NG SIEM - Sophos Central Integration

Sophos Central Integration

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.

Step-by-Step: How to Get Your Sophos Central API Credentials (Client ID, Client Secret, Tenant ID, Request URL)

1. **Log in to Sophos Central Admin** Open your browser and go to:

   https://central.sophos.com Log in with your admin account.
2. **Go to API Credentials Manager** On the left sidebar, click **Global Settings** (gear icon at the bottom). Then click **API Credentials Manager**.
3. **Create a new credential** Click the blue button **+ Add Credential** (top right).
4. **Fill in the details**
   - **Name**: Give it a clear name (e.g., “PowerShell Automation”, “SIEM Integration”, “My Script 2025”)
   - **Role**: Choose the role that matches what you need (usually “Admin” or “Read-Only” is fine)
   - Click **Save** (or **Add**)
5. **Copy the four pieces of information immediately** A new window/pop-up will appear showing:

What you need	Value shown in the portal	Action
Client ID	Long string (e.g., 12345678-abcd-1234-efgh-1234567890ab)	Copy it

What you need	Value shown in the portal	Action
Client Secret	Long secret key	COPY THIS NOW – it will never be shown again!
Tenant ID (Customer ID)	GUID like a1b2c3d4-e5f6-7890-g1h2-i3j4k5l6m7n8	Copy it
Request URL	Use the Whoami endpoint first:	Always use this URL first:
	https://api.central.sophos.com/whoami/v1	

→ Click **Copy** buttons or select + Ctrl+C for each field. → Paste everything into a secure password manager or your script immediately.

6. **Close the window** Once you've copied everything, click **Done** or close the pop-up.

> **Please provide the following information to CyTech:**

- **Client ID:**
- **Client Secret:**
- **Tenant ID:**
- **Request URL:**

Revision #2
Created 23 September 2025 08:16:07 by Richmond Abella
Updated 17 November 2025 09:55:12