

Date: Monday, 10 November 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:

- *AzureDomainJoined*
- *OnPremiseCoManaged*
- *AzureADJoinUsingWhiteGlove*

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**

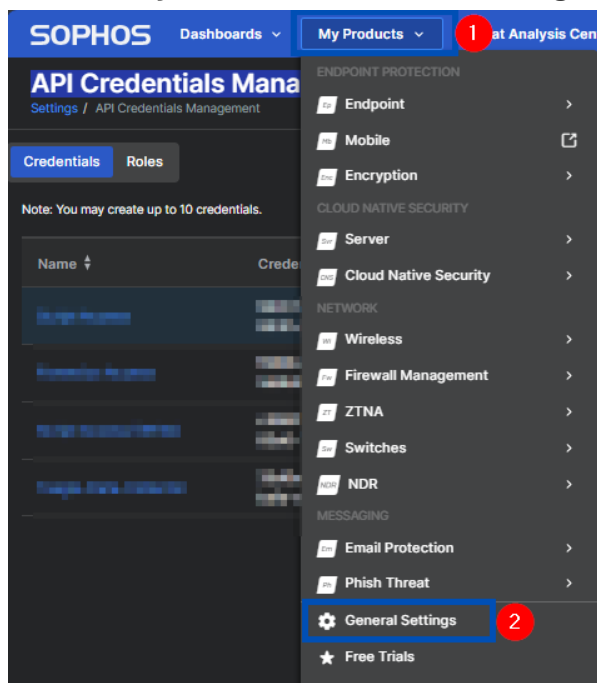
2. Run:
3. `python -m pip install requests ldap3 msal`

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**

Add credential

Credential name *
SophosUnprotectedMachines 1

Description
SophosUnprotectedMachines

Role * Details
Service Principal ReadOnly 2

Notes:

- Upon clicking the Add button, a Client ID and Client Secret will be generated.
- Credentials will expire in 36 months

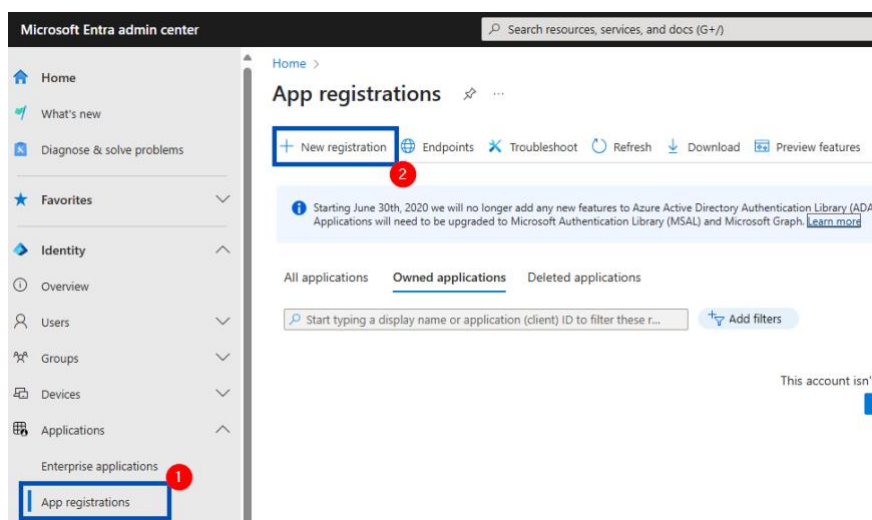
Cancel Add

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 https://central.sophos.com 3

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

SophosUnprotectedMachines ...

Search « Delete Endpoints Preview features

Overview

Quickstart

Integration assistant

Diagnose and solve problems

Manage

Branding & properties

Authentication

Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer). →

Essentials

Display name : SophosUnprotectedMachines

Application (client) ID : 31ee3f54-... Entra_ClientID 1

Object ID : 73172170-... 2

Directory (tenant) ID : e66c4ee6-... 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

Home > App registrations > Register an application > App registrations > SophosUnprotectedMachines

SophosUnprotectedMachines | Certificates & secrets

Search: [] Got feedback?

Overview
Quickstart
Integration assistant
Diagnose and solve problems

Manage
Branding & properties
Authentication
Certificates & secrets
Token configuration
API permissions
Expose an API
App roles
Owners
Roles and administrators
Manifest
Support + Troubleshooting
New support request

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web scheme. For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

Certificates (0) **Client secrets (0)** Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description	Expires	Value
No client secrets have been created for this application.		

Add Cancel

- Click **Add**

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

Certificates (0) **Client secrets (1)** Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

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

Entra_ClientSecret

Assign API Permission

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

SophosUnprotectedMachines | API permissions

Search: [] Refresh Got feedback?

Overview
Quickstart
Integration assistant
Diagnose and solve problems

Manage
Branding & properties
Authentication
Certificates & secrets
API permissions
Expose an API
App roles
Owners
Roles and administrators
Manifest
Support + Troubleshooting
New support request

Granting tenant-wide consent may revoke permissions that have already been granted.

The "Admin consent required" column shows the default value for an organization where this app will be used. [Learn more](#)

Configured permissions

Applications are authorized to call APIs when they are granted permissions by all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission ✓ Grant admin consent for Sophos Professional Services

API / Permissions name	Type	Description
Microsoft Graph (1)	Delegated	Sign in and read user profile

To view and manage consented permissions for individual apps, as well as you

Select an API

Microsoft APIs APIs my organization uses My APIs

Commonly used Microsoft APIs

Microsoft Graph
Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility, and Windows 10. Access Microsoft Entra ID, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.

Azure DevOps
Integrate with Azure DevOps and Azure DevOps server

Azure Rights Management Services
Allow validated users to read and write protected content

Dynamics CRM
Access the capabilities of CRM business software and ERP systems

Intune
Programmatic access to Intune data

Office 365 Management APIs

OneNote

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

Request API permissions

← All APIs

Microsoft Graph
<https://graph.microsoft.com/> Docs

What type of permissions does your application require?

Delegated permissions
Your application needs to access the API as the signed-in user.

Application permissions
Your application runs as a background service or daemon without a signed-in user.

Select permissions

Device.Read.all

Permission Admin consent n

Device (1)

☒ Device.Read.All
Read all devices Yes

> PlaceDevice

> TeamworkDevice

Add permissions Discard

5. Back in the API permissions tab, click:

- **Grant admin consent for [your org]** → Confirm
- **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](#)

+ Add a permission ✓ Grant admin consent for Sophos Professional Services ES

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (2)				***
Device.Read.All	Application	Read all devices	Yes	⚠ Not granted for Sophos... ***
User.Read	Delegated	Sign in and read user profile	No	Remove permission

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 >

[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.
