Mandiant

SYMANTEC DATA LOSS PREVENTION (DLP)

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.

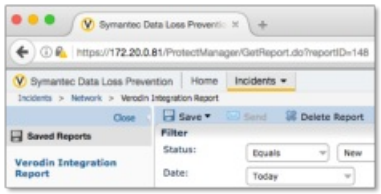
   This user can only be assigned one role.

   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

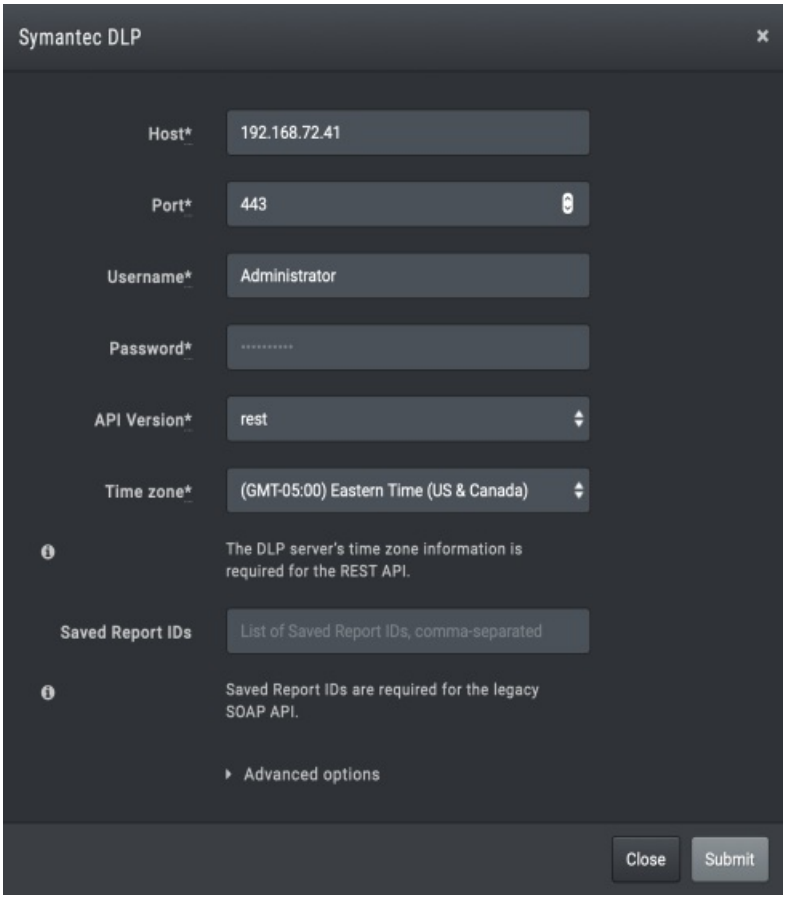
Information to gather before you start:

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.