

Date: Monday, 09 June 2025

Overview

This workflow identifies machines listed in Active Directory or Entra that are missing from Sophos Central, and flags devices as suspicious if they are reporting to the directory, but not to Sophos Central for over three days longer.

The Entra comparison focuses on devices that are either *AzureDomainJoined* or *OnPremiseCoManaged*.

Please ensure all relevant systems, including servers, are properly synced to Entra, as incomplete syncing can result in inaccurate or incomplete reports.

Requirements

Python Installation

Install Python 3 for your operating system using the official guide:

Make sure to tick the - Add Python to PATH at the bottom of the screen below



<https://www.python.org/downloads/>

Required Python Modules

Module	Purpose
requests	For making API calls to Sophos Central
ldap3	For querying Active Directory
msal	For Azure Entra authentication

Installation (Windows)

1. Open **Command Prompt as Administrator**
2. Run:
3. `python -m pip install requests ldap3 msal`

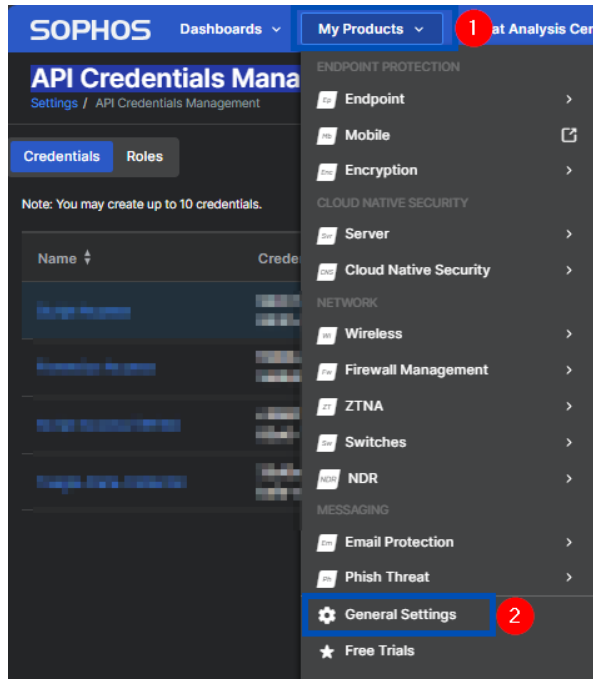


Installation (Mac)

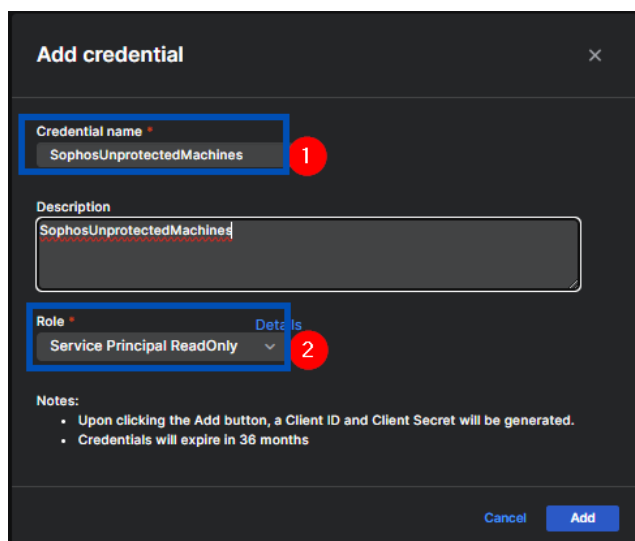
1. Open **Terminal**
2. Run:
3. `python3 -m pip install requests ldap3 msal`

Set Up Sophos Central API Access

1. Log in to **Sophos Central Admin**
2. Go to **My Products** → **General Settings** → **API Credentials Management**



3. Click **Add**
4. **Select the Credential Name: e.g** SophosUnprotectedMachines
5. Select **Service Principal - Read-Only**

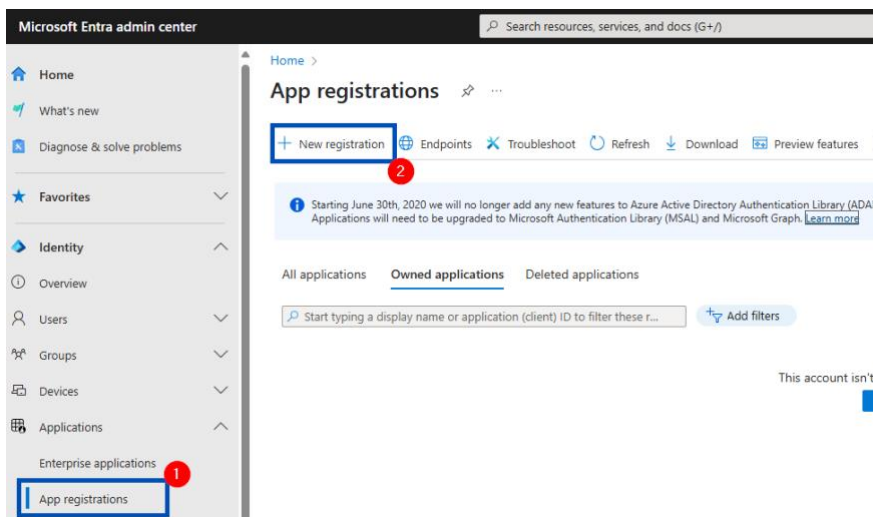


6. Save the **Client ID** and **Secret** securely.

You will not be able to view the secret again.

Set Up Azure Entra Application

1. Log in to the **Azure Portal**: <https://portal.azure.com>
2. Navigate to **Azure Active Directory** → **App registrations**
3. Click **+ New registration**



- **Name:** e.g., SophosUnprotectedMachines
- **Supported account types:** *Accounts in this organizational directory only* (Single Tenant)
- **Redirect URL:** Platform: **Web** > URL: <https://central.sophos.com>

Register an application

* Name

The user-facing display name for this application (this can be changed later).

SophosUnprotectedMachines 1

Supported account types

Who can use this application or access this API?

☒ Accounts in this organizational directory only (Sophos Professional Services E5 only - Single tenant) 2

☐ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)

☐ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

☐ Personal Microsoft accounts only

[Help me choose...](#)

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web 3 <https://central.sophos.com>

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from [Enterprise applications](#).

By proceeding, you agree to the [Microsoft Platform Policies](#)

Register 4

- Click **Register**

Get Your App Credentials

After registering the app, go to its **Overview** page:

- Copy **Application (client) ID** → This is your Entra_ClientID
- Copy **Directory (tenant) ID** → This is your Entra_TenantID

The screenshot shows the 'Overview' page for the application 'SophosUnprotectedMachines'. The left sidebar contains navigation options: Overview, Quickstart, Integration assistant, Diagnose and solve problems, Manage, Branding & properties, and Authentication. The main content area has a 'Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer). →' message. Below this is the 'Essentials' section with the following details:

- Display name: [SophosUnprotectedMachines](#)
- Application (client) ID: [31ee3f54-...](#) (labeled 1) → **Entra_ClientID**
- Object ID: [73172170-...](#)
- Directory (tenant) ID: [e66c4ee6-...](#) (labeled 2) → **Entra_TenantID**
- Supported account types: [My organization only](#)
- Client credentials: [Add a certificate or secret](#)
- Redirect URIs: [1 web, 0 spa, 0 public client](#)
- Application ID URI: [Add an Application ID URI](#)
- Managed application in I...: [SophosUnprotectedMachines](#)

Create a Client Secret

1. Go to **Certificates & secrets**
2. Click **+ New client secret**
 - Description: SophosUnprotectedMachines_Secret
 - Expiry: 12 months

The screenshot shows the 'Certificates & secrets' page for the application 'SophosUnprotectedMachines'. The left sidebar has 'Certificates & secrets' highlighted (labeled 1). The main content area shows 'Client secrets (0)' and a '+ New client secret' button (labeled 2). The 'Add a client secret' dialog is open with the following details:

- Description: [SophosUnprotectedMachines_Secret](#) (labeled 3)
- Expires: [365 days \(12 months\)](#) (labeled 4)
- Buttons: **Add** (labeled 5) and Cancel

- Click **Add**

3. Copy the **Secret Value** immediately → This is your Entra_ClientSecret

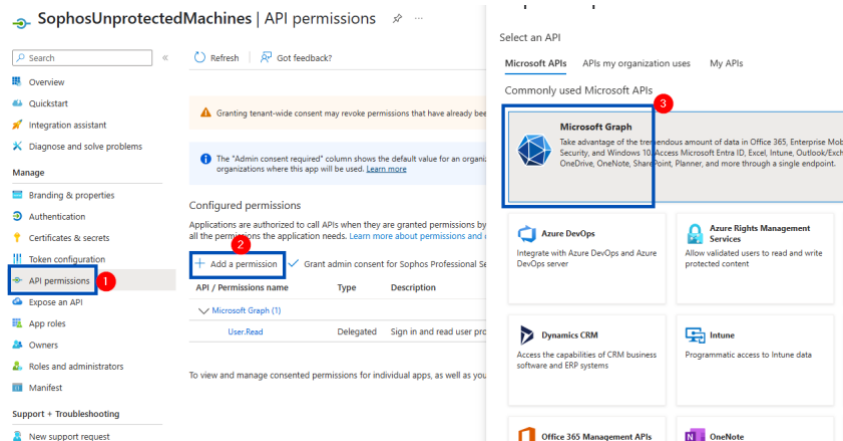
The screenshot shows the 'Certificates & secrets' page with 'Client secrets (1)' selected. A table lists the client secrets:

Description	Expires	Value	Secret ID
SophosUnprotectedMachines_Secret	04/06/2026	DUA8Q~kK... (labeled 1)	1bb27a17-9a...

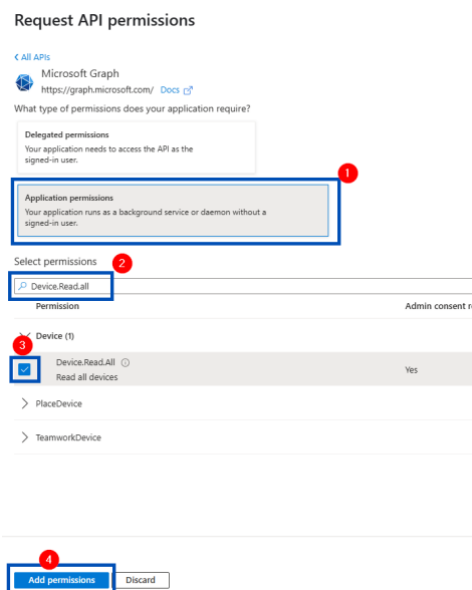
The 'Value' column is highlighted with a blue box and labeled **Entra_ClientSecret**.

Assign API Permission

1. Go to **API permissions** > Click + **Add a permission**
2. Choose **Microsoft Graph**



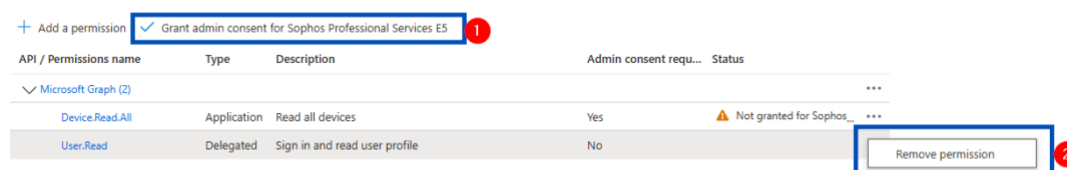
3. Select **Application permissions**
 - o Search for and add: > **Device.Read.All**
4. Click **Add permissions**



5. Back in the API permissions tab, click:
 - o **Grant admin consent for [your org]** → Confirm
 - o **Remove the Permission: User.Read**

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)



To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try [Enterprise applications](#).

**Configuration File (Sophos_Central_Unprotected_Machines_config.ini)**

Create a config file with the following structure. Place it in the **same folder as the script**:

[DEFAULT]

Do not leave the ClientSecret in the config file

The API key only needs to be Service Principal Read-Only

ClientID:<put clientID here>

ClientSecret: < Put Client Secret Value here or leave blank to enter manually >

[REPORT]

ReportName:<put report name here>

ReportFilePath:<put file path here>

[DOMAIN]

Example dc=domain,dc=co,dc=uk

SearchDomain:<put search domain here example>

Example domain\ldap-account

SearchUser:<put ldap search account here example>

Domain controller FQDN or IP address

DomainController:<Put domain controller name FQDN or IP address here>

#LDAP port 636 is LDAPS

LDAPPort:<put the LDAP port here 389 or 636>

[Entra]

Entra_ClientID:<Put Entra App ID here>

Entra_TenantID:<Put Entra Tenant ID here>

Entra_ClientSecret:< Put Entra Client Secret Value here or leave blank to enter manually >

#Do not leave the ClientSecret in the config file.



Running the Script

On Windows:

```
python Sophos_Central_Unprotected_Machines.py
```

On Mac:

```
python3 Sophos_Central_Unprotected_Machines.py
```

Make sure both the script and the config file are in the same directory.
