Mandiant

ARCSIGHT INTEGRATION WITH SECURITY VALIDATION

This integration provides the following benefits:

- Validates that security tools are writing log events to Arcsight to ensure compliance with security policies and regulations
- Collects events generated by security tools that write to Arcsight to test the efficacy and configuration of security controls using Security Validation jobs

Use this document to configure the integration using one of the following methods:

- MSI Integration (Supported and recommended for new integration configurations)
- Legacy Integration (Supported for existing integration configurations)

Configure MSI Integration

This method is the recommended approach for configuring new integrations in Security Validation.

To configure an integration, this document walks you through the following high-level steps:

1. Configure the third-party technology
2. Configure Security Validation
3. Verify connectivity

Configure Arcsight

API Calls

API	Usage
`/detect-api/rest/queryviewers/matrixData/{query_viewer_id}`	Retrieve a list of events from a query viewer in Arcsight
`/detect-api/rest/license/info`	Used to test connectivity and authentication settings
`/detect-api/rest/queryviewers/name/{query_viewer_name}`	Retrieve information about a query viewer in Arcsight
`/www/core-service/rest/LoginService/login/`	Authenticate and retrieve an auth token from Arcsight
`/www/core-service/rest/LoginService/logout/`	Log out from Arcsight

Supported Versions

Arcsight 7.5

Information to gather before you start:

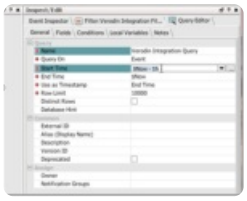
To configure this integration, you need:

- A valid username and password for a user with permissions to use the API endpoints described in the previous step
- The hostname or IP address of your Arcsight instance
- You are ready to configure the integration.

Configure 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`.

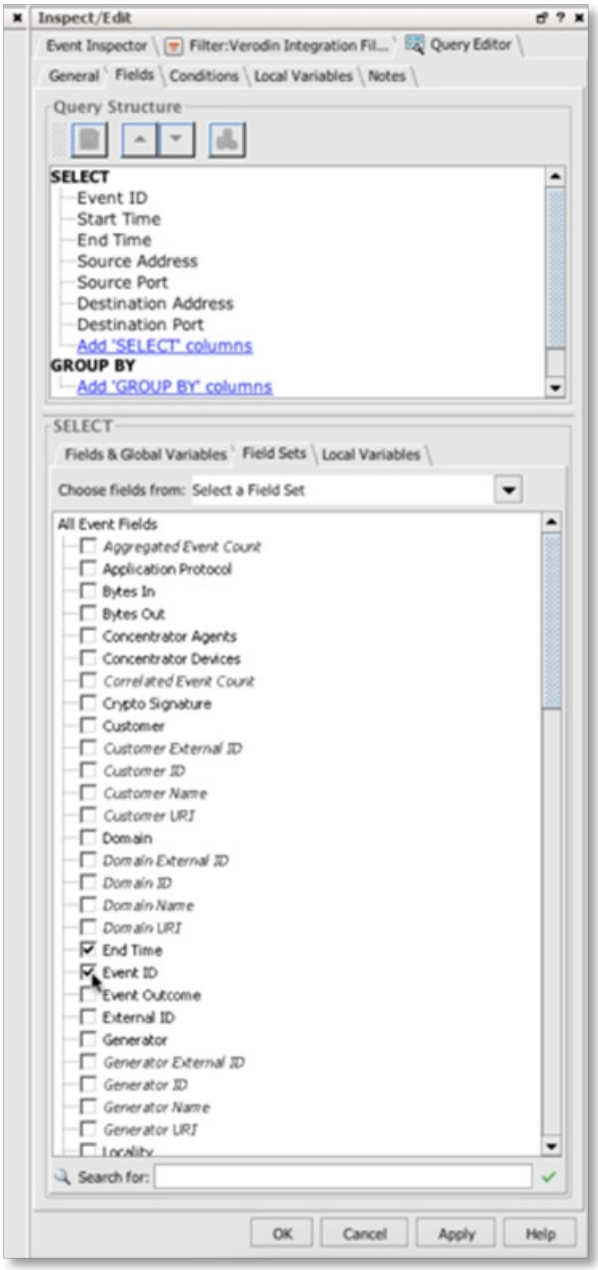


(https://dyzz9obi78pm5.cloudfront.net/app/image/id/629a12eac9cba0017c2f7e8e/n/arcsight-query.png)

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.

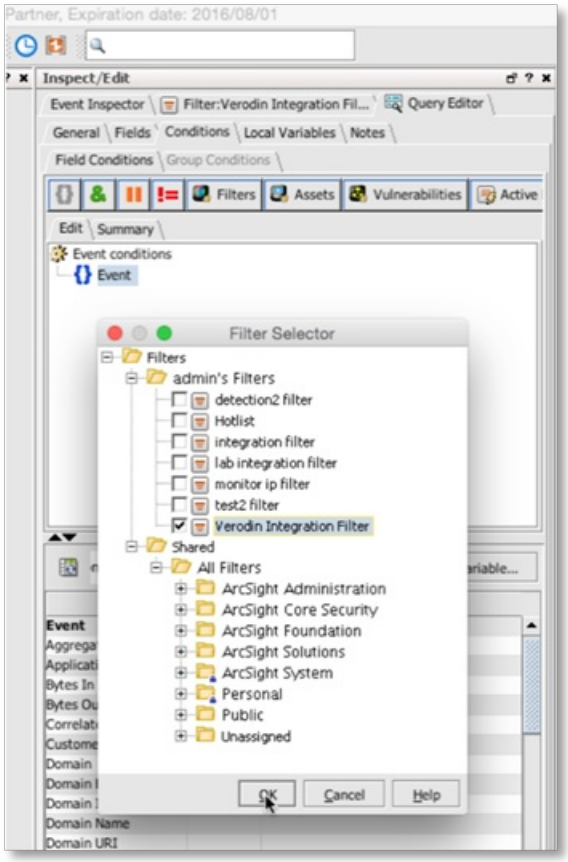


Add Fields to Query

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.

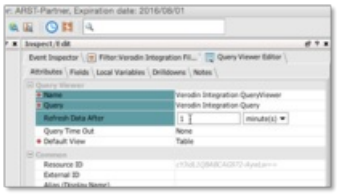
> This query name must be unique across the entire ArcSight ESM. If there is another query with the same name for any user, the integration will not work correctly.

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

(https://dyzz9obi78pm5.cloudfront.net/app/image/id/629a12e4c9cba0017c2f7e63/n/arcsight-7.png)

Set Query

e. Set the refresh interval to 1 minute.



(https://dyzz9obi78pm5.cloudfront.net/app/image/id/629a12e1c9cba0017c2f7e3f/n/arcsight-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.

Configure Security Validation

1. Go to **Settings** > **Integrations**.
2. From the Integrations table, click **Add Integration > Arcsight**.

> You can add this as either a Direct or Remote Integration.

3. Enter a meaningful **Integration Name**.
4. Optional: From the **Proxy** drop-down, choose a proxy profile if one is available. If one isn't available and all outbound connections go through a proxy, first, set up a **Proxy Rule** (https://docs.mandiant.com/home/msv-proxy-rules).
5. Optional: Change the **HttpProtocols** value to determine what protocol is used for requests (**Http** or **Https**).
6. Enter the ArcSight instance domain or IP value for the **Host**. The default is **httpbin.org** (https://httpbin.org).
7. Enter a **Port** value. The default is **443**.
8. Enter the **Username** and **Password** for the account with permissions to use the API endpoints.
9. Optional: Enter the **AWS Session Token**.
10. Optional: Check **Verify Ssl** if you want this verification done for requests to an upstream server.
11. Optional: Change the **Timeout** value if you want a different frequency of requests to an upstream server. The default is **30** (seconds).
12. Optional: Enter the **Query Viewer Name** as shown in the Arcsight console.

13. Optional: Enter the **Alerts Query Viewer Name** as shown in the Arcsight console.
14. Optional: Modify the **Field Map** values, as necessary.

    - Each field map box can hold a JSON-formatted comma-separated list of columns returned by the API to be considered for each field when translating into the normalized event object format. Example: description could be configured to be 'msg_s' or 'SyslogMessage' in some environments. The field map tries both if set to: ['msg_s','SyslogMessage'] and whichever matches first is the column that is used.
    - When configuring an integration in Security Validation, you can assign additional host values in the Field Map settings. If none of the assigned fields return a valid host name, Network Actions may miss matched events from the third-party technology. Additional hosts values helps ensure the likelihood of a match between the two environments.

15. Optional: Modify the **Page Size** to change the request for the upstream server. The default is **500**.
16. Optional: Expand **Advanced options** and update the information as necessary.
    a. 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.

    b. Update **Query Interval** (seconds).
    c. Configure correlation queries:
        i. Select **Correlation Query Enabled** and fill in the **Correlation Query**.
        ii. Modify the **Correlation Query Interval**, if necessary (minutes).
    d. Select **Discover network devices automatically**, the default and recommended option.

    If unselected, reported events won't include product information for any matching network security technology.

    e. Select **Save Suspicious Events**.
    f. Modify the **Event Time Adjustment** (seconds). The default is **0**.
    g. Modify the **Limit** value if you need to prevent a flood of results. This value is set to **10000** by default. This limit applies to both events and alerts individually, so if you set it to **10**, you can still see a maximum of 10 events and 10 alerts.

17. Click **Save**.

Verify connectivity

1. Go to **Settings > Integrations**.

2. From the Direct Integrations table, 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.

For more information on setting up queries, see **Manage Integrations (https://docs.mandiant.com/home/msv-managing-integrations)**.

Configure Legacy Integration

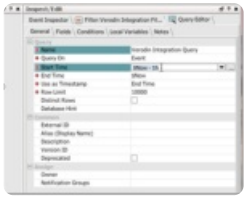
> This document applies to Classic/Legacy Integrations. You may continue to use these integration configurations. While no active development is happening for these integrations, we continue to provide Classic/Legacy Integrations in the product. You do not have to move to MSI Integrations. If your support engineer or TSC recommends or you choose to move to MSI Integrations, you can take advantage of the latest features and functionality. For more information, see the MSI Integration documentation in the **Integrations Overview (https://docs.mandiant.com/home/msv-integrations-overview)**.

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` .

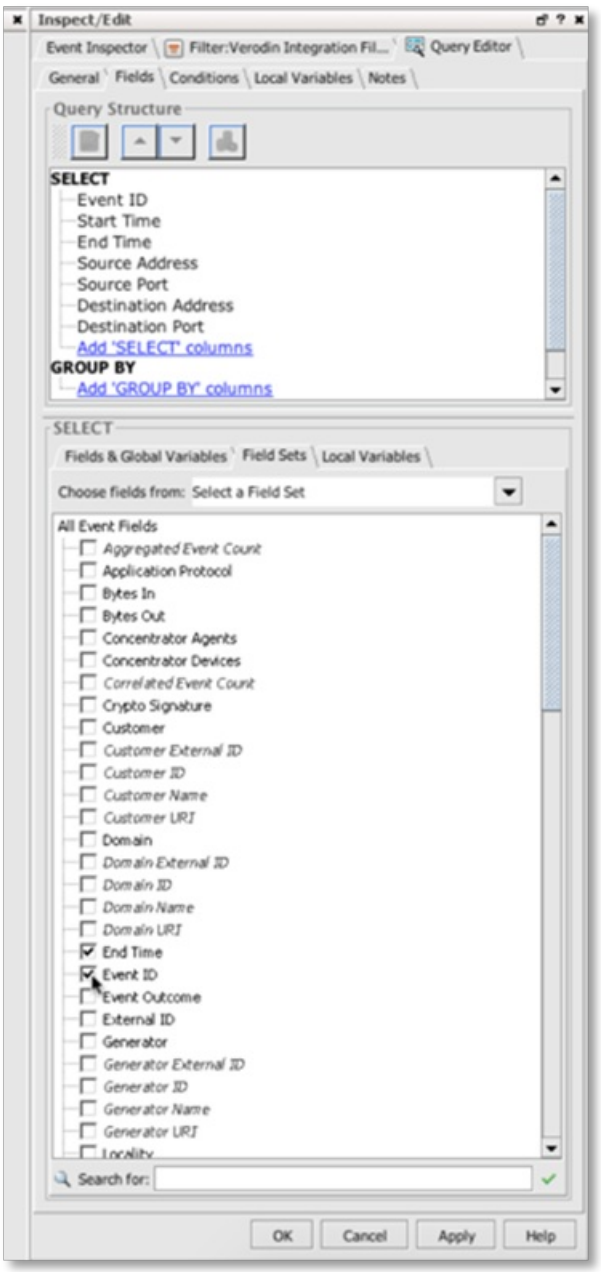


(https://dyzz9obi78pm5.cloudfront.net/app/image/id/629a12eac9cba0017c2f7e8e/n/arcsight-query.png)

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.

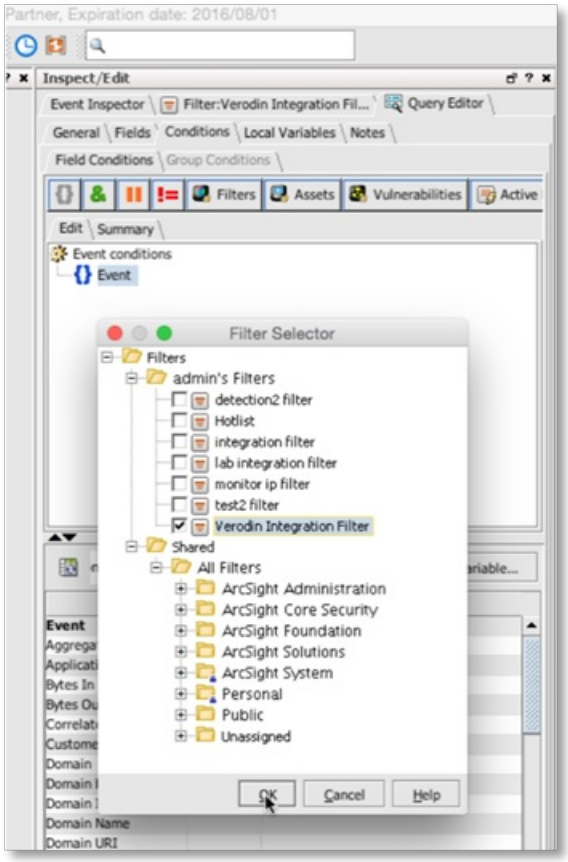


Add Fields to Query

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.

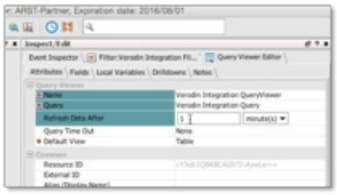
> This query name must be unique across the entire ArcSight ESM. If there is another query with the same name for any user, the integration will not work correctly.

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

(https://dyzz9obi78pm5.cloudfront.net/app/image/id/629a12e4c9cba0017c2f7e63/n/arcsight-7.png)

Set Query

e. Set the refresh interval to 1 minute.



(https://dyzz9obi78pm5.cloudfront.net/app/image/id/629a12e1c9cba0017c2f7e3f/n/arcsight-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://dyzz9obi78pm5.cloudfront.net/app/image/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://dyzz9obi78pm5.cloudfront.net/app/image/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.