

SOPHOS CENTRAL

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 \(https://docs.mandiant.com/home/msv-integrations-overview\)](https://docs.mandiant.com/home/msv-integrations-overview).



This integration is remote capable.

Update Sophos Central

TO ADD A TOKEN TO SOPHOS CENTRAL

1. Open Sophos Central's admin console.
2. Go to **Global Settings** and select **API Token Management**.
3. Click **Add Token**, enter the necessary information, and save your changes.
4. Make a note of both the authorization token and API key.

Update the Validation Platform

Prerequisites

Information to gather before you start:

- Authorization token and API key for Sophos Central.
- The API URL for Sophos.

Configuration

TO ADD THE SOPHOS CENTRAL INTEGRATION

1. Go to **Settings > Integrations**.
2. Click **Add Integration > Sophos Central**
3. Enter **Host**, using the API URL for Sophos Central.
4. Set **Port** to 443.
5. Set **Protocol** to HTTPS.
6. Enter the authorization token and key from Sophos Central.
7. Expand **Advanced options** and update the information if necessary.
8. Click **Submit**.



(<https://dyzz9obi78pm5.cloudfront.net/app/image/id/629a12e0c9cba0017c2f7e39/n/sophos.png>)

Sophos Central Integration

Verify connectivity

TO VERIFY CONNECTIVITY TO SOPHOS CENTRAL

Click **Test** to verify that:

- The Director can communicate with Sophos Central on the port specified.
- The Authorization token and API key are valid and working.