Sophos Integration

Overview

The Sophos Central integration allows you to monitor Alerts and Events logs. Sophos Central is a cloud-native application with high availability. It is a cybersecurity management platform hosted on public cloud platforms. Each Sophos Central account is hosted in a named region. Sophos Central uses well-known, widely used, and industry-standard software libraries to mitigate common vulnerabilities.

Use the Sophos Central integration to collect logs across Sophos Central managed by your Sophos account. Visualize that data in Kibana, create alerts to notify you if something goes wrong, and reference data when troubleshooting an issue.

Compatibility

The Sophos Central Application does not feature version numbers. This integration has been configured and tested against **Sophos Central SIEM Integration API version v1**.

Requirements

You need Elasticsearch for storing and searching your data, and Kibana for visualizing and managing it. You can use our hosted Elasticsearch Service on Elastic Cloud, which is recommended, or self-manage the Elastic Stack on your own hardware.

Setup

Elastic Integration for Sophos Central Settings

The Elastic Integration for Sophos Central requires the following Authentication Settings in order to connect to the Target service:

- Client ID
- Client Secret
- Grant Type
- Scope
- Tenant ID
- Token URL

NOTE: Sophos central supports logs only upto last 24 hrs.

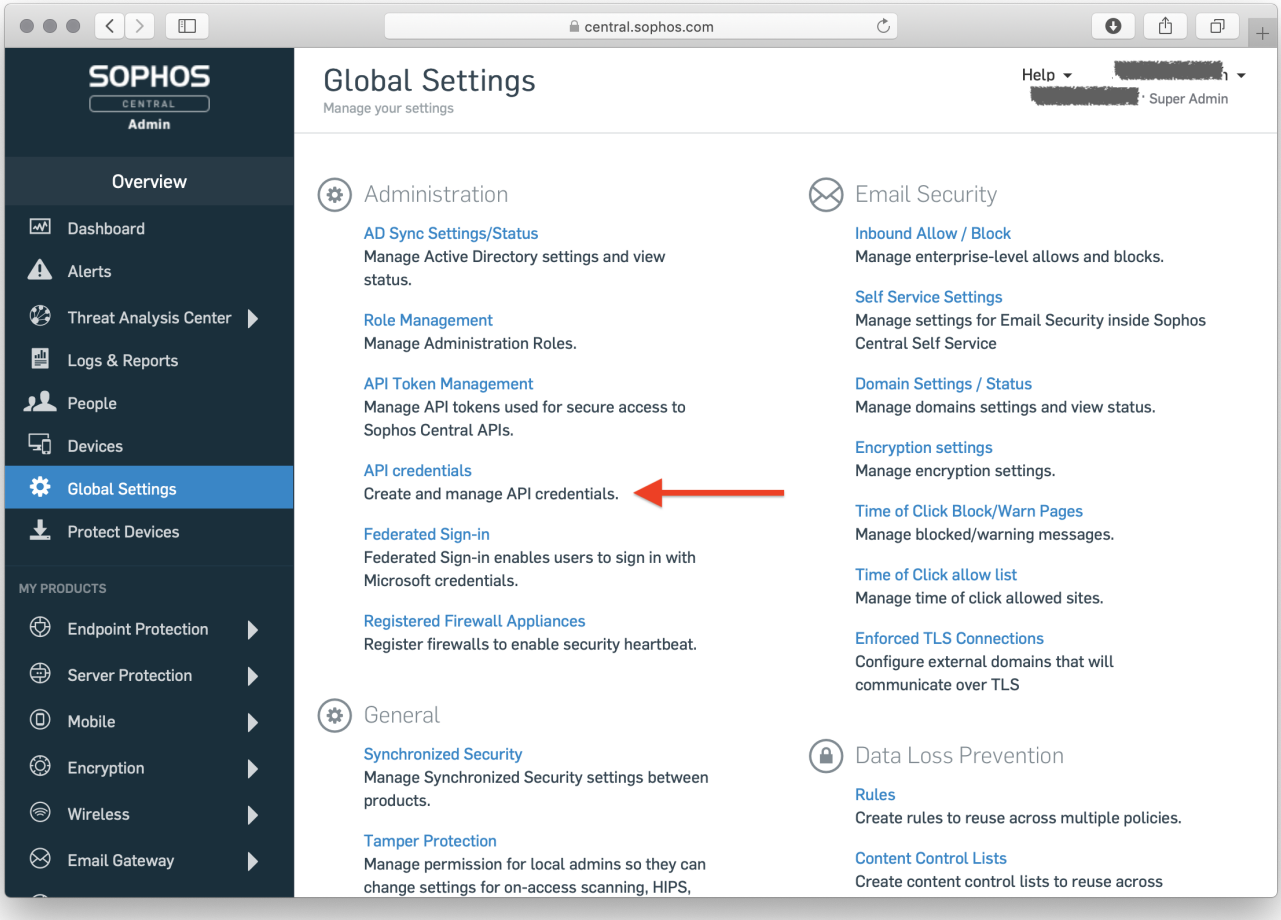
Step 1 - Create a service principal

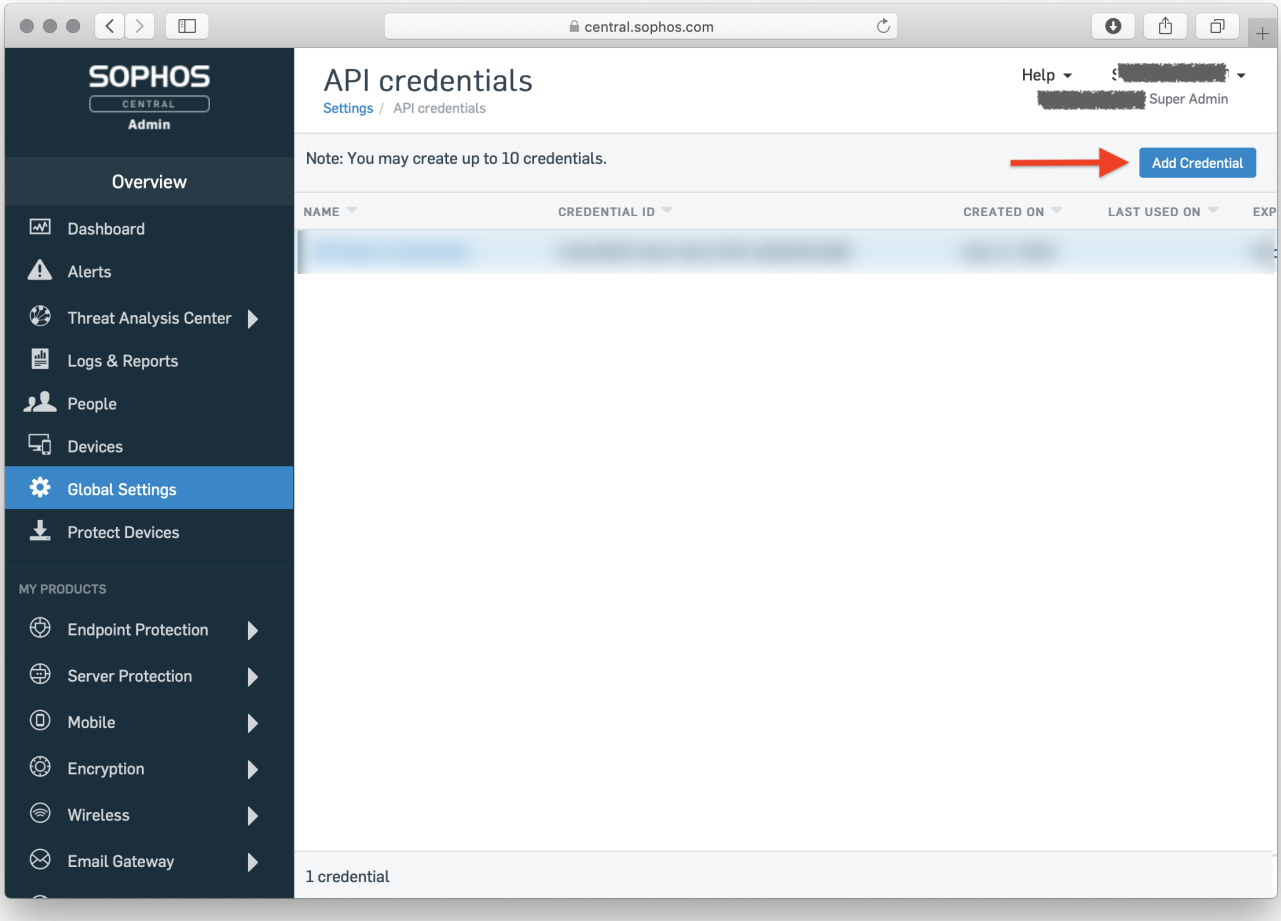
We will show you how you can sign in to Sophos Central Admin and create a service principal. You need to have the Super Admin role to do this.

Step 1a - Sophos Central Admin

Sign in to Sophos Central Admin. Go to https://central.sophos.com/manage.

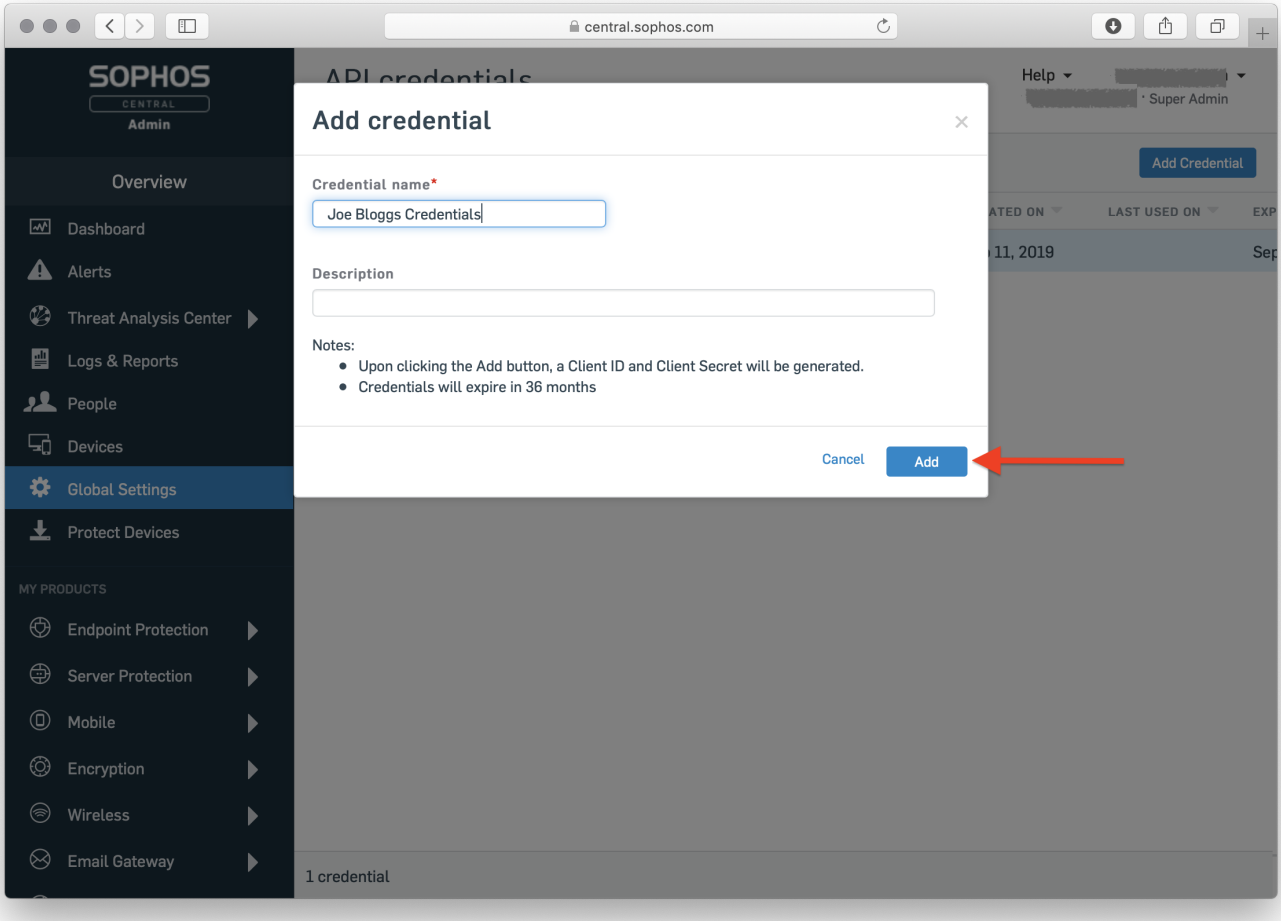
Click 'Global Settings' and then click the "API Credentials" link.





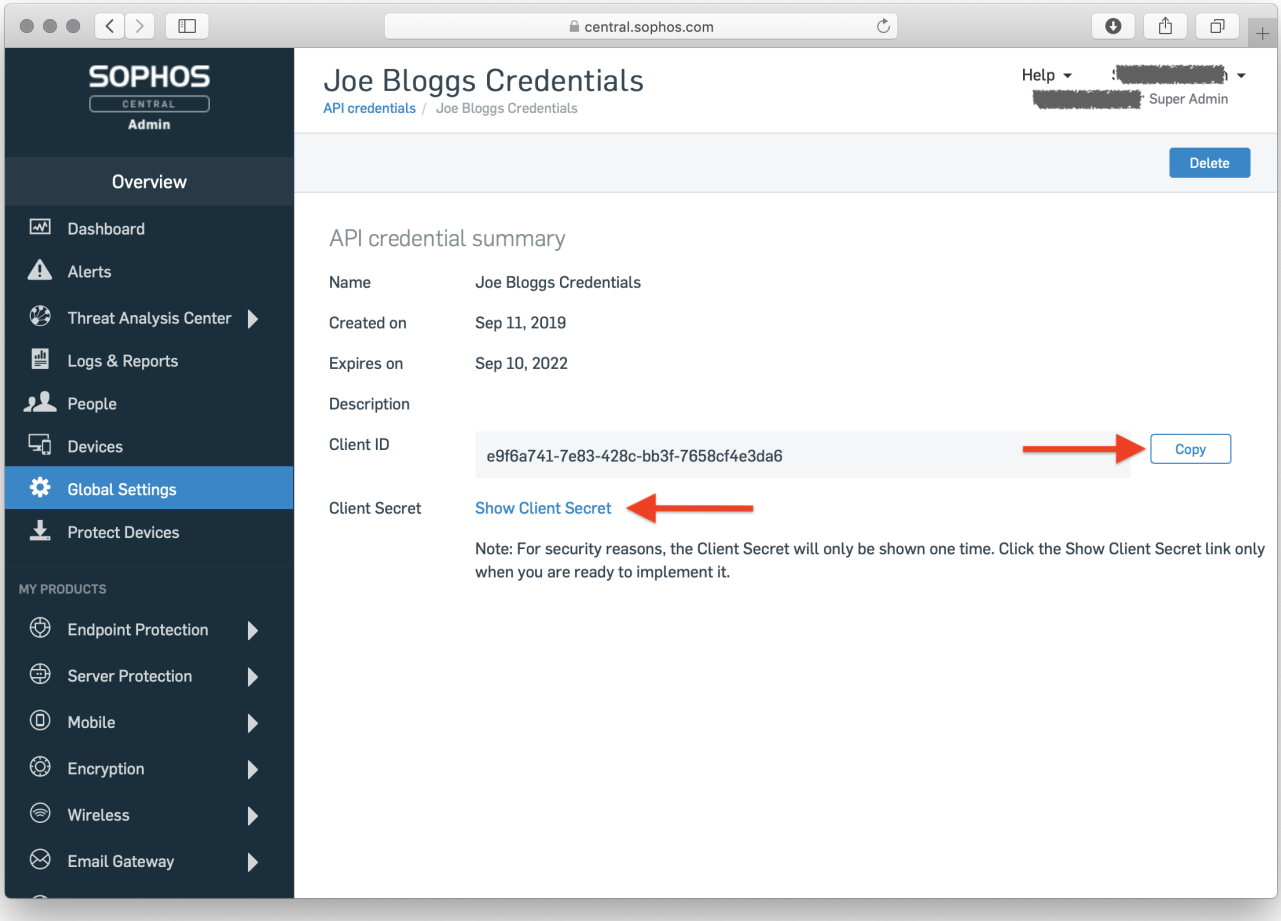
Step 1b - Add a new set of credentials

Supply a name for your credential set and a description, then click 'Add' as shown in the example below.

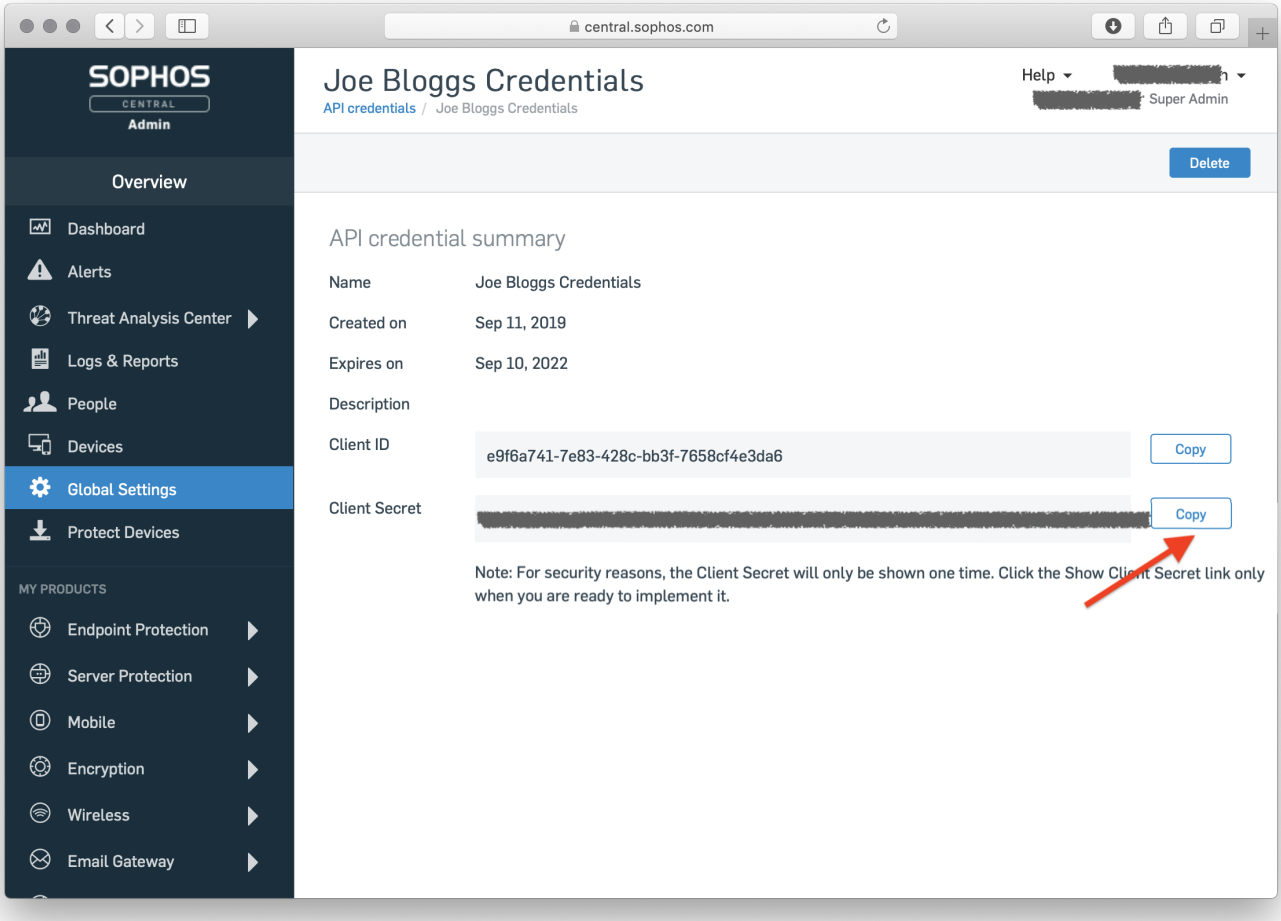


Step 1c - Grab your client ID and secret

Click 'Copy' to note down the client ID. Also show the client secret.



Click 'Copy' to note down the client secret.



⚠ **WARNING:** It is your responsibility to store your client ID and secret securely. If these are lost or stolen, an attacker will be able to call APIs on your behalf and steal your data or cause damage.

If you need further assistance, kindly contact our support at info@cytechint.com for prompt assistance and guidance.

Revision #2
Created 31 October 2024 03:38:58
Updated 31 October 2024 05:13:47