Date: Wednesday, 11 June 2025

Overview

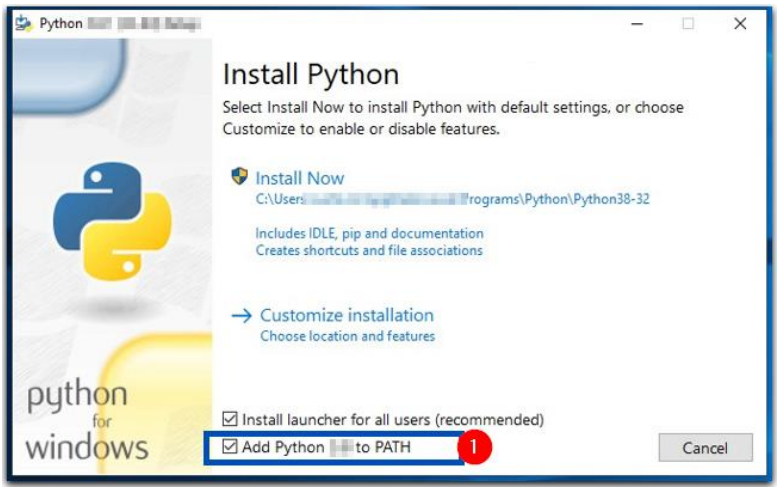
This workflow identifies machines listed in Active Directory or Entra that are missing from Sophos Central, and flags devices as suspicious if they are reporting to the directory, but not to Sophos Central for over three days longer.
The Entra comparison focuses on devices that are either *AzureDomainJoined*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

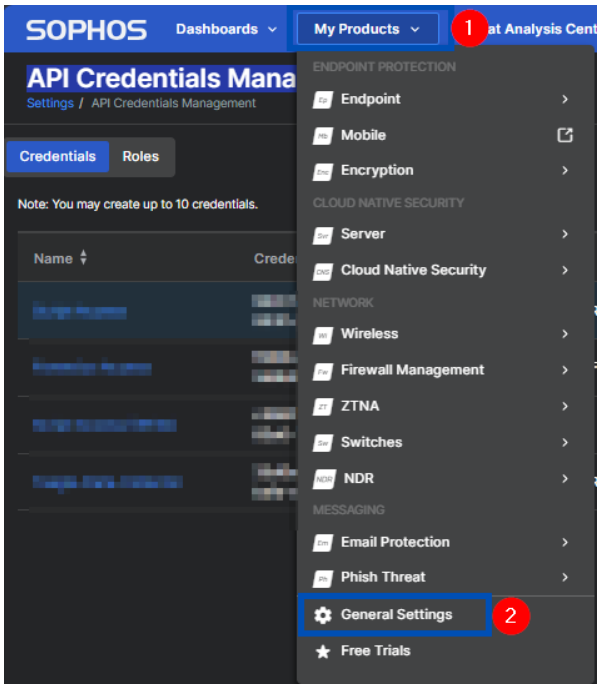
1. Open **Command Prompt as Administrator**
2. Run:
3. *python -m pip install requests ldap3 msal*

Installation (Mac)

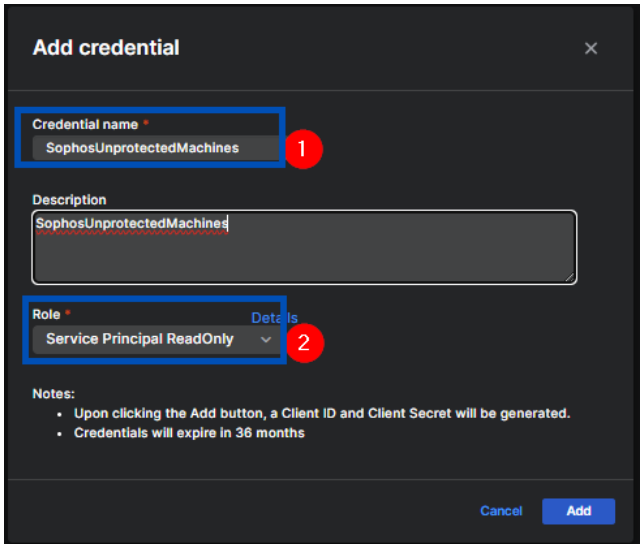
1. Open **Terminal**
2. Run:
3. *python3 -m pip install requests ldap3 msal*

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**

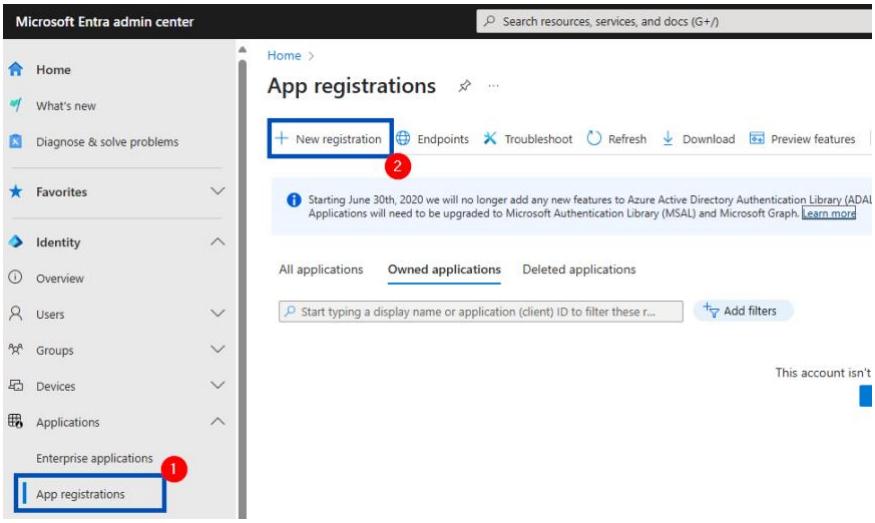


6. Save the **Client ID** and **Secret** securely.

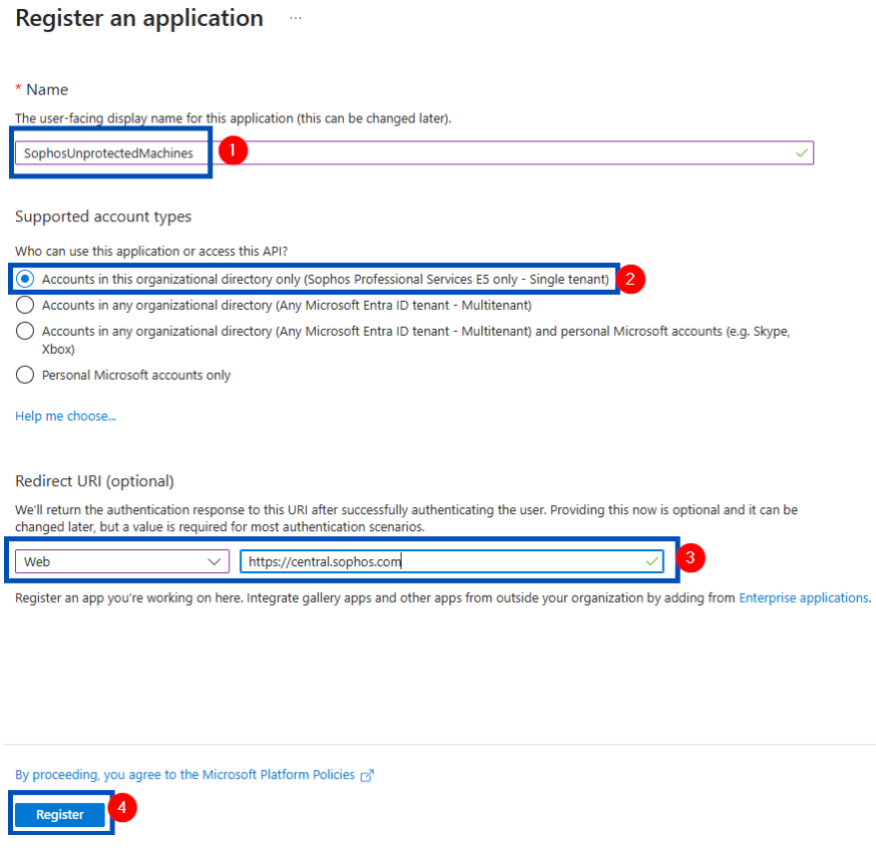
You will not be able to view the secret again.

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

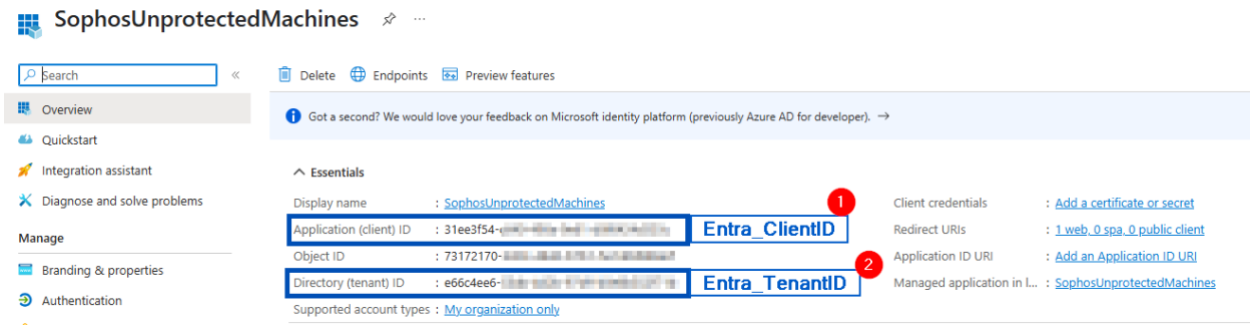


- Click **Register**

Get Your App Credentials

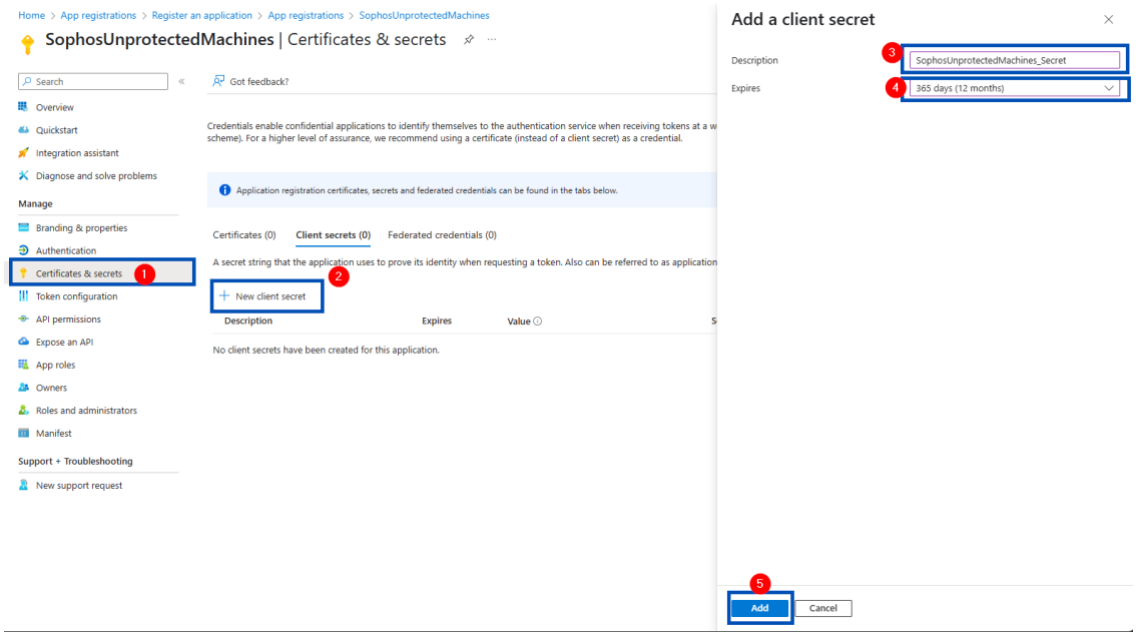
After registering the app, go to its **Overview** page:

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



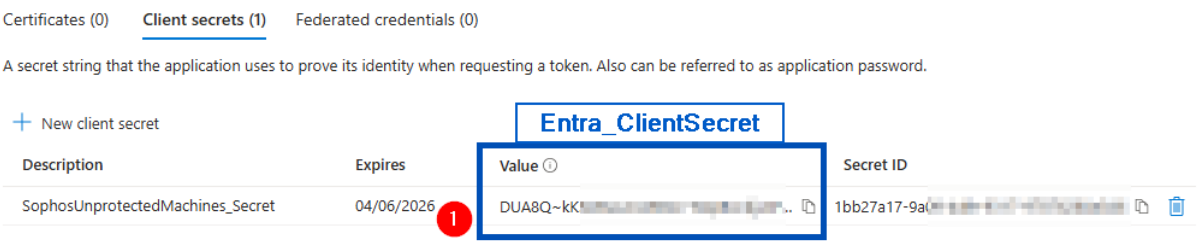
Create a Client Secret

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



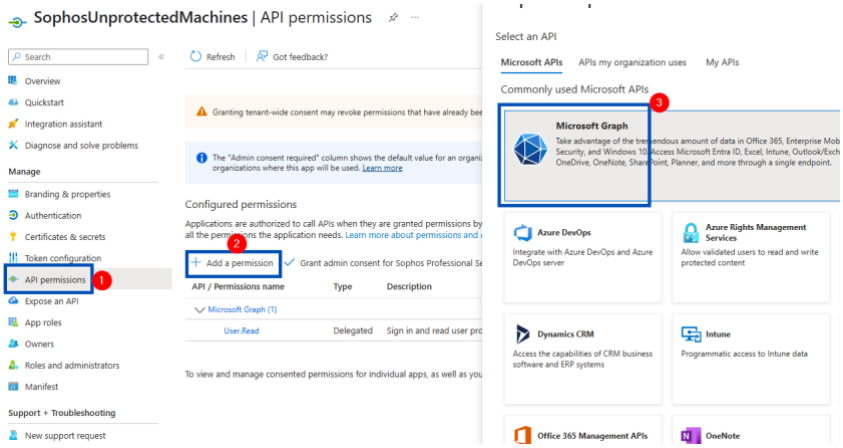
   - Click **Add**

3. Copy the **Secret <u>Value</u>** immediately → This is your Entra_ClientSecret

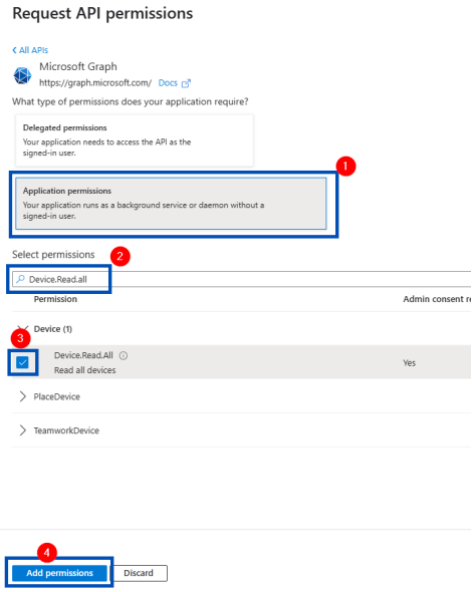


Assign API Permission

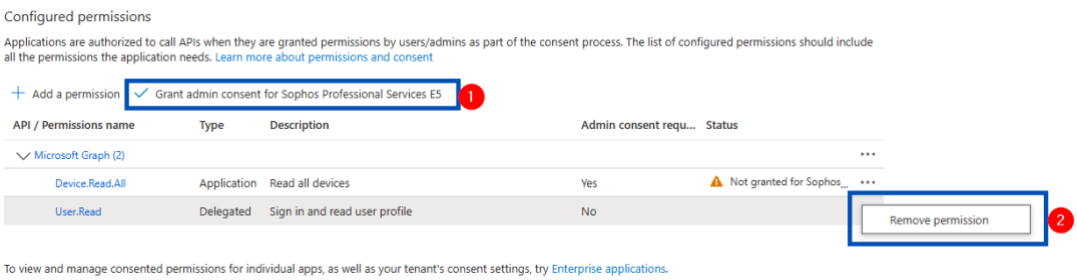
1. Go to **API permissions >** Click **+ Add a permission**
2. Choose **Microsoft Graph**



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



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



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 >

[EXTRA_FIELDS]
# Show sub estate menu if you have a Sophos Central Enterprise Dashboard
Show_sse_menu:1
# Azure Only: List all machines otherwise only show Azure AD joined and Hybrid Azure AD joined machines
List_all_machines:0
```

#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.
