Mandiant

SYMANTEC DLP INTEGRATION WITH SECURITY VALIDATION

This integration collects events generated by Symantec DLP to test the efficacy and configuration of the security control using Security Validation jobs.

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

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

Configure MSI Integration

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

API Calls

API	Usage
`/ProtectManager/webservices/v2/incidents`	Query for events from Symantec DLP
`/ProtectManager/webservices/v2/incidents/statuses`	Used to test connectivity and authentication settings

Supported Versions

All

Before You Begin

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 Symantec DLP instance

Configure Security Validation

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

   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. For the **Host**, enter the hostname of your Symantec DLP instance.
6. Enter a **Port** value. The default is **443**.
7. Change the **HttpProtocols** to use for requests. (**Https** or **Http**.)
8. Enter the **Username** and **Password** for the account the can access the API endpoints.
9. Optional: Change the **Timeout** value if you want a different frequency of requests to an upstream server. The default is **30** (seconds).
10. Optional: Check **Verify Ssl** if you want this verification done for requests to an upstream server.
11. From the **TimeZones** dropdown, select the time zone associated with the Symantec DLP instance.
12. Optional: Add or remove **Queries**, as needed. A default entry is provided.
13. 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.

14. 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. Select **Correlation Query Enabled** and fill in the **Correlation Query**.
    d. Modify the **Correlation Query Interval**, if necessary (minutes).
    e. 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.

    f. Select **Save Suspicious Events**.
    g. Modify the **Event Time Adjustment** (seconds). The default is **0**.
    h. 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.

15. 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 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.

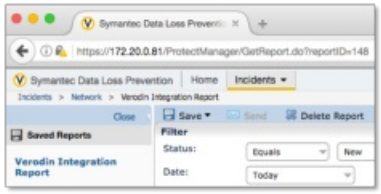
   This user can only be assigned one role.

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

   - `<Username>:<Active_Directory_Domain_In_Upper_Case>`
     or
     `<Role>\<Username>:<Active_Directory_Domain_In_Upper_Case>`
   - 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=<NUMBER>` .



(https://dyzz9obi78pm5.cloudfront.net/app/image/id/629a12d4c9cba0017c2f7dba/n/symantec-dlp.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

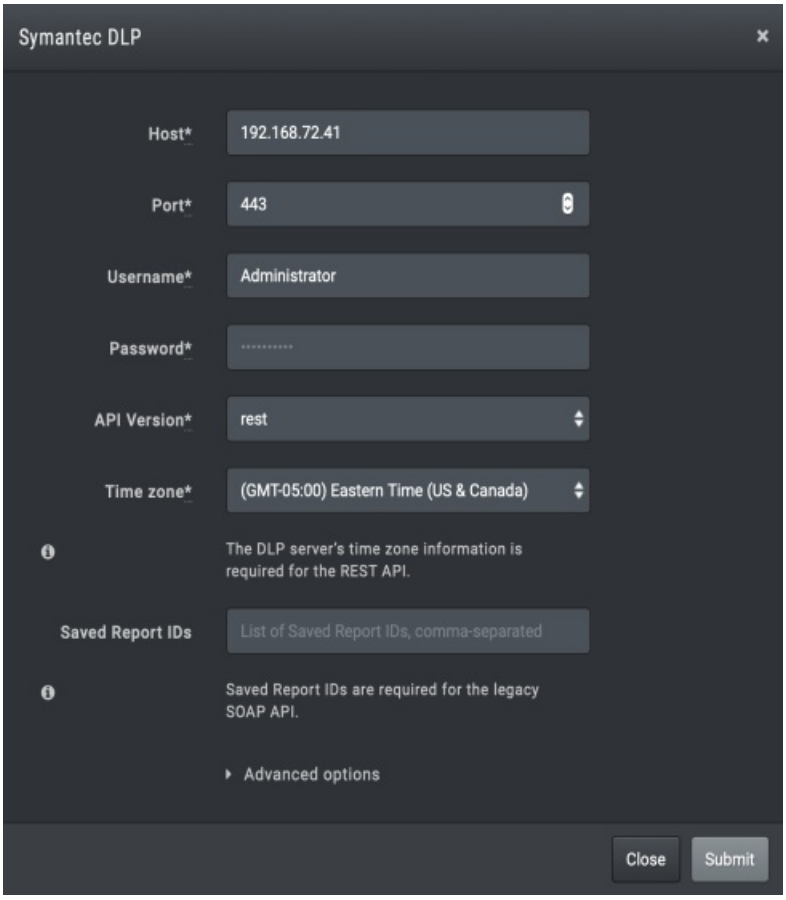
Information to gather before you start:

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.