SYMANTEC ENDPOINT PROTECTION

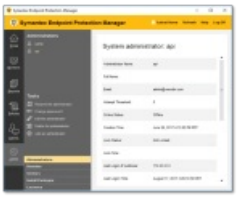
This document applies to Classic/Legacy Integrations. You may continue to use these integration configurations. While no active development is happening for these integrations, we continue to provide Classic/Legacy Integrations in the product. You do not have to move to MSI Integrations. If your support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

Update Symantec EP

TO UPDATE SYMANTEC EP

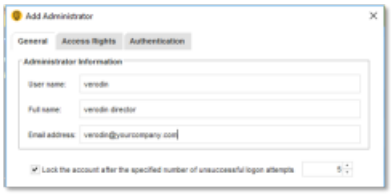
1. Log in to the Symantec Endpoint Protection Manager.
2. Create an admin user.
    a. Click **Admin** in the left-hand pane and select **Add an administrator**.



(https://dyzz9obi78pm5.cloudfront.net/app/image/id/629a12d7c9cba0017c2f7dd8/n/symantec-ep-1a.png)

Create Symantec Endpoint Protection administrator

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



(https://dyzz9obi78pm5.cloudfront.net/app/image/id/629a12e8c9cba0017c2f7e84/n/symantec-ep-1.png)

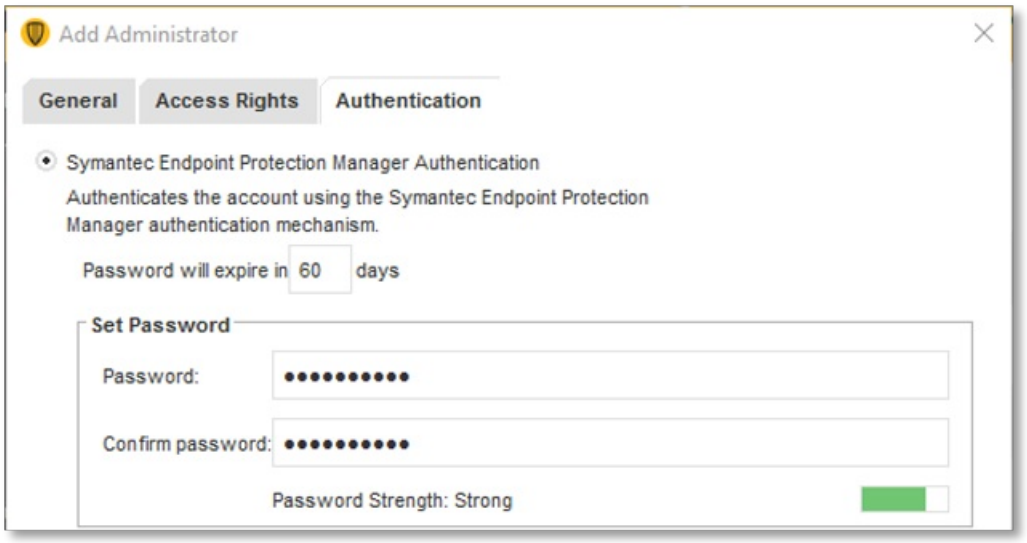
Enter Administrator information

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

(https://dyzz9obi78pm5.cloudfront.net/app/image/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:

- `<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

Syncronize Systems

Mandiant

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://dyzz9obi78pm5.cloudfront.net/app/image/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.