device ID or display name	Computer Name, Host, keyword, Unknown	Yes	Yes

Output:

Case Scope:

Type/Role	Category/Property	Value
Scope Item Property	Okta Device ID	Device ID found in Okta.

Human Readable Output:

Field	Value
Id	guo26deyy0uPUOQep697
Status	ACTIVE
Created	2022-09-12T05:13:39.000Z
Last Updated	2022-09-12T08:53:24.000Z
Resource Type	UDDevice
Resource ID	guo26deyy0uPUOQep697
Display Name	Iphone
Platform	IOS
Registered	true
Secure Hardware Present	true

## 19. Suspend Device

Action capability to suspend user.

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Rollback Mode</b>	Time to rollback this action. Default is no-rollback.	N/A	N/A	No
<b>Device</b>	Display name or Device ID of the device to suspend	Computer Name, Host, Keyword, Unknown	Yes	Yes

Output:

Case Scope: N/A

## 20. Unsuspend Device

Action capability to unsuspend the user.

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Rollback Mode</b>	Time to rollback this action. Default is no-rollback.	N/A	N/A	No
<b>Device</b>	Display name or Device ID of the device to unsuspend	Computer Name, Host, Keyword, Unknown	Yes	Yes

**Output:**

Case Scope: N/A

# Integration Guide for Ones BioAffix

## Integration Overview

Ones BioAffix is a biometric single sign on (Biometric SSO) and biometric identity verification solution which lets organizations to manage their physical security and access. This integration has been tested with Ones BioAffix 4.20.10.1 version.

## Integration Capabilities

ArcSight SOAR has the following integration capability with Ones BioAffix:

- Change User Status (Block & Unblock)
- User Details (Info & Logs)

### Use Case: Blocking Suspicious Employees

Integrated with Ones BioAffix ATAR lets users to investigate suspicious employee traffic through building and block access if needed. This can be performed automatically within a playbook or manually by an analyst.

## Configuration

### Prerequisites

- SOAR connects to Ones BioAffix API via HTTPS. Typically it runs on 8443/tcp\* port. So access to this service is required.
- Credentials of administrator is required for SOAR to connect Ones BioAffix.

### Configuration on Ones BioAffix

- No specific configuration is needed on Ones BioAffix server.

### Configuring SOAR

1. Navigate **Configuration > Credentials** and click **Create Credential**.
2. Fill the Credential Editor form as follows:
  - a. **Internal Credential:**

**Type:** Internal credential.

**Name:** Display name of credential set (i.e., Ones BioAffix Credentials)

**Username:** Administrator username you have on Ones BioAffix.

**Password:** Password for the administrator user you have on Ones BioAffix.

**Private Key:** Empty.

**b. Credential Store:**

**Type:** External credential.

**Name:** Name of the credential with pull path of the safe on store.

3. Navigate to **Configuration > Integrations** and click **Create Integration**.

4. Fill the configuration form as follows:

**Name:** Display name of Ones BioAffix integration on ATAR.

**Type:** Ones BioAffix Server.

**Address:** Address of the integration (the format should be <https://192.168.12.77:8443>).

**Credential:** Name of the credential set you've just created on step 2. (i.e., Ones BioAffix Credentials).

**Trust Invalid SSL Certificates:** Select this if Engine's certificate is self-signed or not recognized by browsers.

**Require Approval From:** Select user(s) from list to ask her/his approval before executing actions on this integration.

**Notify:** Select user(s) from the list to notify when ATAR performs an action on this integration.

5. Click the **Test** button.

6. Click **Save** to complete integration.

## Additional Notes

Due to API behaviour of Ones BioAffix integration, “Date of Birth”, “Phone” and “Profile Photo” of users should be set to execute actions.

# Integration Guide for OpenText Network Detection and Response

## Integration Overview

OpenText NDR gives you access to all of your metadata and PCAPs. Your rapid threat investigation is enabled by an intuitive user interface along with workflows, visualization, analytics, and reports. The result is a single, powerful platform that efficiently and effectively protects enterprise network environments in real-time.

## Integration Capabilities

ArcSight SOAR has the following integration capabilities with Opentext Network Detection and Response :

- List Alerts
- Get Alert Details
- Get SmartPcap
- List Meta Data Activity

## Prerequisites

You must have access to HTTPS as the ArcSight SOAR connects to Opentext NDR NDR API through this service.

## Configuration

### Configuring Opentext Network Detection and Response

1. Authentication:Opentext NDR APIs use an access token to make authorized calls to the API. Opentext NDR REST APIs provide access to resources via URI paths. The token must be used in every REST API call for the tenant.

Authentication Parameters

Request Body:

Parameters	Datatype	Description	Required
Bearer	string	The Bicata REST API v1 access token	Yes

## 2. Additional Configuration:

Configuration Parameter	Description
proxy.id	Proxy device to be used while communicating with the remote system's API
cache.reusing.duration	Default cache-reuse parameter



In the Address configuration, replace the server name with your server name or address.

# Configuring SOAR

1. Click Configuration > Credentials > Create Credentials.
  2. Specify the following parameters values in the Credential Editor form.
- | Type                | Name   | Username              | Password              | Private Key |
|---------------------|--|-----------------------|-----------------------|-------------|
| Internal credential | Display name of credential set (for example, Netskope v1 Credentials). | Opentext NDR Username | Opentext NDR password | N/A         |
3. Click Configuration > Integrations > Upload plugin
  4. Select your integration plugin zip file and click on Save.
  5. Select the integration that you have added to Integrations menu.
  6. Click Save to complete the integration
  7. Click Test, an Integration Successful message is displayed if the credential and address are valid.

# Capabilities

## 1. List Alerts

Enrichment capability to get the list of Alerts.

Input Parameters:

Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
Source IP Address	Source IP Address	["NETWORK_ADDRESS"]	Yes	Yes
Time Range	Time Range	String	No	Yes

Output:

Case Scope:

N/A

Human Readable Output:

The screenshot shows a log viewer interface with the following details:

- Timestamp:** a few seconds ago - 2023-08-08T12:01:12.612799Z
- Event:** A admin executed List Alerts enrichment on Bricata CMC
- Alert Data:**

Timestamp	Src Ip	Src Port	Dest Ip	Dest Port	Severity	Signature	Uuid
2023-08-08T12:01:12.612799Z	162.241.149.195	443	10.2.8.101	49736	1	ET PHISHING Lets Encrypt Free SSL Cert Observed with IDN/Punycode Domain - Possible Phishing	62fc8543-4b88-8eac-5c9b-ac459d591628
2023-08-07T12:01:12.558817Z	162.241.149.195	443	10.2.8.101	49736	1	ET PHISHING Lets Encrypt Free SSL Cert Observed with IDN/Punycode Domain - Possible	4f48c1dd-4053-91ecfea1-703499bac9fa

## 2. Get Alert Details

Enrichment capability for Getting a single alert

Input Parameters:

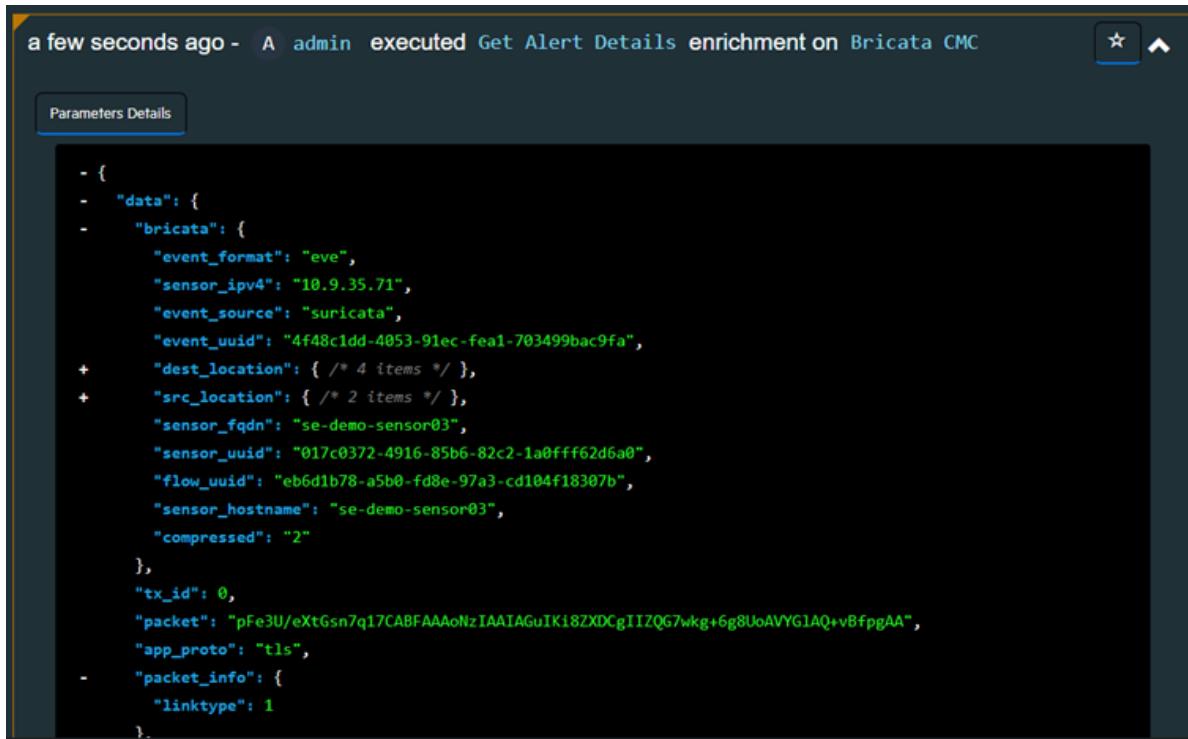
Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
uuid	Alert UUID	["KEYWORD"]	Yes	Yes

Output:

Case Scope:

N/A

Human Readable Output:



```

a few seconds ago - A admin executed Get Alert Details enrichment on Bricata CMC

Parameters Details

{
  "data": {
    "bricata": {
      "event_format": "eve",
      "sensor_ipv4": "10.9.35.71",
      "event_source": "suricata",
      "event_uuid": "4f48c1dd-4053-91ec-fea1-703499bac9fa",
      "dest_location": { /* 4 items */ },
      "src_location": { /* 2 items */ },
      "sensor_fqdn": "se-demo-sensor03",
      "sensor_uuid": "017c0372-4916-85b6-82c2-1a0fff62d6a0",
      "flow_uuid": "eb6d1b78-a5b0-fd8e-97a3-cd104f18307b",
      "sensor_hostname": "se-demo-sensor03",
      "compressed": "2"
    },
    "tx_id": 0,
    "packet": "pFe3U/eXtGsn7q17CABFAAAoNzIAAIAGuIKi8ZxDCgIIZQG7wkg+6g8UoAVYG1AQ+vBfpqAA",
    "app_proto": "tls",
    "packet_info": {
      "linktype": 1
    }
  }
}

```

### 3. Get SmartPcap

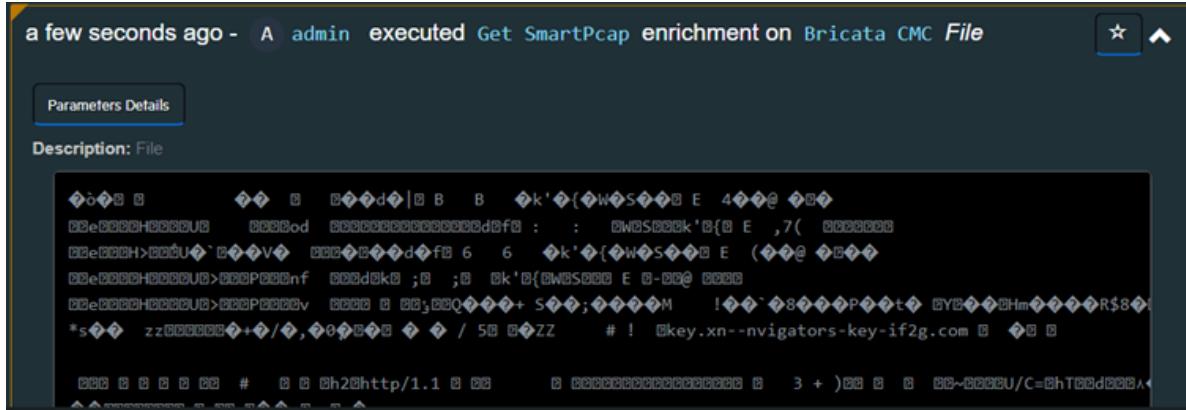
Input Parameters:

Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
uuid	Alert UUID	["KEYWORD"]	Yes	Yes

Output:

Case Scope:

Human Readable Output:



#### 4. Get Meta Data Activity

##### Input Parameter

Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
Hunt By Source IP Address	Source IP Address	["NETWORK_ADDRESS"]	Yes	No
Hunt By Destination IP Address	Destination IP Address	["NETWORK_ADDRESS"]	Yes	No
Time Range	Time Range	String	No	Yes

##### Human Readable Output:

a few seconds ago - S Swarna Dash executed List Metadata Activity enrichment on OPENTEXT\_NDR

Parameters Details

Search

Timestamp Src Ip Src Port Dest Ip Dest Port Event Uuid Service Pcr Orig Bytes Resp Bytes Sensor Hostname

Timestamp	Src Ip	Src Port	Dest Ip	Dest Port	Event Uuid	Service	Pcr	Orig Bytes	Resp Bytes	Sensor Hostname
2024-01-18T08:39:40.19+00:00	10.1.21.101	50465	193.239.84.250	443	c5501d0a-4712-9536-4c8f-39591f2f9894	ssl	0.381844	1451	761	se-demo-sensor03
2024-01-18T08:39:38.71+00:00	10.1.21.101	50464	193.239.84.250	443	56314c35-4ecf-87ae-dbac-4d1fc4d4d09	ssl	-0.290186	1541	2206	se-demo-sensor03
2024-01-18T08:39:38.72+00:00	10.1.21.101	50463	193.239.84.250	443	a7b8fee9-4f70-b885-7d92-ecd6a390b8f0	ssl	0.374635	1395	761	se-demo-sensor03

# Integration Guide for Palo Alto Networks AutoFocus

## Integration Overview

Palo Alto Networks AutoFocus is a threat intelligence platform which allows to search attack indicators and access to details of them. AutoFocus provides the intelligence, analytics, and context required to understand which attacks require immediate response and take decisive action to prevent future attacks.

## Integration Capabilities

ArcSight SOAR has the following integration capabilities with Palo Alto Networks AutoFocus:

- Search Email Address
- Search File Hash
- Search File Name
- Search IP Address
- Search URL

### Use Case: Investigating Phishing Campaigns

SOAR integrates with Palo Alto Networks AutoFocus to search attack indicators. SOAR can follow email inboxes for user's phishing reports and automatically creates an incident record on its service desk. During the investigation of the attack SOAR can extract the sender address, IP address, files in the attachment and ask these indicators to Palo Alto Networks AutoFocus if this is a known attack and previously analyzed. This can be performed automatically within a playbook or manually by an analyst.

## Configuration

### Prerequisites

- SOAR connects to Palo Alto Networks AutoFocus API via HTTPS. Access (<https://autofocus.paloaltonetworks.com> (443/tcp port) is required.
- An API key is required for SOAR to connect Palo Alto Networks AutoFocus.

## Configuration on Palo Alto Networks AutoFocus

No specific configuration is needed. Login to <https://autofocus.paloaltonetworks.com> and note the API key under **Settings > General** menu.

## Configuring SOAR

1. Navigate **Configuration > Credentials** and click **Create Credential**.

2. Fill the Credential Editor form as follows:

**a. Internal Credential:**

**Type:** Internal credential.

**Name:** Display name of credential set (i.e., PAN AutoFocus Credential).

**Username:** Empty.

**Password:** API Key.

**Private Key:** Empty.

**b. Credential Store:**

**Type:** External Credential.

**Name:** Name of the credential with pull path of the safe on store.

3. Navigate **Configuration > Integrations** and click **Create Integration**.

4. Fill the configuration form as follows:

**Name:** Display name of Palo Alto Networks AutoFocus integration on SOAR.

**Type:** Palo Alto Networks AutoFocus.

**Address:** Address of the integration (<https://autofocus.paloaltonetworks.com>).

**Credential:** Name of the credential set you've just created on step 2. (i.e., PAN AutoFocus Credential).

**Configuration:** You need to specify the following configuration parameters

```
# Integration ID of the proxy integration to use when connecting to  
# current integration.  
# If not provided, SOAR will try to use a direct connection.  
#proxy.id=123  
# configure how far (in minutes) into the past this enrichment will look.  
# cache.reusing.duration=20
```

**Trust Invalid SSL Certificates:** Select this if Engine's certificate is self-signed or not recognized by browsers.

**Require Approval From:** Select user(s) from list to ask approval before executing actions on this integration.

**Notify:** Select user(s) from the list to notify when SOAR performs an action on this integration.

5. The **EnrichmentFixedDelay** configuration parameter value must be set to less than 120 seconds because of AutoFocus' requirement. Otherwise AutoFocus API cookie will be expired.
6. Click the **Test** button.
7. Click **Save** to complete integration.

## Integration Guide for Palo Alto Networks Firewall

### Integration Overview

Palo Alto Networks Next Generation Firewall is a security technology that combines firewall, antivirus, intrusion prevention, and virtual private network (VPN) capabilities to provide proactive threat defense that stops attacks before they spread through the network. This integration has been tested with Palo Alto Networks NGFW 9.0.1 version.

### Integration Capabilities

ArcSight SOAR has the following integration capabilities with Palo Alto Firewall (API):

- Block IP
- Block Host
- Block URL
- Disconnect

#### Use Case: Blocking access to malicious IP addresses and hosts

Integrated with Palo Alto Networks NGFW, SOAR blocks malicious IP addresses and hosts on perimeter while responding cyber-attacks. Blocking can be performed automatically within a playbook or manually by an analyst.

# Configuration

## Prerequisites

- SOAR connects to Palo Alto Networks NGFW API via HTTPS. Access to 443/tcp port is required.
- An API key is required for SOAR to connect Palo Alto Networks Firewall.

## Configuration on Palo Alto Networks Firewall (API)

1. Navigate Device menu and create a new Admin Role for SOAR. New role must be restricted to only specific XML API operations. Only required permissions are: "Configuration", "Operational Requests" and "Commit".
2. Do not forget to disable all Web UI and Command Line permissions since they are unnecessary.
3. Create an Administrator account with SOAR API Role you have created in first step.
4. Navigate to Objects > Address Groups and add an address group for IPs to be populated by SOAR actions.
5. Similarly add an address group for hosts/FQDNs to be populated by SOAR.
6. Navigate **Objects > Custom** Objects and add a Custom URL Category to be populated by SOAR.
7. Commit all changes.
8. To obtain API key run the following request from command line.

```
curl -k -X GET 'https://PaloAlto_NGFW_IP/api/?type=keygen& \
user=atarapi&password=password'
```

## Configuring SOAR

1. Navigate **Configuration > Credentials** and click **Create Credential**.
2. Fill the Credential Editor form as follows:

### a. Internal Credential:

**Type:** Internal credential.

**Name:** Display name of credential set (i.e., Palo Alto Firewall Credential).

**Username:** User you have created for SOAR on Palo Alto NGFW.

**Password:** Password of the user you have created for SOAR on Palo Alto NGFW.

**Private Key:** API Key you have created for SOAR.

**b. Credential Store:**

**Type:** External credential.

**Name:** Name of the credential with full path of the safe on store.

3. Navigate **Configuration > Integrations** and click **Create Integration**.

4. Fill the configuration form as follows:

**Name:** Display name of Palo Alto Networks Firewall integration on SOAR.

**Type:** Palo Alto Networks Firewall (API)

**Address:** Address of the integration (the format should be https://192.168.2.78).

**Credential:** Name of the credential set you've just created on step 2. (i.e., Palo Alto Firewall Credential).

**Trust Invalid SSL Certificates:** Select this if web UI's certificate is self-signed or not recognized by browsers.

**Configuration:** You need to specify the following configuration parameters.

```
# Address group to use when blocking IP addresses.  
# This address group should be created in Palo Alto device before use.  
addressgroup.ip=ATAR_BLOCK_IP  
# Address group to use when blocking host names.  
# This address group should be created in Palo Alto device before use.  
addressgroup.host=ATAR_BLOCK_HOST  
# Custom URL category to use when blocking URLs.  
# This custom URL category should be created in Palo Alto device before  
use.  
custom.url.category=ATAR_BLOCK_URL
```

**Require Approval From:** Select user(s) from list to ask her/his approval before executing actions on this integration.

**Notify:** Select user(s) from the list to notify when SOAR performs an action on this integration.

5. Click on the Test button.

6. Click **Save** to complete integration.

## Additional Notes

Palo Alto Networks NGFW integration supports multiple “vsys”. If your firewall has more than one “vsys” SOAR will ask you to choose one while taking action.

# Integration Guide for Palo Alto Networks Panorama

## Integration Overview

The Panorama management server provides centralized monitoring and management of multiple Palo Alto Networks next-generation firewalls and of WildFire appliances and appliance clusters. This integration has been tested with Palo Alto Network Panorama 8.1.0 version.

## Integration Capabilities

ArcSight SOAR has the following integration capabilities with Palo Alto Networks Panorama:

- Block IP address
- Block Host
- Block URL

### **Use Case: Blocking malicious IP addresses on multiple firewall appliances**

With this integration, SOAR can block malicious IP addresses, hosts and URL addresses on multiple firewall devices simultaneously while responding cyber-attacks. This can be performed automatically within a playbook or manually by an analyst.

## Configuration

### Prerequisites

- SOAR connects to Palo Alto Networks Panorama API using HTTPS. Access to 443/tcp port is required.
- An API key is required for SOAR to connect Palo Alto Networks Panorama.
- If users want to use multiple devicegroup, they should write devicegroup names comma separated, for ex: Ankara, Istanbul, Izmir

### Configuration on Palo Alto Networks Panorama

1. Navigate to **Panorama** menu and create a new Admin Role for SOAR. The new role should be

restricted to only specific XML API operations. Only required permissions are: "Configuration", "Operational Requests" and "Commit". Do not forget to disable all Web UI and Command Line permissions since they are unnecessary.

2. Create an Administrator account with **Custom Panorama Admin** type and SOAR API Role you have created in first step.
3. Commit all changes.
4. In order to obtain API key run the following request from command line.

```
curl -k -X GET 'https://Panorama_IP/api/?type=keygen& \
user=atarapi&password=password'
```

## Configuration on SOAR

1. Navigate **Configuration > Credentials** and click **Create Credential**.
2. Fill the Credential Editor form as follows:

**a. Internal Credential:**

**Type:** Internal credential.

**Name:** Display name of credential set (i.e., PAN Panorama Credential).

**Username:** Empty.

**Password:** Empty.

**Private Key:** API Key you have created for SOAR.

**b. Credential Store:**

**Type:** External credential.

**Name:** Name of the credential with pull path of the safe on store.

3. Navigate **Configuration > Integrations** and click **Create Integration**.

4. Fill the configuration form as follows:

**Name:** Display name of Palo Alto Networks Panorama integration on SOAR.

**Type:** Palo Alto Networks Panorama.

**Address:** Address of the integration (<https://10.0.2.254>).

**Credential:** Name of the credential set you've just created on step 2. (i.e., PAN Panorama Credential).

**Trust Invalid SSL Certificates:** Select this if Engine's certificate is self-signed or not recognized by browsers.

**Configuration:** You need to specify the following configuration parameters.

```
# Device group to use when adding and address object.  
# This device group should be created in Palo Alto device before use.  
# If users want to use multiple devicegroups, they should write  
devicegroup  
# names comma separated, for ex: Ankara, Istanbul, Izmir  
devicegroup.name=HeadQuarters  
# Address group to use when blocking IP addresses.  
# This address group should be created in Palo Alto device before use.  
addressgroup.ip=ATAR_BLOCK_IP  
# Address group to use when blocking host names.  
# This address group should be created in Palo Alto device before use.  
addressgroup.host=ATAR_BLOCK_HOST  
# Custom URL category to use when blocking URLs.  
# This custom URL category should be created in Palo Alto device before  
use.  
custom.url.category=ATAR_BLOCK_URL
```

**Require Approval From:** Select user(s) from list to ask her/his approval before executing actions on this integration.

**Notify:** Select user(s) from the list to notify when SOAR performs an action on this integration.

5. Click the **Test** button.
6. Click **Save** to complete integration.

## Integration Guide for Qualys VM

### Integration Overview

Qualys, Inc. is a pioneer and leading provider of cloud-based security and compliance solutions. The Qualys Cloud Platform and its integrated apps help businesses simplify security operations and lower the cost of compliance by delivering critical security intelligence on demand and automating the full spectrum of auditing, compliance, and protection for IT systems and web applications.

### Integration Capabilities

ArcSight SOAR has the following integration capabilities with Qualys VM:

- List Scans
- List Reports

- Download Report
- Get Host Details
- Start Scan
- Scan Status
- Get Vulnerability Report
- Get Compliance Report

## Prerequisites

You must have access to HTTPS as the ArcSight SOAR connects to Qualys VM API through this service.

## Configuration

### Configuring Qualys VM

1. Authentication: Integration requires an address, username, and password to connect and authenticate to Qualys APIs.

Follow these basic steps to generate a username and password, to access the Qualys VM Rest API:

- a. To create a Qualys account, perform the following steps:
  - i. Go to Qualys and click on Try it free. You can also use the Qualys credentials provided by your organisation.
  - ii. Fill out the form with all the required information and click on “Sign up”
  - iii. An email will be sent to you from Qualys with a link and username with an OTP.
  - iv. Follow the instructions in your email to set up your account.
  - v. On the final page, you will see “Address”, and “Password”.
- b. You should save address, username, and password somewhere securely.

#### Authentication Parameters

1. Request Headers:

Parameter	Data type	Description	Required
Username	String	Username of the user.	Yes
Password	String	Password of user account	Yes

## 2. Additional Configuration:

Configuration Parameter	Description
proxy.id	Proxy device to be used while communicating with the remote system's API.
Cache.reusing.duration	Default cache-reuse parameter

# Configuring SOAR

1. Click Configuration > Credentials > Create Credentials.
2. Specify the following parameter values in the Credential Editor form.

Type	Name	Username	Password	Private Key
Internal credential	Display name of credential set (for example, Qualys VM Credentials).	The username to your Qualys VM account	The password to your Qualys VM account	N/A

3. Select your integration plugin zip file and click on Save.
4. Select the integration that you have added to the Integrations menu.
5. Click Save to complete the integration.
6. Click Test, and an Integration Successful message is displayed if the credential and address are valid.

# Integration Capabilities:

## 1. List Scans

Enrichment capability to list vulnerability scans in the user's account. By default the XML output lists scans launched in the past 30 days.

Request Headers:

Username	Password
String	String

Input Parameters:

Path Parameter	Description	Type	Scope restricted (Yes/No)	Required (Yes/No)
Time Range	Fetch the scan details the specified datetime range.	Datetime Range	No	Yes
IP Address	Filter the scan details based on IP address provided	NETWORK_ADDRESS, KEYWORD, UNKNOWN	Yes	Yes

Default Input Parameter:

Query Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
action [Default=fetch]	Action value Fetch. To fetch the report	String	No	No
show_args [Default: True]	To show all the arguments in the response	Bool	No	No
show_status	Shows the status of scan result	Bool	No	No

Output:

Case Scope: N/A

Human Readable Output:

Reference Number	Title	Launch Date	Status	Target
scan/1687502576.49298	Act Sca	2023-06-23T06:42:56Z	Finished	49.205.219.95
scan/1687502420.49295	new_scan12	2023-06-23T06:40:20Z	Finished	49.205.219.95
scan/1687501920.49279	Act Sca	2023-06-23T06:32:00Z	Finished	49.205.219.95
scan/1687433736.47795	*****	2023-06-22T11:35:36Z	Finished	49.205.219.95
scan/1687433525.47790	*****	2023-06-22T11:32:05Z	Finished	49.205.219.95
scan/1687433361.47782	MY test scan	2023-06-22T11:29:21Z	Finished	49.205.219.95
scan/1687350267.45790	new_scan_12345612	2023-06-21T12:24:27Z	Finished	49.205.219.95
scan/1687350083.45782	Act Sca	2023-06-21T12:21:23Z	Finished	49.205.219.95
scan/1687335678.45324	sacn_12345	2023-06-21T08:21:18Z	Finished	49.205.219.95
scan/1687332556.45220	vuln1234	2023-06-21T07:29:16Z	Finished	49.205.219.95
scan/1687250063.43173	Act Sca	2023-06-20T08:34:23Z	Finished	49.205.219.95
scan/1687170464.41270	test qa scan	2023-06-19T10:27:44Z	Finished	49.205.219.95

## 2. List Reports

Enrichment capability to View a list of reports in the user's account when Report Share feature is enabled. The report list output includes all report types, including scorecard reports.

Request Headers:

Username	Password
String	String

**Input Parameters:**

Path Parameter	Description	Type	Scope restricted (Yes/No)	Required (Yes/No)
Report Type	The type of report to filter [All, Scorecard, Remediation, Authentication, Scan, Compliance, Patch, Map, Asset search]	Array of string	No	Yes

**Default Parameters:**

Path Parameter	Description	Type	Scope restricted (Yes/No)	Required (Yes/No)
action [Default=fetch]	Action value Fetch. To fetch the report	String	No	No

**Output:**

Case Scope : N/A

**Human Readable Output:**

Report Id	Title	Type	Output Format	Size	Status	Launch Datetime	Expiration Datetime
5416249	\$%^&*((	Scan	PDF	48.14 KB	Finished	2023-06-22T13:47:53Z	2023-06-29T13:47:54Z
5416235	4567890	Scan	DOCX	143.48 KB	Finished	2023-06-22T13:40:01Z	2023-06-29T13:40:02Z
5416209	vul_scan_rep	Scan	DOCX	50.3 KB	Finished	2023-06-22T13:21:05Z	2023-06-29T13:21:07Z
5416207	Patch_Rep_Te st1	Patch	XML	4.52 KB	Finished	2023-06-22T13:14:04Z	2023-06-29T13:14:06Z
5416195	Comp_Report1	Compliance	HTML	277.08 KB	Finished	2023-06-22T13:09:27Z	2023-06-29T13:09:28Z
5416059	My vuln report1	Scan	PDF	48.06 KB	Finished	2023-06-22T11:52:36Z	2023-06-29T11:52:37Z
5415291	new_patch_rep	Patch	XML	4.52 KB	Finished	2023-06-	2023-06-

**3. Download report**

Enrichment capability to Download a saved report in the user's account. You can download all report types (map, scan, patch, authentication, scorecard, remediation, compliance). This option is available when the Report Share feature is enabled in the user's subscription.

## Request Headers:

Username	Password
String	String

## Input Parameters:

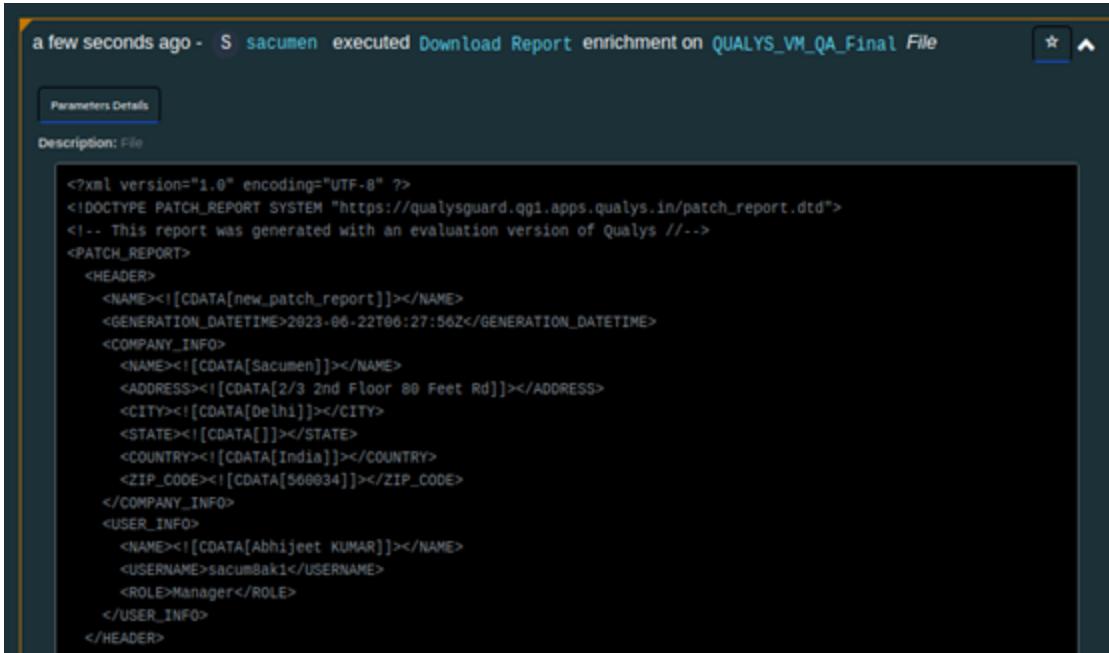
Path Parameter	Description	Type	Scope restricted (Yes/No)	Required (Yes/No)
Report name	Specifies the report name of a saved report that you want to download. The status of the report must be "finished".	String	No	Yes

## Output:

## Case Scope:

Action	Type	Category/ Value
Automatically Set	Scope Item Property	Hash Algorithm
Automatically Set	Scope Item Property	Hash Algorithm
Automatically Set	Scope Item Property	File Name
Automatically Set	Scope Item Property	File Name with Attachment

## Human Readable Output:



a few seconds ago - S sacumen executed Download Report enrichment on `QUALYS_VMS_QA_Final File`

Parameters Details

Description: File

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE PATCH_REPORT SYSTEM "https://qualysguard.cgi.apps.qualys.in/patch_report.dtd">
<!-- This report was generated with an evaluation version of Qualys -->
<PATCH_REPORT>
  <HEADER>
    <NAME><![CDATA[new_patch_report]]></NAME>
    <GENERATION_DATETIME>2023-06-22T06:27:56Z</GENERATION_DATETIME>
    <COMPANY_INFO>
      <NAME><![CDATA[sacumen]]></NAME>
      <ADDRESS><![CDATA[2/3 2nd Floor 80 Feet Rd]]></ADDRESS>
      <CITY><![CDATA[Delhi]]></CITY>
      <STATE><![CDATA[]]></STATE>
      <COUNTRY><![CDATA[India]]></COUNTRY>
      <ZIP_CODE><![CDATA[560034]]></ZIP_CODE>
    </COMPANY_INFO>
    <USER_INFO>
      <NAME><![CDATA[Abhijeet KUMAR]]></NAME>
      <USERNAME>sacum8aki</USERNAME>
      <ROLE>Manager</ROLE>
    </USER_INFO>
  </HEADER>
```

The screenshot shows a software interface for managing scope items. At the top, there is a navigation bar with a 'Filter' dropdown set to 'All' and a 'Add New Scope Item' button. Below the navigation bar is a grid of six small cards representing scope items. To the right of the grid is a larger panel displaying detailed information about a selected item. The detailed information includes:

- Source:** Download Report
- Role:** Related
- Other Roles:** Related
- File Name:** QUALYS\_VM\_QA\_Final//DOWNL0... 06-23 11:08:58 - (2023-06-23 11:08:58)
- Alerts:** Show alerts with this scope item

At the bottom of the interface, there is a footer bar with the text '6 scope items', a search icon, and a dropdown menu.

#### 4. Get host details

Enrichment capability to list of scanned hosts in the user's account. By default, all scanned hosts in the user account are included and basic information about each host is provided.

Request Headers:

Username	String
Password	String

Input Parameters:

Path Parameter	Description	Type	Scope restricted (Yes/No)	Required (Yes/No)
IP Address	The Address to get the host detail	NETWORK_ADDRESS, KEYWORD, UNKNOWN	Yes	Yes

Output:

Case Scope: N/A

**Human Readable Output:**

Key	Value
ID	11894671
IP Address	49.205.219.95
Tracking Method	IP
Last Vulnerability Scan Datetime	2023-06-22T11:36:50Z
Asset Group ID(s)	8974791,8974792
Asset Group Name(s)	TestGroup, Test Asset

Total 6 , items / page      1

**5. Start scan**

Enrichment capability to Launch vulnerability scan in the user's account.

Request Headers:

Username	Password
String	String

Input Parameters:

Path Parameter	Description	Type	Scope restricted (Yes/No)	Required (Yes/No)
Scan name	Name of the scan	String	No	Yes

Output:

Case Scope: N/A

**Human Readable Output:**

Parameters Details		Search
Key	Value	
Scan Name	final test qa scan	
ID	5449949	
Reference	scan/1687519665.49949	

100 ▾  
Total 3 , items / page 1

**6. Scan status**

Enrichment capability to check the status of scan initiated.

Request Headers:

Username	Password
String	String

Input Parameters:

Path Parameter	Description	Type	Scope restricted (Yes/No)	Required (Yes/No)
Scan Name	Name of the scan	String	No	Yes

Output:

Case Scope: N/A

Human Readable Output:

Parameters Details		Search
Key	Value	
Title	final test qa scan	
Launch Datetime	2023-06-23T11:32:24Z	
State	Finished	

100 ▾  
Total 3 , items / page 1

## 7. Get vulnerability report

Enrichment capability to Launch a vulnerability report in the user's account. The Report Share feature must be enabled in the user's subscription.

Request Headers:

Username	Password
String	String

Input Parameters:

Path Parameter	Description	Type	Scope restricted (Yes/No)	Required (Yes/No)
Template Name	Name of the template you want to use for your report.	String	No	Yes
Report Title	A user-defined report title. The title may have a maximum of 128 characters. For a PCI compliance report, the report title is provided by Qualys and cannot be changed.	String	No	Yes
Output Format	One output format may be specified. Supported formats for various reports are below scan report: pdf, html (a zip file), mht, xml, csv, or docx	Array of string	No	Yes
IP Address	Specify IPs/ranges to change (overwrite) the report target, as defined in the report template	NETWORK_ADDRESS, KEYWORD, UNKNOWN	Yes	Yes

Output:

Case Scope:

Action	Type	Category/ Value
Automatically Set	Scope Item Property	Hash Algorithm
Automatically Set	Scope Item Property	Hash Algorithm
Automatically Set	Scope Item Property	File Name
Automatically Set	Scope Item Property	File Name with Attachment

Human Readable Output:

a few seconds ago - S sacramen executed Get Vulnerability Report enrichment on QUALYS\_VM\_QA\_Final File

Description: File

```
%PDF-1.7
%>
7 0 obj
<</Subtype/Image/Width 166/Height 43/Mask[0 0]/BitsPerComponent 8/ColorSpace 5 0 R/Filter/FlateDecode/Length 8 0 R>
stream
x666oooo 60m076oooooooo6oooo
endstream
endobj
8 0 obj
30
endobj
6 0 obj
<</Length 9 0 R/Filter/FlateDecode>>
stream
x666?oooo6o0
endstream
endobj
9 0 obj
14
endobj
10 0 obj
endstream/Transparency 0/Height 22/BitsPerComponent 8/ColorSpace/Name/Length 11 0 R>
```

Filter: All ▾

Add New Scope Item

QUALYS_VM_...	CEBBF29DE18...	7ADEFEC230A...
File - 2023-06-2...	192.128.1.20	790A863E7982...
File - 2023-06-2...	QUALYS_VM_...	DD67E00DC3F...
File - 2023-06-2...	QUALYS_VM_...	BA0F5E01000A...
220590297F64...	10173662A2DD...	QUALYS_VM_...
	00014F3CD6D...	

QUALYS\_VM\_QA\_Final//GET\_VULNERABILITY\_REPORT  
-06-23 12:40:33

Source	Get Vulnerability Report
Role	Related
Other Roles	Related
File Name	QUALYS_VM_QA_Final//GET_VUI 06-23 12:40:33) - (2023-06-23 12:40:33)
Alerts	Show alerts with this scope item

19 scope items

Search

1 ▾ →

## 8. Get compliance report

Enrichment capability to Launch a Compliance report in the user's account. The Report Share feature must be enabled in the user's subscription.

**Request Headers:**

Username	Password
String	String

**Input Parameter:**

Path Parameter	Description	Type	Scope restricted (Yes/No)	Required (Yes/No)
Template Name	Name of the template you want to use for your report.	String	No	Yes
Report Title	A user-defined report title. The title may have a maximum of 128 characters. For a PCI compliance report, the report title is provided by Qualys and cannot be changed.	String	No	Yes
Output Format	One output format may be specified. Supported formats for various reports are below scan report: pdf, html (a zip file), mht, xml, csv, or docx	Array of string	No	Yes
IP Address	Specify IPs/ranges to change (overwrite) the report target, as defined in the report template	NETWORK_ADDRESS, KEYWORD, UNKNOWN	Yes	Yes

**Output:****Case Scope:**

Action	Type	Category/ Value
Automatically Set	Scope Item Property	Hash Algorithm
Automatically Set	Scope Item Property	Hash Algorithm
Automatically Set	Scope Item Property	File Name
Automatically Set	Scope Item Property	File Name with Attachment

**Human Readable Output:**

## 9. Get patch report

Enrichment capability to Launch a patch report in the user's account. The Report Share feature must be enabled in the user's subscription.

## Request Headers:

Username	Password
String	String

Input Parameter:

Path Parameter	Description	Type	Scope restricted (Yes/No)	Required (Yes/No)
Template Name	Name of the template you want to use for your report.	String	No	Yes
Report Title	A user-defined report title. The title may have a maximum of 128 characters. For a PCI compliance report, the report title is provided by Qualys and cannot be changed.	String	No	Yes
Output Format	One output format may be specified. Supported formats for various reports are below scan report: pdf, html (a zip file), mht, xml, csv, or docx	Array of string	No	Yes
IP Address	Specify IPs/ranges to change (overwrite) the report target, as defined in the report template	NETWORK_ADDRESS, KEYWORD, UNKNOWN	Yes	Yes

Output:

Case Scope:

Action	Type	Category/ Value
Automatically Set	Scope Item Property	Hash Algorithm
Automatically Set	Scope Item Property	Hash Algorithm
Automatically Set	Scope Item Property	File Name
Automatically Set	Scope Item Property	File Name with Attachment

Human Readable Output:

a few seconds ago - S sacumen executed Get Patch Report enrichment on QUALYS\_VM\_QA\_Final File

**Parameters Details**

Description: File

```
"asdfghj","06/23/2023 at 13:04:48 (GMT+0000)"
"Qualumen","2/3 2nd Floor 80 Feet Rd",,"Delhi",,"India",,"560034"
"Abhijeet KUMAR","sacumbaki",,"Manager"

Report Summary
Title, Asset Groups, IPs, Asset Tags, Group By, Created on
"asdfghj","","49.205.219.95","","Host","06/23/2023"

Patch Summary
Total Patches, Hosts Requiring Patches, Total Vulnerabilities Addressed
"1","1","3"

Host List
IP, DNS, NetBIOS, OS, Patch Count
"49.205.219.95","broadband.actcorp.in",,"1"

Patches by Host
IP, QID, Vendor ID, Severity, Title, Vulnerability Count, Published
49.205.219.95,"730616","sophos-sa-20220923-sfos-rce","4","Sophos Firewall Remote Code Execution (RCE) Vulnerability (sophos-sa-20220923-sfos-rce) - (49.205.219.95, 730616, 4, Practice, Sophos Firewall Remote Code Execution (RCE) Vulnerability (sophos-sa-20220923-sfos-rce))"

Host Vulnerabilities Fixed by Patch
IP, Patch QID, QID, Severity, Type, Title, Instance, Normalized Instance, Last Detected
49.205.219.95,"730616","730616","4","Practice","Sophos Firewall Remote Code Execution (RCE) Vulnerability (sophos-sa-20220923-sfos-rce) - (49.205.219.95, 730616, 4, Practice, Sophos Firewall Remote Code Execution (RCE) Vulnerability (sophos-sa-20220923-sfos-rce))"
```

**Filter:** All + Add New Scope Item

# 0A3EBC4631E...	# B4F1262A6675...	QUALYS_VM_...	
File - 2023-06-2...	File - 2023-06-2...	File - 2023-06-2...	
# 2658F8A5995F...	# 9613CDE0D79...	QUALYS_VM_...	
# CEBBF29DE18...	# 7ADEFEC230A...	File - 2023-06-2...	
192.128.1.20	# 790A863E7982...	File - 2023-06-2...	

QUALYS\_VM\_QA\_Final//GET\_PATCH\_REPORT.result(2023-06-23 13:04:56) (File)

**Source** Get Patch Report

**Role** Related

**Other Roles** Related

**File Name** QUALYS\_VM\_QA\_Final//GET\_PATCH\_REPORT.result(2023-06-23 13:04:56) - (2023-06-23 13:04:56)

**Alerts** Show alerts with this scope item

27 scope items Q 1 ▾ →

# Integration Guide for Recorded Future

## Integration Overview

Recorded Future is a threat intelligence service which collects and analyzes vast amounts of data to deliver relevant cyber threat insights in real time.

## Integration Capabilities

ArcSight SOAR has the following integration capabilities with Recorded Future:

- Lookup Domain
- Lookup Hash
- Lookup IP Address
- Lookup URL
- Lookup Vulnerability
- Search Entity Lists
- Search Malware

### Use Case: Investigating Phishing Campaigns

SOAR is integrated with Recorded Future, to help investigation and mitigation of phishing campaigns. When a phishing report email comes from user, SOAR extracts the indicators such as IP address, URLs and attachments in message and a new incident is created on SOAR's own Incident Management Service Desk. SOAR then asks these indicators to Recorded Future if this is a known attack and previously analyzed. This can be performed automatically within a playbook or manually by an analyst.

## Configuration

### Prerequisites

- SOAR connects to Recorded Future API via HTTPS. Access to <https://api.recordedfuture.com/v2/> (443/tcp port) is required.
- An API key is required for SOAR to connect Recorded Future service.

## Configuration on Recorded Future

Login to <https://api.recordedfuture.com/v2/> and create a new API key under user Settings > API Access menu and note the API Key and API Password generated. This token is required by SOAR to access the platform for queries.

## Configuring SOAR

1. Navigate **Configuration > Credentials** and click **Create Credential**.
2. Fill the Credential Editor form as follows:

### a. Internal Credential:

**Type:** Internal credential.

**Name:** Display name of credential set (i.e., Recorded Future Credentials).

**Username:** API Key you have created on Recorded Future.

**Password:** API Password for the key you have created on Recorded Future.

**Private Key:** Empty.

### b. Credential Store:

**Type:** External credential.

**Name:** Name of the credential with full path of the safe on store.

3. Navigate **Configuration > Integrations** and click **Create Integration**.

4. Fill the configuration form as follows:

**Name:** Display name of Recorded Future integration on SOAR.

**Type:** Recorded Future.

**Address:** Address of the integration (<https://api.recordedfuture.com/v2/>).

**Configuration:** You need to specify the following configuration parameters.

```
# Integration ID of the proxy integration to use when connecting to
# current integration.
# If not provided, SOAR will try to use a direct connection.
#proxy.id=123
# configure how far (in minutes) into the past this enrichment will look.
#cache.reusing.duration=20
```

**Credential:** Name of the credential set you've just created on step 2. (i.e., Recorded Future Credentials)

**Trust Invalid SSL Certificates:** No need to select.

**Require Approval From:** Select user(s) from list to ask her/his approval before executing actions on this integration. Since SOAR only executes enrichments on Recorded Future, leave it empty.

**Notify:** Select user(s) from the list to notify when SOAR performs an action on this integration. Since SOAR only executes enrichments on Recorded Future, leave it empty.

5. Click on the **Test** button.
6. Click **Save** to complete integration.

# Integration Guide for Robtex Lookup

## 1. Integration Overview

Robtex is used for various kinds of research of IP numbers, domain names, etc.

Robtex uses various sources to gather public information about IP numbers, domain names, host names, Autonomous systems, routes, etc. It indexes the data in a big database and provide free access for the data

## 2. Integration Capabilities

Action

Lookup

## Configuration

### Configuration on Robtex Lookup

SOAR connects to Robtex Lookup integrations via HTTPS. Therefore ATAR should be able to connect this service.

### Configuring SOAR

1. While creating this integration via Integrations tab of Configuration menu:

**Name:** Display name of Robtex lookup integration on SOAR.

**Type:** Robtex lookup.

**Address:** Address of the integration (the address should be <https://www.robtex.com>).

**Configuration:** You need to specify the following configuration parameters

```
# Integration ID of the proxy integration to use when connecting to
# current integration.
# If not provided, ATAR will try to use a direct connection.
#proxy.id=123
# configure how far (in minutes) into the past this enrichment will look.
#cache.reusing.duration=20
```

**Credential:** Name of the credential set.

**Trust Invalid SSL Certificates:** Select this if Engine's certificate is self-signed or not recognized by browsers.

**Require Approval From:** Select user(s) from list to ask her/his approval before executing actions on this integration.

**Notify:** Select user(s) from the list to notify when ATAR performs an action on this integration.

2. Click the **Test** button.
3. Click **Save** to complete integration.

# Integration Guide for Roksit DNS Firewall

## Integration Overview

Roksit DNS Firewall is cloud-based cybersecurity service which provides web security and application control by analyzing DNS traffic.

## Integration Capabilities

ArcSight SOAR has the following integration capability with Roksit DNS Firewall:

- Block hostname

### Use Case: Blocking malicious hosts on DNS

With this integration, SOAR can block malicious hostnames on Roksit DNS Firewall service while responding cyber-attacks. This can be performed automatically within a playbook or manually by an analyst.

## Configuration

### Prerequisites

- SOAR connects to Roksit DNS Firewall API via HTTPS. So access to <https://api.roksit.com> (443/tcp port) is required.
- An API key is required to be created for SOAR to connect to Roksit DNS Firewall. Please contact to service provider.

### Configuration on Roksit DNS Firewall

- No further configuration is needed.

### Configuring SOAR

1. Navigate to **Configuration > Credentials** and click **Create Credential**.
2. Fill the Credential Editor form as follows:
  - a. **Internal Credential:**  
**Type:** Internal credential.

**Name:** Display name of credential set (i.e., Roksit DNS FW Credentials).

**Username:** Empty.

**Password:** API Key you have obtained from Roksit.

**Private Key:** Empty.

**b. Credential Store:**

**Type:** External credential.

**Name:** Name of the credential with full path of the safe on store.

3. **Navigate to Configuration > Integrations and click Create Integration.**

4. Fill the configuration form as follows:

**Name:** Display name of Roksit DNS Firewall integration on SOAR

**Type:** Roksit DNS Firewall

**Address:** Address of the integration (address should be <https://api.roksit.com>).

**Credential:** Name of the credential set you've just created on step 2. (i.e., Roksit DNS FW Credentials)

**Trust Invalid SSL Certificates:** Select this if Engine's certificate is self-signed or not recognized by browsers.

**Require Approval From:** Select user(s) from list to ask her/his approval before executing actions on this integration.

**Notify:** Select user(s) from the list to notify when SOAR performs an action on this integration.

5. Click **Save** to complete integration.

6. Click **Test** to test the integration.

## Additional Notes

- Roksit DNS Firewall integration on SOAR is defined as Advanced Action Script and content of the default script is accessible under **Configuration > Customization Library**.
- While defining the integration first time, you get a warning message as follows. For this type of integration this is the expected behaviour.

# Integration Guide for RSA Security Analytics

## Integration Overview

RSA Security Analytics provides real-time visibility into network traffic with full packet capture—on premises, in the cloud and across virtual infrastructure. It helps to detect threats as they traverse in the network, monitor the timing and movement of attackers across the network and reconstruct entire network sessions to support forensic investigations. This integration has been tested with RSA Security Analytics 11.0.0.0 version.

## Integration Capabilities

ArcSight SOAR has the following integration capabilities with RSA Security Analytics:

- Network Packet Capture (Time range)
- Network Packet Capture (Relative time)

### **Use Case: Investigating suspicious cases using packet captures**

SOAR integrates with RSA Security Analytics to collect full packet capture for a given timeframe. During the investigation of an incident, SOAR can gather packet-capture from RSA Security Analytics with specified parameters such as offender IP, affected usernames, suspicious end-user machines, etc and put the related pcap file into incident timeline for further analysis and keeping evidence purposes. Collecting pcap files can be performed automatically within a playbook or manually by an analyst.

## Configuration

### Prerequisites

- SOAR connects to RSA Security Analytics Network Concentrator's API via HTTP/HTTPS.
- By default API interface works on 50105/tcp port. So access permission to this port is required.
- A user account is required to be created for SOAR to connect to RSA Security Analytics Network Concentrator API.

## Configuration on RSA Security Analytics Suite

1. Login to Security Analytics Suite and navigate to **ADMIN > Services** and then select **Concentrator** service and open up **Security** View by clicking **Actions** icon.
2. Add a new Role to be used for SOAR user. New role should have at least “sdk.content”, “sdk.manage” and “sdk.meta” permissions”.
3. Add a new user with the role you have created in previous step.

## Configuring SOAR

1. Navigate **Configuration > Credentials** and click **Create Credential**.

2. Fill the Credential Editor form as follows:

**a. Internal Credential:**

**Type:** Internal credential.

**Name:** Display name of credential set (i.e., RSA Security Analytics Credential).

**Username:** Username you have created for SOAR on RSA Security Analytics Suite.

**Password:** Password of the user you have created for SOAR on RSA Security Analytics Suite.

**Private Key:** Empty.

**b. Credential Store:**

**Type:** External credential.

**Name:** Name of the credential with pull path of the safe on store.

3. Navigate **Configuration > Integrations** and click **Create Integration**.

4. Fill the configuration form as follows:

**Name:** Display name of RSA Security Analytics integration on SOAR.

**Type:** RSA Security.

**Address:** Address of the integration (the format should be `http[s]://192.168.1.10:50105` or `http[s]://abc.example.com:50105`).

**Credential:** Name of the credential set you've just created on step 2. (i.e., RSA Security Analytics Credential)

**Trust Invalid SSL Certificates:** Select this if device's certificate is self-signed or not recognized by browsers.

**Require Approval From:** Select user(s) from list to ask her/his approval before executing actions on this integration.

**Notify:** Select user(s) from the list to notify when SOAR performs an action on this integration.

5. Click the **Test** button.
6. Click **Save** to complete integration.

## Integration Guide for SailPoint

### Integration Overview

SailPoint's Identity Security product provides a comprehensive platform for managing and governing accounts, roles, and entitlements across applications, systems, data, and cloud services. It enables organizations to identify risks, monitor behaviors, and refine roles, while providing visibility into access across the entire organization.

### Integration Capabilities

ArcSight SOAR has the following integration capabilities with SailPoint:

- Disable Account
- Enable Account
- Get Account Activity
- Get Account Details
- Get Account Entitlements
- Get Account IDs

### Configuration

### Configuring on SailPoint

- SailPoint requires a **Client ID** and **Client Secret** with the ORG\_ADMIN role for access.
- Users with the ORG\_ADMIN role can create a **Client ID** and **Client secret** from [https://{{tenant\\_name}}.api.identitynow.com](https://{{tenant_name}}.api.identitynow.com) after logging in with valid credentials.

# Configuring SOAR

1. Click **Configuration > Credential > Create Credential**.
2. Specify the following parameter values in the **Credential Editor**:

Type	Name	Username	Password	Private Key
Internal Credential	Display name of credential set ( for example, SailPoint Credentials).	Empty	Client ID	Client Secret

3. Click **Configuration > Integrations > Create Integration**.
4. Specify the following parameter values in the **Configuration Form**:

Parameter	Value
Name	Display name of SailPoint integration on SOAR
Type	Advanced Scriptable Device
Address	https://{tenant_name}.api.identitynow.com
Configuration	<p>Specify the following configuration parameter values:</p> <pre># Integration ID of the proxy integration to use when connecting to current integration. # If not provided, ArcSight SOAR will try to use a direct connection. #proxy.id=123</pre> <pre># Maximum number of results to return from the API. # If not provided, the integration will gather all results. #max.result.count = 100</pre>
Credential	Name of the credential set created in step 2. (i.e. SailPoint Credentials).
Trust Invalid SSL Certificates	Select this if Engine's certificate is self-signed or not recognized by browsers. Not selected.
Require Approval From	Select user(s) from list to ask their approval before executing enrichment on this integration.
Notify	Select user(s) from the list who can provide approval when SOAR performs an enrichment on this integration.

5. Click **Test**, an **Integration Successful** message is displayed if the credential and address are valid.
6. Click **Save**.

# Capabilities

## 1. Disable Account

Action capability for disabling an account.

The following table presents the **Disable Account** action capabilities details:

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
Account ID	ID of the account	Keyword, Unknown	Yes	Yes

### Output:

N/A

Human Readable Output

N/A

## 2. Enable Account

Action capability for enabling an account.

The following table presents the **Enable Account** action capabilities details:

Input Parameter	Description	Type	Scope Rescticted (Yes/No)	Required (Yes/No)
Account ID	ID of the account	Keyword, Unknown	Yes	Yes

### Output:

Case Scope

N/A

Human Readable Output

N/A

## 3. Get Account Activity

Enrichment capability for getting account activity.

The following table presents the **Get Account Activity** enrichment capabilities details:

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
Integration	Name of the third party integration	N/A	No	Yes
Username	Identity Username	Unknown, Username, Keyword	Yes	Yes

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
Time Range	Time range picker that filters activities by the time they were created	Relative or absolute time from time range picker	No	Yes
Type	Type of account activity	List option from drop down menu: All, Access Request, Account Attribute Update, Account State Update, Attribute Synchronization Refresh, Certification, Cloud Automated, Cloud Password Request, Identity Attribute Update, Identity Refresh, Lifecycle Change Refresh, Lifecycle State Change	No	Yes

**Output:**

Case Scope

N/A

Human Readable Output

Date	Type	Operation	Status	Details	Id
2022-10-05T16:26:32.518Z	AccountStateUpdate	ENABLE	PENDING	Requester Name: Target Name:	
2022-10-05T16:22:35.078Z	AccountStateUpdate	DISABLE	PENDING	Requester Name: Target Name:	
2022-10-04T19:31:52.745Z	AccountStateUpdate	ENABLE	PENDING	Requester Name: Target Name:	
2022-10-04T19:28:50.540Z	AccountStateUpdate	DISABLE	PENDING	Requester Name: Target Name:	
2022-09-29T18:36:23.130Z	AccountStateUpdate	ENABLE	PENDING	Requester Name: Target Name:	
2022-09-29T18:35:08.203Z	AccountStateUpdate	DISABLE	PENDING	Requester Name: Target Name:	

#### 4. Get Account Details

Enrichment capability for getting account details.

The following table presents the **Get Account Details** enrichment capabilities details:

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
Integration	Name of the third-party integration	N/A	No	Yes
Account ID	ID of the account	Unknown, Keyword	Yes	Yes

#### Output:

Case Scope

N/A

Human Readable Output

Field	Value
Name	[REDACTED]
Account ID	[REDACTED]
Created	[REDACTED]
Modified	[REDACTED]
Source Name	IDN Admin
Source ID	[REDACTED]
Identity ID	[REDACTED]
Attributes	displayName: [REDACTED] givenName: [REDACTED] phoneNumber: [REDACTED] familyName: [REDACTED] name: [REDACTED] id: [REDACTED] email: [REDACTED] idNowDescription: [REDACTED] [REDACTED] [REDACTED]
Native Identity	[REDACTED]
Authoritative	true
Disabled	false
Locked	false
System Account	false
Uncorrelated	false
Manually Correlated	false
Has Entitlements	false

## 5. Get Account Entitlements

Enrichment capability for getting account entitlements.

The following table presents the **Get Account Entitlements** enrichment capabilities details:

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
Integration	Name of the third party integration	N/A	No	Yes
Account ID	ID of the account	Unknown, Keyword	Yes	Yes

### Output:

Case Scope

N/A

## Human Readable Output

Entitlement	Description	Created	Modified	Privileged	Cloud Governed
ORG_ADMIN	Full administrative access to IdentityNow	2021-07-09T15:38:41.024Z	2022-09-28T20:38:13.501Z	false	false

## 6. Get Account IDs

Enrichment capability for getting account IDs.

The following table presents the **Get Account IDs** enrichment capabilities details:

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
Integration	Name of the third party integration	N/A	No	Yes
Username	Identity Username	Unknown, Username , Keyword	Yes	No

### Output:

Case Scope

Action	Type	Category/Value
Add	Keyword	Related/ Account ID(s)

## Human Readable Output

Id	Name	Created	Modified	Source Id	Source Name
[REDACTED]	[REDACTED]	2022-09-09T19:41:23.773Z	2022-09-09T19:41:23.848Z	[REDACTED]	IDN Admin
[REDACTED]	[REDACTED]	2022-09-09T19:41:24.473Z	2022-10-05T16:26:33.002Z	[REDACTED]	IdentityNow
[REDACTED]	N/A			[REDACTED]	

# Integration Guide for SentinelOne

## Overview of the Plugin

SentinelOne Singularity platform is an industry-first data lake that seamlessly fuses together the data, access, control, and integration planes of its endpoint protection (EPP), endpoint detection and response (EDR), IoT security, and cloud workload protection (CWPP) into a centralized platform. With Singularity, organizations gain access to back-end data across the

organization through a single solution, providing a cohesive view of their network and assets by adding a real time, autonomous security layer across all enterprise assets.

## Integration Capabilities

ArcSight SOAR has the following integration capabilities with SentinelOne:

- Disconnect from Network
- Connect to Network
- Get Agent Status/ Get Endpoint Details
- List Installed Applications
- List Events for Endpoint
- List Groups
- Get Group Details
- Get Hash Reputation
- Move Agent to Group
- Add to Blacklist
- Delete from Blacklist
- Get Blacklist
- List Threats
- Get Threat Details
- Update Threat
- Add to Exclusion List
- Remove from Exclusion List
- Scan (Full Disk Scan)

## Prerequisites

You must have access to HTTPS as ArcSight SOAR connects to SentinelOneAPI through this service.

## Configuration

### Configuring SentinelOne

API requires Token authentication which can be extracted from dashboard.

1. Login to Dashboard <https://<instance url>/dashboard>.
2. Click Profile > get User > API Token Generation erate API extract > Regen.
3. Select Regenerate API Token and Extract the Token.



API Token is valid for 6 months, it needs to be regenerated every 6 months.

## Configuring SOAR

1. Click **Configuration > Credential > Create Credential**.
  2. Specify the following parameter values in the Credential Editor form:
- | Type                | Name   | Username | password | Private Key      |
|---------------------|--|----------|----------|------------------|
| Internal credential | Display name of credential set (for example, SentinelOne Credentials). | N/A      | N/A      | ApiToken {token} |
3. Click **Configuration > Integrations > Upload plugin**.
  4. Select your integration plugin zip file and click on save.
  5. Select the integration that you have added to Integrations menu.
  6. Click Save to complete the integration.
  7. Click Test, an Integration Successful message is displayed if the credential and address are valid.

## Integration Capabilities:

### 1. Disconnect from Network

Use this command to isolate (quarantine) endpoints from the network. The agent can communicate with the Management, which lets you analyze and mitigate threats.

- Rollback: Yes
- Duplicate Control: No

### Input Parameters

Parameter	Description	Type	Scope Restricted	Required
Computer Name/ IP Address	Valid Agent Computer Name or IP Address	COMPUTER NAME, NETWORK ADDRESS, KEYWORD, UNKNOWN	Yes	Yes

**Output:**

Case Scope: N/A

Human Readable Output: N/A

**2. Reconnect to Network**

After running the **Disconnect from network** on endpoints, analyze the issue, and mitigate threats. Use this command to reconnect to the network all the endpoints that match the filter.

- Rollback: No
- Duplicate Control: No

**Input Parameters**

Parameter	Description	Type	Scope Restricted	Required
Computer Name/ IP Address	Valid Agent Computer Name or IP Address	COMPUTER NAME, NETWORK ADDRESS, KEYWORD, UNKNOWN	Yes	Yes

**Output:**

Case Scope: N/A

Human Readable Output: N/A

**3. GetAgent Status/ Get Endpoint Detail**

Fetch the details of the Agent.

**Input Parameters**

Parameter	Description	Type	Scope Restricted	Required
Computer Name/ IP Address	Valid Agent Computer Name or IP Address	COMPUTER NAME, NETWORK ADDRESS, KEYWORD UNKNOWN	Yes	Yes

**Output:**

Case Scope: N/A

**Human Readable Output:**

Key	Value
Account ID	1504451660558924435
Account Name	Sacumen - A Division of Clarion Technologies Pvt. Ltd
ID	1591167481362742170
UUID	3764e16b-b32f-fee9-cb40-5e41b3a70c67
Group ID	1504451661020297887
Group Name	Default Group
Agent Version	22.3.3.11
Computer Name	Gauri-Inspiron-15-3511
Model Name	Dell Inc. Inspiron 15 3511
OS Arch	64 bit
OS Name	Linux
CPU Count	1
CPU ID	11th Gen Intel(R) Core(TM) i5-1135G7 @ 2.40GHz
Total Memory	15736
Created At	2023-01-05T09:25:45.008751Z
External IP	223.233.82.194
Firewall Enabled	true
Last Active Date	2023-03-02T10:31:35.291301Z
Last Logged In Username	N/A
License Key	N/A
Network Interfaces	[ { "inet": [ "192.168.1.8" ], "gatewayip": "192.168.1.1", "gatewayMacAddress": "

**4. List Installed Applications**

Get the installed applications for a specific Agent/Endpoint.

**Input Parameters**

Parameter	Description	Type	Scope Restricted	Required
Computer Name/ IP Address	Valid Agent Computer Name or IP Address	COMPUTER NAME, NETWORK ADDRESS KEYWORD UNKNOWN	Yes	Yes

**Output:**

Case Scope: N/A

## Human Readable Output:

Application Name	Version	Installed Date	Size	Publisher
manpages	5.10-1ubuntu1	2022-04-19T10:03:29Z	1709056	Ubuntu Developers &lt;ubuntu-devel-discuss@lists.ubuntu.com&gt;;
openssl	3.0.2-0ubuntu1.8	2023-02-08T07:25:20Z	2102272	Ubuntu Developers &lt;ubuntu-devel-discuss@lists.ubuntu.com&gt;;
xserver-common	2:21.1.3-2ubuntu2.7	2023-02-08T07:25:13Z	246784	Ubuntu X-SWAT &lt;ubuntu-x@lists.ubuntu.com&gt;;
xserver-xephyr	2:21.1.3-2ubuntu2.7	2023-02-08T07:25:23Z	2670592	Ubuntu X-SWAT &lt;ubuntu-x@lists.ubuntu.com&gt;;
xserver-xorg-core	2:21.1.3-2ubuntu2.7	2023-02-08T07:25:13Z	4060160	Ubuntu X-SWAT &lt;ubuntu-x@lists.ubuntu.com&gt;;
python3-pkg-resources	59.6.0-1.2ubuntu0.22.04.1	2023-01-24T04:47:55Z	593920	Ubuntu Developers &lt;ubuntu-devel-discuss@lists.ubuntu.com&gt;;
python3-setuptools	59.6.0-1.2ubuntu0.22.04.1	2023-01-24T04:47:55Z	1788928	Ubuntu Developers &lt;ubuntu-devel-discuss@lists.ubuntu.com&gt;;

## 5. List Events for Endpoints

Get Deep Visibility results from the query that matches the given event type. Valid values for Event Type are:

Because of some limitation with the SentinelOne account, only the "events" event type is supported.

### Input Parameters

Input Parameter	Description	Data type	Scope Restricted	Required
Event Type	The event type to query the event. Supported event type: events	string	No	Yes
Time Range	The time range to fetch the events	String	No	Yes

### Output:

Case Scope: N/A

**Human Readable Output:**

Event Id	Process Id	Process Name	Agent Os	Agent Ip	User	Dns Count	Endpoint Os	File Md5	File Sha256
7923823854 76927488	4492	chrome	linux	223.233.82.1 94	N/A	N/A	linux	N/A	N/A
7923823854 76927490	11038	python3.10	linux	223.233.82.1 94	N/A	N/A	linux	N/A	N/A
7923823854 76927489	11038	python3.10	linux	223.233.82.1 94	N/A	N/A	linux	N/A	N/A
7923823854 76927491	1053	dragent	linux	223.233.82.1 94	N/A	N/A	linux	N/A	N/A
7923823854 76927493	4492	chrome	linux	223.233.82.1 94	N/A	N/A	linux	N/A	N/A
7923823854 76927492	4492	chrome	linux	223.233.82.1 94	N/A	N/A	linux	N/A	N/A

**6. List Groups**

Get a list of groups with details of each group.

**Input Parameters:** N/A

**Default Parameters**

Parameter	Description	Type	Scope Restricted	Required
cursor	Cursor position returned by the last request. Use to iterate over more than 1000 items. Example: "YWdlbnRfaWQ6NTgwMjkzODE="	String	No	Yes
limit	Limit number of returned items (1-1000). Example: "10"	Integer	No	Yes

**Output:**

Case Scope: N/A

Human Readable Output:

ID	Name	Site Id	Creator Name	Created At	Updated At	Total Agents	Type
15044516610202 97887	Default Group	15044516610035 20670	SentinelOne	2022-09- 07T17:56:53.673 07Z	2023-03- 02T09:57:19.777 165Z	3	static
15440861588838 85778	Sacumen_test	15044516610035 20670	Naveen Kumar	2022-11- 01T10:23:34.005 541Z	2023-03- 02T09:57:19.777 165Z	N/A	static

## 7. Get Group Details

Get data of a given Group. To get a Group ID, run **groups**. This command responds with the ID of the Site of the Group, Group name, type (dynamic or static), and similar data. The username provided must have permission for the Site.

### Input Parameters

Parameter	Description	Type	Scope	Restricted	Required
Group Name	Valid group Name to fetch the details	String	No		Yes

### Output:

Case Scope: N/A

Human Readable Output

Key	Value
ID	1504451661020297887
Name	Default Group
Created At	2022-09-07T17:56:53.673077Z
Creator	SentinelOne
Creator ID	433241154985656401
Updated At	2023-03-02T09:57:19.777165Z
Description	N/A
Filter ID	N/A
IS Default	true
Rank	N/A
Registration Token	eyJ1cmwiOiAiaHR0cHM6Ly91c2VhMS1wYXJ0bmVycy5zZW50aW5lbG9uZS5uZXQilCAic2l0ZV9rZXkiOiAiZ19jOTFkNDJhNWFjNzA1Y2UyIn0=
Site ID	1504451661003520670
Type	static

## 8. Get Hash Reputation

Get the reputation of a hash, given the required SHA1. To get a hash, run **threats** (preferably filtered for a Group or Site) and take the file Content Hash value.

### Input Parameters

Parameter	Description	Scope		
		Data type	Restricted	Required
Hash Value	A valid hash value	String	Yes	Yes

### Output:

Case Scope

Action	Type	Category/ Value
Set	Scope Item Property	Hash Reputation Rank

Human Readable Output:

Key	Value
Rank	5

## 9. Move Agent to Group

Move Agents that match the filter to a group. To get the Group ID , run **groups** is required and there can be only one. This will move the matched agents that are on the same site as the given group.

- Rollback: No
- Duplicate Control: No

### Input Parameters

Parameter	Description	Type	Scope Restricted	Required
Group Name	Valid Group Name	String	No	Yes
Computer Name / IP Address	Valid Agent Computer Name	COMPUTER NAME, NETWORK ADDRESS, KEYWORD UNKNOWN	Yes	Yes

### Output:

Case Scope: N/A

Human Readable Output: N/A

## 10. Add to Blacklist

Action capability to add threats that have a SHA1 hash and that match the filter to the Blacklist of the target scope: Global, Account, Site, or Group.

- Rollback: Yes
- Duplicate Control: Yes

### Input Parameters

Parameter	Description	Type	Scope Restricted	Required
Hash Value	Sha1 Hash Value	string	Yes	Yes
Os Type	Os Type enum = [ “linux”, “windows”, “macos”, “windows_legacy” ]	Array[String]	No	Yes

**Default parameters:**

Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
accountId	Get unique Account id from configuration file.	Array [strings]	No	Yes
type	Select Blacklist type as black hash (This would be default option in blacklist type)	string	No	Yes

**Output:**

Case Scope: N/A

Human Readable Output: N/A

**11. Delete from Blacklist**

Action capability to delete the threat from the blacklist.

- Rollback: No
- Duplicate Control: Yes

**Input Parameters**

Parameter	Description	Type	Scope Restricted	Required
Hash Value	Hash Value of the threat	String	Yes	Yes

**Default parameters**

Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
type	Select Blacklist type as black hash (This would be default option in type)	string	No	Yes

**Output:**

Case Scope: N/A

Human Readable Output: N/A

## 12. Get Blacklist

Enrichment capability to get a list of all the items in the blacklist.

Input Parameters: N/A

### Default Parameters

			Scope		
Parameter	Description	Type	Restricted	Required	
cursor	Cursor position returned by the last request. Used to iterate over more than 1000 items. Example: "YWdlbnRfaWQ6NTgwMjkzODE="	String	No	No	
limit	Limit number of returned item (1-1000) Example: "10"	Integer	No	No	

### Output:

Case Scope: N/A

Human Readable Output:

ID	Sha1 Value	Created At	Updated At	Description	Os Type	Account IDs	Type
16194246536421 07653	21881eb8f5b885 b835ffcf8b37d1df e9f48029ea	2023-02- 13T09:07:42.441 252Z	2023-02- 13T09:07:42.439 323Z	Threat Name: view.exe File Name:/home/dee pak/snap/notepa d-plus- plus/common/.wi ne/drive_c/windo ws/syswow64/vie w.exe Threat ID: 16163603738829 66708	linux	[ "1504451660558 924435"]	black_hash
16194246543467 50734	9cbe5534dddb49 9d9184b70d37c1 37c48199c924	2023-02- 13T09:07:42.524 956Z	2023-02- 13T09:07:42.522 789Z	Threat Name: winefile.exe File Name:/home/dee pak/snap/notepa d-plus- plus/common/.wi ne/drive_c/windo ws/syswow64/wi nfile.exe Threat ID: 16163585484966 99720	linux	[ "1504451660558 924435"]	black_hash

## 13. List Threats

Get data of threats.

Input Parameters: N/A

### Default Parameters

Parameter	Description	Type	Scope Restricted	Required
cursor	Cursor position returned by the last request. Use to iterate over more than 1000 items. Example: "YWdlbnRfaWQ6NTgwMjkzODE="	String	No	Yes
limit	Limit the number of returned items (1-1000). Example: "10"	Integer	No	Yes

**Output:**

Case Scope: N/A

Human Readable Output:

ID	Name	Classification	Created At	Identified At	Updated At	Sha1	Mitigation Status	File Size	File Path
1594088535 204088378	eicar.com	Malware	2023-01-09T10:09:21.	2023-01-09T10:09:21. 761467Z	2023-02-22T07:30:05. 594349Z	3395856ce81 f2b7382dee7 2602f798b64 2f14140	mitigated	68	/home/praveen/Downloads/eicar_com/eicar.com
1594089981 936979189	eicar_com.zip	Malware	2023-01-09T10:12:14.	2023-01-09T10:12:14. 226077Z	2023-02-14T04:13:03. 083637Z	d27265074c9 eac2e2122ed 69294dbc4d7 cce9141	mitigated	184	/home/praveen/Downloads/eicar_com.zip
1594107440 526065684	eicar_com (2).zip	Malware	2023-01-09T10:46:55.	2023-01-09T10:46:55. 452182Z	2023-02-13T06:22:07. 190918Z	d27265074c9 eac2e2122ed 69294dbc4d7 cce9141	mitigated	184	/home/praveen/Downloads/eicar_com (2).zip

**14. Get a threat's timeline.**

Input Parameters

Parameter	Description	Type	Scope Restricted	Required
Thread Id	Valid Threat ID	String	No	True

**Output**

Case Scope: N/A

**Human Readable Output:**

Key	Value
Threat ID	1594088535204088378
Threat Name	eicar.com
Threat Classification	Malware
Threat Classification Source	Static
Created At	2023-01-09T10:09:21.761467Z
Updated At	2023-02-22T07:30:05.525940Z
Computer Name	hunters
Confidence Level	malicious
File Path	/home/praveen/Downloads/eicar_com/eicar.com
File Size	68
Site ID	1504451661003520670
Site Name	Default site
Reboot Required	false
Sha1	3395856ce81f2b7382dee72602798b642f14140
Whitening Options	[ "path", "hash" ]
Group Name	Sacumen_test
Account ID	1504451660558924435
Account Name	Sacumen - A Division of Clarion Technologies Pvt. Ltd
Agent OS Name	Linux

**15. Update Threat**

Update the incident details of a threat.

- Rollback: No
- Duplicate Control: No

**Input Parameters**

Parameter	Description	Type	Scope Restricted	Required
Thread Id	Valid Threat ID	String	No	Yes
Status	Incident Status Example: "resolved" enum =[ "unresolved", "in_progress", "resolved" ]	string	No	Yes

**Output:**

Case Scope: N/A

Human Readable Output: N/A

## 16. Add to Exclusion List

Action capability to create exclusion to make your agents suppress alerts and mitigation for items that you consider to be benign or which you require for interoperability.

- Rollback: Yes
- Duplicate Control: Yes

### Input Parameters

Parameter	Description	Type	Scope Restricted	Required
Hash Value	Valid Hash value	string	Yes	Yes
OS Type	Agent OS type enum =[ “linux”, “macos”, “windows”, “windows_legacy”] ]	string	No	Yes

### Default parameters:

Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
accountId	Get unique Account id from configuration file.	Array [strings]	No	No
type	Select Exclusion type as white hash (This would be default option in exclusion type)	string	No	Yes

### Output:

Case Scope: N/A

Human Readable Output: N/A

## 17. Remove from Exclusion List

Every Exclusion opens a possible security hole. If it is decided that an Exclusion (or multiple Exclusions) is not required, use this command to delete it.

- Rollback: No
- Duplicate Control: Yes

### Input Parameters

Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
Parameter	Description	Type	Scope Restricted	Required
Hash Value	Hash value of the exclusion.	string	Yes	Yes

**Default parameters:**

Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
type	Select Exclusion type as white hash (This would be default option in exclusion type)	string	No	Yes

**Output:**

Case Scope: N/A

Human Readable Output: N/A

**18. Scan**

Command to run a Full Disk Scan on Agents that match the filter.

Full Disk Scan finds dormant suspicious activity, threats, and compliance violations that are then mitigated according to the policy. It scans the local file system. Full Disk Scan does not inspect drives that require user credentials (such as network drives) or external drives.

Full Disk Scan does not work on hashes. It does not check each file against the blacklist.

If the Static AI determines that a file is suspicious, the Agent calculates its hash and sees if the hash is in the blacklist. If a file is executed, all aspects of the process are inspected, including hash-based analysis and blacklist checks.

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

- Rollback: No
- Duplicate Control: No

**Input Parameters**

Parameter	Description	Type	Scope Restricted	Required
Computer Name/ IP Address	Valid Agent Computer Name or IP Address	COMPUTER NAME, NETWORK ADDRESS, KEYWORD UNKNOWN	Yes	True

**Output:**

Case Scope: N/A

Human Readable Output: N/A

# Integration Guide for ServiceNow

## Integration Overview

ServiceNow allows you to manage digital workflows for enterprise operations.

## Integration Capabilities

ArcSight SOAR has the following integration capabilities with ServiceNow:

- Close Incident
- Create Incident
- Update Incident

## Prerequisites

You must have access to HTTPS as the ArcSight SOAR connects to ServiceNow API through this service.

## Configuring ServiceNow

1. Create a REST client on SOAR
  - a. Login to SOAR platform.
  - b. Navigate **Configurations > REST CLIENTS**.
  - c. Create a new **REST client** by providing a description.

 You must take a note of your **Client ID** and **Client Secret** as they would be used as username and password during configuring authentication later.
2. **Create a User**
  - a. Login to **ServiceNow** platform.
  - b. Navigate to **User Administration > User**.
  - c. Click **New** to create a new user and specify the required credentials. Note: This username and password is used during the ArcSight SOAR configuration.
  - d. Navigate to **User Administration > User** and edit the user you created newly to assign an admin role.

### 3. Create Rest Messages

- a. Navigate to **System Web Services > Outbound > REST Message**.
- b. Click **New** to create message and specify the following details in the form:

Form Fields	Values
Name	SOAR REST API Requests
Description	SOAR REST API Requests
Endpoint	<itom_host_url>/soar-api/api/v1
<b>Authentication tab</b>	
Authentication type	Basic
Basic Auth Profile	soar credential

- c. Click the Lookup icon to setup Basic Authentication.
  - d. Click **New** and specify the following parameters:
- | Form Fields | Values        |
|-------------|---------------|
| Username    | Client ID     |
| Password    | Client secret |
- e. Click **Submit** and select the newly created **Basic auth profile**.
  - f. Navigate to **System Web Services > Outbound > REST Message** and select **SOAR REST API Requests**.

g. Click **New** and create following HTTP Methods within REST Messages:

i. **Update Case on SOAR Method**

Form Fields	Values
Rest Message	SOAR REST API Requests
Name	Update Case on SOAR
HTTP Method	Patch
Endpoint	<item_host_url>/soar-api/api/v1/case/\${serialId}
<b>Authentication Tab</b>	
Authentication type	Basic
Basic Auth Profile	SOAR default_profile
<b>HTTP Request Tab</b>	
<b>HTTP Headers Section</b>	
Name	Value
Content-Type	application/json
<b>HTTP Query Parameters Section</b>	
Content	\${changes}

Specify the following details and click **Submit**:

ii. **Add Comment to SOAR Case**

Specify the following details and click **Submit**:

Form Fields	Values
Rest Message	SOAR REST API Requests
Name	Add Comment to the SOAR Case
HTTP Method	Post
Endpoint	<item_host_url>/soar-api/api/v1/case-comment
<b>Authentication Tab</b>	
Authentication type	Basic
Basic Auth profile	SOAR default_profile
<b>HTTP Request Tab</b>	
<b>HTTP Headers Section</b>	
Name	Value

Form Fields	Values
Content-Type	application/json
<b>HTTP Query Parameters Section</b>	
Content	{         "serialid": \$(serialid),         "comment": "\$(comment)"     }

#### 4. Create Event Registry

- a. Navigate to **Performance Analytics > System > Event Registry**.
- b. Click **New** to create an event registry and specify the following details in the form:

Form Fields	Values
Event Name	state_change_soar
Table	Incident[incident]

#### 5. Create Script Action

- a. Navigate to **Browse System Policy > Events > Script Actions**.
- b. Click **New** to create script action and specify the following details in the form:

Form Fields	Values
Name	Update Case on SOAR
Event name	state_change_soar
Application	Global
Active	<Mark this checkbox>

Add the following script:

```
try {
r = new sn_ws.RESTMessageV2('SOAR REST API Requests',
'Update Case on SOAR');
updated_fields = JSON.parse(event.parm2);
var serialId = updated_fields["serialId"];
if (updated_fields["caseProperties"] != {}) {
r.setStringParameterNoEscape('changes', JSON.stringify
(updated_fields["caseProperties"]));
r.setStringParameterNoEscape('serialId', serialId);
response = r.execute();
responseBody = response.getBody();
httpStatus = response.getStatusCode();
}
if (updated_fields["caseComment"] != {}) {
r = new sn_ws.RESTMessageV2('SOAR REST API Requests',
```

```

'Add Comment to SOAR Case');
r.setStringParameterNoEscape('serialId', serialId);
var comment = updated_fields["caseComment"]["comment"]
["value"];
r.setStringParameter('comment', comment.replace(/\n/g,
" "));
response = r.execute();
responseBody = response.getBody();
httpStatus = response.getStatusCode();
}

} catch (ex) {
var message = ex.message;
}

```

## 6. Create Business Rules

- Navigate to **System Definition > Business Rules**.
- Click **New** to create business rule and specify the following details in the form:

Form Fields	Values
Name	soar-rule
Table	Incident[incident]
Application	Global
Active	<Mark this checkbox>
Advanced	<Mark this checkbox>
<b>When to run tab</b>	
When	after
Order	1

Form Fields	Values
Update	<Mark this checkbox>
<b>Advanced tab</b>	
Script	<p>Add the following script:</p> <pre>if ((current.operation() == 'update' &amp;&amp; current.state.changes()    current.description.changes()    current.comments.changes()) { var currentValues = { "caseProperties":{}, "caseComment":{}, "serialId": current.short_description.toString().split("-")[0] }; var previousValues = { "state": previous.state.getDisplayValue(), "description": previous.description.getDisplayValue(), "comments": previous.comments.getJournalEntry(1) }; if (current.comments.changes()){ currentValues["caseComment"]["comment"] = {"value": current.comments.getJournalEntry(1)}; } if (current.state.changes()){ currentValues["caseProperties"]["status"] = {"value": current.state.getDisplayValue()}; } if (current.description.changes()){ currentValues["caseProperties"]["description"] = {"value": current.description.getDisplayValue()}; } gs.eventQueue('state_change_soar', current, JSON.stringify(previousValues), JSON.stringify(currentValues)); }</pre>

c. Click **Submit**.

#### 7. Import Certificate (if SOAR has self-signed certificate)

- a. Navigate to System Definition > Certificates.
- b. Click **New** to create new certificate entry.
- c. Click the attachment icon below to **upload your certificate file**. Run the following command to create the certificate

```
openssl s_client -connect cdfhost:cdfport 2>/dev/null </dev/null | sed
-ne '/-BEGIN
CERTIFICATE-/,/-END CERTIFICATE-/p'
```

- d. Save the content with .der extension.

## Configuring ServiceNow with OAuth2

1. Log in to **ServiceNow**.
2. Activate the OAuth 2.0 plugin.
3. In the **sys\_properties** table, set the system property **com.snc.platform.security.oauth.is.active** to **True**.
4. Click System OAuth > Application Registry > New > OAuthAPI for external clients.
5. Specify the following parameters:

Name	Client ID	Client Secret Key	Refresh Token Lifespan	Access Token Lifespan
Enter a unique name	Client ID automatically generated by ServiceNow OAuth server	Client Secret for OAuth application	Time in seconds for which the refresh token is valid	Time in seconds for which the access token is valid



Note down the Client ID and Client Secret as you may need it later.

6. Click Submit.

## Configuring SOAR

1. Click **Configuration > Credential > Create Credential**
2. Specify the following parameters in the **Credential Editor** form:

Type	Name	Username	Password	Private Key
Internal credential	Display name of credential set (for example, ServiceNow Credentials).	Username of the created user on ServiceNow	Password of the created user on ServiceNow	Empty

Check the Cleartext Access option.

3. Click **Configuration > Lists > Create Lists**. The list must two columns with the type **Keyword**. Specify a name for that list and save it. The name of the list is used during integration configuration.
4. Click **Configuration > Integrations > Create Integration**.

5. Specify the following parameter values in the **Configuration Form**.

Parameter	Value				
<b>Name</b>	Display name of the integration.				
<b>Type</b>	ServiceNow				
<b>Address</b>	Address of the ServiceNow integration (the format should be https://dev107155.service-now.com).				
<b>Configuration</b>	<p>Specify the following configuration parameters:</p> <table border="1"> <tr> <td><b>proxy.id</b></td><td>ID of the Proxy integration if you access ServiceNow through a web proxy device. For example: proxy.id = 12345 .</td></tr> <tr> <td><b>list.name</b></td><td>List name that is used for mapping ArcSight SOAR cases to ServiceNow incidents. For example, list.name=servicenowMapList</td></tr> </table>	<b>proxy.id</b>	ID of the Proxy integration if you access ServiceNow through a web proxy device. For example: proxy.id = 12345 .	<b>list.name</b>	List name that is used for mapping ArcSight SOAR cases to ServiceNow incidents. For example, list.name=servicenowMapList
<b>proxy.id</b>	ID of the Proxy integration if you access ServiceNow through a web proxy device. For example: proxy.id = 12345 .				
<b>list.name</b>	List name that is used for mapping ArcSight SOAR cases to ServiceNow incidents. For example, list.name=servicenowMapList				
<b>Credential</b>	Credential that has been defined for this integration under the <b>Credentials</b> menu.				
<b>Trust Invalid SSL Certificates</b>	Select this if web server's certificate is self-signed or is not recognized by browsers.				
<b>Require Approval From</b>	Select user(s) from list to ask the approval before executing actions on this integration.				
<b>Notify</b>	Select user(s) from the list to notify when SOAR performs an action on this integration.				

6. Click **Save** to save the integration definition.
7. Navigate to **Configuration>Customization Library** and edit **ServiceNow Advanced Action Script Default Template**.
8. Select the integration that you have added to **Integrations** menu.
9. Click **Save** to complete the integration.
10. Click **Test**. **Integration Successful** message is displayed if the credential and address are valid.

## Capabilities

1. **Create Incident**

Action capability for creating incident on ServiceNow.

- Rollback: No
- Duplicate Check: Yes

The following table presents the **Create Incident** action capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Category and SubCategory</b>	Category and Subcategory information of created incident	Enum	No	Yes
<b>Description</b>	Servicenow Incident Description	Text	No	Yes
<b>Impact</b>	ServiceNow incident impact	Enum	No	Yes
<b>Urgency</b>	Servicenow Incident Urgency	Enum	No	Yes
<b>Comment</b>	Servicenow Incident Comment	Text	No	Yes
<b>Assignment Group</b>	Servicenow Incident Assignee	Text	No	Yes

## 2. Close Incident

Action capability for closing incident on ServiceNow.

- Rollback: No
- Duplicate Check: No

The following table presents the **Close Incident** action capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>State</b>	Closing State of Servicenow incident.	Enum	No	Yes
<b>Resolution Code</b>	Resolution Code for ServiceNow incident.	Enum	No	Yes
<b>Resolution Note</b>	Resolution Note for ServiceNow incident.	Enum	No	Yes

## 3. Update Incident

Action capability for updating incident on ServiceNow.

The following table presents the **Update Incident** action capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Description</b>	Servicenow Incident Description	Text	No	No
<b>Impact</b>	ServiceNow incident impact	Enum	No	No
<b>Urgency</b>	Servicenow Incident Urgency	Enum	No	No

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Comment</b>	Servicenow Incident Comment	Text	No	No
<b>Assignment Group</b>	Servicenow Incident Assignee	Text	No	No
<b>State</b>	ServiceNow incident status	Enum	No	No

**Output:**

Case Scope: N/A

Human Readable Output: Yes

## Integration Guide for ServiceNow CMDB

### Integration Overview

A configuration management database is a data repository file used to store information about your IT environment. A CMDB's main functions include discovering, controlling, and keeping track of relationships between IT assets. As well as highlighting their individual configurations.

### Integration Capabilities

- List Assets
- Get Asset by ID
- Update Asset Tag

### Integration Configuration

1. Authentication: ServiceNow uses OAuth authentication to authenticate the API. Follow these below steps to configure a service from the ServiceNow Platform:
  - a. Sign into the platform and create an account, create username and password.
  - b. Create an instance to get a service URL. This username and password can be used to get the token to access the APIs.
  - c. Change the Elevate Role to security\_admin.
  - d. Navigate to System OAuth > Application Registry.

- e. Click on new and select Kind of Oauth application as Create an OAuth API endpoint for external clients.
- f. Fill in the details and submit. And save the Client\_ID and Client\_secret to generate the refresh token and access token.
- g. Client creates a POST call and passes the user name, password, client\_id , client\_secret and grant\_type in the Request body using the /x-www-form-urlencoded content type.

#### Body Parameters for the Token generation

Parameters	Value	Data Type	Required
Username	User Name	String	Yes
Password	Account Password	String	Yes
Private Key	Enter your client secret	String	Yes
Grant_type	Grant Type	String	No

#### Sample Request:

```
POST /oauth_token.do HTTP/1.1
Host: <instance>.service-now.com
Content-Type: application/json
{
  "username" : "Your_Username"
  "password" : "Your_Password"
  "client_id" : "YOUR_CLIENT_ID",
  "client_secret" : "YOUR_CLIENT_SECRET",
  "grant_type" : "password"
}
```

#### Sample Response

```
HTTP/1.1 200 OK
{
  "access_token": "uMb-6TIG-
  YCYI8BSnbK7caBamElpR7qWjVkxZpa11cWjD3Z4alwvcnhd19jdzP3f454GHXTib12PPXG
  JdmAlZQ",
  "refresh_token":
  "Tu_YsPq8Eqg9oCD_2HnBNCCd10SXU002jJepwKjCizwMPIqpOP6gN3LwFxE-
  Jh1CuaXjWi-SVqhvo3nv5VXFNg",
  "scope": "useraccount",
  "token_type": "Bearer",
  "expires_in": 1799
}
```

## 2. Additional Configuration

Configuration Parameter	Description
proxy.id	Proxy device to be used while communicating with the remote system's API
cache.reusing.duration	Default cache-reuse parameter
class.name	CMDB class name is the name of the table that contains the desired CI records, such as cmdb_ci_linux_server or cmdb_ci_apache_web_server.
client.id	Provide generated client ID for OAuth authentication.

## Integration Capabilities:

### 1. List Assets

Enrichment capability to retrieve the asset details from the ServiceNow platform by specific asset type.

#### Request headers

Header	Value	Required
Authorization	Bearer token	Yes
Content-type	application/json	Yes

#### Input Parameters:

Parameter	Description	DataType	Scope Restricted	Required
Asset Type	Type of asset, Default: Hardware, Consumable, License, Other, All	Array	No	Yes

#### Output:

Case Scope: N/A

Limitations: N/A

Human Readable Output:

Asset Tag	Display Name	System Id	System Install Date	System Update Date
1256901	1256901 - Apple MacBook Pro 15"	00a96c0d3790200044e0b fc8bcbe5dc3	2020-12-22 07:00:00	2023-11-21 10:01:29
test_asset_tag	test_asset_tag - Gateway DX Series	0196612a37c4200044e0b fc8bcbe5d3a	2022-05-08 07:00:00	2023-11-21 11:47:55
P1000807	P1000807 - Apple MacBook Pro 17"	01a92c0d3790200044e0b fc8bcbe5d36	2021-12-15 07:00:00	2023-11-21 10:01:29
P1000637	P1000637 - Apple MacBook Air 13"	01a9a80d3790200044e0b fc8bcbe5d53	2022-08-09 08:00:00	2023-11-21 10:01:29
P1000443	P1000443 - Lenovo ThinkStation S20	01a9ec0d3790200044e0b fc8bcbe5d93	2020-09-19 08:00:00	2023-11-21 10:01:29
P1000433	P1000433 - Lenovo ThinkStation S20	01a9ec0d3790200044e0b fc8bcbe5dd2	2021-11-24 07:00:00	2023-11-21 10:01:29
P1000337	P1000337 - Dell Inc. Precision T5500 Workstation	02a9604d3790200044e0b fc8bcbe5d26	2021-03-22 07:00:00	2023-11-21 10:01:29

## 2. Get Asset by ID

Enrichment capability to retrieve information about a specific asset by ID.

Request headers

Header	Value	Required
Authorization	Bearer token	Yes
Content-type	application/json	Yes

### Input Parameters

Parameter	Description	DataType	Scope Restricted	Required
System ID	System ID of the record to retrieve	String	No	Yes

Output:

Case Scope: N/A

Limitations: N/A

Human Readable Output:

The screenshot shows two main sections of a ServiceNow CMDB interface. The top section displays detailed parameters for an asset, including its key, value, and various metadata such as Model Category, Model, Company, Cost, Configuration Item, Quantity, Assigned To, and System ID. The bottom section shows system-level information like System Domain, System Install Date, and System Update Date. At the bottom of the page, there is a navigation bar with a dropdown for items per page (set to 100) and a total count of 13 items.

Key	Value
Asset Tag	P1000458
Display Name	P1000458 - IBM Thinkpad T20
Model Category	<a href="https://dev157314.service-now.com/api/now/table/cmdb_model_category/81feb9c137101000deeabfc8bcbe5dc4">https://dev157314.service-now.com/api/now/table/cmdb_model_category/81feb9c137101000deeabfc8bcbe5dc4</a>
Model	<a href="https://dev157314.service-now.com/api/now/table/cmdb_model/0c43b124c611227501522de2a381613e">https://dev157314.service-now.com/api/now/table/cmdb_model/0c43b124c611227501522de2a381613e</a>
Company	ACME Germany
Cost	49.99
Configuration Item	<a href="https://dev157314.service-now.com/api/now/table/cmdb_ci/03a9e40d3790200044e0bfc8bcbe5d6c">https://dev157314.service-now.com/api/now/table/cmdb_ci/03a9e40d3790200044e0bfc8bcbe5d6c</a>
Quantity	1
Assigned To	Terrance Nimmer
System ID	07a9e40d3790200044e0bfc8bcbe5d6b

System Domain	Global
System Install Date	2021-05-02 07:00:00
System Update Date	2023-11-21 10:01:30

Total 13 , items / page 1

### 3. Update Asset Tag

Action capability to update an asset tag.

Rollback: No

Duplicate Control: No

#### Request headers

Header	Value	Required
Authorization	Bearer token	Yes
Content-type	application/json	Yes

#### Input Parameters

Parameter	Description	DataType	Scope Restricted	Required
System ID	Serial number of this asset.	String	No	Yes
Asset Tag	Alphanumeric information assigned by your organization to help track the asset	String	No	Yes

**Output:**

Case Scope: N/A

Limitation: N/A

Human Readable Output: N/A

# Integration Guide for Slack

## Integration Overview

Slack is a messaging app for business that connects people to the information that they need. By bringing people together to work as one unified team, Slack transforms the way that organizations communicate. Slack supports asynchronous work. When work is organized in channels, the users can access the information as per their own time, regardless of the location, time zone or function. It can be used for asking questions, catching up with new developments and share updates without having to coordinate schedules.

## Integration Capabilities

- List Channels
- Get Channel Info
- Create Channel
- Send Message to Channel
- Archive Channel
- Invite User to Channel

## Prerequisites

- You must have access to HTTPS as the ArcSight SOAR connects to Slack API through this service.

## Configuring Slack

1. Log in to your Slack account and create your application using <https://api.slack.com/apps>.
2. Click **Create New App** to create new Slack application from scratch. Also, mention application name and pick your workspace to create the application.
3. Enter into your application and navigate to **Oauth and Permissions**.
4. Click **Scopes > User Token Scopes** provide the below scope permissions:

Capability	Scope Permissions Required
List Channels	channels:read, groups:read, im:read, mpim:read, identify:basic
Get Channel Information	channels:read, groups:read, im:read, mpim:read, identify:basic
Create Channel	channels:write, groups:write, im:write, mpim:write
Send Message to channel	chat:write
Archive Channel	channels:write, groups:write, im:write, mpim:write
Invite User to Channel	channels:write, groups:write, im:write, mpim:write

5. After all the scopes are added then install your application.
6. Navigate to **OAuth and permissions > OAuth tokens for Workspace** to find your User Oauth token. This User OAuth token is used to access the slack api.

## Configuring SOAR

1. Click **Configuration > Credential > Create Credential**.
2. Specify the following parameter values in the **Credential Editor**:

Type	Name	Username	Password	Private Key
Internal Credential	Display name of credential set ( for example, Slack Credentials).	N/A	N/A	Bearer {Token}

3. Click **Save** to complete the integration
4. Click **Test**, an **Integration Successful** message is displayed if the credential and address are valid.

# Capabilities

## 1. List Channels

Enrichment capability for retrieving channels list.

The following table provides the List Channels enrichment capability details:

Input Parameter	Description	Type	Scope Restricted(Yes/No)	Required (Yes/No)
Integration	Name of the third party integration	Integration	N/A	Yes

### Output:

Case Scope

Action	Type	Category/Value
None	N/A	N/A

### Human Readable Output:

Channel Name	Channel Id	Channel Type	Topic	Purpose	Total Members	Created By	Create Time
random	C049XFVNJ1L	Private	N/A	This channel is for... well, everything else. It's a place for team jokes, spur-of-the-moment ideas, and funny GIFs. Go wild!	4	chethan.p	2022-11-09T06:18:00.0Z
create_private_channel	C049Y56N62J	Private	N/A	N/A	1	chethan.p	2022-11-09T09:00:37.0Z
microfocusconnector	C04A44DRVVO	Private	N/A	This channel is for everything #microfocusconnector. Hold meetings, share docs, and make decisions together with your team.	0	chethan.p	2022-11-09T06:21:03.0Z
microfocusconnector	C04A6HRD65S	Private	N/A	This channel is for everything #microfocusconnector. Hold meetings, share docs, and make decisions	3	chethan.p	2022-11-09T06:19:36.0Z

## 2. Get Channel Info

Enrichment capability for retrieving channel information.

The following table provides the **Get Channel Info** enrichment capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
Integrtation	Name of the third party integration	Integration	N/A	Yes
Channel Name	Name of the channel	Username Keyword Unknown	Yes	Yes

**Output**

Case Scope

Action	Type	Category/Value
None	N/A	N/A

Human Readable Output:

Key	Value
Channel Name	create_private_channel
Channel ID	C049Y56N62J
Topic	N/A
Purpose	N/A
Total Members	1
Created By	chethan.p
Creation Time	2022-11-09T09:00:37.0Z
Is Archived	true

**3. Create Channel**

Action capability for creating a new channel.

- Rollback: No
- Duplicate Control: Yes

The following table provides the **Create Channel** enrichment capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
Integration	Name of the third party integration	Integration	N/A	Yes
Channel Name	Name of the channel	N/A	N/A	Yes

**Output:**

Case Scope

N/A

Human Readable Output

#### 4. Send Message to Channel

Action capability to send text messages to channel.

- Rollback: No
- Duplicate Control: No

The following table provides the channel Information action capability details

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
Integration	Name of the third party integration	Integration	N/A	Yes
Channel Name	Name of the channel	Username Keyword Unknown	Yes	Yes
Message	Text message to send to channel	String	No	Yes

#### Output:

Case Scope

N/A

Human Readable Output

#### 5. Archive Channel

Action capability to archive the channel.

- Rollback: No
- Duplicate Control: No

The following table provides the **Archive Channel** action capability details

Input Parameter	Description	Type	Scope Restricted(Yes/No)	Required (Yes/No)
Integration	Query string for the search	Integration	Yes	Yes
Channel Name	Name of the channel	Username Keyword Unknown	Yes	Yes

#### Output:

Case Scope

N/A

Human Readable Output

#### 6. Invite User to Channel

Action capability to invite user to a channel.

- Rollback: No
- Duplicate Control: No

The following table provides the Invite User to Channel action capability details:

<b>Input Parameter</b>	<b>Description</b>	<b>Type</b>	<b>Scope Restricted (Yes/No)</b>	<b>Required (Yes/No)</b>
Integration	Name of the third party integration	Integration	N/A	Yes
Channel Name	Name of the channel	Username Keyword Unknown	Yes	Yes
User Name	Name of the Slack user	Username Keyword Unknown	Yes	Yes

#### **Output:**

Case Scope

N/A

Human Readable Output

N/A

# Integration Guide for SMTP Mail Server

## Integration Overview

ArcSight SOAR uses the SMTP Server to send emails and notification messages. ATAR can also use the same integration to access inboxes to read emails, such as device action approvals if it is configured as an IMAP server.

## Integration Capabilities

- Action
- Send email

## Prerequisites

- SOAR connects to SMTP Mail Server integration via Simple Mail Transfer Protocol. Therefore SOAR must be able to connect this service.
- A user's credential is required for SMTP AUTH. The same credential will be used if IMAP is configured.

## Configuration

### Configuring SOAR Email Notification

1. Click Configuration > Parameters.
2. Search for **NotificationEMailFrom** > Edit and set Email address.
3. Search for **ApprovalEMailFrom** > Edit and set Email address.
4. Search for **ApprovalEMailEnabled** > Edit and set it as **True**.
5. Search for **OutgoingMailIntegration** > Edit and add SMTP Integration ID.
6. Search for **IncomingMailIntegration** > Edit and add SMTP Integration ID.

### Configuring SOAR

1. Click **Configuration > Integrations > Create Integration**.
2. Specify the following parameter values in the **Configuration** form:

Parameter	Value
Name	Display name of the SMTP Mail Server integration..
Type	SMTP Mail Server
Address	Address of the integration (the format should be 1.1.1.1 or abc.example.com).
Configuration	<p>Specify the following configuration parameters:</p> <pre>mail.default-encoding is the encoding format of emails. mail.transport.protocol is the default message transport protocol. mail.smtp.auth specifies whether SMTP Authentication will be enabled or not. It can be "true" or "false". mail.smtp.port is the port for the SMTP service. mail.smtp.starttls.enable specifies whether TLS for SMTP will be enabled or not. It can be "true" or "false". mail.store.protocol is the protocol to access inboxes (for email reading). Default value is "imaps". mail.imaps.host is the address of the IMAPS server. mail.imaps.port is the port for IMAPS service. # Server type should be default for standard SMTP connections, the type should be exchange-online to enable token authentication for Exchange Online SMTP devices.e. smtp.server.type=exchange-online # Imap mail account for token authentication connections imap.mail.account=imap.account@somehost.com # Imap message polling period in millis, the default value is 10000 ms #imap.polling.period=10000 # Integration ID of the proxy integration to use when connecting to current integration. # If not provided, ArcSight SOAR will try to use a direct connection. #proxy.id=123</pre>
	<p>Specify the following to enable OAuth2 in SMTP:</p> <pre>smtp.server.type=exchange-online imap.mail.account=imap.account@somehost.com</pre>
Credential	Select newly created OAuth2 credential as credential.
Trust Invalid SSL Certificates	Select this if Engine's certificate is self-signed or is not recognized by browsers
Require Approval From	Select users from the list who can provide approval before executing actions on this integration
Notify	Select user(s) from the list to notify when SOAR performs an action on this integration.

3. Click **Test** to test the integration.
4. Click **Save** to complete the integration.

## Additional Notes

- If a SMTP integration is used without credentials then it can't be used as incoming e-mail processor and for approvals.
- The global configuration parameter EMailDevice, under the Parameters tab of **Configuration** menu, configures the default mail server to be used in sending notifications and emails. Therefore, you must set the value of this parameter to the ID value for the SMTP Mail.
- SMTP Mail Server Integration with server type exchange online only supports basic authentication proxy servers. NTLM authentication is not supported.

# Integration Guide for Sophos XG Firewall

## Integration Overview

Sophos XG Firewall is an integrated security platform featuring next gen firewall capabilities.

## Integration Capabilities

ArcSight SOAR has the following integration capability with Sophos XG Firewall:

- Block IP
- Block FQDN
- Block URL
- Block Email Sender

### **Use Case: Blocking bad actors on firewalls**

With this integration, SOAR can block malicious IP addresses, hosts and URL addresses on firewall devices while responding cyber-attacks. This can be performed automatically within a playbook or manually by an analyst.

## Configuration

### Prerequisites

- SOAR connects to Sophos XG Firewall API via management port. So access permission to this port is required.
- A user account for SOAR to connect to Sophos XG Firewall.

### Configuration on Sophos XG Firewall

1. Click **Configure > Authentication > Users menu** and add an administrator user account.
2. Create a new profile or select a suitable one from the Profile list. Profile should have the following permissions:
  - Read-write for Objects
  - Web & content filter

- Email protection
- None for the rest of the permissions

3. Navigate to **Backup & Firmware > API** to enable API Configuration and add SOAR IP Address to the Allowed IP Address list.
4. Click **Administration > Device Access** to ensure that SOAR's assigned zone can access the HTTPS service of Sophos. You can prefer to create a Local Service ACL Exception Rule as well. For more information consult the Sophos How to use API documentation for further information.
1. Click **Configuration > Credentials > Create Credential**.
2. Specify the following parameter values in the **Credential Editor**:

a. **Internal Credential**

Parameter	Value
Type	Internal Credential
Name	Display name of credential set (For example, Sophos XG Credentials)
Username	Username you have created on firewall.
Password	Password you have created on firewall.
Private Key	Empty

b. **Credential Store:**

Parameter	Value
Type	External Credential
Name	Name of the credential with pull path of the safe on store

3. Click **Configuration > Integrations > Create Integration**.
4. Specify the following parameter values in the **Configuration** form:

Parameter	Value
Name	Display name of Sophos XG integration on SOAR.
Type	Sophos XG Firewall.
Address	Address of the firewall (the format should be https://192.168.10.1:4444)

Parameter	Value
Configuration	<p>Specify the following configuration parameters:</p> <pre># IP host group name for adding ip hosts to block iphost.group.name=ATAR_IP_BLOCK # FQDN host group name for adding fqdns to block fqdnhost.group.name=ATAR_HOST_BLOCK # Web filter url group name for adding urls to block webfilterurl.group.name=ATAR_URL_BLOCK</pre>
Credential	Name of the credential set created on step 2 (For example, Sophos XG Credentials)
Trust Invalid SSL Certificates	Select this if Management UI's certificate certificate is self-signed or is not recognized by browsers
Require Approval From	Select users from the list who can provide approval before executing actions on this integration
Notify	Select user(s) from the list to notify when SOAR performs an action on this integration. Since SOAR only executes enrichments on Symantec DLP, leave it empty

5. Click **Test** to test the integration.
6. Click **Save** to complete the integration.

## Additional Notes

- IP, FQDN and URL filter groups are automatically created by SOAR if they don't exist.1. IP, Host and URL filter groups are automatically created by SOAR if they don't exist.
- Sophos XG Firewall URL Filtering only accepts URLs with the following format <http://www.example.com>. URI paths are not accepted through API. Therefore SOAR transparently trim the URI part while submitting to Sophos XG Firewall.
- SOAR stores blocked email addresses in a list to keep track. Sophos currently does not provide a method to get the current list and any update will overwrite the list with the new address so administrator should only update the MTA Blocked Sender List through SOAR. Also this list is kept for each different Sophos integration but creating a second integration for the same device can lead to data inconsistency.

# Integration Guide for SORBS Query

## Integration Overview

SORBS Query provides free access to its DNS-based Block List to effectively block mail from more than 12 million host servers known to disseminate spam, phishing, attacks and other forms of malicious emails.

## Integration Capabilities

- Action
- Check IP

## Configuration

### Configuration on SORBS Query

- ATAR connects to SORBS integrations's API via HTTPS. Therefore ATAR should be able to connect this service.

## Configuring SOAR

### Configuring SOAR

1. Click **Configuration > Integrations > Create Integration**.
2. Specify the following parameter values in the **Configuration** form:

Parameter	Value
Name	Display name of SORBS Query integration on SOAR.
Type	SORBS Query.
Address	Address of the integration (the address should be http[s]://dnsbl.sorbs.net).

Parameter	Value
Trust Invalid SSL Certificates	Select this if Engine's certificate certificate is self-signed or is not recognized by browsers
Require Approval From	Select users from the list who can provide approval before executing actions on this integration
Notify	Not Applicable

3. Click **Test** to test the integration.
4. Click **Save** to complete the integration.

# folIntegration Guide for Symantec Advanced Threat Protection

## Integration Overview

Symantec Advanced Threat Protection is Symantec's endpoint protection platform closely works with SEP Manager.

## Integration Capabilities

- Action Capabilities
- Quarantine Endpoint (isolate\_endpoint and rejoin\_endpoint)
- Delete File From Endpoint (delete\_endpoint\_file)
- Enrichment Capabilities
- Get Events (/events)

## Configuration

### Configuring Symantec Advanced Threat Protection

Symantec ATP uses https (tcp/443) for API access by default.

1. Click **Settings > Data Sharing > OAuth Clients > Add application with custo role** to add the API application.
2. The image in the **Privileges** section represents how the custom role must be configured.  
After creating user, Symantec displays the **client secret** and **client id**, which is used in SOAR configuration modal.

### Configuring SOAR

1. Navgate to **Configuration > Integrations**.
2. Specify the following parameter values in the **Integrations Editor**:

Parameter	Value
Name	Display name of Symantec Advanced Threat Protection integration on SOAR
Type	Symantec Advanced Threat Protection.
Address	Address of the integration (in the following format: https://1.1.1.1)
Configuration	Specify the following configuration parameters. <code>#EVENT_RESULT_LIMIT</code>
Credential	Name of the credential set created under the <b>Credentials</b> menu. You must use <b>client id</b> as username and <b>client secret</b> as password.
Trust Invalid SSL Certificates	Select this if Engine's certificate is self-signed or is not recognized by browsers
Require Approval From	Select users from list who can provide approval before executing actions on this integration
Notify	Select users from the list to notify when SOAR performs an action on this integration

3. Click **Save** to save the integration.
4. Navigate to **Configuration>Customization Library** and edit **Symantec Advanced Threat Protection Advanced Action Script Default Script Template**.
5. Select the integration that you have added to Integrations menu.
6. Click **Save** to complete the integration.
7. Click **Test**, an **Integration Successful** message is displayed if the credential and address are valid.

# Integration Guide for Symantec Bluecoat Malware Analysis Appliance (MAA)

## Integration Overview

Symantec Bluecoat MAA is a malware analyzer sand-box solution. SOAR uses Symantec Bluecoat Malware Analysis Appliance to analyze files and URLs.

## Integration Capabilities

- Action
- File Analysis
- Hash Analysis
- URL Analysis

## Prerequisites

- SOAR connects to Symantec Bluecoat MAA's Remote API (RAPI) via HTTPS. Therefore, SOAR should be able to connect this service.
- A user account is required for SOAR to connect to Symantec Bluecoat MAA.

## Configuration

### Configuring SOAR

1. Click **Configuration > Credentials > Create Credential**.
2. Specify the following parameter values in the **Credential Editor**:

#### Internal Credential

Parameter	Value
Type	Internal Credential
Name	Display name of credential set (For example, BlueCoat Malware Analysis Appliance Credentials)

Parameter	Value
Username	Username of the administrator
Password	Password of the admin user
Private Key	Empty

### 3. Credential Store:

Parameter	Value
Type	External Credential
Name	Name of the credential with pull path of the safe on store

### 4. Navigate to Configuration > Integrations.

### 5. Specify the following parameter values in the Integrations Editor:

Parameter	Value
Name	Display name of Symantec Bluecoat MAA integration on SOAR.
Type	Symantec Bluecoat MAA .
Address	Address of the integration (in the following format: http[s]://1.1.1.1:1234
Credential	Name of the credential set created under the <b>Credentials</b> menu.
Trust Invalid SSL Certificates	Select this if Engine's certificate is self-signed or is not recognized by browsers
Require Approval From	Select users from list who can provide approval before executing actions on this integration
Notify	Select users from the list to notify when SOAR performs an action on this integration

### 6. Click **Test** to test the integration.

### 7. Click **Save** to save the integration.

## Integration Guide for Symantec BlueCoat Proxy SG

### Integration Overview

BlueCoat Proxy SG is a secure web gateway solution developed by Symantec which controls the users' access to web content. This integration has been tested with Symantec BlueCoat Proxy SG 6.6.4.2 version.

## Integration Capabilities

SOAR has the following integration capability with Symantec BlueCoat Proxy SG

- Block

### **Use Case: Blocking access to malicious URL**

SOAR can integrate with Symantec BlueCoat Proxy SG to block malicious URLs detected while responding an incident. Blocking can be performed automatically within a playbook or manually by an analyst.

## Configuration

### Prerequisites

- SOAR connects to Symantec BlueCoat Proxy SG Management UI through HTTPS in order to download existing copy of local database. As Management Console runs on 8082 /tcp port, so access to this port is required.
- SOAR connects to Symantec BlueCoat Proxy SG via SSH to immediate update of local database. So access to 22/tcp port is required.
- Symantec BlueCoat Proxy SG connects back to SOAR API to gather new copy of the local database. As SOAR API runs on 443/tcp port, so access from BlueCoat Proxy SG to this service is required.
- Admin user credentials are required for SOAR to connect Symantec BlueCoat Proxy SG

## Configuring SOAR

1. Click **Configuration > Credentials > Create Credential**.
2. Specify the following parameter values in the **Credential Editor**:

**a. Internal Credential**

Parameter	Value
Type	Internal Credential
Name	Display name of credential set (For example, BlueCoat Proxy SG Credentials)
Username	Username of the administrator
Password	Password of the admin user
Private Key	Empty

**b. Credential Store:**

Parameter	Value
Type	External Credential
Name	Name of the credential with pull path of the safe on store

3. Click **Configuration > Integrations > Create Integration.**

4. Specify the following parameter values in the **Configuration** form:

Parameter	Value
Name	Display name of Symantec BlueCoat Proxy SG integration on SOAR
Type	Symantec BlueCoat Proxy SG
Address	Address of the integration ( in the following format: https://192.168.2.99)

Parameter	Value
Configuration	<p>Specify the following configuration parameters:</p> <pre># Default category to block URLs. If empty, value of # BlueCoatDefaultBlockListCategoryName configuration #category=soar # parameter will be used. # Comma (,) separated list of IP addresses of Bluecoat # servers that are allowed to retrieve blocked URL list. # servers that are allowed to retrieve blocked URL list. # servers that are allowed to retrieve blocked URL list. #allowedaddresses= # Default block list source URL. This URL should be pointed out # third-party block list source address. If unspecified, value # of BlueCoatDefaultBlockListURL will be used. #blocklistssource= # Connect to Bluecoat Proxy using SSH with provided # credential and execute commands to immediately force # refresh of the block list. Default is false. #forcerefresh.enabled=false</pre> <p>For a third party blacklist to work correctly it must be structured as follows:</p> <p>For example,</p> <p>If you want to work with separate categories you can give a different category name to differentiate between SOAR sourced URL's and the third-party URL's.</p> <pre>define category "soar" www.example.com www.example.com/example.asp example.com 192.168.201.57 end category "soar"</pre>
Credential	Name of the credential set created on step 2 (For example, BlueCoat Proxy SG Credentials)
Trust Invalid SSL Certificates	Select this if Management Consoles's certificate is self-signed or is not recognized by browsers
Require Approval From	Select users from the list who can provide approval before executing actions on this integration
Notify	Not Applicable

5. Click **Save** to complete the integration.
6. Click **Configuration > REST Clients > Create REST Clients** to create client credentials.
7. Fill the description and Client ID.



Bluecoat allows maximum of 31 character. Make sure Client ID is within that range.

8. Click **Save**. A **REST Client Details** successful message is shown.
9. Click the copy icon to save the Client ID and Client Secret.

## Configuring Symantec BlueCoat Proxy SG

1. Click **Configuration > Content Filtering > General** and enable **Local Database**.
2. Click **Configuration > Content Filtering > Local Database** and configure copy of local database URL accessible on SOAR . The format should be `https://cdf/soar-api/api/bluecoat/list/integrationId}`  
integrationId: ID of BlueCoat Proxy SG integration on SOAR.
3. To create client credential login to Bluecoat SSH and run the following commands:

```
enable
config terminal
content-filter
local
download username <client-id>
download password <client-secret>
```

4. Click SOAR > Configuration > Integration > BlueCoat Proxy SG and click Test to test the integration.

## Additional Notes

- Due to update mechanism of Blucoat Proxy SG's Content Filter/Local Database, BlueCoat Proxy SG retrieves the list of items to be blocked from a URL located on a web server that is accessible by the Proxy SG. SOAR maintains a copy of Content Filter/Local Database and is accessible on `https://cdf/soar-api/api/bluecoat/list/integrationId}`.
- SOAR connects to management console and downloads a copy of the Content Filter/Local Database before adding new entries. If SOAR is the only place managing Content Filter/Local Database, you don't need to provide this access since SOAR always has the latest copy.
- After updating the list of items to be blocked on itself, SOAR might connect to BlueCoat Proxy SG via SSH and trigger an immediate download of the Content Filter/ Local Database file. This operation requires to access privileged-mode. In order to use this method set `forcerefresh.enabled=true` on integration configuration. List of commands executed during this operation can be found under **Configuration > Customization Library > Symantec BlueCoat Proxy SG SSH Integration Action (Block) Default Template**.
- If **Automatically check for updates** is set on Content Filter/Local Database configuration BlueCoat periodically connects and checks the latest version of the list. If you don't want immediate update you may set `forcerefresh.enabled=false` on integration configuration and prefer to use automatic updates.

- After the Integration is complete, if you get a certificate related error **Server certificate signed by unknown CA Download failed** do the following :
  - a. Install the missing CA Certificate and restart the database download.
  - b. Download the CDF external certificate.
  - c. Click **Configuration > SSL > CA Certificates** and import the certificate into the ProxySG appliance CA Certificates and name it as **CDF\_ca**.
  - d. Click **CA Certificate Lists > Browser-trusted** and add the certificate to the browser-trusted list.
  - e. Apply the configuration changes.
  - f. Create a block action on SOAR and view the action result to make sure that the download is working properly.



Click **Configuration > SSL > Device Profiles** and make sure that the **Device Profile** is set to **browser-trusted**.

- If you get a error for **Hostname in server certificate does not match URL hostname** then disable **Verify Peer** option for default **Device Profile** on Bluecoat Proxy SG device.

# Integration Guide for Symantec Bluecoat Site Review

## Integration Overview

Bluecoat Site Review is a site to report uncategorized URLs to Symantec/Bluecoat.

## Integration Capabilities

- Action
- Report Uncategorized URL (should get URL from scope)

## Configuration

### Configuration on Bluecoat Site Review

No requirements

### Configuring SOAR

- In SOAR **Configuration**, specify **Name**, **Address** and **submissionEmailAddress** to check submission result from returning mail.



Note: Add a dummy credential that can be removed in future releases.

# Integration Guide for Symantec Data Loss Prevention (DLP)

## Integration Overview

Symantec DLP is a solution to ensure that sensitive data is not lost, misused, or accessed by unauthorized users. This integration has been tested with Symantec DLP 14.6.0200 version.

## Integration Capabilities

SOAR has the following integration capabilities with Symantec DLP:

- Retrieve incidents

### **Use Case: Investigating Suspicious Behaviour**

During investigation of a suspicious behaviour of an employee or an endpoint, SOAR integrated with Symantec DLP, can get access the related DLP incidents for better understanding of the case. Investigation can be performed automatically within a playbook or manually by an analyst.

## Configuration

### Prerequisites

- SOAR connects to Symantec DLP API via HTTPS. Access to 443/tcp port is required.
- A user account is required for SOAR to connect to Symantec DLP.

### Configuring Symantec DLP

1. Login to Symantec DLP Enforce Server and navigate to **System > Login Management > Roles** to create a web service role. The web service role should have the following permissions:
  - Incidents: View
  - Perform Attribute Lookup
  - Incident Reporting and Update API: Incident Reporting

- Display Attributes: All,
  - Custom Attributes: View all
2. Click **System > Login Management > DLP Users** and add a DLP user account with the role that is created on previous step.
  3. Login to Symantec DLP Enforce server administration console with the DLP user account created in previous step.
  4. Click **Incidents > Incident Reports** and select a system defined incident list, such as **Incidents - All**.
  5. Edit report filters to narrow down the results to be returned if needed. In the **Summarize by** menu verify that **and** are both selected.
  6. Save the report as a new private report and note the new report's ID.

## Configuring SOAR

1. Click **Configuration > Credentials > Create Credential**.
2. Specify the following parameter values in the **Credential Editor**:
  - a. **Internal Credential**

Parameter	Value
Type	Internal Credential
Name	Display name of credential set (For example, Symantec DLP Credentials)
Username	User you have created for SOAR on Symantec DLP.
Password	Password of the user you have created for SOAR on Symantec DLP
Private Key	Empty

- b. **Credential Store:**

Parameter	Value
Type	External Credential
Name	Name of the credential with pull path of the safe on store

3. Click **Configuration > Integrations > Create Integration**.
4. Specify the following parameter values in the **Configuration** form:

Parameter	Value
Name	Display name of Symantec DLP integration on SOAR.
Type	Symantec Data Loss Prevention.

Parameter	Value
Address	Address of the integration ( in the following format: https://192.168.2.15)
Configuration	Specify the following configuration parameters: <pre># Report id report.id=221</pre>
Credential	Name of the credential set created on step 2 (For example, Symantec DLP Credentials)
Trust Invalid SSL Certificates	Select this if Web UI's certificate certificate is self-signed or is not recognized by browsers
Require Approval From	Select users from the list who can provide approval before executing actions on this integration
Notify	Select user(s) from the list to notify when SOAR performs an action on this integration. Since SOAR only executes enrichments on Symantec DLP, leave it empty

5. Click **Test** to test the integration.
6. Click **Save** to complete the integration.

## Additional Notes

For the details of web service role and report creation please refer to [Symantec™ Data Loss Prevention Incident Reporting and Update API Developers Guide](#).

# Integration Guide for Symantec DeepSight Intelligence

## Integration Overview

Symantec DeepSight Intelligence is a commercial threat intelligence service which provides actionable intelligence with context and technical details surrounding a threat so teams can quickly assess cyber risk and implement proactive controls.

## Integration Capabilities

ArcSight SOAR has the following integration capabilities with Symantec DeepSight Intelligence Service:

- Ingest intelligence data as alert
- Domain Query
- File Query
- IP Query

### Use Case: Investigating Phishing Campaigns

SOAR is integrated with Symantec DeepSight Intelligence, to help investigation and mitigation of phishing campaigns. When a phishing report email comes from user, SOAR extracts the indicators such as IP address, domains and attachments in message and a new incident is created on SOAR's own Incident Management Service Desk. SOAR then asks these indicators to Symantec DeepSight Intelligence if this is a known attack and previously analyzed. This can be performed automatically within a playbook or manually by an analyst.

## Configuration

### Prerequisites

- SOAR connects to Symantec DeepSight API via HTTPS. Access to <https://deepsightapi.symantec.com/v1/> (443/tcp port) and <https://datafeeds.symantec.com/> (443/tcp port) is required.
- A user account and a certificate-password pair are required for SOAR to connect to Symantec DeepSight. These will be supplied by Symantec through DeepSight portal.

## Configuring Symantec DeepSight Intelligence

SOAR requires a username and password to be created on Symantec DeepSight for authentication purposes for Alert Source. If enrichment capabilities are to be used an API key must be enabled and created. Use an administrator account to enable API Access for the account you wish to use in SOAR.

1. Select **user's detail** tab. The tab includes a section for DeepSight API Token. Select **Enable Access**
2. Login with the SOAR account to the DeepSight portal.
3. Click **Settings > My Profile** and locate the **DeepSight API Token** tab.
4. Copy the API key.

## Configuring SOAR

1. Click **Configuration > Credentials > Create Credential**.
2. Specify the following parameter values in the **Credential Editor**:
  - a. **Internal Credential**

Parameter	Value
Type	Internal Credential
Name	Display name of credential set (For example, Symantec DeepSight Credentials).
Username	Empty
Password	API Key you've get from Symantec DeepSight Intelligence platform.
Private Key	Empty

- b. **Credential Store:**

Parameter	Value
Type	External Credential
Name	Name of the credential with pull path of the safe on store

## Configuring Symantec DeepSight Intelligence as Alert Source

1. Click **Configuration > Alert Source > Create Alert Source Configuration**.
2. Specify the following parameter values in the **Configuration** form:

Parameter	Value
Name	Display name of Symantec DeepSight Intelligence Alert Source on SOAR.
Type	Symantec DeepSight Intelligence Datafeeds
Address	Address of the Symantec DeepSight Intelligence DataFeeds ( <a href="https://datafeeds.symantec.com/v1/">https://datafeeds.symantec.com/v1/</a> ).
Configuration	<p>Specify the following configuration parameters:</p> <pre># Number of item to ingest per data feed type on first integration alertCountPerFeedType=1000 # Minimum item reputation value to turn into Alert on SOAR minReputationToAlert=10 #usable behaviour names : attack,attacks,bot,cnc,fraud,malware,phish,spam,phish_host #behaviourNames=attack,bot,CnC,fraud,malware,spam # Integration ID of the proxy integration to use when connecting to current source. # If not provided, SOAR will try to use a direct connection. #proxy.id=5422 # configure how far (in minutes) into the past this enrichment will look. #cache.reusing.duration=20</pre>
Credential	Name of the credential set created on step 2 (For example, Symantec DeepSight Credentials)
Trust Invalid SSL Certificates	Select this if Web UI's certificate certificate is self-signed or is not recognized by browsers
Require Approval From	Select users from the list who can provide approval before executing actions on this integration. Since SOAR only executes enrichment on Symantec DeepSight, leave it empty.
Visible Alert Fields	You may define which alarm fields will be displayed on Incident Management Service Desk.

## Configuring Symantec DeepSight Intelligence as Integration

1. Click **Configuration > Alert Source > Create Alert Source Configuration**.
2. Specify the following parameter values in the **Configuration** form:

Parameter	Value
Name	Display name of Symantec DeepSight Cyber Intelligence integration on SOAR.
Type	Symantec DeepSight Cyber Intelligence
Address	Address of Symantec DeepSight Cyber Intelligence ( <a href="https://deepsightapi.symantec.com/v1">https://deepsightapi.symantec.com/v1</a> )
Configuration	<p>Specify the following configuration parameters:</p> <pre># Integration ID of the proxy integration to use when connecting to current integration. # If not provided, SOAR will try to use a direct connection. #proxy.id=123 # configure how far (in minutes) into the past this enrichment will look. #cache.reusing.duration=20</pre>
Credential	Name of the credential set created on step 2 (For example, Symantec DeepSight Credentials)
Trust Invalid SSL Certificates	Select this if Web UI's certificate certificate is self-signed or is not recognized by browsers
Require Approval From	Select users from the list who can provide approval before executing actions on this integration. Since SOAR only executes enrichment on Symantec DeepSight, leave it empty.
Notify	Select users from the list to notify when SOAR performs an action on this integration. Since SOAR only executes enrichment on Symantec DeepSight, leave it empty.

3. Click **Test** to test the integration.
4. Click **Save** to complete the integration

# Integration Guide for Symantec Endpoint Protection Manager

## Integration Overview

Symantec Endpoint Protection Manager (SEP Manager) is a management platform for security software suite, which consists of anti-malware, intrusion prevention and firewall features for server and desktop computers. This integration has been tested with Symantec Endpoint Protection Manager 14.2.760 version.

## Integration Capabilities

SOAR has the following integration capabilities with Symantec Endpoint Protection Manager:

- Start Scan on Client
- Block File Hash
- Get Client Info

### **Use Case: Starting scan jobs on suspicious endpoints.**

During the course of and investigation or responding a ongoing cyber-attack, it is required to run scan jobs on suspicious endpoints to validate the threat. SOAR can start scan jobs on Symantec Endpoint Protection Manager to help on deciding the next course of action.

This can be performed automatically within a playbook or manually by an analyst.

## Configuration

### Prerequisites

- SOAR needs to connect Symantec Endpoint Protection Manager API and Database.
- Access to 8443/tcp, 8446/tcp port for API access and 1433/tcp, 1434/udp port for database access is required.
- User accounts for API access and database access are required for SOAR to connect to Symantec Endpoint Protection Manager.

## Configuring Symantec Endpoint Protection Manager

1. Login to SEP Management Server on <https://SEPManger:8443/console/apps/sepm> and create an administrator account on **Admin** tab.
2. Click **Policy > Policy Components > File Fingerprint Lists** and add a File Fingerprint List.
3. You might create a file containing MD5 value of eicar.com test signature  
44d88612fea8a8f36de82e1278abb02f: to upload a file to create the list.
4. Login to SEP Manager Web Service Application Registration on  
<https://SEPManger:8446/sepm> with the admin account you've created on previous step and register a webservice application to be used by SOAR.



**Note** the Client ID and Client Secret values are generated.

5. Create a database user that has select permissions and ensure that the SQL Browser service is configured and running on MSSQL Server.

## Configuring SOAR

1. Click **Configuration > Credentials > Create Credential**.
2. Specify the following parameter values in the **Credential Editor**:
  - a. **Internal Credential**

Parameter	Value
Type	Internal Credential
Name	Display name of credential set (For example, SEP Manager Credentials).
Username	Username you have created for SOAR on Symantec Endpoint Protection Manager
Password	Password of the user you have created for ATAR on Symantec Endpoint Protection Manager.
Private Key	Empty

3. b. **Credential Store:**

Parameter	Value
Type	External Credential
Name	Name of the credential with full path of the safe on store

3. To create credentials to be used for database connection:

### a. Internal Credential

Parameter	Value
Type	Internal Credential
Name	Display name of credential set (For example, SEP Manager DB Credentials).
Username	Database username you have created for SOAR on SEP Manager Database.
Password	Password of the user you have created for SOAR on SEP Manager Database.
Private Key	Empty

### b. Credential Store:

Parameter	Value
Type	External Credential
Name	Name of the credential with full path of the safe on store

4. Click **Configuration > Integrations > Create Integration**.

5. Specify the following parameter values in the **Configuration** form:

Parameter	Value
Name	Display name of Symantec Endpoint Protection Manager integration on SOAR
Type	Symantec Endpoint Protection Manager
Address	Address of the integration ( in the following format: https://192.168.2.140)
Configuration	Specify the following configuration parameters:  <pre>client.id=xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx client.secret=xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx #domainName= directdbaccess.enabled=true directdbaccess.jdbcurl= jdbc:sqlserver://192.168.2.140:1433\\SEPMDB;database=sem5 directdbaccess.credential=33323 # Integration ID of the proxy integration to use when connecting to # current integration. # If not provided, ATAR will try to use a direct connection. #proxy.id=123</pre>
Credential	Name of the credential set created on step 2 (For example, SEP Manager Credentials).
Trust Invalid SSL Certificates	Select this if Engine's certificate is self-signed or is not recognized by browsers
Require Approval From	Select users from the list who can provide approval before executing actions on this integration
Notify	Select user(s) from the list to notify when ATAR performs an action on this integration.

6. Click **Test** to test the integration.

7. Click **Save** to complete the integration.

## Additional Notes

Symantec Endpoint Protection Manager Webservice registration works on 8446/tcp port by default. If it is different than this value, you might configure it using **DefaultSEPMRestApiPort** parameter under **Configuration > Parameters**.

# Integration Guide for Symantec Managed Security Services (MSS)

## Integration Overview

Symantec Managed Security Services (MSS) provides its customers security monitoring and real-time security analytics services including strategic insights needed to prioritize and respond to incidents and build strategies to protect the assets, reputations and viability of their organizations.

## Integration Capabilities

SOAR has the following integration capabilities with Symantec MSS:

- Ingest Incident Records as Alert
- Update MSS incident record
- Close MSS incident

### Use Case #1: Investigating and Mitigating Cyber-attacks

Integrated with Symantec MSS, ATAR periodically collects new incidents and update the statuses of the open incidents as they change in Symantec MSS system. When an incident record is created on Symantec MSS, ATAR automatically collects Incident Details such as Analyst Comment, Signatures that are triggering this alert, Comments that are added to the incident and possible Attachments inside this alert and creates a new incident on its own Incident Management Service Desk.

## Configuration

## Prerequisites

- SOAR connects to Symantec MSS API via HTTPS. So access permission to <https://api.managedsecurity.com> is required.
- A user account and a certificate-password pair are required for ATAR to connect to Symantec MSS API.

## Configuring Symantec MSS

The Symantec MSS service uses client-side certificates for authentication.

1. Click **Profile > Certificates > Create a certificate.**
2. Select the **type of service** for the certificate.
3. Set the expiration date for the certificate. The available values are 6 months, 1 year, and 2 years.
4. [Optional] Specify the name for the certificate.
5. Click **Register.**



The certificates are enabled by default upon creation, but must be downloaded and installed before they can be used.

## Configuring SOAR

To use the client-side certificate created on Symantec MSS, you must convert it with **openssl** command line tool as following:

```
openssl pkcs12 -in <certificate_created_in_MSS_Portal>.p12 -clcerts -nodes -out <output_file>
```

## Configuring Credentials

1. Click **Configuration > Credentials > Create Credential.**
2. Specify the following parameter values in the **Credential Editor**:
3. **Internal Credential**

Parameter	Value
Type	Internal Credential
Name	Display name of credential set (For example, Symantec MSS Credentials)).
Username	Empty
Password	Empty.
Private Key	Paste the content of the <output_file>.pem file into the Private Key area.



The external credential stores can not be used with this integration type.

## Configuring Symantec MSS as Alert Source

1. To add a new incident severity configuration, click **Configuration > Incidents > Severities**.

Symantec MSS integration requires the following incident severity definitions:

- Informational
- Warning
- Critical
- Emergency

2. To add a new incident statuses configuration, click **Configuration > Incidents > Statuses**.

Symantec MSS integration requires the following incident status definitions:

- New
- In Progress as Open statuses
- False Positive
- Resolved
- Deferred
- No Action as closed statuses.

3. Click **Configuration > Alert Source > Create Alert Source Configuration**.

4. Specify the following parameter values in the **Configuration** form:

Parameter	Value
Name	Display name of Symantec MSS Alert Source on SOAR
Type	Symantec MSS
Address	Address of Symantec MSS service ( in the following format: <a href="https://api.monitoredsecurity.com">https://api.monitoredsecurity.com</a> ).
Alert Severities	Mapping of alert severity values to SOAR incident severities.

Parameter	Value
Configuration	<pre>Specify the following configuration parameters: # Enables incident sync # Default: false #incident.autoSync=true # Request timeout in minutes # If not provided, ATAR will use 10 by default #request.timeout=10 # Enable auto closing ATAR incidents when the related Symantec MSS incident is closed, # Default: false #incident.autoClose=true # Enable auto reopening ATAR incidents when the related Symantec MSS incident is reopened, # Default: false #incident.autoReopen=true # Scope fields to be extracted from base events and/or correlated events (field1:CATEGORY:ROLE, # CATEGORY is any of: EMAIL_ADDRESS, HASH, HOST, MAC_ADDRESS, NETWORK_ADDRESS, # COMPUTER_NAME, UNKNOWN, URL, USERNAME, PROCESS # ROLE is any of: OFFENDER, IMPACT, RELATED # # Note: The fields in the baseevent.scope example below are always extracted by default. # Note: Extraction with same field name overrides the default one. # Note: Extraction with different field name does not override the default behaviour and extracted # Note: Field names must start with / character # # Example: baseevent.scope=/sourceIPString:NETWORK_ADDRESS:OFFENDER # baseevent.scope= # # Example: correlated.scope=/sourcev6:NETWORK_ADDRESS:OFFENDER # correlated.scope= # How far (in days) into the past ATAR will look for remote incidents at the initial sync task # If not provided, ATAR will use 14 days by default #days.to.look.back.at.initial.sync=14</pre>
Credential	Name of the credential set you have created (For example, Symantec MSS Credentials).
Trust Invalid SSL Certificates	Select this if Engine's certificate is self-signed or is not recognized by browsers
Visible Alert Fields	Select alarm fields that has to be displayed on Incident Management Service Desk.
Notify	Select user(s) from the list to notify when ATAR performs an action on this integration.

5. Click **Test** to test the integration.
6. Click **Save** to complete the integration.

## Configuring Symantec MSS as an Integration

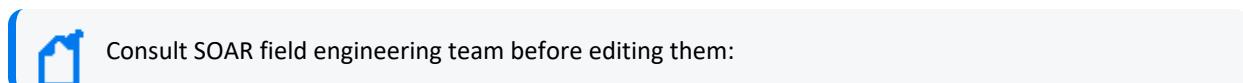
1. Click **Configuration > Integrations > Create Integration**.
2. Specify the following parameter values in the **Configuration** form:

Parameter	Value
Name	Display name of Symantec MSS integration on SOAR
Type	Symantec MSS
Address	Address of Symantec MSS service ( in the following format: <a href="https://api.monitoredsecurity.com">https://api.monitoredsecurity.com</a> ).
Configuration	Specify the following configuration parameters: <code>#proxy.id=5422</code>
Credential	Name of the credential set you have created (For example, ArcSight ESM Credentials).
Trust Invalid SSL Certificates	Select this if Engine's certificate is self-signed or is not recognized by browsers
Require Approval From	Select user(s) from list to ask her/his approval before executing actions on this integration.
Notify	Select user(s) from the list to notify when ATAR performs an action on this integration.

3. Click **Test** to test the integration.
4. Click **Save** to complete the integration.

## Additional Notes

The following configuration parameters can be used for fine tuning the integration.



Parameter Name	Description	Default Value
SymantecMssListenerMaxRetrySeconds	Symantec MSS listener queue max message retry in seconds	1800
SymantecMssListenerQueueConcurrency	Upper limit of Symantec MSS Listener consumer thread count	3
SymantecMssSyncLookBehindMinutes	Minutes to look behind to incident in Symantec MSS SyncTask	20

SymantecMssListenerMaxRetrySeconds	Symantec MSS listener queue max message retry in seconds	1800
SymantecMssListenerQueueConcurrency	Upper limit of Symantec MSS Listener consumer thread count	3
SymantecMssSyncLookBehindMinutes	Minutes to look behind to incident in Symantec MSS SyncTask	20

SymantecMssSyncPeriod Period in seconds to sync Symantec MSS incidents 60  
Below Automation Bit sample could be used to automatically close incidents via Trigger.

```
atar.require("underscore");
var remoteStatusList = [
'False Positive',
'Resolved',
'Deferred',
'No Action'
];
var remoteStatus = 'Resolved';
var statusName = atar.getTicket().getTicketStatus().getName();
if (_.contains(remoteStatusList, statusName)) {
remoteStatus = statusName;
}
var params = {'INCIDENT_CLOSING_STATUS': remoteStatus};
atar.action(ActionPluginCapability.CLOSE INCIDENT, atar.getAlert(),
atar.device("Symantec MSS Integration"), params);
```

# Integration Guide for Symantec Messaging Gateway

## Integration Overview

Symantec Messaging Gateway (Brightmail) is an email gateway which is used to filter incoming and outgoing emails. This integration has been tested with Symantec Messaging Gateway 10.6.5-1 version.

## Integration Capabilities

SOAR has the following integration capabilities with Symantec Messaging Gateway:

- Block Sender
- Block in Dictionary

### Use Case: Blocking phishing attacks

SOAR can follow the email inboxes for user's phishing reports and automatically creates an incident record on its service desk. To stop the phishing campaigns, SOAR can extract the sender address, IP, e-mail subject and block them on Symantec Messaging Gateway.

This can be performed automatically within a playbook or manually by an analyst.

## Configuration

### Prerequisites

- SOAR connects to Symantec Messaging Gateway via HTTPS. Access to 443/tcp port is required.
- A user account for SOAR to connect Symantec Messaging Gateway.

### Configuring Symantec Messaging Gateway

1. Click **Administration > Users** and select **Create a new administration policy** to create an administrator account. Select **Manage Policies** right.  
Disable all other rights since they are unnecessary.
2. Click **Content > Dictionaries** to create a dictionary.

3. To block hosts and IP addresses, SOAR uses **Local Bad Sender IPs** and **Local Bad Sender Domains**.

## Configuring SOAR

1. Navigate to **Configuration > Credentials** and click **Create Credential**.

2. Fill the **Credential Editor** form with following parameter values:

- a. **Internal Credential:**

Parameter	Value
Type	Internal Credential
Name	Display name of credential set (For example, Symantec Messaging Gateway Credential)
Username	Username you have created of SOAR on Symantec Messaging Gateway
Password	Password of the user you have created of SOAR on Symantec Messaging Gateway.
Private Key	Empty

- b. **Credential Store**

Parameter	Value
Type	External Credential
Name	Name of the credential with full path of the safe on store

3. Click **Configuration > Integrations > Create Integration**.

4. Fill the configuration form with the following parameter values:

Parameter	Value
Name	Display name of Symantec Messaging Gateway integration on SOAR.
Type	Symantec Messaging Gateway.
Address	Address of the integration (the format must be 192.168.2.212).)
Configuration	You need to specify the following configuration parameters. You can define multiple dictionaries by separating " ", for example, dictionary.name=SOAR Dictionary 1   SOAR Dictionary 2
Credential	Name of the credential set you've just created on step 2 (for example, Symantec Messaging Credential).

Parameter	Value
Trust Invalid SSL Certificates	Select this if Symantec Messaging Gateway's certificate is self-signed or not recognized by browsers.
Require Approval From	Select user(s) from list to ask her/his approval before executing actions on this integration.
Notify	Select user(s) from the list to notify when SOAR performs an action on this integration.

5. Click **Test** to test the integration.
6. Click **Save** to complete integration.

# Integration Guide for Tenable Nessus

## Integration Overview

Tenable Nessus is a vulnerability scanner used to detect vulnerabilities on the network. SOAR uses Tenable Nessus to gather vulnerability information to enrich incidents' context.

## Integration Capabilities

- Action
- Get Scan List
- Get All Vulnerabilities on a Scan

## Configuration

### Configuring Tenable Nessus

- SOAR connects to Tenable Nessus' API via HTTPS. Therefore SOAR must be able to connect this service.
- A user credential is required.

### Configuration on SOAR

#### Configuring SOAR

1. Navigate to **Configuration > Integrations**.
2. In the **Integrations Editor**, specify the following parameter values:

Parameter	Value
Name	Display name of Tenable Nessus integration on SOAR
Type	Tenable Nessus.
Address	Address of the integration (in the following format: http[s]://1.1.1.1:1234 or http [s]://abc.example.com:1234
Credential	Credential defined for the integration under the <b>Credentials</b> menu

Parameter	Value
Trust Invalid SSL Certificates	Select this if Engine's certificate is self-signed or is not recognized by browsers
Require Approval From	Select users from the list who can provide approval before executing actions on this integration
Notify	Select users from the list to notify when SOAR performs an action on this integration

3. Click **Test** to test the integration.
4. Click **Save** to complete the integration.

# Integration Guide for Tenable Security Center

## Integration Overview

Tenable Security Center (Tenable SC) is a vulnerability management solution that provides visibility into network by identifying all vulnerabilities, misconfigurations and malware attack on assets and gives ability to manage and measure your cyber risk.

SOAR has the following integration capabilities with Tenable Security Center:

- Get Assets
- Get Vulnerabilities (System-wide)
- Get Vulnerabilities on IP

### **.Use Case: Getting vulnerability details of assets**

SOAR can integrate with Tenable Security Center to gather additional information about an asset during incident investigation. Knowing existing vulnerabilities on a system can help SOC analysts to understand possible root cause of an incident more precisely.

## Configuration

### Prerequisites

- SOAR connects to Tenable Security Center's API using HTTPS. Typically an access permission to 443/tcp port is required.
- A user account for SOAR to connect to Tenable Security Center.

## Configuring Tenable Security Center

1. Login to Tenable Security Center with Security Manager User.



Note: This user account is different from admin account.

2. Navigate to **Users > Groups** and add a group to define the objects that SOAR can access. You must at select atleast one item from **Viewable Hosts and Repositories** lists.  
There is no need to share any object under **Share to Group** tab.
3. To add user for SOAR access, navigate to **Users > Users**. Select **No Role** and **SOAR Access Group** in **Membership**.

## Configuring SOAR

1. Navigate to **Configuration > Credentials** and click **Create Credential**.
2. Fill the **Credential Editor** form with following parameter values:
  - a. **Internal Credential:**

Parameter	Value
Type	Internal Credential
Name	Display name of credential set (For example, Tenable SC Credential)
Username	User you have created of SOAR on Tenable Security Center.
Password	Password of the user you have created of SOAR on Tenable Security Center.
Private Key	Empty

  
  3. Click **Configuration > Integrations > Create Integration**.
  4. Fill the configuration form with the following parameter values:
 

Parameter	Value
Name	Display name of Tenable Security Center integration on SOAR.
Type	Tenable Security Center.
Address	Address of the integration (the format must be https://1.1.1.1:1234 or https://abc.example.com:1234)
Credential	Name of the credential set you've just created on step 2 ( for example, Tenable SC Credential).
Trust Invalid SSL Certificates	Select this if Engine's certificate is self-signed or not recognized by browsers.
Require Approval From	Select user(s) from list to ask her/his approval before executing actions on this integration.
Notify	Select user(s) from the list to notify when SOAR performs an action on this integration.
  5. Click **Test** to test the integration.
  6. Click **Save** to complete integration.

# Integration Guide for Trend Micro Apex Central

## Integration Overview

**Trend Micro Apex Central** is a web-based console that provides centralized management for Trend Micro products and services at the gateway, mail server, file server and corporate desktop levels.

## Integration Capabilities

- Quarantine

## Prerequisites

- Access to the HTTPS is needed as ArcSight SOAR connects to Trend Micro Apex Central API through this service.

## Configuring Trend Micro Apex Central

1. Login to Trend Micro Apex Central and navigate to **Administration** tab.
2. Click **Settings < Automation API Access Settings** and add a new application as follows:

The screenshot shows the 'Automation API Access Settings' page in the Trend Micro Apex Central interface. The 'Enable application integration using Apex Central Automation APIs' checkbox is checked. The 'Application Access Settings' section contains the following information:

- Application name: SOAR
- Application ID: 017D4FE3-0440-49E0-A25F-76731FB99193
- API key: E44E37D7-3E02-4EF5-9F71-4C08D2959396
- API type: Isolate/Restore endpoint connections
- Communication time-out: 120 seconds

At the bottom of the form are 'Save' and 'Cancel' buttons.

3. Note down the **Application ID** and **API Key** (for your reference later) after saving the

application as follows:

The screenshot shows the 'Automation API Access Settings' page in Trend Micro Apex Central. At the top, there's a navigation bar with links like Dashboard, Directories, Policies, Threat Intel, Response, Detections, Administration, Help, and Trend Micro Vision One. Below the navigation bar, the page title is 'Automation API Access Settings'. A sub-header states: 'Automation API access settings allow third-party programs to integrate with Apex Central through use of public APIs.' There are two main sections: 'Application Name' and 'API Key'. Under 'Application Name', there's a table with one row containing 'SOAR' in the 'Application Name' column, '017D4FE3-0440-496D-A25F-76731FB99193' in the 'Application ID' column, and a long hex string in the 'API Key' column. Both the 'Application ID' and 'API Key' columns are highlighted with red boxes.

## Configuring SOAR

1. Click **Configuration > Credentials > Create Credentials**.
2. Specify the following parameter values in the **Credential Editor**:

### **Internal Credential:**

Parameter	Value
Type	Internal Credential
Name	Display name of credential set (For example, Trend Micro Apex Central Credentials)
Username	Empty
Password	Application ID that you've noted from created application.
Private Key	API Key that you have noted before from the created application.

3. Click **Configuration > Integrations > Create Integration**.

Specify the following parameter values in the **Configuration** form.:

Parameter	Value
Name	Display name of Trend Micro Apex Central integration on SOAR
Type	Trend Micro Apex Central
Address	Address of the integration (the format must be ( <a href="https://czbxlz.manage.trendmicro.com">https://czbxlz.manage.trendmicro.com</a> )
Credential	Name of the credential set that you created on step 2. (For example, Trend Micro Apex Central Credentials).

Parameter	Value
Trust Invalid SSL Certificates	Select this if Trend Micro Apex Central's certificate is self signed or it is not recognized by browsers.
Require Approval Form	Select user(s) from list who can provide approval before executing actions on this integration.
Notify	Select user(s) from the list to notify when SOAR performs an action on this integration.

4. Click **Save** to save the integration definition.
5. Navigate to **Configuration>Customization Library** and edit **Trend Micro Apex Central Advanced Action Script Default Script Template**.
6. Select the integration that you have added to **Integrations** menu.
7. Click **Save** to complete the integration.
8. Click **Test**, an **Integration Successful** message is displayed if the credential and address are valid

## Capabilities

### Quarantine

Action capability for quarantine a Hostname, IP address and MAC addresss.

- Rollback: Yes
- Duplicate Control: No

Input Parameter	Description	Type	Scope	
			Restricted	Required
<b>Rollback Mode</b>	Time to rollback this action. Default is no-rollback.	N/A	N/A	No
<b>MAC Address / Network Address / Hostname</b>	MAC Address/Network Address/Hostname to quarantine	MAC Address Network Address Hostname	Yes	Yes

Output:

Case Scope: N/A

Human Readable Output: N/A

# Integration Guide for Trend Micro Vision One

## Integration Overview

**Trend Micro Vision One** is a purpose-built threat defense platform that provides added value and new benefits beyond XDR solutions, allowing you to see more and respond faster.

## Integration Capabilities

ArcSight SOAR has the following integration capabilities with Trend Micro Vision One:

- Get Observed Attack Techniques
- Query Operating Systems
- Get Exception List
- Get Suspicious Object List
- Add Objects to Suspicious Object List
- Add Objects to Exception List
- Delete Objects from Suspicious Object List
- Delete Objects from Except List
- Prerequisites

You must have access to HTTPS as the ArcSight SOAR connects to Trend Micro Vision One to API through this service.

## Configuration

### Configuring Trend Micro Vision One

1. Login to the **Vision Platform** and create a user with the **Master Administrator** role and **Trend Micro Vision One™ console and APIs** access level.
2. Get access token of the created user that is used as a credential on ArcSight SOAR.

# Configuring SOAR

1. Click **Configuration > Credential > Create Credential**.
2. Specify the following parameter values in the **Credential Editor** form.

Type	Name	Username	Password	Private Key
Internal credential	Display name of credential set (for example, Trend Micro Vision One Credential).			Bearer<space><access-token>

3. Click **Configuration > Integrations > Create Integration**.
4. Specify the following parameter values in the **Configuration** form.

Parameter	Value	
Name	Display name of the integration.	
Type	Trend Micro Vision One.	
Address	URL of API (for example, <a href="#">API trend micro</a> ).	
Configuration	Specify the following configuration parameters:	
	<b>cache.reusing.duration</b>	Configure how far (in minutes) into the past this enrichment will look. For example: <code>cache.reusing.duration=20</code> .
	<b>proxy.id</b>	ID of the proxy integration when you access Trend Micro Vision One through a web proxy device. For example, <code>proxy.id = 12345</code> .
Credential	Credential that has been defined for this integration under the <b>Credentials</b> menu.	
Trust Invalid SSL Certificates	Select this if web server's certificate is self-signed or is not recognized by browsers.	
Require Approval From	Select user(s) from list to ask the approval before executing actions on this integration.	
Notify	Select user(s) from the list to notify when SOAR performs an action on this integration.	

5. Click **Save** to save the integration definition.
6. Navigate to **Configuration>Customization Library** and edit **Trend Micro Vision One Advanced Action Script Default Template**.
7. Select the integration that you have added to **Integrations** menu.
8. Click **Save** to complete the integration.
9. Click **Test**, an **Integration Successful** message is displayed if the credential and address are valid.

# Capabilities

## 1. Get Observed Attack Techniques

Enrichment capability for getting observed attack techniques.

The following table presents the **Get Observed Attack Techniques** action capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Integration</b>	Name of the third party integration.	Integration	No	Yes
<b>Risk Levels</b>	Single or comma seperated risk values (high, critical, low, info, undefined, medium).	Text	No	No
<b>Tactic IDs</b>	Single or comma seperated tactid id values .	Text	No	No
<b>Technique IDs</b>	Single or comma seperated technique id values.	Text	No	No
<b>Name Filter</b>	Detection Filter name .	Text	No	No
<b>Endpoint Name</b>	Name of the endpoint.	Computer Name, Host, Keyword, Unknown	Yes	No
<b>Time Range</b>	Time range for attack times.	Time Range	No	Yes

### Output:

Case Scope:

Action	Type	Category/ Value
Add	Scope Item	Keyword (Related)

### Human Readable Output:

Detected Time	Associated Endpoint	Risk Level	Detection Filter	Description	Tactic	Technique	Highlighted Details
2023-09-09T11:00:00Z	W32 Process[2023-09-09T11:00:00Z]	Info	System Network Config Discovery via WMI	Detected attempt of benign compromise - T1587	T1584	[1] Microsoft Windows WMI Activity	
2023-09-09T11:00:00Z	W32 Process[2023-09-09T11:00:00Z]	Info	Service Execution via Service Control Manager	Service Control Manager Command-line executed a process	T1541-002	[1] Command/Control [Exploitation]	
2023-09-09T11:00:00Z	W32 Process[2023-09-09T11:00:00Z]	Info	Execution of Windows Command Line Interface	Windows Command Line Interface command-line executed in the session	T1584-002	"cmd"	
2023-09-09T11:00:00Z	W32 Process[2023-09-09T11:00:00Z]	Info	System Network Config Discovery via WMI	Detected attempt of benign compromise - T1587	T1584	[1] Microsoft Windows WMI Activity	
2023-09-09T11:00:00Z	W32 Process[2023-09-09T11:00:00Z]	Info	Service Execution via Service Control Manager	Service Control Manager Command-line executed a process	T1541-002	[1] Command/Control [Exploitation]	
2023-09-09T11:00:00Z	W32 Process[2023-09-09T11:00:00Z]	Info	Execution of Windows Command Line Interface	Windows Command Line Interface command-line executed in the session	T1584-002	"cmd"	
2023-09-09T11:00:00Z	W32 Process[2023-09-09T11:00:00Z]	Info	System Network Config Discovery via WMI	Detected attempt of benign compromise - T1587	T1584	[1] Microsoft Windows WMI Activity	

## 2. Query Operating Systems

Enrichment capability for operating system information for all agents active in the last seven days.

The following table presents the **Query Operating Systems** action capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Integration</b>	Name of the third party integration.	Integration	No	Yes

**Output:**

Case Scope:

Action	Type	Category/ Value
<b>Add</b>	Scope Item	Keyword (Related)

Human Readable Output:

Count
0

**3. Get Exception List**

Enrichment capability for information about domains, file SHA-1 values, IP addresses, or URLs that are in the Exception List.

The following table presents the **Get Exception List** action capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Integration</b>	Name of the third party integration.	Integration	No	Yes
<b>Type</b>	Single or comma seperated types ("domain", "ip", "sha1", "url").	Text	No	No

**Output:**

Case Scope:

Action	Type	Category/ Value
<b>Add</b>	Scope Item	Keyword (Related)

Human Readable Output:

Type	Value	Description	Last Modified
domain	cominsurancefraud.com	malicious social URL domain	2023-08-05T14:42:45Z
url	http://cominsurancefraud.com	fake insurance website	2023-08-05T14:42:45Z

**4. Get Suspicious Object Lists**

Enrichment capability for information about domains, file SHA-1 values, IP addresses, or URLs that are in the Suspicious Object List

The following table presents the **Get Suspicious Object** action capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Integration</b>	Name of the third party integration.	Integration	No	Yes
<b>Type</b>	Single or comma seperated types ("domain", "ip", "sha1", "url").	Text	No	No
<b>Content Filter</b>	Filters the list to suspicious objects that exactly match the specified string.	Text	No	No

**Output:**

Case Scope:

Action	Type	Category/ Value
<b>Add</b>	Scope Item	Keyword (Related)

Human Readable Output:

Type	Name	Score	Time Action	Risk Level	Min Threat	Last Modified	Engaged Time
URL	URL:1.ME.TG	Medium	Block	High	Low	2023-08-09T14:15:00Z	2023-08-09T14:15:00Z
URL	http://www.123456789.com	Medium	Block	High	Low	2023-08-09T14:15:00Z	2023-08-09T14:15:00Z
URL	http://www.123456789.com	Medium	Block	High	Low	2023-08-09T14:15:00Z	2023-08-09T14:15:00Z
URL	http://www.123456789.com	Medium	Block	High	Low	2023-08-09T14:15:00Z	2023-08-09T14:15:00Z
URL	http://www.123456789.com	Medium	Block	High	Low	2023-08-09T14:15:00Z	2023-08-09T14:15:00Z

**5. Add Objects to Suspicious Object List**

Action capability for Adding domains, file SHA-1 values, IP addresses, or URLs to the Suspicious Object List.

- Rollback: Yes
- Duplicate Check: No

The following table presents the **Add Objects to Suspicious Object List** action capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
<b>Rollback Mode</b>	Time to rollback this action. Default is no-rollback.	Relative Time	No	No
<b>Value</b>	The value of the suspicious object which will be added.	Host, Network Address, Hash, URL	Yes	Yes
<b>Description</b>	Record description info.	Text	No	No

Input Parameter	Description	Type	Scope Restricted (Yes/No)	Required (Yes/No)
<b>Scan Action</b>	Suspicious object record scan action, when not set, use system default settings. Risk Level. Type's scan action.	Enum	No	No
<b>Risk Level</b>	Suspicious object risk level when not set, use default value - high.	Enum	No	No
<b>Expired Day</b>	Suspicious object record expired day, when not set, use system default settings. Expired Day.	Text	No	No

**Output:**

Case Scope:

Action	Type	Category/ Value
Add	Scope Item	Keyword (Related)

Human Readable Output: N/A

**6. Add Objects to Exception List**

Action capability for Adding domains, file SHA-1 values, IP addresses, or URLs to the Exception List and prevents these objects from being added to the Suspicious Object List.

- Rollback: Yes
- Duplicate Check: No

The following table presents the **Add Objects to Exception List** action capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Rollback Mode</b>	Time to rollback this action. Default is no-rollback.	Integration	No	Yes
<b>Value</b>	Suspicious object record value,it support full match or partial match, DOMAIN partial match: (with a wildcard before 1st, example, example.com) IP partial match: (ip range example, 200.102.35.1-200.102.35.254,cidr example: 200.102.35.1/24) URL Partial match: (support wildcard 'http://.', 'https://.' at beginning, or '' at the end, or both two wildcards, example, https://.example.com/path1/) SHA1 (only full match).	Text	No	No
<b>Description</b>	Exception description info.	Text	No	No

**Output:**

**Case Scope:**

Action	Type	Category/ Value
Add	Scope Item	Keyword (Related)

Human Readable Output: N/A

**7. Delete Objects from Exception List**

Action capability for Deleting domains, file SHA-1 values, IP addresses, or URLs from the Exception List.

- Rollback: Yes

- Duplicate Check: No

The following table presents the **Delete Objects from Exception List** action capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Rollback Mode</b>	Time to rollback this action. Default is no-rollback.	Relative Time	No	No
<b>Value</b>	Suspicious object record exception value.	Host, Network Address, Hash, URL	Yes	Yes

**Output:****Case Scope:**

Action	Type	Category/ Value
Add	Scope Item	Keyword (Related)

Human Readable Output: N/A

**8. Delete Objects from Suspicious Object List**

Action capability for Deleting domains, file SHA-1 values, IP addresses, or URLs from the Suspicious Object List:

- Rollback: Yes
- Duplicate Check: No

The following table presents the **Delete Objects from Suspicious Object List** action capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Rollback Mode</b>	Time to rollback this action. Default is no-rollback.	Relative Time	No	No
<b>Value</b>	Suspicious object record exception value.	Host, Network Address, Hash, URL	Yes	Yes

**Output:**

Case Scope:

Action	Type	Category/ Value
Add	Scope Item	Keyword (Related)

Human Readable Output: N/A

# Integration Guide for Turkcell Threat Intelligence

## Integration Overview

Turkcell Threat Intelligence is a service which lets users to query reputation of Indicators of Compromise such as data leakage, brand protection, and vulnerability modules.

## Integration Capabilities

ArcSight SOAR has the following integration capabilities with Turkcell Threat Intelligence:

- Domain Query
- Email Query
- Hash Query
- IP Query

### Use Case: Investigating Phishing Campaigns

SOAR integrates with Turkcell Threat Intelligence or Bozok to investigate and mitigate phishing campaigns. SOAR extracts the indicators such as sender address, IP address, and URLs from a phishing report email of the user and creates a new incident on the Incident Management Service Desk. SOAR then checks with Turkcell Threat Intelligence or Bozok if this is a known attack and previously analyzed. This investigation can either be performed automatically within a playbook or manually by an analyst.

## Configuration

### Prerequisites

- Access to <https://bozok.turkcell.com.tr> (443/tcp port) as SOAR connects to Turkcell Threat Intelligence/Bozok API through HTTPS
- An API key for SOAR to connect to Turkcell Threat Intelligence/Bozok service

### Configuration on Turkcell Threat Intelligence or Bozok

- No specific configuration is needed on Turkcell Threat Intelligence or Bozok.

## Configuring SOAR

1. Click **Configuration > Credentials > Create Credential**.
2. Specify the following parameter values in the **Credential Editor form**:

**a. Internal Credential:**

Parameter	Value
Type	Internal Credential
Name	Display name of credential set (For example, Turkcell Threat Intelligence Credentials)
Username	Empty
Password	Empty
Private Key	API key obtained from the service provider

**b. Credential Store:**

Parameter	Value
Type	External credential
Name	Name of the credential with full path of the safe on store

3. Click **Configuration > Integrations > Create Integration**.
4. Specify the following parameter values in the **Configuration form**:

Parameter	Value
Name	Display name of Turkcell Threat Intelligence integration on SOAR
Type	Turkcell Threat Intelligence
Address	Address of Turkcell Threat Intelligence service(in the following format: (https://bozok.turkcell.com.tr))
Credential	Name of the credential set created (For example, Turkcell Threat Intelligence Credentials)
Trust Invalid SSL Certificates	Unselect

Parameter	Value
Configuration	<p>Specify the following configuration parameters:</p> <pre># Integration ID of the proxy integration to use when connecting to current integration. # If not provided, SOAR will try to use a direct connection. proxy.id=5434 # configure how far (in minutes) into the past this enrichment will look. cache.reusing.duration=60</pre>
Require Approval From	Not applicable as SOAR executes enrichment on Turkcell Threat Intelligence
Notify	Not applicable as SOAR executes enrichment on Turkcell Threat Intelligence

**Integration Editor**

Name *	Turkcell TI - Bozok
Type *	Turkcell Threat Intelligence / Bozok
Address *	https://bozok.turkcell.com.tr
Configuration	<pre># Integration ID of the proxy integration to use when connecting to current integration. # If not provided, ATAR will try to use a direct connection.  #proxy.id=123  # configure how far (in minutes) into the past this enrichment will look. #cache.reusing.duration=20</pre>
Credential *	Turkcell TI Credentials <span style="float: right;">▲ Create</span>
Trust Invalid SSL Certificates	<input checked="" type="checkbox"/>
Require Approval From	No selected principal
Notify	No selected principal
Tags	
<a href="#">Show additional parameters</a> <span style="float: right;"><b>Test</b> <b>Close</b> <b>Save</b></span>	

5. Click **Test** to test the integration.
6. Click **Save** to save the integration.

# Integration Guide for Udger

## Integration Overview

**Udger** is a query detection repository service that works for both cloud-based and local executions. Udger also provides Data Center name of given IP and many more.

## Integration Capabilities

ArcSight SOAR has the following integration capabilities with Udger:

- Parse

## Prerequisites

- You must have access to HTTPS as the ArcSight SOAR connects to [Udger API](#) through this service.
- API Token is needed to access Udger REST API.

## Configuration

### Configuring Udger

1. Login to [udger](#) and navigate to **Products > Cloud Parser**.

- Click **Subscribe Now**.
- Select **Subscription Package > Activate**.



Note: You can activate free package for the trial usage

- The access key is displayed in **My Account > General**



Note: Copy the access key as this is required during creating credential.

### Configuring SOAR

1. Click **Configuration > Integration > Create Integration**.
2. In **Configuration Editor**, select **Udger** in **List of Type**.

3. Navigate to **Credential** and click **Create** to create new credential. Specify following values in the **Credential Editor**:

Type	Username	Password	Private Key	Check
Internal Credential			<b>Access Key</b> that is copied from <b>Udger</b> web site (navigate to <b>My Account &gt; General</b> tab on <b>Udger</b> UI).	<b>Clear Text Access</b> checkbox.

4. Click **Save** to save the integration definition.
5. Navigate to **Configuration>Customization Library** and edit **Udger Advanced Action Script Default Template**.
6. Select the integration that you have added to **Integrations** menu.
7. Click **Save** to complete the integration.
8. Click **Test**, an **Integration Successful** message is displayed if the credential and address are valid.

## Capabilities

### 1. Parser

Parsing given IP and return JSON detail including Datacenter Name

The following table presents the **Parser** capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>IP</b>	A valid IP Address to retrieve data.	Network Address Host	Yes	Yes
<b>User Agent</b>	User Agent information to query on IP.	Unknown Keyword	Yes	No

### Output:

Case Scope:

Scope Item Property **Cloud Name** is added to the related scope item. When you click the related scope item to view its properties, a cloud name result is displayed.

The following table presents the case scope details:

Action	Type	Category/ Value
<b>Set</b>	Scope Item Property	Cloud Name

Human Readable Output:

Field	Value
ip_address_crawler_category	
ip_address_crawler_category_code	
ip_address_crawler_family	
ip_address_crawler_family_code	
ip_address_crawler_family_homepage	
ip_address_crawler_family_icon	
ip_address_crawler_family_info_url	
ip_address_crawler_family_vendor	
ip_address_crawler_family_vendor_code	
ip_address_crawler_family_vendor_homepage	
ip_address_crawler_last_seen	
ip_address_crawler_name	
ip_address_crawler_respect_robotsTxt	
ip_address_crawler_ver	
ip_address_crawler_ver_major	

# Integration Guide for Urlscan

## Integration Overview

The **URLscan** API allows you to submit URLs to scan, retrieve scan results, download Document Object Model (DOM) snapshots and page screenshots and search existing scans for different types of indicators.

## Integration Capabilities

ArcSight SOAR has the following integration capabilities with urlscan:

- Search Domain
- Search Hash
- Search IP
- Search URL
- Submit URL

## Configuration

### Prerequisites

- You must have access to HTTPS as the ArcSight SOAR connects to [urlscan io](#) API through this service.
- URLScan requires an API key for access.

## Configuring SOAR

1. Click **Configuration > Credential > Create Credential**.
2. Specify the following parameter values in the **Credential Editor** form:

Type	Name	Username	Password	Private Key
Internal credential	Display name of credential set (for example, URL Scan API Credential).	Empty	Empty	Access Token

3. Click **Configuration > Integrations > Create Integration**.
4. Specify the following parameter values in the **Configuration** form.

Parameter	Value	
Name	Display name of the integration.	
Type	Urlscan.io	
Address	Address of the integration (the format must be https://urlscan.io).	
Configuration	Specify the following configuration parameters:	
	<b>proxy.id</b>	ID of the proxy integration if you access Urlscan.io through a web proxy device. For example: proxy.id = 12345 .
Credential	Credential that has been defined for this integration in the <b>Credentials</b> menu.	
Trust Invalid SSL Certificates	Select this if web server's certificate is self-signed or is not recognized by browsers.	
Require Approval From	Select user(s) from list to ask the approval before executing actions on this integration.	
Notify	Select user(s) from the list to notify when SOAR performs an action on this integration.	

5. Click **Save** to save the integration definition.
6. Navigate to **Configuration>Customization Library** and edit **Urlscan Advanced Action Script Default Template**.
7. Select the integration that you have added in the **Integrations** menu.
8. Click **Save** to complete the integration.
9. Click **Test**, an **Integration Successful** message is displayed if the credential and address are valid.

## Capabilities

### 1. Search Domain

Enrichment capability for retrieving domain information for a relative time range.

The following table presents the **Search Domain** action capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Bucket Name</b>	Name of the third party integration.	Integration	N/A	Yes
<b>Domain</b>	Domain to be queried from Urlscan.	Hash	Yes	Yes

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
Relative Time Range	Specific relative time period that will be checked.	Time unit Hour (s) Day(s) Week(s) Month(s)	N/A	Yes

**Output:**

Case Scope:

Enrichment	Type	Category Value
None	N/A	N/A

## Human Readable Output:

**2. Search Hash**

Enrichment capability for retrieving hash information for a relative time range.

The following table presents the **Search Hash** action capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
Integration	Name of the third party integration.	Integration	N/A	Yes
SHA-256	SHA-256 hash value to be queried from Urlscan.	Hash	Yes	Yes
Relative Time Range	Specific relative time period that will be checked.	Time unit Hour (s) Day(s) Week(s) Month(s)	N/A	Yes

**Output:**

Case Scope:

Enrichment	Type	Category Value
None	N/A	N/A

## Human Readable Output:

Page_server	Page_url	Task_domain	Screenshot	Page_ip	Task_time	Result	Page_domain	Task_tags	Page_status	Indexedat	Task_url	Page_country
GitHub.com	https://xn--2vur9cm62vfndsgj7axn-6qq98bb3xu/	Iw0925520.git hub.io	https://urlscan.io/screenshots/55c24ba6-ce92-46fa-962c-d47edc977a.png	185.199.108.153	2021-01-29T20:44:23.905Z	https://urlscan.io/api/v1/result/55c24ba6-ce92-46fa-962c-d47edc977a/	178.254.22.2	xn--2vur9cm62vfndsgj7axn-6qq98bb3xu/	200	2021-07-04T08:20:10.634Z	https://Iw0925520.git hub.io/	US

### 3. Search IP

Enrichment capability for retrieving IP information for a relative time range.

The following table presents the **Search IP** action capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Integration</b>	Name of the third party integration.	Integration	N/A	Yes
<b>IP</b>	Network address to be queried from Urlscan.	Network Address	Yes	Yes
<b>Relative Time Range</b>	Specific relative time period that will be checked.	Time unit Hour(s) Day(s) Week(s) Month(s)	N/A	Yes

#### Output:

Case Scope:

Enrichment	Type	Category Value
None	N/A	N/A

#### Human Readable Output:

Page_server	Page_url	Task_domain	Screenshot	Page_ip	Task_time	Result	Page_domain	Task_tags	Page_status	Indexedat	Task_url	Page_country
Apache	https://178.254.22.2:422.238/	178.254.22.2	https://urlscan.io/screenshots/72fe1e25-72fe-43fd-b0a5-7cbe3ef5ab04.png	178.254.22.2	2021-09-29T08:06:27.855Z	https://urlscan.io/api/v1/result/72fe1e25-72fe-43fd-b0a5-7cbe3ef5ab04/	178.254.22.2	["kndprod"]	200	2021-09-29T08:06:34.176Z	https://178.254.22.2:422.238/	DE

### 4. Search URL

Enrichment capability for retrieving URL information for a relative time range..

The following table presents the **Search URL** action capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
<b>Integration</b>	Name of the third party integration.	Integration	N/A	Yes
<b>URL</b>	URL to be queried from Urlscan.	URL	Yes	Yes

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
Relative Time Range	Specific relative time period that will be checked.	Time unit Hour(s) Day(s) Week(s) Month(s)	N/A	Yes

**Output:**

Case Scope:

Enrichment	Type	Category Value
None	N/A	N/A

Human Readable Output:

Server	Url	Screenshot	Ip	Domain	Tags	Indexedat	Country
ATS/9.1.10.2 5	https://13.250.173.68/	https://urlscan.io/screenshots/2fd9b716-4619-4317-a7b5-436b3e737758.png	13.250.173.68	13.250.173.68	[ "nonprod" ]		SG

**5. Submit URL**

Enrichment capability for submitting a URL for investigation.

The following table presents the **Submit URL** action capability details:

Input Parameter	Description	Type	Scope Restricted (Yes/ No)	Required (Yes/ No)
Integration	Name of the third party integration.	Integration	N/A	Yes
URL	URL to be queried from Urlscan.	URL	Yes	Yes
Tag	User-defined tags to annotate this scan, for example, phishing or malicious. Limited to 10 tags.	String	N/A	No
Visibility	Submitting visibility option which could either be Public, Private or Unlisted	String Public Unlisted Private	N/A	Yes
Do not Use Cache	If this option is checked, SOAR does not use cached results.	Boolean	N/A	No

**Output:**

Case Scope:

Enrichment	Type	Category Value
None	N/A	N/A

Human Readable Output:

Field	Value
categories	
score	0
page_server	nginx
page_url	https://www.microfocus.com/en-us/home
page_asnname	AKAMAI-ASN1_NL
page_ptr	a104-126-37-176.deploy.static.akamaitechnologies.com
page_ip	104.126.37.176
page_domain	www.microfocus.com
page_asn	AS26940
page_country	DE
page_city	Frankfurt am Main

# Integration Guide for VirusTotal

## Integration Overview

VirusTotal inspects suspicious files and URLs to detect types of malware with over seventy antivirus scanners and URLs or domain blacklisting services, in addition to a myriad of tools to extract signals from the studied content.

## Integration Capabilities

SOAR has the following integration capability with VirusTotal:

- Domain Query
- Domain/Downloaded Files Query
- Domain/Subdomains Query
- Domain/URLs Query
- File Query
- Hash Query
- IP Query
- IP/Downloaded Files Query
- IP/Passive DNS Query
- IP/URLs Query
- URL Query

### Use Case: Blocking access to malicious URL

During the investigation of an attack, SOAR checks for suspicious IP addresses, URLs, files, and hash values to VirusTotal if these indicators are known and previously analyzed. According to returned confidence score, SOAR decides on the next course of action. This investigation can either be performed automatically within a playbook or manually by an analyst.

## Configuration

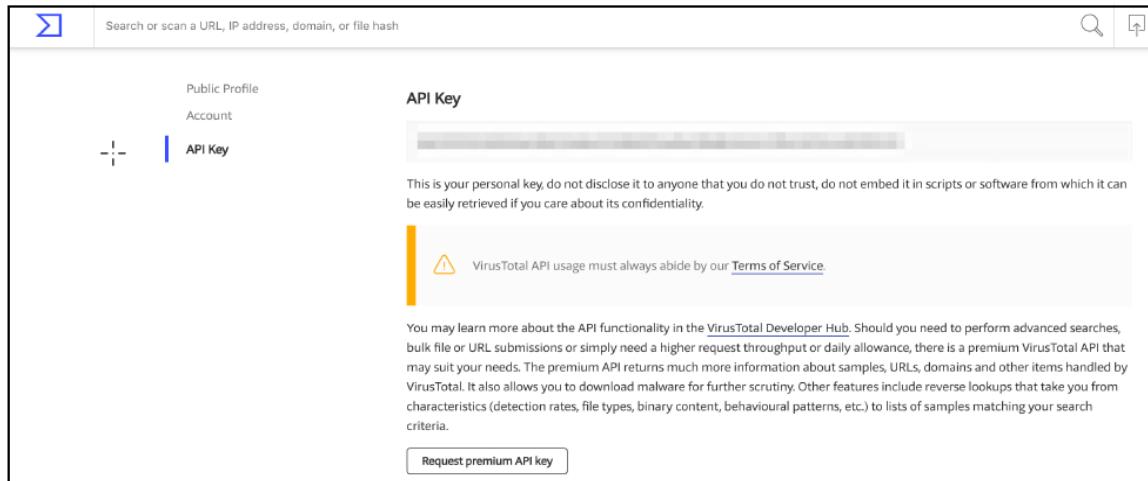
### Prerequisites

- VirusTotal API version 3
- Access to tcp port 443 as SOAR connects to VirusTotal API <http://www.virustotal.com>

- An API key for SOAR to connect to VirusTotal

## Configuring VirusTotal

- No specific configuration is needed on VirusTotal.
- Login to <https://www.virustotal.com> with your username and make a note of the API key under **Settings> API Key**.



## Configuring SOAR

1. Click **Configuration > Credentials > Create Credential**.
2. Specify the following parameter values in the **Credential Editor**:

### a. Internal Credential

Parameter	Value
Type	Internal Credential
Name	Display name of credential set (For example, VirusTotal Credentials)
Username	Empty
Password	Empty
Private Key	API Key you have on VirusTotal

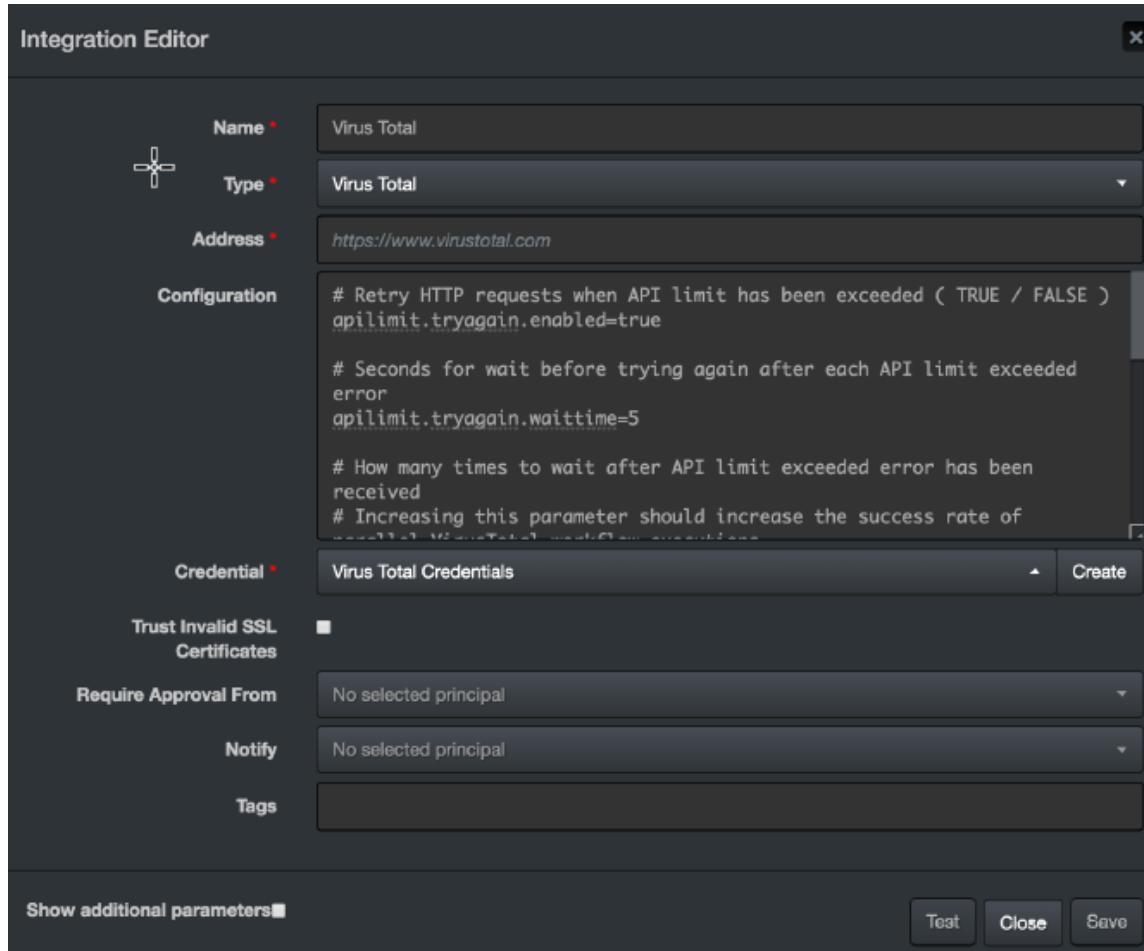
### b. Credential Store:

Parameter	Value
Type	External Credential
Name	Name of the credential with full path of the safe on store

3. Navigate to **Configuration > Integrations > Create Integration**.

4. Specify the following parameter values in the **Configuration form**:

Parameter	Value
Name	Display name of VirusTotal integration on SOAR
Type	VirusTotal
Address	Address of the integration (in the following format <code>https://www.virustotal.com</code> )
Configuration	<p>Specify the following configuration parameters:</p> <pre># Retry HTTP requests when API limit has been exceeded ( TRUE / FALSE ) apilimit.tryagain.enabled=true # Seconds for wait before trying again after each API limit exceeded error apilimit.tryagain.waittime=5 apilimit.tryagain.waittime=5 # How many times to wait after API limit exceeded error has been received # Increasing this parameter should increase the success rate of parallel VirusTotal workflow apilimit.tryagain.waitlimit=3 # Integration ID of the proxy integration to use when connecting to current integration. # If not provided, ATAR will try to use a direct connection. #proxy.id=123 # configure how far (in minutes) into the past this enrichment will look. #cache.reusing.duration=20 # Enrichment timeout duration after start time ( in seconds  ) scan.query.timeout=3600 # Expiration period of hash scans # If not provided, ATAR will use 30 days by default #scan.result.expiration.period.in.days=30 # VirusTotal APIv3 parameter # Limits page count for relation queries. SOAR will use 1 page by default #scan.result.page.count.max=1</pre>
Trust Invalid SSL Certificates	Unselect
Require Approval From	Not applicable
Notify	Not applicable



5. Click **Test** to test the integration.
6. Click **Save** to complete the integration.

## Additional Notes

- Domain and IP-related queries retrieve results in 40-item batches. For some IOCs, this may result in too many consecutive queries and long query-times.
- The file queries are limited to 32MB due to limits with VirusTotal API.
- Domain or URLs, Domain or Downloaded Files, IPor URLs, and IP or Downloaded Files only return the scope items with confidence score greater than 0.

# Integration Guide for VMware ESXi

## Integration Overview

SOAR uses VMware ESXi(Elastic Sky X integration) to perform some actions on the virtual machines (VMs).

## Integration Capabilities

### Action

- Create Snapshot of a VM
- Export VM
- Get Information of All VMs
- Power On VM
- Power Off VM
- Reset VM
- Reboot VM
- Standby VM
- Suspend VM

## Configuration

### Configuring VMware ESXi

- Access to HTTPs for SOAR to connect to VMware ESXi Server's SDK
- SOAR account with admin role

### Configuring SOAR

1. Navigate to **Configuration > Integrations**.
2. In the Integrations Editor, specify the following parameter values:

Parameter	Value
Name	Display name of VMware ESXi integration on SOAR
Type	VMware ESXi
Address	Address of the integration (in the following format: http[s]://1.1.1.1:1234[/sdk] or http[s]://abc.example.com:1234[/sdk])
Credential	Credential defined for the integration under the Credentials menu
Trust Invalid SSL Certificates	Select this if Engine's certificate is self-signed or is not recognized by browsers
Require Approval From	Select users from the list who can provide approval before executing actions on this integration
Notify	Select users from the list to notify when SOAR performs an action on this integration

**Integration Editor**

Name *	VMware ESXi
Type *	VMware ESXi
Address *	https://1.1.1.1:1234/sdk
Credential *	VMware ESXi <input type="button" value="Create"/>
Trust Invalid SSL Certificates	<input checked="" type="checkbox"/>
Require Approval From	No selected principal
Notify	No selected principal
Tags	
<input type="button" value="Show additional parameters"/> <input type="button" value="Test"/> <input type="button" value="Close"/> <input type="button" value="Save"/>	

3. Click **Test** to test the integration.
4. Click **Save** to complete the integration.

# Integration Guide for VxStream Sandbox

## Integration Overview

VxStream Sandbox is an automated malware analysis system that includes the unique Hybrid Analysis technology. It is available as a standalone software package that is automatically deployed within your local infrastructure and operates without an external dependency or callback mechanism. It is possible to execute files on any Windows guest image (For example, a copy of your local workstation) and has a variety of integration and interface capabilities.

The feature set of VxStream Sandbox is extensive, with hundreds of generic indicators at its core. It detects unknown threats independent of Anti-Virus signatures. Empowered by Hybrid Analysis, the entire process memory gets analyzed using multiple timed snapshots, including the runtime sample. This feature allows the extraction of more indicators (Strings/API calls) regardless of execution. This approach enables the analysis of dormant code, evasive conditions, and extracts more valuable IOCs.

## Integration Capabilities

### Action

- Hash analysis

## Configuration

### Configuration on VxStream Sandbox

- Access to HTTPs for SOAR to connect to VxStream Sandbox

### Configuring SOAR

1. Navigate to **Configuration > Integrations**.
2. In the **Integrations Editor** window, specify the following parameter values:

Parameter	Value
Name	Display name of VxStream Sandbox integration on SOAR
Type	VxStream Sandbox
Address	Address of the integration (in the following format: <a href="https://www.hybrid-analysis.com">https://www.hybrid-analysis.com</a> )

Parameter	Value
Configuration	<p>Specify the following configuration parameters:</p> <pre># Integration ID of the proxy integration to use when connecting to # current integration. # If not provided, ATAR will try to use a direct connection. #proxy.id=123 # configure how far (in minutes) into the past this enrichment will look. #cache.reusing.duration=20</pre>
Credential	Credential defined for the integration under the Credentials menu
Trust Invalid SSL Certificates	Select this if Engine's certificate is self-signed or is not recognized by browsers
Require Approval From	Select users from the list who can provide approval before executing actions on this integration
Notify	Select users from the list to notify when SOAR performs an action on this integration

**Integration Editor**

Name *	VxStream Sandbox
Type *	VxStream Sandbox
Address *	https://www.hybrid-analysis.com
Configuration	<pre># Integration ID of the proxy integration to use when connecting to current integration. # If not provided, ATAR will try to use a direct connection.  #proxy.id=123  # configure how far (in minutes) into the past this enrichment will look. #cache.reusing.duration=20</pre>
Credentials *	VxStream Sandbox <span style="float: right;">Create</span>
Trust Invalid SSL Certificates	<input checked="" type="checkbox"/>
Require Approval From	No selected principal
Notify	No selected principal
Tags	
<a href="#">Show additional parameters</a> <span style="float: right;"><b>Test</b> <b>Close</b> <b>Save</b></span>	

3. Click **Test** to test the integration.
4. Click **Save** to complete the integration.

# Integration Guide for WinRM

## Integration Overview

This appendix provides a detailed, step-by-step configuration procedure to enable SOAR to properly work with WinRM.

## Configuration On Domain-Controller

- **To create a Group Policy object for your domain:**

1. Navigate to **Start > Control Panel**.
2. In the Control Panel, select **Administrative Tools > Group Policy Management**.
3. From the menu tree, click **Domains > [your domain's name]**.
4. Right-click and select **Create a GPO in this domain, and Link it here**.
5. Input **WinRM-SOAR**.
6. Execute the following command:

```
reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v LocalAccountTokenFilterPolicy /t REG_DWORD /d 1 /f
```

7. Click **OK**.

- **To edit the new Group Policy object you created:**

1. Right-click on the new WinRM-SOAR Group Policy Object and select **Edit**.
2. From the menu tree, click **Computer Configuration > Policies**.
3. In the **Policies**, click **Administrative Templates: Policy definitions > Windows Components > Windows Remote Management (WinRM)**.
4. Navigate to **WinRM Service**.



**Note:** After editing the Group Policy Object, three WinRM service settings are enabled.

- a. **To Allow remote server management through WinRM**

- i. Right-click either **Allow automatic configuration of listeners(Windows Server 2010)** or **Allow remote server management through WinRM(Windows Server 2012)**

- ii. Click **Edit**.
  - iii. To allow remote server management through WinRM, select **Enabled**.
  - iv. Enter an asterisk (\*) in each field.
  - v. Click **OK**.
- b. **To Allow unencrypted traffic through WinRM**
- i. Right-click **Allow unencrypted traffic** and click **Edit**.
  - ii. Select **Enabled** and click **OK**.

Now the Windows Remote Management is enabled on the Group Policy.

- c. **To Enable the Service that goes with it**
- i. In the **Group Policy Management Editor window**, click **Preferences > Control Panel Settings > Services**.
  - ii. Right-click **Services** and select **New > Service**.
  - iii. Select **Automatic** as the startup.
  - iv. Enter **WinRM** as the service name.
  - v. Select **Start service** as the service action.
  - vi. Select **This account** to log in as.
  - vii. Enter **NT AUTHORITY\NetworkService** as the user and use a space character as the password.
  - viii. Click **OK**.

• **To allow inbound remote administration by updating the firewall rules:**

The steps enable the following firewall rules:

- Windows Firewall: Allow inbound remote administration exception
- Windows Firewall: Allow ICMP exception

1. In the **Group Policy Management Editor**, click **Computer Configuration > Policies**.
2. Click **Administrative Templates: Policy definitions > Network > Network Connections > Windows Firewall > Domain Profile**.
3. Right-click **Windows Firewall: Allow inbound remote administration exception** and click **Edit**.
4. Select **Enabled**.
5. Enter an asterisk (\*) into each field and click **Ok**.

6. Right-click **Windows Firewall: Allow ICMP exception** and click **Edit**.
  7. Select **Enabled**.
  8. Select **Allow inbound echo request** and click **Ok**.
- To create a new inbound firewall rule and update the network list manager for unidentified networks:
    1. Click **Computer Configuration > Windows Settings > Security Settings > Windows Firewall with Advanced Security > Inbound Rules**.
    2. Right-click **Inbound Rules** and click **New Rule**.
    3. Select **Predefined**.
    4. Select **Windows Remote Management** from the list of services.
    5. Click **Next**.
    6. Unselect the entry profile **Public** and click **Next**.
    7. Click **Finish**.
    8. Right-click the new rule and click **Properties**.
    9. Click the **Advanced** tab and unselect all and select **Private**.
    10. Click the **Scope tab**.
    11. Check these IP addresses on Remote IP Address and specify IP address of the SOAR machine and click **OK**.
    12. From the menu tree, click **Computer Configuration > Windows Settings > Security Settings > Network List Manager Policies**.
    13. Right-click **Unidentified Networks** and click **Properties**.
    14. Select the **Location type to Private** and click **Ok**.

## Configuring SOAR

Use the format *username/Computer name* as WinRM credentials. For example, *localadmin/DEV-EXCHANGE18*.

## Configuring Domain-Controller for WinRM HTTPS Transport

1. Open the Certificate Authority management console.
2. Right-click **Certificate Templates** and select **Manage**.
3. In the template management console, scroll down and select **Web Server template**.
4. Right-click **Web Server Template**, select **Duplicate Template**.
5. In the **Certificate Property Window** for the new template, navigate to the **General Tab**.

**6. Set Display Name and Template Name to SOARWINRMHTTPS.**

**Note:** Use the same name without spaces. If there is a space that leads to a bug where the process to enroll a new certificate repeats.

7. In the **Subject Name** tab, select **Build from this Active Directory information**.
8. In the **Subject name format** select **Common Name** and select **DNS name**.
9. Click **Security** > specify the **Domain Computers** group for the domain. Allow Read, Enroll and Autoenroll and click **OK**.
10. In the **Certificate Authority management console**, right-click **Certificate Templates** and select **New Template**.
11. Double-click **SOARWINRMHTTPS** and close the window.
12. Navigate to **Start > Control Panel**.
13. Select **Administrative Tools** and **Group Policy Management**.
14. In the Menu tree, click **Domains > [your domain's name]**.
15. Create a batch script for starting WinRM HTTPS Listener named **SoarWinRMSSLStartupScript.ps1**.
16. Copy and paste the following code into **AtarWinRMSSLStartupScript.ps1**:

```
Start-Transcript C:\Scripts\transaction.log
$sysinfo = Get-WmiObject -Class Win32_ComputerSystem
$server = "{0}.{1}" -f $sysinfo.Name, $sysinfo.Domain
$LatestThumb = Invoke-Command -ScriptBlock {
    Get-ChildItem -Path Cert:\LocalMachine\My |
    where {$_.subject -match "CN=$server"} |
    Sort-Object -Property NotAfter -Descending |
    Select-Object -Last 1 -ExpandProperty Thumbprint
} -ErrorAction Stop
#If HTTPS Listener does not exist create Listener with quick config.Else evaluate
# available certificates ,sort them by expire date , select first thumbprint
$result=((Get-ChildItem -Path WSMAN:\localhost\Listener).keys) -match 'HTTPS'
if($result.Count -eq 0) {
    Set-WSManQuickConfig -UseSSL -Force
} else {
    Set-WSManInstance -ResourceURI winrm/config/Listener \
    -SelectorSet @{'Address=*';Transport="HTTPS"} \
    -ValueSet @{CertificateThumbprint=$LatestThumb.Thumbprint[1]}
    Restart-Service -Force -Name WinRM
}
Stop-Transcript
```

17. Navigate to **Start > Control Panel**.
18. Select Administrative Tools > Group Policy Management.
19. Right-click **WinRM-SOAR** and click **Edit**.
20. Click **Computer Configuration > Policies > Windows Settings > Security Settings > Public Key Policies**.
21. Double-click **Certificate Services Client - Auto-Enrollment**.
22. Set the **Configuration Model** to **Enable**.
23. Select **Renew expired certificates, update pending certificates, and remove revoked certificates**.and **Update certificates that use certificate templates**.
24. Click **Ok**.
25. Click **Computer Configuration > Policies > Windows Settings > Scripts**.
26. Double-click **Startup**.
27. In the **PowerShell Scripts**, click **Add> Browse** the file named **AtarWinRMSSLStartupScript.ps1**. and click **OK**.

## Force Group Policy Update

Use the following PowerShell commands to force a Policy Update as described in the command block:

```
$computers = Get-ADComputer -Filter *
$computers | ForEach-Object -Process {Invoke-GPUpdate -Computer $_.name \
-RandomDelayInMinutes 0 -Force}
```

## Additional Notes

The following patch must be applied to the target computer for WinRM to work without an error:

<https://support.microsoft.com/en-us/kb/2842230>

## Support

### Contact Information

Phone	A list of phone numbers is available on the Technical Support Page: <a href="https://softwaresupport.softwaregrp.com/support-contact-information">https://softwaresupport.softwaregrp.com/support-contact-information</a>
Support Web Site	<a href="https://softwaresupport.softwaregrp.com/">https://softwaresupport.softwaregrp.com/</a>
ArcSight Product Documentation	<a href="https://www.microfocus.com/documentation/arcsight/">https://www.microfocus.com/documentation/arcsight/</a>

# Send Documentation Feedback

If you have comments about this document, you can [contact the documentation team](#) by email. If an email client is configured on this computer, click the link above and an email window opens with the following information in the subject line:

## **Feedback on Integration Guides (SOAR 3.11 3.11)**

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to MFI-Documentation-Feedback@opentext.com.

We appreciate your feedback!