MANDIANT
NOW PART OF Google Cloud

Mandiant Security Validation Integrations Guide

NOVEMBER 15, 2023

Table of Contents

SECURITY VALIDATION

Every organization wants to be able to quickly and confidently know that their environment is unlikely to be compromised by the latest attack. Moreover, there is a need to quantify their security posture with data that clearly shows the effectiveness of their security controls. This data helps them establish a baseline, avoid security "drift," and maintain their defenses.

That's where Mandiant's Security Validation Solutions can help. Informed by Mandiant frontline threat intelligence on the latest attacker tactics, techniques, and procedures (TTPs), our solutions continuously validate and measure the effectiveness of your cybersecurity controls.

Security Validation Benefits

Security Validation helps you answer these critical questions:

- Can you be compromised?
- Are your cyber defenses working?
- Are you prepared for the next ransomware or cyber attack?

Here's how Security Validation can help:

- Capture data so you can be confident in your answers
- Gain greater visibility into your security architecture and threats that matter to quantify cyber security risk
- Pinpoint vulnerabilities in your security program that need immediate attention and continuous measurement of improvements over time
- Report evidence of our security effectiveness and prove the value of security investments
- Arm leadership with data to rationalize current and future investments

Operationalize Threat Intelligence

Security Validation starts with insight into what's most important to test against and how to optimize defenses based on Mandiant's knowledge of who and what is targeting your industry or peers. The Security Validation attack library represents thousands of attacks in every stage of the adversary attack lifecycle and is kept up to date with the latest known threats.

Emulate Real Attacks

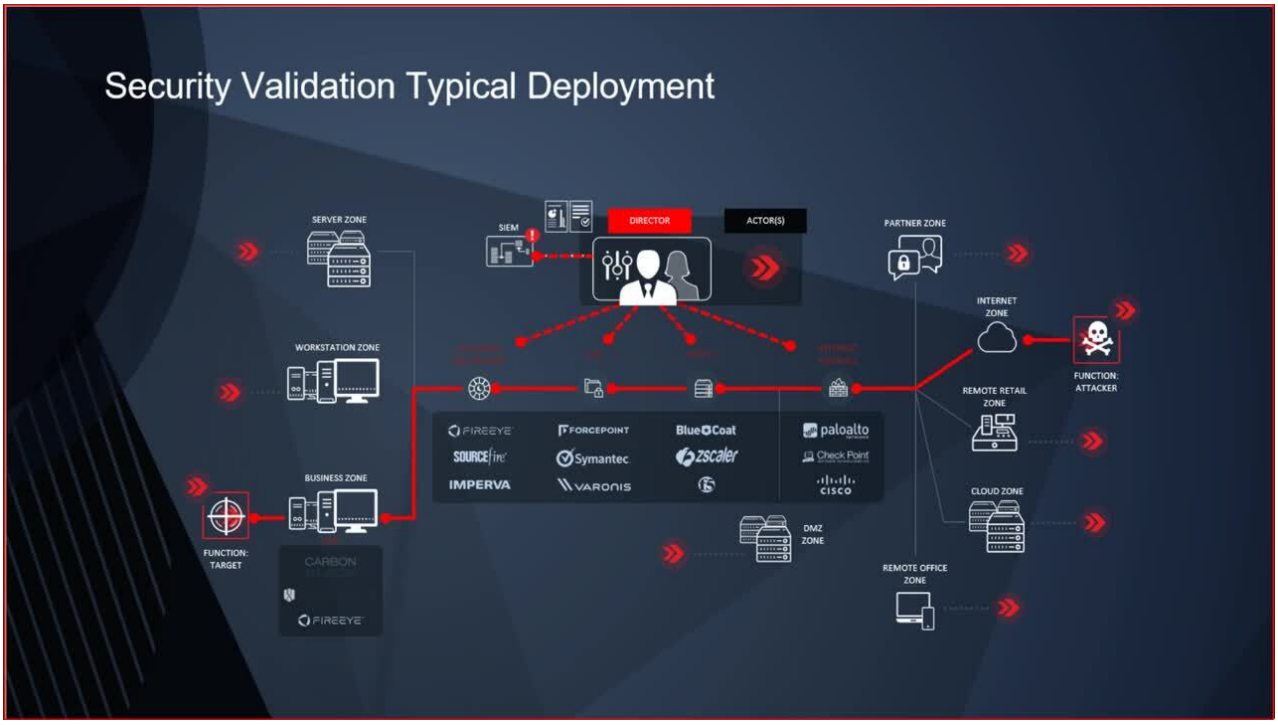
Mandiant's Security Validation infrastructure enables the emulation of real attack binaries and malware against your security environment. These tests are conducted safely, authentically, and provide a true test of effectiveness. Security Validation automates and offers a wide breadth and depth of attacker TTPs to test against the MITRE ATT&CK Framework and other industry-leading frameworks.

Quantify and Minimize Your Risk

Security Validation enables your team to make data-driven changes required to address gaps in security, misconfigurations, and redundancies. With Security Validation, your team can visualize which controls deliver the most value to your security architecture. Security teams can proactively implement and track improvements over time, optimize cyber defenses, and make the right investments in the future.

Mandiant **Security Validation** **(https://docs.mandiant.com/home/security-validation-on-prem-and-saas)** consists of two flavors, available in either an MSV (on-prem) or MA-SV (SaaS) version.

Video Overview



SECURITY VALIDATION: MSV (ON-PREM) AND MA-SV (SAAS)

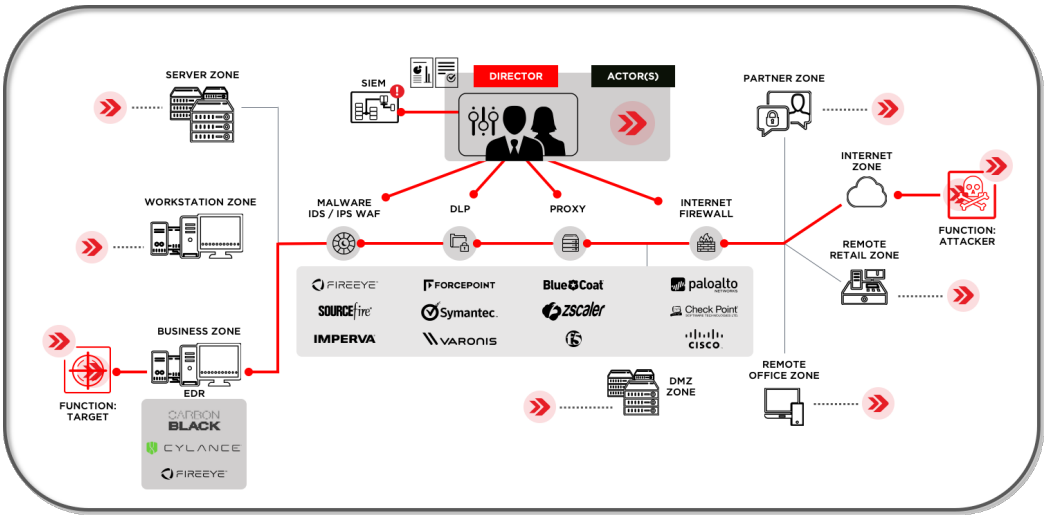
Our Security Validation platform is informed by Mandiant frontline threat intelligence on the latest attacker tactics, techniques, and procedures (TTPs) to continuously validate and measure the effectiveness of your cybersecurity controls.

Mandiant Advantage Security Validation safely processes advanced cyberattack security content within production networks. It's designed so that defenses respond to it as if an attack is taking place across the most critical areas of networks. The software produces evidence that shows how people, processes, and technologies perform when specific malicious behaviors are encountered, such as attacks by a specific threat actor or attack vector.

The core Validation components are:

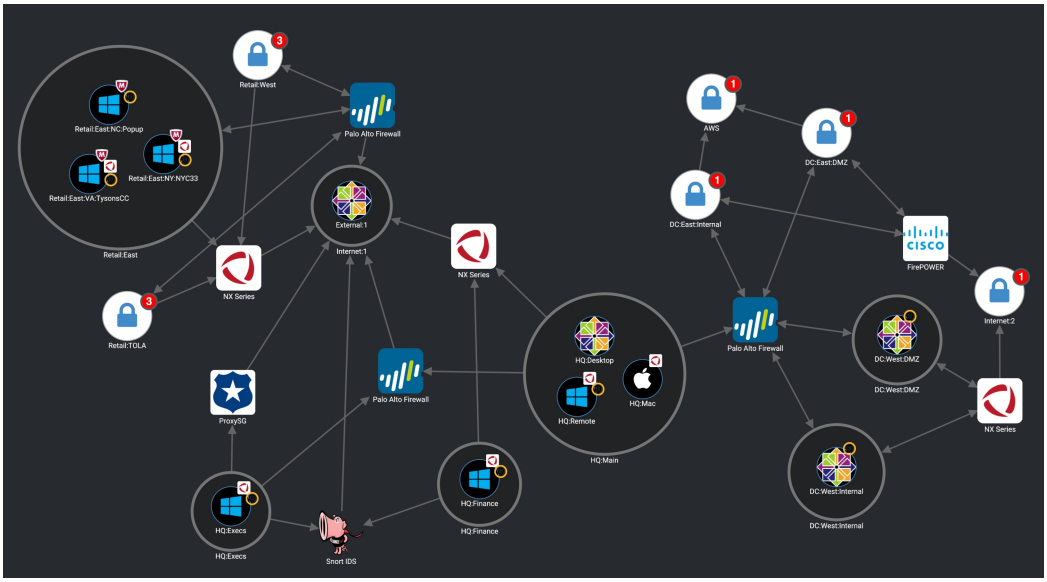
- The **Director**: The main component of the platform that provides the following functionality:
  - Acts as the Integration point for your SIEM and other components of your security stack
  - Hosts the Content Library (Actions, Sequences, Evaluations, and Files) used for testing your security controls
  - Manages the Actor assignment during testing
  - Aggregates testing results and facilitates report creation
  - Maintains connections with the Mandiant Updater and Content Services, letting you automatically receive updates to both the platform and its content
- **Actors** (also referred to as Flex, Endpoint, and Network Actors): The components that safely perform tests in production environments. Specifically, use Actors to verify the configuration and test the effectiveness of:
  - Network Security Controls
  - Windows, Mac, and Linux endpoint controls
  - Email controls

The following image provides an example of a common Validation Platform deployment in a customer environment. You can see where Actors have been deployed, what systems would potentially see the traffic for tests run between Actors, and how the Director is the component that receives the information from the systems in the environment based on an integration with a SIEM. The image also clearly shows that tests are run between Actors and not directly on systems in your environment.



Validation Platform running a test in an example environment

Once you have your environment configured and have started running tests, you are able to see your overall Validation Platform deployment and the security technologies that blocked and fired events when tests were run.



Validation Platform map

Outside the base Validation Platform deployment, there are additional features that may be included in your subscription or on-prem version of Security Validation. These features include:

- **Protected Theater**: Lets you safely run destructive endpoint tests
- **Email Theater**: Lets you run email-based tests
- **AEDA (Advanced Environmental Drift Analysis)**: Lets you continuously test your environment and provides early alerts for defensive regressions
- **TAAM (Threat Actor Assurance Module)**: Lets you operationalize your commercial threat intelligence platform
- **Cloud Validation Module**: Lets you test your cloud security controls

This feature is released in Limited Availability.
For more information, please contact your TSC or go to **https://www.mandiant.com/support**.

INTEGRATIONS OVERVIEW

This document applies to Classic Integrations. While the Integrations solution is available, it is no longer actively maintained. Mandiant recommends that you plan a switch to Preview Integrations so you can take advantage of the latest features and functionality. Preview Integrations configuration steps are provided in the Director web interface. For more details, see the **Preview Integrations Documentation** (https://docs.mandiant.com/home/msv-preview-integrations).

Need access to the Integration information offline? We've created a **PDF of all general available MSV Integration features** (https://docs.mandiant.com/help/download-full-pdf/id/620d7e13ccb103e8557b25b0/cid/637278c2057fb00b713611af). This was last updated July 17, 2023.

- Links in the Table of Contents will take you to a page in the PDF.
- Links in the body of the PDF will take you to the Mandiant Docs Portal (which requires you to sign in using your Mandiant Advantage credentials) or a page on the internet.
- If an image has a link, it takes you to a larger version of the image in the Mandiant Docs Portal.

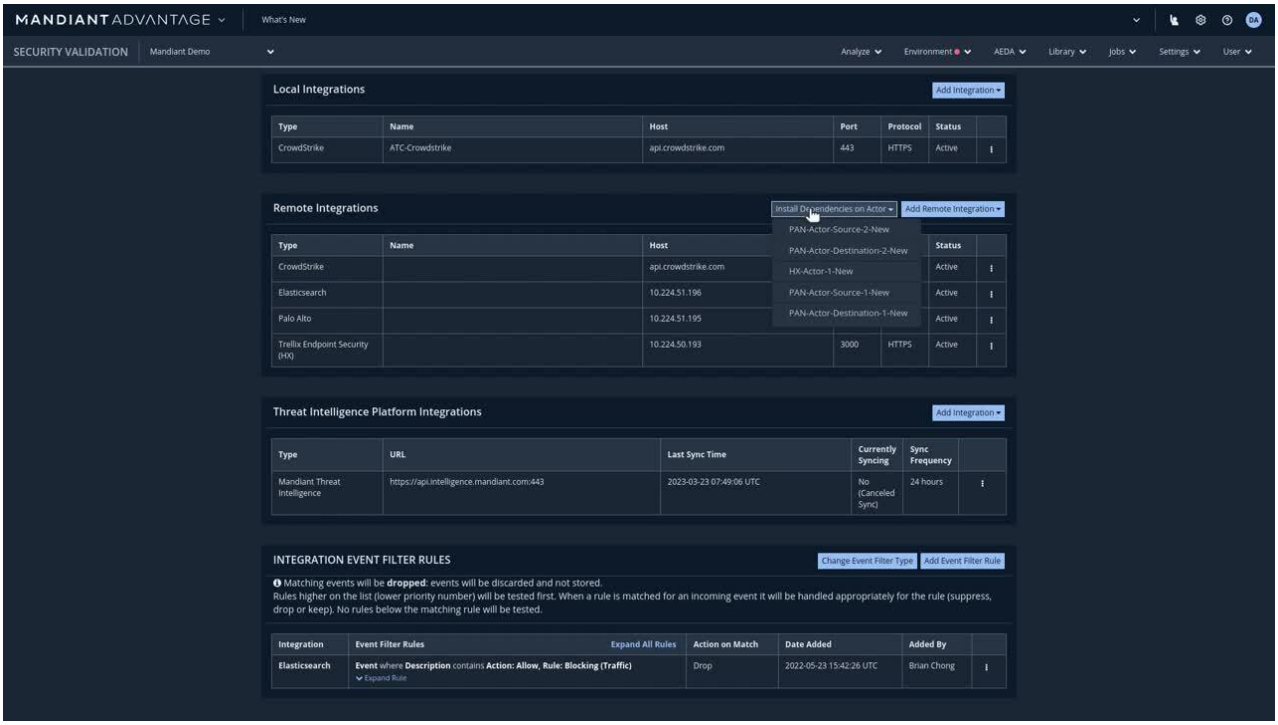
Integrations are a primary component of the Validation Platform. By integrating with security devices, the platform receives events that allow you to measure the effectiveness of those devices. You can integrate with the following types of security devices:

- Security information and event monitoring (SIEM) solutions
- Intrusion detection systems (IDS)
- Intrusion prevention systems (IPS)
- Firewalls
- Data loss prevention solutions (DLP)
- Log management platforms
- Threat Intelligence Platforms (TIPs)
- Threat Intelligence Feeds (TIFs)

The TIPs and TIFs are part of the Threat Actor Assurance Module (TAAM) and are used to pull in information for Threat Actors. For all others, the platform gathers empiric data on detections and event generation when Jobs are processed.

Mandiant Advantage Security Validation (MA-SV) has Integrations for over 50 different technologies. While all integrations have some shared configuration, there are differences. This includes available queries, variables that can be used, and fields used in mapping events from your technology to the integration in the platform. Non-SIEM integrations can also be identified as security technologies with prevention and detection settings. **Mandiant Advantage for Splunk** (https://docs.mandiant.com/home/ma-mandiant-advantage-for-splunk) can also be used with Security Validation, allowing you to view information from Security Validation directly in Splunk using the Security Validation Overview and Security Validation Details Dashboards.

This video walks you through configuring integrations in the Mandiant Advantage Security Validation (MA-SV) platform.



To help you with your integration configuration, the following topics are available:

- **Integration Queries Overview** (https://docs.mandiant.com/home/msv-integration-queries-overview)
- **Variables used in Integration Queries** (https://docs.mandiant.com/home/msv-variables-in-integration-queries)
- **Integrations - Field Details** (https://docs.mandiant.com/home/msv-integrations-field-details)

The following tables display important information about all integrations, organized by type (SIEM, Network, Endpoint, and TAAM). Information such as an integration's name, vendor, minimum supported version, remote capability, and proxy support capability, is included. Integration technologies may be listed in more than one table.

If the supported version/API is listed as "N/A", it means that the technology either does not have versions or that a specific version is not needed for the Security Validation integration to work. If the supported version/API is listed as "All", it means that all versions of the technology work with the Security Validation integration.

SIEM

Integration Name	Vendor	Supported Version/API	Remote Capable?	Proxy Support Local?[1]
AlertLogic (https://docs.mandiant.com/home/msv-alertlogic)	Alert Logic	APIv3	Yes	No
AlienVault (https://docs.mandiant.com/home/alienvault)	Alientvault	5.3.x	No	No
ArcSight (https://docs.mandiant.com/home/arcsight)	Micro Focus	6.8, 6.11	Yes	No

Integration Name	Vendor	Supported Version/API	Remote Capable?	Proxy Support Local?[1]
Microsoft Azure Log Analytics (https://docs.mandiant.com/home/msv-microsoft-azure-log-analytics)	Microsoft	APIv1	Yes	Yes*
Microsoft Azure Sentinel (https://docs.mandiant.com/home/msv-microsoft-azure-sentinel-2227)	Microsoft	APIv1	Yes	Yes*
Chronicle Backstory (https://docs.mandiant.com/home/msv-chronicle-backstory)	Chronicle	APIv1	No	Yes*
Cisco Firepower Management Center (FMC) (https://docs.mandiant.com/home/msv-cisco-firepower-management-center-fmc)	Cisco	5.5+	No	No
Devo (https://docs.mandiant.com/home/msv-devo)	Devo	APIv2	Yes	Yes
Elasticsearch (https://docs.mandiant.com/home/msv-elasticsearch)	Elastic	5.x, 6.x, 7.x	Yes	No
Exabeam Data Lake (https://docs.mandiant.com/home/msv-exabeam-data-lake)	Exabeam	DL-i33.1	Yes	Yes*
Trellix Helix (https://docs.mandiant.com/home/msv-fireeye-helix)	Trellix	API v1	Yes	Yes*
Google BigQuery (https://docs.mandiant.com/home/msv-google-bigquery)	Google	API v2	No	No
Google Cloud Logging (https://docs.mandiant.com/home/msv-google-cloud-logging)	Google	API v2	No	No
Graylog (https://docs.mandiant.com/home/msv-graylog)	Graylog	3.3.3+	Yes	Yes*
Juniper Secure Analytics (JSA) (https://docs.mandiant.com/home/msv-juniper-secure-analytics-jsa)	Juniper Networks	7.2.x, 7.3.x	Yes	No
LogRhythm Elasticsearch (https://docs.mandiant.com/home/msv-logrhythm-elasticsearch)	Logrhythm	7.2.x, 7.3.x	Yes	No
LogRhythm SQL (https://docs.mandiant.com/home/msv-logrhythm-sql)	Logrhythm	7.2.x, 7.3.x	No	No

Integration Name	Vendor	Supported Version/API	Remote Capable?	Proxy Support Local?[1]
LogZilla (https://docs.mandiant.com/home/msv-logzilla)	Logzilla	6.9+	Yes	Yes*
Trellix Enterprise Security Manager (https://docs.mandiant.com/home/msv-mcafee-enterprise-security-manager-esm)	Trellix	9.6.0, 10.1	Yes	No
RSA NetWitness Respond (https://docs.mandiant.com/home/msv-rsa-netwitness-respond)	RSA	N/A	Yes	Yes
IBM QRadar (https://docs.mandiant.com/home/msv-ibm-qradar)	IBM	7.2.x, 7.3.x, 7.5x	Yes	No
Securonix SNYPR (https://docs.mandiant.com/home/msv-securonix-snypr)	Securonix	Latest Version	Yes	Yes*
Splunk (https://docs.mandiant.com/home/msv-splunk)	Splunk	6.x+	Yes	Yes*
Splunk Enterprise Security (https://docs.mandiant.com/home/msv-splunk-enterprise-security)	Splunk	4.8.x+	Yes	Yes*
Sumo Logic (https://docs.mandiant.com/home/msv-sumo-logic)	Sumo Logic	19.x	Yes	Yes*
Threat Stack (https://docs.mandiant.com/home/msv-threat-stack)	Threat Stack	APIv2	Yes	Yes*

[1]If you see Yes* for Proxy support, it does not include Socks and NLTM.

Network

Integration Name	Vendor	Supported Version/API	Remote Capable?	Proxy Support Local?[2]
Check Point (https://docs.mandiant.com/home/msv-check-point)	Check Point	R71+	No	No
Cisco Firepower Management Center (FMC) (https://docs.mandiant.com/home/msv-cisco-firepower-management-center-fmc)	Cisco	5.5+	No	No
AWS CloudTrail (https://docs.mandiant.com/home/msv-aws-cloudtrail)	AWS	N/A	No	No

Integration Name	Vendor	Supported Version/API	Remote Capable?	Proxy Support Local?[2]
AWS CloudWatch (https://docs.mandiant.com/home/msv-aws-cloudwatch)	AWS	N/A	No	No
Darktrace (https://docs.mandiant.com/home/msv-darktrace)	Darktrace	N/A	Yes	Yes*
Exabeam Advanced Analytics (https://docs.mandiant.com/home/msv-exabeam-advanced-analytics)	Exabeam	N/A	Yes	Yes*
Trellix Network Security (NX) (https://docs.mandiant.com/home/msv-fireeye-integration)	Trellix	API v1.2; CMS >=7.6	Yes	Yes*
Trellix Email Security - Cloud (ETP) (https://docs.mandiant.com/home/msv-fireeye-etp)	Trellix	N/A	Yes	Yes
AWS GuardDuty (https://docs.mandiant.com/home/msv-aws-guardduty)	AWS	N/A	No	No
Trellix Network DLP (https://docs.mandiant.com/home/msv-mcafee-epo-dlp)	Trellix	15.x, 16.x	Yes	No
Palo Alto Networks Firewalls/Panorama (https://docs.mandiant.com/home/msv-palo-alto-networks-firewallspanorama)	Palo Alto	7.x - 10.x	Yes	Yes*
RSA NetWitness (https://docs.mandiant.com/home/msv-rsa-netwitness)	RSA	3.3.3.3	Yes	No
Security Onion - ELK (https://docs.mandiant.com/home/msv-security-onion-elk)	SecurityOnion	All	Yes	No
Security Onion - ELSA (https://docs.mandiant.com/home/msv-security-onion-elsa)	SecurityOnion	All	Yes	No
Symantec Data Loss Prevention (DLP) (https://docs.mandiant.com/home/msv-symantec-data-loss-prevention-dlp)	Symantec	All	No	No
Threat Stack (https://docs.mandiant.com/home/msv-threat-stack)	Threat Stack	API v2	Yes	Yes*

Integration Name	Vendor	Supported Version/API	Remote Capable?	Proxy Support Local?[2]
Tipping Point IDS/IPS (https://docs.mandiant.com/home/msv-tipping-point-idsips)	Trend Micro	4.1.x	Yes	Yes*
VMware AppDefense (https://docs.mandiant.com/home/msv-vmware-appdefense)	VMWare	API v1	Yes	Yes*

[2]If you see Yes* for Proxy support, it does not include Socks and NLTM.

Endpoint

Integration Name	Vendor	Supported Version/API	Remote Capable?	Proxy Support Local?[3]
Carbon Black CB Protection (https://docs.mandiant.com/home/carbon-black-cb-protection)	Carbon Black	API v1	Yes	Yes*
Carbon Black CB Response (https://docs.mandiant.com/home/msv-carbon-black-cb-response)	Carbon Black	>= 5.5	Yes	No
Carbon Black Cloud (https://docs.mandiant.com/home/msv-carbon-black-cloud)	Carbon Black	Alerts API v6	Yes	Yes*
Cisco Advanced Malware Protection (AMP) (https://docs.mandiant.com/home/msv-cisco-advanced-malware-protection-amp)	Cisco	API v1	Yes	Yes*
CrowdStrike (https://docs.mandiant.com/home/msv-crowdstrike)	Crowdstrike	API v3.x	Yes	Yes*
Cybereason (https://docs.mandiant.com/home/msv-cybereason)	Cybereason	16.x,17.x	Yes	Yes*
Cylance (https://docs.mandiant.com/home/msv-cylance)	Cylance	API v2	Yes	Yes*
Microsoft Defender Advanced Threat Protection (ATP) (https://docs.mandiant.com/home/msv-microsoft-defender-advanced-threat-protection-atp)	Microsoft	N/A	Yes	Yes*

Integration Name	Vendor	Supported Version/API	Remote Capable?	Proxy Support Local?[3]
Endgame (https://docs.mandiant.com/home/msv-endgame)	EndGame	API v1	Yes	Yes*
Trellix Endpoint Security (HX) (https://docs.mandiant.com/home/msv-fireeye-endpoint-security)	Trellix	API v1.2 ; CMS >=7.6	Yes	Yes*
Trellix Endpoint Security (https://docs.mandiant.com/home/msv-mcafee-epo)	Trellix	5.5+	Yes	Yes*
Trellix Network DLP (https://docs.mandiant.com/home/msv-mcafee-epo-dlp)	Trellix	5.5+	Yes	Yes*
Netskope (https://docs.mandiant.com/home/msv-netskope)	Netskope	78.1.0.333+	Yes	Yes*
Palo Alto Networks Cortex XDR (https://docs.mandiant.com/home/msv-palo-alto-networks-cortex-xdr)	Palo Alto Networks	API v1	Yes	Yes*
SentinelOne (https://docs.mandiant.com/home/msv-sentinelone)	SentinelOne	API v2	Yes	Yes*
Sophos Central (https://docs.mandiant.com/home/msv-sophos-central)	Sophos	API v1	Yes	No
Symantec Data Loss Prevention (DLP) (https://docs.mandiant.com/home/msv-symantec-data-loss-prevention-dlp)	Symantec	All	Yes	Yes*
Symantec Endpoint Protection (https://docs.mandiant.com/home/msv-symantec-endpoint-protection)	Symantec	14.x	Yes	No
Threat Stack (https://docs.mandiant.com/home/msv-threat-stack)	ThreatStack	API v2	Yes	Yes*
VMware AppDefense (https://docs.mandiant.com/home/msv-vmware-appdefense)	VMWare	API v1	Yes	Yes*

[3]If you see Yes* for Proxy support, it does not include Socks and NLTM.

Threat Intelligence Platforms and Feeds

Threat Intelligence Integrations are an important component of TAAM, allowing you to bring your threat intelligence information into the Validation Platform. Both threat intelligence Platforms (TIPs) and Threat Intelligence Feeds (TIFs) can be integrated, including:

Integration Name	Vendor	Supported Version/API
Anomali (https://docs.mandiant.com/home/msv-anomali)	Anomali	2.5.5+
CrowdStrike Intel (https://docs.mandiant.com/home/msv-crowdstrike-intel)	CrowdStrike	API V1 and V2
Mandiant Threat Intelligence (https://docs.mandiant.com/home/msv-mandiant-threat-intel)	Mandiant	API V4
Intel471 (https://docs.mandiant.com/home/msv-intel471)	Intel 471	N/A
Threat Connect (https://docs.mandiant.com/home/msv-threat-connect)	Threat Connect	API V2
Threat Quotient (https://docs.mandiant.com/home/msv-threat-quotient)	ThreatQuotient	N/A

These integrations focus on adversaries rather than Indicators of Compromise (IOCs), and are used to populate the Threat Actor Library. Through API calls, the Validation Platform collects information. The following adversary types are available for the integrations listed:

Threat Intelligence Integration	Threat Actor Group (Name)	Threat Actor (Malware)	Threat Actor Aliases	Threat Actor Country Data	Analyst Description	Tactics, Techniques, Procedures (TTPS)
Anomali	✔		✔	✔	✔	✔
CrowdStrike Intel	✔	✔	✔		✔	
Threat Connect	✔		✔	✔	✔	✔
Mandiant Threat Intelligence	✔		✔	✔	✔	✔
Intel471		✔			✔	

By default, threat intel Integrations sync every 24 hours. These times can be adjusted, with a minimum frequency of 15 hours. You can also manually sync if necessary, or pause the integration.

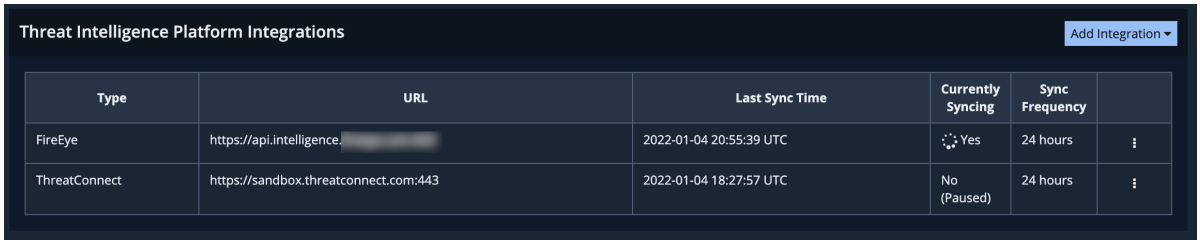
> Some TIPs and TIFs have rate limits, including daily limits, on their APIs, so you do not want to sync too often. If you have reached your rate limit and try to sync, the sync fails silently because the APIs do not provide notification that the rate limit has been met. If you try to sync and it does not allow you to, wait a few hours and try again. If you cannot wait, you can try using an API key tied to a different account since rate limits are often by user.

When your integration syncs the first time, two things occur:

- Threat Actor profiles are created

- Two types of TAAM-specific Evaluations are created: General TAAM Evaluations and Priority TAAM Evaluations. For more information about these Evaluations, see **TAAM Evaluations (https://docs.mandiant.com/home/taam-evaluations)**.For more information about these Evaluations, see the TAAM Guide.

TAAM-specific integrations are managed on the Integrations page. All integrations support proxy use. See the Admin guide for additional information on setting up the proxy assignment.



Threat Intelligence Platform Integrations table on Integrations Page

Remote Integrations

Installing the integration in the standard method doesn't always work because communication would be prevented by network boundary issues. In that case, you can configure a Remote Integration. Remote Integrations are integrations that are installed on a Security Validation Platform Actor that then communicate over a network boundary through an integrated proxy function.

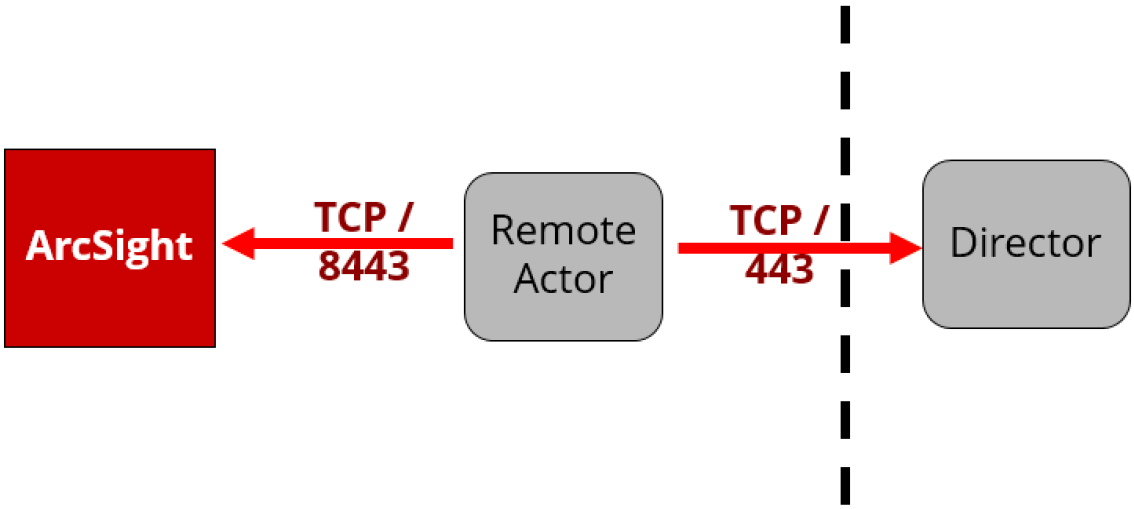
Prerequisites

Before an Actor can host a Remote Integration, a set of dependencies must be installed. You only see the button to install the dependencies if you have Actors that:

- Meet the requirements that follow for a Remote Integration
- Don't have the dependencies installed already

Only Actors installed from virtual appliances are capable of serving as a host for an integration. The Actor is required to:

- Be deployed as a Linux Network Actor OVA that has 2 CPUs, 8 GB RAM, and at least 50 GB disk space
- Communicate with the integration on its required API port
- Connect to the Director over HTTPS / 443
- Use Pull as the communication mode



Example of how traffic flows with Remote integrations

Any required updates to the integrations occur when the Actor is updated.

Change Actor Communication Mode

Once the Linux Network Actor is deployed and registered with the Director, you must change the communications mode for the Actor from “Push” to “Pull."

1. From the Director, go to **Environments** > **Actors**.
2. Click **more** ⋮ to the right of the Actor that is going to be a Remote Integration Actor and select **Edit**.
3. Change the Actor's **Comm mode** to **Pull**.
4. Click **Update Actor** to save the changes.

Install Dependencies on Actor

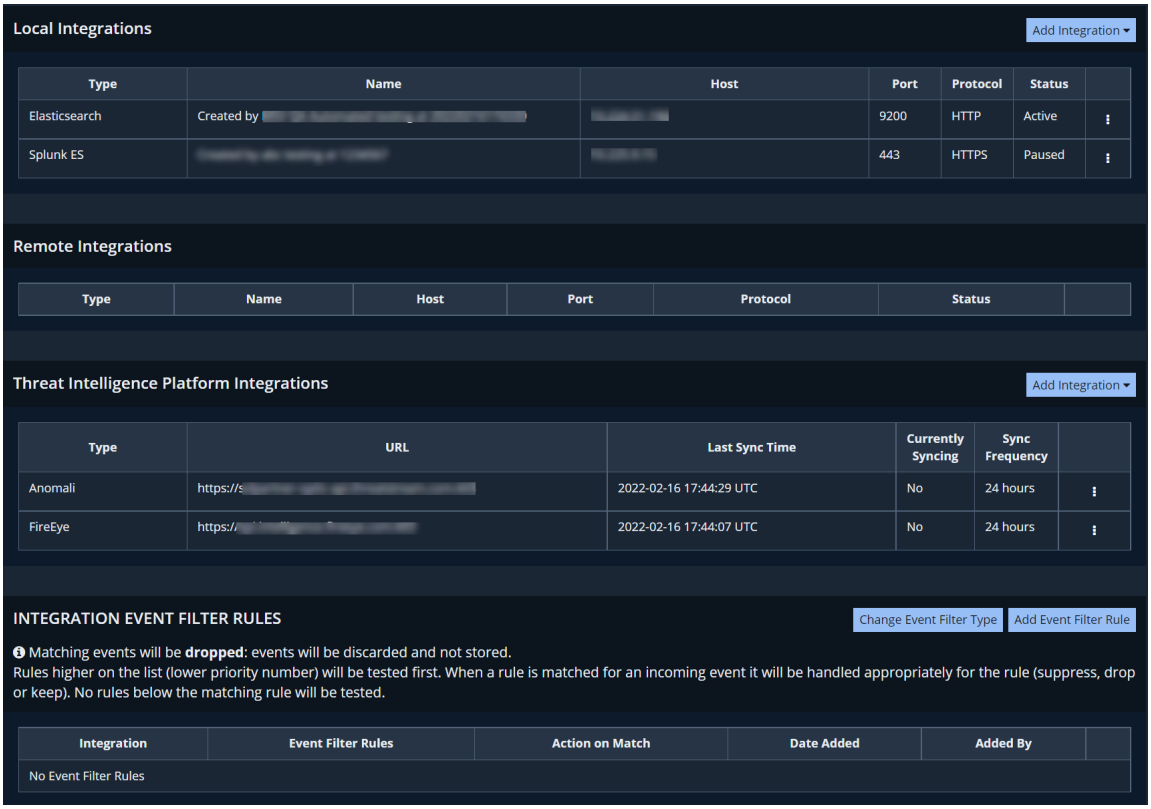
1. Go to **Settings** > **Integrations**.
2. Select **Install Dependencies on Actor**.
3. Select the Actor that you set up in the previous procedure and wait for the installation process to complete.
4. When you want to add an integration to MSV that is on-prem and not accessible directly by the Director, go to **Settings** > **Integrations**, and then select **Add Remote Integration**. When MSV queries that integration, the queries go through the Actor instead of the Director.

CONFIGURING & MANAGING INTEGRATIONS

> This document applies to Classic Integrations. While the Integrations solution is available, it is no longer actively maintained. Mandiant recommends that you plan a switch to Preview Integrations so you can take advantage of the latest features and functionality. Preview Integrations configuration steps are provided in the Director web interface. For more details, see the **Preview Integrations Documentation (https://docs.mandiant.com/home/msv-preview-integrations)**.

Access the Integrations area of the platform by going to **Settings** > **Integrations**. Here you will see all Local and Remote Integrations that you have configured.

When configuring the integrations, you can assign a name, allowing for easier identification if you have the same integration in multiple areas of your environment. This name is also used in various areas of the platform, such as looking at Detected Events for a Job.

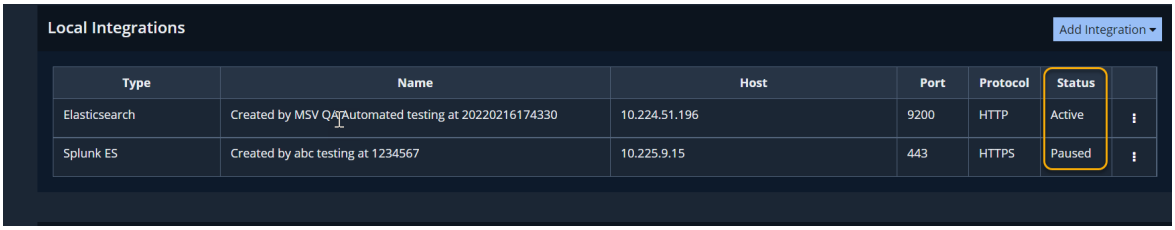


(https://d383cql5uq169w.cloudfront.net/app/image/pid/620d7e13ccb103e8557b25b0/id/629a12d5c9cba0017c2f7dc8/n/main-integrations.png)

Integrations

Use the vertical ellipses in the last column of each table to manage your Integrations in the Integration manager.

> You can quickly see whether an integration is "Paused" or "Active" in the Status column of the Local Integrations table.

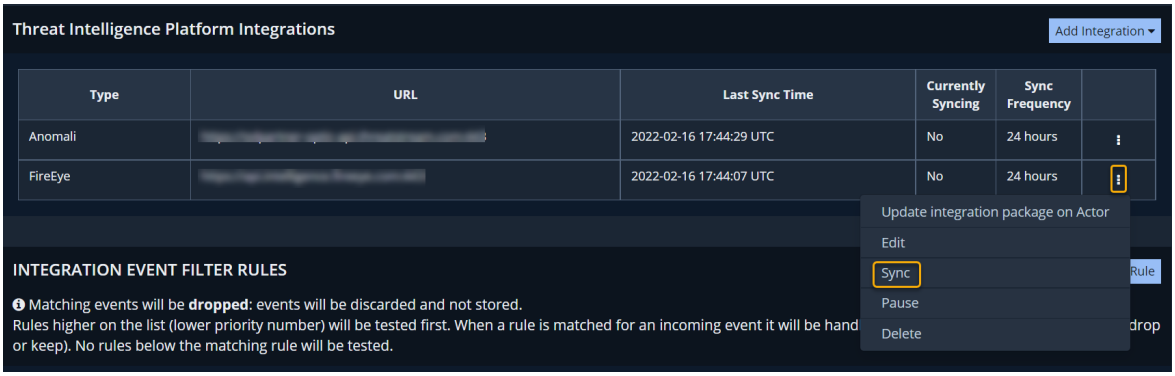


(https://d383cql5uq169w.cloudfront.net/app/image/pid/620d7e13ccb103e8557b25b0/id/629a12e5c9cba0017c2f7e6b/n/integrations-actions.png)

Status of Local Integrations

To sync an integration

1. Go to **Settings** > **Integrations**.
2. Locate the integration you want to sync in the appropriate table.
3. Click the vertical ellipses in the last column.
4. Click **Sync** in the drop-down list.
5. Wait for the sync to complete.



(https://d383cql5uq169w.cloudfront.net/app/image/pid/620d7e13ccb103e8557b25b0/id/629a12dfc9cba0017c2f7e31/n/integrations-sync.png)

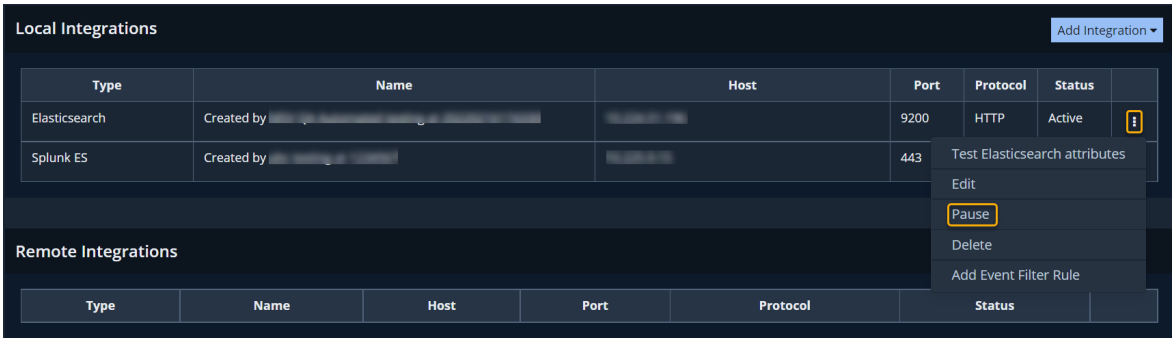
Syncing an Integration

Use the same process to update Cylance's device list.

To pause an integration

Pause an integration to prevent it from syncing but have it retain its information in our database.

1. Go to **Settings** > **Integrations**.
2. Locate the integration you want to pause in the appropriate table.
3. Click the vertical ellipses in the last column.
4. Click **Pause** in the drop-down list.



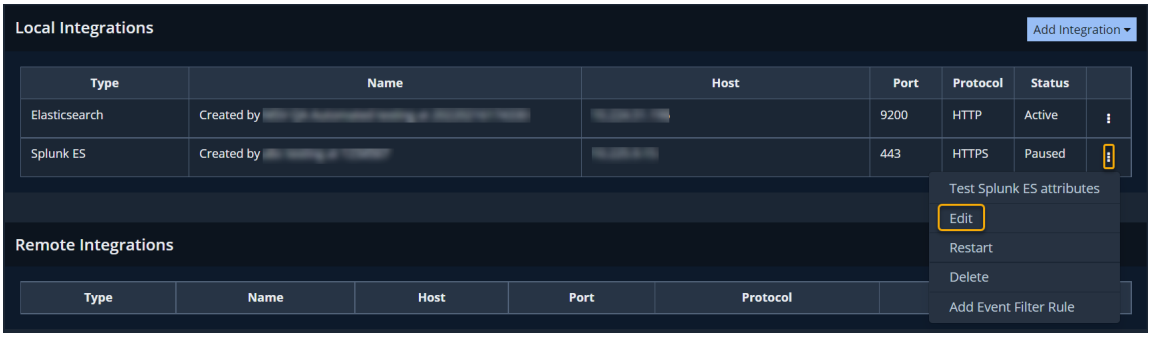
(https://d383cql5uq169w.cloudfront.net/app/image/pid/620d7e13ccb103e8557b25b0/id/629a12d6c9cba0017c2f7dcf/n/integrations-pause.png)

Pausing an Integration

When you are ready to have the integration running again, click the ellipses again; then click **Restart**.

To edit an integration

1. Go to **Settings** > **Integrations**.
2. Locate the integration you want to edit in the appropriate table.
3. Click the vertical ellipses in the last column.
4. Click **Edit** in the drop-down list.
5. Make changes as needed and click **Submit**.



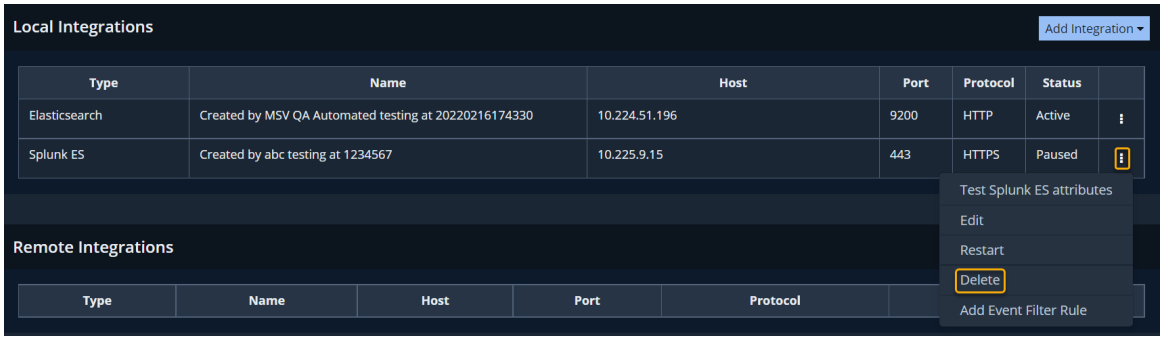
(https://d383cql5uq169w.cloudfront.net/app/image/pid/620d7e13ccb103e8557b25b0/id/629a12d7c9cba0017c2f7dd2/n/integrations-edit.png)

Editing an Integration

Use the Delete option to delete an integration that you no longer need.

To delete an integration

1. Go to **Settings** > **Integrations**.
2. Locate the integration you want to delete in the appropriate table.
3. Click the vertical ellipses in the last column.
4. Click **Delete** in the drop-down list. A message displays asking if you are sure you want to delete the integration.
5. Click **OK** to delete the integration. Click **Cancel** if you do not want to delete this integration.



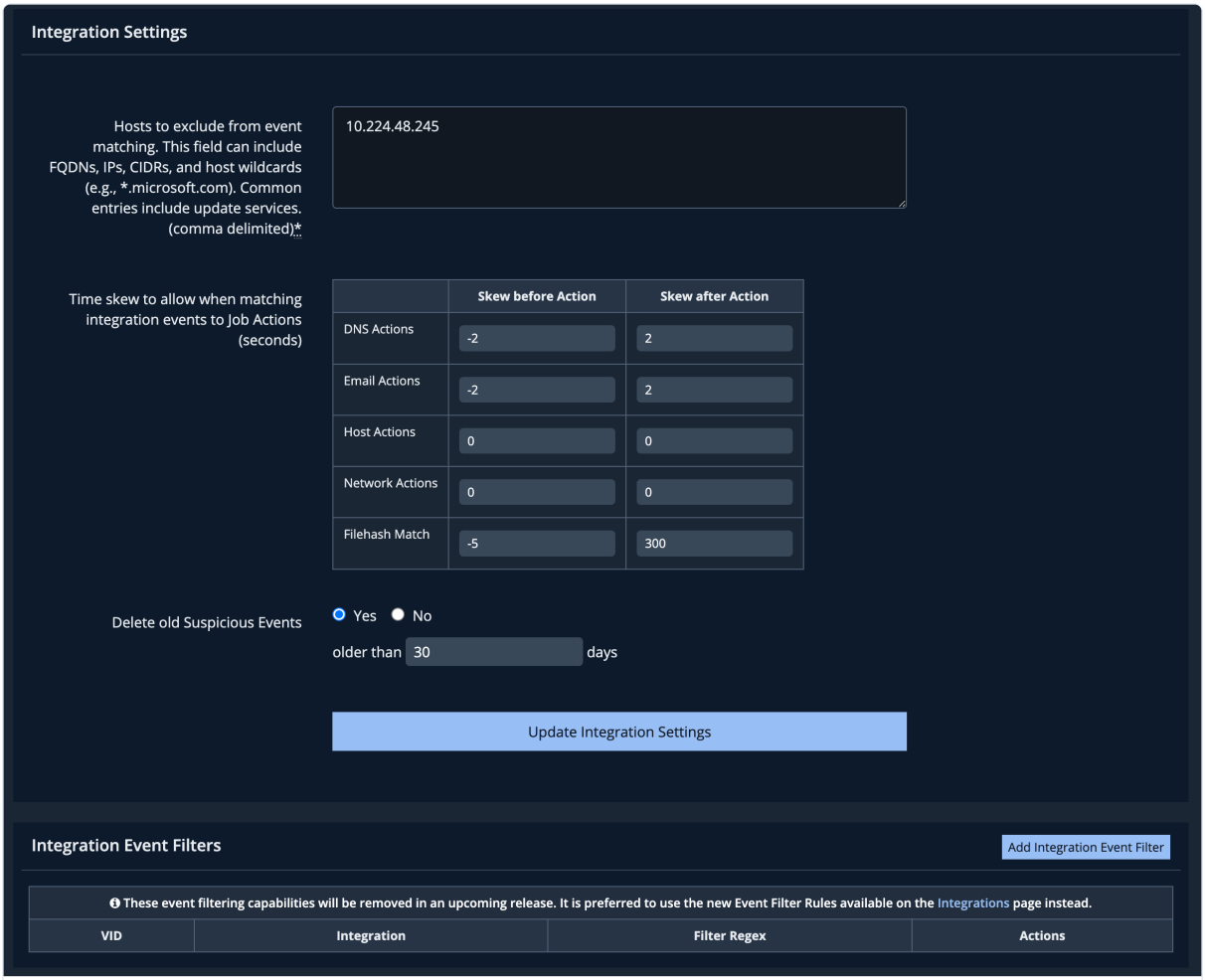
(https://d383cql5uq169w.cloudfront.net/app/image/pid/620d7e13ccb103e8557b25b0/id/629a12e1c9cba0017c2f7e3e/n/integrations-delete.png)

Deleting an Integration

Integrations Settings

There are some Integrations settings that can impact all the integrations in the platform. These are found on the Integration Settings page. On this page you can

- Add a list of hosts that you want to be excluded from event matching.
  - The Director IP is automatically added to the list.
  - You can add IP addresses, FQDNs, CIDRs, and Wildcard FQDNs. Separate the entries with commas.
- Define the time skew you want to use when matching integration events to specific types of Job Actions. This allows you to account for any variances you might see.
- Configure the settings for deleting Suspicious Events.
  This helps free up disk space and is more efficient than removing them from the Suspicious Events page.



Integrations Settings page

In addition to the above Integration settings, there is a section to add Integration Event Filters. This feature was deprecated so we no longer provide instructions on how to manage these. A new **Event Filter Rules (https://docs.mandiant.com/home/msv-event-filter-rules)** features replaces the event filters and is available on the main Integrations page of the platform.

Integrations & SSL Certificates

Valid SSL Certificates are not required for Integrations. Unless noted in the specific integration, SSL verification has been disabled for integrations.

CARBON BLACK CB RESPONSE

> This document applies to Classic Integrations. While the Integrations solution is available, it is no longer actively maintained. Mandiant recommends that you plan a switch to Preview Integrations so you can take advantage of the latest features and functionality. Preview Integrations configuration steps are provided in the Director web interface. For more details, see the **Preview Integrations Documentation (https://docs.mandiant.com/home/msv-preview-integrations)**.

This integration is remote capable.

Generate an API key for CB Response

The CB Response integration supports V1 and V2 of the Carbon Black API.

API tokens are tied to user accounts and inherit the user's privileges. When capturing the API key, use an account with the necessary privileges.

Read permissions are required, at minimum.

TO GENERATE AN API KEY

1. Access your profile by logging into the Carbon Black server, clicking your name, and choosing **Profile**.
2. Click the **API Token** link and copy your API token from the text box.

   Each user receives their own unique API token. This token has the same privileges that are assigned to your name. The token does not expire.

Update the Validation Platform

Prerequisites

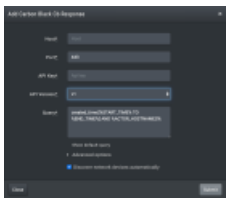
Information to gather before you start:

- API key for CB Response.
- IP address or FQDN used to access CB Response.

Configuration

TO ADD THE CARBON BLACK CB RESPONSE INTEGRATION

1. Go to **Settings** > **Integrations**.
2. Click **Add Integration** > **Carbon Black CB Response**.
3. Enter the **Host** and **API Key** information.
4. Select the API Version.
5. Expand **Advanced options** and update the information if necessary.
6. Click **Submit**.



(https://d383cql5uq169w.cloudfront.net/app/image/pid/620d7e13ccb103e8557b25b0/id/629a12dcc9cba0017c2f7e11/n/cb-response.png)

Carbon Black CB Response Integration

Verify Connectivity

TO VERIFY CONNECTIVITY TO THE CB RESPONSE HOST

Click **Test** to verify that:

- The Director can communicate with the CB Response IP address on the port specified.
- The API key is working and has the necessary privileges.

CARBON BLACK CLOUD

> This document applies to Classic Integrations. While the Integrations solution is available, it is no longer actively maintained. Mandiant recommends that you plan a switch to Preview Integrations so you can take advantage of the latest features and functionality. Preview Integrations configuration steps are provided in the Director web interface. For more details, see the **Preview Integrations Documentation (https://docs.mandiant.com/home/msv-preview-integrations)**.

This integration is remote capable.

Since the API used is the same, the Carbon Black Cloud integration enables the Validation Platform Director to pull events from many of Carbon Black's products, including:

- Carbon Black Cloud
- Carbon Black Defense
- Carbon Black Threat Hunter

Update Carbon Black Cloud

Identify or create credentials to access Carbon Black Cloud with read access, at minimum.

API tokens are tied to user accounts and inherit the user's privileges. When capturing the API key, use an account with the necessary privileges.

TO IDENTIFY THE API AND ORGANIZATION KEYS

1. Sign into Carbon Black using the appropriate credentials.
2. Navigate in the Carbon Black Cloud console to **Settings > API Access**.
3. Select **Access Levels** and click **+ Add Access Level**.

(https://d383cql5uq169w.cloudfront.net/app/image/pid/620d7e13ccb103e8557b25b0/id/629a12dec9cba0017c2f7e1f/n/cb-api-access.png)

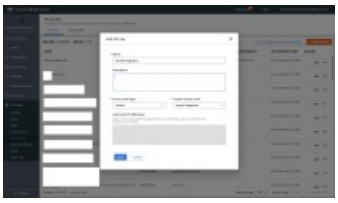
Carbon Black API Access

4. Fill in the details for the Access Level and select the **Alerts - General Information - org.alerts - READ permission** and click **Save**.

(https://d383cql5uq169w.cloudfront.net/app/image/pid/620d7e13ccb103e8557b25b0/id/629a12e6c9cba0017c2f7e75/n/cb-add-access-level.png)

Carbon Black Add Access Level

5. Click **API Keys** at the top of the window and click **+ Add API Key**.
6. Name the key and select **Custom** in the **Access Level type** drop-down list; then, select the Access Level you created in step **Select Access Levels and click + Add Access Level.Carbon Black API Access** .



(https://d383cql5uq169w.cloudfront.net/app/image/pid/620d7e13ccb103e8557b25b0/id/629a12e2c9cba0017c2f7e4f/n/cb-add-api-key.png)

Carbon Black Add API Key

7. Click **Save** and copy/paste your credentials into the integration.

The Org Key displays in the upper-left of the window.

API Calls

The following API calls are used by the Validation Platform.

Purpose	Call
default query	/alert/_search

Update the Validation Platform

Prerequisites

Information to gather before you start:

- Port info
- Host info

> Look at the web address of your Carbon Black Cloud console to identify the Host. For more information, see the **Carbon Black documentation (https://developer.carbonblack.com/reference/carbon-black-cloud/authentication/#building-your-base-urls)**.

- Organization Key
- API ID and API Secret Key

Configuration

TO ADD CARBON BLACK CLOUD

1. Go to **Settings** > **Integrations**.
2. Click **Add Integration** > **Carbon Black Cloud**.
3. (Optional) Replace the default **Host** value with the host from your Carbon Black Cloud console.
4. Enter the **Port**.
5. Enter the **Organization Key**.
6. Enter the **API ID** and **API Secret Key**.
7. Review and update the **Query**.
8. Expand **Advanced options**.
9. (Optional) Update **Query time** and **Delay time**.

The **Query time** is the amount of time (minutes) before and after the query runs that the looks for events, while the **Delay time** is the amount of time (minutes) that the platform waits to run the query after a Job Action. For example, you configure your integration with the following values: **Query time** = 5, **Query interval** = 30 seconds, and **Delay time** = 0. When a Job Actions starts at 12:00:00, the first time the query runs, the platform looks for events from 11:55:00 to 12:00:00. Then 30 seconds later, it looks for events from 11:55:30 to 12:00:30. This interval continues, with the last query looking from 12:00:00 to 12:05:00. If you instead configured the **Delay time** to equal 10, it would run the same query, but it wouldn't start that query until 12:10:00.

If your monitors are set to run more frequently than the query time, it will impact the pass/fail results for AEDA monitors.

10. Modify the **Query Interval** and **Event Time Adjustment**, if necessary.
11. (Optional) Assign a **Name**.
12. (Optional) Select **Discover network devices automatically**.
13. Click **Submit**.

(https://d383cql5uq169w.cloudfront.net/app/image/pid/620d7e13ccb103e8557b25b0/id/629a12dec9cba0017c2f7e27/n/cb-cloud.png)

Carbon Black Cloud Integration

Verify connectivity

TO VERIFY CONNECTIVITY TO INTEGRATION

Click **Test** to verify that:

- The Director can communicate with the integration host on the port and protocol specified.
- The integration credentials are valid and working.

CISCO ADVANCED MALWARE PROTECTION (AMP)

> This document applies to Classic Integrations. While the Integrations solution is available, it is no longer actively maintained. Mandiant recommends that you plan a switch to Preview Integrations so you can take advantage of the latest features and functionality. Preview Integrations configuration steps are provided in the Director web interface. For more details, see the **Preview Integrations Documentation (https://docs.mandiant.com/home/msv-preview-integrations)**.

Update Cisco AMP

Verify that the Director can resolve and communicate to AMP's API, located at **https://api.amp.cisco.com (https://api.amp.cisco.com/)**.

Update the Validation Platform

Prerequisites

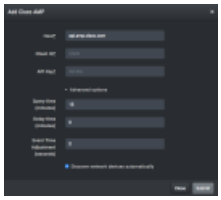
Information to gather before you start:

1. Identify the client ID for AMP communications.
2. Identify the API Key for AMP communications.
    a. Log in to https://console.amp.sourcefire.com (NA) or https://console.eu.amp.sourcefire.com (EU).
    b. From the **Accounts** menu, navigate to the Business Page.
    c. Click **Edit**.
    d. Click **Regenerate** to generate the Client ID and API Key (this button is located under "Features" next to"3rd Party API Access") .

Configuration

TO ADD THE CISCO AMP INTEGRATION

1. Go to **Settings** > **Integrations**.
2. Click **Add Integration** and choose **Cisco AMP**.
3. Enter information for the **Host**, **Client ID**, and **API Key**.
4. Expand **Advanced options** and update the information if necessary.
5. Click **Submit**.



(https://d383cql5uq169w.cloudfront.net/app/image/pid/620d7e13ccb103e8557b25b0/id/629a12d8c9cba0017c2f7dda/n/cisco-amp.png)

Add Cisco AMP Integration

Verify connectivity

TO VERIFY CONNECTIVITY TO CISCO AMP

Click **Test** to verify that the Director can communicate with the Cisco host using the provided client ID and API key.

CROWDSTRIKE

> This document applies to Classic Integrations. While the Integrations solution is available, it is no longer actively maintained. Mandiant recommends that you plan a switch to Preview Integrations so you can take advantage of the latest features and functionality. Preview Integrations configuration steps are provided in the Director web interface. For more details, see the **Preview Integrations Documentation (https://docs.mandiant.com/home/msv-preview-integrations)**.

This integration is remote capable.

Update CrowdStrike

- Create a Username with the appropriate privileges, which requires a minimum of read on detections.
- Obtain your API key
  - Standard (Legacy) API: Contact Crowdstrike's customer support and request an API key.

    It may take a few days before they generate it and send it to you.

  - OAuth2 API key: Self-provision your API key on your portal

Update the Validation Platform

Prerequisites

Information to gather before you start:

1. Create a Username in CrowdStrike.
2. Identify the API key.

Configuration

TO ADD THE CROWDSTRIKE INTEGRATION

1. Go to **Settings** > **Integrations**.
2. Click **Add Integration** > **CrowdStrike**.

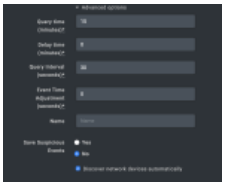
(https://d383cql5uq169w.cloudfront.net/app/image/pid/620d7e13ccb103e8557b25b0/id/629a12ebc9cba0017c2f7e9e/n/crowdstrike

CrowdStrike Integration

> If you use the %HOST_CLI_ACTOR_HOSTNAMES% variable, the platform will substitute the plain hostname and the information from the Alternate Hostname field on the Actor configuration page.

3. Modify the **Host** and **Port**, if necessary.
4. Select your **Authentication Method**.
   a. Standard (Legacy) API: Legacy API Key
   b. OAuth2 API key: OAuth2
5. Enter Credentials for your Authentication method.
   a. Standard API: Username and API Key
   b. OAuth2: Client ID and Client Secret
6. Modify the **Query**, as necessary.

7. Expand **Advanced options**.



(https://d383cql5uq169w.cloudfront.net/app/image/pid/620d7e13ccb103e8557b25b0/id/629a12d9c9cba0017c2f7ded/n/crowdstrike-adv.png)

CrowdStrike Integration - Advanced options

8. (Optional) Select **Discover network devices automatically**.
9. Modify the **Query Interval** and **Event Time Adjustment**, if necessary.
10. (Optional) Assign a **Name**.
11. (Optional) Choose **Yes** to save suspicious events.
12. Click **Submit**.

Verify Connectivity

TO VERIFY CONNECTIVITY TO CROWDSTRIKE

Click **Test** to verify that the Director can communicate with the CrowdStrike host using the provided Username and API key.

CYBEREASON

This document applies to Classic Integrations. While the Integrations solution is available, it is no longer actively maintained. Mandiant recommends that you plan a switch to Preview Integrations so you can take advantage of the latest features and functionality. Preview Integrations configuration steps are provided in the Director web interface. For more details, see the **Preview Integrations Documentation (https://docs.mandiant.com/home/msv-preview-integrations)**.

This integration is remote capable.

Update Cybereason

Identify or create credentials to access Cybereason with read access, at minimum.

Update the Validation Platform

Prerequisites

Information to gather before you start:

- Cybereason Host and Port.
- Cybereason account with read access, at minimum.

Configuration

TO ADD THE CYBEREASON INTEGRATION

1. Go to **Settings** > **Integrations**.
2. Click **Add Integration** > **Cybereason**.
3. Enter the **Host** information.
4. Update the default **Port** and **Protocol** information if necessary (Port may be 8443 instead of 443 if it is hosted by Cybereason).
5. Enter the **Username** and **Password**.
6. Expand **Advanced options**.
7. (Optional) Update **Query time** and **Delay time**.

   The **Query time** is the amount of time (minutes) before and after the query runs that the looks for events, while the **Delay time** is the amount of time (minutes) that the platform waits to run the query after a Job Action. For example, you configure your integration with the following values: **Query time** = 5, **Query interval** = 30 seconds, and **Delay time** = 0. When a Job Actions starts at 12:00:00, the first time the query runs, the platform looks for events from 11:55:00 to 12:00:00. Then 30 seconds later, it looks for events from 11:55:30 to 12:00:30. This interval continues, with the last query looking from 12:00:00 to 12:05:00. If you instead configured the **Delay time** to equal 10, it would run the same query, but it wouldn't start that query until 12:10:00.

   If your monitors are set to run more frequently than the query time, it will impact the pass/fail results for AEDA monitors.

8. Enable and configure the **Malware query**.
9. (Optional) Assign a **Name**.
10. Click **Submit**.

(https://d383cql5uq169w.cloudfront.net/app/image/pid/620d7e13ccb103e8557b25b0/id/629a12dfc9cba0017c2f7e30/n/cybereason-1.png)

Cybereason Integration

Verify connectivity

TO VERIFY CONNECTIVITY TO CYBEREASON

Click **Test** to verify that:

- The Director can communicate with the Cybereason host on the port and protocol specified.
- The Cybereason credentials are valid and working.

CYLANCE

> This document applies to Classic Integrations. While the Integrations solution is available, it is no longer actively maintained. Mandiant recommends that you plan a switch to Preview Integrations so you can take advantage of the latest features and functionality. Preview Integrations configuration steps are provided in the Director web interface. For more details, see the **Preview Integrations Documentation (https://docs.mandiant.com/home/msv-preview-integrations)**.

Cylance maintains a history of threats and does not report new threats of the same type. If you want Actions to be identified each time they are run, you must delete Quarantined items in Cylance before running the Action.

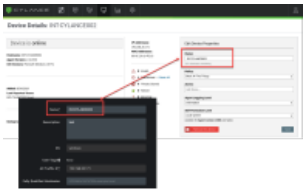
TO DELETE QUARANTINED ITEMS IN CYLANCE

In the Cylance Portal, navigate to the Device representing the Validation Platform Actor and delete all the Quarantined items.

Update Cylance

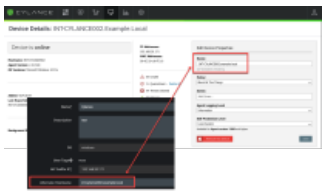
Add a Device entry in Cylance for each Endpoint Actor in the Validation Platform from which you want to receive Cylance events.

- The name of the Device entry in Cylance must match either the Validation Platform Actor Name or its Alternate Hostname.
  If the names do not match, events will not be related correctly.
- This entry must have Read permissions for Devices, Threat, and User.
- The device names in Cylance and the Actors configured in the platform are automatically synced every 15 minutes.



(https://d383cql5uq169w.cloudfront.net/app/image/pid/620d7e13ccb103e8557b25b0/id/629a12e9c9cba0017c2f7e8c/n/cylance-actor-option1.png)

Cylance Device name matching Actor Name



(https://d383cql5uq169w.cloudfront.net/app/image/pid/620d7e13ccb103e8557b25b0/id/629a12e6c9cba0017c2f7e72/n/cylance-actor-option2.png)

Cylance Device name matching Actor's Alternate Hostname

Update the Validation Platform

Prerequisites

Information to gather before you start:

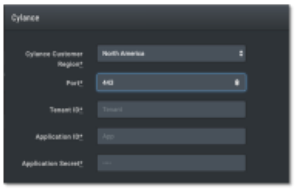
- Cylance Port information.
- Cylance Tenant ID, Application ID, and Application Secret.

Configuration

TO ADD THE CYLANCE INTEGRATION

1. Go to **Settings** > **Integrations**.
2. Click **Add Integration** > **Cylance**.

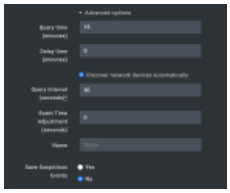
> You can add this as either a Local or Remote Inetgration.



(https://d383cql5uq169w.cloudfront.net/app/image/pid/620d7e13ccb103e8557b25b0/id/629a12e2c9cba0017c2f7e47/n/cylance.pı

Cylance Integration

3. Choose the **Cylance Customer Region**.
4. (Optional) Update the default **Port**.
5. Enter the **Tenant ID** and **Application ID**.
6. Enter the **Application Secret**.
7. Expand **Advanced options**.



(https://d383cql5uq169w.cloudfront.net/app/image/pid/620d7e13ccb103e8557b25b0/id/629a12d8c9cba0017c2f7de2/n/cylance-adv.png)

Cylance Integration (Advanced Options)

8. (Optional) Update **Query time** and **Delay time**.

> The **Query time** is the amount of time (minutes) before and after the query runs that the looks for events, while the **Delay time** is the amount of time (minutes) that the platform waits to run the query after a Job Action. For example, you configure your integration with the following values: **Query time** = 5, **Query interval** = 30 seconds, and **Delay time** = 0. When a Job Actions starts at 12:00:00, the first time the query runs, the platform looks for events from 11:55:00 to 12:00:00. Then 30 seconds later, it looks for events from 11:55:30 to 12:00:30. This interval continues, with the last query looking from 12:00:00 to 12:05:00. If you instead configured the **Delay time** to equal 10, it would run the same query, but it wouldn't start that query until 12:10:00.

> If your monitors are set to run more frequently than the query time, it will impact the pass/fail results for AEDA monitors.

9. Modify the **Query Interval** and **Event Time Adjustment**, if necessary.
10. (Optional) Select **Discover network devices automatically**.
11. (Optional) Assign a **Name**.
12. (Optional) Choose **Yes** to save suspicious events.
13. Click **Submit**.

Verify connectivity

TO VERIFY CONNECTIVITY TO CYLANCE

Click **Test** to verify that:

- The Director can communicate with the Cylance host on the port and protocol specified.
- Cylance credentials are valid and working.

Error: Invalid JWT Payload

There are two places you might see this error:

- In the UI when running the test query
- In the logs when Cylance tries to match events during a Job

There are several possible causes of this issue:

1. (Most Common) - The Time on the Director is out of sync with the Cylance Server by +/- 15 minutes. The Cylance Server uses NTP to stay accurate.
2. The Keys that were entered were mistyped or copy/pasted wrong.
3. The wrong key may have been used. For example, entering the App Token into the App Secret field.
4. (Unconfirmed) The Cylance keys being used are expired or not recognized by Cylance.

ENDGAME

> This document applies to Classic Integrations. While the Integrations solution is available, it is no longer actively maintained. Mandiant recommends that you plan a switch to Preview Integrations so you can take advantage of the latest features and functionality. Preview Integrations configuration steps are provided in the Director web interface. For more details, see the **Preview Integrations Documentation (https://docs.mandiant.com/home/msv-preview-integrations)**.

The Endgame Integration requires that the time on the Director and Actor to be kept synchronized. If there is a time skew, the integration will not be able to retrieve the proper data.

This integration is remote capable.

Update Endgame

TO UPDATE ENDGAME

1. Define a username with a user role that allows access to Alerts in Endgame.
2. Configure the Actor in the Validation Platform to match the name shown as the Endgame Sensor in the Endgame Portal.

Update the Validation Platform

Prerequisites

Information to gather before you start:

- Identify the Sensor Transceiver Address in the endgame Portal and verify that the Validation Platform Actor can access it.
- Identify the Endgame Host.
- Identify the Port used by Endgame.
- Obtain credentials that allows access to Alerts in Endgame.

Configuration

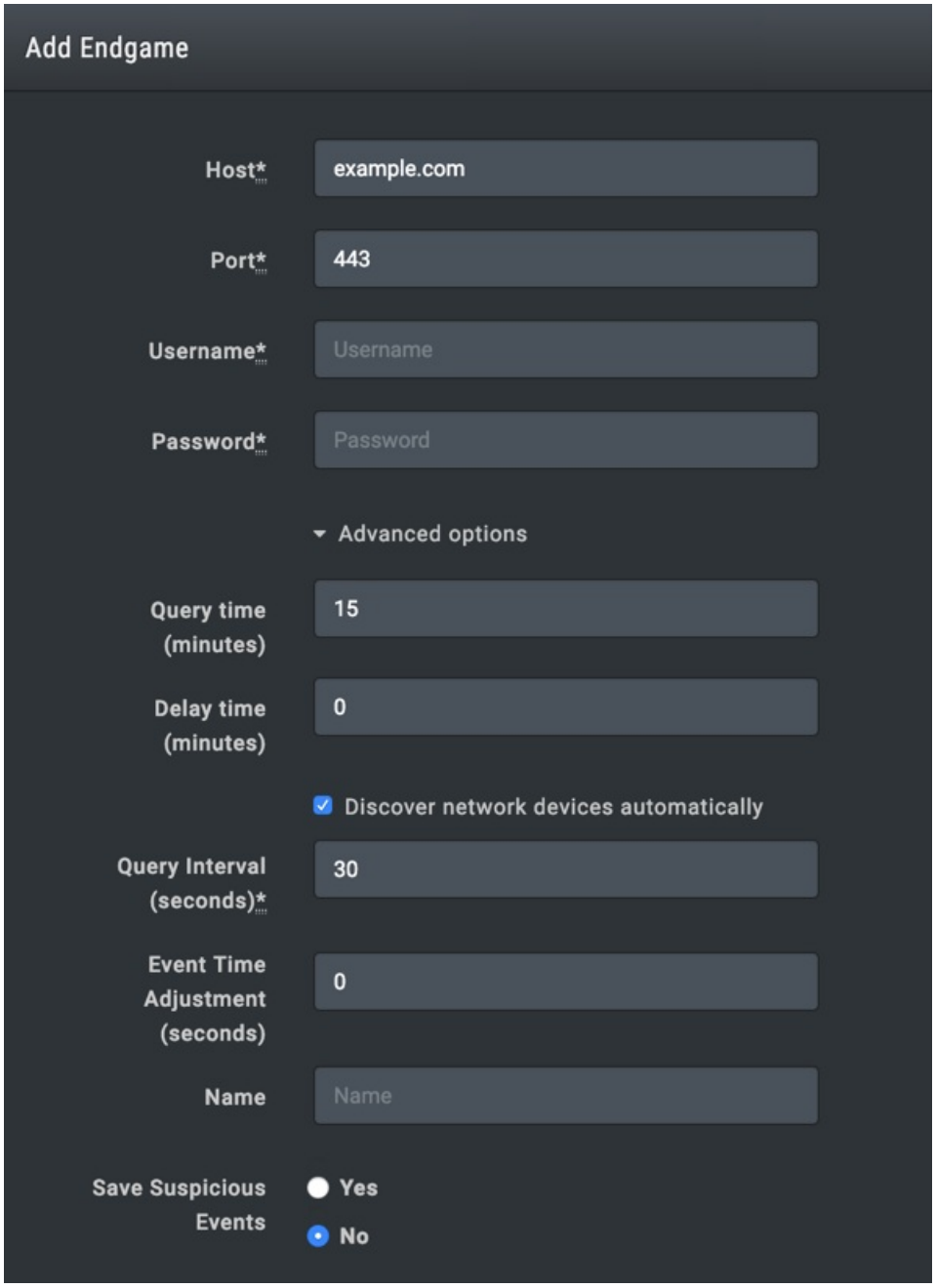
TO ADD THE ENDGAME INTEGRATION

1. Go to **Settings** > **Integrations**.
2. Click **Add Integration** > **Endgame**.
3. Enter information for the **Host**, **Port**, **Username**, and **Password**.
4. Expand **Advanced options**.
5. (Optional) Update **Query time** and **Delay time**.

   The **Query time** is the amount of time (minutes) before and after the query runs that the looks for events, while the **Delay time** is the amount of time (minutes) that the platform waits to run the query after a Job Action. For example, you configure your integration with the following values: **Query time** = 5, **Query interval** = 30 seconds, and **Delay time** = 0. When a Job Actions starts at 12:00:00, the first time the query runs, the platform looks for events from 11:55:00 to 12:00:00. Then 30 seconds later, it looks for events from 11:55:30 to 12:00:30. This interval continues, with the last query looking from 12:00:00 to 12:05:00. If you instead configured the **Delay time** to equal 10, it would run the same query, but it wouldn't start that query until 12:10:00.

   If your monitors are set to run more frequently than the query time, it will impact the pass/fail results for AEDA monitors.

6. (Optional) Clear **Discover network devices automatically**.
7. Modify the **Query Interval** and **Event Time Adjustment**, if necessary.
8. (Optional) Assign a **Name**.
9. (Optional) Choose **Yes** to save suspicious events.
10. Click **Submit**.



Verify Connectivity

TO VERIFY CONNECTIVITY TO ENDGAME

Click **Test** to verify that:

- The Director can communicate with the Endgame Host on the port specified.
- The Username and Password are valid.

TRELLIX ENDPOINT SECURITY (HX)

> This document applies to Classic Integrations. While the Integrations solution is available, it is no longer actively maintained. Mandiant recommends that you plan a switch to Preview Integrations so you can take advantage of the latest features and functionality. Preview Integrations configuration steps are provided in the Director web interface. For more details, see the **Preview Integrations Documentation (https://docs.mandiant.com/home/msv-preview-integrations)**.

 This integration is remote capable.

Update Trellix Endpoint Security (HX)

Create a Trellix Endpoint Security (HX) API Account for use with the Validation Platform. This must use the API_Analyst role.

API Calls

The following API calls are used by the Validation Platform.

Purpose	Call
Login for a token	`/hx/api/v3/token`
Alerts query	`/hx/api/v3/alerts/?agent. id=(DeviceId)&limit=(PageLimit)&offset=(PageOffset)&filterQuery=(ReportedAtTimestampFilterQuery)`
Hosts Query	`/hx/api/v3/hosts`

Update the Validation Platform

Prerequisites

Information to gather before you start:

1. Identify the Trellix Endpoint Security (HX) Host and Port information.
2. Have a Trellix Endpoint Security (HX) API User Account with the API_Analyst role.

Configuration

TO ADD THE TRELLIX ENDPOINT SECURITY (HX) INTEGRATION

1. Go to **Settings** > **Integrations**.
2. Click **Add Integration** > **Trellix Endpoint Security (HX)**.

    You can add this as either a Local or Remote Integration.

3. Enter information for the **Host**, **Port**, **Username**, and **Password**.

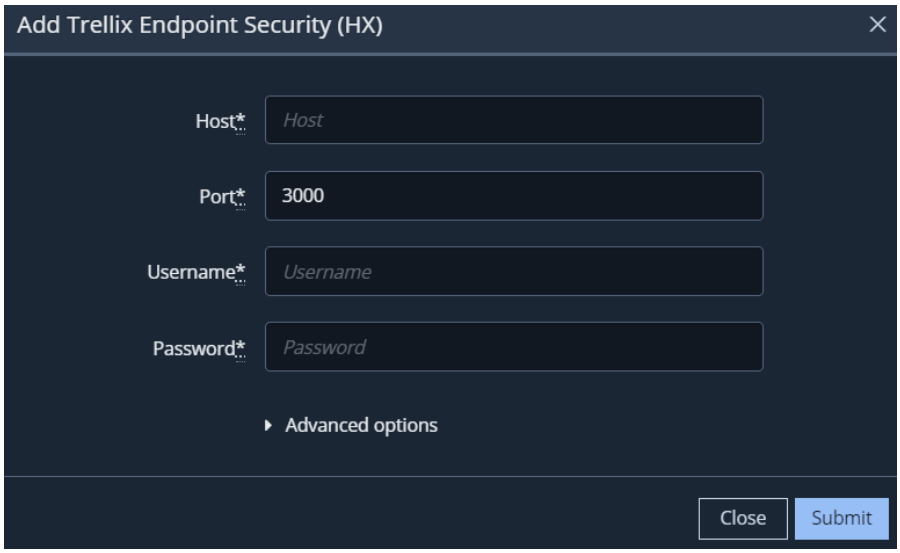
    Port 3000 is required for on-prem HX appliances

4. Expand **Advanced options** and update the information if necessary.
5. (Optional) Update **Query time** and **Delay time**.

The **Query time** is the amount of time (minutes) before and after the query runs that the looks for events, while the **Delay time** is the amount of time (minutes) that the platform waits to run the query after a Job Action. For example, you configure your integration with the following values: **Query time** = 5, **Query Interval** = 30 seconds, and **Delay time** = 0. When a Job Actions starts at 12:00:00, the first time the query runs, the platform looks for events from 11:55:00 to 12:00:00. Then 30 seconds later, it looks for events from 11:55:30 to 12:00:30. This interval continues, with the last query looking from 12:00:00 to 12:05:00. If you instead configured the **Delay time** to equal 10, it would run the same query, but it wouldn't start that query until 12:10:00.

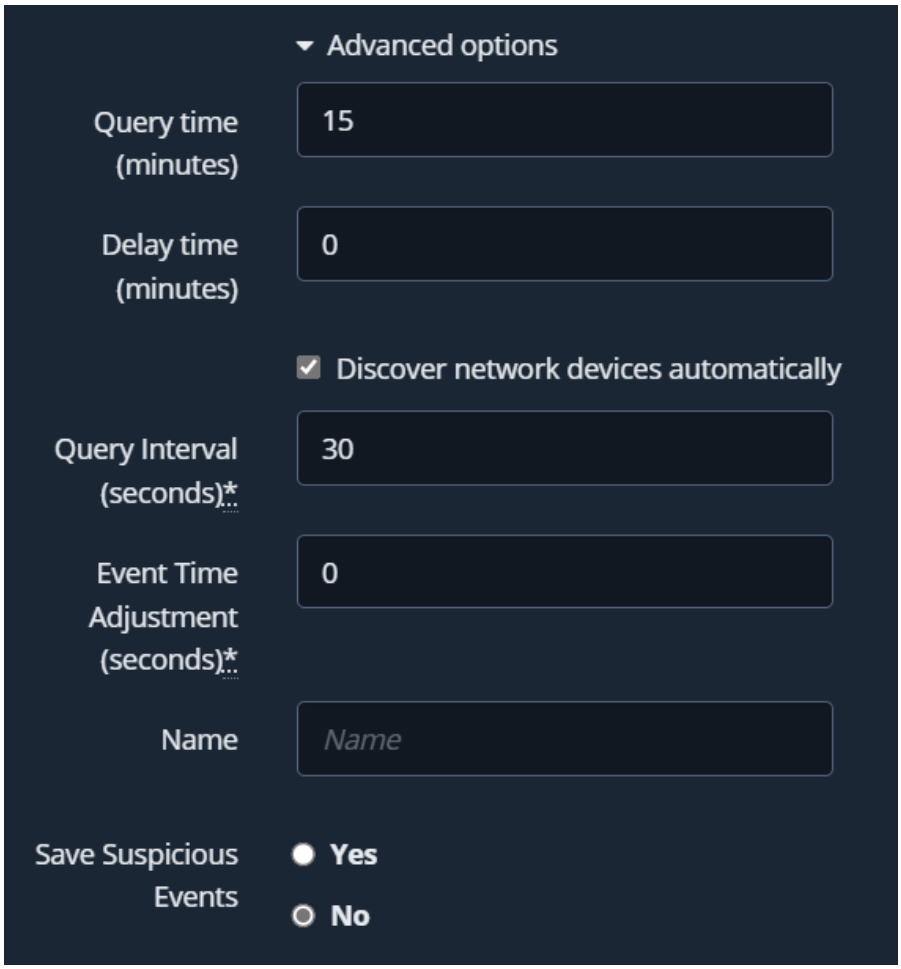
If your monitors are set to run more frequently than the query time, it will impact the pass/fail results for AEDA monitors.

6. (Optional) Select **Discover network devices automatically**.
7. Modify the **Query Interval** and **Event Time Adjustment**, if necessary.
8. (Optional) Assign a **Name**.
9. (Optional) Choose **Yes** to save suspicious events.
10. Click **Submit**.



(https://app.knowledgeowl.com/app/image/pid/620d7e13ccb103e8557b25b0/id/63ebf667c0da4a6d8947e740/n/trellix-endpoint-security-hx.png?imgkey=3c1881a2cce84a39ccf1bf98f3036ff3)

Trellix Endpoint Security (HX) Integration



(https://app.knowledgeowl.com/app/image/pid/620d7e13ccb103e8557b25b0/id/63ecf34defbf62424e348ffe/n/trellix-endpoint-security-hx-advanced-options.png?imgkey=3c1881a2cce84a39ccf1bf98f3036ff3)

Trellix Endpoint Security (HX) Integration - Advanced options

Verify Connectivity

TO VERIFY CONNECTIVITY TO TRELLIX ENDPOINT SECURITY (HX)

Click **Test** to verify that:

- The Director can communicate with the Trellix Endpoint Security (HX) console using the provided host and user information.
- The Webservice API is enabled and allowing communication.

If the test is not successful, messages will be displayed to help identify possible issues, such as no connection to the API server.

TRELLIX ENDPOINT SECURITY

> This document applies to Classic Integrations. While the Integrations solution is available, it is no longer actively maintained. Mandiant recommends that you plan a switch to Preview Integrations so you can take advantage of the latest features and functionality. Preview Integrations configuration steps are provided in the Director web interface. For more details, see the **Preview Integrations Documentation (https://docs.mandiant.com/home/msv-preview-integrations)**.

 This integration is remote capable.

Update Trellix Endpoint Security

Identify or create credentials to access Trellix Endpoint Security with read permissions, at minimum.

API Calls

The following API call is used by the Validation Platform.

Purpose	Call
executeQuery for events	`/remote/core.executeQuery?target='EPOEvents'&where=$query`

Update the Validation Platform

Prerequisites

Information to gather before you start:

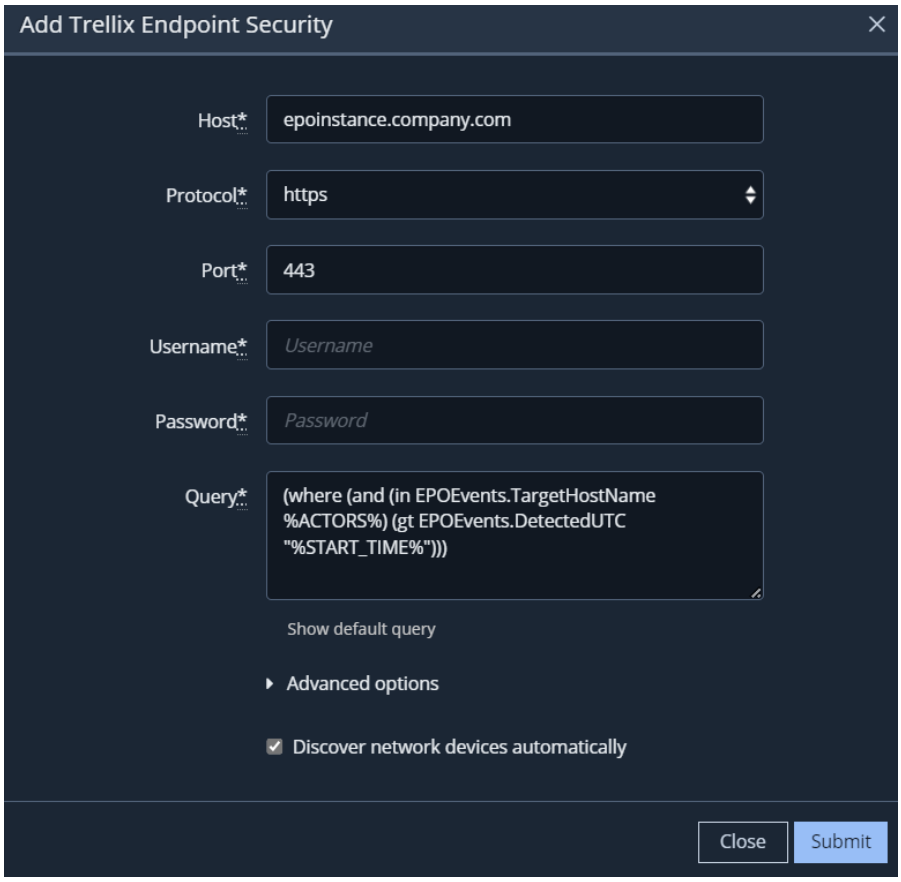
- IP address/host information used to access Trellix Endpoint Security (ESM or ePO)
- Port for Trellix Endpoint Security (ESM or ePO) communications (default is 443)
- Identify whether the protocol is HTTP or HTTPS for connections to the port (default is HTTPS)

Configuration

TO ADD THE TRELLIX ENDPOINT SECURITY INTEGRATION

1. Go to **Settings** > **Integrations**.
2. Click **Add Integration** > **Trellix Endpoint Security**.

    You can add this as either a Local or Remote Integration.
3. Enter information for the **Host**, **Protocol**, **Port**, **Username** and **Password** or **API Token**.
4. If necessary, modify the **Query**.
5. Expand **Advanced options** and update the information, if necessary.
6. Click **Submit**.



(https://app.knowledgeowl.com/app/image/pid/620d7e13ccb103e8557b25b0/id/63ebec7a11381978570523b1/n/trellix-endpoint-security.png?imgkey=3c1881a2cce84a39ccf1bf98f3036ff3)

Trellix Endpoint Security Integration

Verify Connectivity

TO VERIFY CONNECTIVITY TO TRELLIX ENDPOINT SECURITY

Click **Test** to verify that:

- The Director can communicate with the IP address on the port specified.
- Credentials are valid and working.

MICROSOFT DEFENDER ADVANCED THREAT PROTECTION (ATP)

This document applies to Classic Integrations. While the Integrations solution is available, it is no longer actively maintained. Mandiant recommends that you plan a switch to Preview Integrations so you can take advantage of the latest features and functionality. Preview Integrations configuration steps are provided in the Director web interface. For more details, see the **Preview Integrations Documentation (https://docs.mandiant.com/home/msv-preview-integrations)**.

This integration is remote capable.

Update Defender ATP

1. Identify or create credentials to access integration with read access, at minimum.
2. Identify the following values in the Azure Web portal:

Refer to the **Microsoft documentation (https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/exposed-apis-create-app-webapp?view=o365-worldwide)** for instructions on creating an app to get this information.

   - Client ID
   - Client Secret
   - Authorization URL
   - Tenant ID

API Calls

The following API calls are used by the Validation Platform.

Purpose	Call
Get alerts for the Actor	/api/alerts
Get authorization token	Authorization URL provided by Defender ATP

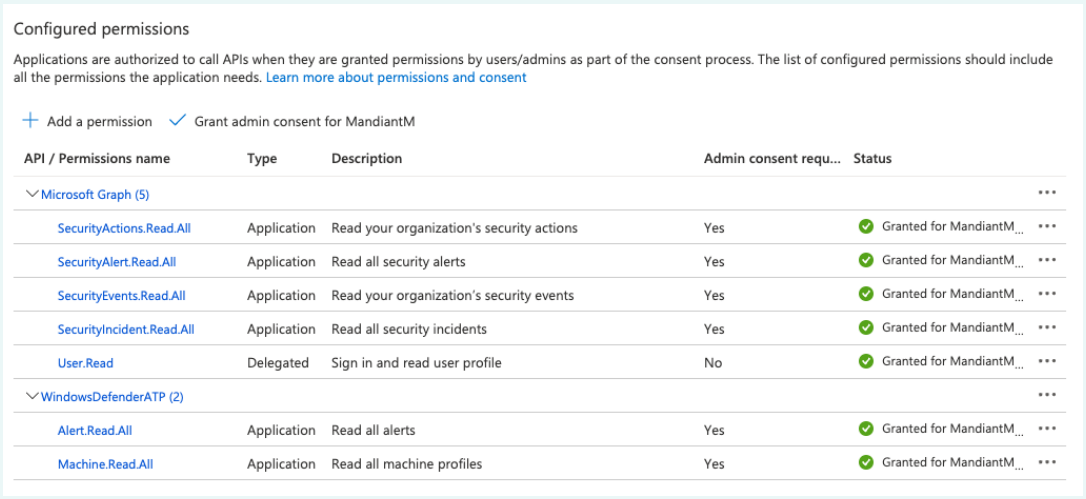
Update the Validation Platform

Prerequisites

Information to gather before you start:

- Identify the host, or geographic region, of your Defender ATP instance (US, UK, or EU).
- Identify the Port used for Defender ATP communication (this defaults to 443).
- Identify the Client ID unique to your application.
- Identify the Client Secret unique to your application.
- Identify the Authorization URL unique to your application.
- Identify the Tenant ID unique to your application.

Microsoft SIEM API is being replaced with Microsoft Graph for accessing Defender events. If your system employs Microsoft Graph, the settings shown here will need to be configured before you can successfully integrate with Microsoft Defender ATP.



Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. Learn more about permissions and consent

+ Add a permission ✓ Grant admin consent for MandiantM

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (5)				
SecurityActions.Read.All	Application	Read your organization's security actions	Yes	Granted for MandiantM...
SecurityAlert.Read.All	Application	Read all security alerts	Yes	Granted for MandiantM...
SecurityEvents.Read.All	Application	Read your organization's security events	Yes	Granted for MandiantM...
SecurityIncident.Read.All	Application	Read all security incidents	Yes	Granted for MandiantM...
User.Read	Delegated	Sign in and read user profile	No	Granted for MandiantM...
WindowsDefenderATP (2)				
Alert.Read.All	Application	Read all alerts	Yes	Granted for MandiantM...
Machine.Read.All	Application	Read all machine profiles	Yes	Granted for MandiantM...

TO ADD THE DEFENDER ATP INTEGRATION

1. Go to **Settings** > **Integrations**.
2. Click **Add Integration** > **Defender ATP**.

   You can add this as either a Local or Remote Integration.

3. Enter information for the **Host**, **Port**, and **Protocol**.

   The host is auto-populated with the required info for the current API version but can be changed to one of the options listed below the **Host** text box.

4. Enter information for the **Client ID** and **Client Secret**.
5. (Optional) Update the **API Version**. This is set to the current supported API by default.
6. Update the **Auth URL**.

   This is set correctly for MS Defender for Endpoint API. Update this if you are not using the MS Defender for Endpoint API.

7. Add the **Tenant ID**.

   This is necessary if you're using the MS Defender for Endpoint API.

8. Add the **Resource**.

   This is necessary if you are using the Legacy SIEM API.

   Microsoft Defender ATP Integration

9. Expand **Advanced options** and update the information if necessary.
10. Click **Submit**.

Verify connectivity

TO VERIFY CONNECTIVITY TO DEFENDER ATP

Click **Test** to verify that:

- The Director can communicate with the integration host on the port and protocol specified.
- The integration credentials are valid and working.

NETSKOPE

> This document applies to Classic Integrations. While the Integrations solution is available, it is no longer actively maintained. Mandiant recommends that you plan a switch to Preview Integrations so you can take advantage of the latest features and functionality. Preview Integrations configuration steps are provided in the Director web interface. For more details, see the **Preview Integrations Documentation (https://docs.mandiant.com/home/msv-preview-integrations)**.

This integration is remote capable.

Update Netskope

- Identify or create credentials to access Netskope with read access, at minimum
- Verify your Netskope instance uses v1 of the API

API Calls

The following API calls are used by the Validation Platform.

Purpose	Call
Get alerts	/api/v1/alerts

Update the Validation Platform

Prerequisites

Information to gather before you start:

- Identify the host, port, and protocol associated with your Netskope instance
- In Netskope, navigate to Settings > Tools > Rest API to obtain the API key

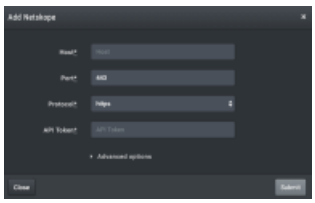
Configuration

TO ADD NETSKOPE

1. Go to **Settings** > **Integrations**.
2. Click **Add Integration** > **Netskope**.

   You can add this as either a Local or Remote Inetgration.

3. Enter information for the Host, Port, and Protocol.
4. Enter the API Token.
5. Expand **Advanced options** and update the information if necessary.
6. Click **Submit**.



(https://d383cql5uq169w.cloudfront.net/app/image/pid/620d7e13ccb103e8557b25b0/id/629a12efc9cba0017c2f7eca/n/netskope.png)

Netskope Integration

Verify connectivity

TO VERIFY CONNECTIVITY TO NETSKOPE

Click **Test** to verify that:

- The Director can communicate with the integration host on the port and protocol specified.
- The integration credentials are valid and working.

PALO ALTO NETWORKS CORTEX XDR

> This document applies to Classic Integrations. While the Integrations solution is available, it is no longer actively maintained. Mandiant recommends that you plan a switch to Preview Integrations so you can take advantage of the latest features and functionality. Preview Integrations configuration steps are provided in the Director web interface. For more details, see the **Preview Integrations Documentation (https://docs.mandiant.com/home/msv-preview-integrations)**.

Cortex XSOAR from Palo Alto Networks is a security orchestration, automation, and response (SOAR) platform that unifies case management, automation, real-time collaboration, and threat intel management to serve security teams across the incident lifecycle.

 This integration is remote capable.

This integration requires three steps:

1. Create Credentials to Access Cortex XDR via API from the Security Validation Platform.
2. Add the Cortex XDR Integration to the Security Validation Platform.
3. Verify connectivity.

Create Credentials to Access Cortex XDR via API from the Security Validation Platform

- Identify the hostname used to access Palo Alto Cortex XDR.
- Identify the port used for Palo Alto Cortex XDR communication.
- Identify the ID and Key used to access the Palo Alto Cortex XDR API.

 See the **Cortex XDR API documentation (https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-api/cortex-xdr-api-overview/get-started-with-cortex-xdr-apis)** for information on generating and accessing these values.

API Calls

The following API calls are used by the Validation Platform:

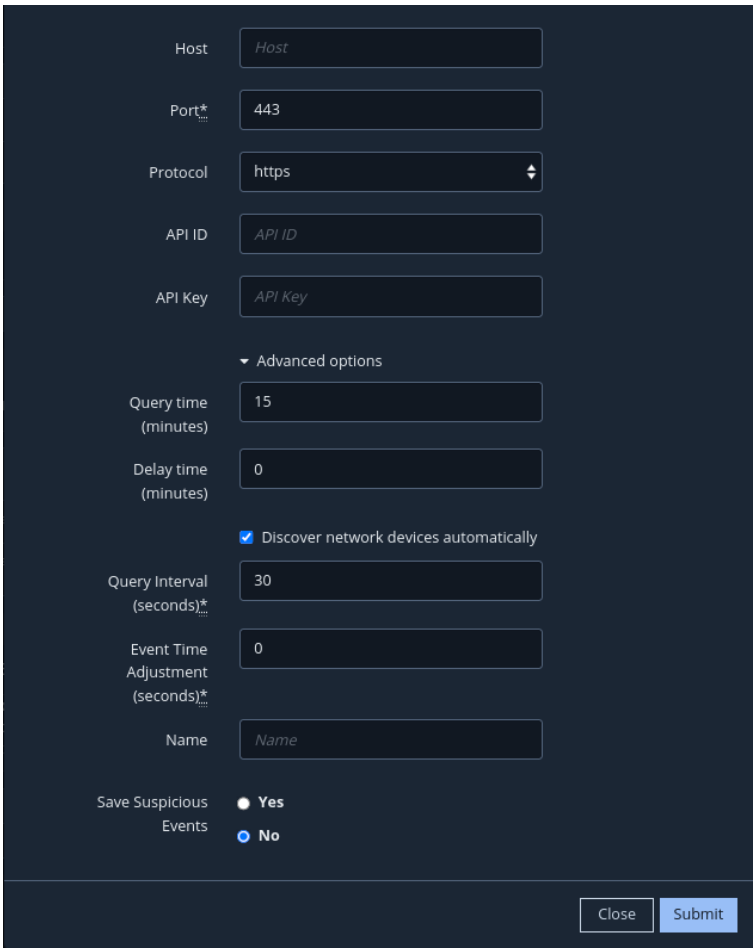
Purpose	Call
Get list of events	/public_api/v1/incidents/get_incidents
Get event data	/public_api/v1/incidents/get_incident_extra_data

Add the Cortex XDR Integration to the Security Validation Platform

1. Go to **Settings** > **Integrations.**
2. Click **Add Integration > Palo Alto Cortex XDR**.

    You can add this as either a Local or Remote integration.
3. Enter information for the **Host**, **Port**, and **Protocol**.
4. Enter your Cortex XDR **API ID** and **API Key**.
5. Expand **Advanced options**.
6. Modify the **Query Time** (optional), **Delay Time** (optional), **Query Interval,** and **Event Time Adjustment**, if necessary.
7. (Optional) Assign a **Name**.

8. (Optional) Choose **Yes** to save suspicious events.
9. Click **Submit**.



Set up Proxy Assignment

If all outbound connections go through a proxy, you may want to set up a proxy definition and assignment for your integration. To learn more about setting up the rule and assignment, see **Proxy Settings (https://docs.mandiant.com/home/msv-proxy-rules)**.

Verify connectivity

Click the Action menu and select **Test Palo Alto Cortex XDR attributes** to verify that:

- The Director can communicate with the Cortex XDR host on the port and protocol specified.
- The Cortex XDR credentials are valid and working.

Troubleshooting

In the event of an error, please provide the exact error message from Cortex XDR. If requested by Mandiant Support, please also provide appropriate logs from Cortex XDR. Instructions for exporting logs can be found in the **Cortex XDR Log Format Documentation (https://docs-cortex.paloaltonetworks.com/r/Cortex-XDR/Cortex-XDR-Prevent-Administrator-Guide/Log-Formats)**.

SENTINELONE

> This document applies to Classic Integrations. While the Integrations solution is available, it is no longer actively maintained. Mandiant recommends that you plan a switch to Preview Integrations so you can take advantage of the latest features and functionality. Preview Integrations configuration steps are provided in the Director web interface. For more details, see the **Preview Integrations Documentation (https://docs.mandiant.com/home/msv-preview-integrations)**.

The SentinelOne Integration uses SentinelOne's API to function correctly. Versions 2.0 and 2.1 of the SentinelOne API are supported.

The API request that the SentinelOne integration uses is bound by time limits. The time on the Director and Actor must be kept synchronized, or else no events will match.

This integration is remote capable.

Update SentinelOne

TO UPDATE SENTINELONE

1. Define a username that will be attached to the API key that the Validation Platform will use. The username must have at least Site Viewer access.
2. Use the SentinelOne Portal to generate an API key that can be used in the integration setup in the Director.

Update Security Validation

Prerequisites

Information to gather before you start:

- The SentinelOne API key.
- The name of the host where SentinelOne is installed.
- The Actor configured with the exact name of the host that is running SentinelOne (shown in the SentinelOne Portal).

Configuration

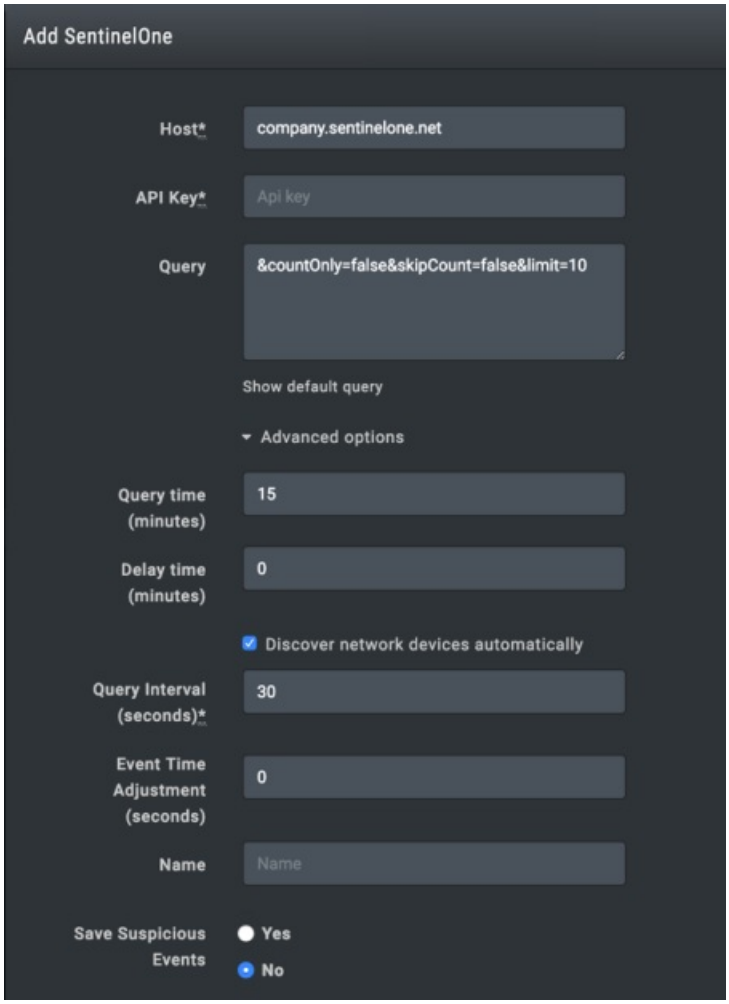
TO ADD THE SENTINELONE INTEGRATION

1. Go to **Settings** > **Integrations**.
2. Click **Add Integration** > **SentinelOne**.
3. Enter the **Host**.
   This is the SentinelOne address given to the customer by SentinelOne.
4. Enter the **API Key**.
5. Select the **API Version**.
6. (Optional) Update the **Query**.
7. Expand **Advanced options**.
8. (Optional) Update **Query time** and **Delay time**.

The **Query time** is the amount of time (minutes) before and after the query runs that the looks for events, while the **Delay time** is the amount of time (minutes) that the platform waits to run the query after a Job Action. For example, you configure your integration with the following values: **Query time** = 5, **Query interval** = 30 seconds, and **Delay time** = 0. When a Job Actions starts at 12:00:00, the first time the query runs, the platform looks for events from 11:55:00 to 12:00:00. Then 30 seconds later, it looks for events from 11:55:30 to 12:00:30. This interval continues, with the last query looking from 12:00:00 to 12:05:00. If you instead configured the **Delay time** to equal 10, it would run the same query, but it wouldn't start that query until 12:10:00.

If your monitors are set to run more frequently than the query time, it will impact the pass/fail results for AEDA monitors.

9. (Optional) Clear **Discover network devices automatically**.
10. Modify the **Query Interval** and **Event Time Adjustment**, if necessary.
11. (Optional) Assign a **Name**.
12. (Optional) Choose **Yes** to save suspicious events.
13. Click **Submit**.



SentinelOne Integration

Verify Connectivity

TO VERIFY CONNECTIVITY TO SENTINEL ONE

Click **Test** to verify that:

- The Director can communicate with the Sentinel One IP address on the port specified.
- The API key is working and has the necessary privileges.

SOPHOS CENTRAL

> This document applies to Classic Integrations. While the Integrations solution is available, it is no longer actively maintained. Mandiant recommends that you plan a switch to Preview Integrations so you can take advantage of the latest features and functionality. Preview Integrations configuration steps are provided in the Director web interface. For more details, see the **Preview Integrations Documentation (https://docs.mandiant.com/home/msv-preview-integrations)**.

This integration is remote capable.

Update Sophos Central

TO ADD A TOKEN TO SOPHOS CENTRAL

1. Open Sophos Central's admin console.
2. Go to **Global Settings** and select **API Token Management**.
3. Click **Add Token**, enter the necessary information, and save your changes.
4. Make a note of both the authorization token and API key.

Update the Validation Platform

Prerequisites

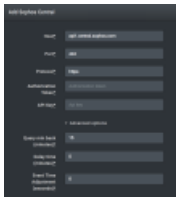
Information to gather before you start:

- Authorization token and API key for Sophos Central.
- The API URL for Sophos.

Configuration

TO ADD THE SOPHOS CENTRAL INTEGRATION

1. Go to **Settings** > **Integrations**.
2. Click **Add Integration** > **Sophos Central**
3. Enter **Host**, using the API URL for Sophos Central.
4. Set **Port** to 443.
5. Set **Protocol** to HTTPS.
6. Enter the authorization token and key from Sophos Central.
7. Expand **Advanced options** and update the information if necessary.
8. Click **Submit**.



(https://d383cql5uq169w.cloudfront.net/app/image/pid/620d7e13ccb103e8557b25b0/id/629a12e0c9cba0017c2f7e39/n/sophos.png)

Sophos Central Integration

Verify connectivity

TO VERIFY CONNECTIVITY TO SOPHOS CENTRAL

Click **Test** to verify that:

- The Director can communicate with Sophos Central on the port specified.
- The Authorization token and API key are valid and working.

SYMANTEC ENDPOINT PROTECTION

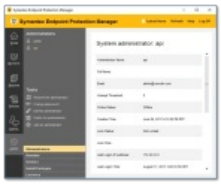
This document applies to Classic Integrations. While the Integrations solution is available, it is no longer actively maintained. Mandiant recommends that you plan a switch to Preview Integrations so you can take advantage of the latest features and functionality. Preview Integrations configuration steps are provided in the Director web interface. For more details, see the **Preview Integrations Documentation (https://docs.mandiant.com/home/msv-preview-integrations)**.

This integration can match events based on file hashes.

Update Symantec EP

TO UPDATE SYMANTEC EP

1. Log in to the Symantec Endpoint Protection Manager.
2. Create an admin user.
    a. Click **Admin** in the left-hand pane and select **Add an administrator**.



(https://d383cql5uq169w.cloudfront.net/app/image/pid/620d7e13ccb103e8557b25b0/id/629a12d7c9cba0017c2f7dd8/n/symaep-1a.png)

Create Symantec Endpoint Protection administrator

b. In the General tab, enter a **User name**, **Full name**, and **Email address**.

(https://d383cql5uq169w.cloudfront.net/app/image/pid/620d7e13ccb103e8557b25b0/id/629a12e8c9cba0017c2f7e84/n/symantec-ep-1.png)

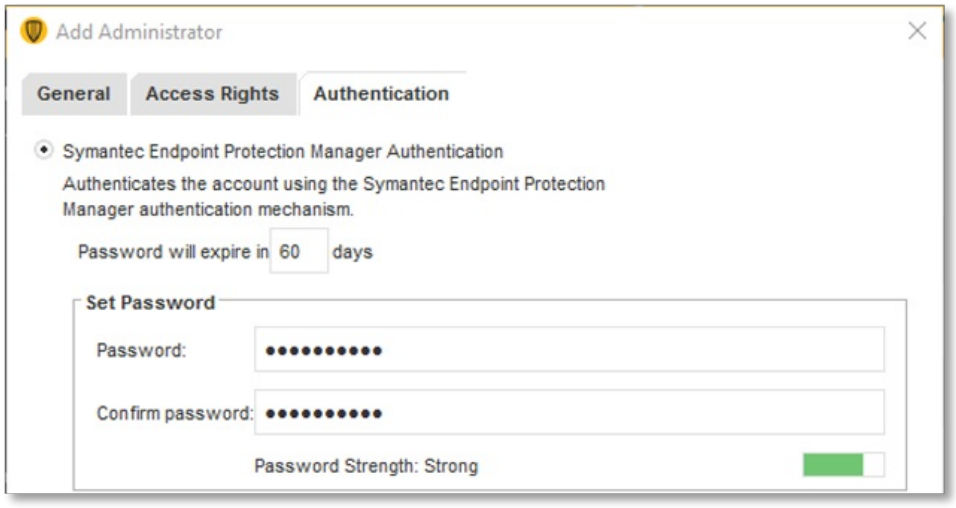
Enter Administrator information

c. In the Access Permissions tab, select **System Administrator**.

(https://d383cql5uq169w.cloudfront.net/app/image/pid/620d7e13ccb103e8557b25b0/id/629a12e5c9cba0017c2f7e6f/n/symantec-ep-2.png)

Add Administrator

d. On the Authentication tab, choose **Symantec Endpoint Protection Manager Authentication** and set a password. You may want to increase the password expiration time for this account (depending on your policy requirements for integration/service accounts).



Set Administrator password

e. Click **Save** to create the account.

If you're using Active Directory to authenticate your API user, the username must be specified in a non-standard manner:

- `:`
  or
  `\:`
- Examples: `svc-verodin:ACME.COM OR api-user\svc-verodin:ACME.COM`
- Reference: https://www.symantec.com/connect/forums/ad-user-authentication-dlp-reporting-and-updating-api#comment-8394101

Syncronize Systems

Time plays an important part in event matching when tests are run. After you update SEP, verify the following systems are all using the same time: the endpoint, the Validation Platform Director, the Windows system running SEP Manager (SEPM), and real time.

Update the Validation Platform

Prerequisites

Information to gather before you start:

1. Identify the IP address or hostname used to access Symantec Endpoint Protection.
2. Identify the port for Symantec Endpoint Protection communications (typically 8445).
3. Identify or create credentials to access Symantec Endpoint Protection.

Configuration

TO ADD THE SYMANTEC EP INTEGRATION

1. Go to **Settings** > **Integrations**.
2. Click **Add Integration** > **Symantec EP**.
3. Enter information for the **Host**, **Port**, **Username**, and **Password**.
4. Expand **Advanced options**.
5. (Optional) Update **Query time** and **Delay time**.

   The **Query time** is the amount of time (minutes) before and after the query runs that the looks for events, while the **Delay time** is the amount of time (minutes) that the platform waits to run the query after a Job Action. For example, you configure your integration with the following values: **Query time** = 5, **Query interval** = 30 seconds, and **Delay time** = 0. When a Job Actions starts at 12:00:00, the first time the query runs, the platform looks for events from 11:55:00 to 12:00:00. Then 30 seconds later, it looks for events from 11:55:30 to 12:00:30. This interval continues, with the last query looking from 12:00:00 to 12:05:00. If you instead configured the **Delay time** to equal 10, it would run the same query, but it wouldn't start that query until 12:10:00.

   If your monitors are set to run more frequently than the query time, it will impact the pass/fail results for AEDA monitors.

6. Verify that the correct **Version** is selected. Authentication may fail if the incorrect version is selected.
7. Select the **Timestamp Format**.
8. Modify the **Query Interval**, if necessary.
9. Modify the **Event Time Adjustment**.

   The timestamp retrieved from SEPM is not the time the event occurred on the host but is the time that SEPM received the event from the Symantec agent running on the host. The time difference varies from environment to environment, so you need to adjust the Event Time Adjustment field to account for the change in your environment. We have seen -12 work in many environments, but there is not a one-size-fits all value for it.

10. (Optional) Assign a **Name**.
11. (Optional) Choose **Yes** to save suspicious events.
12. Click **Submit**.

(https://d383cql5uq169w.cloudfront.net/app/image/pid/620d7e13ccb103e8557b25b0/id/629a12ddc9cba0017c2f7e14/n/symantec-ep.png)

Symantec Endpoint Protection Integration

Verify connectivity

TO VERIFY CONNECTIVITY TO SYMANTEC EP

Click **Test** to verify that:

- The Director can communicate with Symantec EP using the port specified.
- User credentials are working.

SYMANTEC DATA LOSS PREVENTION (DLP)

> This document applies to Classic Integrations. While the Integrations solution is available, it is no longer actively maintained. Mandiant recommends that you plan a switch to Preview Integrations so you can take advantage of the latest features and functionality. Preview Integrations configuration steps are provided in the Director web interface. For more details, see the **Preview Integrations Documentation (https://docs.mandiant.com/home/msv-preview-integrations)**.

This integration is not remote capable.

Update Symantec DLP

TO UPDATE SYMANTEC DLP

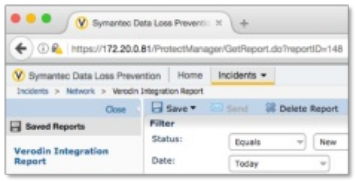
1. Note what version of Symantec DLP you have.
   - If your version is older than 15.7, see steps **4** and **5** below to gather required Report IDs.
   - If your version is newer than 15.7, identify the time zone used for your Symantec DLP server.
2. Verify that there is a role with adequate permissions for the API user to inherit.
   a. In Incidents section, select **View** and then **Perform Attribute Lookup**.
   b. In Incidents section, go to the Incident Reporting and Update API section, and select **Incident Reporting** and then **Incident Update**.
3. Create a user for the integration. Setup should include the following:
   a. Select **password access**.
   b. Under Report Preferences, select Include **Incident Violations in XML Export** and **Include Incident History in XML Export**.
   c. Assign the role from Step 1 to this user and make it the default role.

   This user can only be assigned one role.

   If you're using Active Directory to authenticate your API user, the username must be specified in a non-standard manner:

   - `:`
     or
     `\:`
   - Examples: `svc-verodin:ACME.COM OR api-user\svc-verodin:ACME.COM`
   - Reference: https://www.symantec.com/connect/forums/ad-user-authentication-dlp-reporting-and-updating-api#comment-8394101
4. (Optional) Log into the newly-created user account, and create a new Network Incident Report with the following settings:
   a. Set the Filter Status to **Equals** and **New**.
   b. Set the Filter Date to **Today**.
   c. Click **Advanced Filter & Summarization**.
   d. Add a Source IP filter.
   e. Add a **Is Any Of** condition.
   f. Add a comma-delimited list of Actor IP addresses.
   g. Save and name the report.
5. (Optional) Obtain the saved report ID number .
   a. In the left column of the DLP web UI, click the name of the newly created report

b. In the browser's location bar, find the report number located in the URL as `?reportID=`.



(https://d383cql5uq169w.cloudfront.net/app/image/pid/620d7e13ccb103e8557b25b0/id/629a12d4c9cba0017c2f7dba/n/symadlp.png)

Finding the Report Number

API Calls

The following API call is used by the Validation Platform.

Purpose	Call
Get incident details	`/ProtectManager/services/v2011/incidents`

Update the Validation Platform

Prerequisites

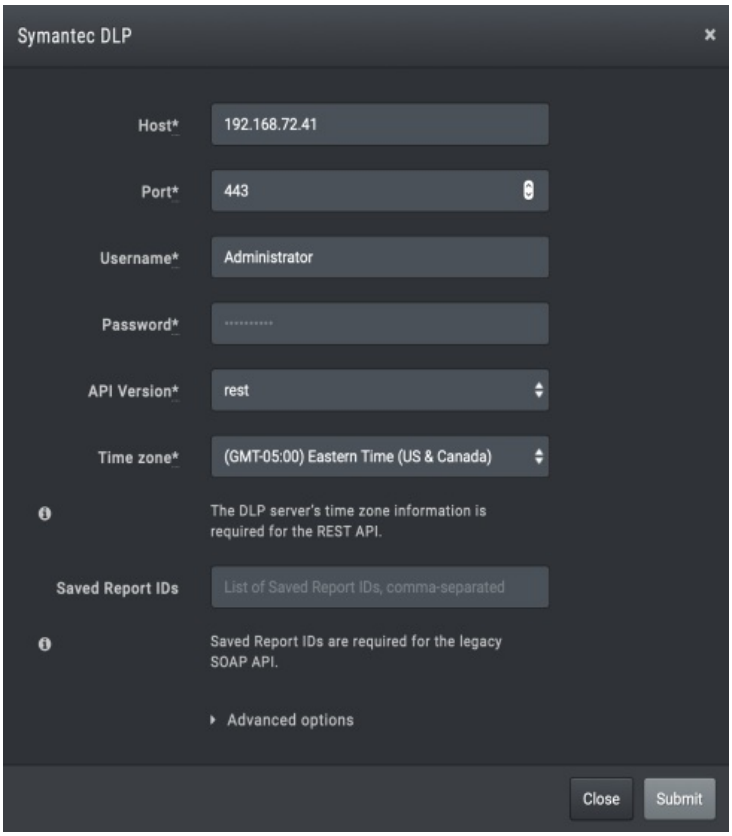
Information to gather before you start:

1. IP address or hostname used to access Symantec DLP.
2. Port for Symantec DLP communications (typically 443).
3. Identify the Symantec DLP user credentials.
4. Identify the timezone used for the Symantec DLP server.
5. Capture the list of Saved Report IDs.

Configuration

TO ADD THE SYMANTEC DLP INTEGRATION

1. Go to **Settings** > **Integrations**.
2. Click **Add Integration** > **Symantec DLP**.
3. Enter information for the **Host**, **Port**, **Username**, and **Password**.
4. Select the API used in your version of Symantec DLP.
    a. If you selected soap, enter the Saved Report IDs identified in **the steps above**.
    b. If you selected rest, enter the time zone of the Symantec DLP server.



Symantec DLP Integration

5. Expand **Advanced options** and update the information if necessary.
6. Click **Submit**.

Verify connectivity

TO VERIFY CONNECTIVITY TO SYMANTEC DLP

Click **Test** to verify that:

- The Director can communicate with Symantec DLP using the port specified.
- User credentials are working.

AWS CLOUDTRAIL

This document applies to Classic Integrations. While the Integrations solution is available, it is no longer actively maintained. Mandiant recommends that you plan a switch to Preview Integrations so you can take advantage of the latest features and functionality. Preview Integrations configuration steps are provided in the Director web interface. For more details, see the **Preview Integrations Documentation (https://docs.mandiant.com/home/msv-preview-integrations)**.

This requires the Cloud Validation license.

Using the Security Validation API, the AWS CloudTrail integration focuses on the management events performed on assets in the Amazon Web Services (AWS) platform.

Update AWS

You must have an AWS account.

- Create the API credentials and note the Access Key and Secret Access Key.

Update the Validation Platform

Prerequisites

Information to gather before you start:

- Add the AWS account to your Allow list.
- Know your Amazon region.
  The following regions are supported:
  - ap-northeast-1
  - ap-northeast-2
  - ap-northeast-3
  - ap-southeast-1
  - ap-southeast-2
  - ap-south1
  - ca-central-1
  - eu-central-1
  - eu-west-1
  - eu-west-2
  - eu-west-3
  - sa-east-1
  - us-east-1
  - us-east-2
  - us-west-1
  - us-west-2
  - us-gov-east-1
  - us-gov-west-1

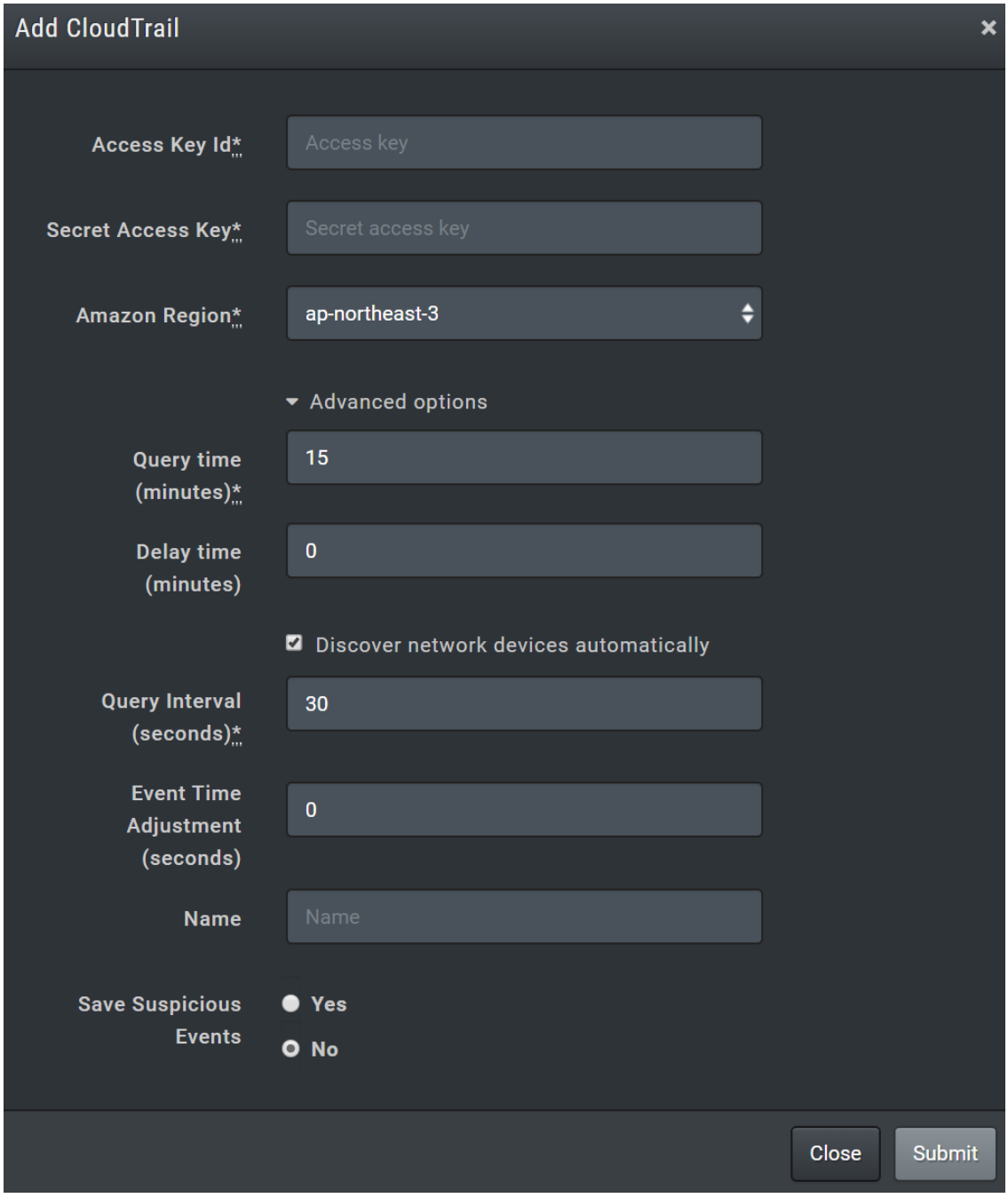
    See the **AWS documentation (https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.RegionsAndAvailabilityZones.html)** for information on the different regions and their full names.

- Have the Access key and the Secret access key

Configuration

TO ADD THE AWS CLOUDTRAIL INTEGRATION

1. Go to **Settings** > **Integrations**.
2. Click **Add Integration** > **CloudTrail**.



Add AWS CloudTrail

3. Enter the **Access key Id** and the **Secret access key**.
4. Select the **Amazon Region**.
5. Expand **Advanced options**.
6. Set the **Query time**.
7. (Optional) Set the **Delay time**.

8. (Optional) Select **Discover network devices automatically**.
9. Specify the **Query interval**.
10. (Optional) Set the **Event Time Adjustment**.
11. Assign a **Name**.
12. (Optional) Choose whether to save suspicious events.
13. Click **Submit**.

Verify connectivity

TO VERIFY CONNECTIVITY TO AWS CLOUDTRAIL

- Click **Test** to verify that the keys and region information is correct.

AWS CLOUDWATCH

This document applies to Classic Integrations. While the Integrations solution is available, it is no longer actively maintained. Mandiant recommends that you plan a switch to Preview Integrations so you can take advantage of the latest features and functionality. Preview Integrations configuration steps are provided in the Director web interface. For more details, see the **Preview Integrations Documentation (https://docs.mandiant.com/home/msv-preview-integrations)**.

This requires the Cloud Validation license.

Update AWS CloudWatch

Identify or create credentials to access CloudWatch with read access and CloudWatchLogsFullAccess permission, at minimum.

API Calls

The following API calls are used by the Validation Platform.

Purpose	Call
Create query	Ruby Aws::CloudWatchLogs::Client.start_query
Get query results	Ruby Aws::CloudWatchLogs::Client. get_query_results

Update the Security Validation Platform

Prerequisites

Information to gather before you start:

- CloudWatch Access Key ID

  An AWS admin can generate this for you.

- CloudWatch Secret Access Key
- The Amazon region associated with your account.
  The following regions are supported:
  - ap-northeast-1
  - ap-northeast-2
  - ap-northeast-3
  - ap-southeast-1
  - ap-southeast-2
  - ap-south1
  - ca-central-1
  - eu-central-1
  - eu-west-1
  - eu-west-2
  - eu-west-3
  - sa-east-1
  - us-east-1
  - us-east-2
  - us-west-1

- us-west-2
- us-gov-east-1
- us-gov-west-1

> See the **AWS documentation (https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.RegionsAndAvailabilityZones.html)** for information on the different regions and their full names.

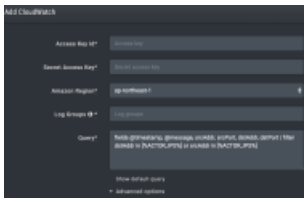
Configuration

TO ADD THE AWS CLOUDWATCH INTEGRATION

1. Go to **Settings** > **Integrations**.
2. Click **Add Integration** > **CloudWatch**.

> You can add this as either a Local or Remote Inetgration.

3. Enter the **Access key Id** and the **Secret Access Key**.
4. Select an **Amazon Region**.
5. Enter the **Log Groups** from CloudWatch.
6. (Optional) Configure the **Query**.



(https://d383cql5uq169w.cloudfront.net/app/image/pid/620d7e13ccb103e8557b25b0/id/629a12e3c9cba0017c2f7e54/n/aws-cloudwatch.png)

AWS Cloudwatch Integration

7. Expand **Advanced options**.
8. (Optional) Update **Query time** and **Delay time**.

> The **Query time** is the amount of time (minutes) before and after the query runs that the looks for events, while the **Delay time** is the amount of time (minutes) that the platform waits to run the query after a Job Action. For example, you configure your integration with the following values: **Query time** = 5, **Query interval** = 30 seconds, and **Delay time** = 0. When a Job Actions starts at 12:00:00, the first time the query runs, the platform looks for events from 11:55:00 to 12:00:00. Then 30 seconds later, it looks for events from 11:55:30 to 12:00:30. This interval continues, with the last query looking from 12:00:00 to 12:05:00. If you instead configured the **Delay time** to equal 10, it would run the same query, but it wouldn't start that query until 12:10:00.

> If your monitors are set to run more frequently than the query time, it will impact the pass/fail results for AEDA monitors.

9. (Optional) Select **Enable query for Malicious DNS Actions**, then
   a. Enter the Log Groups to use with Malicious DNS Actions
   b. Configure the **Query**.

This query will only be used when you run Malicious DNS Actions or Captive DNS Actions.

10. (Optional) Select **Enable query for Email Actions**, then
    a. Enter the Log Groups to use with Email Actions.
    b. Configure the **Query**.

    This query will only be used when you run Malicious DNS Actions or Captive DNS Actions.

11. (Optional) Select **Enable query for Host CLIActions** and:
    a. Enter the Log Groups to use with Host CLI Actions
    b. Configure the **Query**.

    This query will only be used when you run Malicious DNS Actions or Captive DNS Actions.

12. Identify the field name mappings for the following (there could be multiple of each, depending on log sources and configuration): **Verify full list and order in UI**
    - Source IP
    - Destination IP
    - Source Port
    - Destination Port
    - Event Source Host
    - Event Start Time (timestamp)
    - Unique ID
    - Event Signature ID
    - Event Description
    - Email Sender
    - Email Recipient
    - Email Subject
    - URL
    - Username
13. Modify the **Query Interval** and **Event Time Adjustment**, if necessary.
14. (Optional) Assign a **Name**.
15. (Optional) Choose **Yes** to save suspicious events.
16. Click **Submit**.

AWS CloudWatch Integration (Advanced Options)

Verify connectivity

TO VERIFY CONNECTIVITY TO AWS CLOUDWATCH

Click **Test** to verify that:

- The Director can communicate with the integration host on the port and protocol specified.
- The integration credentials are valid and working.

AWS GUARDDUTY

This document applies to Classic Integrations. While the Integrations solution is available, it is no longer actively maintained. Mandiant recommends that you plan a switch to Preview Integrations so you can take advantage of the latest features and functionality. Preview Integrations configuration steps are provided in the Director web interface. For more details, see the **Preview Integrations Documentation (https://docs.mandiant.com/home/msv-preview-integrations)**.

This requires the Cloud Validation license.

The Amazon GuardDuty integration provides events similar to a firewall or endpoint AV tool.

This integration is currently limited since it's behavior based. This means once it identifies a threat & you tell it that it's ok, it will no longer fire on that threat.

Update AWS

You must have an AWS account.

- Create the API credentials and note the Access Key and Secret Access Key.

Update the Validation Platform

Prerequisites

Information to gather before you start:

- Add the AWS account to your Allow list
- Know your Amazon region.
  The following regions are supported:
  - ap-northeast-1
  - ap-northeast-2
  - ap-northeast-3
  - ap-southeast-1
  - ap-southeast-2
  - ap-south1
  - ca-central-1
  - eu-central-1
  - eu-west-1
  - eu-west-2
  - eu-west-3
  - sa-east-1
  - us-east-1
  - us-east-2
  - us-west-1
  - us-west-2
  - us-gov-east-1
  - us-gov-west-1

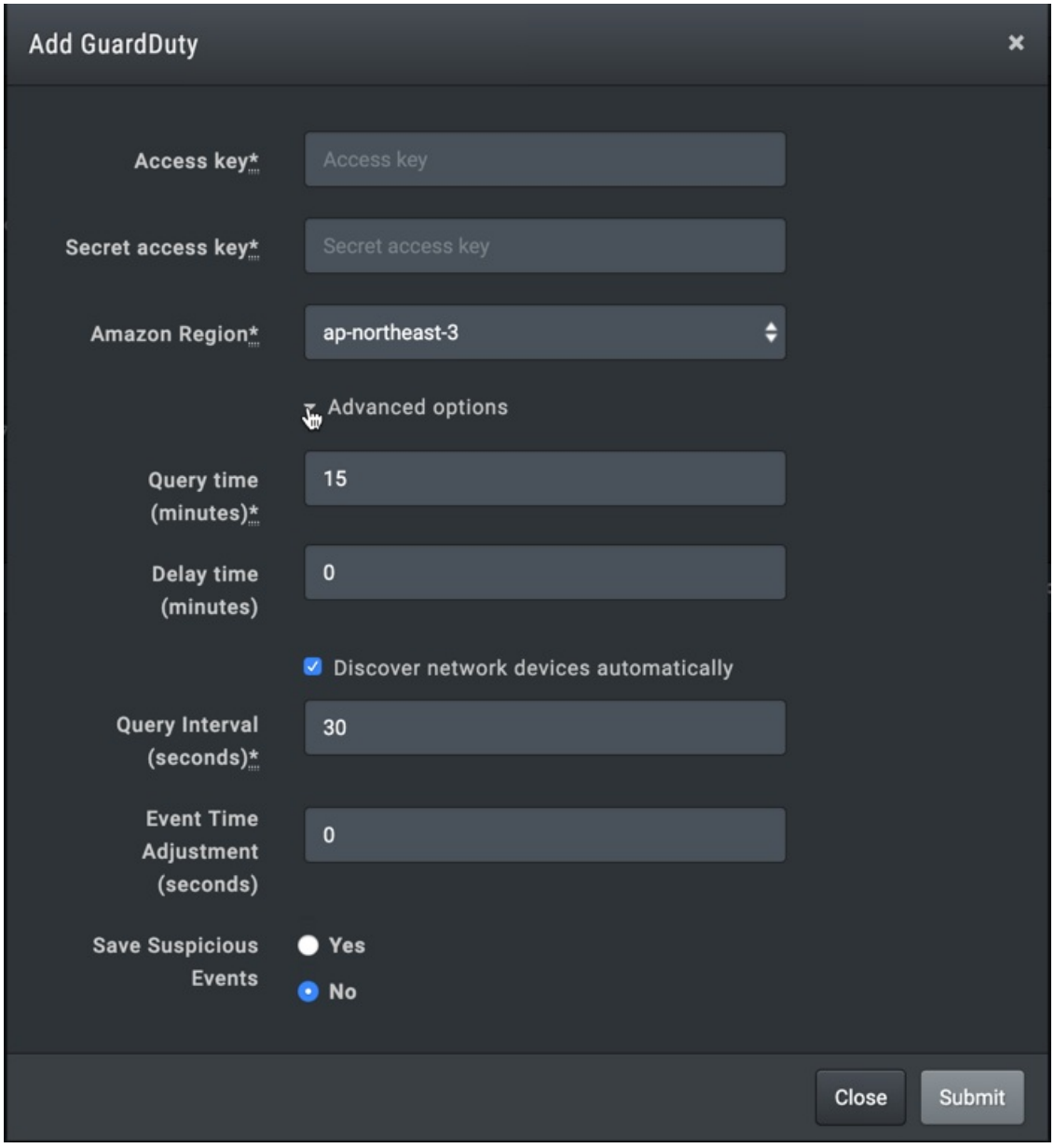
    See the **AWS documentation (https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.RegionsAndAvailabilityZones.html)** for information on the different regions and their full names.

- Have the Access key and the Secret access key

Configuration

TO ADD THE AWS CLOUDTRAIL INTEGRATION

1. Go to **Settings** > **Integrations**.
2. Click **Add Integration** > **GuardDuty**.



Add AWS GuardDuty

3. Enter the **Access key Id** and the **Secret access key**.
4. Select the **Amazon Region**.
5. Expand **Advanced options**.
6. Update the **Query time** and the **Delay time** information.
7. (Optional) Select **Discover network devices automatically**.
8. Specify the **Query interval**.

9. (Optional) Set the **Event Time Adjustment**.
10. Assing a **Name**.
11. (Optional) Choose whether to save suspicious events.
12. Click **Submit**.

Verify connectivity

TO VERIFY CONNECTIVITY TO AWS GUARDDUTY

- Click **Test** to verify that the keys and region information is correct.

CHECK POINT

> This document applies to Classic Integrations. While the Integrations solution is available, it is no longer actively maintained. Mandiant recommends that you plan a switch to Preview Integrations so you can take advantage of the latest features and functionality. Preview Integrations configuration steps are provided in the Director web interface. For more details, see the **Preview Integrations Documentation (https://docs.mandiant.com/home/msv-preview-integrations)**.

This integration is not remote capable.

Update Check Point

Check Point requires several initial configuration steps. For help completing the configuration, please review Check Point's documentation and contact their support team as necessary.

Prerequisites

Before starting the update, gather this information:

- Identify your Check Point version.
- Determine where the logs are being sent (Check Point Management or to a separate log server).
- Download the Check Point `opsec_pull_cert` utility. You can find this utility on the Check Point Support Center site.

TO CONFIGURE CHECK POINT (OVERVIEW)

1. Locate and read the Check Point OPSEC LEA documentation. You can find this on the Check Point Support Center site.
2. Download the `OPSEC SDK 6.1 tar.gz` file.
3. Create the OPSEC application.
    a. Use the Check Point SmartConsole or the desired CMA/Domain on the Provider.
    b. Name the new OPSEC application ***VerodinLEA***.

    You can use any name, but VerodinLEA is recommended by convention.

    The Security Validation integration with Check Point currently only supports the sslca auth method.

    c. Consult the Check Point documentation for more information.
4. Create an OPSEC application certificate in the Check Point SmartConsole using the command line.
    a. Run the following command in the Check Point `opsec_pull_cert` utility with the correct information from the customer:
    `opsec_pull_cert -h -n -p -o c:\cert\opsec.p12`
    b. Capture the one-time password you enter; this will be used when you create an OPSEC LEA connection and pull the p12 authentication file.

    The password must not include any of the following special characters: exclamation (!), circumflex accent (^), tilde (~), grave accent (`), quotation ("), or apostrophe (').

    c. Consult the Check Point documentation for more information.
5. After the OPSEC application initializes, note the opsec_sic_name that is generated. You will need this opsec_sic_name and the LEA server's opsec_sic_name.

a. The Server OPSEC SIC name and the OPSEC Sic name are tied to the certificate created in step 4 above.
b. You can also get the OPSEC SIC name and LEA Server OPSEC SIC name by running this command in Expert mode from the management server. Look for the SmartConsole SIC ID in the results to get the correct name:
`cpca_client lscert -stat Valid -kind SIC`

6. Install the database.
    a. In the SmartConsole, under Policy, install the database for your Management Server.
    b. Consult the Check Point documentation for more information.

Update the Validation Platform

Prerequisites

Information to gather before you start:

1. Ensure that you are running CentOS 7.0 or newer.
2. Have the OPSEC SDK Dependency file (Check_Point_OPSEC_SDK_6.1_linux50.tar.gz). See Check Point's knowledge base for more information.
3. Have an active, configured OPSEC LEA Application for use with the Validation Platform.
    a. Obtain OPSEC authentication file.
    b. Identify the LEA Server IP and Port (this defaults to 18184).
    c. Identify the OPSEC SIC and LEA Server OPSEC SIC names you noted in Step 5 above.

Configuration

TO ADD THE CHECK POINT INTEGRATION

1. Go to **Settings** > **Integrations**.
2. Click **Add Integration** > **Check Point**.
3. Browse for and select the OPSEC SDK 6.1 tar.gz file. When selected, the file will immediately start uploading.
4. Enter **IP**, **Port**, **OPSEC SIC Name**, and **LEA Server OPSEC SIC Name**. See **Check Point Firewall Integration (https://d383cql5uq169w.cloudfront.net/app/image/pid/620d7e13ccb103e8557b25b0/id/629a12d8c9cba0017c2f7ddf/n/checkpoint.pr**
    - In the **OPSEC SIC Name** field, enter the OPSEC Application name you created in Step 3 in **To configure Check Point (overview)**
    - In the **LEA Server OPSEC SIC Name** field, enter the SmartConsole SID ID you noted in Step 5 in **To configure Check Point (overview)**.
5. Browse for and select the OPSEC Key (.p12 authentication) file.
6. Expand **Advanced options**.
7. Modify the **Query Interval** and **Event Time Adjustment**, if necessary.
8. (Optional) Assign a **Name**.
9. (Optional) Choose **Yes** to save suspicious events.
10. Click **Submit**.

(https://d383cql5uq169w.cloudfront.net/app/image/pid/620d7e13ccb103e8557b25b0/id/629a12d8c9cba0017c2f7ddf/n/checkpoint.png)

Check Point Firewall Integration

Verify connectivity

TO VERIFY CONNECTIVITY TO CHECK POINT

Click **Test** to verify that the Director can communicate with the Check Point host using the provided setup information.

CISCO FIREPOWER MANAGEMENT CENTER (FMC)

> This document applies to Classic Integrations. While the Integrations solution is available, it is no longer actively maintained. Mandiant recommends that you plan a switch to Preview Integrations so you can take advantage of the latest features and functionality. Preview Integrations configuration steps are provided in the Director web interface. For more details, see the **Preview Integrations Documentation (https://docs.mandiant.com/home/msv-preview-integrations)**.

This integration is not remote capable.

Update Cisco FMC

TO UPDATE CISCO FMC

- Configure FMC to enable Database Access.
- Identify or create credentials to access FMC with read permissions, at minimum.

Update the Validation Platform

Prerequisites

Information to gather before you start:

- Have the JDBC Driver (see Chapter 2 of the Firepower Systems Database Guide. This file will be in the client.zip)
- Obtain the version of Java that works with FMC; this is `jre-8u181-linux-x64.rpm` and should be approximately 62MB in size.
- Identify the hostname/IP for FMC communications.
- Identify the Port used (this defaults to 2000).
- Open the Ports 1500 and 2000 to allow the system to communicate.
- Obtain a username and password.

Configuration

TO ADD THE CISCO FIREPOWER INTEGRATION

1. Go to **Settings** > **Integrations**.
2. Click **Add Integration** > **Cisco Firepower**.

(https://d383cql5uq169w.cloudfront.net/app/image/pid/620d7e13ccb103e8557b25b0/id/629a12edc9cba0017c2f7ead/n/cisco-firepower-management.png)

Cisco Firepower Integration

3. If you see a message that Java is not installed, go to the **Upload Java RPM** field, click **Browse**, and select the install file; once you select it, the install will start.

   you will not be able to click **Submit** until Java has finished installing.

4. Enter information for the **Host**, **Port**, **Username**, and **Password**.
5. Review and update the **Query**.

6. Review and update the **File query**.
7. Select the **Version**.
8. Click **Browse**, then select the Client Zip file you downloaded.
9. Expand **Advanced options**.

(https://d383cql5uq169w.cloudfront.net/app/image/pid/620d7e13ccb103e8557b25b0/id/629a12dec9cba0017c2f7e2b/n/cisco-firepower-management-1.png)

Cisco Firepower Integration (Advanced Options)

10. (Optional) Update **Query time** and **Delay time**.

> The **Query time** is the amount of time (minutes) before and after the query runs that the looks for events, while the **Delay time** is the amount of time (minutes) that the platform waits to run the query after a Job Action. For example, you configure your integration with the following values: **Query time** = 5, **Query interval** = 30 seconds, and **Delay time** = 0. When a Job Actions starts at 12:00:00, the first time the query runs, the platform looks for events from 11:55:00 to 12:00:00. Then 30 seconds later, it looks for events from 11:55:30 to 12:00:30. This interval continues, with the last query looking from 12:00:00 to 12:05:00. If you instead configured the **Delay time** to equal 10, it would run the same query, but it wouldn't start that query until 12:10:00.

> If your monitors are set to run more frequently than the query time, it will impact the pass/fail results for AEDA monitors.

11. (Optional) Change the **Java Keystore Password** and **Java Keystore Path**.

> These fields will be pre-populated with the default information and only need to be modified if you've updated the password or path.

12. (Optional) Select the check box **Enable Cisco AMP Support** and adjust the **Amp query** as needed.
13. (Optional) Select the check box **Enable the special query for Host CLI Actions** and add the query.
14. Modify the **Query Interval** and **Event Time Adjustment**, if necessary.
15. (Optional) Assign a **Name**.
16. (Optional) Choose **Yes** to save suspicious events.
17. (Optional) Select **Discover network devices automatically**.
18. Click **Submit**.

> If you enable the Host CLI Actions query and use the %HOST_CLI_ACTOR_HOSTNAMES% variable, the platform will substitute the plain hostname and the information from the Alternate Hostname field on the Actor configuration page.

Verify connectivity

TO VERIFY CONNECTIVITY TO CISCO FMC

Click **Test** to verify that the Director can communicate with the Cisco FMC host using the provided host, port, and user

credentials.

DARKTRACE

> This document applies to Classic Integrations. While the Integrations solution is available, it is no longer actively maintained. Mandiant recommends that you plan a switch to Preview Integrations so you can take advantage of the latest features and functionality. Preview Integrations configuration steps are provided in the Director web interface. For more details, see the **Preview Integrations Documentation (https://docs.mandiant.com/home/msv-preview-integrations)**.

This integration is remote capable.

Update integration

Identify or create an API key for use with the Validation Platform. This is done by signing into Darktrace and going to Admin > Config > API Token Generate.

API Calls

The following API calls are used by the Validation Platform.

Purpose	Call
Verify we can read devices	`/devices?seensince=7days`
Get Device Specific Details by IP	`/devices?ip=:ip`
Get Events for Device within specific timeframe	`/details?did=:did&starttime=:start_time&endtime=:end_time`

Update the Validation Platform

Prerequisites

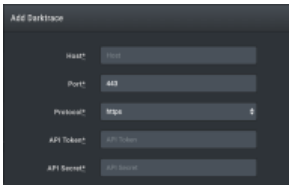
Information to gather before you start:

- Hostname
- Port
- API Key
- API Secret

Configuration

TO ADD THE INTEGRATION

1. Go to **Settings** > **Integrations**.
2. Click **Add Integration** > **Darktrace**.



(https://d383cql5uq169w.cloudfront.net/app/image/pid/620d7e13ccb103e8557b25b0/id/629a12e9c9cba0017c2f7e8d/n/darktrace1.

Darktrace Integration

3. Enter the **Host** and **Port**.
4. Select the **Protocol**.
5. Enter the **API Token** and **API Secret**.
6. Expand **Advanced options**.

(https://d383cql5uq169w.cloudfront.net/app/image/pid/620d7e13ccb103e8557b25b0/id/629a12e7c9cba0017c2f7e7a/n/darktrace-adv.png)

Advanced section of Darktrace Integration

7. (Optional) Update **Query time** and **Delay time**.

> The **Query time** is the amount of time (minutes) before and after the query runs that the looks for events, while the **Delay time** is the amount of time (minutes) that the platform waits to run the query after a Job Action. For example, you configure your integration with the following values: **Query time** = 5, **Query interval** = 30 seconds, and **Delay time** = 0. When a Job Actions starts at 12:00:00, the first time the query runs, the platform looks for events from 11:55:00 to 12:00:00. Then 30 seconds later, it looks for events from 11:55:30 to 12:00:30. This interval continues, with the last query looking from 12:00:00 to 12:05:00. If you instead configured the **Delay time** to equal 10, it would run the same query, but it wouldn't start that query until 12:10:00.

> If your monitors are set to run more frequently than the query time, it will impact the pass/fail results for AEDA monitors.

8. (Optional) Clear **Discover network devices automatically**.
9. Modify the **Query Interval** and **Event Time Adjustment**, if necessary.
10. (Optional) Assign a **Name**.
11. (Optional) Choose **Yes** to save suspicious events.
12. Click **Submit**.

Verify connectivity

TO VERIFY CONNECTIVITY TO INTEGRATION

Click **Test** to verify that:

- The Director can communicate with the integration host on the port and protocol specified.
- The integration credentials are valid and working.

If you see the following error, either the API Key or the API Secret is incorrect or there is a time mismatch:

```
Api signature Error
```

Requests to API are signed with a timestamp. If the requesting machine (Director or Remote Actor) is out of time sync more than a few minutes, the requests will fail.

EXABEAM ADVANCED ANALYTICS

> This document applies to Classic Integrations. While the Integrations solution is available, it is no longer actively maintained. Mandiant recommends that you plan a switch to Preview Integrations so you can take advantage of the latest features and functionality. Preview Integrations configuration steps are provided in the Director web interface. For more details, see the **Preview Integrations Documentation (https://docs.mandiant.com/home/msv-preview-integrations)**.

This integration is remote capable.

Update Exabeam Advanced Analytics

Identify or create credentials to access Exabeam Advanced Analytics with read access, at minimum. The Validation Platform uses the Exabeam user profile to query for events, so it is important that you identify an Exabeam user profile with the appropriate permissions.

API Calls

The following API calls are used by the Validation Platform.

Purpose	Call
Authentication login	/api/auth/login?username=:username&password=:password
Authentication logout	/api/auth/logout
Get user sessions	/uba/api/user/:username/timeline/entities/all
Get details from a specific session	/uba/api/session/:session_id/info

The Director time must be synchronized in order to successfully make API calls. Discrepancies in time will result in test query failure and missed events.

Update the Validation Platform

Prerequisites

Information to gather before you start:

- Identify the hostname/IP used to access Exabeam Advanced Analytics.
- Identify the Port used for Exabeam Advanced Analytics communication (this defaults to 8484).
- Identify whether the protocol is HTTP or HTTPS for connections to the Exabeam Advanced Analytics port.
- Obtain the username and password of an Exabeam account with appropriate access permissions; or, obtain an API token from the Exabeam Portal.

  For older versions of Exabeam Analytics (i51 and older), use username/password authentication.
  For newer versions of Exabeam Analytics (i52 and newer), use the API Token authentication.

Configuration

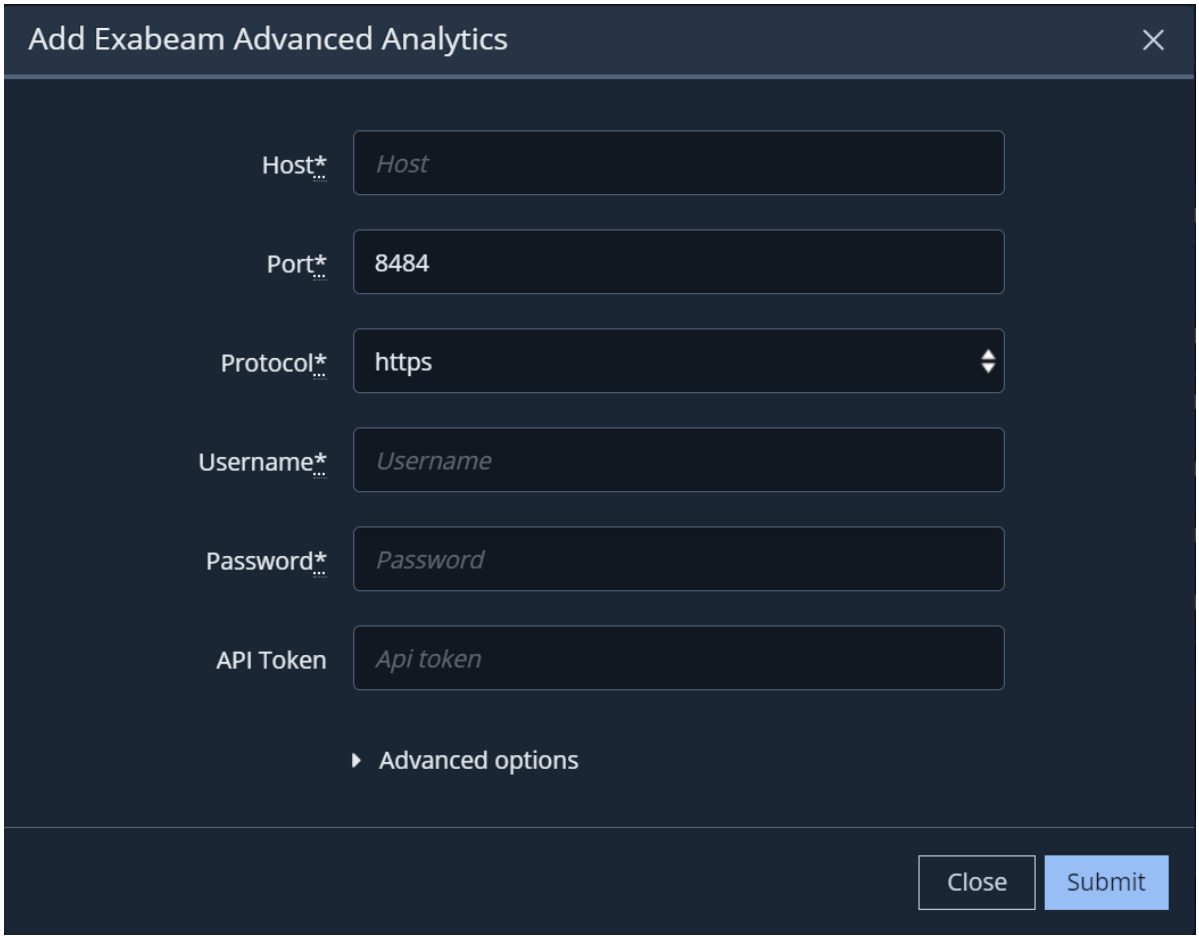
TO ADD THE EXABEAM ADVANCED ANALYTICS INTEGRATION

1. Go to **Settings** > **Integrations**.
2. Click **Add Integration** > **Exabeam Advanced Analytics**.
3. Enter information for the **Host**, **Port**, **Protocol**, **Username** and **Password** or **API Token**.

If you are authenticating your Exabeam account with Domain Logon (Active Directory), you must enter the username in lower case. For example, the username `ExampleUserName` would need to be entered as `exampleusername`.

4. Expand **Advanced options** and update the information if necessary.
5. Click **Submit**.

You must select the Exabeam user profile when running an Action in order for the Action to be recognized by Exabeam queries.



Exabeam Advanced Analytics Integration

Verify connectivity

TO VERIFY CONNECTIVITY TO EXABEAM ADVANCED ANALYTICS

Click **Test** to verify that:

- The Director can communicate with the Exabeam host on the port and protocol specified.
- The Exabeam credentials are valid and working.

TRELLIX EMAIL SECURITY - CLOUD (ETP)

> This document applies to Classic Integrations. While the Integrations solution is available, it is no longer actively maintained. Mandiant recommends that you plan a switch to Preview Integrations so you can take advantage of the latest features and functionality. Preview Integrations configuration steps are provided in the Director web interface. For more details, see the **Preview Integrations Documentation (https://docs.mandiant.com/home/msv-preview-integrations)**.

To validate the effectiveness of Trellix Email Security - Cloud (ETP), this integration uses the Trellix Email Security - Cloud (ETP) API. When you run email Actions, the Trellix Email Security - Cloud (ETP) API will use a verdict (Antispam, Antivirus, Advanced Threat, or Clean) and an action (Delivered, Rejected, or Quarantined) to determine whether the Action has passed or failed.


This integration is remote capable.

Update Trellix Email Security - Cloud (ETP)

Using your IAM account, create an API key for use with the Validation Platform. Verify your key has the same Email Security entitlements used in other API keys.

API Calls

The following API calls are used by Validation Platform.

Purpose	Call
Get email metadata	`/api/v1/messages/trace`
Get alert info	`/api/v1/alerts`

Update the Security Validation Platform

Prerequisites

Information to gather before you start:

- Identify your Trellix Email Security - Cloud (ETP) host, which is dependent on the region associated with your instance.
- Identify your API key.

Configuration

TO ADD THE TRELLIX EMAIL SECURITY - CLOUD (ETP) INTEGRATION

1. Go to **Settings** > **Integrations**.
2. Click **Add Integration** > **Trellix Email Security - Cloud (ETP)**.

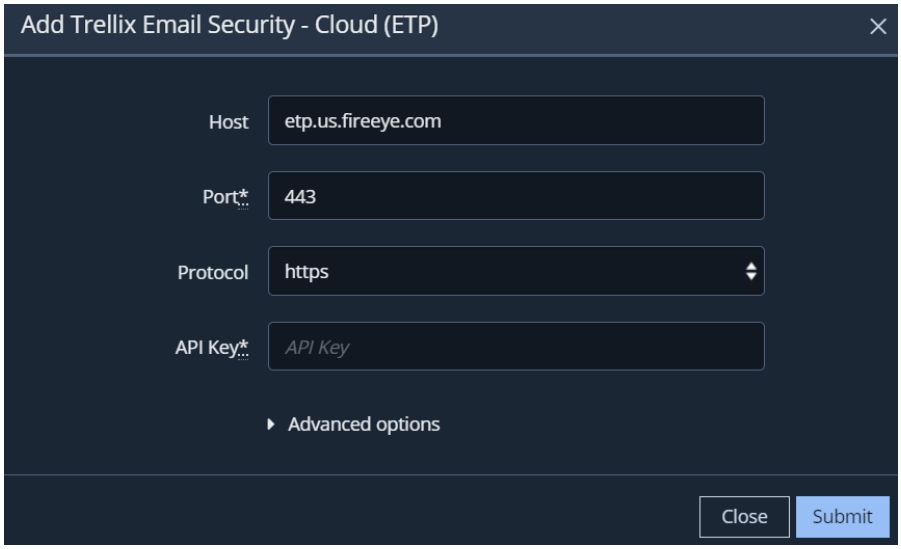
   
   You can add this as either a Local or Remote Integration.

3. Enter information for the **Host**, **Port**, and **Protocol**.
4. Enter your API key.
5. Expand **Advanced options**.
6. (Optional) Update **Query time** and **Delay time**.

The **Query time** is the amount of time (minutes) before and after the query runs that the looks for events, while the **Delay time** is the amount of time (minutes) that the platform waits to run the query after a Job Action. For example, you configure your integration with the following values: **Query time** = 5, **Query Interval** = 30 seconds, and **Delay time** = 0. When a Job Actions starts at 12:00:00, the first time the query runs, the platform looks for events from 11:55:00 to 12:00:00. Then 30 seconds later, it looks for events from 11:55:30 to 12:00:30. This interval continues, with the last query looking from 12:00:00 to 12:05:00. If you instead configured the **Delay time** to equal 10, it would run the same query, but it wouldn't start that query until 12:10:00.

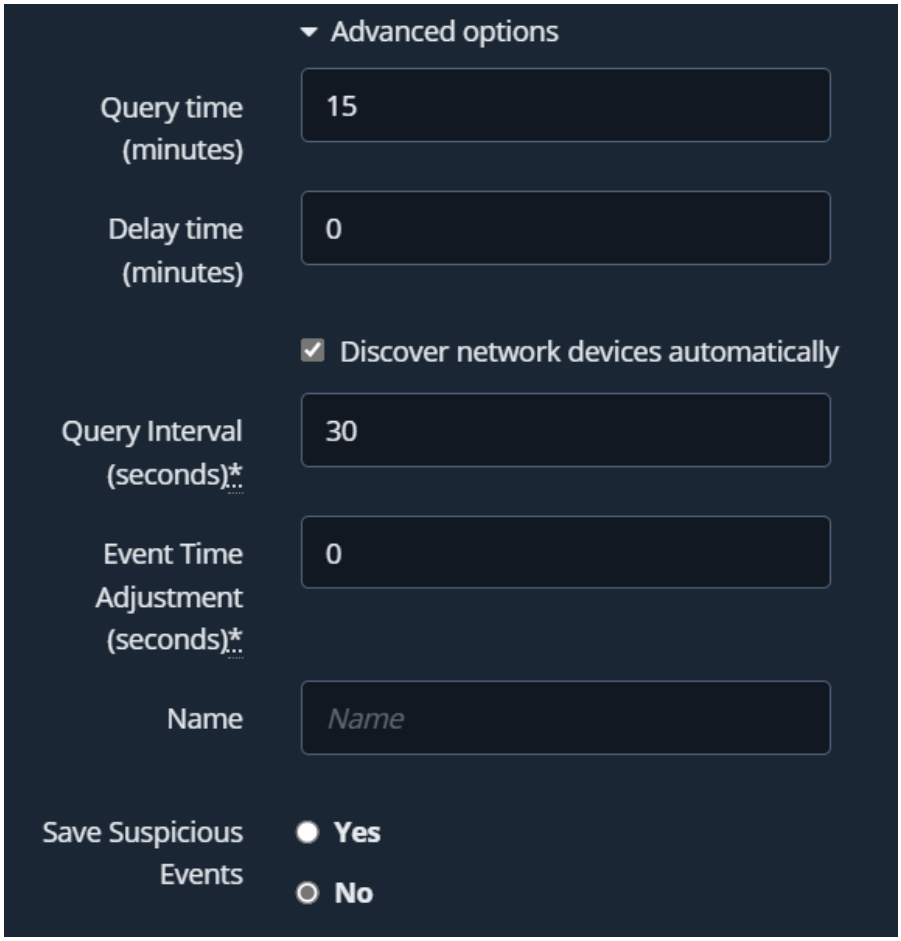
If your monitors are set to run more frequently than the query time, it will impact the pass/fail results for AEDA monitors.

7. (Optional) Select **Discover network devices automatically**.
8. Modify the **Query Interval** and **Event Time Adjustment**, if necessary.
9. (Optional) Assign a **Name**.
10. (Optional) Choose **Yes** to save suspicious events.
11. Click **Submit**.



(https://app.knowledgeowl.com/app/image/pid/620d7e13ccb103e8557b25b0/id/63ebf6fa0846174d1601ecf8/n/trellix-email-security-cloud-etp.png?imgkey=3c1881a2cce84a39ccf1bf98f3036ff3)

Trellix Email Security - Cloud (ETP) Integration



(https://app.knowledgeowl.com/app/image/pid/620d7e13ccb103e8557b25b0/id/63ecf35c8cd1f37fec0fe5da/n/trellix-email-security-cloud-etp-advanced-options.png?imgkey=3c1881a2cce84a39ccf1bf98f3036ff3)

Trellix Email Security - Cloud (ETP) Integration - Advanced options

Verify Connectivity

TO VERIFY CONNECTIVITY TO TRELLIX EMAIL SECURITY - CLOUD (ETP)

Click **Test** to verify that:

- The Director can communicate with the integration host on the port and protocol specified.
- The integration credentials are valid and working.

TRELLIX NETWORK SECURITY (NX) INTEGRATION

> This document applies to Classic Integrations. While the Integrations solution is available, it is no longer actively maintained. Mandiant recommends that you plan a switch to Preview Integrations so you can take advantage of the latest features and functionality. Preview Integrations configuration steps are provided in the Director web interface. For more details, see the **Preview Integrations Documentation (https://docs.mandiant.com/home/msv-preview-integrations)**.

The Trellix Network Security (NX) integration enables the Validation Platform Director to pull events from many of Trellix's products, including Central Management (CM Series), Network Security (NX Series), and Email Security (EX Series).

This integration is remote capable.

Update Trellix

1. Enable the Trellix API.
    a. In a terminal window, log in to the command-line interface (CLI) on the appliance where you will run the Web Services API.
    b. Enable the CLI configuration mode:

```
hostname > enable
hostname # configure terminal
```

    c. Enable the Web Services API:

```
hostname (config) # wsapi enable
```

    d. Verify that the Web Service API is enabled.
    For example, if you run the `show wsapi` command on the Trellix CM 4400 and the Web Services API is enabled, the Server Enabled status should be **yes**.

```
Hostname (config) # show wsapi
wsapi status:
Server Enabled:yes
Current State:running
Max Alerts:200
Max Minute Threshold:1000
Max Day Threshold:1000000
OS Changes:no
```

2. Create a Web Services API User Account (api_analyst or api_monitor) that has monitor/read access.
    - api_analyst can read and update alerts, read reports and statistics, and submit objects.
    - api_monitor can read alerts and read reports.

For full details on setting up user accounts, see the appropriate Trellix Administration Guide.

API Calls

The following API calls are used by the Validation Platform.

Purpose	Call
Login for a token	`/wsapis/v2.0.0/auth/login`
Logout	`/wsapis/v2.0.0/auth/logout`
Alerts query	`/wsapis/v2.0.0/alerts?start_time='%Y-%m-%dT%H:%M:%S.%L%:z'`
SmartVision Alerts	`/wsapis/v2.0.0/smartvision/alert`
IPS Events	`/wsapis/v2.0.0/events`

Update the Validation Platform

Prerequisites

Information to gather before you start:

1. Identify the Trellix Host and Port information.
2. Have a monitor/read Web Services API User Account.

To add the Trellix Network Security (NX) integration

1. Go to **Settings** > **Integrations**.
2. Click **Add Integration** > **Trellix Network Security (NX)**.

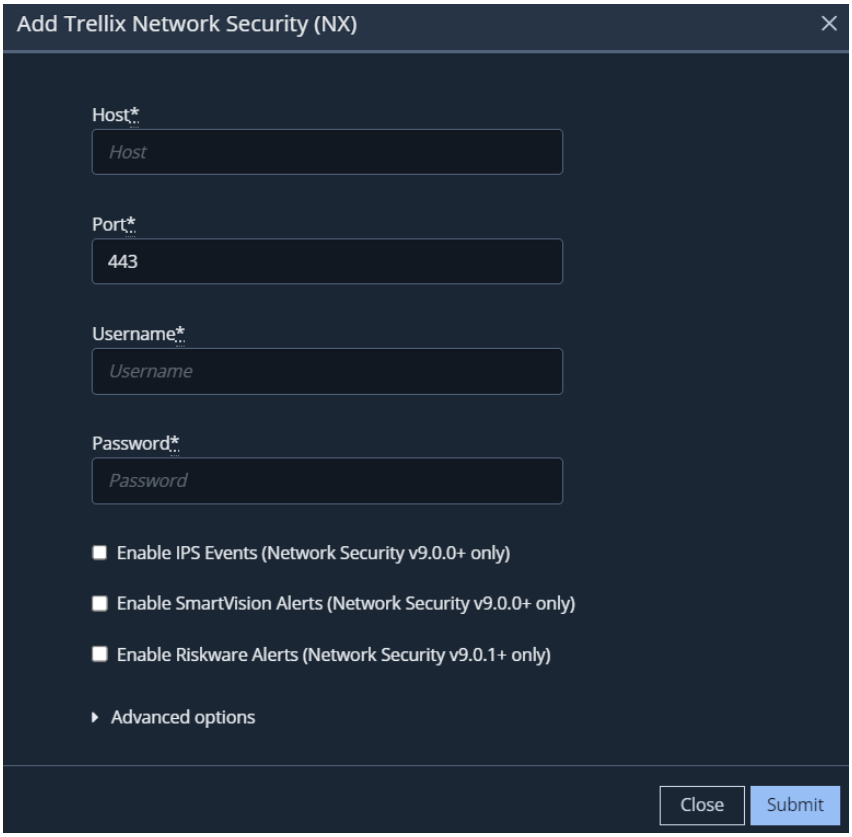
   You can add this as either a Local or Remote Integration.

3. Enter information for the **Host**, **Port**, **Username**, and **Password**.
4. (Optional) **Enable IPS Events**, **Enable SmartVision Alerts**, or **Enable Riskware Alerts**, as necessary.

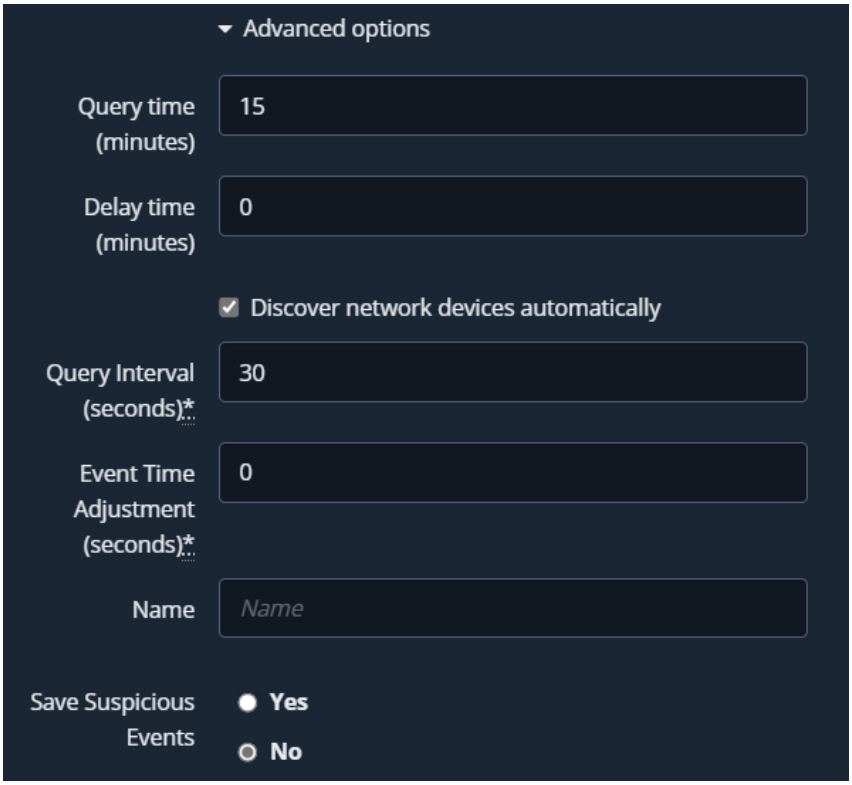
   Events correlated to Network Security IPS Events and SmartVision Alerts include "IPS Event" and "SmartVision Alert" in the event message section, respectively.

5. Expand **Advanced options** and update the information if necessary.
6. Click **Submit**.

   The query includes information that allows event matching based on any file hashes included in an Action.



Trellix Network Security (NX) Integration



Trellix Network Security (NX) Integration - Advanced options

Verify Connectivity

Click **Test** to verify that:

- The Director can communicate with the Trellix console using the provided host and user information.
- The API Server is enabled and allowing communication.

If the test is not successful, messages will be displayed to help identify possible issues, such as no connection to the API server.

TRELLIX NETWORK DLP

> This document applies to Classic Integrations. While the Integrations solution is available, it is no longer actively maintained. Mandiant recommends that you plan a switch to Preview Integrations so you can take advantage of the latest features and functionality. Preview Integrations configuration steps are provided in the Director web interface. For more details, see the **Preview Integrations Documentation (https://docs.mandiant.com/home/msv-preview-integrations)**.

This integration is remote capable.

Update Trellix Network DLP

Identify or create credentials to access ePO with read permissions, at minimum.

Update the Validation Platform

Prerequisites

Information to gather before you start:

- IP address/host information used to access Trellix (ESM or ePO)
- Port for Trellix (ESM or ePO) communications (default is 443)
- Identify whether the protocol is HTTP or HTTPS for connections to the port (default is HTTPS)

Configuration

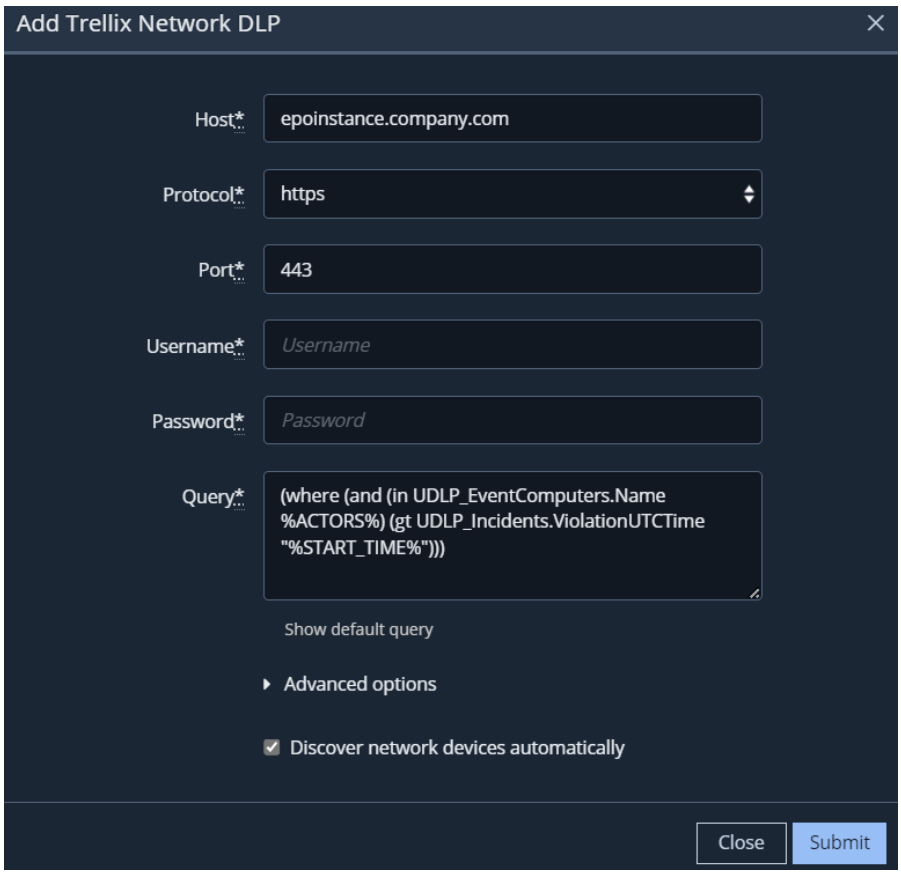
TO ADD THE TRELLIX NETWORK DLP INTEGRATION

1. Go to **Settings** > **Integrations**.
2. Click **Add Integration** > **Trellix Network DLP**.

   You can add this as either a Local or Remote Integration.

3. Enter information for the **Host**, **Protocol**, **Port**, **Username** and **Password** or **API Token**.
4. If necessary, modify the **Query**.
5. Expand **Advanced options** and update the information, if necessary.
6. Click **Submit**.



(https://app.knowledgeowl.com/app/image/pid/620d7e13ccb103e8557b25b0/id/63ebeef4e298e17f0819260b/n/trellix-network-dlp.png?imgkey=3c1881a2cce84a39ccf1bf98f3036ff3)

Trellix Network DLP Integration

Verify Connectivity

TO VERIFY CONNECTIVITY TO TRELLIX NETWORK DLP

Click **Test** to verify that:

- The Director can communicate with IP address on the port specified.
- Credentials are valid and working.

PALO ALTO NETWORKS FIREWALLS/PANORAMA

> This document applies to Classic Integrations. While the Integrations solution is available, it is no longer actively maintained. Mandiant recommends that you plan a switch to Preview Integrations so you can take advantage of the latest features and functionality. Preview Integrations configuration steps are provided in the Director web interface. For more details, see the **Preview Integrations Documentation (https://docs.mandiant.com/home/msv-preview-integrations)**.

This integration enables the Security Validation Director to pull events from individual Palo Alto Networks firewalls or from a Panorama management console managing multiple firewalls. Events may be pulled from the Threat, Wildfire, Data Filtering, and Traffic modules. A single integration is recommended if Panorama is available rather than connecting to each firewall individually.

> This integration is remote capable.

The Time zone field in the Integration is very important. If you do not set it to match the time zone of the PA firewall or Panorama, all events will be marked as UTC, not local time. This means your events may not appear when you run Actions.

Update Palo Alto

Palo Alto recommends setting up a separate admin account for API access:

1. Go to **https://docs.paloaltonetworks.com/pan-os**.
2. Search for "enable-api-access". In the results, you can open the most recent document version or access other versions.

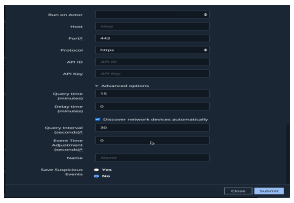
Supported Palo Alto and Panorama Versions

- Palo Alto Networks versions 7.x, 8.x
- Panorama versions 7.x, 8.x, 9.x

Update the Security Validation Platform

TO ADD THE PALO ALTO INTEGRATION

1. Go to **Settings** > **Integrations**.
2. Click **Add Integration** > **Palo Alto**.



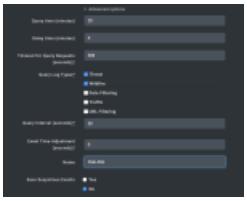
(https://d383cql5uq169w.cloudfront.net/app/image/pid/620d7e13ccb103e8557b25b0/id/629a12e3c9cba0017c2f7e52/n/palo-alto.png)

Palo Alto Integration

3. Enter information for the **Host**, **Port**, **Username**, and **Password**.
4. Change the **Palo Alto Type** to match your configuration.
5. Modify the **Query**, as necessary.
6. Update the **Time zone**.

The time zone needs to match the time zone of the PA firewall or Panorama; if it doesn't, all events are assumed to be in UTC, not local time

7. Expand **Advanced options**.



(https://d383cql5uq169w.cloudfront.net/app/image/pid/620d7e13ccb103e8557b25b0/id/629a12efc9cba0017c2f7ec6/n/palo-alto-adv.png)

Palo Alto Integration - Advanced options

8. (Optional) Update **Query time** and **Delay time**.The **Query time** is the amount of time (minutes) before and after the query runs that the looks for events, while the **Delay time** is the amount of time (minutes) that the platform waits to run the query after a Job Action. For example, you configure your integration with the following values: **Query time** = 5, **Query interval** = 30 seconds, and **Delay time** = 0. When a Job Actions starts at 12:00:00, the first time the query runs, the platform looks for events from 11:55:00 to 12:00:00. Then 30 seconds later, it looks for events from 11:55:30 to 12:00:30. This interval continues, with the last query looking from 12:00:00 to 12:05:00. If you instead configured the **Delay time** to equal 10, it would run the same query, but it wouldn't start that query until 12:10:00.If your monitors are set to run more frequently than the query time, it will impact the pass/fail results for AEDA monitors.
9. (Optional) Update **Timeout for Query Requests**.
10. Select the **Log Types**.
11. Modify the **Query Interval** and **Event Time Adjustment**, if necessary.
12. (Optional) Assign a **Name**.
13. (Optional) Choose **Yes** to save suspicious events.
14. Click **Submit**.

Verify connectivity

TO VERIFY CONNECTIVITY TO PALO ALTO / PANORAMA

Click **Test** to verify that:

- The Director can communicate with the Panorama console or individual firewalls on the port specified.
- Credentials are valid and working.
- Appropriate Logs are coming in.

RSA NETWITNESS

> This document applies to Classic Integrations. While the Integrations solution is available, it is no longer actively maintained. Mandiant recommends that you plan a switch to Preview Integrations so you can take advantage of the latest features and functionality. Preview Integrations configuration steps are provided in the Director web interface. For more details, see the **Preview Integrations Documentation (https://docs.mandiant.com/home/msv-preview-integrations)**.

This integration is remote capable.

Update the Validation Platform

Prerequisites

Information to gather before you start:

1. IP address used to access the RSA NetWitness concentrator.
2. Port for the concentrator communication (default is 50105).
3. Identify whether the protocol is HTTP or HTTPS for connections to the RSA NetWitness concentrator port.
4. Identify or create the credentials to access RSA NetWitness's concentrator.
5. Identify the field name mappings for the following:

   There could be multiple of each, depending on log sources and configuration.

   a. Source IP
   b. Destination IP
   c. Source Port
   d. Destination Port
   e. Event Start Time (timestamp)
   f. Event Unique ID
   g. Event Signature ID
   h. Event Description
   i. Event Source Host

Configuration

TO ADD THE RSA NETWITNESS INTEGRATION

1. Go to **Settings** > **Integrations**.
2. Click **Add Integration** > **RSA NetWitness**.

(https://app.knowledgeowl.com/app/image/pid/620d7e13ccb103e8557b25b0/id/62982c7dad331e21d9050edf/n/netwitness.png imgkey=3c1881a2cce84a39ccf1bf98f3036ff3)

RSA NetWitness Integration

3. Enter information for the **Host**, **Port**, **Protocol**, **Username** and **Password** or **API Token**.
4. (Optional) Enter information in the **Query** dialog box to query for base events. Click **Show default query** to see the

default query information.

5. Expand **Advanced options**.

(https://app.knowledgeowl.com/app/image/pid/620d7e13ccb103e8557b25b0/id/62982c7dad331e21d9050ee2/n/netwitness-adv.png?imgkey=3c1881a2cce84a39ccf1bf98f3036ff3)

RSA NetWitness Integration (Advanced Options)

6. (Optional) Update the **User Agent**.
7. To enable a query for ESA alerts, check the **Enable query for Alerts** check box.
8. (Optional) Enter information in the **Alert Query** dialog box to query for ESA alerts.

> The default time for an alert can be up to 30 minutes off from when the event fired. If this is the case you must add another field to your alerts with the proper time and add that time to the start_time field map for correlations to work properly.

9. Review the field name mappings; update as necessary.
    a. Inputs are enclosed by square brackets `[]`.
    b. Inputs are columns that could contain the info (`["time"]`).
    c. If there could be multiple commas, enclosed in one set of brackets, encompassed in quotes, and separated by commas (`["msg.id","reference.id", "rid"]`).
10. (Optional) Assign a **Name**.
11. (Optional) Choose **Yes** to save suspicious events.
12. Click **Submit**.

Verify Connectivity

TO VERIFY CONNECTIVITY TO RSA NETWITNESS

Click **Test** to verify that:

- The Director can communicate with NetWitness on the port and protocol specified.
- Credentials are valid and working.

SECURITY ONION - ELK

> This document applies to Classic Integrations. While the Integrations solution is available, it is no longer actively maintained. Mandiant recommends that you plan a switch to Preview Integrations so you can take advantage of the latest features and functionality. Preview Integrations configuration steps are provided in the Director web interface. For more details, see the **Preview Integrations Documentation (https://docs.mandiant.com/home/msv-preview-integrations)**.

This integration is remote capable.

Update Security Onion - ELK

Do the following to allow access to the API port via Security Onion's built-in Firewall.

TO ALLOW ACCESS TO THE API PORT

1. Run the `so-allow` command.
2. Choose option **e**.
3. Enter the `director's ip address` .

Update the Validation Platform

Prerequisites

Information to gather before you start:

1. Host and port used for Security Onion - ELK.
2. Identify whether the protocol is HTTP or HTTPS for connections .
3. Identify or create the credentials to access Security Onion.

Configuration

TO ADD THE SECURITY ONION - ELK INTEGRATION

1. Go to **Settings** > **Integrations**.
2. Click **Add Integration** > **Security Onion - ELK**.

(https://d383cql5uq169w.cloudfront.net/app/image/pid/620d7e13ccb103e8557b25b0/id/629a12e6c9cba0017c2f7e76/n/sec-onion-elk.png)

Security Onion ELK Integration

3. Enter information for the **Host**, **Port**, **Username**, and **Password**.
4. Expand **Advanced options**.

(https://d383cql5uq169w.cloudfront.net/app/image/pid/620d7e13ccb103e8557b25b0/id/629a12e1c9cba0017c2f7e43/n/sec-onion-elk1.png)

Security Onion ELK Field mappings

5. Review the field name mappings and update as necessary. Default mappings exist for Snort and Bro.
    a. You can use standard UNIX wildcards in the Index name, allowing you to match several index files (for example, `snort-*` matches `snort-123` and `snort-abc`).
    b. Inputs are enclosed by square brackets `[]`.
    c. Inputs point to the path location (`["_id"]`).
    d. Nested locations should be enclosed in one set of brackets, encompassed in quotes, and separated by commas (`["_source","src_ip"]`).
6. Add a new **Index** and configure those fields, if necessary.
7. Modify the **Query Interval** and **Event Time Adjustment**, if necessary.
8. (Optional) Select **Discover network devices automatically**.
9. (Optional) Assign a **Name**.
10. (Optional) Choose **Yes** to save suspicious events.
11. Click **Submit**.

Verify connectivity

TO VERIFY CONNECTIVITY TO SECURITY ONION - ELK

Click **Test** to verify that:

- The Director can communicate with Security Onion - ELK with the host, port, and credentials provided.

SECURITY ONION - ELSA

> This document applies to Classic Integrations. While the Integrations solution is available, it is no longer actively maintained. Mandiant recommends that you plan a switch to Preview Integrations so you can take advantage of the latest features and functionality. Preview Integrations configuration steps are provided in the Director web interface. For more details, see the **Preview Integrations Documentation (https://docs.mandiant.com/home/msv-preview-integrations)**.

This integration is remote capable.

Update Security Onion - ELSA

TO UPDATE SECURITY ONION - ELSA

1. Create a username.
2. If using API authentication, identify the token to be used.

Update the Validation Platform

Prerequisites

Information to gather before you start:

1. Host and port used for Security Onion - ELSA (defaults are auto-populated).
2. Identify whether the protocol is HTTP or HTTPS for connections.
3. Identify or create the credentials to access Security Onion.

Configuration

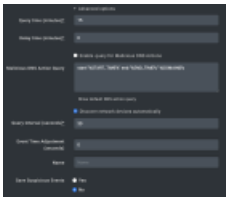
TO ADD THE SECURITY ONION - ELSA INTEGRATION

1. Go to **Settings** > **Integrations**.
2. Click **Add Integration** > **Security Onion - ELSA**.

(https://d383cql5uq169w.cloudfront.net/app/image/pid/620d7e13ccb103e8557b25b0/id/629a12d8c9cba0017c2f7ddb/n/so-elsa-836.png)

Security Onion ELSA Integration

3. If necessary, change the **Host** and **Port**.
4. Choose the **Protocol** and **Credential type**.
5. Enter the credentials. Expand Advanced options.



(https://d383cql5uq169w.cloudfront.net/app/image/pid/620d7e13ccb103e8557b25b0/id/629a12d7c9cba0017c2f7dd6/n/so-elsa-adv.png)

6. (Optional) Update **Query time** and **Delay time**.

The **Query time** is the amount of time (minutes) before and after the query runs that the looks for events, while the **Delay time** is the amount of time (minutes) that the platform waits to run the query after a Job Action. For example, you configure your integration with the following values: **Query time** = 5, **Query interval** = 30 seconds, and **Delay time** = 0. When a Job Actions starts at 12:00:00, the first time the query runs, the platform looks for events from 11:55:00 to 12:00:00. Then 30 seconds later, it looks for events from 11:55:30 to 12:00:30. This interval continues, with the last query looking from 12:00:00 to 12:05:00. If you instead configured the **Delay time** to equal 10, it would run the same query, but it wouldn't start that query until 12:10:00.

If your monitors are set to run more frequently than the query time, it will impact the pass/fail results for AEDA monitors.

7. (Optional) Select **Enable query for Malicious DNS Actions** and configure the **Query**. This query will only be used when you run Malicious DNS Actions or Captive DNS Actions.
8. (Optional) Select **Discover network devices automatically**.
9. Modify the **Query Interval** and **Event Time Adjustment**, if necessary.
10. (Optional) Assign a **Name**.
11. (Optional) Choose **Yes** to save suspicious events.
12. Click **Submit**.

Verify connectivity

TO VERIFY CONNECTIVITY TO SECURITY ONION - ELSA

Click **Test** to verify that:

- The Director can communicate with Security Onion - ELSA with the host, port, and credentials provided.

Run a Malicious or Captive DNS Action and then review the last run query to verify:

- The custom DNS query works as expected (if configured).

SYMANTEC DATA LOSS PREVENTION (DLP)

> This document applies to Classic Integrations. While the Integrations solution is available, it is no longer actively maintained. Mandiant recommends that you plan a switch to Preview Integrations so you can take advantage of the latest features and functionality. Preview Integrations configuration steps are provided in the Director web interface. For more details, see the **Preview Integrations Documentation (https://docs.mandiant.com/home/msv-preview-integrations)**.

This integration is not remote capable.

Update Symantec DLP

TO UPDATE SYMANTEC DLP

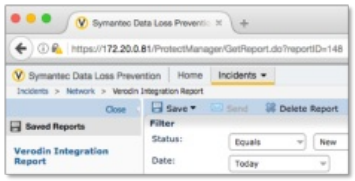
1. Note what version of Symantec DLP you have.
   - If your version is older than 15.7, see steps **4** and **5** below to gather required Report IDs.
   - If your version is newer than 15.7, identify the time zone used for your Symantec DLP server.
2. Verify that there is a role with adequate permissions for the API user to inherit.
   a. In Incidents section, select **View** and then **Perform Attribute Lookup**.
   b. In Incidents section, go to the Incident Reporting and Update API section, and select **Incident Reporting** and then **Incident Update**.
3. Create a user for the integration. Setup should include the following:
   a. Select **password access**.
   b. Under Report Preferences, select Include **Incident Violations in XML Export** and **Include Incident History in XML Export**.
   c. Assign the role from Step 1 to this user and make it the default role.

   This user can only be assigned one role.

   If you're using Active Directory to authenticate your API user, the username must be specified in a non-standard manner:

   - `:`
     or
     `\:`
   - Examples: `svc-verodin:ACME.COM OR api-user\svc-verodin:ACME.COM`
   - Reference: https://www.symantec.com/connect/forums/ad-user-authentication-dlp-reporting-and-updating-api#comment-8394101
4. (Optional) Log into the newly-created user account, and create a new Network Incident Report with the following settings:
   a. Set the Filter Status to **Equals** and **New**.
   b. Set the Filter Date to **Today**.
   c. Click **Advanced Filter & Summarization**.
   d. Add a Source IP filter.
   e. Add a **Is Any Of** condition.
   f. Add a comma-delimited list of Actor IP addresses.
   g. Save and name the report.
5. (Optional) Obtain the saved report ID number .
   a. In the left column of the DLP web UI, click the name of the newly created report

b. In the browser's location bar, find the report number located in the URL as `?reportID=`.



(https://d383cql5uq169w.cloudfront.net/app/image/pid/620d7e13ccb103e8557b25b0/id/629a12d4c9cba0017c2f7dba/n/symadlp.png)

Finding the Report Number

API Calls

The following API call is used by the Validation Platform.

Purpose	Call
Get incident details	`/ProtectManager/services/v2011/incidents`

Update the Validation Platform

Prerequisites

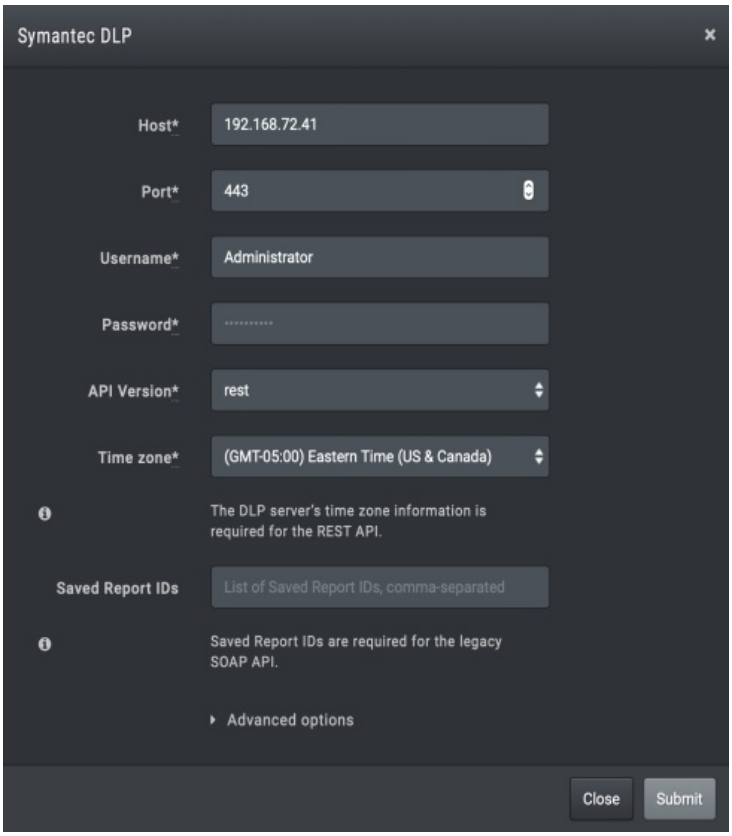
Information to gather before you start:

1. IP address or hostname used to access Symantec DLP.
2. Port for Symantec DLP communications (typically 443).
3. Identify the Symantec DLP user credentials.
4. Identify the timezone used for the Symantec DLP server.
5. Capture the list of Saved Report IDs.

Configuration

TO ADD THE SYMANTEC DLP INTEGRATION

1. Go to **Settings** > **Integrations**.
2. Click **Add Integration** > **Symantec DLP**.
3. Enter information for the **Host**, **Port**, **Username**, and **Password**.
4. Select the API used in your version of Symantec DLP.
    a. If you selected soap, enter the Saved Report IDs identified in **the steps above**.
    b. If you selected rest, enter the time zone of the Symantec DLP server.



Symantec DLP Integration

5. Expand **Advanced options** and update the information if necessary.
6. Click **Submit**.

Verify connectivity

TO VERIFY CONNECTIVITY TO SYMANTEC DLP

Click **Test** to verify that:

- The Director can communicate with Symantec DLP using the port specified.
- User credentials are working.

THREAT STACK

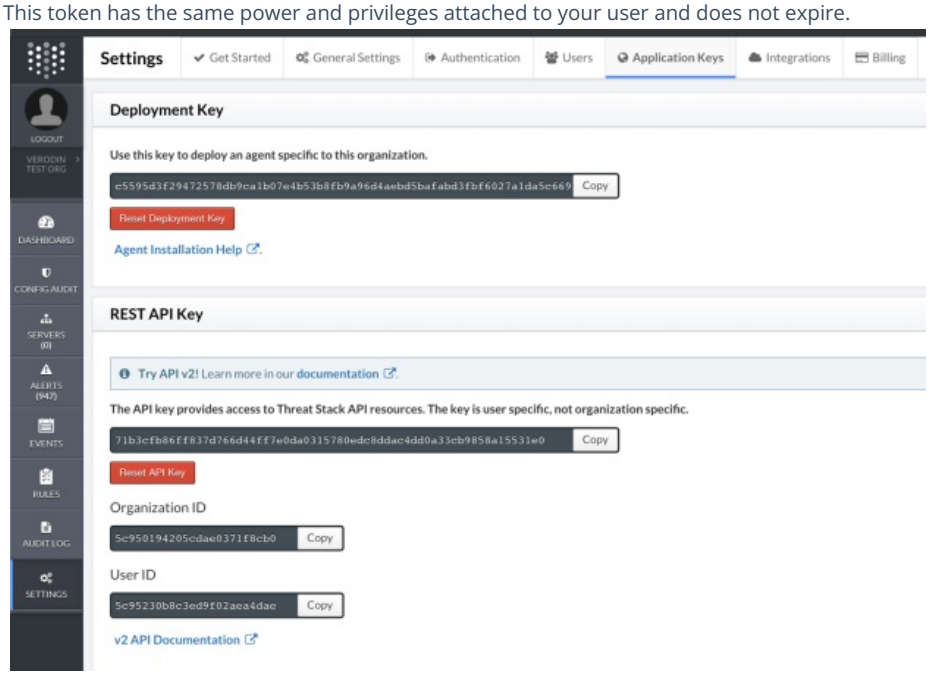
> This document applies to Classic Integrations. While the Integrations solution is available, it is no longer actively maintained. Mandiant recommends that you plan a switch to Preview Integrations so you can take advantage of the latest features and functionality. Preview Integrations configuration steps are provided in the Director web interface. For more details, see the **Preview Integrations Documentation (https://docs.mandiant.com/home/msv-preview-integrations)**.

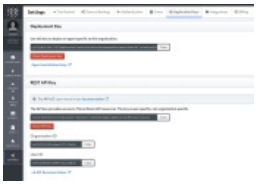
Generate an API key for Threat Stack

API tokens are tied to user accounts and inherit the user's privileges. When capturing the API key, use an account with the necessary privileges. Read permissions are required, at minimum.

TO GENERATE AN API KEY FOR THREAT STACK

1. Log into Threat Stack and bring up the main settings.
2. Select **Application Keys** from the menu.
3. From the **Rest API Key** section, copy the API Key, Organization ID, and User ID for use when creating the Validation Platform integration.
    a. Each user receives their own, unique API token.
    b. This token has the same power and privileges attached to your user and does not expire.





(https://d383cql5uq169w.cloudfront.net/app/image/pid/620d7e13ccb103e8557b25b0/id/629cec35e07dc756be50aa1d/n/threat keys.png)

Threat Stack REST API key

Update the Validation Platform

Prerequisites

Information to gather before you start:

- API key for Threat Stack.

- IP address or FQDN used to access Threat Stack.

Configuration

TO ADD THE THREAT STACK INTEGRATION

1. Go to **Settings** > **Integrations**.
2. Click **Add Integration** > **Threat Stack**.
3. Complete the general information to add the Threat Stack integration.

   The Host, Port, and Protocol have default values. Do not change these unless directed to do so by Threat Stack or Validation Platform.

   a. Enter the **User ID** you copied from Threat Stack.
   b. Enter the **API Key** you copied from Threat Stack.
   c. Enter the **Organization ID** you copied from Threat Stack.

4. Expand **Advanced options**.
5. (Optional) Update **Query time** and **Delay time**.

   The **Query time** is the amount of time (minutes) before and after the query runs that the looks for events, while the **Delay time** is the amount of time (minutes) that the platform waits to run the query after a Job Action. For example, you configure your integration with the following values: **Query time** = 5, **Query interval** = 30 seconds, and **Delay time** = 0. When a Job Actions starts at 12:00:00, the first time the query runs, the platform looks for events from 11:55:00 to 12:00:00. Then 30 seconds later, it looks for events from 11:55:30 to 12:00:30. This interval continues, with the last query looking from 12:00:00 to 12:05:00. If you instead configured the **Delay time** to equal 10, it would run the same query, but it wouldn't start that query until 12:10:00.

   If your monitors are set to run more frequently than the query time, it will impact the pass/fail results for AEDA monitors.

6. (Optional) Clear **Discover network devices automatically**.
7. Modify the **Query Interval** and **Event Time Adjustment**, if necessary.
8. (Optional) Assign a **Name**.
9. (Optional) Choose **Yes** to save suspicious events.
10. Click **Submit**.

(https://d383cql5uq169w.cloudfront.net/app/image/pid/620d7e13ccb103e8557b25b0/id/629cec35e07dc756be50aa1b/n/threatstack.png)

Threat Stack Integration

Verify connectivity

TO VERIFY CONNECTIVITY TO THREAT STACK

Click **Test** to verify that:

- The Director can communicate with the Threat Stack host on the port specified.
- The API key is working and has the necessary privileges .

TIPPING POINT IDS/IPS

> This document applies to Classic Integrations. While the Integrations solution is available, it is no longer actively maintained. Mandiant recommends that you plan a switch to Preview Integrations so you can take advantage of the latest features and functionality. Preview Integrations configuration steps are provided in the Director web interface. For more details, see the **Preview Integrations Documentation (https://docs.mandiant.com/home/msv-preview-integrations)**.

This integration is remote capable.

Update TippingPoint

The Validation Platform requires an exclusive user account. Create an account that has, at minimum, Access SMS Web Services permissions.

API Calls

The following API Calls are used by the Validation Platform.

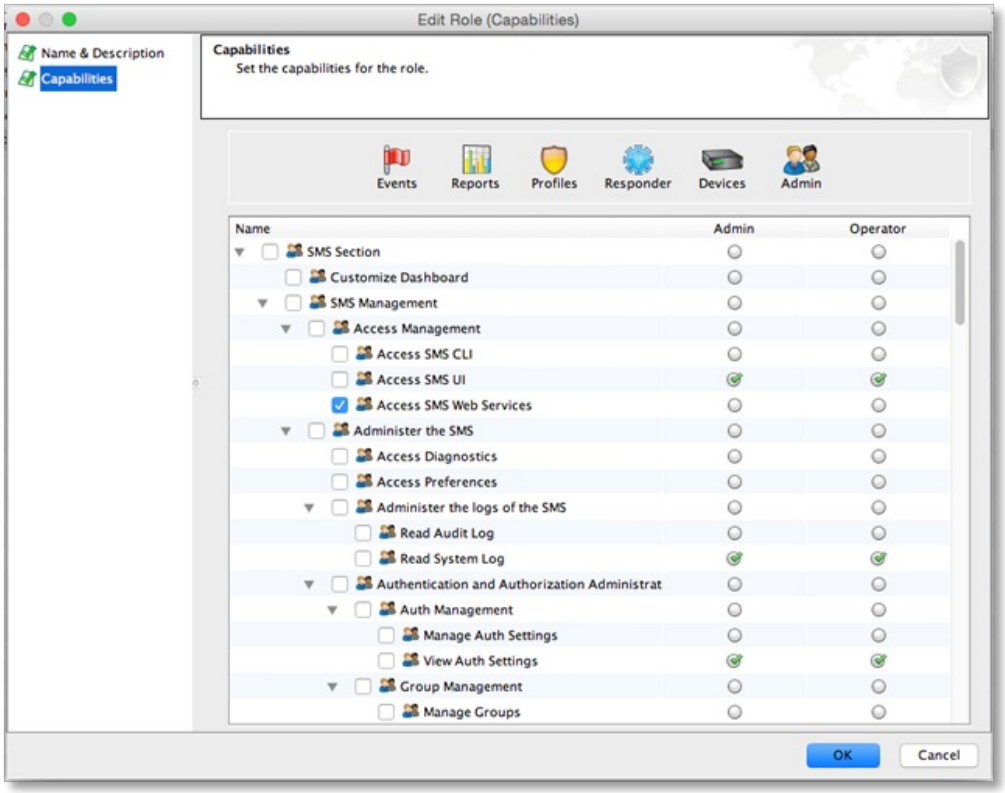
Purpose	Call
Query Alerts	`/dbAccess/tptDBServlet` with `GetData` method in the `ALERTS` table. Uses begin_time and end_time to timebox the query.
Update signatures	`/dbAccess/tptDBServlet` with `DataDictionary` method in the `SIGNATURE` table. This is retrieving signatures from TippingPoint to update our cache, not changing configuration on TippingPoint devices.

Update the Validation Platform

Prerequisites

Information to gather before you start:

1. Identify the IP address used to access TippingPoint SMS host.
2. Identify the port for TippingPoint SMS host communications (default is 443).
3. Identify whether the protocol is HTTP or HTTPS for connections to the TippingPoint SMS host port.
4. Identify or create credentials to access TippingPoint.

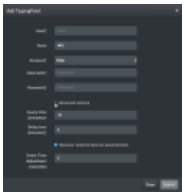


Tipping Point Credentials

Configuration

TO ADD THE TIPPING POINT INTEGRATION

1. Go to **Settings** > **Integrations**.
2. Click **Add Integration** > **TippingPoint**.
3. Enter information for the **Host**, **Port**, **Protocol**, **Username** and **Password** or **API Token**.
4. Expand **Advanced options** and update the information if necessary.
5. Click **Submit**.
6. Click **Update Signatures** to download the TippingPoint signature set from the SMS server.



(https://d383cql5uq169w.cloudfront.net/app/image/pid/620d7e13ccb103e8557b25b0/id/629a12d8c9cba0017c2f7de0/n/tippingpoint.pn

Tipping Point Integration

Verify connectivity

TO VERIFY CONNECTIVITY TO TIPPINGPOINT

Click **Test** to verify that:

- The Director can communicate with TippingPoint using the port specified.
- User credentials are working.

VMWARE APPDEFENSE

> This document applies to Classic Integrations. While the Integrations solution is available, it is no longer actively maintained. Mandiant recommends that you plan a switch to Preview Integrations so you can take advantage of the latest features and functionality. Preview Integrations configuration steps are provided in the Director web interface. For more details, see the **Preview Integrations Documentation (https://docs.mandiant.com/home/msv-preview-integrations)**.

This integration uses HTTPS and Port 443.

This integration is remote capable.

Update VMware AppDefense

You must create a new integration in the integrations section of AppDefense. If the Validation Platform is not listed in the dropdown list, you can use the Splunk option since it generates a normal API key.

Update the Validation Platform

Prerequisites

Information to gather before you start:

- Your VMware AppDefense Organization ID.
- API Key.

Configuration

TO ADD THE VMWARE APPDEFENSE INTEGRATION

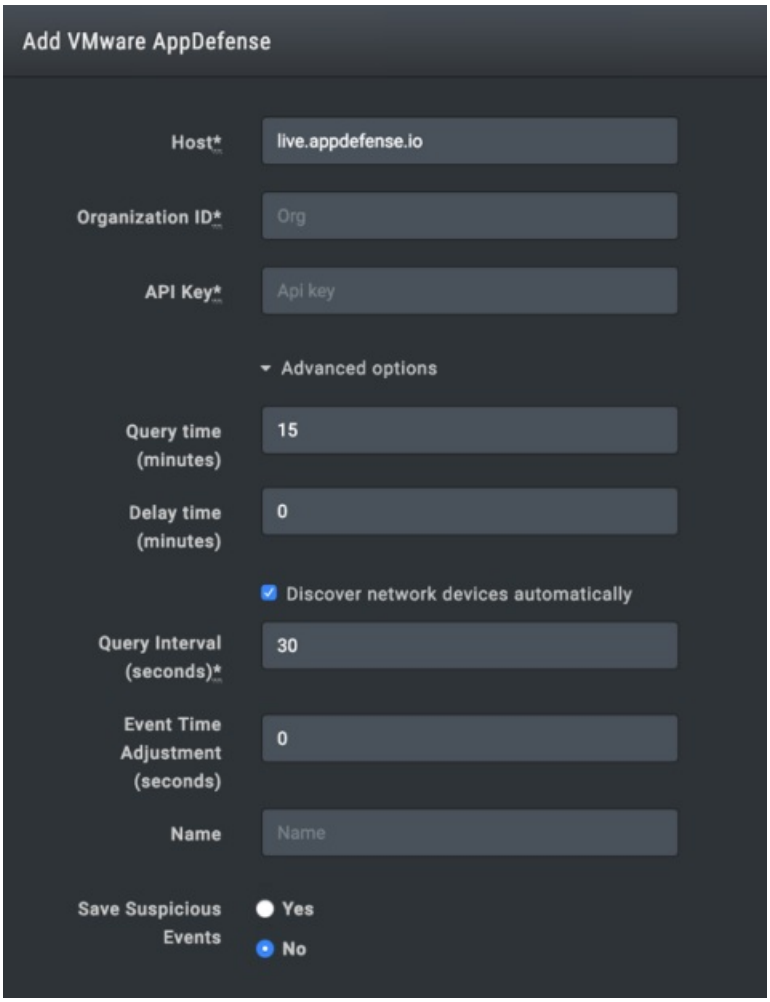
1. Go to **Settings** > **Integrations**.
2. Click **Add Integration** > **VMware AppDefense**.
3. Enter the **Organization ID**.
4. Enter the **API Key.**
5. Expand **Advanced options**.
6. (Optional) Update **Query time** and **Delay time**.

The **Query time** is the amount of time (minutes) before and after the query runs that the looks for events, while the **Delay time** is the amount of time (minutes) that the platform waits to run the query after a Job Action. For example, you configure your integration with the following values: **Query time** = 5, **Query interval** = 30 seconds, and **Delay time** = 0. When a Job Actions starts at 12:00:00, the first time the query runs, the platform looks for events from 11:55:00 to 12:00:00. Then 30 seconds later, it looks for events from 11:55:30 to 12:00:30. This interval continues, with the last query looking from 12:00:00 to 12:05:00. If you instead configured the **Delay time** to equal 10, it would run the same query, but it wouldn't start that query until 12:10:00.

If your monitors are set to run more frequently than the query time, it will impact the pass/fail results for AEDA monitors.

7. (Optional) Clear **Discover network devices automatically**.
8. Modify the **Query Interval** and **Event Time Adjustment**, if necessary.
9. (Optional) Assign a **Name**.
10. (Optional) Choose **Yes** to save suspicious events.

11. Click **Submit**.



VMware AppDefense Integration

Verify Connectivity

TO VERIFY CONNECTIVITY TO VMWARE APPDEFENSE

Click **Test** to verify that:

- The Director can communicate with VMware AppDefense using the Organization ID specified on the port specified.
- The API key is valid and working.

ALERTLOGIC

> This document applies to Classic Integrations. While the Integrations solution is available, it is no longer actively maintained. Mandiant recommends that you plan a switch to Preview Integrations so you can take advantage of the latest features and functionality. Preview Integrations configuration steps are provided in the Director web interface. For more details, see the **Preview Integrations Documentation (https://docs.mandiant.com/home/msv-preview-integrations)**.

This integration is remote capable.

Update the Validation Platform

Prerequisites

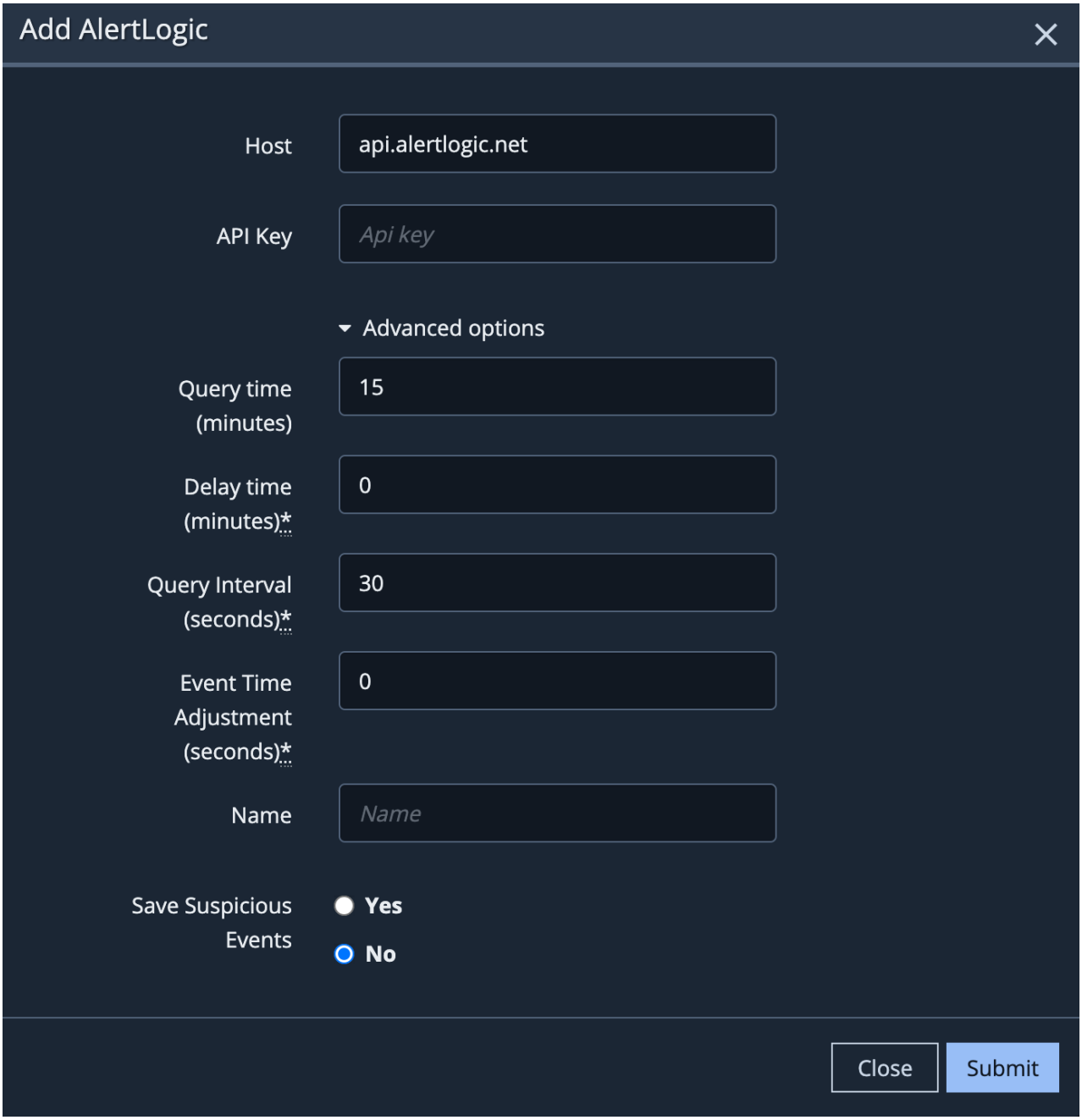
Information to gather before you start:

- AlertLogic Host.
- AlertLogic API key.

Configuration

TO ADD THE ALERTLOGIC INTEGRATION

1. Go to **Settings** > **Integrations**.
2. Click **Add Integration** > **AlertLogic**.
3. Enter the **Host** and the **API Key**.
4. Expand **Advanced options** and update the information if necessary.
5. Click **Submit**.



Verify connectivity

TO VERIFY CONNECTIVITY TO ALERTLOGIC

Click **Test** to verify that the Director can communicate with AlertLogic using the host and API information.

ALIENVAULT

> This document applies to Classic Integrations. While the Integrations solution is available, it is no longer actively maintained. Mandiant recommends that you plan a switch to Preview Integrations so you can take advantage of the latest features and functionality. Preview Integrations configuration steps are provided in the Director web interface. For more details, see the **Preview Integrations Documentation (https://docs.mandiant.com/home/msv-preview-integrations)**.

This integration is not remote capable.

Update AlienVault

TO UPDATE ALIENVAULT

Insert the Validation Platform Director public key in the file `home/avapi/.ssh/authorized_keys`.

This allows the Director to run queries using the `avapi` user.

This generally requires the AlienVault root password.

Update the Validation Platform

Prerequisites

Information to gather before you start:

- IP address used to access AlienVault.
- Port for AlienVault-related SSH communications (default is 22).

Configuration

TO ADD THE ALIENVAULT INTEGRATION

1. Go to **Settings** > **Integrations**.
2. Click **Add Integration** > **AlienVault**.
3. Enter the **Host**.
4. If necessary, update the **Port**.
5. Expand **Advanced options**.
6. If necessary, adjust any additional fields (such as **Query** and **Correlation query**) that were pre-populated for you.
7. Click **Submit**.

(https://d383cql5uq169w.cloudfront.net/app/image/pid/620d7e13ccb103e8557b25b0/id/629a12ddc9cba0017c2f7e1c/n/alienvault-1.png)

AlienVault Integration

Verify connectivity

TO VERIFY CONNECTIVITY TO ALIENVAULT

Click **Test** to verify that the Director can:

- Communicate with AlienVault IP address on the port specified.
- SSH to the AlienVault host using the `avapi` user without providing a password (using RSA/DSA keys).

ARCSIGHT

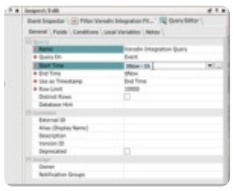
This document applies to Classic Integrations. While the Integrations solution is available, it is no longer actively maintained. Mandiant recommends that you plan a switch to Preview Integrations so you can take advantage of the latest features and functionality. Preview Integrations configuration steps are provided in the Director web interface. For more details, see the **Preview Integrations Documentation (https://docs.mandiant.com/home/msv-preview-integrations)**.

This integration is remote capable.

Update ArcSight

TO UPDATE ARCSIGHT

1. Create credentials for the Validation Platform to use to access ArcSight.
2. Read permissions are acceptable, for the detect API.
3. Within the ArcSight Console, create a new Query.
    a. Open the Menu and choose **Query**.
    b. Click **New**.
    c. Name the Query.
    d. Change the Start Time attribute to `$Now - 15m` .



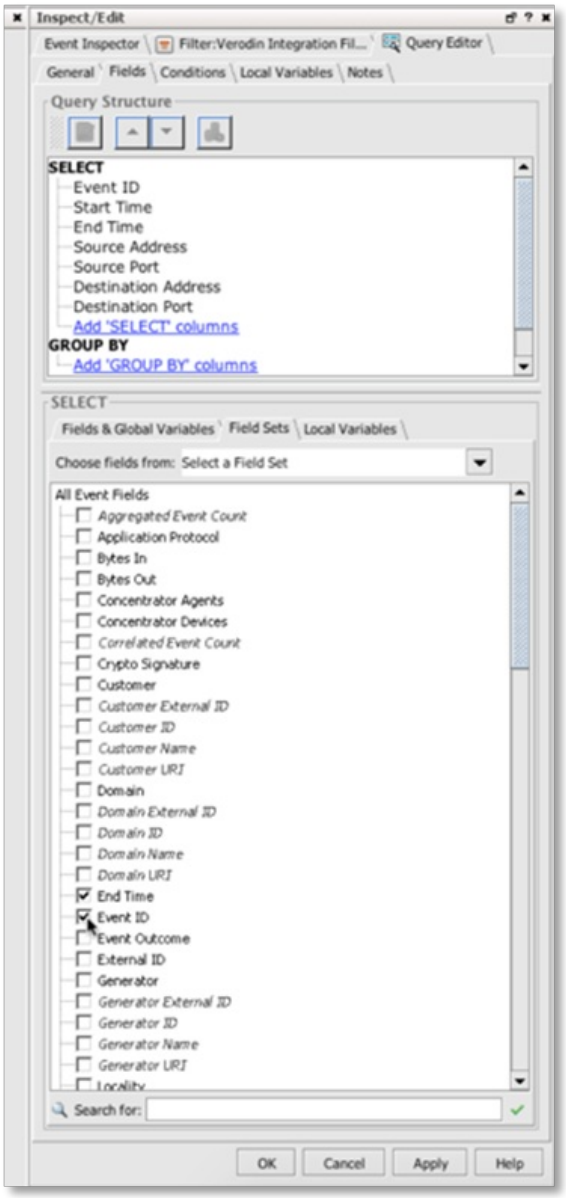
(https://d383cql5uq169w.cloudfront.net/app/image/pid/620d7e13ccb103e8557b25b0/id/629a12eac9cba0017c2f7e8e/n/arcsi

query.png)

Set start time

    e. Click the **Fields** tab and under the SELECT heading, add the following fields to the query:

- * Add these fields if you want the Validation Platform to find events associated with Email Actions.
- ** These fields might also contain email addresses.

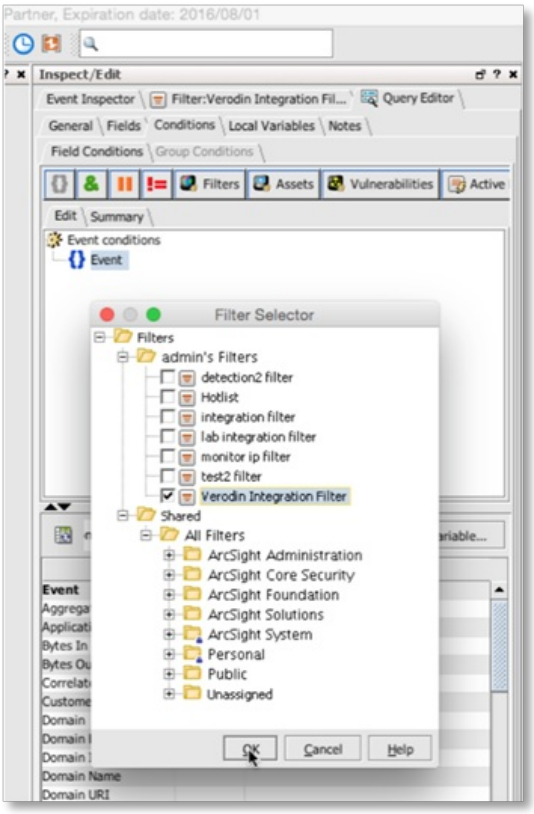


Add Fields to Query

i. Start Time
ii. End Time
iii. Event ID
iv. Name
v. Source Address
vi. Source Port
vii. Destination Address
viii. Destination Port
ix. Type
x. Device Facility
xi. Device Vendor
xii. Device Product.
xiii. Device Version.
xiv. Device Address
xv. Attacker DNS Domain*

xvi. Attacker User Name*
xvii. Attacker User ID*
xviii. Request*
xix. Request URL*
xx. Source User Name**
xxi. Destination User Name**
xxii. Target User Name**

f. Click **OK** to save the Query.



Set Filter

4. Within the ArcSight Console, create a new Query Viewer.
   a. Open the menu and choose **Query Viewer**.
   b. Click **New**.
   c. Name the Query Viewer.

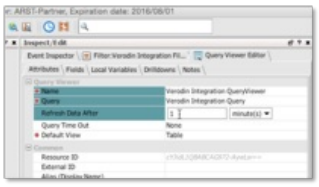
> This query name must be unique across the entire ArcSight ESM. If there is another query with the same name for any user, the integration will not work correctly.

   d. Set the query to the one created in the previous step.

(https://d383cql5uq169w.cloudfront.net/app/image/pid/620d7e13ccb103e8557b25b0/id/629a12e4c9cba0017c2f7e63/n/arcsi7.png)

Set Query

e. Set the refresh interval to 1 minute.



(https://d383cql5uq169w.cloudfront.net/app/image/pid/620d7e13ccb103e8557b25b0/id/629a12e1c9cba0017c2f7e3f/n/arcsi
8.png)

Set Refresh Interval

f. Click **OK** to save the Query Viewer and select the folder to save it in.
g. Capture the Query Viewer name for integration with the Validation Platform.

> Capture it exactly, including case.

API Calls

The following API calls are used by the Validation Platform.

Purpose	Call
Login for a token	`core-service/rest/LoginService/login`
Get Query Viewer ID	`/detect-api/rest/queryviewers/name/(query_viewer_name)`
Get Query Viewer Records	`/detect-api/rest/queryviewers/matrixData/(query_viewer_id)`
Logout	`/www/core-service/rest/LoginService/logout`

Update the Validation Platform

Prerequisites

Information to gather before you start:

- Identify the IP address used to access ArcSight.
- Identify the port for ArcSight communications (default is 8443).
- Identify whether the protocol is HTTP or HTTPS for connections to the ArcSight port.
- For version 7.2 and older:
  - Filter Name
  - Filter URI
  - Query Viewer Name
- For version 7.3 and newer:
  - Query Viewer Name

Configuration

TO ADD THE ARCSIGHT INTEGRATION

> Field values are case sensitive.

1. Go to **Settings** > **Integrations**.
2. Click **Add Integration** > **ArcSight**.

(https://d383cql5uq169w.cloudfront.net/app/image/pid/620d7e13ccb103e8557b25b0/id/629a12efc9cba0017c2f7ec8/n/arcsight-general.png)

ArcSight Integration

3. Enter information for the **Host**, **Port**, **Protocol**, **Username** and **Password** or **API Token**.
4. Enter the **Query Viewer name**.
5. Expand **Advanced options**.

(https://d383cql5uq169w.cloudfront.net/app/image/pid/620d7e13ccb103e8557b25b0/id/629a12d6c9cba0017c2f7dc9/n/arcsight-advanced.png)

ArcSight Integration (Advanced Options)

6. Update the **Action match time**.

> This field determines how far in the past we consider our Job Actions for matching. The Query Viewer time configured in Arcsight determines how far in the past the integration queries for events.

7. (Optional) Update the **Delay time**.
8. Update **Query timeout**.
9. (Optional) Select **Require event to match rule for detection**.
10. (Optional) Select **Discover network devices automatically**.
11. Modify the **Query Interval** and **Event Time Adjustment**, if necessary.
12. (Optional) Assign a **Name**.
13. (Optional) Choose **Yes** to save suspicious events.
14. Click **Submit**.

Verify connectivity

TO VERIFY CONNECTIVITY TO ARCSIGHT

Click **Test** to verify that:

- The Director can communicate with ArcSight IP address on the port specified.
- The ArcSight credentials are valid and working.

Field Value Notes

If the Request URL field is present in the query viewer, the integration will attempt to capture the information from the Request URL field when the Destination Port field is empty for an event.

CHRONICLE BACKSTORY

> This document applies to Classic Integrations. While the Integrations solution is available, it is no longer actively maintained. Mandiant recommends that you plan a switch to Preview Integrations so you can take advantage of the latest features and functionality. Preview Integrations configuration steps are provided in the Director web interface. For more details, see the **Preview Integrations Documentation (https://docs.mandiant.com/home/msv-preview-integrations)**.

This integration is not remote capable.

Update Backstory

Identify or create credentials to access Chronicle Backstory with read access, at minimum.

API Calls

The following API calls are used by the Validation Platform.

Purpose	Call
To get all events associated	backstory.googleapis.com/v1/asset/listevents

Update the Validation Platform

Prerequisites

Information to gather before you start:

- Identify the ProjectID associated with your Chronicle Backstory account

If you have multiple Chronicle Backstory integrations, each must have a unique project ID

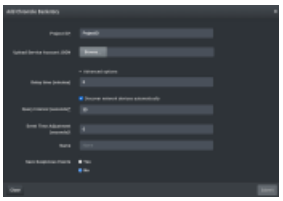
- In Chronicle Backstory, download your Service Account JSON file

If you have multiple Chronicle Backstory integrations, a single Service Account JSON file can be shared between each integration

Configuration

TO ADD THE CHRONICLE BACKSTORY INTEGRATION

1. Go to **Settings** > **Integrations**.
2. Click **Add Integration** > **Integration**.
3. Enter the Project ID from Chronicle Backstory.
4. Upload your Chronicle Backstory Service Account JSON file.
5. Expand **Advanced options** and update the information if necessary.
6. (Optional) Assign a **Name**.
7. (Optional) Choose **Yes** to save suspicious events.
8. Click **Submit**.



(https://d383cql5uq169w.cloudfront.net/app/image/pid/620d7e13ccb103e8557b25b0/id/629a12d9c9cba0017c2f7de9/n/chronicle-backstory.png)

Chronicle Backstory Integration

Verify connectivity

TO VERIFY CONNECTIVITY TO CHRONICLE BACKSTORY

Click **Test** to verify that:

- The Director can communicate with the integration host on the port and protocol specified.
- The integration credentials are valid and working.

DEVO

This document applies to Classic Integrations. While the Integrations solution is available, it is no longer actively maintained. Mandiant recommends that you plan a switch to Preview Integrations so you can take advantage of the latest features and functionality. Preview Integrations configuration steps are provided in the Director web interface. For more details, see the **Preview Integrations Documentation** (https://docs.mandiant.com/home/msv-preview-integrations).

This integration is remote capable.

Update Devo

1. In the Devo UI, navigate to Administration > Credentials > Authentication Tokens.
    a. Grant permissions for each table as needed.
2. Combine all the tables you want to validate into a single union table and name the table my.synthesis.fireeye.data.

    We ask that you do this because each Devo integration supports one table query at a time.

3. Map any relevant fields in your union table to the equivalent fields used by the Devo integration. The following table displays some default union table fields and how they map to the integration's fields.

Union Table Field	Integration Field
srcIp	Source IP
destIp	Destination IP
destPort	Destination Port
srcPort	Source Port

If you try to run a query with the name of a field that does not exist, the query will error. Verify your union table fields are properly mapped to the integration fields.

Supported Integration API Versions

- APIv2

API Calls

The following API calls are used by Validation Platform.

Purpose	Call
Query tables for events	/search/query

Update the Security Validation Platform

Prerequisites

Information to gather before you start:

- Identify your Devo host, port, and protocol

- Identify your Devo API token

Configuration

TO ADD THE DEVO INTEGRATION

You can create multiple Devo integrations for the same union table. If you do this, remember to always update the default queries with the correct table and field names.

1. Go to **Settings** > **Integrations**.
2. Click **Add Integration** > **Devo**.
3. Enter the Host, Port, and Protocol.
4. Enter your API Token.
5. Update the Query as needed.
6. Expand **Advanced options**.
7. (Optional) Update **Query time** and **Delay time**.

The **Query time** is the amount of time (minutes) before and after the query runs that the looks for events, while the **Delay time** is the amount of time (minutes) that the platform waits to run the query after a Job Action. For example, you configure your integration with the following values: **Query time** = 5, **Query interval** = 30 seconds, and **Delay time** = 0. When a Job Actions starts at 12:00:00, the first time the query runs, the platform looks for events from 11:55:00 to 12:00:00. Then 30 seconds later, it looks for events from 11:55:30 to 12:00:30. This interval continues, with the last query looking from 12:00:00 to 12:05:00. If you instead configured the **Delay time** to equal 10, it would run the same query, but it wouldn't start that query until 12:10:00.

If your monitors are set to run more frequently than the query time, it will impact the pass/fail results for AEDA monitors.

8. (Optional) Select **Enable query for Malicious DNS Actions** and configure the **Query**. This query will only be used when you run Malicious DNS Actions or Captive DNS Actions.
9. (Optional) Select **Enable query for Email Actions** and configure the **Query**. This query will be only be used when you run Email Actions.
10. (Optional) Select **Enable query for Host CLI Actions** and configure the **Query**. This query will only be used when you run Host CLI Actions.

If you enable the Host CLI Actions query and use the %HOST_CLI_ACTOR_HOSTNAMES% variable, the platform will substitute the plain hostname and the information from the Alternate Hostname field on the Actor configuration page.

11. Identify the field name mappings for the following (there could be multiple of each, depending on log sources and configuration):
    - Source IP
    - Destination IP
    - Source Port
    - Destination Port
    - Event Source Host
    - Event Start Time (timestamp)
    - Event Signature ID

- Event Description
- Email Sender
- Email Recipient
- Email Subject
- URL
- Username

12. Modify the **Query Interval** and **Event Time Adjustment**, if necessary.
13. (Optional) Assign a **Name**.
14. (Optional) Choose **Yes** to save suspicious events.
15. Click **Submit**.

(https://d383cql5uq169w.cloudfront.net/app/image/pid/620d7e13ccb103e8557b25b0/id/629a12e9c9cba0017c2f7e87/n/devo.png)

Devo Integration

Verify connectivity

TO VERIFY CONNECTIVITY TO DEVO

Click **Test** to verify that:

- The Director can communicate with the integration host on the port and protocol specified.
- The integration credentials are valid and working.

ELASTICSEARCH

> This document applies to Classic Integrations. While the Integrations solution is available, it is no longer actively maintained. Mandiant recommends that you plan a switch to Preview Integrations so you can take advantage of the latest features and functionality. Preview Integrations configuration steps are provided in the Director web interface. For more details, see the **Preview Integrations Documentation (https://docs.mandiant.com/home/msv-preview-integrations)**.

This integration uses the Elasticsearch Scroll API to support querying large data sets.

This integration is remote capable.

Update Elasticsearch

Identify or create the credentials to access Elasticsearch, if applicable.

- Elasticsearch does not provide authentication by default.
- Authentication can be added with Elastic X-Pack, a third-party plug-in, or by using a reverse proxy like nginx.

Update the Validation Platform

Prerequisites

Information to gather before you start:

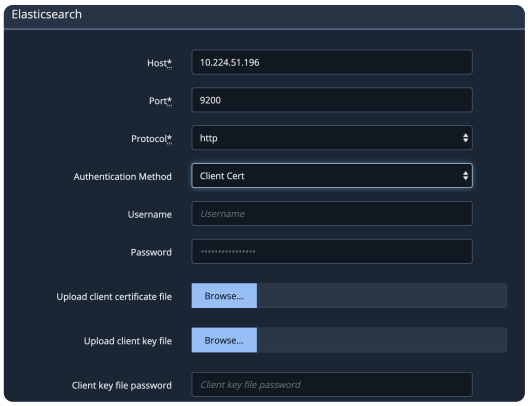
1. Identify the IP address used to access Elasticsearch. This could be direct access to an Elasticsearch node, Primary node, or something such as an nginx reverse proxy.
2. Identify the port for Elasticsearch communication (default is 9200).
3. Identify whether the protocol is HTTP or HTTPS for connections to the Elasticsearch port.
4. Identify the field name mappings for the following (there could be multiple of each, depending on log sources and configuration):
    - Source IP
    - Destination IP
    - Source Port
    - Destination Port
    - Event Start Time (timestamp)
    - URL/Domain
    - Email Sender
    - Email Recipient
    - Email Subject
    - User
    - Event Unique ID
    - Event Signature ID
    - Event Description
    - Event Source Host

Organizations can create a query index for the integration. With this configuration, searches will query all indexes, which is less efficient than running against a specified index.

Configuration

TO ADD THE ELASTICSEARCH INTEGRATION

1. Go to **Settings** > **Integrations**.
2. Click **Add Integration** > **Elasticsearch**.

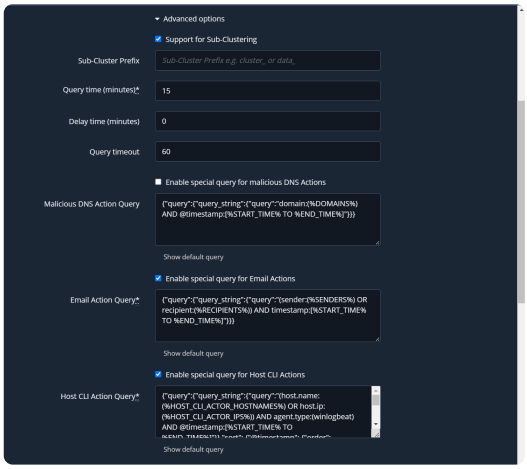


(https://d383cql5uq169w.cloudfront.net/app/image/pid/620d7e13ccb103e8557b25b0/id/629a12d5c9cba0017c2f7dc3/n/elasticsearch

Elasticsearch Integration

3. Enter information for the **Host**, **Port, and Protocol.**
4. Select your Authentication method.
    - **None**: Skip the Username, Password, and Client fields.
    - **Basic**: Enter a Username and password.
    - **Client Cert**: Upload the client certification file, the client key file, and add the client key file password.

      The remote Elasticsearch integration doesn't support client-cert authentication.
5. Update the Query, if needed.
6. Expand **Advanced options**.



Elasticsearch Integration (Advanced Options)

7. (Optional) Select **Support for sub-clustering**. When you select this option, a **Sub-Cluster Prefix** input field displays below the option, which allows you to enter a custom sub-cluster prefix (i.e., `cluster_` or `data_`, etc.).

   If a Director had any existing ElasticSearch integrations with the **Support for sub-clustering** box checked prior to an upgrade, after the upgrade that field will be set with `cluster_` by default. However, you can edit the field to be any custom sub-cluster prefix you want.
8. (Optional) Update **Query time** and **Delay time**.

The **Query time** is the amount of time (minutes) before and after the query runs that the looks for events, while the **Delay time** is the amount of time (minutes) that the platform waits to run the query after a Job Action. For example, you configure your integration with the following values: **Query time** = 5, **Query interval** = 30 seconds, and **Delay time** = 0. When a Job Actions starts at 12:00:00, the first time the query runs, the platform looks for events from 11:55:00 to 12:00:00. Then 30 seconds later, it looks for events from 11:55:30 to 12:00:30. This interval continues, with the last query looking from 12:00:00 to 12:05:00. If you instead configured the **Delay time** to equal 10, it would run the same query, but it wouldn't start that query until 12:10:00.

If your monitors are set to run more frequently than the query time, it will impact the pass/fail results for AEDA monitors.

9. (Optional) Select **Enable query for Malicious DNS Actions** and configure the **Query**. This query will only be used when you run Malicious DNS Actions or Captive DNS Actions.
10. (Optional) Select **Enable query for Email Actions** and configure the **Query**. This query will be only be used when you run Email Actions.
11. (Optional) Select **Enable query for Host CLI Actions** and configure the **Query**. This query will only be used when you run Host CLI Actions.

    If you enable the Host CLI Actions query and use the %HOST_CLI_ACTOR_HOSTNAMES% variable, the platform will substitute the plain hostname and the information from the Alternate Hostname field on the Actor configuration page.

12. (Optional) Select **Discover network devices automatically**.
13. Review the field name mappings for the `__default__` index; update as necessary.
    a. You can use standard UNIX wildcards in the Index name, allowing you to match several index files (for example, `snort-*` matches `snort-123` and `snort-abc`).
    b. Inputs are enclosed by square brackets `[]`.
    c. Inputs point to the path location (`["_id"]`).
    d. Nested locations should be enclosed in one set of brackets, encompassed in quotes, and separated by commas (`["_source","src_ip"]`).

Elasticsearch Integration (Advanced Options)

14. (Optional) Add a new **Index** and configure those fields.

    You can delete any Index except the `__default__` by selecting it and clicking **Remove index**.

15. Modify the **Query Interval** and **Event Time Adjustment**, if necessary.
16. (Optional) Assign a **Name**.
17. (Optional) Choose **Yes** to save suspicious events.
18. Click **Submit**.

    A message notifies you if there are errors in the Indexes. You must resolve the errors before you can save the integration.

Verify connectivity

TO VERIFY CONNECTIVITY TO ELASTICSEARCH

Click **Test** to verify that:

- The Director can communicate with Elasticsearch host IP address on the port specified.
- The Elasticsearch credentials are authorized to perform queries on the index or indexes with relevant data.

Run a Malicious or Captive DNS Action and then review the last run query to verify:

- The custom DNS query works as expected (if configured).

EXABEAM DATA LAKE

> This document applies to Classic Integrations. While the Integrations solution is available, it is no longer actively maintained. Mandiant recommends that you plan a switch to Preview Integrations so you can take advantage of the latest features and functionality. Preview Integrations configuration steps are provided in the Director web interface. For more details, see the **Preview Integrations Documentation (https://docs.mandiant.com/home/msv-preview-integrations)**.

 This integration is remote capable.

Update Exabeam Data Lake

Identify or create credentials to access Exabeam Data Lake with read access, at minimum.

API Calls

The following API calls are used by the Validation Platform.

Purpose	Call
Authentication	/api/auth/login
Logout	/api/auth/logout
Get Events	/dl/api/es/search

Update the Validation Platform

Prerequisites

Information to gather before you start:

- Identify the hostname/IP used to access Exabeam Data Lake.
- Identify the Port used for Exabeam Data Lake communication (this defaults to 8484).
- Identify whether the protocol is HTTP or HTTPS for connections to the Exabeam Data Lake port.
- Obtain the username and password of an Exabeam account with appropriate access permissions; or, obtain an API token from the Exabeam Portal.

 For older versions of Exabeam Data Lake (i34 and older), use username/password authentication. For newer versions of Exabeam Data Lake (i35 and newer), use API Token authentication.

Configuration

TO ADD THE EXABEAM DATA LAKE INTEGRATION

1. Go to **Settings** > **Integrations**.
2. Click **Add Integration** > **Exabeam Data Lake**.

    You can add this as either a Local or Remote Integration.

3. Enter information for the **Host**, **Port**, **Protocol**, **Username** and **Password** or **API Token**.

> If you are authenticating your Exabeam account with Domain Logon (Active Directory), you must enter the username in lower case. For example, the username `ExampleUserName` would need to be entered as `exampleusername`.

4. Review and update the **Query**, as necessary.
5. Update the Page Size, as necessary.
6. Expand **Advanced options** and update the information if necessary.
7. Click **Submit**.

(https://d383cql5uq169w.cloudfront.net/app/image/pid/620d7e13ccb103e8557b25b0/id/629a12dcc9cba0017c2f7e0c/n/exabeam-data-lake.png)

Exabeam Data Lake Integration

Verify connectivity

TO VERIFY CONNECTIVITY TO DATA LAKE

Click **Test** to verify that:

- The Director can communicate with the integration host on the port and protocol specified.
- The integration credentials are valid and working.

TRELLIX HELIX

> This document applies to Classic Integrations. While the Integrations solution is available, it is no longer actively maintained. Mandiant recommends that you plan a switch to Preview Integrations so you can take advantage of the latest features and functionality. Preview Integrations configuration steps are provided in the Director web interface. For more details, see the **Preview Integrations Documentation (https://docs.mandiant.com/home/msv-preview-integrations)**.

 This integration is remote capable.

Update Trellix Helix

Using your IAM account, create an API key for use with the Validation Platform. Verify your key has the following Helix entitlements, at a minimum:

- tap.events.browse
- tap.events.read
- tap.alerts.browse
- tap.alerts.read
- tap.lists.browse
- tap.lists.read
- tap.search.*

API Calls

The following API calls are used by the Validation Platform.

Purpose	Call
Get Events	`/v1/search`
Alerts query	`/v3/alerts`

Update the Validation Platform

Prerequisites

Information to gather before you start:

1. Identify your Trellix FQDN. Trellix FQDNs are based on the region associated with your instance:
    - US: apps.fireeye.com
    - EU: helix.eu.fireeye.com
    - AP: helix.ap.fireeye.com
2. Identify your Helix Instance ID.
3. Check whether your Helix instance is configured to leave alerts open, close alerts, or a combination of both.

Configuration

TO ADD THE TRELLIX HELIX INTEGRATION

1. Go to **Settings** > **Integrations**.
2. Click **Add Integration** > **Trellix Helix**.

 You can add this as either a Local or Remote Integration.

3. Enter information for the **FQDN**, **Helix Instance ID**, and **API Key**.
4. Select whether the Validation Platform should look for open Helix alerts, closed Helix alerts, or both.
5. Update the **Query**, as necessary.
6. Expand **Advanced options**.
7. (Optional) Update **Query time** and **Delay time**.

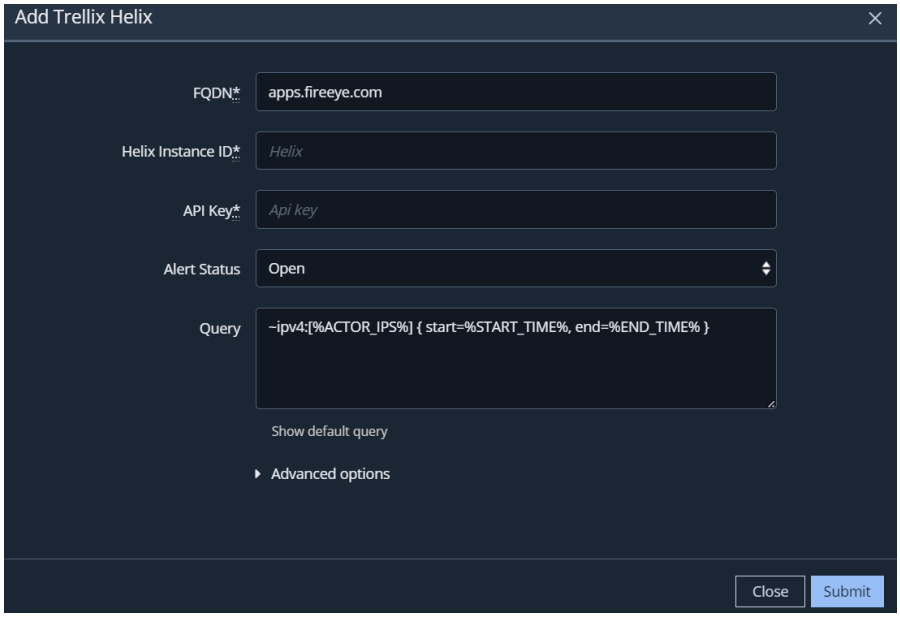
   The **Query time** is the amount of time (minutes) before and after the query runs that the looks for events, while the **Delay time** is the amount of time (minutes) that the platform waits to run the query after a Job Action. For example, you configure your integration with the following values: **Query time** = 5, **Query interval** = 30 seconds, and **Delay time** = 0. When a Job Actions starts at 12:00:00, the first time the query runs, the platform looks for events from 11:55:00 to 12:00:00. Then 30 seconds later, it looks for events from 11:55:30 to 12:00:30. This interval continues, with the last query looking from 12:00:00 to 12:05:00. If you instead configured the **Delay time** to equal 10, it would run the same query, but it wouldn't start that query until 12:10:00.

   If your monitors are set to run more frequently than the query time, it will impact the pass/fail results for AEDA monitors.

8. (Optional) Select **Enable query for Malicious DNS Actions** and configure the **Query**. This query will only be used when you run Malicious DNS Actions or Captive DNS Actions.
9. (Optional) Select **Enable query for Email Actions** and configure the **Query**. This query will be only be used when you run Email Actions.
10. (Optional) Select **Enable query for Host CLI Actions** and configure the **Query**. This query will only be used when you run Host CLI Actions.

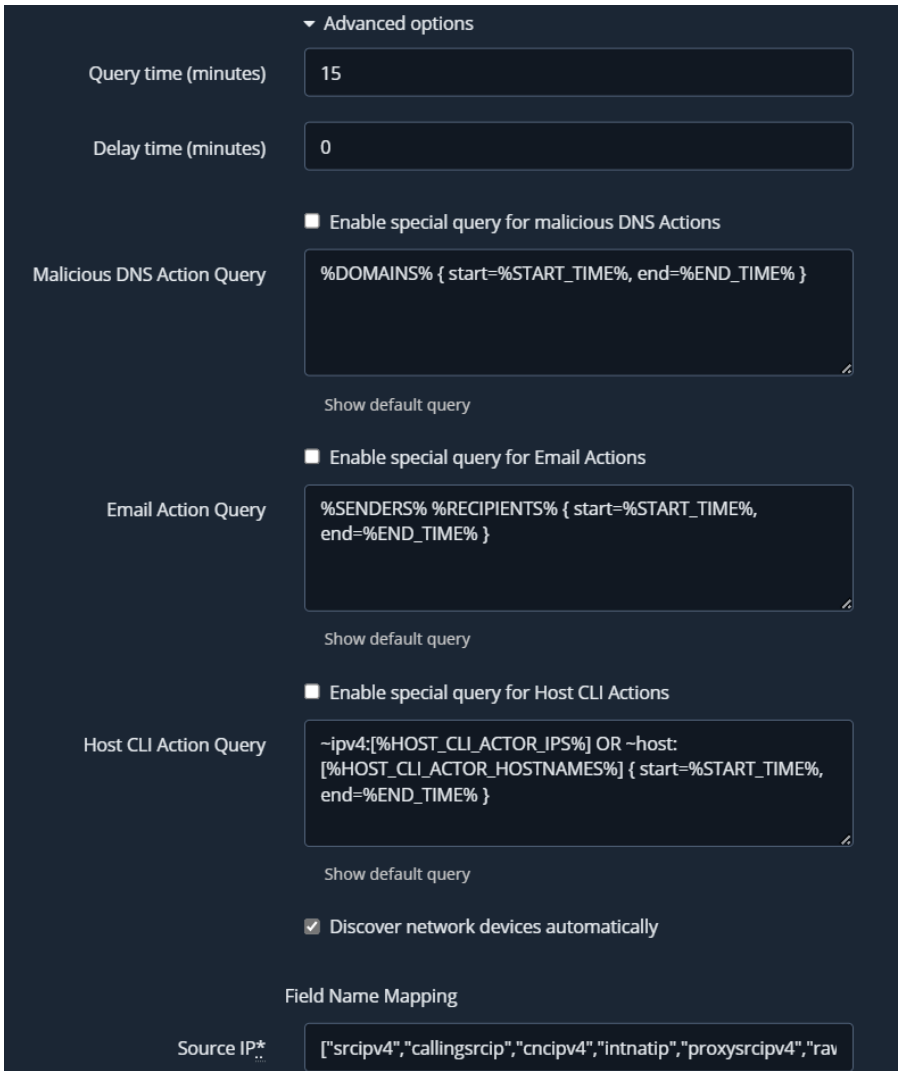
    If you enable the Host CLI Actions query and use the %HOST_CLI_ACTOR_HOSTNAMES% variable, the platform will substitute the plain hostname and the information from the Alternate Hostname field on the Actor configuration page.

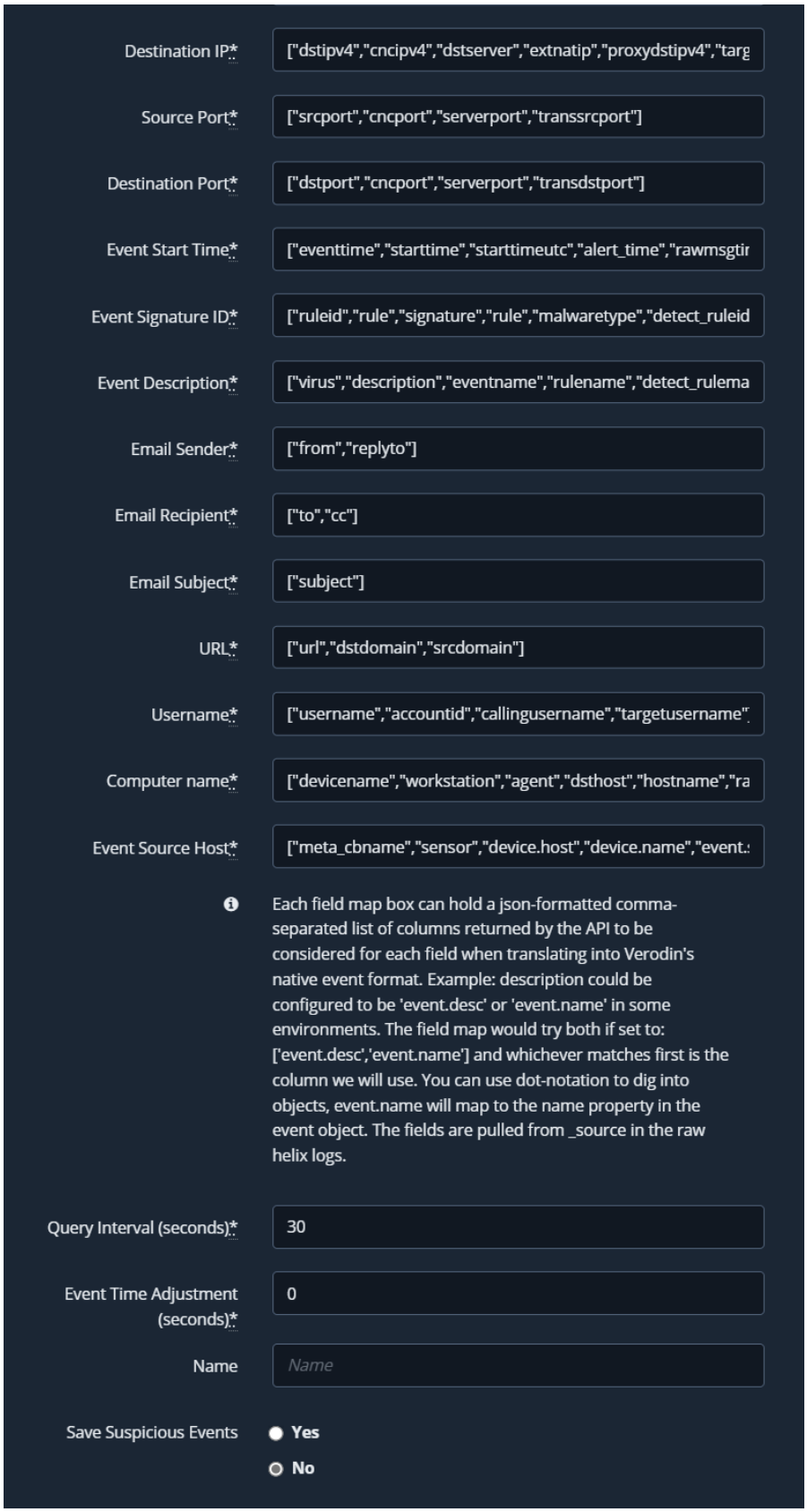
11. (Optional) Select **Discover network devices** automatically.
12. Review and update the **Field Name Mapping** fields.
13. Modify the **Query Interval** and **Event Time Adjustment**, if necessary.
14. (Optional) Assign a **Name**.
15. (Optional) Choose **Yes** to save suspicious events.
16. Click **Submit**.



(https://app.knowledgeowl.com/app/image/pid/620d7e13ccb103e8557b25b0/id/63ebf77ac9ec1e48182a725a/n/trellix-helix.png?imgkey=3c1881a2cce84a39ccf1bf98f3036ff3)

Trellix Helix Integration





(https://app.knowledgeowl.com/app/image/pid/620d7e13ccb103e8557b25b0/id/63ecf3409427d260527efc4d/n/trellix-helix-advanced-options.png?imgkey=3c1881a2cce84a39ccf1bf98f3036ff3)

Trellix Helix Integration - Advanced options

Verify Connectivity

TO VERIFY CONNECTIVITY TO TRELLIX HELIX

Click **Test** to verify that:

- The Director can communicate with the Trellix Helix console using the provided host and user information.
- The API Server is enabled and allowing communication.

If the test is not successful, messages will be displayed to help identify possible issues, such as no connection to the API server.

GOOGLE BIGQUERY

This document applies to Classic Integrations. While the Integrations solution is available, it is no longer actively maintained. Mandiant recommends that you plan a switch to Preview Integrations so you can take advantage of the latest features and functionality. Preview Integrations configuration steps are provided in the Director web interface. For more details, see the **Preview Integrations Documentation** (https://docs.mandiant.com/home/msv-preview-integrations).

This integration is not remote capable.

Update Google BigQuery

Identify or create the service account credentials to access BigQuery.

- BigQuery does not support API keys, you must use a service account.
- Authentication requires the json file for the service account for the BigQuery project.

The service account created must have a minimum of **Data Viewer role** (https://cloud.google.com/bigquery/docs/access-control#bigquery.dataViewer) permissions in order to complete the API call.

Update the Validation Platform

Prerequisites

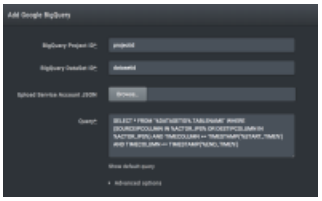
Information to gather before you start:

1. Identify the BigQuery project ID.
2. Identify the BigQuery data set ID.
3. Identify the table and schema used in the data set.
4. Identify the json file for the service account authentication.
5. Identify the field name mappings for the following:
    - Source IP
    - Destination IP
    - Source Port
    - Destination Port
    - Event Start Time (timestamp)
    - Event Unique ID
    - Event Signature ID
    - Event Description

Configuration

TO ADD THE GOOGLE BIGQUERY INTEGRATION

1. Go to **Settings** > **Integrations**.
2. Click **Add Integration** > **Google BigQuery**.



(https://d383cql5uq169w.cloudfront.net/app/image/pid/620d7e13ccb103e8557b25b0/id/629a12dbc9cba0017c2f7e01/n/google-bigquery.png)

Google BigQuery Integration

3. Enter the **Project ID**, **DataSet ID**, and upload the json file for the service account.
4. Modify the **Query** with the appropriate columns for the table's schema.

   Do not change the words inside the percent (%) symbols

5. Expand **Advanced options**.

(https://d383cql5uq169w.cloudfront.net/app/image/pid/620d7e13ccb103e8557b25b0/id/629a12dcc9cba0017c2f7e07/n/google-bigquery-adv.png)

Google BigQuery Integration (Advanced Options)

6. (Optional) Update **Query time** and **Delay time**.

   The **Query time** is the amount of time (minutes) before and after the query runs that the looks for events, while the **Delay time** is the amount of time (minutes) that the platform waits to run the query after a Job Action. For example, you configure your integration with the following values: **Query time** = 5, **Query interval** = 30 seconds, and **Delay time** = 0. When a Job Actions starts at 12:00:00, the first time the query runs, the platform looks for events from 11:55:00 to 12:00:00. Then 30 seconds later, it looks for events from 11:55:30 to 12:00:30. This interval continues, with the last query looking from 12:00:00 to 12:05:00. If you instead configured the **Delay time** to equal 10, it would run the same query, but it wouldn't start that query until 12:10:00.

   If your monitors are set to run more frequently than the query time, it will impact the pass/fail results for AEDA monitors.

7. (Optional) Select **Enable query for Malicious DNS Actions** and configure the **Query**. This query will only be used when you run Malicious DNS Actions or Captive DNS Actions.
8. (Optional) Select **Enable query for Email Actions** and configure the **Query**. This query will be only be used when you run Email Actions.
9. Review the field name mappings and update as necessary.
   a. The field should only contain the name of the column in your table schema that maps to the given field name.
   b. Example: `Source IP: source_ip`
10. (Optional) Select **Discover network devices automatically**.
    If this is not selected, new events processed by the integration will not have discovered or related network or endpoint security technologies.
11. Modify the **Query Interval** and **Event Time Adjustment**, if necessary.
12. (Optional) Assign a **Name**.
13. (Optional) Choose **Yes** to save suspicious events.

14. Click **Submit**.

Verify connectivity

TO VERIFY CONNECTIVITY TO GOOGLE BIGQUERY

Click **Test** to verify that:

- The Director can communicate with Google BigQuery, and the Project ID and DataSet ID are correct.
- The service account credentials provided can perform queries on the project, dataset, and table.

Run a Malicious or Captive DNS Action and then review the last run query to verify:

- The custom DNS query works as expected (if configured).

GOOGLE CLOUD LOGGING

> This document applies to Classic Integrations. While the Integrations solution is available, it is no longer actively maintained. Mandiant recommends that you plan a switch to Preview Integrations so you can take advantage of the latest features and functionality. Preview Integrations configuration steps are provided in the Director web interface. For more details, see the **Preview Integrations Documentation (https://docs.mandiant.com/home/msv-preview-integrations)**.

> This requires the Cloud Validation license.

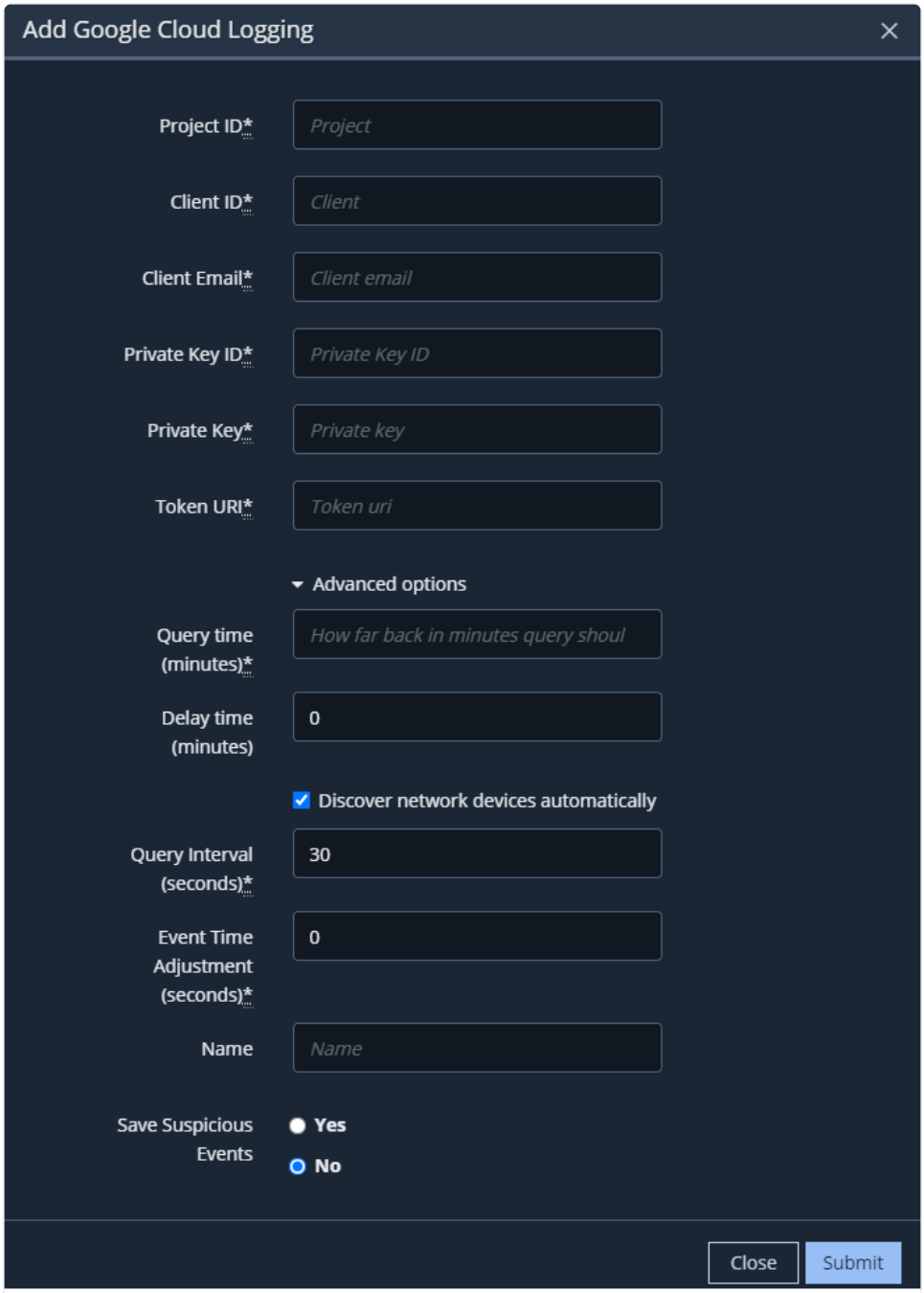
The Google Cloud Logging integration provides events to help you validate security controls of the Google Cloud environment when running Cloud Validation Actions.

Google Cloud Requirements

- Google Cloud does not support API keys, you must use a service account.
- Create a key for your service account in the Google Cloud console.
- After the key is created, you can use a JSON file containing the Service Account Credentials to create this integration.
- The service account must have access to the following minimum permissions:
  - `logging.logEntries.list`
  - `logging.privateLogEntries.list`
  - `logging.views.access`
- These permissions can be provided by the Private Logs Viewer role, though this role might contain a few extra permissions.

Configure Google Cloud Logging Integration

1. Go to **Settings** > **Integrations**.
2. Click **Add Integration** > **Google Cloud Logging**.



Configuration Page for Google Cloud Logging

3. Enter the following required values:
    - **Project ID**
    - **Client ID**
    - **Client Email**
    - **Private Key ID** and **Private Key**
    - **Token URI**
4. (Optional) Expand Advanced options and configure the following, as needed:
    - Set the **Query time**.
    - Set the **Delay time**.

The **Query time** is the amount of time (minutes) before and after the query runs that the platform looks for events, while the **Delay time** is the amount of time (minutes) that the platform waits to run the first query after a Job Action starts. For example, you configure your integration with the following values: **Query time** = 5, **Query interval** = 30 seconds, and **Delay time** = 0. When a Job Actions starts at 12:00:00, the first time the query runs, the platform looks for events from 11:55:00 to 12:00:00. Then 30 seconds later, it looks for events from 11:55:30 to 12:00:30. This interval continues, with the last query looking from 12:00:00 to 12:05:00. If you instead configured the **Delay time** to equal 10, it would run the same query, but it wouldn't start that query until 12:10:00.

If your monitors are set to run more frequently than the query time, this configuration impacts the pass/fail results for AEDA monitors.

- Select **Discover network devices automatically**.
- Specify the **Query Interval**.
- Set the **Event Time Adjustment**.
- Assign a **Name**.
- Choose whether to save suspicious events.

5. Click **Submit**.

Verify connectivity

Click **Test** to verify that:

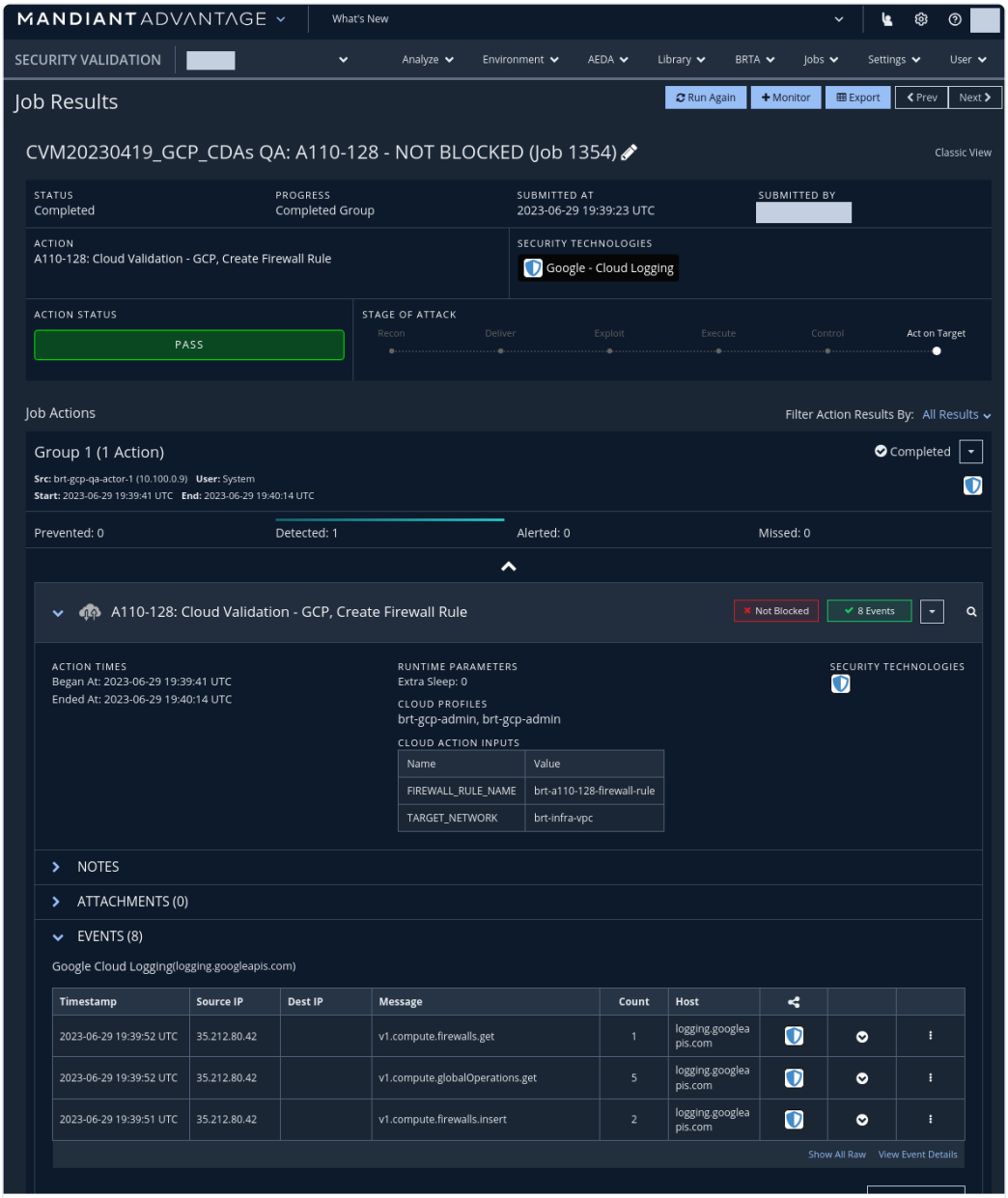
- The Director can communicate with Google Cloud Logging, and the Project ID and Client ID are correct.
- The Service Account Credentials provided can perform queries.

Audit logs

Audit logs are used and require setup in your Google Cloud environment. Data Access audit logs are disabled by default for every Google Cloud Service except BigQuery. For events to be created for Cloud Actions concerned with data access (such as Cloud Validation - GCP, List Firewall Rules (A300-004)), you need to follow the **Enable Data Access audit logs (https://cloud.google.com/logging/docs/audit/configure-data-access)** guide.

Sample Action

The following image shows an example of Job Results for a Cloud Action. The Job Results show events that are retrieved through the Google Cloud Logging integration:



Cloud Action for Google Cloud Logging Events

GRAYLOG

> This document applies to Classic Integrations. While the Integrations solution is available, it is no longer actively maintained. Mandiant recommends that you plan a switch to Preview Integrations so you can take advantage of the latest features and functionality. Preview Integrations configuration steps are provided in the Director web interface. For more details, see the **Preview Integrations Documentation (https://docs.mandiant.com/home/msv-preview-integrations)**.

This integration is remote capable.

Update Graylog

Identify or create credentials to access Graylog with read access, at minimum.

API Calls

The following API calls are used by the Validation Platform.

Purpose	Call
Search raw logs	/api/search/universal/absolute
Search alert events	/api/events/search

Due to a limitation in the Graylog API, the Validation Platform alert correlations are only populated by Graylog filter alerts.

Update the Validation Platform

Prerequisites

Information to gather before you start:

- Identify the hostname/IP used to access Graylog.
- Identify the Port used for Graylog communication (this defaults to 443).
- Identify whether the protocol is HTTP or HTTPS for connections to the Graylog port.
- Obtain the username and password of a Graylog account with appropriate access permissions.

Configuration

TO ADD THE GRAYLOG INTEGRATION

1. Go to **Settings** > **Integrations**.
2. Click **Add Integration** > **Graylog**.

   You can add this as either a Local or Remote Integration.
3. Enter information for the **Host**, **Port**, **Protocol**, **Username** and **Password** or **API Token**.
4. Review and update the **Query**.

   The %ACTOR_IPS% variable can be used in all queries. This improves event matching.

(https://d383cql5uq169w.cloudfront.net/app/image/pid/620d7e13ccb103e8557b25b0/id/629a12efc9cba0017c2f7ec5/n/graylog.pr

Graylog Integration

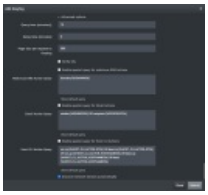
5. Expand **Advanced options**.
6. (Optional) Update **Query time** and **Delay time**.

> The **Query time** is the amount of time (minutes) before and after the query runs that the platform looks for events, while the **Delay time** is the amount of time (minutes) that the platform waits to run the first query after a Job Action starts. For example, you configure your integration with the following values: **Query time** = 5, **Query interval** = 30 seconds, and **Delay time** = 0. When a Job Actions starts at 12:00:00, the first time the query runs, the platform looks for events from 11:55:00 to 12:00:00. Then 30 seconds later, it looks for events from 11:55:30 to 12:00:30. This interval continues, with the last query looking from 12:00:00 to 12:05:00. If you instead configured the **Delay time** to equal 10, it would run the same query, but it wouldn't start that query until 12:10:00.

> If your monitors are set to run more frequently than the query time, this configuration impacts the pass/fail results for AEDA monitors.

7. (Optional) Select **Enable query for Malicious DNS Actions** and configure the **Query**. This query will only be used when you run Malicious DNS Actions or Captive DNS Actions.
8. (Optional) Select **Enable query for Email Actions** and configure the **Query**. This query will only be used when you run Email Actions.
9. (Optional) Select **Enable query for Host CLI Actions** and configure the **Query**. This query will only be used when you run Host CLI Actions.

> If you enable the Host CLI Actions query and use the %HOST_CLI_ACTOR_HOSTNAMES% variable, the platform will substitute the plain hostname and the information from the Alternate Hostname field on the Actor configuration page.



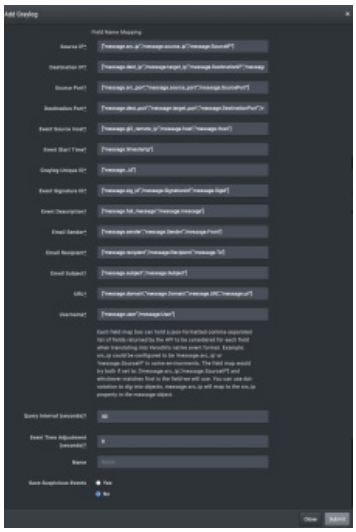
(https://d383cql5uq169w.cloudfront.net/app/image/pid/620d7e13ccb103e8557b25b0/id/629a12dbc9cba0017c2f7e03/n/graylog-adv-1.png)

Graylog Integration (Advanced Options)

10. Identify the field name mappings for the following (there could be multiple of each, depending on log sources and configuration):
    - Source IP
    - Destination IP
    - Source Port
    - Destination Port
    - Event Source Host

- Event Start Time (timestamp)
- Graylog Unique ID
- Event Signature ID
- Event Description
- Email Sender
- Email Recipient
- Email Subject
- URL
- Username

11. Modify the **Query Interval** and **Event Time Adjustment**, if necessary.
12. (Optional) Assign a **Name**.
13. (Optional) Choose **Yes** to save suspicious events.
14. Click **Submit**.



Graylog Integration (Advanced Options)

Verify connectivity

TO VERIFY CONNECTIVITY TO GRAYLOG

Click **Test** to verify that:

- The Director can communicate with the integration host on the port and protocol specified.
- The integration credentials are valid and working.

IBM QRADAR

> This document applies to Classic Integrations. While the Integrations solution is available, it is no longer actively maintained. Mandiant recommends that you plan a switch to Preview Integrations so you can take advantage of the latest features and functionality. Preview Integrations configuration steps are provided in the Director web interface. For more details, see the **Preview Integrations Documentation (https://docs.mandiant.com/home/msv-preview-integrations)**.

This integration is remote capable.

Update the Validation Platform

Prerequisites

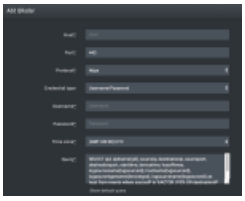
Information to gather before you start:

1. IP address used to access QRadar.
2. Port for QRadar communications (default is 443).
3. Identify whether the protocol is HTTP or HTTPS for connections to the QRadar port (default is HTTPS).
4. Identify or create credentials to access QRadar. Admin permissions are required, at minimum.
5. Identify the timezone of the QRadar host.

Configuration

TO ADD THE QRADAR INTEGRATION

1. Go to **Settings** > **Integrations**.
2. Click **Add Integration** > **QRadar**.



(https://d383cql5uq169w.cloudfront.net/app/image/pid/620d7e13ccb103e8557b25b0/id/629a12d8c9cba0017c2f7ddd/n/qradar-836.png)

QRadar Integration

3. Enter information for the **Host**, **Port**, and **Protocol**.
4. Select the **Credential type** and add the appropriate credentials.
5. Change the **Time zone** to match that of the QRadar host.
6. Review and update the **Query** to include instance-specific field names, sources, data types, and other customizations.

   The default queries can be viewed by clicking **Show default query.**

   The query includes information that allows event matching based on any file hashes included in an Action.

7. Expand **Advanced options**.

(https://d383cql5uq169w.cloudfront.net/app/image/pid/620d7e13ccb103e8557b25b0/id/629a12d7c9cba0017c2f7dd5/n/qradar-adv.png)

QRadar Integration - Advanced section

8. (Optional) Update **Query time** and **Delay time**.

   The **Query time** is the amount of time (minutes) before and after the query runs that the platform looks for events, while the **Delay time** is the amount of time (minutes) that the platform waits to run the first query after a Job Action starts. For example, you configure your integration with the following values: **Query time** = 5, **Query interval** = 30 seconds, and **Delay time** = 0. When a Job Actions starts at 12:00:00, the first time the query runs, the platform looks for events from 11:55:00 to 12:00:00. Then 30 seconds later, it looks for events from 11:55:30 to 12:00:30. This interval continues, with the last query looking from 12:00:00 to 12:05:00. If you instead configured the **Delay time** to equal 10, it would run the same query, but it wouldn't start that query until 12:10:00.

   If your monitors are set to run more frequently than the query time, this configuration impacts the pass/fail results for AEDA monitors.

9. (Optional) Review and update the populated query information (**Flows query**, **Offense query** fields, **Offense query** filter, **Correlated Events Query**).
10. (Optional) Select **Enable query for Malicious DNS Actions** and configure the **Query**. This query will only be used when you run Malicious DNS Actions or Captive DNS Actions.
11. (Optional) Select **Enable query for Email Actions** and configure the **Query**. This query will be only be used when you run Email Actions.
12. (Optional) Select **Enable query for Host CLI Actions** and configure the **Query**. This query will only be used when you run Host CLI Actions.

    If you enable the Host CLI Actions query and use the %HOST_CLI_ACTOR_HOSTNAMES% variable, the platform will substitute the plain hostname and the information from the Alternate Hostname field on the Actor configuration page.

13. (Optional) Select **Discover network devices automatically**.
14. Modify the **Query Interval** and **Event Time Adjustment**, if necessary.
15. (Optional) Assign a **Name**.
16. (Optional) Choose **Yes** to save suspicious events.
17. Click **Submit**.

The QRadar integration can also include these two fields in its queries:

- `host`, which when populated will be used to indicate the source of the events.
- `url`, which when populated is used for matching events to DNS query Actions.

  The url field is not a default qradar field, so you name it yourself. For example, `select qid, qidname(qid), "DNS_Domain" as url, sourceip,`

Verify connectivity

TO VERIFY CONNECTIVITY TO QRADAR

Click **Test** to verify that:

- The Director can communicate with QRadar on the port and protocol specified.
- QRadar credentials are valid and working.
- Times match.

Run a Malicious or Captive DNS Action and then review the last run query to verify:

- The custom DNS query works as expected (if configured).

JUNIPER SECURE ANALYTICS (JSA)

> This document applies to Classic Integrations. While the Integrations solution is available, it is no longer actively maintained. Mandiant recommends that you plan a switch to Preview Integrations so you can take advantage of the latest features and functionality. Preview Integrations configuration steps are provided in the Director web interface. For more details, see the **Preview Integrations Documentation (https://docs.mandiant.com/home/msv-preview-integrations)**.

This integration is remote capable.

Update Juniper JSA

Set up the credentials that will be used with the Validation Platform.

- Username and password or authentication token.
- Admin permissions are required, at minimum .

Update the Validation Platform

Prerequisites

Information to gather before you start:

1. Identify the IP address.
2. Identify the port communications (default is 443).
3. Identify whether the protocol is HTTP or HTTPS (default is HTTPS).
4. Have the credential information .
5. Identify the timezone of the Juniper host.

Configuration

TO ADD THE JUNIPER JSA INTEGRATION

1. Go to **Settings** > **Integrations**.
2. Click **Add Integration** > **Juniper JSA**.

(https://d383cql5uq169w.cloudfront.net/app/image/pid/620d7e13ccb103e8557b25b0/id/629a12e5c9cba0017c2f7e6c/n/juniper-jsa.png)

Juniper JSA Integration

3. Populate the **Host**, **Port**, and **Protocol** information.
4. Enter information for the **Host**, **Port**, and **Protocol**.
5. Select the **Credential type** and enter the appropriate credentials.
6. Change the **Time Zone** to match that of the Juniper JSA host.
7. Expand **Advanced options**.

(https://d383cql5uq169w.cloudfront.net/app/image/pid/620d7e13ccb103e8557b25b0/id/629a12edc9cba0017c2f7eae/n/juniper-jsa-advanced.png)

Juniper JSA Integration (Advanced Options)

8. (Optional) Update **Query time** and **Delay time**.

   The **Query time** is the amount of time (minutes) before and after the query runs that the platform looks for events, while the **Delay time** is the amount of time (minutes) that the platform waits to run the first query after a Job Action starts. For example, you configure your integration with the following values: **Query time** = 5, **Query interval** = 30 seconds, and **Delay time** = 0. When a Job Actions starts at 12:00:00, the first time the query runs, the platform looks for events from 11:55:00 to 12:00:00. Then 30 seconds later, it looks for events from 11:55:30 to 12:00:30. This interval continues, with the last query looking from 12:00:00 to 12:05:00. If you instead configured the **Delay time** to equal 10, it would run the same query, but it wouldn't start that query until 12:10:00.

   If your monitors are set to run more frequently than the query time, this configuration impacts the pass/fail results for AEDA monitors.

9. (Optional) Review and update the populated query information (**Flows query**, **Offense query fields**, **Offense query filter**, **Correlated Events Query**.
10. (Optional) Enable the special query for DNS Actions and define the Query.
11. (Optional) Enable the special query for Email Actions and define the Query.
12. (Optional) Enable the special query for Host CLI Actions and define the **Query**.

    If you enable the Host CLI Actions query and use the %HOST_CLI_ACTOR_HOSTNAMES% variable, the platform will substitute the plain hostname and the information from the Alternate Hostname field on the Actor configuration page.

13. (Optional) Select **Discover network devices automatically**.
14. Modify the **Query Interval** and **Event Time Adjustment**, if necessary.
15. (Optional) Assign a **Name**.
16. (Optional) Choose **Yes** to save suspicious events.
17. Click **Submit**.

Verify connectivity

TO VERIFY CONNECTIVITY TO JUNIPER JSA

Click **Test** to verify that:

- The Director can communicate with Juniper JSA on the port and protocol specified.
- Credentials are valid and working.
- Times match.

LOGRHYTHM ELASTICSEARCH

> This document applies to Classic Integrations. While the Integrations solution is available, it is no longer actively maintained. Mandiant recommends that you plan a switch to Preview Integrations so you can take advantage of the latest features and functionality. Preview Integrations configuration steps are provided in the Director web interface. For more details, see the **Preview Integrations Documentation (https://docs.mandiant.com/home/msv-preview-integrations)**.

This integration is remote capable.

Update LogRhythm Elasticsearch

Prerequisites

1. Ensure network connectivity between the DX and the Security Validation Director.
2. Identify the IP address used to access Elasticsearch. This could be direct access to an Elasticsearch node, Primary node, or something such as an nginx reverse proxy.

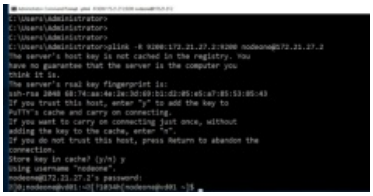
Configuration

Complete the following steps on the LogRhythm Server (if single-tiered deployment) or DX (administrative access not required).

On the LogRhythm Server

SSH from the LogRhythm DX to the Validation Platform Director.

- On a Microsoft(R) Windows(R) host, plink.exe can be used as follows:
  `plink -R 9200:localhost:9200 nodeone@DIRECTORIP`
- If linux DX, use normal ssh instead of plink:
  `ssh -N -R 9200:localhost:9200 nodeone@DIRECTORIP`



(https://d383cql5uq169w.cloudfront.net/app/image/pid/620d7e13ccb103e8557b25b0/id/629a12ecc9cba0017c2f7ea1/n/lge-step1.png)

SSH from LogRhythm to the Validation Platform Director

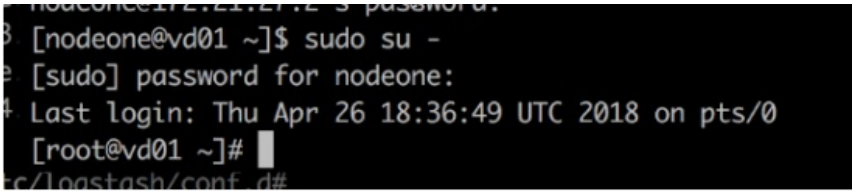
On the Validation Platform Director (CLI)

1. SSH to the Security Validation Director using the "nodeone" password.
   a. `ssh nodeone@DIRECTOR_IP`

(https://d383cql5uq169w.cloudfront.net/app/image/pid/620d7e13ccb103e8557b25b0/id/629a12eac9cba0017c2f7e93/n/lge-step2.png)

SSH to the Validation Platform Director using nodeone password

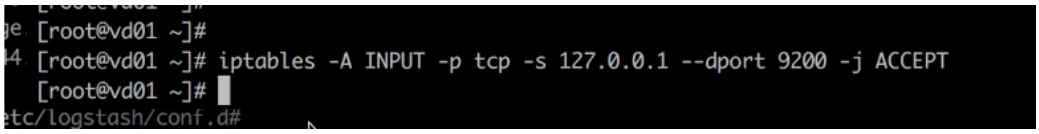
2. Assume root access.
    a. `sudo su -`



(https://d383cql5uq169w.cloudfront.net/app/image/pid/620d7e13ccb103e8557b25b0/id/629a12ebc9cba0017c2f7e98/n/lge-step3.png)

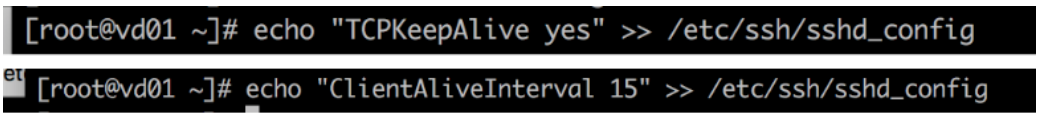
Assume root access

3. Add the following custom iptables rule to allow communication to Elastic over the SSH tunnel:
    a. `iptables -A INPUT -p tcp -s 127.0.0.1 --dport 9200 -j ACCEPT`



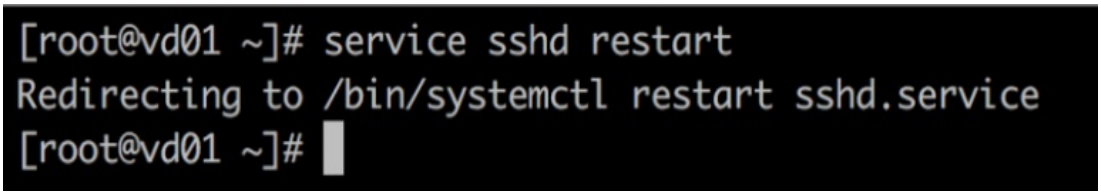
Add iptables Rules

4. Add the following configuration lines to `/etc/ssh/sshd_config`.
    a. `TCPKeepAlive yes`
    b. `ClientAliveInterval 15`



Configure Keepalive

5. Restart the SSH service.
    `service sshd restart`



(https://d383cql5uq169w.cloudfront.net/app/image/pid/620d7e13ccb103e8557b25b0/id/629a12efc9cba0017c2f7ec7/n/lge-step6.png)

Restart SSH service

Update the Validation Platform

Prerequisites

Information to gather before you start:

1. Identify the port for Elasticsearch communication (default is 9200).
2. Identify whether the protocol is HTTP or HTTPS for connections to the Elasticsearch port.
3. Identify the field name mappings for the following (there could be multiple of each, depending on log sources and

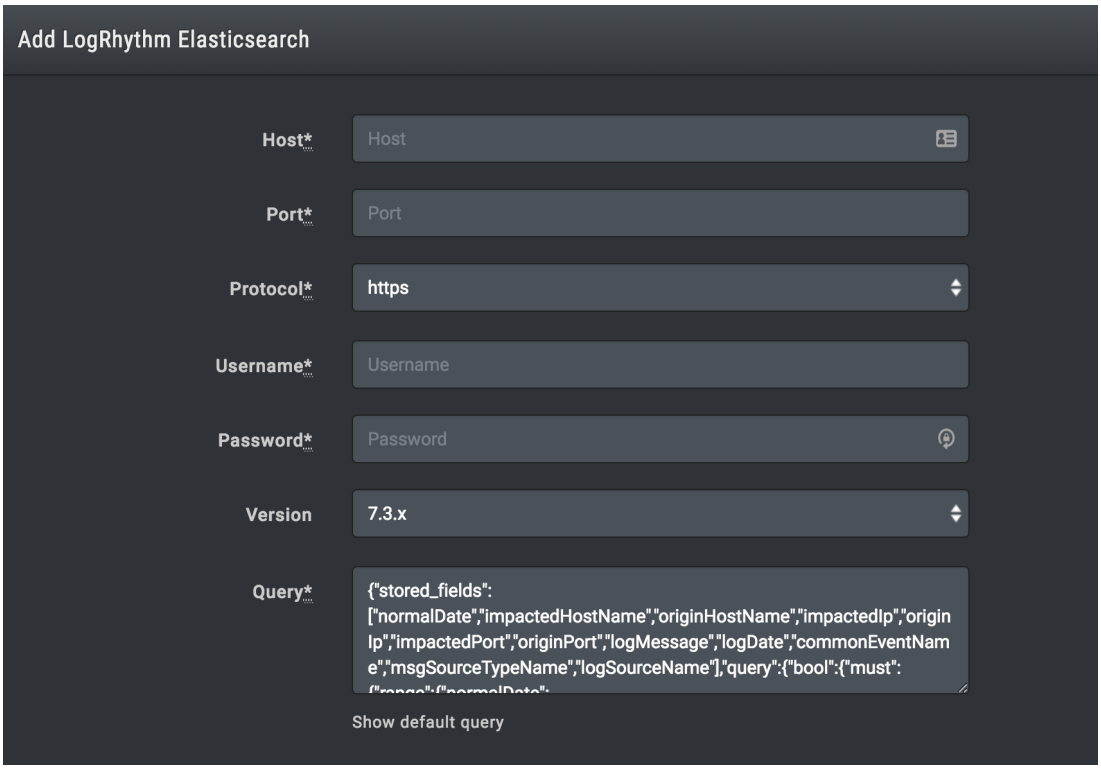
configuration):

- Source IP
- Destination IP
- Source Port
- Destination Port
- Event Start Time (timestamp)
- Event Unique ID
- Event Signature ID
- Event Description
- Event Source Host

Configuration

TO ADD THE LOGRHYTHM ELASTICSEARCH INTEGRATION

1. Go to **Settings** > **Integrations**.
2. Click **Add Integration** > **LogRhythm Elasticsearch**.



LogRhythm Elasticsearch Integration

3. Enter the **Host**.

   This will almost always be either "localhost" or "127.0.0.1".

4. Enter the **Port**, **Protocol**, and if using, the **Username** and **Password**.
5. Select the appropriate version.

   This may adjust the default query and field name mapping section.

6. Review and update the **Query**, if necessary.
7. Expand **Advanced options**.

(https://d383cql5uq169w.cloudfront.net/app/image/pid/620d7e13ccb103e8557b25b0/id/629a12dec9cba0017c2f7e24/n/logrhythm-elasticsearch-advanced.png)

LogRhythm Elasticsearch Integration (Advanced Options)

8. (Optional) Update **Query time** and **Delay time**.

   The **Query time** is the amount of time (minutes) before and after the query runs that the platform looks for events, while the **Delay time** is the amount of time (minutes) that the platform waits to run the first query after a Job Action starts. For example, you configure your integration with the following values: **Query time** = 5, **Query interval** = 30 seconds, and **Delay time** = 0. When a Job Actions starts at 12:00:00, the first time the query runs, the platform looks for events from 11:55:00 to 12:00:00. Then 30 seconds later, it looks for events from 11:55:30 to 12:00:30. This interval continues, with the last query looking from 12:00:00 to 12:05:00. If you instead configured the **Delay time** to equal 10, it would run the same query, but it wouldn't start that query until 12:10:00.

   If your monitors are set to run more frequently than the query time, this configuration impacts the pass/fail results for AEDA monitors.

9. (Optional) Enable the special query for Host CLI Actions and review the **Query**.

   If you enable the Host CLI Actions query and use the %HOST_CLI_ACTOR_HOSTNAMES% variable, the platform will substitute the plain hostname and the information from the Alternate Hostname field on the Actor configuration page.

10. (Optional) Select **Discover network devices automatically**.
11. Review and update the field name mapping section.
    a. Inputs are enclosed by square brackets `[ ]`.
    b. Inputs point to the path location (`["_id"]`).
    c. Nested locations should be enclosed in one set of brackets, encompassed in quotes, and separated by commas (`["_source","src_ip"]`).
12. Modify the **Query Interval** and **Event Time Adjustment**, if necessary.
13. (Optional) Assign a **Name**.
14. (Optional) Choose **Yes** to save suspicious events.
15. Click **Submit**.

Verify connectivity

TO VERIFY CONNECTIVITY TO LOGRHYTHM ELASTICSEARCH

Click **Test** to verify that:

- The Director can communicate with the Elasticsearch host IP address on the port specified.
- The Elasticsearch credentials can perform queries on the index or indexes with relevant data.

Updating the Integration

If you update LogRhythm, you will need to update the integration within the Validation Platform. Modifying the version may adjust the default query and the field name mapping section.

Any changes you made previously to the query and field mapping will be retained. Review the default query and the field name mapping sections to verify that no additional changes are required.

LOGRHYTHM SQL

> This document applies to Classic Integrations. While the Integrations solution is available, it is no longer actively maintained. Mandiant recommends that you plan a switch to Preview Integrations so you can take advantage of the latest features and functionality. Preview Integrations configuration steps are provided in the Director web interface. For more details, see the **Preview Integrations Documentation (https://docs.mandiant.com/home/msv-preview-integrations)**.

This integration is not remote capable.

Update LogRhythm SQL

- Verify you have the latest LogRhythm Knowledge Base updates added to your instance. These updates contain rules and identifiers for various actors and actions.
- Disable LogMart on any log sources where it is not explicitly required. The resources used by LogMart can cause delays when Actions are run.

Update the Validation Platform

Prerequisites

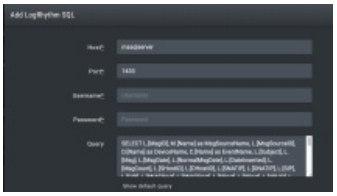
Information to gather before you start:

- Identify the host (name or IP) and Port information.
- Have a valid account for LogRhythm SQL.

Configuration

TO ADD THE LOGRHYTHM SQL INTEGRATION

1. Go to **Settings** > **Integrations**.
2. Click **Add Integration** > **LogRhythm SQL**.



(https://d383cql5uq169w.cloudfront.net/app/image/pid/620d7e13ccb103e8557b25b0/id/629a12e0c9cba0017c2f7e34/n/logrhythm-sql.png)

LogRhythm SQL Integration

3. Enter information for the **Host**, **Port**, **Username**, and **Password**.
4. Expand **Advanced options**.

(https://d383cql5uq169w.cloudfront.net/app/image/pid/620d7e13ccb103e8557b25b0/id/629a12dfc9cba0017c2f7e2e/n/logrhythm-sql-adv.png)

LogRhythm SQL Integration

5. (Optional) Update **Query time** and **Delay time**.

The **Query time** is the amount of time (minutes) before and after the query runs that the platform looks for events, while the **Delay time** is the amount of time (minutes) that the platform waits to run the first query after a Job Action starts. For example, you configure your integration with the following values: **Query time** = 5, **Query interval** = 30 seconds, and **Delay time** = 0. When a Job Actions starts at 12:00:00, the first time the query runs, the platform looks for events from 11:55:00 to 12:00:00. Then 30 seconds later, it looks for events from 11:55:30 to 12:00:30. This interval continues, with the last query looking from 12:00:00 to 12:05:00. If you instead configured the **Delay time** to equal 10, it would run the same query, but it wouldn't start that query until 12:10:00.

If your monitors are set to run more frequently than the query time, this configuration impacts the pass/fail results for AEDA monitors.

6. (Optional) Select **Enable query for Malicious DNS Actions** and configure the **Query**. This query will only be used when you run Malicious DNS Actions or Captive DNS Actions.
7. (Optional) Select **Enable query for Email Actions** and configure the **Query**. This query will be only be used when you run Email Actions.
8. (Optional) Select **Enable query for Host CLI Actions** and configure the **Query**. This query will only be used when you run Host CLI Actions.

   If you enable the Host CLI Actions query and use the %HOST_CLI_ACTOR_HOSTNAMES% variable, the platform will substitute the plain hostname and the information from the Alternate Hostname field on the Actor configuration page.

   If you find that LogRhythm SQL is matching too many noisy logs, we recommend you add MsgSourceID to the WHERE clause in the Host CLI Actions query. For example, WHERE L.[NormalMsgDate] = '%START_TIME%' AND L.[MsgSourceID] = 1. If the events are still too noisy, consider adjusting your Risk Based Priority (RBP) settings in LogRhythm.

9. (Optional) Select **Discover network devices automatically**.
10. Modify the **Query Interval** and **Event Time Adjustment**, if necessary.
11. (Optional) Assign a **Name**.
12. (Optional) Choose **Yes** to save suspicious events.
13. Click **Submit**.

Verify Connectivity

TO VERIFY CONNECTIVITY

Click **Test** to verify that:

- The Director can communicate with the LogRhythm SQL host on the port specified.
- The LogRhythm SQL credentials are valid and working.

LOGZILLA

> This document applies to Classic Integrations. While the Integrations solution is available, it is no longer actively maintained. Mandiant recommends that you plan a switch to Preview Integrations so you can take advantage of the latest features and functionality. Preview Integrations configuration steps are provided in the Director web interface. For more details, see the **Preview Integrations Documentation (https://docs.mandiant.com/home/msv-preview-integrations)**.

This integration is not remote capable.

Update Logzilla

1. Identify or create credentials to access integration with read access, at minimum.
2. Generate a new authorization token in the LogZilla command line:
    a. `logzilla authtoken`

API Calls

The following API calls are used by the Validation Platform.

Purpose	Call
Query events and notifications	/api/query

Update the Validation Platform

Prerequisites

Information to gather before you start:

- Identify the hostname/IP used to access LogZilla.
- Identify the Port used for Graylog communication (this defaults to 443).
- Identify whether the protocol is HTTP or HTTPS for connections to the LogZilla port.
- Obtain the Auth Token of a LogZilla account with appropriate access permissions.

Configuration

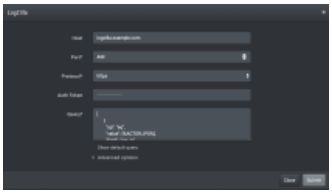
TO ADD THE LOGZILLA INTEGRATION

1. Go to **Settings** > **Integrations**.
2. Click **Add Integration** > **LogZilla**.

    You can add this as either a Local or Remote Inetgration.

3. Enter information for the **Host**, **Port**, and **Protocol**.
4. Review and update the **Query**.

    The %ACTOR_IPS% variable can be used in all queries. This improves event matching.



(https://d383cql5uq169w.cloudfront.net/app/image/pid/620d7e13ccb103e8557b25b0/id/629a12dfc9cba0017c2f7e33/n/logzilla.pr

LogZilla Integration

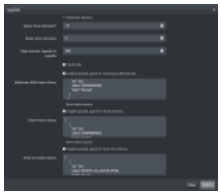
5. Expand **Advanced options**.
6. (Optional) Update **Query time** and **Delay time**.

> The **Query time** is the amount of time (minutes) before and after the query runs that the platform looks for events, while the **Delay time** is the amount of time (minutes) that the platform waits to run the first query after a Job Action starts. For example, you configure your integration with the following values: **Query time** = 5, **Query interval** = 30 seconds, and **Delay time** = 0. When a Job Actions starts at 12:00:00, the first time the query runs, the platform looks for events from 11:55:00 to 12:00:00. Then 30 seconds later, it looks for events from 11:55:30 to 12:00:30. This interval continues, with the last query looking from 12:00:00 to 12:05:00. If you instead configured the **Delay time** to equal 10, it would run the same query, but it wouldn't start that query until 12:10:00.

> If your monitors are set to run more frequently than the query time, this configuration impacts the pass/fail results for AEDA monitors.

7. (Optional) Select **Enable query for Malicious DNS Actions** and configure the **Query**. This query will only be used when you run Malicious DNS Actions or Captive DNS Actions.
8. (Optional) Select **Enable query for Email Actions** and configure the **Query**. This query will be only be used when you run Email Actions.
9. (Optional) Select **Enable query for Host CLI Actions** and configure the **Query**. This query will only be used when you run Host CLI Actions.

> If you enable the Host CLI Actions query and use the %HOST_CLI_ACTOR_HOSTNAMES% variable, the platform will substitute the plain hostname and the information from the Alternate Hostname field on the Actor configuration page.



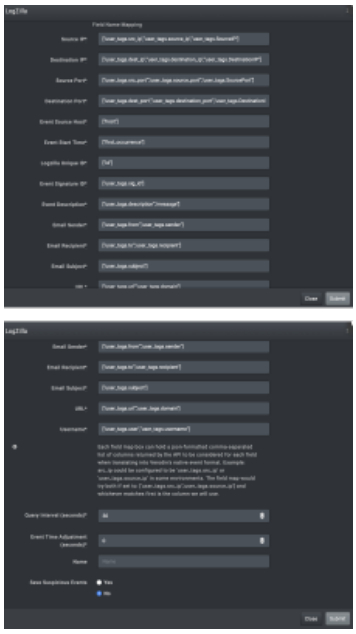
(https://d383cql5uq169w.cloudfront.net/app/image/pid/620d7e13ccb103e8557b25b0/id/629a12e5c9cba0017c2f7e66/n/logzilla-adv-1.png)

LogZilla Integration (Advanced Options)

10. Identify the field name mappings for the following (there could be multiple of each, depending on log sources and configuration):
    - Source IP
    - Destination IP
    - Source Port
    - Destination Port
    - Event Source Host
    - Event Start Time (timestamp)
    - LogZilla Unique ID
    - Event Signature ID
    - Event Description
    - Email Sender
    - Email Recipient
    - Email Subject
    - URL

- Username

11. Modify the **Query Interval** and **Event Time Adjustment**, if necessary.
12. (Optional) Assign a **Name**.
13. (Optional) Choose **Yes** to save suspicious events.
14. Click **Submit**.



LogZilla Integration (Advanced Options)

Verify connectivity

TO VERIFY CONNECTIVITY TO LOGZILLA

Click **Test** to verify that:

- The Director can communicate with the integration host on the port and protocol specified.
- The integration credentials are valid and working.

TRELLIX ENTERPRISE SECURITY MANAGER

> This document applies to Classic Integrations. While the Integrations solution is available, it is no longer actively maintained. Mandiant recommends that you plan a switch to Preview Integrations so you can take advantage of the latest features and functionality. Preview Integrations configuration steps are provided in the Director web interface. For more details, see the **Preview Integrations Documentation (https://docs.mandiant.com/home/msv-preview-integrations)**.

The Trellix Enterprise Security Manager Integration supports correlation events when using Trellix Enterprise Security Manager v10.x.

This integration is remote capable.

Update Trellix Enterprise Security Manager

TO UPDATE TRELLIX ENTERPRISE SECURITY MANAGER

1. Identify or create credentials to access Nitro with reporting permissions, at minimum.
2. Ensure that the credentials use Greenwich Mean Time and "YYYY-MM-DD HH:MM:SS" date/time format.

Update the Validation Platform

Prerequisites

Information to gather before you start:

- IP address/host information used to access Trellix (ESM or ePO)
- Port for Trellix (ESM or ePO) communications (default is 443)
- Identify whether the protocol is HTTP or HTTPS for connections to the port (default is HTTPS)

Configuration

TO ADD THE TRELLIX ENTERPRISE SECURITY MANAGER INTEGRATION

1. Go to **Settings** > **Integrations**.
2. Click **Add Integration** > **Trellix Enterprise Security Manager**.

You can add this as either a Local or Remote Integration.

3. Enter information for the **Host**, **Port**, **Protocol**, **Username** and **Password** or **API Token**.
4. If necessary, modify the **Query**.
5. Expand **Advanced options**.
6. (Optional) Update **Query time** and **Delay time**.

The **Query time** is the amount of time (minutes) before and after the query runs that the platform looks for events, while the **Delay time** is the amount of time (minutes) that the platform waits to run the first query after a Job Action starts. For example, you configure your integration with the following values: **Query time** = 5, **Query interval** = 30 seconds, and **Delay time** = 0. When a Job Actions starts at 12:00:00, the first time the query runs, the platform looks for events from 11:55:00 to 12:00:00. Then 30 seconds later, it looks for events from 11:55:30 to 12:00:30. This interval continues, with the last query looking from 12:00:00 to 12:05:00. If you instead configured the **Delay time** to equal 10, it would run the same query, but it wouldn't start that query until 12:10:00.

If your monitors are set to run more frequently than the query time, this configuration impacts the pass/fail results for AEDA monitors.

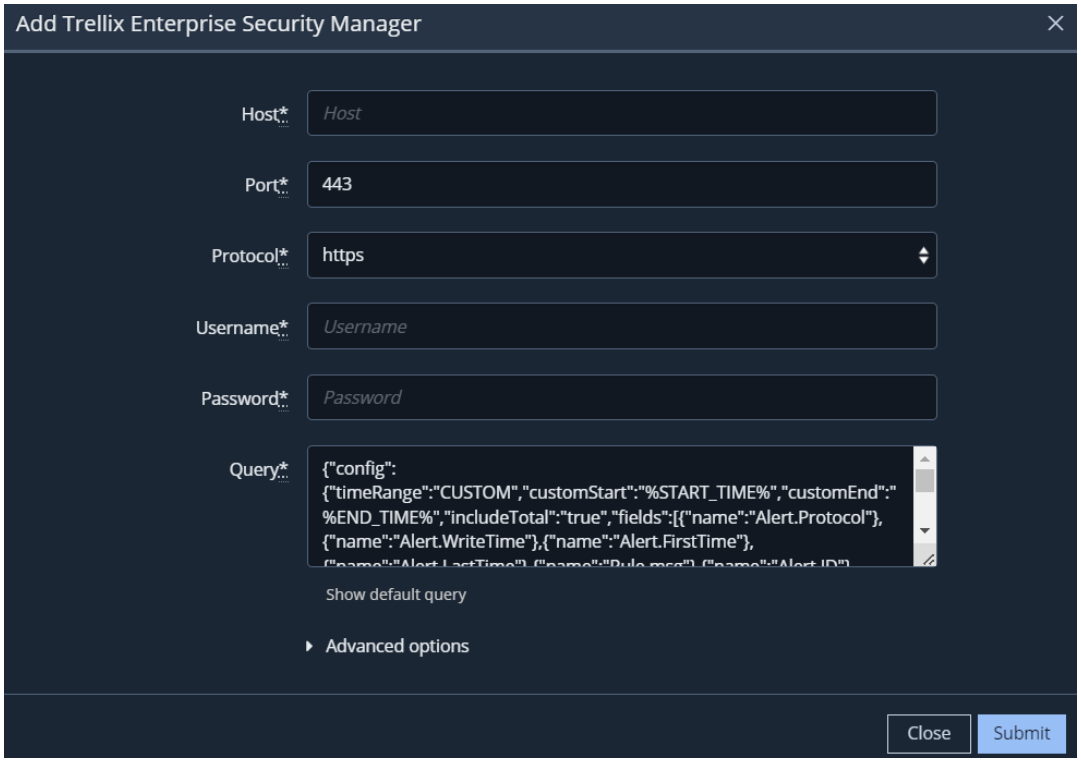
7. (Optional) Select **Enable query for Host CLI Actions** and configure the **Query**. This query will only be used when you run Host CLI Actions.

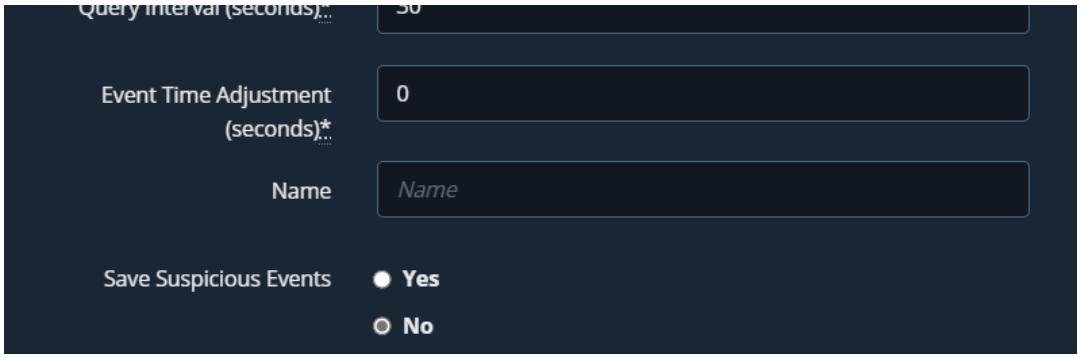
   If you enable the Host CLI Actions query and use the %HOST_CLI_ACTOR_HOSTNAMES% variable, the platform will substitute the plain hostname and the information from the Alternate Hostname field on the Actor configuration page.

8. (Optional) Select **Enable query for Malicious DNS Actions** and configure the **Query**. This query will only be used when you run Malicious DNS Actions or Captive DNS Actions.
9. (Optional) Select **Enable query for Email Actions** and configure the **Query**. This query will be only be used when you run Email Actions.
10. Verify that the **Device List Refresh Interval** is correct.
11. (Optional) Review and update the **Device Type List** information.
12. Enter the **McAfee version**.

    If you are using version 11.0 or greater, you must enter your version number in this field to use the current version of Trellix Enterprise Security Manager's API. By default, version 10 is assumed.

13. Modify the number of **Query Checks** and the **Query Check Interval**, if needed.
14. Modify the **Query Interval** and **Event Time Adjustment**, if necessary.
15. (Optional) Assign a **Name**.
16. (Optional) Choose **Yes** to save suspicious events.
17. Click **Submit**.





(https://app.knowledgeowl.com/app/image/pid/620d7e13ccb103e8557b25b0/id/63ecf2d822231f4e6777d2b7/n/trellix-enterprise-security-manager-advanced-options.png?imgkey=3c1881a2cce84a39ccf1bf98f3036ff3)

Trellix Enterprise Security Manager Integration - Advanced options

Verify Connectivity

TO VERIFY CONNECTIVITY TO TRELLIX ENTERPRISE SECURITY MANAGER

Click **Test** to verify that:

- The Director can communicate with Trellix Enterprise Security Manager IP address on the port specified.
- Credentials are valid and working.

MICROSOFT AZURE LOG ANALYTICS

> This document applies to Classic Integrations. While the Integrations solution is available, it is no longer actively maintained. Mandiant recommends that you plan a switch to Preview Integrations so you can take advantage of the latest features and functionality. Preview Integrations configuration steps are provided in the Director web interface. For more details, see the **Preview Integrations Documentation (https://docs.mandiant.com/home/msv-preview-integrations)**.

Update Azure Log Analytics

- Identify or create credentials to access Log Analytics with read access, at minimum.
- Verify you have access to the Log Analytics API with Data.Read permission.
- Identify the following values:
  - Client ID
  - Client Secret
  - Tenant ID
  - Workspace ID

These values are generated when you configure Log Analytics. If you have not yet registered Log Analytics as an application in Azure, refer to the **Microsoft documentation (https://docs.microsoft.com/en-us/azure/active-directory-b2c/tutorial-register-applications?tabs=app-reg-ga)** for further assistance .

- Set up Tables in Log Analytics.

Queries in the Azure Log Analytics integration will error if corresponding Tables are not configured in Log Analytics. For example, the default Malicious DNS Action Query in the integration needs the DnsEvents table in Log Analytics to be configured.

TO ACCESS THE CLIENT ID, CLIENT SECRET, TENANT ID, AND WORKSPACE ID

If you do not already know the values required to add the Azure Log Analytics integration, you must locate them in the Azure portal.

Refer to the **Microsoft documentation (https://docs.microsoft.com/en-us/azure/active-directory-b2c/tutorial-register-applications?tabs=app-reg-ga)** for further assistance identifying these values.

1. In the Azure Log Analytics portal, take note of your **Workspace ID**.
2. In the Azure Active Directory portal, take note of your **Tenant ID**.
3. In the Azure Active Directory portal, navigate to **App registrations** > **New registration**.
4. Enter the required registration information.
   a. Take note of the **Client ID**.
   b. The required **Redirect URI** field can be set to your Director's URL.
5. Navigate to the **Certificates & Secrets** page.
6. Create a new client secret and take note of the value.

TO ADD THE DATA.READ API PERMISSION

1. In the Azure Log Analytics portal, navigate to the **API Permissions** page.
2. Add Log Analytics **Data.Read** permission.

3. Get administrator approval for the application.

API Calls

The following API calls are used by the Validation Platform.

Purpose	Call
Auth	https://login.microsoftonline.com/{tenent_id}/oauth2/token  For Azure Government (GovCloud): https://login.microsoftonline.us/{tenent_id}/oauth2/token
Query Log Analytics	https://api.loganalytics.io/v1/workspaces/{workspace_id}/query  For Azure Government (GovCloud): https://api.loganalytics.us/v1/workspaces/{workspace_id}/query

Update the Validation Platform

Prerequisites

This integration requires the Cloud Validation Module.

Information to gather before you start:

- Identify the Client ID unique to your application.
- Identify the Client Secret unique to your application.
- Identify the Tenant ID.
- Identify the Workspace ID.

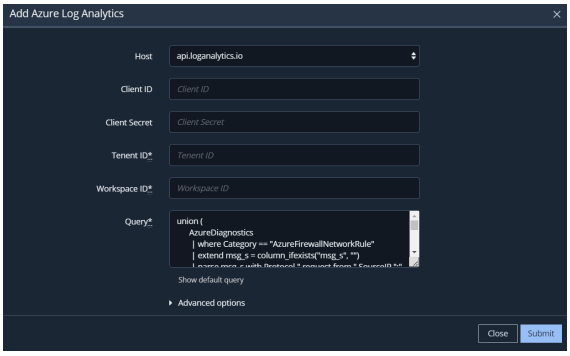
Configuration

TO ADD THE AZURE LOG ANALYTICS INTEGRATION

1. Go to **Settings** > **Integrations**.
2. Click **Add Integration** > **Azure Log Analytics**.

    You can add this as either a Local or Remote Integration.

3. From the **Host** drop-down list, select the appropriate value depending on your Azure Log Analytics environment:
   - The entry ending in **.io** for standard Azure environments
   - The entry ending in **.us** for Azure Government (GovCloud) environments
4. Enter **Client ID** and **Client Secret**.
5. Enter **Tenant ID** and **Workspace ID**.
6. Modify the **Query**, as necessary.



Microsoft Azure Log Analytics Integration

7. Expand **Advanced options**.
    a. (Optional) Update **Query time (minutes)** and **Delay time (minutes)**.

> The **Query time** is the amount of time (minutes) before and after the query runs that the platform looks for events, while the **Delay time** is the amount of time (minutes) that the platform waits to run the first query after a Job Action starts. For example, you configure your integration with the following values: **Query time** = 5, **Query interval** = 30 seconds, and **Delay time** = 0. When a Job Actions starts at 12:00:00, the first time the query runs, the platform looks for events from 11:55:00 to 12:00:00. Then 30 seconds later, it looks for events from 11:55:30 to 12:00:30. This interval continues, with the last query looking from 12:00:00 to 12:05:00. If you instead configured the **Delay time** to equal 10, it would run the same query, but it wouldn't start that query until 12:10:00.

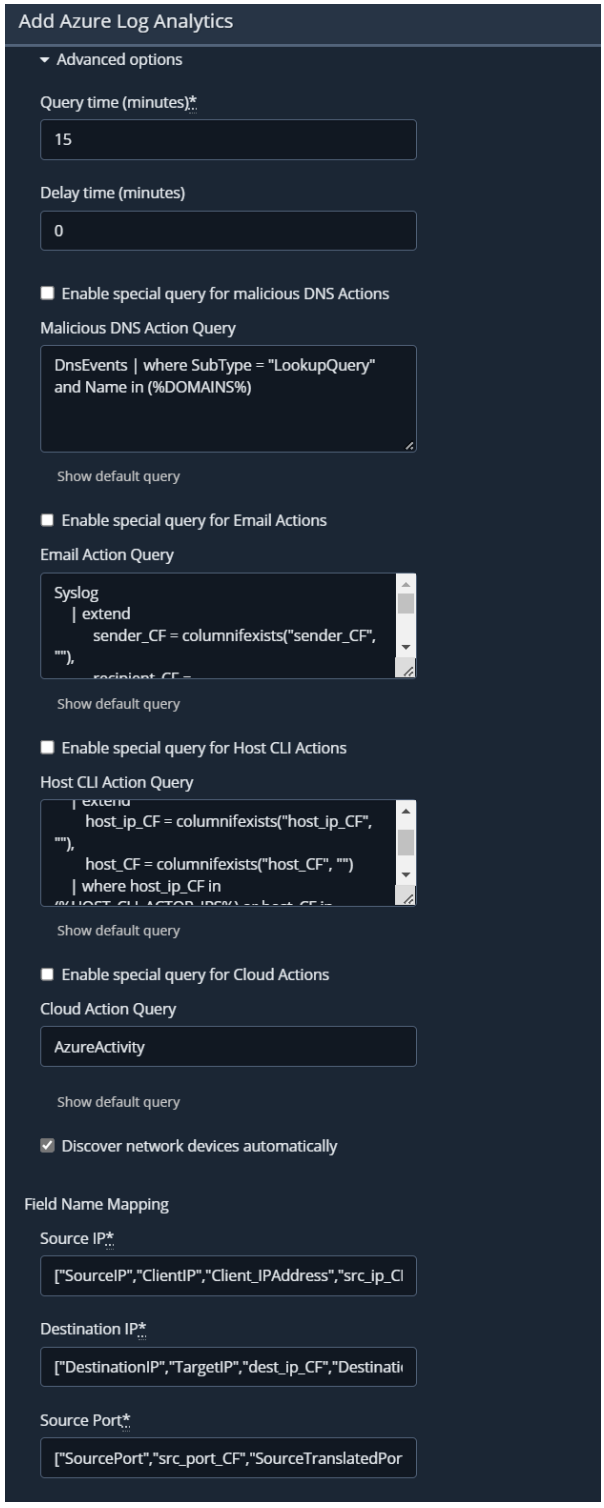
> If your monitors are set to run more frequently than the query time, this configuration impacts the pass/fail results for AEDA monitors.

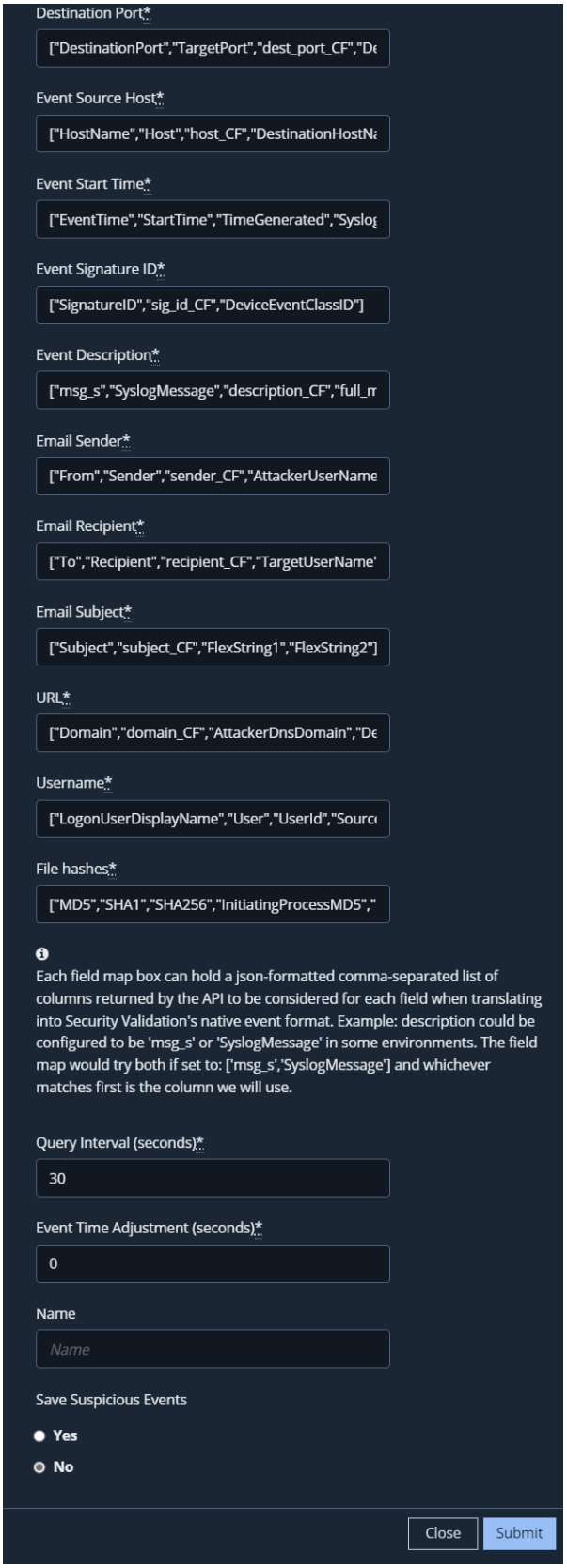
    b. (Optional) Select **Enable query for Malicious DNS Actions** and configure the **Query**. This query will only be used when you run Malicious DNS Actions or Captive DNS Actions.
    c. (Optional) Select **Enable query for Email Actions** and configure the **Query**. This query will be only be used when you run Email Actions.
    d. (Optional) Select **Enable query for Host CLI Actions** and configure the **Query**. This query will only be used when you run Host CLI Actions.
    e. If applicable, select **Enable special query for Cloud Actions** and configure the **Query**.
    f. (Optional) Select **Discover network devices automatically**.
    g. Modify **Field Name Mapping** for the following, as necessary:
        - **Source IP**
        - **Destination IP**
        - **Source Port**
        - **Destination Port**
        - **Event Source Host**
        - **Event Start Time**
        - **Event Signature ID**
        - **Event Description**
        - **Email Sender**
        - **Email Recipient**
        - **Email Subject**
        - **URL**

- **Username**
- **File hashes**

h. Modify the **Query Interval (seconds)** and **Event Time Adjustment (seconds)**, if necessary.
i. (Optional) Assign a **Name**.
j. (Optional) Choose **Yes** to **Save Suspicious Events**.

8. Click **Submit**.





Azure Log Analytics Integration - Advanced Options

Verify connectivity

TO VERIFY CONNECTIVITY TO AZURE LOG ANALYTICS

Click **Test** to verify that:

- The Director can communicate with the integration host on the port and protocol specified.
- The integration credentials are valid and working.

MICROSOFT AZURE SENTINEL

This document applies to Classic Integrations. While the Integrations solution is available, it is no longer actively maintained. Mandiant recommends that you plan a switch to Preview Integrations so you can take advantage of the latest features and functionality. Preview Integrations configuration steps are provided in the Director web interface. For more details, see the **Preview Integrations Documentation** (https://docs.mandiant.com/home/msv-preview-integrations).

If you're looking for raw event data, you should implement the **Microsoft Azure Log Analytics** (https://docs.mandiant.com/home/msv-microsoft-azure-log-analytics) integration. The integration described here, for Microsoft Azure Sentinel, addresses alerts associated with that event data.

This integration is remote-capable.

Update Microsoft Azure Sentinel

- Identify or create credentials to access Sentinel with read access, at minimum.
- Add the Microsoft Sentinel Reader role to the app that you are creating and registering.
- Verify you have access to the Log Analytics API with Data.Read permission.
- Identify the following values in the Azure Web portal:

  These values are generated when you configure Azure Log Analytics.

  - Client ID
  - Client Secret
  - Tenant ID
  - Workspace ID

- Set up Tables in Log Analytics.

  Queries in the Azure Sentinel integration will error if corresponding Tables are not configured in Log Analytics. For example, the default Malicious DNS Action Query in the integration needs the DnsEvents table in Log Analytics to be configured.

TO ACCESS THE CLIENT ID, CLIENT SECRET, TENANT ID, AND WORKSPACE ID

If you do not already know the values required to add the Azure Sentinel integration, you must locate them in the Azure portal.

- Refer to the **Microsoft documentation** (https://docs.microsoft.com/en-us/azure/active-directory-b2c/tutorial-register-applications?tabs=app-reg-ga) for further assistance identifying these values.
- If you have already noted the Client ID, Client Secret, Tenant ID, and Workspace ID for the **Microsoft Azure Log Analytics** (https://docs.mandiant.com/home/msv-microsoft-azure-log-analytics) Integration, you can reuse those values for the Azure Sentinel Integration.

1. In the Azure Log Analytics portal, take note of your **Workspace ID**.
2. In the Active Directory portal, take note of your **Tenant ID**.
3. In the Active Directory portal, navigate to **App registrations** > **New registration**.
4. Enter the required registration information.

a. Take note of the **Client ID**.
b. The required **Redirect URI** field can be set to your Director's URL.

5. Navigate to the **Certificates & Secrets** page.
6. Create a new client secret and take note of the value.

TO ADD THE DATA.READ API PERMISSION

1. In the Azure Log Analytics portal, navigate to the **API Permissions** page.
2. Add Log Analytics **Data.Read** permission.
3. Get administrator approval for the application.

API Calls

The following API calls are used by the Validation Platform.

Purpose	Call
Auth	https://login.microsoftonline.com/{tenent_id}/oauth2/token For Azure Government (GovCloud): https://login.microsoftonline.us/{tenent_id}/oauth2/token
Query Log Analytics	https://api.loganalytics.io/v1/workspaces/{workspace_id}/query For Azure Government (GovCloud): https://api.loganalytics.us/v1/workspaces/{workspace_id}/query

Update the Validation Platform

Prerequisites

Information to gather before you start:

- Identify the Client ID unique to your application.
- Identify the Client Secret unique to your application.
- Identify the Tenant ID.
- Identify the Workspace ID.

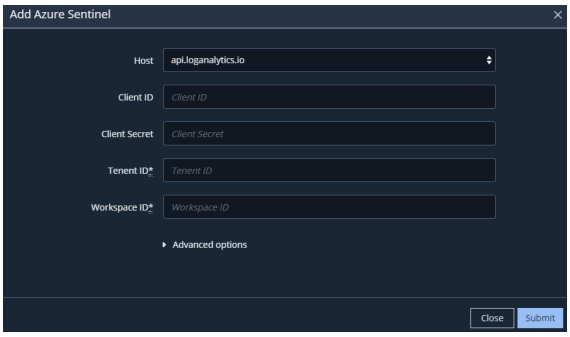
Configuration

TO ADD THE AZURE SENTINEL INTEGRATION

1. Go to **Settings** > **Integrations**.
2. Click **Add Integration** > **Azure Sentinel**.

   You can add this as either a Local or Remote Integration.

3. From the **Host** drop-down list, select the appropriate value depending on your Azure Sentinel environment:
   - The entry ending in **.io** for standard Azure environments
   - The entry ending in **.us** for Azure Government (GovCloud) environments
4. Enter **Client ID** and **Client Secret**.
5. Enter **Tenant ID** and **Workspace ID**.



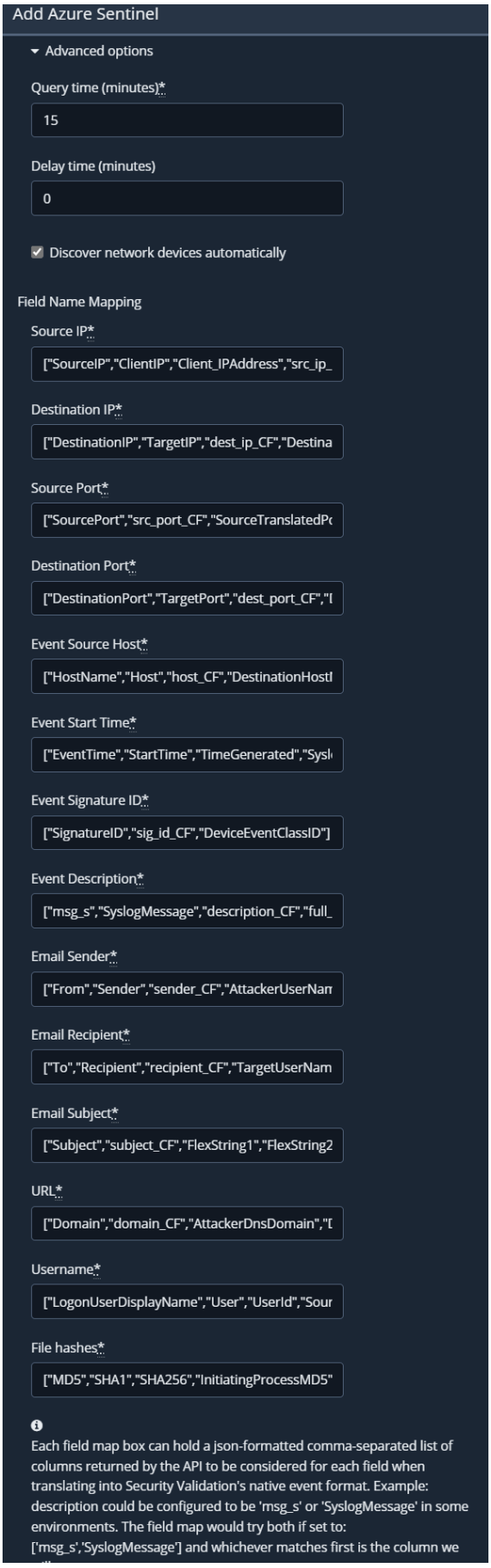
Microsoft Azure Sentinel Integration

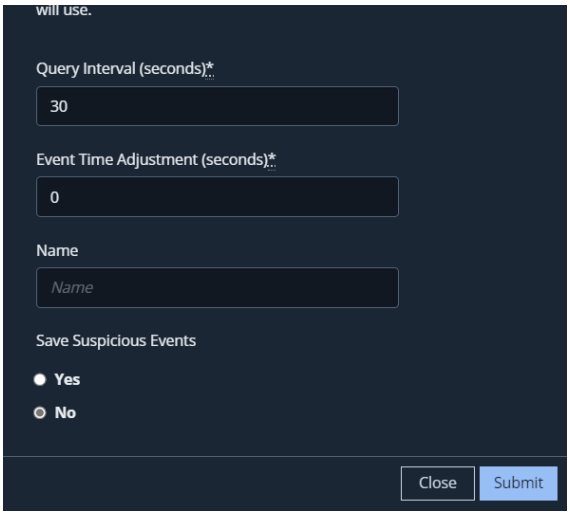
6. Expand **Advanced options** and update the information as necessary.
    a. (Optional) Update **Query time (minutes)** and **Delay time (minutes)**.

> The **Query time** is the amount of time (minutes) before and after the query runs that the platform looks for events, while the **Delay time** is the amount of time (minutes) that the platform waits to run the first query after a Job Action starts. For example, you configure your integration with the following values: **Query time** = 5, **Query interval** = 30 seconds, and **Delay time** = 0. When a Job Actions starts at 12:00:00, the first time the query runs, the platform looks for events from 11:55:00 to 12:00:00. Then 30 seconds later, it looks for events from 11:55:30 to 12:00:30. This interval continues, with the last query looking from 12:00:00 to 12:05:00. If you instead configured the **Delay time** to equal 10, it would run the same query, but it wouldn't start that query until 12:10:00.

> If your monitors are set to run more frequently than the query time, this configuration impacts the pass/fail results for AEDA monitors.

    b. (Optional) Select **Discover network devices automatically**.
    c. Modify **Field Name Mapping** for the following, as necessary:
        - **Source IP**
        - **Destination IP**
        - **Source Port**
        - **Destination Port**
        - **Event Source Host**
        - **Event Start Time**
        - **Event Signature ID**
        - **Event Description**
        - **Email Sender**
        - **Email Recipient**
        - **Email Subject**
        - **URL**
        - **Username**
        - **File hashes**
    d. Modify the **Query Interval (seconds)** and **Event Time Adjustment (seconds)**, if necessary.
    e. (Optional) Assign a **Name**.
    f. (Optional) Choose **Yes** to **Save Suspicious Events**.
7. Click **Submit**.





Microsoft Azure Sentinel Integration - Advanced Options

Verify connectivity

TO VERIFY CONNECTIVITY TO MICROSOFT AZURE SENTINEL

Click **Test** to verify that:

- The Director can communicate with the integration host on the port and protocol specified.
- The integration credentials are valid and working.

RSA NETWITNESS RESPOND

> This document applies to Classic Integrations. While the Integrations solution is available, it is no longer actively maintained. Mandiant recommends that you plan a switch to Preview Integrations so you can take advantage of the latest features and functionality. Preview Integrations configuration steps are provided in the Director web interface. For more details, see the **Preview Integrations Documentation (https://docs.mandiant.com/home/msv-preview-integrations)**.

Update RSA NetWitness Respond

Identify or create credentials to access NetWitness Respond with read access, at minimum.

API Calls

The following API calls are used by Validation Platform.

Purpose	Call
Generate auth token	/rest/api/auth/userpass
Get incident information	/rest/api/incidents
Get alerts for each incident	/rest/api/incidents/{incident_id}/alerts

Update the Security Validation Platform

Prerequisites

Information to gather before you start:

- Identify the host, port, and protocol associated with your NetWitness Respond server
- Identify your NetWitness Respond username and password

Configuration

TO ADD THE RSA NETWITNESS RESPOND INTEGRATION

1. Go to **Settings** > **Integrations**.
2. Click **Add Integration** > **RSA NetWitness Respond**.
3. Enter information for the **Host**, **Port**, **Protocol**, **Username** and **Password** or **API Token**.
4. Expand **Advanced options**.
5. (Optional) Update **Query time** and **Delay time**.

> The **Query time** is the amount of time (minutes) before and after the query runs that the platform looks for events, while the **Delay time** is the amount of time (minutes) that the platform waits to run the first query after a Job Action starts. For example, you configure your integration with the following values: **Query time** = 5, **Query interval** = 30 seconds, and **Delay time** = 0. When a Job Actions starts at 12:00:00, the first time the query runs, the platform looks for events from 11:55:00 to 12:00:00. Then 30 seconds later, it looks for events from 11:55:30 to 12:00:30. This interval continues, with the last query looking from 12:00:00 to 12:05:00. If you instead configured the **Delay time** to equal 10, it would run the same query, but it wouldn't start that query until 12:10:00.

> If your monitors are set to run more frequently than the query time, this configuration impacts the pass/fail results for AEDA monitors.

6. Modify the **Query Interval** and **Event Time Adjustment**, if necessary.
7. (Optional) Assign a **Name**.
8. (Optional) Choose **Yes** to save suspicious events.
9. Click **Submit**.

(https://d383cql5uq169w.cloudfront.net/app/image/pid/620d7e13ccb103e8557b25b0/id/629a12edc9cba0017c2f7eb3/n/rsa-netwitness-respond.png)

RSA NetWitness Respond

Verify connectivity

TO VERIFY CONNECTIVITY TO RSA NETWITNESS RESPOND

Click **Test** to verify that:

- The Director can communicate with the integration host on the port and protocol specified.
- The integration credentials are valid and working.

SECURONIX SNYPR

> This document applies to Classic Integrations. While the Integrations solution is available, it is no longer actively maintained. Mandiant recommends that you plan a switch to Preview Integrations so you can take advantage of the latest features and functionality. Preview Integrations configuration steps are provided in the Director web interface. For more details, see the **Preview Integrations Documentation (https://docs.mandiant.com/home/msv-preview-integrations)**.

This integration is remote capable.

Update Securonix SNYPR

Identify or create credentials to access Securonix with read access, at minimum.

API Calls

The following API calls are used by the Validation Platform.

Purpose	Call
/Snypr/ws/token/generate	Get API access token for all calls
/Snypr/ws/spotter/index/search?query=(query)...	Timeboxed Query for getting events from Securonix

Update the Security Validation Platform

Prerequisites

Information to gather before you start:

- Identify the hostname used to access Securonix SNYPR
- Identify the port used for Securonix communication
- Identify the username and password for your Securonix account

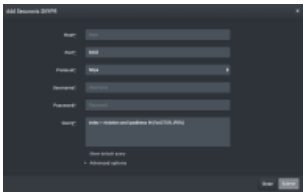
Configuration

You can add this as either a Local or Remote Integration.

TO ADD THE SECURONIX SNYPR INTEGRATION

1. Go to **Settings** > **Integrations**.
2. Click **Add Integration** > **Securonix SNYPR**.
3. Enter information for the **Host**, **Port**, **Protocol**, **Username** and **Password** or **API Token**.
4. Review and update the Query as needed.

   The %ACTOR_IPS% variable can be used in all queries. This improves event matching.



(https://d383cql5uq169w.cloudfront.net/app/image/pid/620d7e13ccb103e8557b25b0/id/629a12ddc9cba0017c2f7e1d/n/securonisnypr.png)

Securonix SNYPER Integration

5. Expand **Advanced options**.
6. (Optional) Update **Query time**, if necessary.
7. (Optional) Update the **Page size**, if necesary.
8. (Optional) Enable **Verify SSL**, if necessary.
9. (Optional) Select **Enable query for Malicious DNS Actions** and configure the **Query**. This query will only be used when you run Malicious DNS Actions or Captive DNS Actions.
10. (Optional) Select **Enable query for Email Actions** and configure the **Query**. This query will only be used when you run Email Actions.
11. (Optional) Select **Enable query for Host CLI Actions** and configure the **Query**. This query will only be used when you run Host CLI Actions.

    If you enable the Host CLI Actions query and use the %HOST_CLI_ACTOR_HOSTNAMES% variable, the platform will substitute the plain hostname and the information from the Alternate Hostname field on the Actor configuration page.

12. Identify the field name mappings for the following (there could be multiple of each, depending on log sources and configuration):
    - Source IP
    - Destination IP
    - Source Port
    - Destination
    - Port
    - Event Source Host
    - Host
    - Event Start Time (timestamp)
    - Event Unique ID
    - Event Signature ID
    - Event Description
    - Email Sender
    - Email Recipient
    - Email Subject
    - URL
    - Username
13. Modify the **Query Interval** and **Event Time Adjustment**, if necessary.
14. (Optional) Update **Query time** and **Delay time**.

    The **Query time** is the amount of time (minutes) before and after the query runs that the platform looks for events, while the **Delay time** is the amount of time (minutes) that the platform waits to run the first query after a Job Action starts. For example, you configure your integration with the following values: **Query time** = 5, **Query interval** = 30 seconds, and **Delay time** = 0. When a Job Actions starts at 12:00:00, the first time the query runs, the platform looks for events from 11:55:00 to 12:00:00. Then 30 seconds later, it looks for events from 11:55:30 to 12:00:30. This interval continues, with the last query looking from 12:00:00 to 12:05:00. If you instead configured the **Delay time** to equal 10, it would run the same query, but it wouldn't start that query until 12:10:00.

    If your monitors are set to run more frequently than the query time, this configuration impacts the pass/fail results for AEDA monitors.

15. (Optional) Assign a **Name**.
16. (Optional) Choose **Yes** to save suspicious events.
17. Click **Submit**.

Securonix SNYPER Integration - advanced options

Verify connectivity

TO VERIFY CONNECTIVITY TO SECURONIX SNYPR

Click **Test** to verify that:

- The Director can communicate with the integration host on the port and protocol specified.
- The integration credentials are valid and working.

SPLUNK

> This document applies to Classic Integrations. While the Integrations solution is available, it is no longer actively maintained. Mandiant recommends that you plan a switch to Preview Integrations so you can take advantage of the latest features and functionality. Preview Integrations configuration steps are provided in the Director web interface. For more details, see the **Preview Integrations Documentation (https://docs.mandiant.com/home/msv-preview-integrations)**.

This document describes the steps required to integrate Splunk with the Mandiant Security Validation (MSV) Platform.

This integration is remote capable.

API Calls

The following API calls are used when integrating with MSV Platform.

Purpose	Call
Login	/services/auth/login
Search	/services/search/jobs/export  This API uses exec_mode set to blocking to run the query.

Prerequisites

Information to gather before you start:

1. IP address used to access Splunk.
2. Port for Splunk communications (default is 8089).
3. Identify whether the protocol is HTTP or HTTPS for connections to the Splunk port.
4. Identify or create credentials to access Splunk. Read permissions are required.
5. Identify the field name mappings for the following:
    a. Source IP
    b. Destination IP
    c. Source Port
    d. Destination Port
    e. Event Signature ID
    f. Event Name
    g. Event Source Host

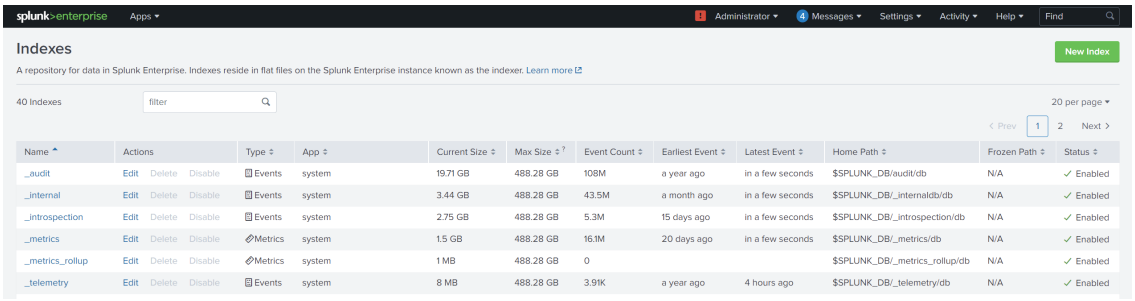
     There could be multiple field names, depending on log sources and configurations.

6. Verify that the Splunk account has the following capabilities enabled:
    - accelerate_search
    - edit_search_schedule_window
    - export_results_is_visible
    - get_metadata
    - get_typeahead
    - list_accelerate_search

- list_inputs
- list_metrics_catalog
- pattern_detect
- request_remote_tok
- rest_apps_view
- rest_properties_get
- rest_properties_set
- run_collect
- run_mcollect
- schedule_rtsearch
- search
- User is set to the GMT/UTC timezone

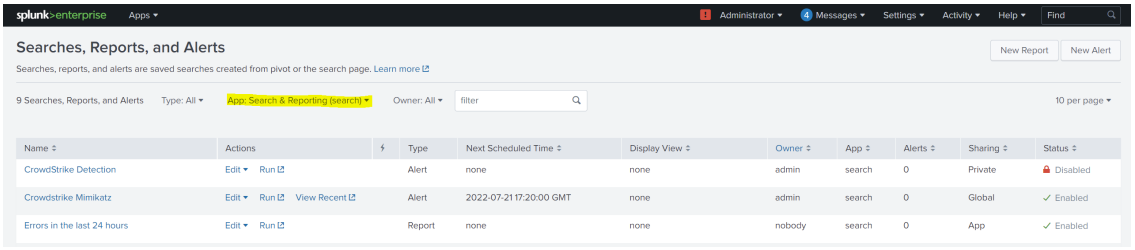
Create Alert conditions within Splunk

1. Create an index to store the alert. **Settings > Indexes > New Index**. Fill in the name of the index.



Splunk Indexes

2. Create an alert by going to: **Settings > Searches, Reports, and Alerts**. Do this step in the **Search & Reporting (search) app**. Select **New Alert**.



Splunk Searches, Reports, and Alerts

3. On the **New Alert** page, enter the following:

> Creating a Crowdstrike alert for demo purposes which is triggered whenever Splunk sees the `event.FileName=mimikatz.exe` and `action=blocked`

   a. **Name**: `Crowdstrike Mimikatz`
   b. **Search**: `index="crowdstrike" AND action="blocked" AND "event.FileName"="mimikatz.exe"`
   c. **Alert Type**: Scheduled

> This step sets up the alert search to run every `15min`

      i. **Run on Cron Schedule**

d. **Time Range**: `Last 15 minutes`

> This setting should match your Cron schedule to avoid duplicating alerts.

e. **Cron Expression**: `*/15 * * * *`
f. **Expires**: `24 Hours` (default)
g. **Trigger Conditions**:
    i. **Trigger alert when**: Number of Results is greater than 0

    > Whenever it's detected, an alert is triggered.

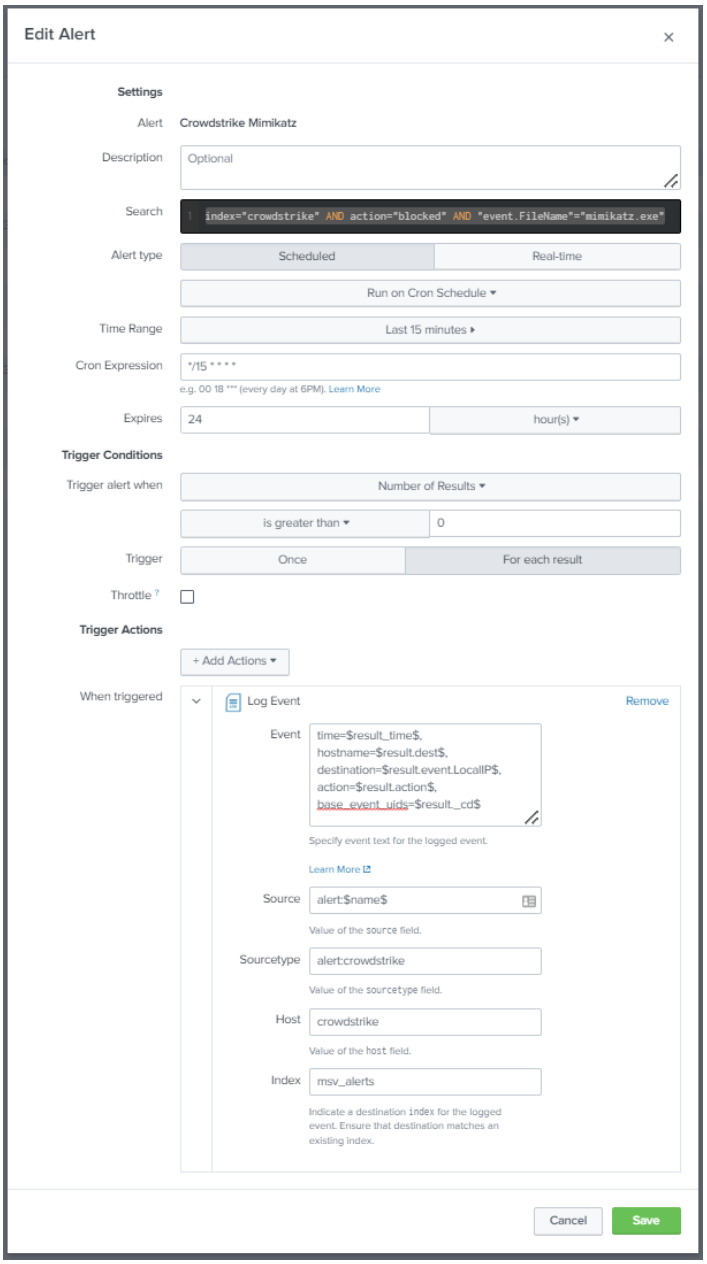
    ii. **Trigger**: For each Result
    iii. **Throttle**: Unchecked

h. **Trigger Actions**:
    i. **When triggered**: Log Event
    ii. **Event**: Do not hesitate to add other fields if necessary, but it is the basic information that is required. In particular, the `base_event_uids=$result._cd$` that will link to the base event for MSV to match it.

```
time=$result_time$,
hostname=$result.dest$,
destination=$result.event.LocalIP$,
action=$result.action$,
base_event_uids=$result._cd$
```

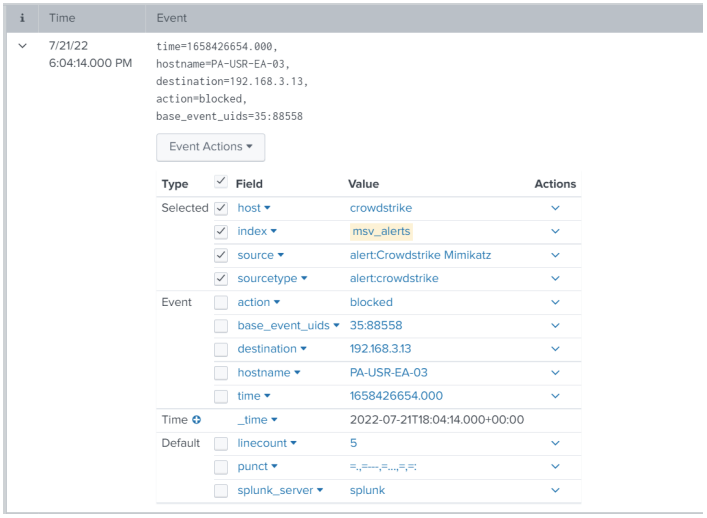
        - `$result.[field from source event]$` are the fields to match.

    iii. **Source**: `alert:$name$` The name of the event in the alert index
    iv. **Sourcetype**: `alert:crowdstrike` The source type of the event in the alert index
    v. **Host**: `crowdstrike` The name of the Host in the alert index
    vi. **Index**: `msv_alerts` The name of the index that was created in **Step 1**.



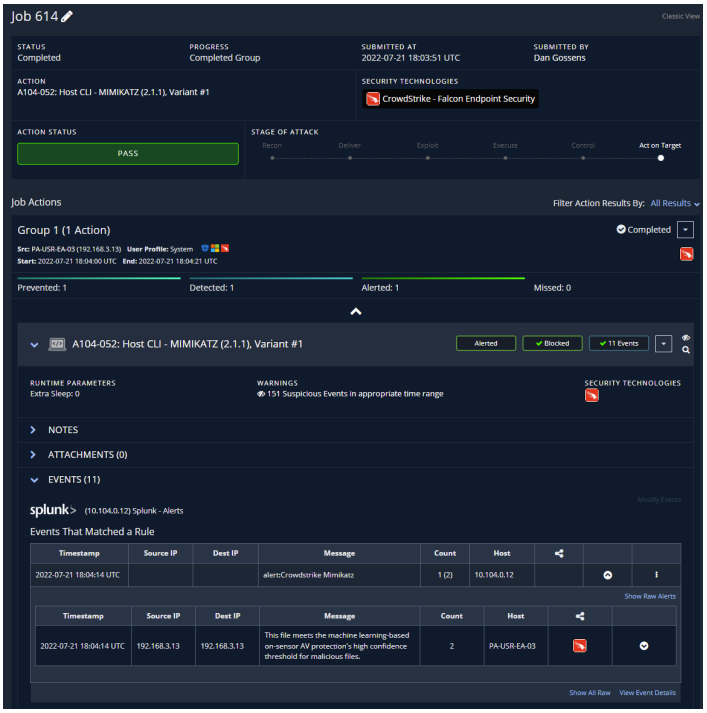
Splunk Edit Alert

For corresponding MSV setup, refer to the **enabling Correlation Query** section. The following is an example of an alert that has been triggered:



Splunk Triggered Alert

The Action which triggered this alert:



Action for the Alert

Add the Splunk Integration

The `%ACTOR_IPS%` variable can be used in all queries. This variable improves event matching.

1. Go to **Settings** > **Integrations**.
2. Click **Add Integration** > **Splunk**.
3. Enter information for the **Host**, **Port**, **Protocol**, **Username,** and **Password** or **API Token**.
4. Set the **Authentication Method** (defaults to Token with Bearer Token, Basic, and Token+Cookie as additional options).

a. The Token method authenticates by logging in and creating a session token, not by using a token that you provide to the Security Validation Platform.
b. The Bearer Token method authenticates over HTTP without requiring the Username and Password values. Bearer tokens are permanent unless they are revoked or given an expiry time by a Splunk system administrator.
c. Basic Authentication Use Case: Your Splunk instance is behind a proxy and there's the possibility of requests hitting different search heads; if you were using token authentication, the token created by logging into one search head would not work for requests on another search head.

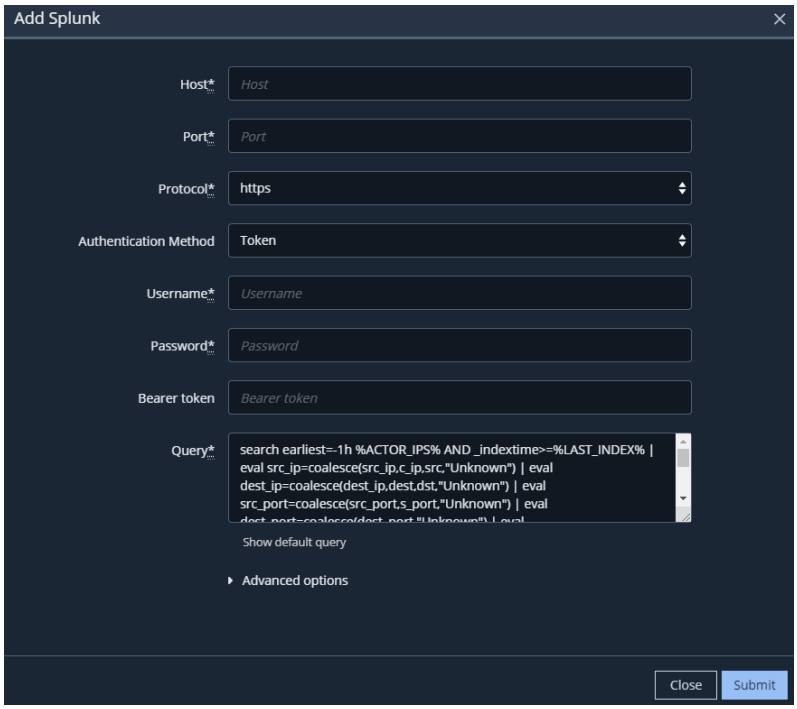
If you are using a load balancer, try using Token+Cookie for the authentication type. Otherwise, verify that the credentials are correct.

5. Review and update the **Query** to include instance-specific field names, sources, data types, and other customizations.
This Integration supports the following variables inside queries:

Variable	Description
%ACTOR_IPS%	IP addresses of Actors used to run an Action.
%DOMAINS%	Domain names queried in recent DNS Actions.
%SENDERS%	Email addresses and user names of senders in recent email Actions.
%RECIPIENTS%	Email addresses and user names of recipients of recent email Actions.
%HOST_CLI_ACTOR_IPS%	IP addresses of Actors that recently ran a Host CLI Action.
%HOST_CLI_ACTOR_HOSTNAMES%	Hostname of Actors that recently ran a Host CLI Action.
%LAST_INDEX%	The start time for the query window.

The default queries can be viewed by clicking **Show default query.**

The query includes information that allows event matching based on any file hashes included in an Action.



Splunk Integration

6. Expand **Advanced options**.
7. (Optional) Update **Query time (minutes)** and **Delay time (minutes)**.

   The **Query time** is the amount of time (minutes) before and after the query runs that the platform looks for events, while the **Delay time** is the amount of time (minutes) that the platform waits to run the first query after a Job Action starts. For example, you configure your integration with the following values: **Query time** = 5, **Query interval** = 30 seconds, and **Delay time** = 0. When a Job Actions starts at 12:00:00, the first time the query runs, the platform looks for events from 11:55:00 to 12:00:00. Then 30 seconds later, it looks for events from 11:55:30 to 12:00:30. This interval continues, with the last query looking from 12:00:00 to 12:05:00. If you instead configured the **Delay time** to equal 10, it would run the same query, but it wouldn't start that query until 12:10:00.

   If your monitors are set to run more frequently than the query time, this configuration impacts the pass/fail results for AEDA monitors.

8. (Optional) Select **Enable query for Malicious DNS Actions** and configure the **Query**. This query will only be used when you run Malicious DNS Actions or Captive DNS Actions.
9. (Optional) Select **Enable query for Email Actions** and configure the **Query**. This query will only be used when you run Email Actions.
10. (Optional) Select **Enable query for Host CLI Actions** and configure the **Query**. This query will only be used when you run Host CLI Actions.

    If you enable the Host CLI Actions query and use the `%HOST_CLI_ACTOR_HOSTNAMES%` variable, the platform substitutes the plain hostname and the information from the Alternate Hostname field on the Actor configuration page.

11. (Optional) Select **Pre-Process Event Correlation**.

12. (Optional) Select **Enable correlation query** and fill in the pertinent information from the alert that was created in Splunk to set up MSV to search for the Splunk alerts.

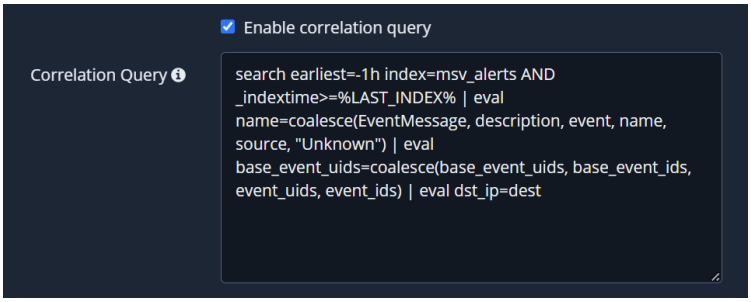
    Correlation queries let the Security Validation Platform recognize Splunk summary indexes as alerts in Job Action results. To build and use a Correlation Query on the platform, you must have a summary index. Correlation alerts populate this summary index. Use the name of the index in the integration's Correlation Query.

    In the index, each row must contain a property for base event UIDs. The property should be an array of _cd values from the base events to which the alert is correlating.
    _cd is an internal property to Splunk and does not show up by default, but it does exist by default in every index row. If your base_event_uids are stored as a string separated by commas, you can split your query by adding ' `| eval base_event_uids = split(base_event_uids, ",")` ' to the end of it. See the **Splunk documentation (https://docs.splunk.com/Documentation/Splunk/8.1.0/Knowledge/Setupsummaryindexes)** for information on creating summary indexes.

    - In the Correlation Query, replace CHANGE_ME_CORRELATION_INDEX with the name of your populated index in Splunk.

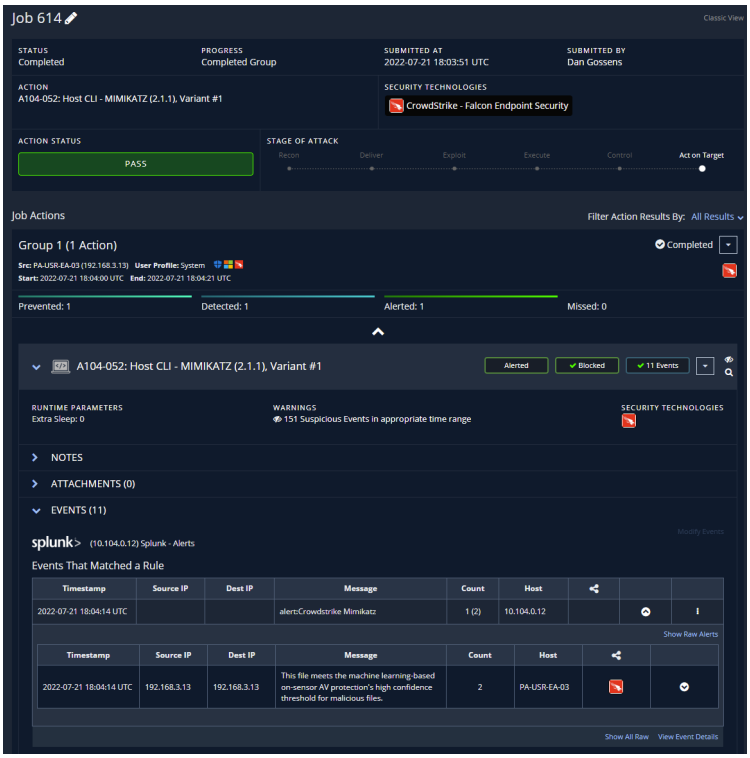
      See **Correlated Events (https://docs.mandiant.com/home/correlated-events)** for information about how the Security Validation Platform matches correlated events to a Job Action.

      For further assistance configuring the Correlation Query to work with a summary index, contact **Support (https://www.mandiant.com/support) (https://mandiant.com/support)**.

      Correlation Query

    - After the 15-minute runtime, you see that the alert correlated to the original Action run.



Correlated Action

13. (Optional) For **Timeout for Query Requests (seconds)**, enter how much time to allow before the query times out. This timeout applies to all queries that you configure for this integration.
14. (Optional) Select **Discover network devices automatically**.
15. Modify the **Query Interval (seconds)** and **Event Time Adjustment (seconds)**, if necessary.
16. (Optional) Assign a **Name**.
17. (Optional) Choose **Yes** to save suspicious events.
18. Click **Submit**.

Splunk Integration - Advanced Options

Verify Connectivity to Splunk

Click **Test** to verify that:

- The Director can communicate with Splunk on the port and protocol specified.
- The user credentials are working.

If there is an issue when running the test, a message identifies the specific cause of the error, helping to identify the settings you need to review.

Run a Malicious or Captive DNS Action and then review the last run query to verify:

- The custom DNS query works as expected (if configured).

Troubleshooting Jobs

If events are missing when running Jobs, check the integration's last query. It contains the specific query and errors that occurred when the query was run. In addition, it can provide status information when events for a Job are being processed.

SPLUNK ENTERPRISE SECURITY

> This document applies to Classic Integrations. While the Integrations solution is available, it is no longer actively maintained. Mandiant recommends that you plan a switch to Preview Integrations so you can take advantage of the latest features and functionality. Preview Integrations configuration steps are provided in the Director web interface. For more details, see the **Preview Integrations Documentation (https://docs.mandiant.com/home/msv-preview-integrations)**.

This integration is remote capable.

API Calls

The following API calls are used by the Validation Platform.

Purpose	Call
Login	`/services/auth/login`
Search	`/services/search/jobs/export`  This API uses exec_mode set to blocking to run the query.
Search for notables	Step 1: `/services/search/jobs/export using `| rest /services/saved/searches | where `` Step 2: After getting the list of notable events, we hit the following two for each notable that matched our query: • Retrieve parser for the notable query ◦ `/services/search/parser` • Use parsed notable to search for base events with the Search API call.

Update the Validation Platform

Prerequisites

Information to gather before you start:

1. IP address used to access Splunk.
2. Port for Splunk communications (default is 8089).
3. Identify whether the protocol is HTTP or HTTPS for connections to the Splunk port.
4. Identify or create credentials to access Splunk. Read permissions are required.
5. Identify the field name mappings for the following:
    a. Source IP
    b. Destination IP
    c. Source Port
    d. Destination Port
    e. Event Signature ID

f. Event Name
g. Event Source Host

There could be multiple field names, depending on log sources and configurations.

6. Verify that the Splunk account has the following capabilities enabled:
   - accelerate_search
   - edit_search_schedule_window
   - export_results_is_visible
   - get_metadata
   - get_typeahead
   - list_accelerate_search
   - list_inputs
   - list_metrics_catalog
   - pattern_detect
   - request_remote_tok
   - rest_apps_view
   - rest_properties_get
   - rest_properties_set
   - run_collect
   - run_mcollect
   - schedule_rtsearch
   - search
   - User is set to the GMT/UTC timezone

Configuration

TO ADD THE SPLUNK ES INTEGRATION

The %ACTOR_IPS% variable can be used in all queries. This variable improves event matching.

1. Go to **Settings** > **Integrations**.
2. Click **Add Integration** > **Splunk ES**.
3. Enter information for the **Host**, **Port**, **Protocol**, **Username,** and **Password** or **API Token**.
4. Set the **Authentication Method** (defaults to Token with Bearer Token, Basic, and Token+Cookie as additional options).
   a. The Token method authenticates by logging in and creating a session token, not by using a token that you provide to the Validation Platform.
   b. The Bearer Token method authenticates over HTTP without requiring the Username and Password values. Bearer tokens are permanent unless they are revoked or given an expiry time by a Splunk system administrator.
   c. Basic Authentication Use Case: Your Splunk instance is behind a proxy and there's the possibility of requests hitting different search heads; if you were using token authentication, the token created by logging into one search head would not work for requests on another search head.

If you are using a load balancer, try using Token+Cookie for the authentication type. Otherwise, verify that the credentials are correct.

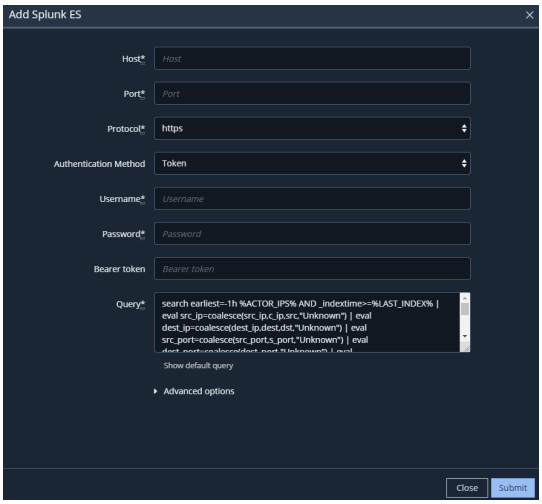
5. Review and update the **Query** to include instance-specific field names, sources, data types, and other customization.

   This Integration supports the following variables inside queries:

Variable	Description
%ACTOR_IPS%	IP addresses of Actors used to run an Action.
%DOMAINS%	Domain names queried in recent DNS Actions.
%SENDERS%	Email addresses and user names of senders in recent email Actions.
%RECIPIENTS%	Email addresses and user names of recipients of recent email Actions.
%HOST_CLI_ACTOR_IPS%	IP addresses of Actors that recently ran a Host CLI Action.
%HOST_CLI_ACTOR_HOSTNAMES%	Hostname of Actors that recently ran a Host CLI Action.
%LAST_INDEX%	The start time for the query window.

The default queries can be viewed by clicking **Show default query**.

The query includes information that allows event matching based on any file hashes included in an Action.



Splunk ES Integration

6. Expand **Advanced options**.
7. (Optional) Update **Query time (minutes)** and **Delay time (minutes)**.

The **Query time** is the amount of time (minutes) before and after the query runs that the platform looks for events, while the **Delay time** is the amount of time (minutes) that the platform waits to run the first query after a Job Action starts. For example, you configure your integration with the following values: **Query time** = 5, **Query interval** = 30 seconds, and **Delay time** = 0. When a Job Actions starts at 12:00:00, the first time the query runs, the platform looks for events from 11:55:00 to 12:00:00. Then 30 seconds later, it looks for events from 11:55:30 to 12:00:30. This interval continues, with the last query looking from 12:00:00 to 12:05:00. If you instead configured the **Delay time** to equal 10, it would run the same query, but it wouldn't start that query until 12:10:00.

If your monitors are set to run more frequently than the query time, this configuration impacts the pass/fail results for AEDA monitors.

8. (Optional) Enter the **App Namespace** to use for requests for this Splunk integration.
9. Update **Correlation Query** as necessary.

   - Depending on your Splunk ES environment, some searches for base events require additional manipulation to correctly match against Security Validation Actions. You can add **search replacement** strings that rewrite parts of the Correlation Query when searching for a notable event's base event or events.
   - %HOST_CLI_ACTOR_IPS% and %HOST_CLI_ACTOR_HOSTNAMES%, which correspond to any Actor IP addresses or hostnames that were recently used to run Host CLI Actions, can be used in this query. If no Actors were included, the variables in the query are replaced with an empty set of parentheses. This substitution is necessary to prevent errors when the query runs.
   - See **Correlated Events (https://docs.mandiant.com/home/correlated-events)** for information about how the Validation Platform matches correlated events to a Job Action.

10. (Optional) Select **Pre-Process Event Correlation**.
11. (Optional) Select **Auto-generate tstats drilldown searches** .

    When base events and their corresponding notable events come from correlation searches that use the tstats command, a programmatic drilldown search is needed for the Validation Platform to identify them. If the Auto-generate tstats drilldown searches option is enabled, values from notable events are automatically added to a new search that finds the correct base events. When base events are identified, the corresponding notable event is correlated to a Job.

12. (Optional) Select **Add additional filters to tstats to improve performance** .
13. (Optional) Enter rules in **Include subsearches in tstats drilldown for these rules (comma separated)** . This field lets you tell the platform which rules should also be applied to the tstats drilldown (by default, subsearches are only applied to the base search).

    Example: `RULE_123,RULE_456`
14. (Optional) Enter rules in **Add actor info to base event searches for these notable rules only (comma separated)**. This field lets you define which notable base event queries should be modified to add known actor info before running.
15. (Optional) Select **Add actor info to all base event searches** . When selected, this option will override the previous field and modify all notable base event queries to add known actor info before running.
16. (Optional) Select **Enable query for Malicious DNS Actions** and configure the **Query**. This query will only be used when you run Malicious DNS Actions or Captive DNS Actions.
17. (Optional) Select **Enable query for Email Actions** and configure the **Query**. This query will only be used when you run Email Actions.
18. (Optional) Select **Enable query for Host CLI Actions** and configure the **Query**. This query will only be used when you run Host CLI Actions.

    If you enable the Host CLI Actions query and use the %HOST_CLI_ACTOR_HOSTNAMES% variable, the platform will substitute the plain hostname and the information from the Alternate Hostname field on the Actor configuration page.

19. (Optional) For **Timeout for Query Requests (seconds)**, enter how much time to allow before the query times out. This timeout applies to all queries that you configure for this integration.
20. (Optional) Add **Search replacements** for the Correlation Query.

    The Validation Platform uses Splunk ES base events to accurately match Actions against notable events in Splunk ES. If base events cannot be identified, notable events will not be correlated to Security Validation Actions. Search replacements are applied to base event searches to prevent failed searches and misidentification of notable events.

    a. Under **Regex**, enter a Ruby-compatible regular expression (regex) that matches notable event fields from the Correlation Query. As an example, your Correlation Query might search for the following source and

destination IP addresses in notable events:
`search src=10.10.0.* dest=10.10.0.*`

A matching regex pattern search would be:
`search (src=[\d.*]+ dest=[\d.*]+)`

b. Under **Replacement**, refer to the captured groups in your regex and add any notable event fields that will help identify base events. Use `\` to refer to the captured groups in your regex, starting at `\1` for the first captured group. Use `%{field_name}` to list notable event fields that you want to be searched. The field name used inside the brackets will automatically return the value identified in the event search. Field names used must exactly match the field name used in notable events. You might use a unique field name shared between your Splunk ES notable events and their corresponding base event. For example, if you know that your Splunk ES notable events share the unique field name "signature" with their corresponding base event, you could include it in your replacement. Using the regex pattern and field name "signature" would look like:
`search \1 signature="%{signature}"`

After entering the regex pattern and replacement pair, the modified search in Splunk ES would be:
`search src=10.10.0.* dest=10.10.0.* signature="Example event"`

Regex	Replacement
search (src=[\d.*]+ dest=[\d.*]+)	search \1 signature="%{signature}"

(https://d383cql5uq169w.cloudfront.net/app/image/pid/620d7e13ccb103e8557b25b0/id/629a12e1c9cba0017c2f7e42/n/splu
es-search-replacement.png)

An example search replacement

21. (Optional) Select **Discover network devices automatically**.
22. Modify the **Query Interval (seconds)** and **Event Time Adjustment (seconds)**, if necessary.
23. (Optional) Assign a **Name**.
24. (Optional) Choose **Yes** to save suspicious events.
25. Click **Submit**.

Splunk ES Integration - Advanced Options

SAML is not supported.

Verify connectivity

TO VERIFY CONNECTIVITY TO SPLUNK ES

Click **Test** to verify that:

- The Director can communicate with Splunk on the port and protocol specified.
- The User credentials are working.

If there is an issue running the test, a message identifies the specific cause of the error, helping pinpoint the settings you need to review.

Run a Malicious or Captive DNS Action and then review the last run query to verify:

- The custom DNS query works as expected (if configured).

Troubleshooting Jobs

If events are missing when running Jobs, check the integration's last query. It contains the specific query and errors that occurred when the query was run. In addition, it can provide status information when events for a Job are being processed.

VIEWING INDEX DATA FOR SPLUNK EVENTS

If you are tuning Splunk and want to verify events are going into the expected index, you can get this information from the Validation Platform using the Director or the API.

Configure Splunk

To capture the index information for events coming from Splunk, you must add **index** to the list of fields in your Splunk queries. Otherwise it won't be present in the events the Validation Platform receives.

Viewing the Index Information in the Director

TO VIEW INDEX DATA FOR SPLUNK EVENTS

1. Open the Job that has Splunk Events you want to review.
2. Click the Events cell to bring up the detected event for the Action.
3. Click **View Event Details**. This displays the a table listing all the Events.
4. Expand one or expand all Events by clicking **Show All**. The index will be listed in the untranslated field in the table.

Viewing the Index Information using the API

To view the integration event data for one Action in a Job, use the following call:

```
GET /integration_events?filter[job_action_id]=1&filter[integration_id]=2
```

To view the integration event data for multiple Actions in a Job, use the following call:

```
GET /integration_events?filter[job_action_id]=1,2,3,4,5&limit=500
```

From those results, you could use the following python request to parse out the index information.

```
# Get events for JobActions 1-5 from Integration 2:
params = {'filter[job_action_id]': '1,2,3,4,5',
'filter[integration_id]': 2,
}
resp = requests.get('https:///integration_events.json',
auth=(, ),
verify=False,
params=params)
for event in resp.json():
print("index:", event['untranslated']['index'], "\tevent:", event['description'])
```

SUMO LOGIC

This document applies to Classic Integrations. While the Integrations solution is available, it is no longer actively maintained. Mandiant recommends that you plan a switch to Preview Integrations so you can take advantage of the latest features and functionality. Preview Integrations configuration steps are provided in the Director web interface. For more details, see the **Preview Integrations Documentation (https://docs.mandiant.com/home/msv-preview-integrations)**.

This integration is remote capable.

Update Sumo Logic

TO UPDATE SUMO LOGIC

1. Generate a Sumo Logic API Access ID/Key pairing specifically for the Validation Platform's use. Refer to the **Sumo Logic Documentation (https://help.sumologic.com/Manage/Security/Access-Keys)** for instructions.

   Sumo Logic may not recognize the `validation.cloud` FQDN extension. When you configure your API Access ID/Key in Sumo Logic's admin console, you do not need to specify the domain.

2. Create a Sumo Logic account with sufficient permissions. Read permissions are required, at minimum.
3. (Optional) Create a custom field for the event_time field Security Validation uses. The default time in Sumo Logic may be incorrect because it is based on ingest time, not detect time. If you are concerned about this, you can create a new field, such as timestamp, to capture the required info. An example of this is shown in the code below. For additional details, see Sumo Logic's documentation on formatDate.

```
| formatDate(toLong(timestamp*1000),"MM-dd-yyyy'T'HH:mm:ss'Z'") as event_time
```

Update the Validation Platform

Prerequisites

Information to gather before you start:

1. Identify the Sumo Logic host used to access the Sumo Logic cloud. The host is visible in the URL after logging in to the Sumo Logic web user interface.
2. API Access ID/Key.
3. Sumo Logic credentials.
4. Identify the field name mappings for the following (there could be multiple of each, depending on log sources and configuration):
   a. Source IP
   b. Destination IP
   c. Source Port
   d. Destination Port
   e. Event Signature ID
   f. Event Name
   g. Event Source Host
   h. Event Time

Configuration

TO ADD THE SUMO LOGIC INTEGRATION

1. Go to **Settings** > **Integrations**.

2. Click **Add Integration** > **Sumo Logic**.
3. Select the Host.
3. Enter the **API Access ID** and **Key**.
4. Review and update the **Query** to include instance-specific field names.

   The default queries can be viewed by clicking **Show default query**.

5. Expand **Advanced options**.
6. (Optional) Update **Query time** and **Delay time**.

   The **Query time** is the amount of time (minutes) before and after the query runs that the platform looks for events, while the **Delay time** is the amount of time (minutes) that the platform waits to run the first query after a Job Action starts. For example, you configure your integration with the following values: **Query time** = 5, **Query interval** = 30 seconds, and **Delay time** = 0. When a Job Actions starts at 12:00:00, the first time the query runs, the platform looks for events from 11:55:00 to 12:00:00. Then 30 seconds later, it looks for events from 11:55:30 to 12:00:30. This interval continues, with the last query looking from 12:00:00 to 12:05:00. If you instead configured the **Delay time** to equal 10, it would run the same query, but it wouldn't start that query until 12:10:00.

   If your monitors are set to run more frequently than the query time, this configuration impacts the pass/fail results for AEDA monitors.

7. (Optional) Select **Enable query for Host CLI Actions** and configure the **Query**. This query will only be used when you run Host CLI Actions.

   If you enable the Host CLI Actions query and use the %HOST_CLI_ACTOR_HOSTNAMES% variable, the platform will substitute the plain hostname and the information from the Alternate Hostname field on the Actor configuration page.

8. (Optional) Select **Discover network devices automatically**.
9. Modify the **Query Interval** and **Event Time Adjustment**, if necessary.
10. (Optional) Assign a **Name**.
11. (Optional) Choose **Yes** to save suspicious events.
12. Click **Submit**.

(https://d383cql5uq169w.cloudfront.net/app/image/pid/620d7e13ccb103e8557b25b0/id/629a12dbc9cba0017c2f7e05/n/sumo.png)

Sumo Logic Integration

Verify connectivity

TO VERIFY CONNECTIVITY TO SUMO LOGIC

Click **Test** to verify that:

- The Director can communicate with Sumo Logic using the API access information on the port and protocol

specified.
- User credentials are working.

ANOMALI - TAAM INTEGRATION

> This document applies to Classic Integrations. While the Integrations solution is available, it is no longer actively maintained. Mandiant recommends that you plan a switch to Preview Integrations so you can take advantage of the latest features and functionality. Preview Integrations configuration steps are provided in the Director web interface. For more details, see the **Preview Integrations Documentation (https://docs.mandiant.com/home/msv-preview-integrations)**.

API Calls

The following API calls are used by the Validation Platform to bring in the Threat Actor information. Since Anomali allows you to mark Threat Actors as important, this information is also conveyed to the Threat Actor profiles in the platform.

Purpose	Call
Retrieve the Threat Actor list	/api/b1/actors
Retrieve Threat Actor details	/api/v1/actor/

If there are others sources going into Anomali, that information will also be captured and brought into the Validation Platform.

Prerequisites

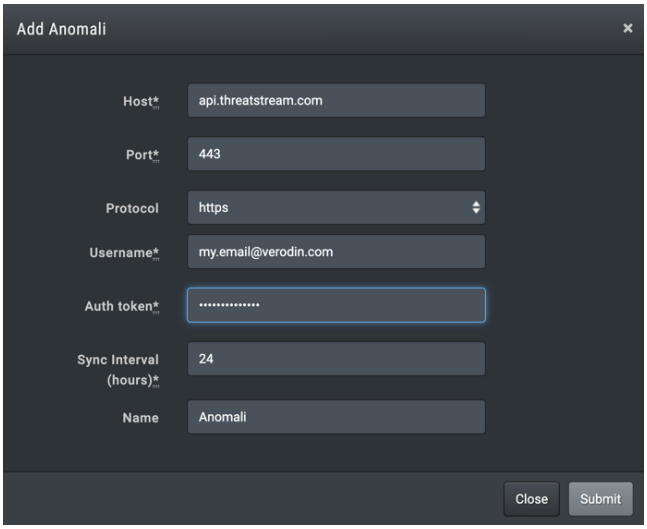
Information to gather before you start:

- Identify the host, port, and protocol.
- Identify the username and authentication token. Any account that has API access can be used.

Configuration

TO ADD THE ANOMALI THREAT INTELLIGENCE INTEGRATION

1. Go to **Settings** > **Integrations**.
2. In the Threat Intelligence Platform Integrations table, click **Add Integration** > **Anomali**.
3. Enter the **Host**.
4. Enter the **Port**.
5. Select the **Protocol**.
6. Enter the **Username**.
7. Enter the **Auth token**.
8. Enter the **Sync Interval** in hours (default: 24 hours).
9. (Optional) Assign a **Name**.
10. Click **Submit**. The integration automatically starts to sync after it is added.



Add Anomali Integration

CROWDSTRIKE INTEL

> This document applies to Classic Integrations. While the Integrations solution is available, it is no longer actively maintained. Mandiant recommends that you plan a switch to Preview Integrations so you can take advantage of the latest features and functionality. Preview Integrations configuration steps are provided in the Director web interface. For more details, see the **Preview Integrations Documentation (https://docs.mandiant.com/home/msv-preview-integrations)**.

API Calls

The CrowdStrike API is used by the Validation Platform to bring in the Threat Actor information. Both the OAuth2 and legacy CrowdStrike API key are supported in the CrowdStrike integration.

Purpose	Call
Threat Actor List Query	/actors/queries/actors/v1
Threat Actor Details Query	/actors/entities/actors/v1?ids={actor_id}
Threat Actor Malware Families	/indicator/v2/search/?actor.match={actor_name}

Prerequisites

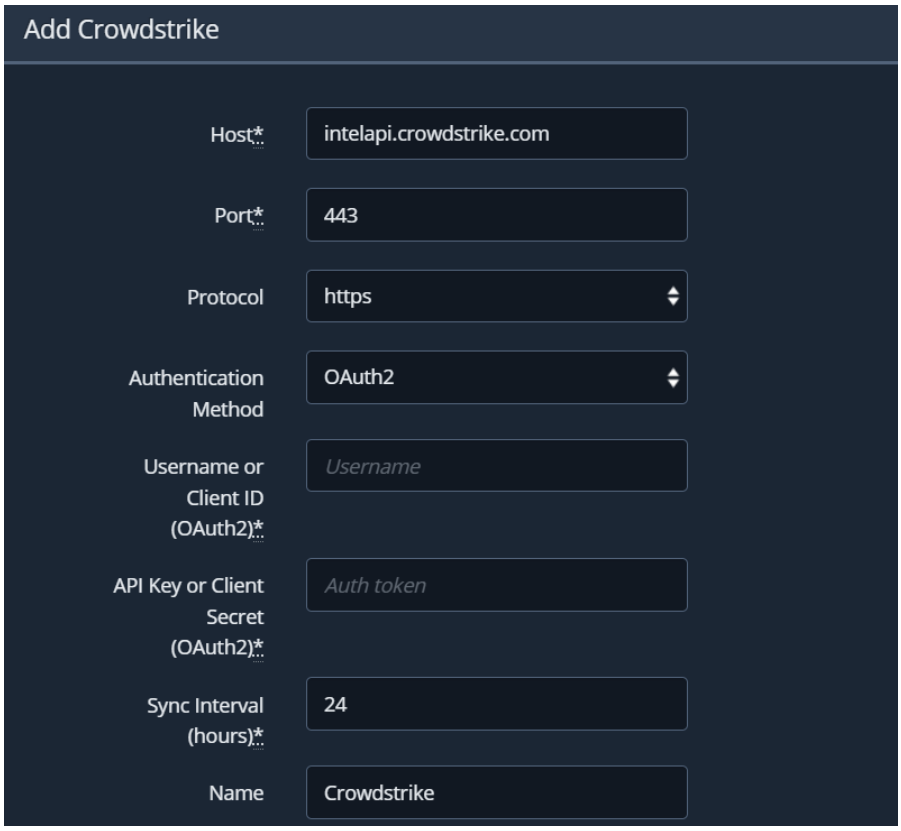
Information to gather before you start:

- Identify the host, port, and protocol.
- Identify the username and authentication token. Any account that has API access can be used. That account must have the following API permissions:
  - Read: Actors (Falcon X)
  - Read: IOCs (Indicators of Compromise)

Configuration

TO ADD THE CROWDSTRIKE THREAT INTELLIGENCE INTEGRATION

1. Go to **Settings** > **Integrations**.
2. In the Threat Intelligence Platform Integrations table, click **Add Integration** > **Crowdstrike**.
3. Enter the **Host**.
4. Enter the **Port**.
5. Select the **Protocol**.
6. Select the **Authentication Method**.
7. Enter the Username or Client ID.
   - If you are using Legacy API Key, enter the Username.
   - If you are using OAuth2, enter the Client ID.
8. Enter the API Key or Client Secret.
   - If you are using Legacy API Key, enter the API Key.
   - If you are using OAuth2, enter the Client Secret.
9. Enter the **Sync Interval** in hours (default: 24 hours).
10. (Optional) Assign a **Name**.
11. Click **Submit**. The integration automatically starts to sync after it is added.



Add Crowdstrike Intel Integration

MANDIANT THREAT INTELLIGENCE - TAAM INTEGRATION

> This document applies to Classic Integrations. While the Integrations solution is available, it is no longer actively maintained. Mandiant recommends that you plan a switch to Preview Integrations so you can take advantage of the latest features and functionality. Preview Integrations configuration steps are provided in the Director web interface. For more details, see the **Preview Integrations Documentation (https://docs.mandiant.com/home/msv-preview-integrations)**.

API Calls

The Validation Platform uses the Mandiant API v4 for its Mandiant Threat Intelligence integration. The integration provides APT and FIN threat actor details. It also includes different threat actor families and improved details for all threat actors.

The following API calls are used by the Validation Platform.

Purpose	Call
Retrieves the Threat Actor Overview Report generalized data	`/v4/actor/`
Retrieves the Threat Actor Description	`/v4/actor/:id`
Retrieves the MITRE ATT&CK tags associated with that threat actor	`/v4/actor/:id/attack-patterns`

Prerequisites

Information to gather before you start:

- Identify the port and protocol.
- Use an active account with API access.
- Obtain the Mandiant Advantage Threat Intelligence (MATI) API Public Key and Private Key. For more information see **Threat Intelligence Account Management (https://docs.mandiant.com/home/mati-manage-account-settings)**.

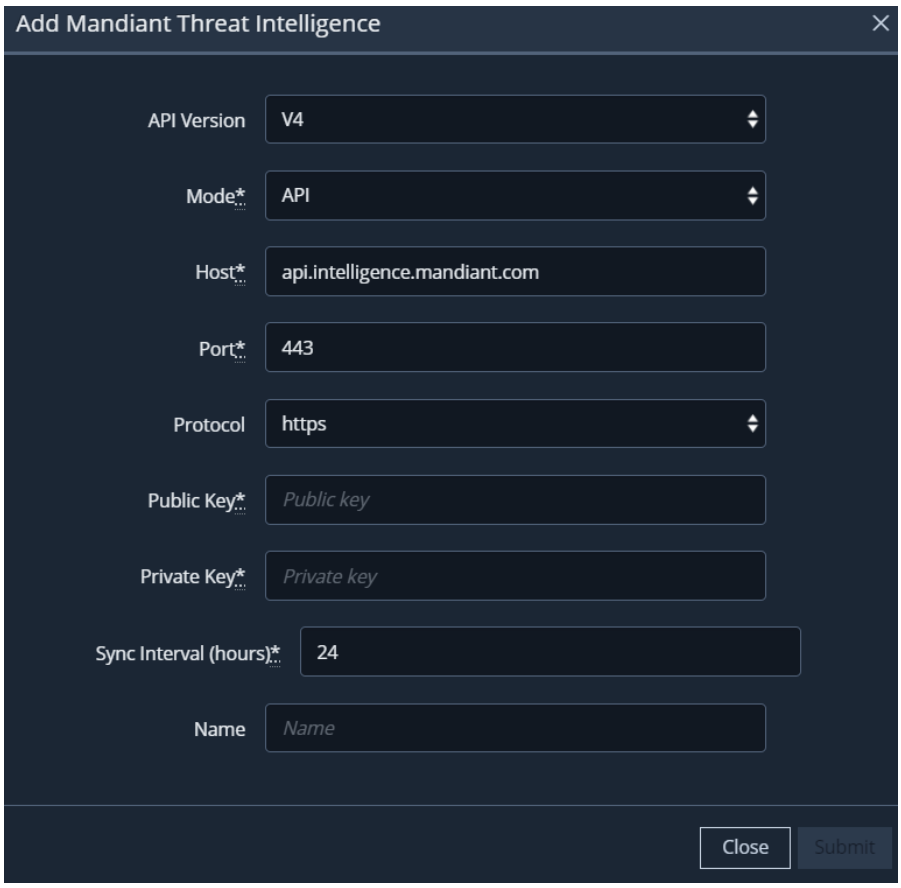
Configuration

To add the Mandiant Threat Intelligence Integration

1. Go to **Settings** > **Integrations**.
2. In the Threat Intelligence Platform Integrations table, click **Add Integration** > **Mandiant Threat Intelligence**.
3. The **API version** auto-populates to **V4**.
4. Select the **Mode**.

   > The only time you'd change this from API to FILE is if you are in an air-gapped environment. If you do choose FILE, you will select the JSON file and then skip to step 10.

5. The **Host** field auto-populates to **api.intelligence.mandiant.com**.
6. Enter the **Port**.
7. Select the **Protocol**.
8. Enter the **Public Key**.
9. Enter the **Private Key**.
10. Enter the **Sync Interval** in hours (default: 24 hours).
11. (Optional) Assign a **Name**.
12. Click **Submit**. The integration automatically starts to sync after it is added.



Add Mandiant Threat Intelligence Integration

INTEL471 - TAAM INTEGRATION

> This document applies to Classic Integrations. While the Integrations solution is available, it is no longer actively maintained. Mandiant recommends that you plan a switch to Preview Integrations so you can take advantage of the latest features and functionality. Preview Integrations configuration steps are provided in the Director web interface. For more details, see the **Preview Integrations Documentation (https://docs.mandiant.com/home/msv-preview-integrations)**.

Intel471 can be used to bring Malware Family information into the Validation Platform. In the Threat Actor Library, the Malware Families will include malware related (Malware:Hancitor for example) TTPs. Intel471 does map to MITRE ATT&CK Tactics, but the Threat Actor Library excludes these because they are not granular enough to accurately relate to Actions.

API Calls

The following API calls are used by the Validation Platform.

Purpose	Call
Retrieve the Malware Details	/v1/malwareReports?threatType=malware
	/v1/events?threatType=malware&malwareFamily={malware_family}

Prerequisites

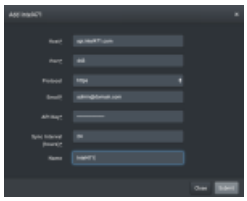
Information to gather before you start:

- Identify the host, port, and protocol.
- Identify the Email address and API key. Any account that has API access can be used.

Configuration

TO ADD THE INTEL471 INTEGRATION

1. Go to **Settings** > **Integrations**.
2. In the Threat Intelligence Platform Integrations table, click **Add Integration** > **Intel471**.
3. Enter the **Host**.
4. Enter the **Port**.
5. Select the **Protocol**.
6. Enter the **Email**.
7. Enter the **API Key**.
8. Enter the **Sync Interval** in hours (default: 24 hours).
9. (Optional) Assign a **Name**.
10. Click **Submit**. The integration automatically starts to sync after it is added.



(https://d383cql5uq169w.cloudfront.net/app/image/pid/620d7e13ccb103e8557b25b0/id/629a12d4c9cba0017c2f7db5/n/intel471.png)

Add Intel471 Integration

THREATCONNECT

> This document applies to Classic Integrations. While the Integrations solution is available, it is no longer actively maintained. Mandiant recommends that you plan a switch to Preview Integrations so you can take advantage of the latest features and functionality. Preview Integrations configuration steps are provided in the Director web interface. For more details, see the **Preview Integrations Documentation (https://docs.mandiant.com/home/msv-preview-integrations)**.

API Calls

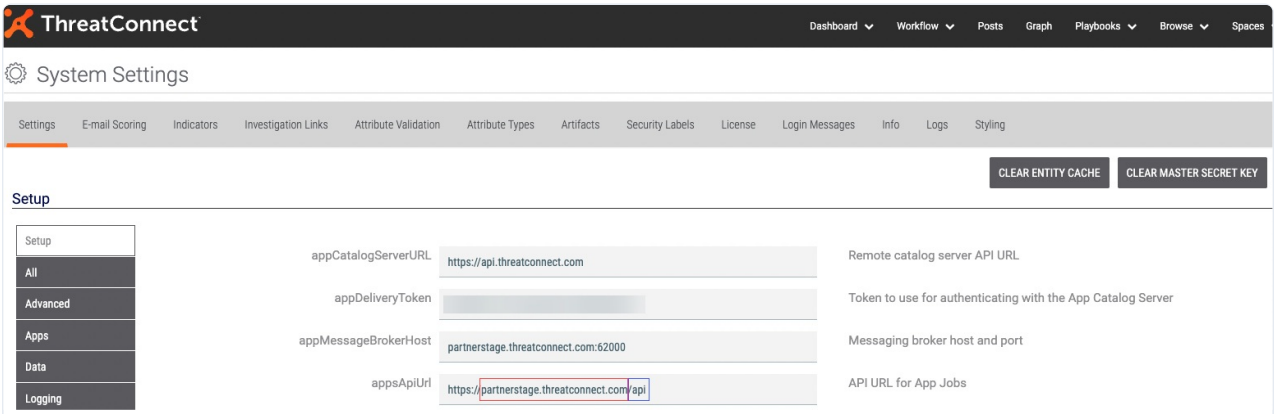
The following API calls are used by the Validation Platform.

Purpose	Call
Retrieve a List of Owners	/v2/owners
Retrieve a List of Threat Actor and details	/v2/groups/adversaries
Retrieve threat actor MITRE ATT&CK tags	/v2/groups/adversaries//groups/threats

Prerequisites

Gather the following information from your ThreatConnect environment before you start.

- Identify the host (red highlighted FQDN of the **appsApiUrl** in the following screenshot), port, and protocol. Note that your appsApiUrl may differ from the one shown in the screenshot.
- Identify the username, API root (blue highlighted value in the following screenshot), Access ID, and API key. Any account that has API access can be used.



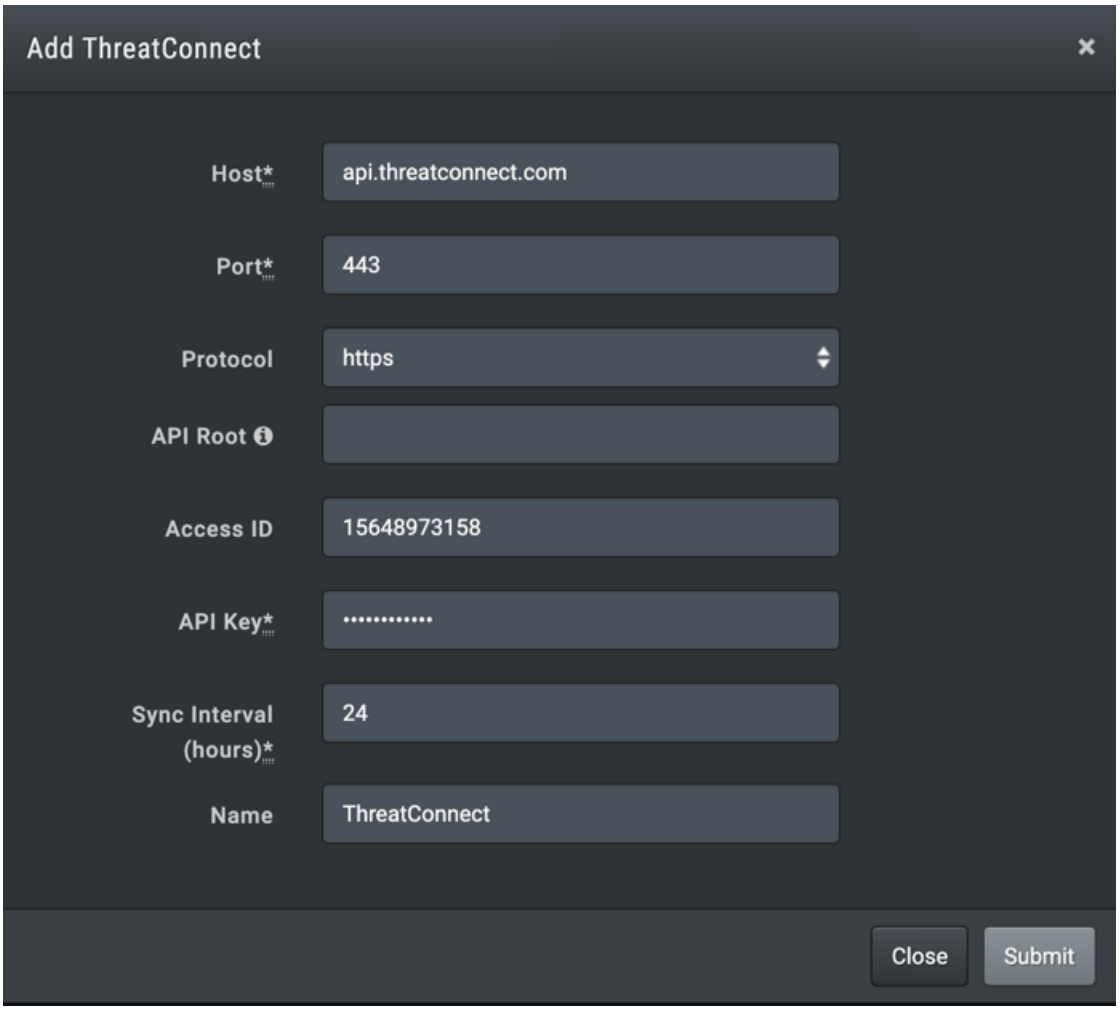
appsApiURL value (Host highlighted in red, API Root highlighted in blue) on the ThreatConnect system settings page

Configuration

TO ADD THE THREATCONNECT INTEGRATION

1. Go to **Settings** > **Integrations**.
2. In the Threat Intelligence Platform Integrations table, click **Add Integration** > **ThreatConnect**.
3. For **Host**, enter the FQDN value (this comes from the **appsApiUrl** field that you noted in the ThreatConnect environment).
4. Enter the **Port**.
5. Select the **Protocol**.

6. Enter the **API Root**, if one is available from the ThreatConnect environment.
   This is an optional prefix to add to API calls. If unsure, check to see if there is an API value after the **appsApiUrl** FQDN in the ThreatConnect environment.
7. Enter the **Access ID**.
8. Enter the **API Key**.
9. Enter the **Sync Interval** in hours (default: 24 hours).
10. (Optional) Assign a **Name**.
11. Click **Submit**. The integration automatically starts to sync after it is added.



Add ThreatConnect Integration

THREAT QUOTIENT - TAAM INTEGRATION

> This document applies to Classic Integrations. While the Integrations solution is available, it is no longer actively maintained. Mandiant recommends that you plan a switch to Preview Integrations so you can take advantage of the latest features and functionality. Preview Integrations configuration steps are provided in the Director web interface. For more details, see the **Preview Integrations Documentation (https://docs.mandiant.com/home/msv-preview-integrations)**.

This integration is not remote capable.

Update Threat Quotient

Identify or create credentials to access Threat Quotient with read access, at minimum.

API Calls

The following API calls are used by Validation Platform.

Purpose	Call
Get Access Token	/token
Get Threat Actors (Paginated)	/adversaries
Get Actor Descriptions	/adversaries/{actor_id}/description
Get Actor Location	/adversaries/{actor_id}/attributes?attribute_name=Country
Get Actor Aliases	/adversaries/{actor_id}/?with=adversaries
Get Actor Malware Used	/adversaries/{actor_id}/malware
Get Actor Attacks (MITRE)	/adversaries/{actor_id}/malware

Update the Security Validation Platform

Prerequisites

Information to gather before you start:

- Identify the host, port, and protocol associated with your Threat Quotient instance
- Identify the email, and password associated with your Threat Quotient account
- Identify your Client ID in the **Settings** section of the Threat Quotient SNYPR Web Portal

Configuration

TO ADD THE THREAT QUOTIENT INTEGRATION

1. Go to **Settings** > **Integrations**.
2. Click **Add Integration** > **Threat Quotient**.
3. Enter the Host, Port, and Protocol.
4. Enter the Email, Password, and Client ID.
5. Enter the **Sync Interval** in hours (default: 24 hours).
6. (Optional) Assign a **Name**.
7. Click **Submit**.

(https://d383cql5uq169w.cloudfront.net/app/image/pid/620d7e13ccb103e8557b25b0/id/629a12d4c9cba0017c2f7dbd/n/threat-quotient.png)

Threat Quotient

Verify connectivity

TO VERIFY CONNECTIVITY TO THE THREAT QUOTIENT INTEGRATION

Click **Test** to verify that:

- The Director can communicate with the integration host on the port and protocol specified.
- The integration credentials are valid and working.

WINDOWS DEFENDER: ESTABLISH EXCLUSIONS

Security Validation validates the effectiveness of your security technologies. For MSV and MA-SV, this is done by installing Actors in locations around your network. Endpoint security technologies running on the Actor may flag Mandiant services that are required to run Actions. In order for these Actors to be effective and carry out Actions, certain endpoint files pertaining to the execution of these Actors must be added to the allowlist with the security technologies installed on the host.

> The following information is based on the security technology manufacturer's documentation. If the steps do not match your UI, consult the technology's documentation directly.

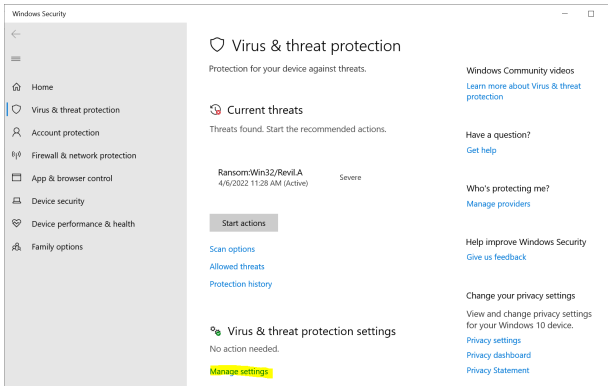
If your network includes Windows Defender, the Mandiant Advantage team recommends creating exclusions within Windows Defender. These exclusions quiet detections for known paths and allow trusted processes to run. There are four different methods that you can use:

- Local UI
- PowerShell (administrator)
- Registry
- Domain Level GPO Exclusions

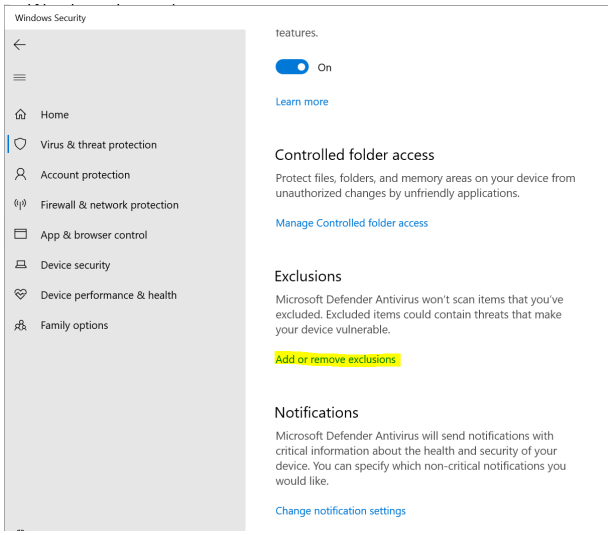
> If your security controls prevent you from using wildcards, you can use the full filenames or hashes instead. If you choose to use the hashes, Windows Defender needs to be updated for each Security Validation release. A list of the filenames and their hashes (for the current version) is located in **Windows 64-bit Actor Artifacts and Services (https://docs.mandiant.com/home/msv-windows-64-bit-actor-artifacts-and-services)**.

Local UI

1. Navigate to **Start** > **Settings** > **Updates and Security** > **Windows Security** > **Virus & threat protection** and select **Manage Settings**.



2. Scroll down to the Exclusions section and select **Add or remove exclusions**.

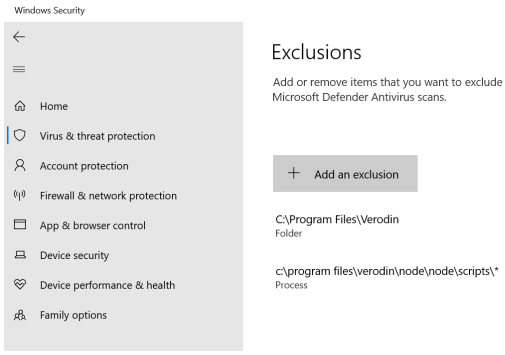


3. Select **Add an exclusion** and add both of the following:

   Folder: `C:\Program Files\Verodin`

   Process: `C:\Program Files\Verodin\node\node\scripts\*`

   RDV should be able to execute after these exclusions are in place.



PowerShell (administrator)

As an administrator, you can add the required exclusions through PowerShell:

```
Add-MpPreference -ExclusionPath "C:\Program Files\Verodin\" -Force
```

```
Add-MpPreference -ExclusionProcess "C:\Program Files\Verodin\node\node\scripts\*"
```

Registry

You can find the exclusions in the registry here: `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender\Exclusions`.

In this registry entry, you see *Paths* and *Processes.* You can add them there manually or run the following:

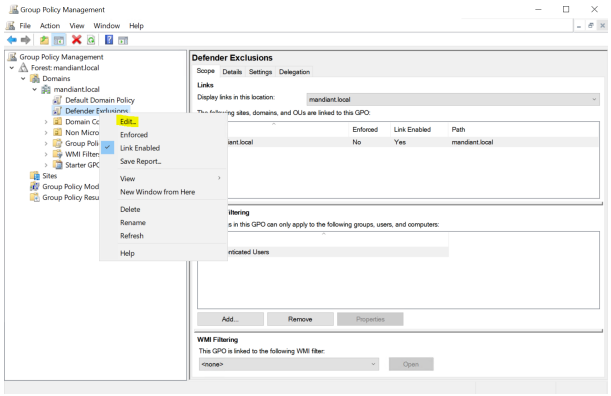
```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender\Exclusions\Paths]
"C:\\Program Files\\Verodin\\"=dword:00000000
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender\Exclusions\Processes]
"C:\\Program Files\\Verodin\\node\\node\\scripts\\*"=dword:00000000
```

Domain Level GPO Exclusions

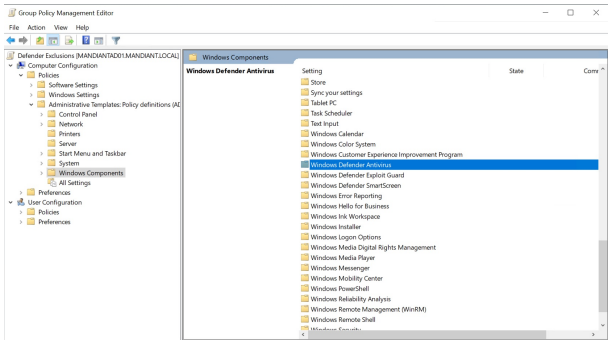
If Windows Defender is being used and it's managed by GPO, here's a quick overview on how to add those exclusions.

These exclusions must be added at the Domain level and the user must have permissions to edit GPOs.

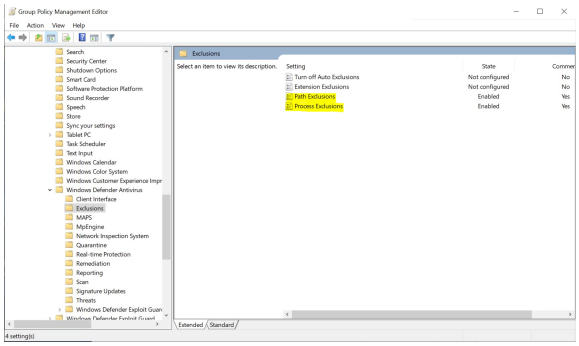
1. **Start** > **Run** > **gpmc.msc** (you must have permissions to modify GPOs). If Group Policy is not installed, you can download the remote tools pack which contains these items.
2. Go to **Forest** > **Domains** > **Domain Name** and either edit an existing policy or create a new one.

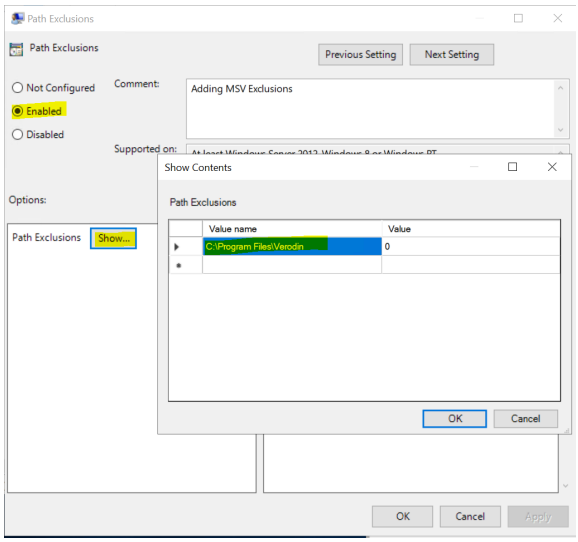


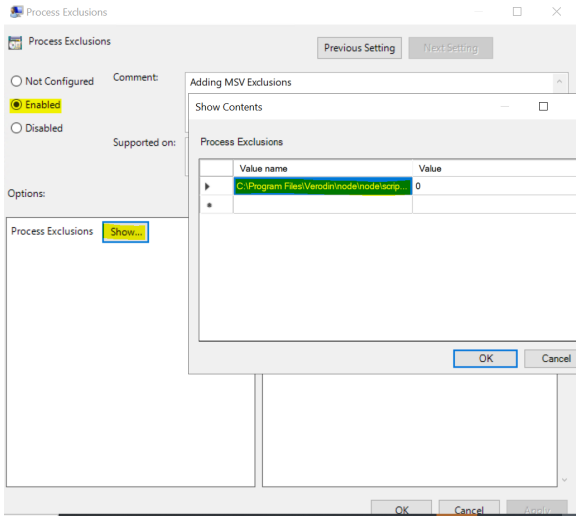
3. Select **Computer Configuration** > **Policies** > **Administrative Templates** > **Windows Components** > **Windows Defender Antivirus** > **Exclusions**.



4. Edit the **Path Exclusions** and **Process Exclusions** to include the MSV folder and processes.
    a. For Path: `C:\Program Files\Verodin`
    b. For Process: `C:\Program Files\Verodin\node\node\scripts\*`







5. Make sure the group policy is applied to the correct systems and you should see the exclusions locally.

CROWDSTRIKE: EXCLUSIONS & LOCAL LOGS

Security Validation validates the effectiveness of your security technologies. This is done by installing Actors in locations around your network. Endpoint security technologies running on the Actor may flag Mandiant services that are required to run Actions. In order for these Actors to be effective and carry out Actions, certain endpoint files pertaining to the execution of these Actors must be added to the allowlist with the security technologies installed on the host.

> The following information is based on the security technology manufacturer's documentation. If the steps do not match your UI, consult the technology's documentation directly.

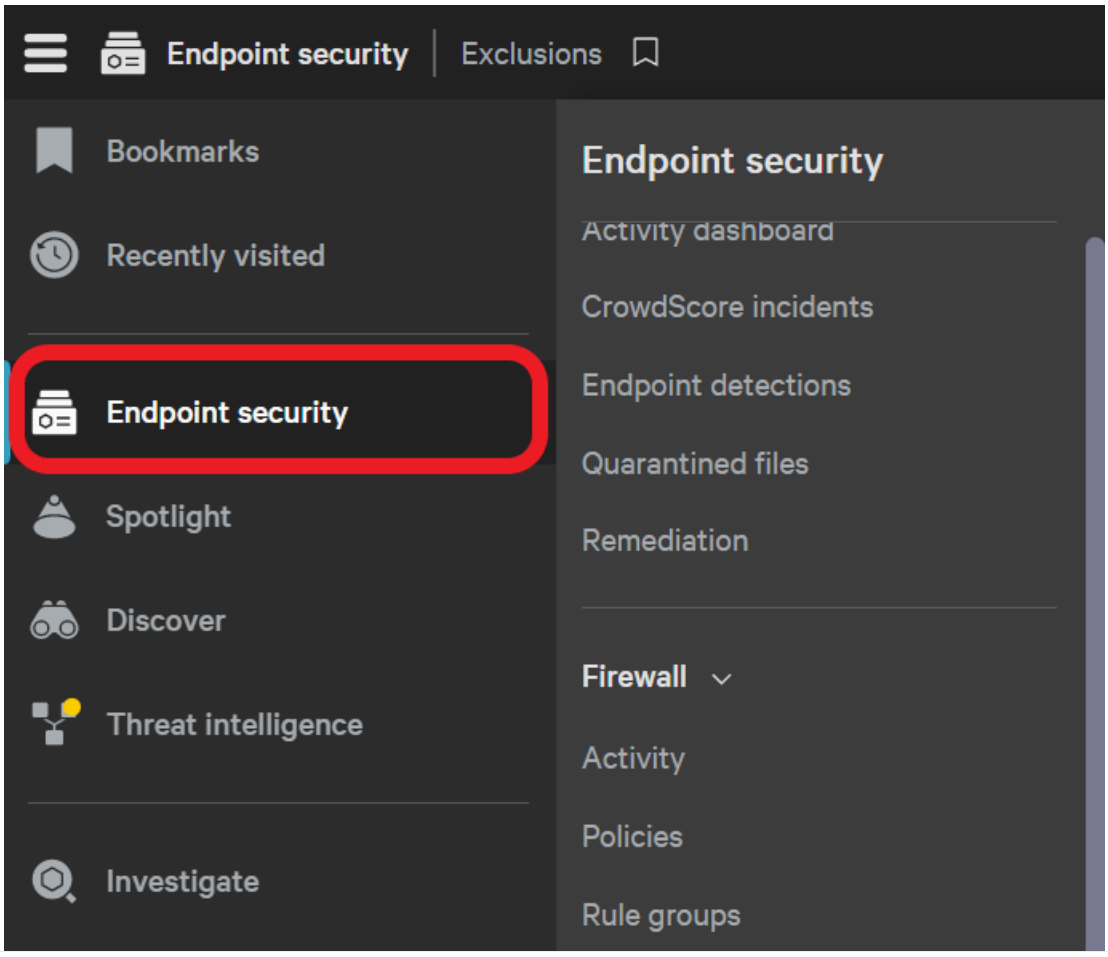
When using Security Validation on a network that includes CrowdStrike, the Mandiant Advantage team recommends completing the following two processes:

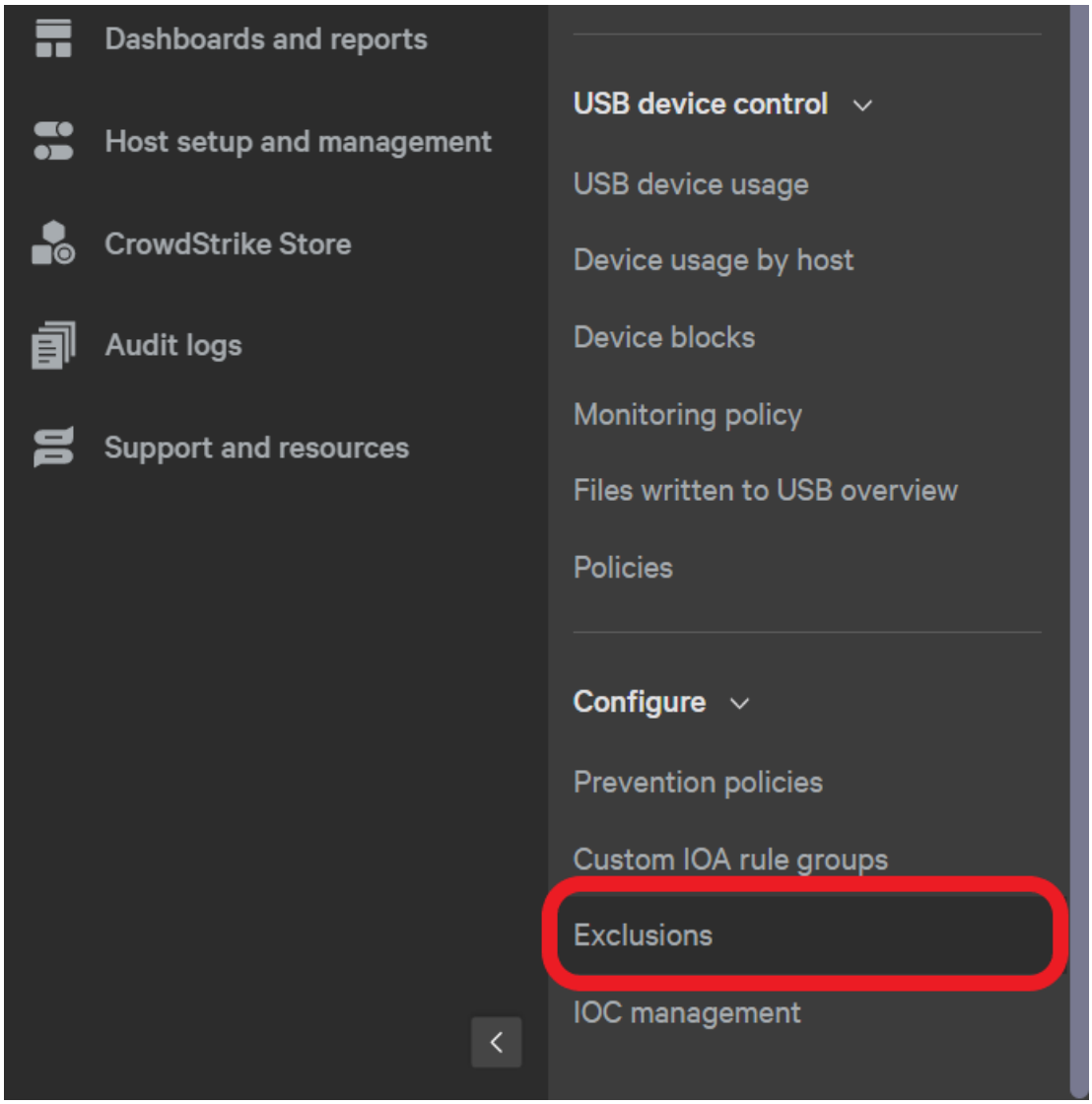
- **Establish Exclusions in CrowdStrike:** Instructions on how to create exclusions within CrowdStrike to quiet detections for known file paths and allow trusted processes to run.
- **Enable Local Logs** in **CrowdStrike:** Instructions on how to set-up local logging for CrowdStrike on Windows endpoints.

CrowdStrike: Establish Exclusions

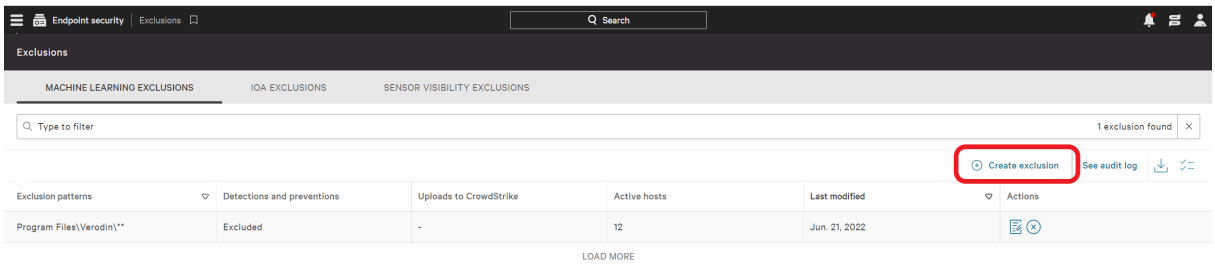
These are instructions on how to create exclusions within CrowdStrike to quiet detections for known file paths and allow trusted processes to run.

1. Navigate to Exclusions menu item: **Configuration > Endpoint security > Exclusions**.

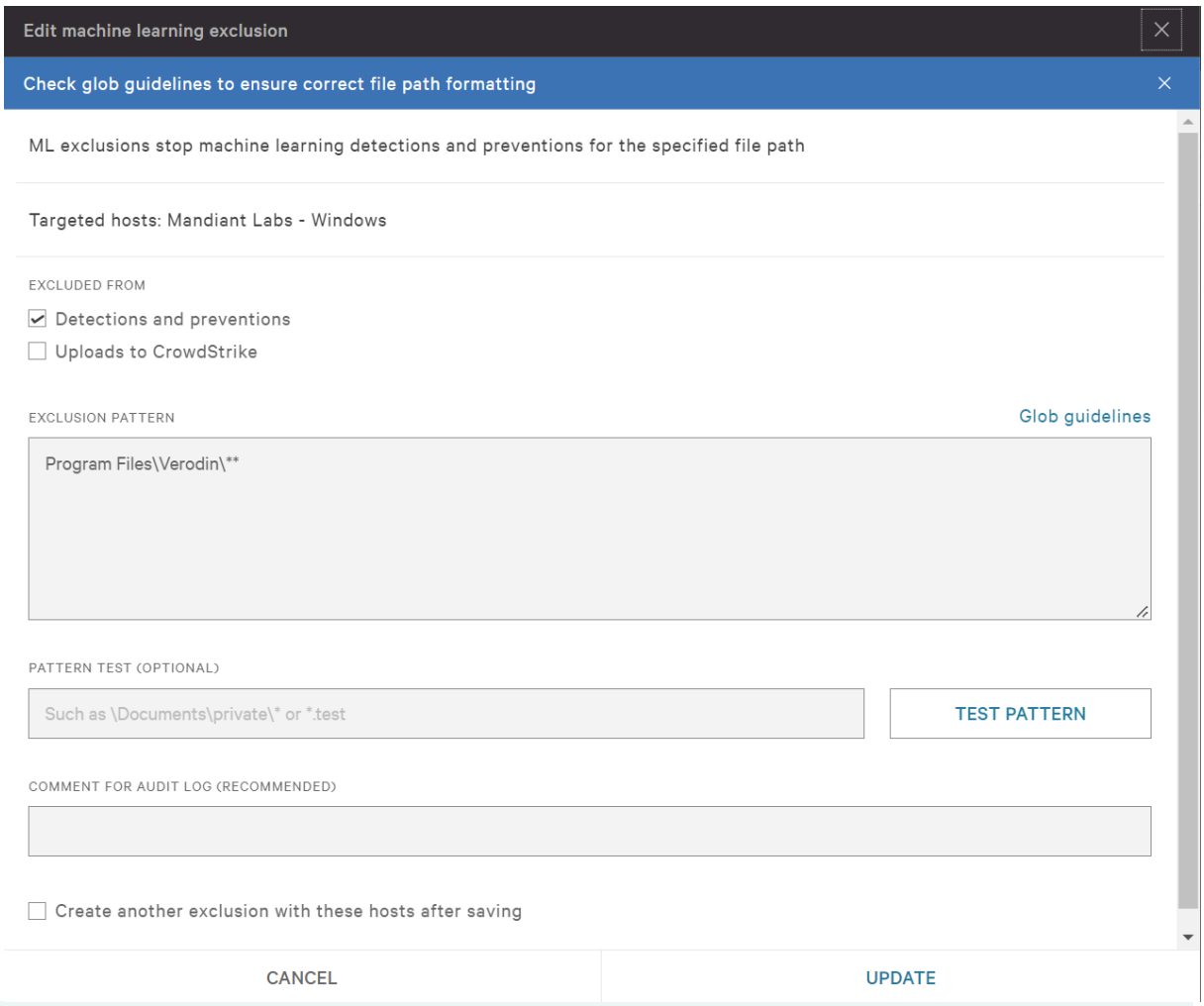




2. Select **Create exclusion** under the MACHINE LEARNING EXCLUSIONS tab.



3. Select the group you would like to apply the exclusions to.
4. Add *Program Files/Verodin/*** to exclude all subfolders and processes within that folder, which is the Security Validation directory.



NOTE: If your security controls prevent you from using wildcards, you can use the full file names or hashes instead. If you choose to use the hashes, CrowdStrike will need to be updated each Validation release. A list of the file names and their hashes (for the current version) is located in the Windows Actor Install QS Guide.

5. Click **Update** to apply the exclusion.

CrowdStrike: Enable Local Logs

These are instructions on how to set-up local logging for CrowdStrike on Windows endpoints.

1. Create a file with the extension .reg titled *crowdstrike_local_log_enable.reg*.
2. Copy and paste the following into your file:

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SYSTEM\CrowdStrike\{9b03c1d9-3138-44ed-9fae-d9f4c034b88d}\{16e0423f-7058-48c9-a204-725362b67639}\Default]
"AFLAGS"=hex:03,00,00,00
```

3. Open a command prompt and run the following command to enable logging:

```
regedit crowdstrike_local_log_enable.reg
```

4. The logs can be found at `Falcon Sensor-CSFalconService/Operational`.

SENTINELONE: CONFIGURE EXCLUSIONS

Security Validation validates the effectiveness of your security technologies. This is done by installing Actors in locations around your network. Endpoint security technologies running on the Actor may flag Mandiant services that are required to run Actions. In order for these Actors to be effective and carry out Actions, certain endpoint files pertaining to the execution of these Actors must be added to the allowlist with the security technologies installed on the host.

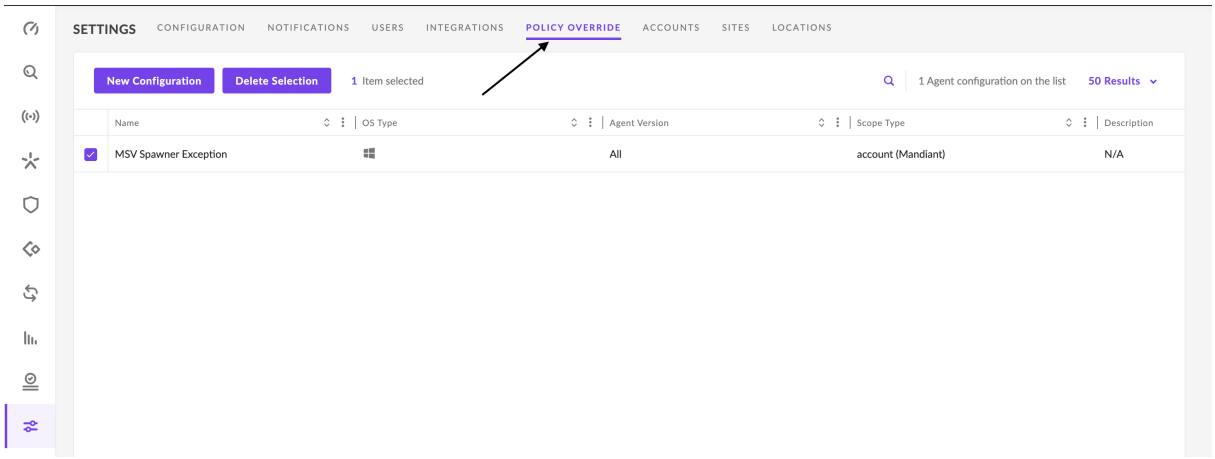
> The following information is based on the security technology manufacturer's documentation. If the steps do not match your UI, consult the technology's documentation directly.

When using Security Validation on a network that includes SentinelOne, the Mandiant Advantage team recommends configuring exclusions using the following process.

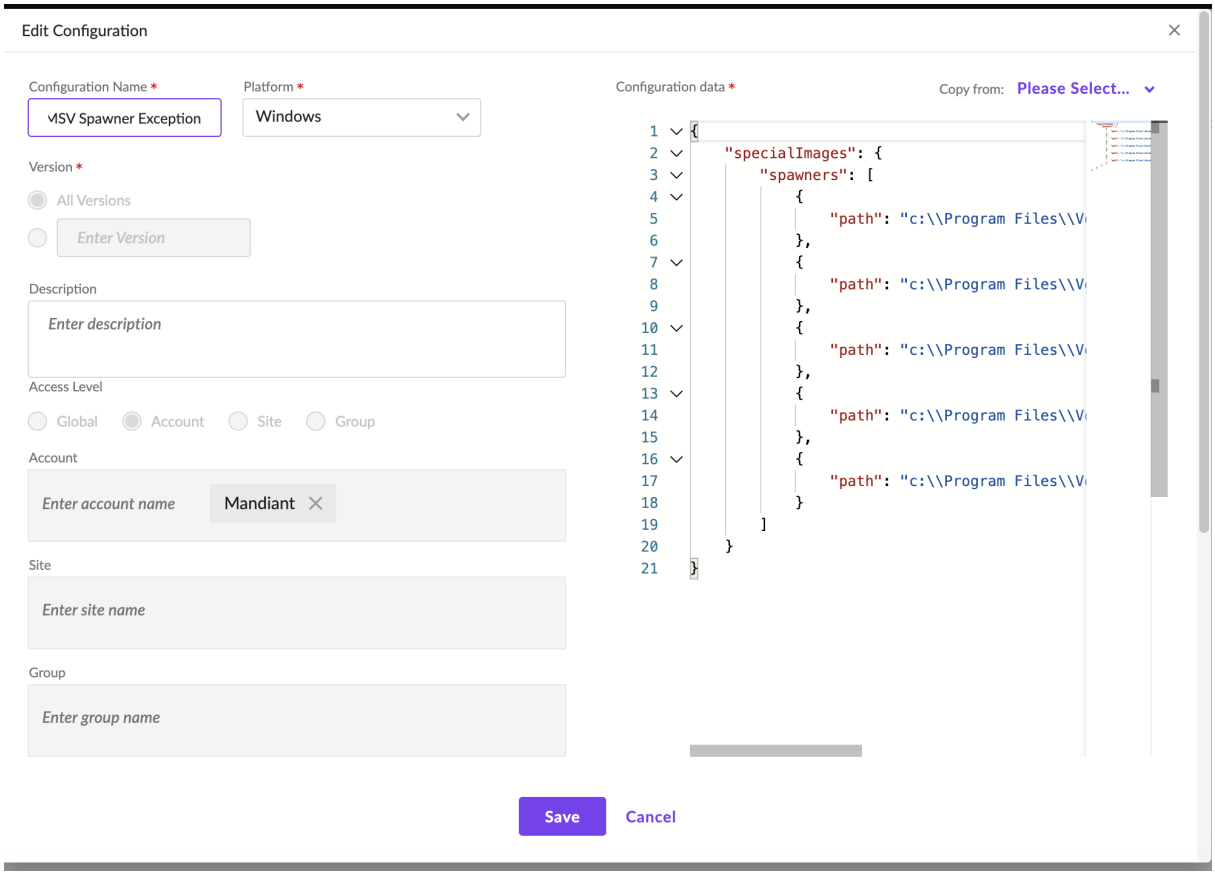
Configure Exclusions

The policy override for SentinelOne (S1) can be set up using the following steps.

1. Locate **SETTINGS** in the menu pane of the S1 management console.
2. Select **POLICY OVERRIDE** tab.



3. Select **New Configuration**.
4. Add a custom JSON policy override, which S1 calls a Spawner rule.
5. Enter **Name** and **Description** (optional).
6. Select either an Account, Site, or Group for this policy overrides to apply to.
7. Copy and paste the **JSON config** into the **Configuration data** pane.



8. **Save** the configuration.

JSON Exclusion Data

```
{
 "specialImages": {
   "spawners": [
     {
       "path": "c:\\Program Files\\Verodin\\node\\node\\scripts\\verodin_backend_service.exe"
     },
     {
       "path": "c:\\Program Files\\Verodin\\node\\node\\scripts\\verodin_backend.exe"
     },
     {
       "path": "c:\\Program Files\\Verodin\\node\\node\\scripts\\verodin_endpoint_service.exe"
     },
     {
       "path": "c:\\Program Files\\Verodin\\node\\node\\scripts\\cli_executer.exe"
     },
     {
       "path": "c:\\Program Files\\Verodin\\node\\node\\scripts\\change_user.exe"
     },
     {
       "path": "c:\\Program Files\\Verodin\\node\\node\\scripts\\verodin_network_service.exe"
     }
   ]
 }
}
```

EVENT FILTER RULES

> This document applies to Classic Integrations. While the Integrations solution is available, it is no longer actively maintained. Mandiant recommends that you plan a switch to Preview Integrations so you can take advantage of the latest features and functionality. Preview Integrations configuration steps are provided in the Director web interface. For more details, see the **Preview Integrations Documentation (https://docs.mandiant.com/home/msv-preview-integrations)**.

The Security Validation platform captures all events its integrations see when Jobs are run. Some of these events may just be noise or not directly related to the test you're running, so you don't want them to be counted towards the results of the Job. To assist you with excluding these events, the platform includes Integration Event Filter Rules.

An overview of the functionality includes:

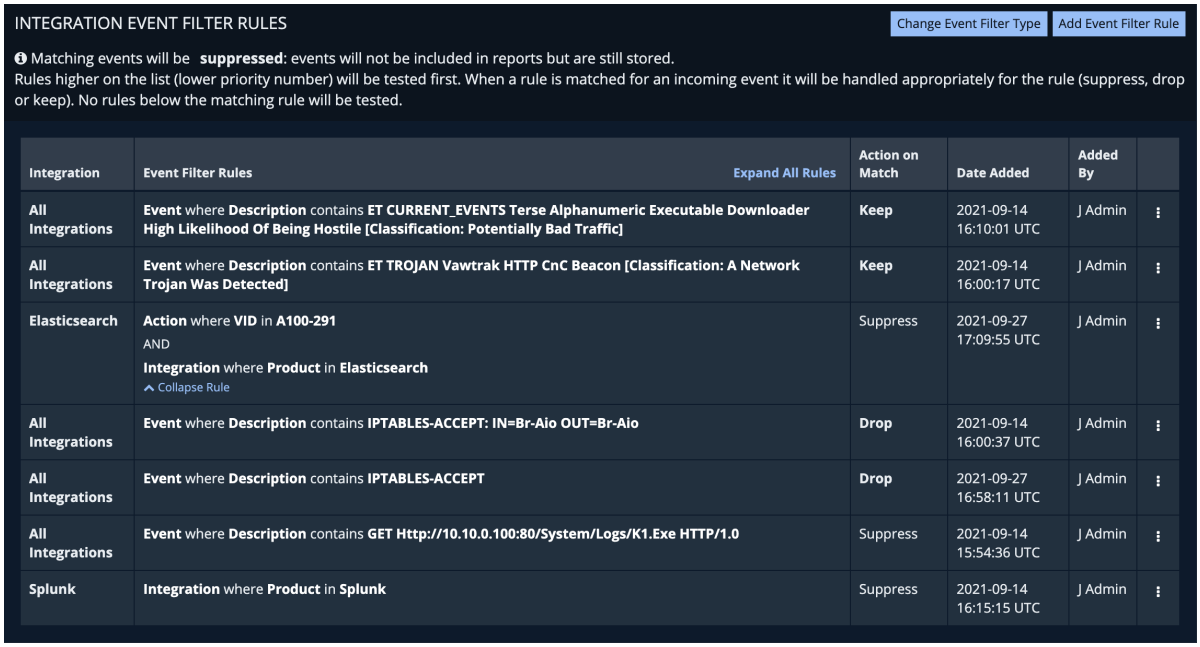
- The platform will have a default filter type that's automatically applied to all Filter Rules you create - suppressed or dropped are the two options.
- Individual Filter rules can be configured to override the platform's default Action. In addition to having suppressed and dropped as options, you can also configure the rule to Keep specific events.
- The filter rules are displayed in the order they are applied when a Job is run, which is configured when creating and editing the rules.
- The Job Results include a section for each Action that displays which Event filter rules were applied and what action that rule completed.

Viewing all Event Filter Rules

There are several places in the Director where you can view Event Filter Rules. However, the only place you can see them all and what order they run is in the Event Filter Rules Table on the Integrations page.

> If an Event Filter Rule is bolded, it means the Event Filter Type is manually set and does not use the global Event Filter Type.

To view all Event Filter Rules configured for your environment, go to **Settings** > **Integrations**.



Event Filter Rules table

Important Definitions

When creating event filter rules, you configure them to use one of three types: suppress, drop, or keep.

Term	Definition	Examples of when to use
Suppress	Events will not be included in reports but are still stored	You want to see the events when you view the Job Action, but you do not want it to count towards the Job Action's pass / fail / detected information.
Drop	Events are discarded and not stored	There is no need to track the specific events when running tests.
Keep	Events will remain associated to the Job Action	If you want events to remain and you have other event filter rules that would either suppress or drop them. For example, you have an Event Filter Rule that suppresses events for an Action type but you want the events to remain for specific Actions.

Required Permissions

The ability to view, create, and edit Event Filter Rules and the ability to manually drop Events from Jobs is controlled by several system-level permissions, as described in the following table.

Event & Event Filter Rules Permissions

Action	Required Permission	Roles with the permission by default
Create / Edit Event Filter Rules	Settings - Edit	System Admin, Power User
View Event Filter Rules	Settings - View	System Admin, Power User, Users
Drop / Suppress Events directly from Job Results	Integration Events - Edit	System Admin

How the Director processes Event Filter Rules

Event Filter rules run against new Jobs only, not Jobs that have run in the past. Once an event is filtered by a rule, the results will not change for that event, regardless of other rules that run or of any changes you make to the filter rule. Changing an Event Filter Rule during the event matching window will only impact events that have not already been processed.

Event Filter Rules are also applied in a specific order - the order of the rules in the Integration Event Filter Rules table determines the order the rules are processed. Knowing this gives you some general best practices to follow when considering your ordering:

- Order rules so specific rules run before general ones
  Example 1: Keep a specific event for a type of Action before suppressing the same event for other Action types
- Example 2: Suppress events with a specific description before suppressing events for different instances of an integration
- If you create a rule that keeps events, because it's important those events are always associated with Job Actions, those rules need to run first
  Example: When testing your environment for a specific type of Action, you may want to keep all Events for that Action type, including events that are dropped by a rule further down in the list

Event Suppression can also filter events. This filtering works at the level of the Director where Integration Events are matched with Job Actions that are responsible for them. Most feature-specific events are affected by event suppression because they all create Director-level events. Note that events that have been filtered out through of the the event filter types do not show up when creating monitors. For more information, see **Reassigning, Suppressing, and Dropping Events from Jobs (https://docs.mandiant.com/home/msv-reassigning-suppressing-and-dropping-events)**.

If you have many rules, instead of using the rule's arrows to move it, use the Insert Above or Insert Below option on another rule to move it.

WORKING WITH EVENT FILTER RULES

> This document applies to Classic Integrations. While the Integrations solution is available, it is no longer actively maintained. Mandiant recommends that you plan a switch to Preview Integrations so you can take advantage of the latest features and functionality. Preview Integrations configuration steps are provided in the Director web interface. For more details, see the **Preview Integrations Documentation** (https://docs.mandiant.com/home/msv-preview-integrations).

There are four places you can view and create Event Filter Rules in the platform, three of which prepopulate the first condition for you if you're creating a new rule. In addition, two of those areas allow you to edit and delete the event Filter Rules.

Location	Prepopulated Condition
Integration Event Filter Rules Table on Integration Page	N/A
An Integration in the Integrations Table on the Integrations page	Automatically adds the Integration
Action Preview / Action Details	Automatically adds the VID
Event section for a Job Action	Automatically adds the Event Description

This topic covers:

- Configuring the Event Filter Type, used as the default for all Event Filter Rules
- Creating Event Filter Rules
- Updating and Deleting Event Filter Rules

To Configure the Event Filter Type

To allow you to quickly update the behavior of your event filter rules, there is a global event filter type. When creating and editing rules, you can override this setting.

1. Go to **Settings** > **Integrations** and click **Change Event Filter Type** in the Integration Event Filter Rules table.
2. Choose your option, Suppress Events or Drop Events, and click **Save**. This will be what happens to Events that match an Event Filter rule in jobs moving forward, unless you override the setting.

To add an event filter rule

> New Event Filter Rules only apply to new Jobs, they do not change Jobs that ran before the rule was created.

1. Locate the Event Filter Rules section of the page and click Add Event Filter Rule.
   - Go to **Settings** > **Integrations** and click **Add Event Filter Rule**.
   - Go to **Settings** > **Integrations**, select an Integration's action menu and click **Add Event Filter Rule**.
   - Scroll to the Event Filter Rule section of an Action and click **Add Event Filter Rule**.
   - Open the Events section for a Job Action, select an Event's action menu, and click **Add Event Filter Rule**.
2. (Optional) If you don't want to use the system setting for what happens with the event, click Override system settings and select the setting you want instead. In addition to Suppress Events & Drop Events, you also have the option to Keep Events that match your rule.
3. In the Event Filter Rule tab, add your Conditions.
   - The first condition will be added automatically if you start from an Action or an Event
   - When you add multiple conditions, the event must match all conditions for the rule to be applied

- Conditions can be defined for Actions, Integrations, and Events

4. In the Event JSON tab, add your filter rules using the various drop down fields and their conditions. When you have added all your conditions for each JSON drop-down option, click **Add to Rule**.
   - "description": This is the description of the Event. Conditions include:
     - In
     - Not In
     - Contains
     - Doesn't Contain
     - Starts With
     - Ends With
   - "dest_ip": This is the destination IP address for the Event. Conditions include:
     - In
     - Not In
   - "host": This is the host for the Event. Conditions include:
     - In
     - Not In
   - "src_ip": This is the source IP address for the Event. Conditions include:
     - In
     - Not In
5. Select the Priority tab and order the Event Filter Rules based on how you want them to run.
6. Click **Save**.

(https://d383cql5uq169w.cloudfront.net/app/image/pid/620d7e13ccb103e8557b25b0/id/62880ba6445d5e3e714b3bec/n/json-event-filter-ex1.png)

Example of Event JSON tab

(https://d383cql5uq169w.cloudfront.net/app/image/pid/620d7e13ccb103e8557b25b0/id/62880ba6445d5e3e714b3bee/n/json-event-filter-ex2.png)

Example of Event Condition Options

(https://d383cql5uq169w.cloudfront.net/app/image/pid/620d7e13ccb103e8557b25b0/id/62880ba6445d5e3e714b3bf0/n/json-event-filter-int-host-ex.png)

Example of Integration and Host Options

(https://d383cql5uq169w.cloudfront.net/app/image/pid/620d7e13ccb103e8557b25b0/id/62880ba7445d5e3e714b3bf2/n/json-event-filter-int-product-ex.png)

Example of Integration and Product Options

To edit an event filter rule

Changes to Event Filter Rules only apply to new Jobs, they do not change Jobs that ran before the rule was updated.

1. Locate the Event Filter Rules you want to change and click the edit Event Filter Rule option.
    - Go to **Settings** > **Integrations**. Select the filter's action menu and click **Edit Event Filter Rule**.
    - Scroll to the Event Filter Rule section of an Action. Select the filter's action menu and click **Edit Event Filter Rule**.
2. Modify any of the settings you want to change.
    - Override the System Setting (Action on Match)
    - Add / remove Conditions
    - Change the priority (change when the filter rule runs compared to other filter rules)
3. Click **Save**.

To Delete an event filter rule

Deleting Event Filter Rules do not change Jobs results.

1. Locate the Event Filter Rules you want to change and click **Delete**.
    - Go to **Settings** > **Integrations**. Select the filter's action menu and click **Delete**.
    - Scroll to the Event Filter Rule section of an Action. Select the filter's action menu and click **Delete**.
2. Confirm you want to delete by clicking **OK**.

USING EVENT FILTER RULES

> This document applies to Classic Integrations. While the Integrations solution is available, it is no longer actively maintained. Mandiant recommends that you plan a switch to Preview Integrations so you can take advantage of the latest features and functionality. Preview Integrations configuration steps are provided in the Director web interface. For more details, see the **Preview Integrations Documentation (https://docs.mandiant.com/home/msv-preview-integrations)**.

Event Filter Rules should be setup when first configuring your Director and when you add or modify your security controls. You may also want to configure new rules when you are troubleshooting issues in your environment and when you start testing new use cases (Action Types).

> Events on Jobs that come directly from Endpoint Products cannot have rules created around them. Instead, you will need to suppress or drops those events when reviewing the Job.

Eliminate "noise" events

By default, the pass / fail rules for Jobs consider a Job Action that was either Blocked or Detected to have passed. If your security controls are sending Events that don't indicate that the Job Action was actually detected, you're getting a false positive. Setting up Event Filter Rules to drop those events will give you a more clear picture of the security of your environment. This could include keeping events for some types of Actions but suppressing those same events for other Action Types because they aren't pertinent. For example, suppressing Network Events for Host CLI Actions.

Isolate Integrations

There are several reasons you might want to isolate an integration:

- You have an Integration that contains multiple products, such as ePO, and you don't want to see event IDs for modules that don't relate to your detection.
- You have the same Integration on multiple hosts and they are not receiving the same events. So, you suppress events from one or more so you can focus on the host that you suspect is misconfigured.
- You are comparing integrations to gain a perspective on how each of them are working.
- Events from some security controls are only going into one integration and not the other.

INTEGRATION QUERIES OVERVIEW

Integrations include queries that allow the Validation Platform to identify the events coming from security controls. Many of our integrations make the query configurable. This requires the owner of the control and the owner of the Validation Platform to communicate which modifications and tuning are appropriate given the tests being run and the controls being validated.

As an example, Splunk's query should only include indexes that store logs relevant to the Actions being run, which means you include indexes for firewalls but not web servers.

By default, a Job will query an integration for 15 minutes with a frequency of once every 30 seconds. You can configure both of these times in the Integrations' Advanced Settings section.

As the criteria for the queries age out of that window, they are removed from the query. When the query ages out, the security control no longer queries and the integration service moves into a sleep state waiting for more Actions to be run.

Some integrations have queries that you define based on your integration's settings. The most common query type is an overall query, but there might also be queries related to specific Action types or specific for the integration. The following tables show which queries are available for each integration, grouped by integration type.

When setting up Actors that will be used to run Host CLI Actions, always assign its Alternate Hostname. Integrations that support Host CLI-specific queries use the information in this field, as well as the simple hostname, when the %HOST_CLI_ACTOR_HOSTNAMES% variable is used.

SIEMs and Event Aggregators

SIEMs and Event Aggregators	Available Queries				
Technology Name	**General**	**Malicious DNS Action**	**Email Action**	**Host CLI**	**Special**
Alert Logic					
Alienvault USM / OSSIM	✔				✔
ArcSight ESM					✔
Azure Sentinel	✔	✔	✔	✔	
Chronicle Backstory					
Cisco Firepower	✔			✔	✔
Elasticsearch	✔	✔	✔	✔	
Exabeam Data Lake	✔	✔	✔	✔	

SIEMs and Event Aggregators	Available Queries				
Technology Name	**General**	**Malicious DNS Action**	**Email Action**	**Host CLI**	**Special**
Google BigQuery	✔	✔	✔		
Graylog					
Helix	✔	✔	✔	✔	
Juniper Secure Analytics (JSA)	✔	✔	✔	✔	✔
Logrhythm Elasticsearch	✔				
Logrhythm SQL	✔	✔	✔	✔	
Logzilla	✔	✔	✔	✔	
Trellix Enterprise Security Manager	✔	✔	✔	✔	
QRadar	✔	✔	✔	✔	✔
Splunk	✔	✔	✔	✔	✔
Splunk ES	✔	✔	✔	✔	✔
Sumo Logic	✔			✔	
Threat Stack					

Network Technologies

Network Technologies	Available Queries				
Technology Name	**General**	**Malicious DNS Action**	**Email Action**	**Host CLI**	**Special**
Check Point (also supports their NGFW)	✔				
RSA Netwitness	✔				
Security Onion - ELK	✔				

Network Technologies	Available Queries				
Technology Name	**General**	**Malicious DNS Action**	**Email Action**	**Host CLI**	**Special**
Security Onion - ELSA	✔	✔			
Cisco Firepower FMC	✔			✔	✔
CloudTrail					
CloudWatch	✔	✔	✔	✔	
Darktrace					
Exabeam Advanced Analytics					
Trellix (supports CMS, Email, NX)					
GuardDuty					
Trellix Network DLP	✔				
Palo Alto Network Firewalls & Panorama	✔				
Securonix SNYPR					
Threat Stack					
Tipping Point SMS					
VMware AppDefense					

Endpoint Technologies

Endpoint Technologies	Available Queries				
Technology Name	**General**	**Malicious DNS Action**	**Email Action**	**Host CLI**	**Special**
Carbon Black Cloud (Also works with Defense, PSC, and ThreatHunter)	✔				

Endpoint Technologies	Available Queries				
Technology Name	**General**	**Malicious DNS Action**	**Email Action**	**Host CLI**	**Special**
Carbon Black CB Protection					
Carbon Black CB Response	✔				
Cisco AMP					
Crowdstrike	✔				
Cybereason	✔				✔
Cylance PROTECT					
Microsoft Defender ATP					
EndGame					
Trellix Endpoint Security (HX)					
Trellix Endpoint Security	✔				
Trellix Network DLP	✔				
Netskope					
SentinelOne	✔				
Sophos Central					
Symantec DLP					
Symantec EP					
Threat Stack					
VMware AppDefense					

INTEGRATIONS - FIELD DETAILS

Before submitting events to the Director for processing, they need to be translated into the data structure that the Director expects. This is a dictionary of key value pairs where the key names must correspond to valid fields for the event objects in Director.

The following sections provides details for the fields used and criteria requirements to match events to Job Actions.

Event Fields

Some integrations have field mappings sections that tells the platform which fields from the integration to match against. To improve event matching to Job Actions, it is best practice to populate as many of the fields as possible for each event. The following integrations have these field mapping sections: Azure Sentinel, Azure LogAnalytics, Elasticsearch, FireEye Helix, Graylog, LogRhythm Elasticsearch, Logzilla, and Securonix SNYPR. There are other integrations, such as Splunk and Splunk ES, that will require similar configuration in the integration itself.

Field Name	Description
computer	An optional field for the computer name used when matching Host CLI Actions. When present, this is checked against the hostname known for the Actor involved in the Action.
description	A human-friendly description or name of the event.
dest_ip	For network events, the destination IP Address of the event. This is an optional field, but if present it must be a string of at most 255 characters. It can be an IP address in dotted-quad format, a hostname, or an FQDN.
dest_port	For network events, the destination port of the event. This is an optional field that should have an integer between 0 and 65535 when populated.
email_recipient	For events created in response to email Actions, this could be the username or email address of the email sender.
email_sender	For events created in response to email Actions, this could be the username or email address of the email sender.
email_subject	For events created in response to email Actions, this could be the subject of the email that was sent.
filehashes	Optional field for events that contain one or more hashes of files. If present, it is used when matching Actions where the hashes of the file is involved. This can contain multiple hashes, separated by a pipe character |, such as when an event has an MD5 and a SHA256 value.

Field Name	Description
host	This is what is displayed as the event source in the Director UI. In most cases it would be the sensor/device that generated the event, but it could be something different based on the needs of a specific integration.
raw_event	Whenever possible, this would be the original raw event (eg, in the case of a SIEM, it might be the log line received over syslog). If that's not available, a JSON dump of the raw event fields is typically used.
sid	A short identifier of the type of event. This is strictly optional and is not displayed in the UI or used for matching an event to a Job Action.
src_ip	For network events, the source IP Address of the event. It can be an IP address in dotted-quad format, a hostname, or an FQDN.
src_port	For network events, the source port of the event. This is an optional field that should have an integer between 0 and 65535 when populated.
start_time	The timestamp for the event. This should be a string in ISO8601 format to avoid problems with timezone differences.
url	Optional field that currently isn't displayed in the UI anywhere. However, it is used for matching Malicious DNS Query Actions. If you run that type of Action, the field should be the domain name.
user	An optional field for events that contain a username, for example events from certain endpoint products might have this. This is not currently shown in the UI or used for matching Job Actions.

Network Action Matching Criteria

There are specific criteria an event must meet to match a Network Job Action. In the following table, the Match Type column contains the string the platform uses to indicate the match. These strings can be seen in an API response.

Match Type	Description
actor_address/time/file hash	This match type is only available for Job Actions that use a file from the File Library. • The start_time of the event is within the Job Action began_at and ended_at times • One of the IP addresses in the event matches an Actor IP Address from the Job Action • The filehashes field in the event matches one of the files used in the Job Action
actor_address/time/port	• The start_time of the event is within the Job Action began_at and ended_at times • One of the IP addresses in the event matches an Actor IP address from the Job Action • The src_port and dest_port fields in the event match the Job Action conversations

Match Type	Description
actor_address/time/single_port	This match type is often encountered when the Job Action ran through a proxy to an AWS Actor. • The start_time of the event is within the Job Action began_at and ended_at times • One of the IP addresses in the event matches an Actor IP Address from the Job Action • Either the src_port or dest_port field in the event matches a Job Action conversation
address/port	• The source and destination IP addresses of the event match conversations from the Job Action • The source and destination ports of the event match conversations from the Job Action
address/port/time	• The source and destination IP addresses of the event match conversations from the Job Action • Source and destination ports of the event match conversations from the Job Action • The start_time field for the event is within the Job Action began_at and ended_at times
address/time	• The source and destination IP addresses of the event match conversations from the Job Action • The start_time field for the event is within the Job Action began_at and ended_at times • The event is missing the src_port or dest_port fields
address/time/job_action_no_ports	• The source and destination IP addresses of the event match conversations from the Job Action • The start_time field for the event is within the Job Action began_at and ended_at times • There are no ports recorded for the Job Action conversations (eg, for ICMP traffic)
dns:time/domain	The Job Action is a Malicious DNS Query. • The start_time of the event is within the Job Action began_at and ended_at times • The url field for the event is the domain requested in the Job Action
email:address/time	The Job Action is an email Action • The email_subject field for the event is blank • The start_time of the event is within the Job Action began_at and ended_at times • The email_sender and email_recipient fields for the event are present and match the email addresses used in the Job Action

Match Type	Description
email:subject/uid	The Job Action is an email Action. • The email_subject for the event is present • The subject ontains the Job Action's unique email identifier string
port_scan:address/time/single_port	The Job Action is a port scan Action. • The start_time of the event is within the Job Action began_at and ended_at times • The source and destination IP addresses of the event match conversations from the Job Action • A single port from the event matches one from the Job Action

Host CLI Action Matching Criteria

Host CLI Actions have a specific set of criteria that an event must meet that is similar, but different from Network Job Actions. In the following table, the Match Type column contains the string the platform uses to indicate the match. These strings can be seen in an API response.

Match Type	Description
host_cli:host/time	• The start_time of the event is within the Job Action began_at and ended_at times and the host or computer field for the event matches an Actor IP address or hostname from the Job Action • For hostnames, this match is case-insensitive
host_cli:host/time/filehash	• The event filehashes field is present and matches a file used in the Action • The event time is between the Job Action began_at and ended_at times using the Filehash Match time skew on the Integration Settings page • The host or computer field for the event matches an Actor IP address or hostname from the Job Action
host_cli:ip/time	• The start_time of the event is within the Job Action began_at and ended_at times and the src_ip or dest_ip field of the event matches the Actor's management IP address • For Protected Host CLI Actions, this can also match on the management IP address of the Protected Theater involved in running the Action

VARIABLES USED IN INTEGRATION QUERIES

The following table contains a list of Security Validation-provided variables that can be used in queries, and the type of queries where they can be used, if the integration supports that type of query.

Some integrations have special queries. For example, Splunk has a correlation query and Cisco Firepower has a file query and an Amp query. Rather than list these integration-specific queries separately, they are combined in one column.

TIP: If the integration in the platform doesn't have the query type indicated, you can't use that variable in a query. For example, %DOMAINS% can only be used by integrations that have a Malicious DNS Action Query.

	Query Type				
Variable	**General**	**Malicious DNS Action**	**Email Action**	**Host CLI**	Integration-specific
%DOMAINS%		✔			
%HOST_CLI_ACTOR_HOSTNAMES%				✔	
%ACTOR_IPS%	✔				✔
%END_TIME%	✔	✔	✔	✔	✔
%HOST_CLI_ACTOR_IPS%				✔	
%LAST_INDEX% (Splunk / Splunk ES)	✔	✔	✔	✔	✔
%RECIPIENTS%			✔		
%SENDERS%			✔		
%START_TIME%	✔	✔	✔	✔	✔

CORRELATED EVENTS

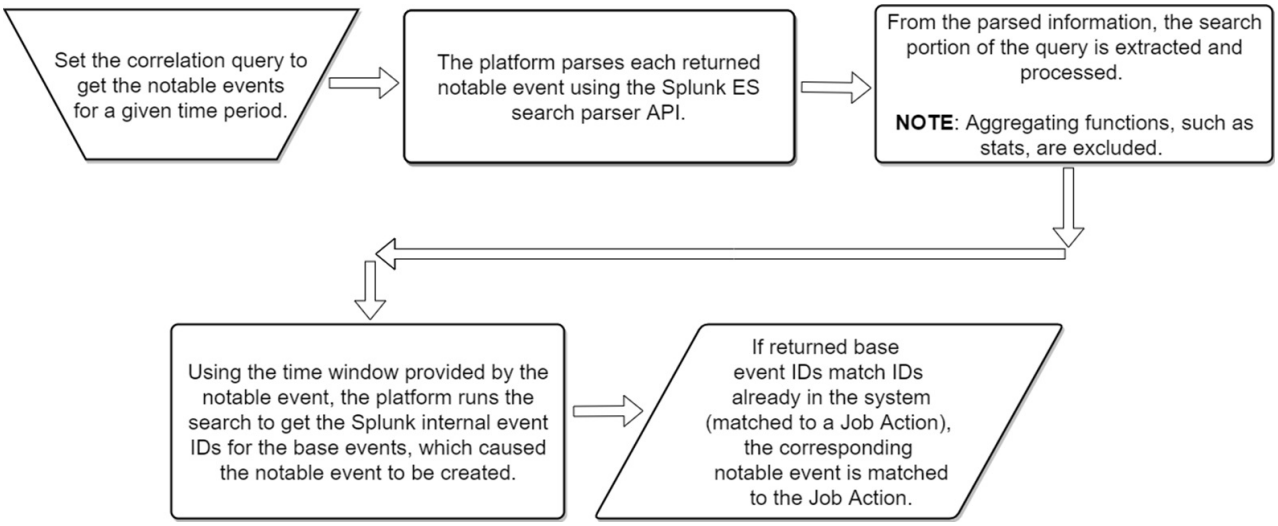
Event correlation is a method that uses security technology event data to analyze and identify relationships. Different events are connected to identifiable patterns through event correlation. If those patterns pose a threat to security, event correlation offers a full context and logical analysis through a sequence of related events. As a result, security analysts are able to make a well-thought-out decision on what to do next to respond and investigate.

The Security Validation integrations work on a premise of getting `raw_events` and `raw_alerts` from a security technology. Integrations convert raw events and alerts into a standard data model (such as `src_ip`, `dst_ip`, `host`) by means of translation. At this translation stage, the UID is determined for an event. Often times, it's a value that is taken from the security technology API data. However, not all technologies provide an acceptable UID. In these cases, a UID is synthesized by MSV through a process of combining multiple fields and generating a unique value. This UID for each event is fundamental to the alert, as it's the value that makes up the `base_events_uids` in the alert. If an event has a UID that matches a UID from the alert's `base_events_uids` list, it's considered to be correlated.

Not all events are correlated with an alert, and in certain systems, not all alerts will have a correlated `base_events_uids` list.

Correlated Events in Splunk Integration

As an example, consider the Splunk integration. In this integration, you can correlate events when the data is indexed. The Security Validation Platform matches correlated events to a Job Action only if one of its base events was matched to a Job Action. When a base event is matched, the platform uses the correlation query to find events that matched Actions and their corresponding base events. See the following image for an example of a correlation query workflow.



Example of a correlation query for Splunk ES

Event correlation is summarized in the following steps:

1. **Event Filtering**: In this step, you set the time period to get the notable events using a correlation query.
2. **Event Parsing**: Extract the search portion of the query and process it using the Splunk ES search parser API.
3. **Event Aggregation**: In this step, the exact duplicates of the same event are also merged. Such duplicates may have been caused by network instability. For example, suppose that the same event is sent twice by the event source. The first instance was not acknowledged in time, but both instances eventually arrived at the event destination.
4. **Get Splunk internal Event IDs**: Using the time window provided, the platform runs the search to get the Splunk internal event IDs for the base events.

5. **Root Cause Analysis**: It consists of analyzing dependencies between events. In this step, you detect whether some events can be explained by others. If the base event IDs match to a Job Action, the corresponding notable event is matched to the Job Action.

Intrusion detection is a scenario where event correlation can be used. For instance, suppose that an employee account has not been accessed for a long time and suddenly many login attempts are noticed. That account may start executing suspicious commands. Event correlation can be used in this scenario to send an alert that indicates an attack is in progress.

See **Splunk (https://docs.mandiant.com/home/msv-splunk)** and **Splunk Enterprise Security (https://docs.mandiant.com/home/msv-splunk-enterprise-security)** articles for more information and sample correlation queries.

SUSPICIOUS EVENTS / MISSING EVENTS

When the Director has an issue correlating an event with a job, it stores it as a Suspicious Event. This can happen for several reasons:

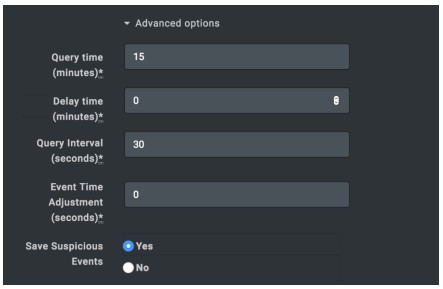
- If the event fails to match the Job's parameters. This occurs when the destination IP is missing.
- If there is an issue with the ports available in the logging.
- If the time of the events drifts from what the Director has observed from the time sources configured at job execution.

Saving Suspicious Events

Allowing Suspicious Events to be saved is a configuration tied to each Integration. By default, this is disabled.

TO SAVE SUSPICIOUS EVENTS

1. Go to **Settings** > **Integrations**.
2. If the Integration already exists, click **Edit**.
   If the Integration is new, click **Add Integration** and select the Integration.
3. Expand **Advanced options**.
4. Scroll to the bottom, and choose **Yes** to save suspicious events.
5. Click **Submit**.
   Suspicious Events are saved and viewable in the platform.



Saving Suspicious Events

Working with Suspicious Events

Access the list of suspicious events by:

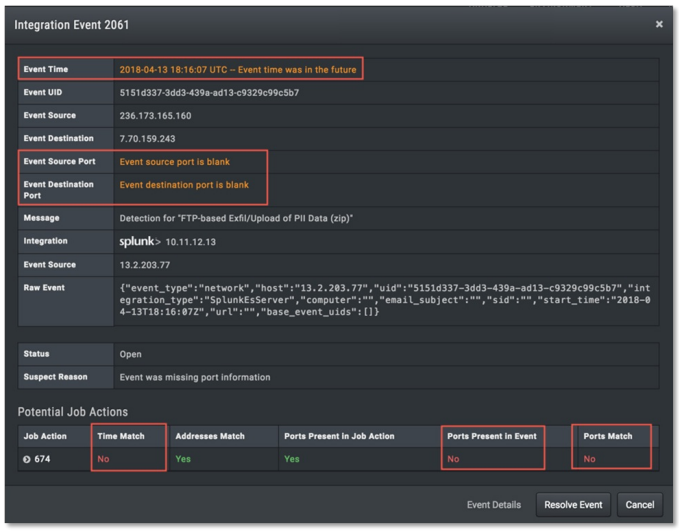
- Selecting the Jobs menu and choosing **Suspicious events**.
- Selecting a Job from the Process Job Actions page that is part of the Effectiveness Validation Process (EVP).
- Clicking the Suspicious Events icon for an Action on the Job Results page.
- Clicking the Suspicious Event Warning for an Action on the Job Results page.

(https://d383cql5uq169w.cloudfront.net/app/image/pid/620d7e13ccb103e8557b25b0/id/629a12dcc9cba0017c2f7e06/n/susp-events-missing-1.png)

Working with Suspicious Events

Clicking **View Event** on a Suspect Integration Event shows the Event details where you can see which fields of the event failed to match the job in two sections.

You can use this information to review the integration details and make or request any required changes.



Integration Event

Once you are satisfied that you have identified the root cause of the failure, click **Resolve event**, and enter information on why you're resolving the event.

When you click **Submit**, the event is removed from the page (but not added to the original job). If you have admin permissions, you can also delete suspect integration events. You can delete all, filtered, or selected events.

IMPORTANT: Deleting events is audited but cannot be reverted.

After the Integration and any other issues have been resolved, rerun the job to verify the changes have resolved the issue and that you aren't seeing the same suspicious events.

Deleting Suspicious Events

The Validation Platform can be configured to automatically remove old Suspicious Events. This helps free up disk space and is more efficient than removing them from the Suspicious Events page.

TO DELETE OLD SUSPICIOUS EVENTS:

1. Go to **Settings** > **Director Settings**.
2. Select **Integrations**.
3. Select **Yes** for Delete old Suspicious Events
4. Enter the number of days they should be kept and click **Update Integration Settings**.

NOTE: At minimum, you must keep them for a day.