ARCSIGHT

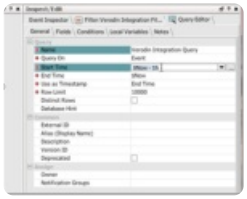
This document applies to Classic/Legacy Integrations. You may continue to use these integration configurations. While no active development is happening for these integrations, we continue to provide Classic/Legacy Integrations in the product. You do not have to move to MSI Integrations. If your support 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`.

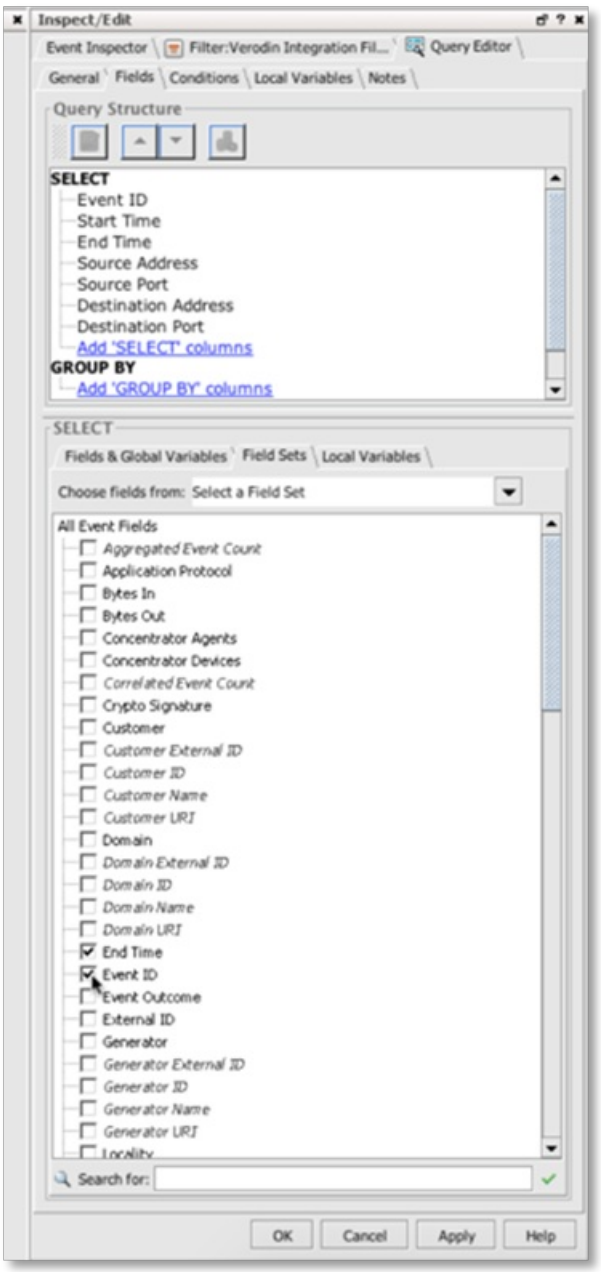


(https://dyzz9obi78pm5.cloudfront.net/app/image/id/629a12eac9cba0017c2f7e8e/n/arcsight-query.png)

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.

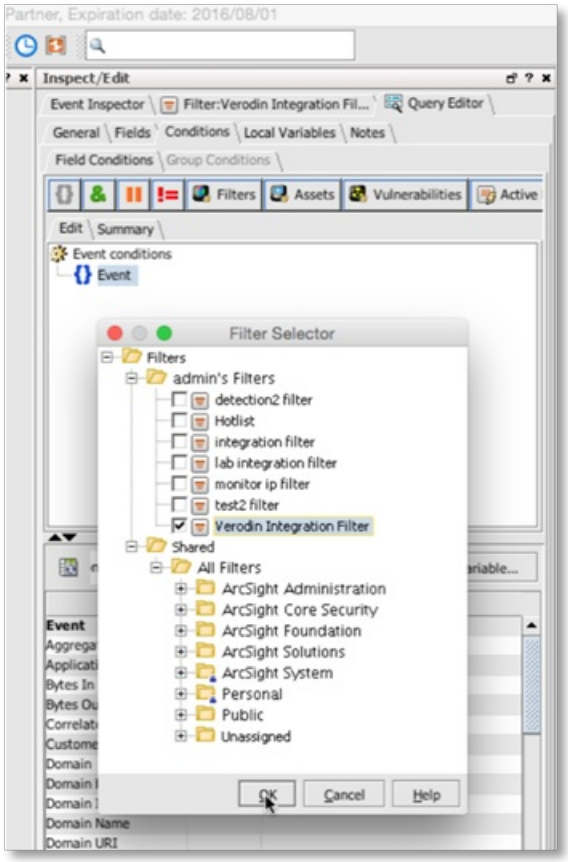


Add Fields to Query

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.

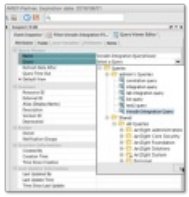


Set Filter

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.

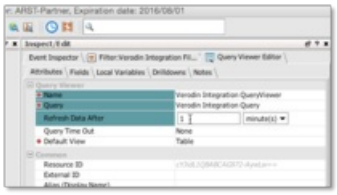
d. Set the query to the one created in the previous step.



(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.