Installation and Configuration Manual

Copyright notice

Disclaimer

The use of this document is for informational purposes only and reflects the publisher's opinion as per date of publishing. Liability is limited to the publisher's terms and conditions as depicted in the underlaying master-agreement and/or purchase order.

Contents

Introduction

This document describes how to install and configure the Cyber Security Assessment Tool (CSAT) on a freshly installed, clean and up-to-date Operating System in the customer's IT environment. This CSAT Installation and Configuration Manual is complemented with the CSAT E-learning videos, available in the CSAT Partner Portal.

CSAT license key

For each installation of the CSAT server software a unique license key is required. Make sure that you have a valid license key available for the assessment type that you are going to perform.

CSAT version support

QS solutions supports the last two published versions of CSAT. Instructions on how you can upgrade your installed CSAT server to a current version can be found in chapter 4 of this manual.

CSAT bugfixes

Bugfixes will only be applied to the latest version of CSAT. When a potential blocking bug is found and solved, a hotfix or a new CSAT version will be released.

Installation Requirements

CSAT installations only work on clean operating system installations. This means the operating system is a default Windows installation, using Microsoft installation media, and is not joined to a domain. Existing components or hardening might interfere with the CSAT components.

If you want to apply hardening, and Active Directory Domain Policies to your operating system, you should do this after installing CSAT. Installing CSAT on a system that is not a clean installation could fail and possibly make the device unstable or unusable for its purpose.

The following Operating Systems are supported to install CSAT server:

- Windows Server 2022
- Windows Server 2019
- Windows Server 2016

The following operating systems are not officially supported to install CSAT server. You can use these systems at your own risk:

- Windows 11 Professional or Enterprise, build 22H2 or newer
- Windows 10 Professional or Enterprise, build 22H2 or newer
- Other Windows 10 and 11 versions not listed above

Please note that while the CSAT server may function on these unsupported systems, we do not guarantee full compatibility or provide technical support for them.

When you install the CSAT server software, PostgreSQL, WAMP, CloudLab TCO, and Microsoft .NET Core will also be installed on the device. To install CSAT, you must have (local) administrator privileges on the device. During the installation, the CSAT server may need to connect to "https://download.microsoft.com/download/" and "https://go.microsoft.com/fwlink/?LinkID=2099383" to download .NET framework, if necessary.

The minimal requirements for the CSAT server are:

Windows updates	Up to date with the latest Windows updates
CPU cores	Four CPU cores
CPU speed	1.4 GHz (2.0 GHz recommended)
Memory	8 GB
Hard disk	60 GB free space (SSD recommended)
.NET Framework	Version 4.8 or higher

Should you choose to use an Azure Virtual Machine, we recommend using the Azure template D4s_v5 or one with better specifications. CSAT is also listed in the Azure Marketplace.

For the best CSAT experience we recommend installing and opening CSAT with either Edge or Chrome on the CSAT server. See the 'CSAT Scan and installation requirements' document for all the details of the CSAT server preparation.

CSAT Download

Download the latest CSAT software installer version from the CSAT Partner Portal. Make sure to also download the latest available Questionnaire template (Excel file), Report template (Word file) and Presentation template (PowerPoint file) from the CSAT Partner Portal.

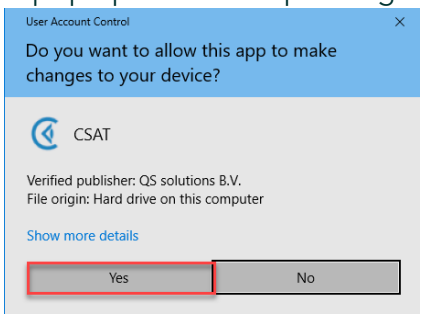
CSAT Installation

For each installation of the CSAT server software a unique License key is required. Make sure that you have a valid license key available for the assessment type that you are going to perform.

To install the CSAT software follow these steps:

1. Run the CSAT installer:
2. The following screen might pop up if you start the installation on a machine without an internet connection

3. Click 'More info'
4. After this click 'Run anyway'
5. A pop up will show up asking for your consent

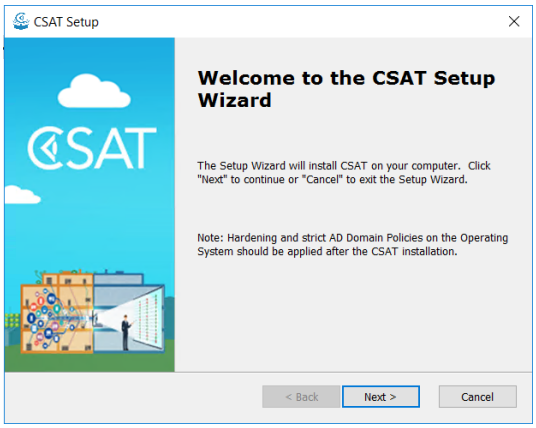


6. Click 'Yes' to continue
7. The CSAT Setup Wizard will first ask you to select a language

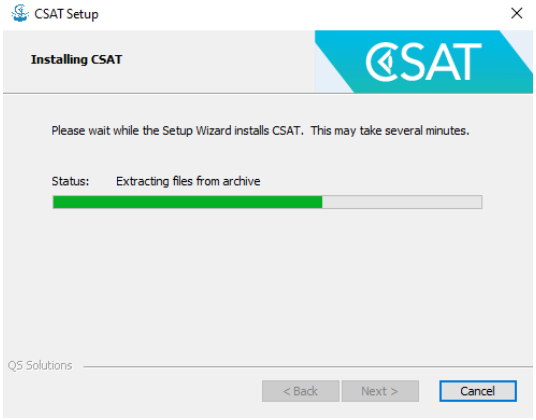
8. The prerequisites will be checked. If there are any prerequisites that need to be installed, it will be shown here. Click 'Next' to continue. The installation of the prerequisites will now start if there are any, if all the prerequisites are already installed this screen will be skipped.
   CSAT's dedicated instance with PostgreSQL will be installed. A PostgreSQL install

window will be show during the installation. **Do not interrupt this process**. Once the installation of PostgreSQL is finished, Microsoft .NET Core will be installed. **Do not interrupt this process**

9. After the prerequisites are installed, the CSAT Setup Wizard will be started. Click 'Next' to continue



10. The End User License Agreement will now show. To continue with the installation, you must select 'I accept the terms in the License Agreement' and click 'Next'
11. The next step will ask for the license key. Enter the license key.
12. In the next step select the folder where you want the CSAT to be installed. Click 'Next' to continue with the default or click 'Browse' to change the destination folder
13. On the next screen, click 'Install' to start the installation of CSAT
14. The installation of CSAT will now start. A command prompt will show shortly, this is part of the installation, **do not interrupt this process**



15. After CSAT is installed, the following screen will be presented.

16. Click on 'Finish' to exit the Setup Wizard. A Browser window should now popup, pointing to https://localhost:4432/. You can find the default user account and password for the CSAT application in Chapter 5.2

Upgrade CSAT version

You can update from any CSAT 2.05 version to the current version by downloading the CSAT installation package to the machine where CSAT is currently installed and then run the installer.

If you want to update from a CSAT version before 2.04.3, you need to download CSAT version 2.04.3 and 2.05.0 from these URL's:
https://csatrelease.blob.core.windows.net/release/CSATv2.04.3.zip.

https://csatrelease.blob.core.windows.net/release/CSATv2.05.0.zip

First update the installation to CSAT version 2.04.3 and login into CSAT. Then upgrade to CSAT version 2.05.0 and login into CSAT. After the update to 2.05.0 you can upgrade to any version after 2.05.0.

When you are logged in to the CSAT server with the previous CSAT version installed, start the CSAT installer. When you have completed the installation, you can login to the CSAT application. When you login for the first time after the upgrade, the database will be automatically upgraded to the correct version. Note that the first login after the upgrade can take longer because the database is upgraded during the first login. If you have any issues updating CSAT, get in touch with our email support: sc.csat@qssolutions.nl

CSAT installer command line options

The CSAT installer has various command line options.

To install CSAT with a debug log, use the following option.

- "/l* debug.log"

Where the C:\install.log is the save location for the debug log. As an example, this can show in CMD as:

```
C:\WINDOWS\system32>Csatinstall.exe /l* C:\install.log
```

To install CSAT silent, use the following command line option.

- /exenoui /qn PIDKEY="123456-456789"

The PIDKEY value is the product key for CSAT. As an example, this can show in CMD as:

```
C:\>Csatinstall.exe /exenoui /qn PIDKEY="123456-456789"
```

To install CSAT and skip the reboot check, use the following command line option.

- RP=FALSE

As an example, this can show in CMD as:

```
C:\WINDOWS\system32>Csatinstall.exe RP=FALSE
```

Security Total cost of ownership(TCO) module

The installation of CSAT includes an embedded version of The CloudLab. This addition allows for the creation of a Security Total Cost of Ownership (TCO) analysis based on data from CSAT. The Security TCO data will be included in the "Export All" feature. When imported into the Power BI template, the Security TCO will be visualized in various charts. This embedded version is a complete offline version of The CloudLab.

CSAT Configuration

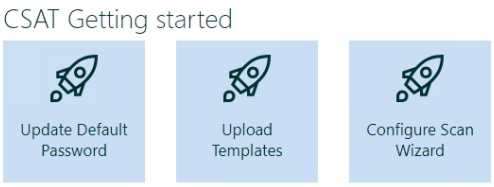
After the CSAT server software is installed, there are several configuration steps to prepare CSAT for your assessment. Make sure you have the following files available on the CSAT server:

- CSAT Questionnaire template
- CSAT Report template
- CSAT Presentation template

There are different types of assessment that you can perform, be sure that you have all the correct files for your assessment type. You can find these files on the CSAT Partner Portal.

Getting started

The first time you start CSAT you will see the 'CSAT Getting started' icons. With these items you can quickly jump to unconfigured elements in CSAT.

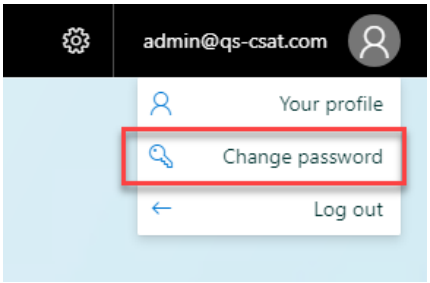


Update default admin password

The default admin login for CSAT is:

Account name: admin@qs-csat.com
Password: Welkom112!!@

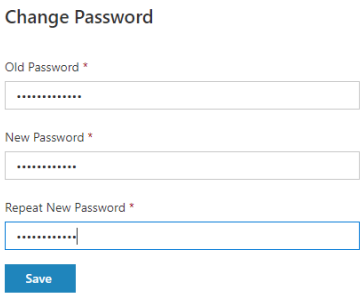
It is recommended to change the default CSAT admin password. You can change the password by clicking in the top right corner on the account name (admin@qs-csat.com) and choose 'Change password'.



The new password must be at least 8 characters and must contain characters from the following categories:

- Uppercase letters. For example, A, B, C

- Lowercase letters. For example, a, b, c
- Numbers. For example, 1, 2, 3
- Special characters. For example !, @, *



When you have entered a new password, click the 'Save' button. A notification will confirm that the password is changed.

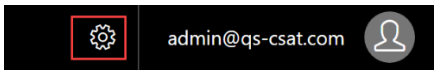
Upload templates

To answer the questionnaire, generate the report and generate the presentation from CSAT, you first need to upload the template files in CSAT. When importing files into CSAT, ensure that the files are not encrypted. Encrypted files, such as those with information protection, will result in an error when uploaded to CSAT.

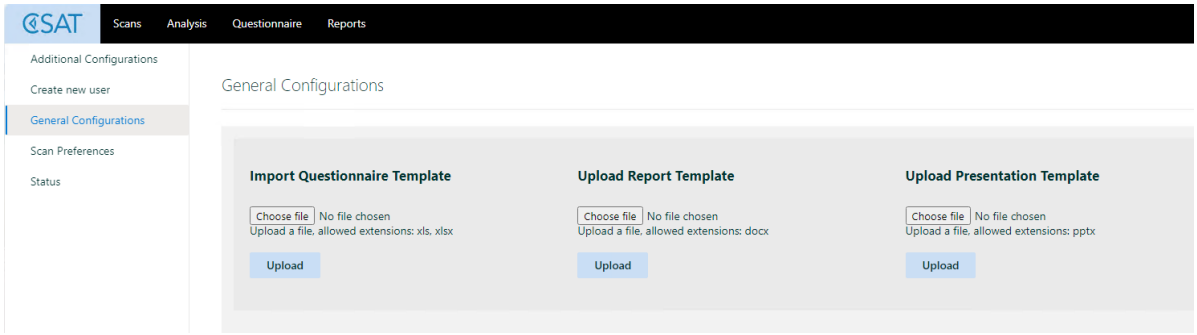
First, make sure that the Following files are placed on the CSAT server.

- CSAT Questionnaire Template (.xlsx file)
- CSAT Report Template (.docx file)
- CSAT Presentation template (.pptx file)

Now, open the configuration menu in CSAT by clicking on the Gear icon in the top right corner.



Go to the tab 'General Configuration', choose 'Browse', and upload the corresponding file.



Note: Importing a new Questionnaire file will **delete all given answers in the current assessment.**

You will be asked for your confirmation.
Click 'Yes' to import the file. A notification is shown when the import is successful.

Scan configuration

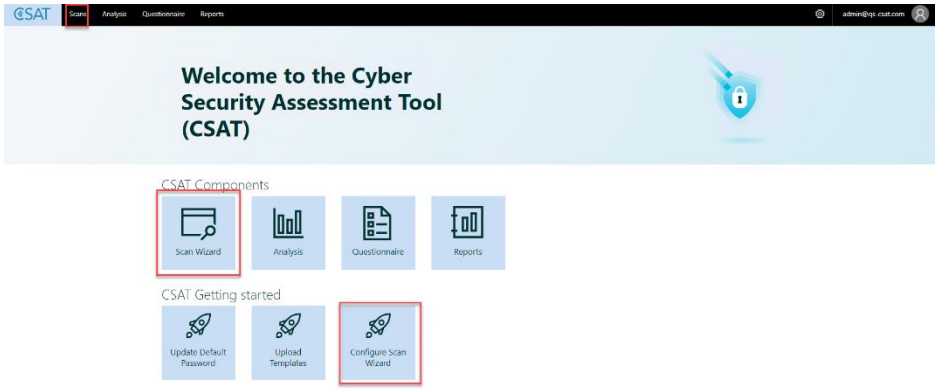
Scan Wizard

CSAT scans are configured via a wizard that guides you through the setup of scans.

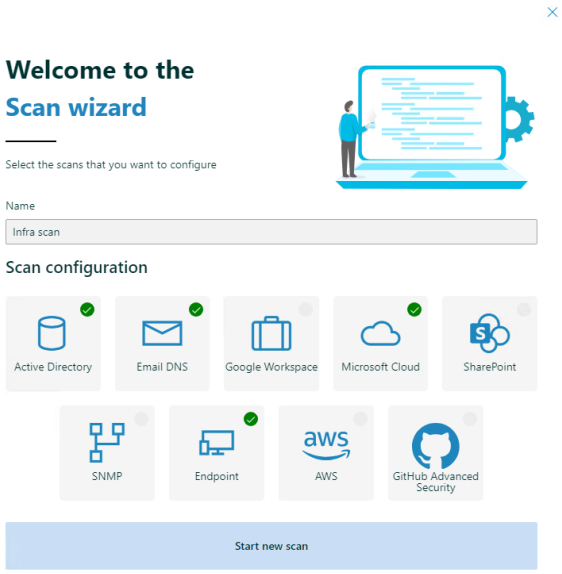
The Scan Wizard is used to define the scope of scans in assessments, and it is used to set up and configure the scans.

There are different ways to start the Scan Wizard:

- Via the 'Configure Scan Wizard' tile in the 'CSAT Getting started' section on the home page. This tile is only shown until you kicked off the Scan Wizard for the first time
- Via the 'Scan Wizard' tile in the 'CSAT Components' section on the home page
- Via the 'Scans' tab in the top-level navigation on home page



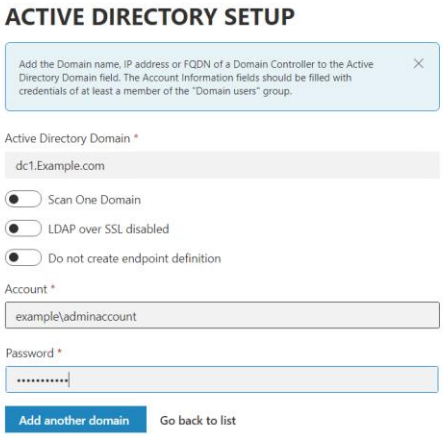
When you start the Scan Wizard, you see the following screen:



On this first page of the wizard, you can enter a name for your scan and select which scan(s) you want to setup. When the green checkmark is shown in the tile the scan is selected, by default all scans are selected. Click 'Start new scan' to move forward in the wizard and to set up the selected scans.

Setup Active Directory scan

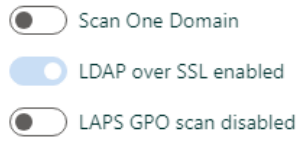
a. When you have selected the Active Directory (AD) scan, the page in the setup wizard opens (see screenshot below). You need to fill in various information to scan the AD. The field 'Active Directory Domain' can be the Domain name, IP address of a domain controller or a FQDN (Fully Qualified Domain Name) of a Domain Controller
b. If the switch for the domains is set to 'Scan One Domain' The Account fields should be filled with credentials of at least a member of the domain users
c. If the switch for the domain is set to 'Scan all Sub Domains', the Account fields should be filled with credentials of at least a member of the domain administrator or enterprise administrator group
   A filled in example is as follows:



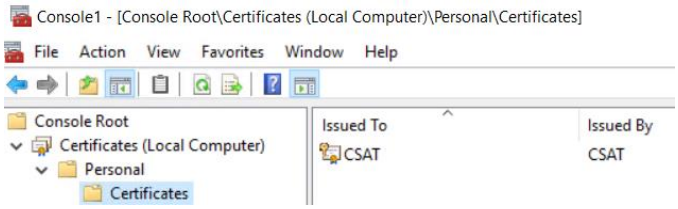
d. You can add multiple Active Directory Domains here by adding them with the 'Add another domain' button

LDAP SSL

To scan the AD with LDAP SSL you can enable the option 'LDAP over SSL enabled'.



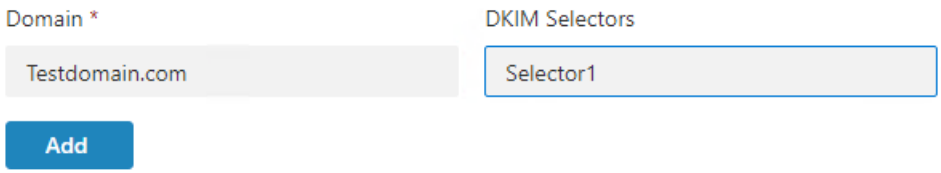
Note: When enabling the LDAP SSL scan, the CSAT certificate of the CSAT server must be imported on the AD server in the personal store. This CSAT certificate can be found on the CSAT server in the personal folder of the computer store.



Setup Email DNS scan

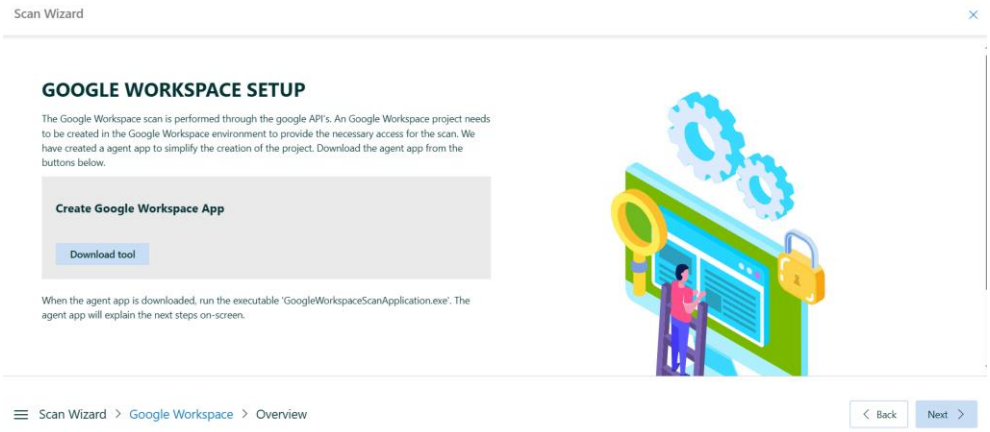
CSAT can check the external e-mail DNS records for various values. With this scan, CSAT will retrieve DNS Sec information and the SPF, DMARC and DKIM records from the entered domain(s). Enter an email domain and click 'Add' to enter one or more domains.

A DKIM Selector is a header added to email messages. The header contains values that allow a receiving mail server to validate the email message, by looking up a sender's DKIM key and using it to verify the encrypted signature. Some email service providers, such as Office 365 and Google, have standard DKIM Selectors values. In that case, nothing needs to be entered in the DKIM Selectors field, by default CSAT checks the most used selectors. If your customer has defined their own selector, enter that selector value in the DKIM Selector field.

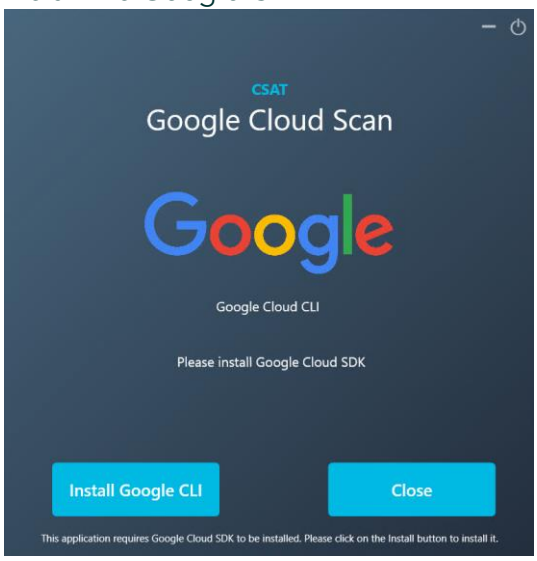


Setup Google Workspace scan

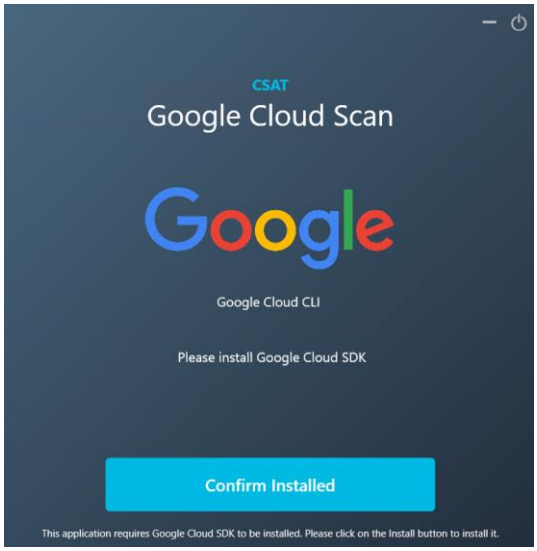
a. The Google Workspace scan is performed through the available API's. An Google Workspace project needs to be created in the Google Workspace tenant to provide the necessary access for the CSAT scan. The tool to create the project can be downloaded via the buttons in the wizard.



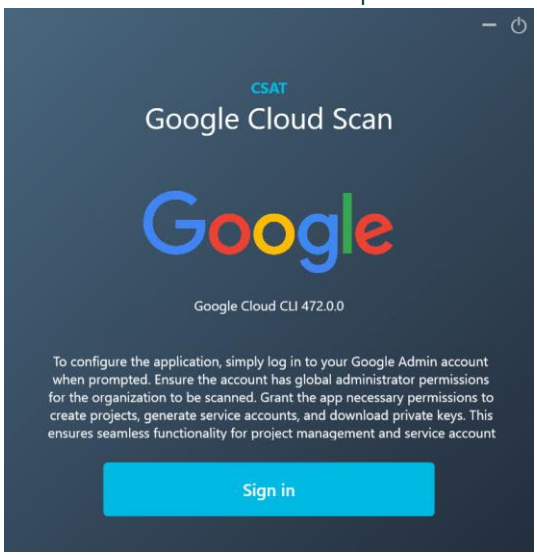
b. On the first wizard page for the Google Workspace scan, you need to click on the button 'Download tool'. Extract the downloaded zip file and run the executable 'GoogleCreator.exe' on the CSAT server. To create the project the Google CLI needs to be installed, if the Google CLI is not installed the first page will show the button to install the Google CLI



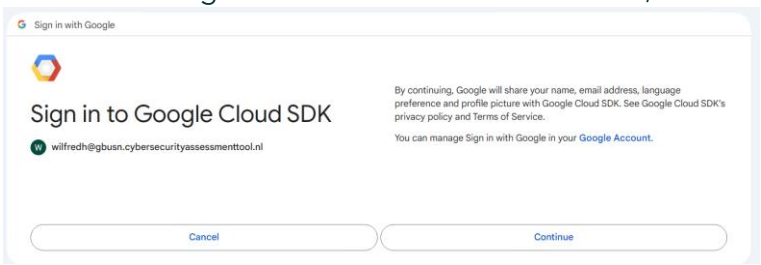
c. Follow the steps to install the Google CLI. When the CLI is installed, click on the button 'Confirm installed'

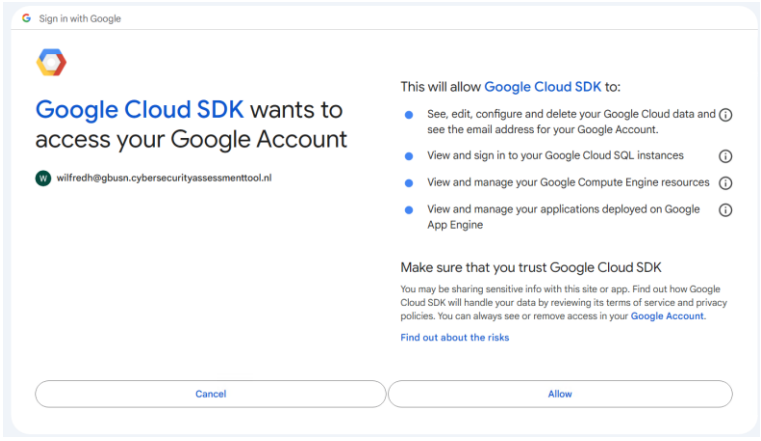


d. The scan application will explain what will be created. To continue, click on the 'Sign in' button and login with a Google Administrator Account of the Google Workspace environment. See an example below

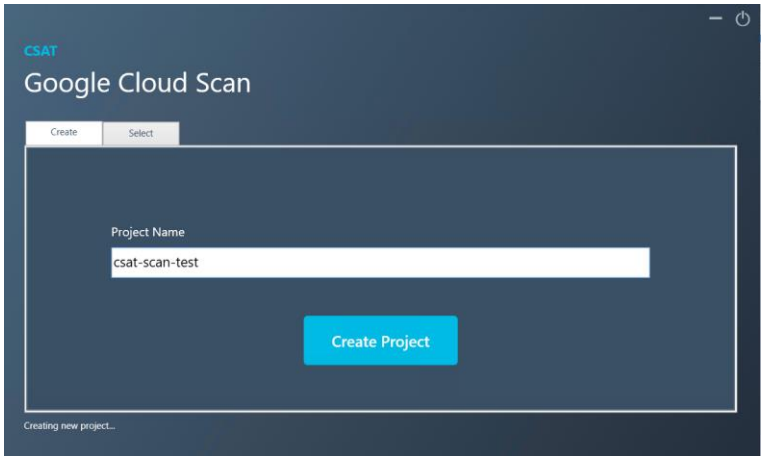


e. When the Google Cloud SDK is not used before, the following screens can be shown

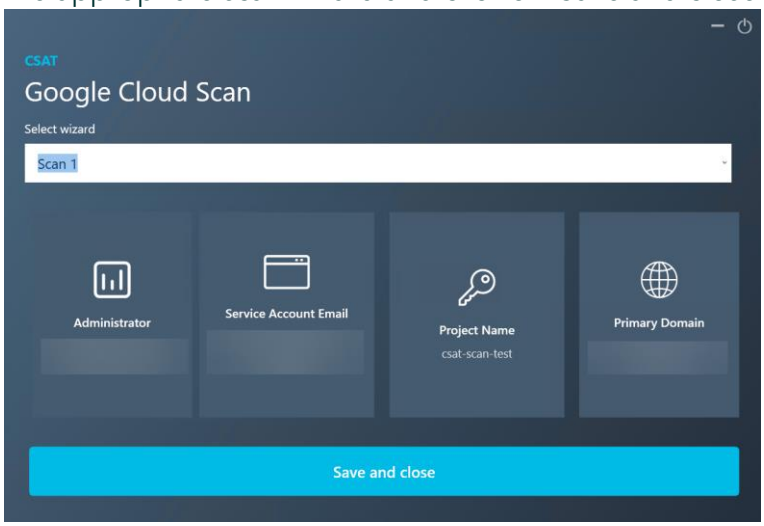




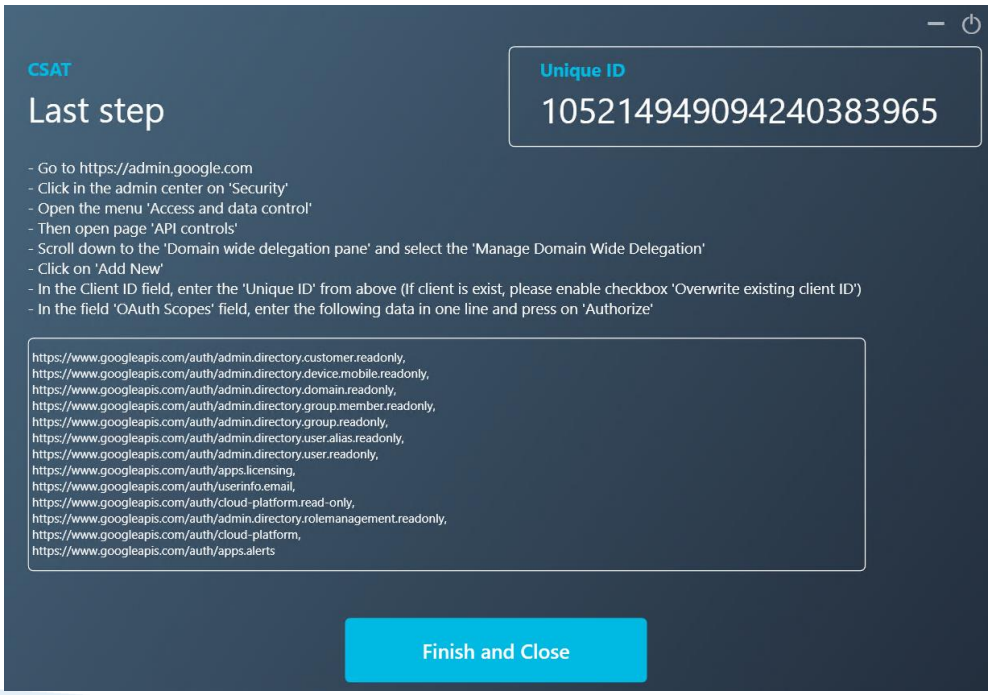
f. After the login, you can name the project that will be used during the scan



g. After the creation the scan application can save the scan information into CSAT. Select the appropriate scan wizard and click on 'Save and close'

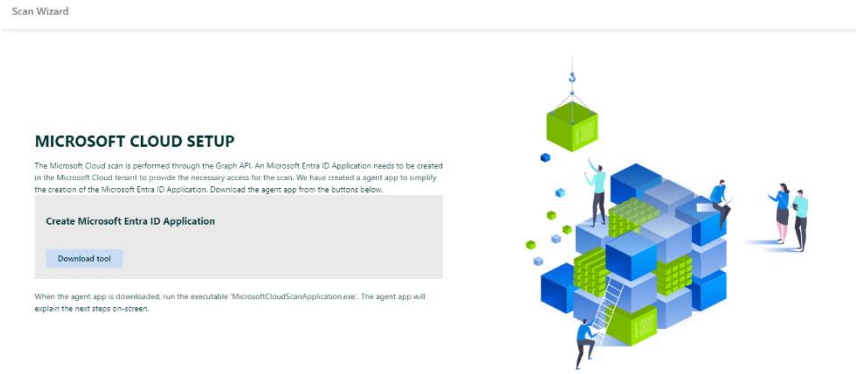


h. After the save and close there are a few steps necessary to finish the scan application. These steps need to be completed manually. How to compete the steps is shown on screen.

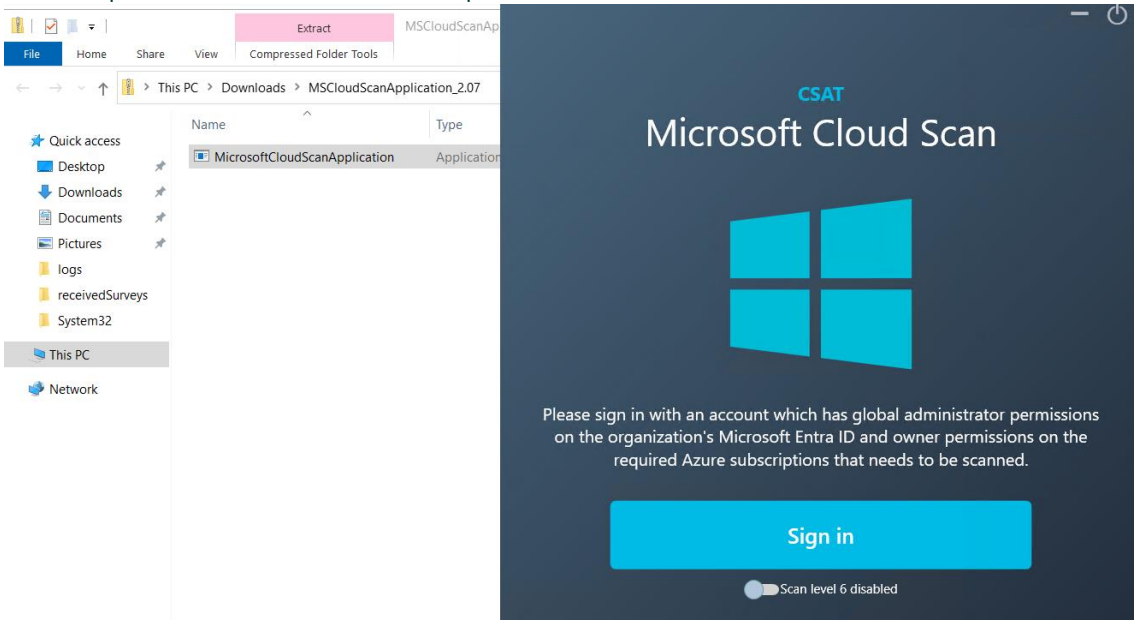


Setup Microsoft Cloud scan

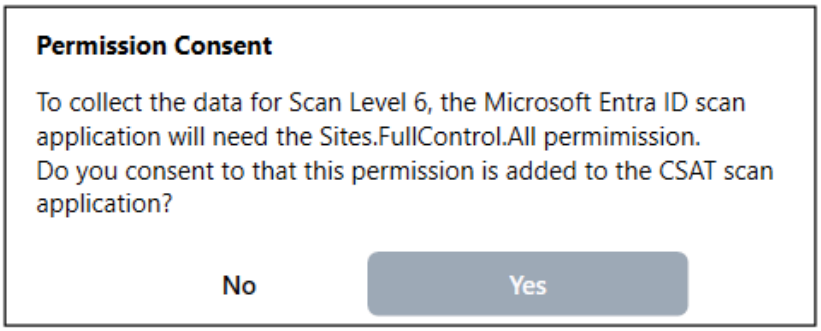
a. The Microsoft Cloud scan is performed through the Graph API. An Azure AD Application needs to be created in the Microsoft Cloud tenant to provide the necessary access for the CSAT scan. The tool to create the Azure AD application can be downloaded via the buttons in the wizard or from the CSAT general settings menu



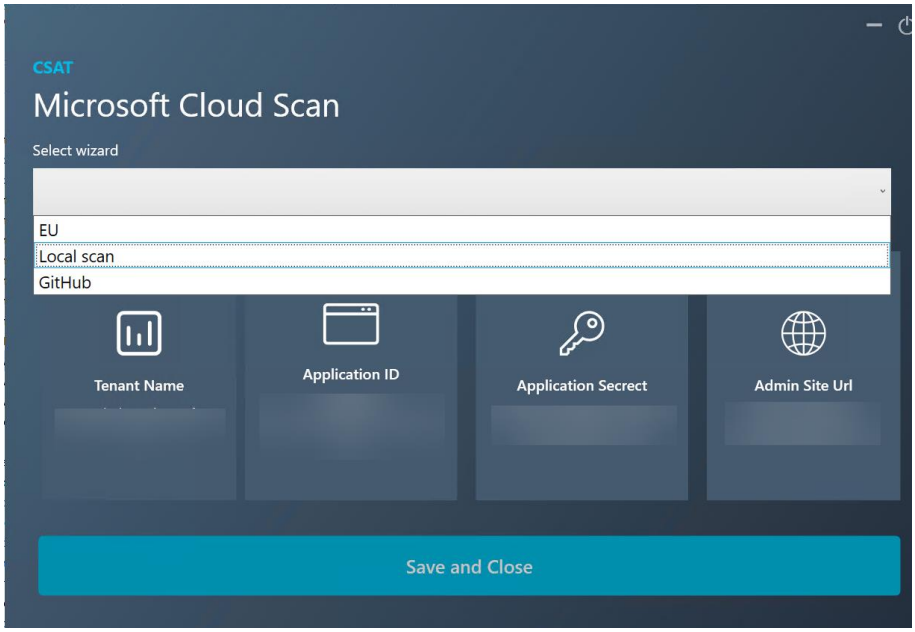
b. On the first wizard page for the Microsoft Cloud scan, you need to click on the button 'Download tool'. Extract the downloaded zip file and run the executable 'AzureAppCreator.exe' on the CSAT server. Enter login credentials of a Global Administrator account of the Microsoft Cloud tenant. The executable will explain the next steps on-screen. See an example below



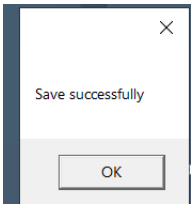
c. If you enable the scan level 6, the scan application will need the SharePoint - Sites.FullControl.All permissions, therefore a consent message will be shown to ensure that these permissions are added to the application.



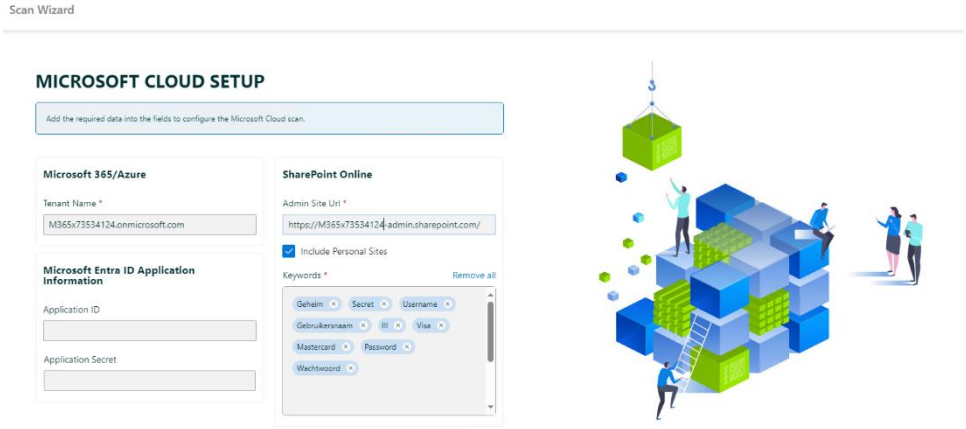
d. The Application will create the Microsoft Entra ID application that is used to scan the Microsoft Cloud. When the application is created, and you have multiple wizards, a screen will be shown where you can select to which wizard the application should be saved.



e. When the data is saved a confirmation button will be shown and the app creator will be closed.



f. Move forward in the wizard by clicking 'Next' and you will see the screen below



Note: In the wizard the Application ID and Application Secret are shown empty. The fields however are required. When information is added previously the database will have the information. If necessary, the Azure AD Application Information can also be entered manually. The Tenant name is the.onmicrosoft.com name of the tenant, The Application ID and Application Secret can be copied from the Azure App creator. The Admin Site URL is the SharePoint Online admin center URL.

g. On the wizard page in the previous step i., you can enter a list of words in the 'Keywords field'. CSAT will then use the SharePoint Online search service to find documents that hold one or more of these entered keywords.
To add one keyword, type in the keyword in the keywords field and press enter. To enter multiple keywords at once, use the following format:

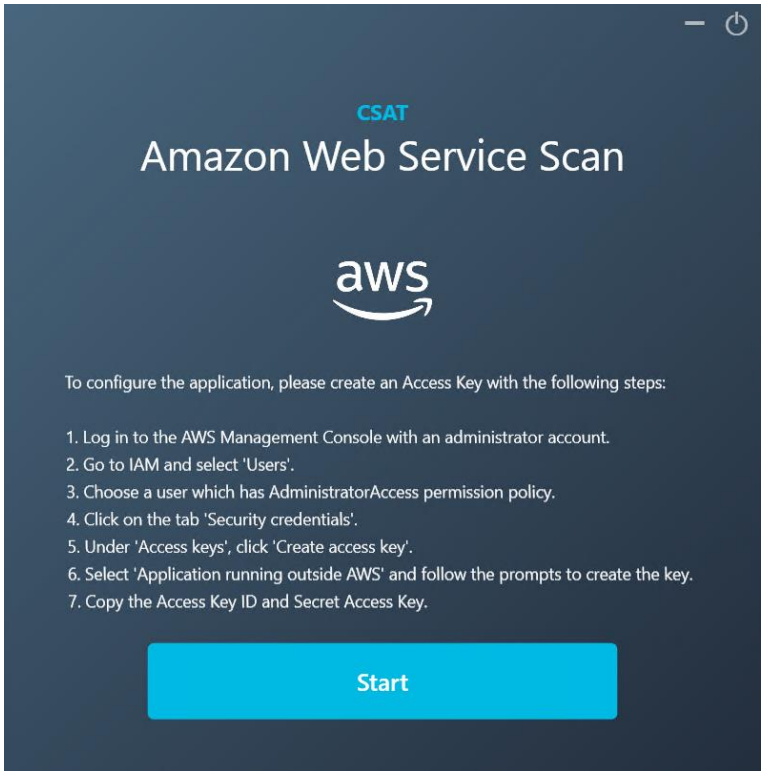
Keyword1, Keyword2, Keyword3

After you typed in the comma separated keywords press enter to insert the keywords

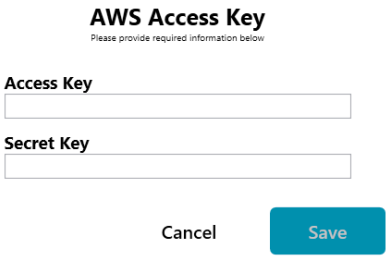
Setup Amazon Web Services scan

a. The Amazon Web Services scan is performed through the AWS API. A scan creator tool is used to make this process as easy as possible. Download the AWS scan application via the buttons in the wizard or from the CSAT general settings menu.

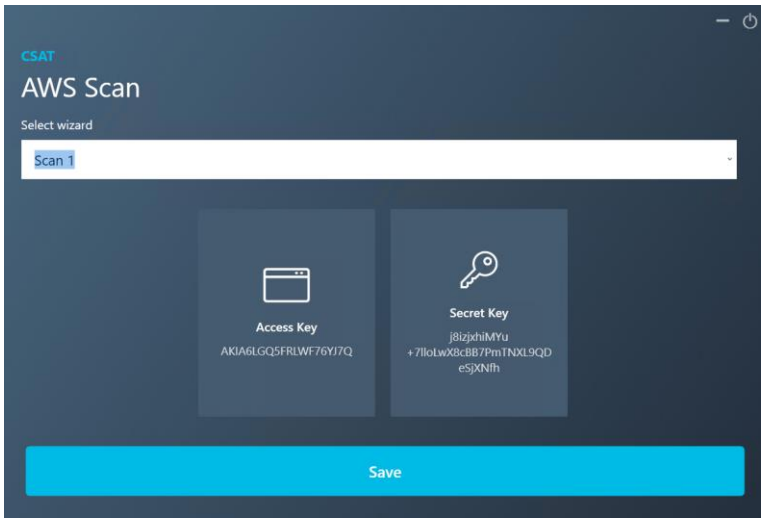
b. On the first wizard page for the AWS scan, you need to click on the button 'Download tool'. Extract the downloaded zip file and run the executable 'AWSScanApplication.exe' on the CSAT server. The executable will explain the next steps on-screen. See an example below



c. When you select start the Access key ID and Secret Access key will be asked, this will be the connection for the AWS creator to the AWS environment.



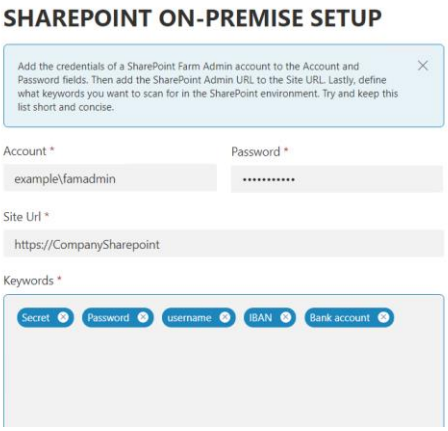
d. Then the application will create a 'CSATScan' user that will be granted the necessary permissions. This is the account that will be used in CSAT to scan the AWS environment. The scan creator will ask in which CSAT wizard the information should be saved.

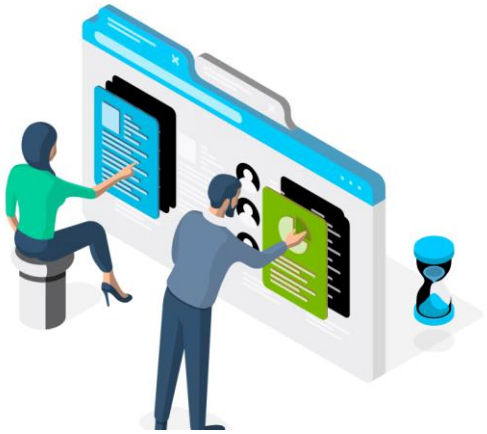


e. Click on save and the information will be saved into the correct CSAT scan wizard.

Setup SharePoint On-Premises scan

a. To set up the SharePoint On-Premises scan, add the credentials of a SharePoint Farm Admin account to the Account and Password fields. Then add the SharePoint Admin URL to the Site URL. In the 'Keywords field' enter words you want to search for in documents that are stored in the SharePoint On-Premises environment. A filled in example is as follows:

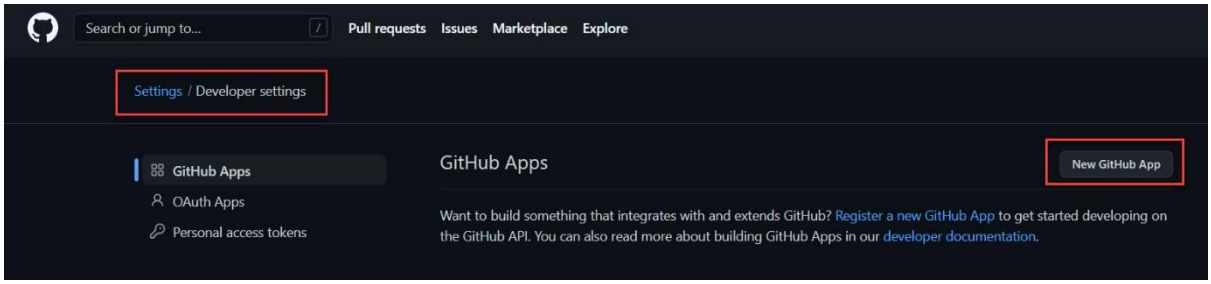




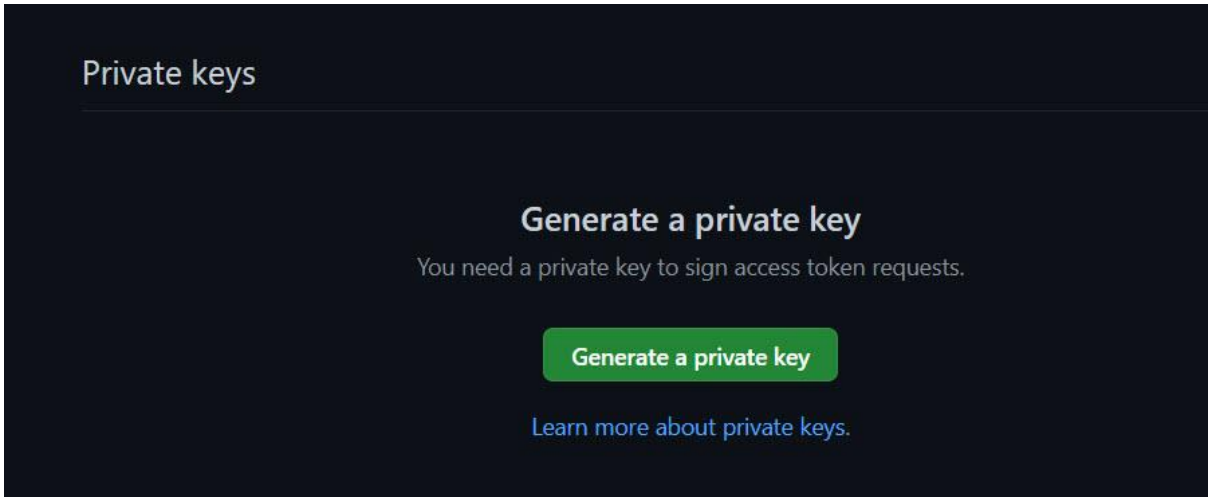
Setup GitHub scan

CSAT collects data from GitHub Advanced Security features. Instead of scanning the code directly (which would require different setups for each codebase), it gathers results from the code scanning actions you've configured and run on your GitHub repositories.

The GitHub Advanced Security data collection is performed through the GitHub API. A GitHub app needs to be created. Navigate to the GitHub Settings - Developer settings - GitHub Apps (https://github.com/settings/apps) and select 'New GitHub App'.



Give the GitHub app a name, in the 'Homepage URL' fill in the value 'https://localhost'. Change the Webhook to not be active since that is not necessary. Scroll to the bottom of the page and change the 'Where can this GitHub App be installed?' to 'Any account', then click on 'Create GitHub app'. When the app is created, on the general tab Scroll to 'Private keys' and select 'Generate a private key'.



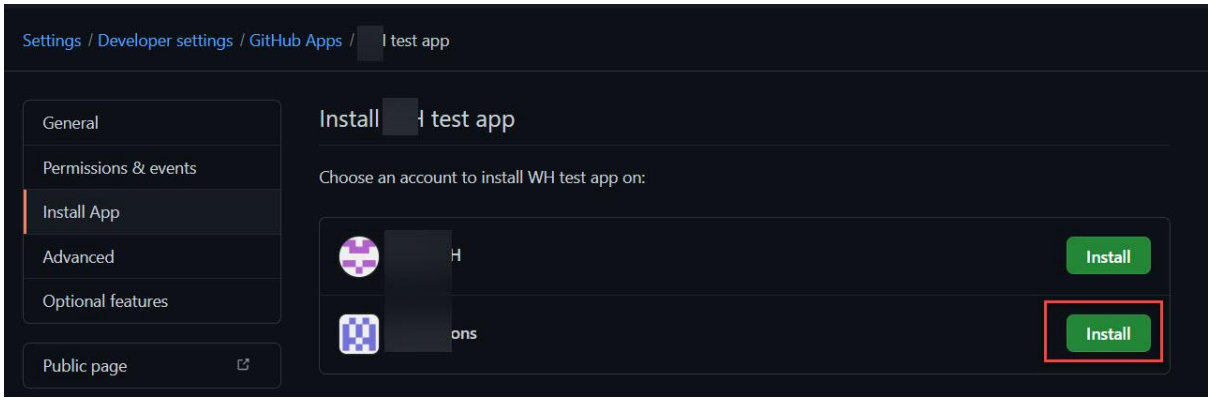
A .PEM file will be downloaded, save this file carefully. Navigate to the 'Permissions & events' and add the following Repository permissions:

- Code scanning alerts - Access: Read-Only
- Dependabot alerts - Access: Read-Only
- Dependabot secrets - Access: Read-Only
- Metadata - Access: Read-Only
- Secret scanning alerts - Access: Read-Only
- Secrets - Access: Read-Only

and the following Organization permissions:

- Organization dependabot secrets - Access: Read-Only
- Secrets - Access: Read-Only

When the permissions have been set, navigate to the 'Install App' page, and install the created application on the GitHub organization.

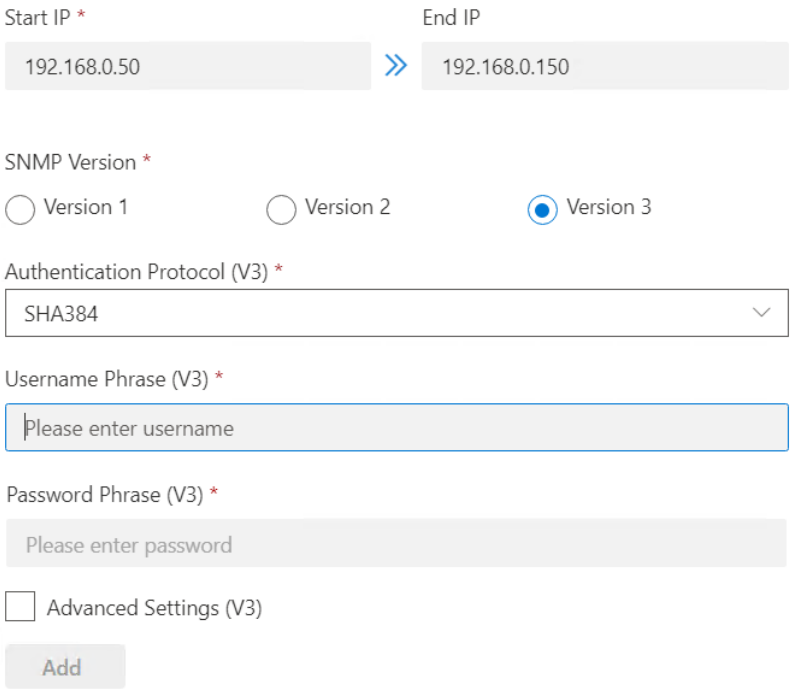


When installing the app, you can decide if you want to collect data from all repositories or only specific repositories. select which option is required and click on 'Install'.

Setup SNMP scan

The SNMP scan discovers SNMP v1, v2 and v3 devices on the network. Enter the IP range, select the SNMP version. When SNMP v1 or v2 is selected, enter the community string that is configured on the network devices. If no community string is entered in the SNMP config, the scan will be done with public string.

When SNMP v3 is selected, the authentication fields will change since SNMP v3 has different options compared to SNMP v1 and v2. Fill in the 'authentication protocol', 'username phrase' and 'password Phrase' and click on Add. If there are specific settings in the SNMP setup you can enable the 'Advanced settings' and configure the settings.



Note: The SNMP v3 scan supports the following Authorization protocols: SHA1, SHA192, SHA384, SHA512, MD5 and the following Privacy settings: DES, Triple DES, AES/AES128, AES192, AES256.

Setup Endpoint scan

Three scan methods

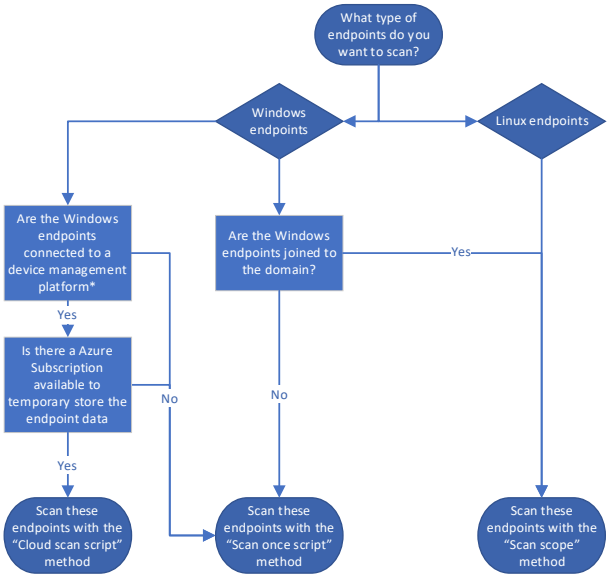
The Endpoint scan is used to collect relevant data from Windows and/or Linux machines in the customer's environment. Both servers and workstations can be scanned.

There are three methods to perform a scan on the Windows or Linux endpoints:

1. Scan scope method - Directly from the CSAT interface, via the Scan Wizard, using the local AD, an IP range, CIDR, or list of machines
2. Cloud scan script method - Via Microsoft Endpoint Manager or another MDM tool, by pushing PowerShell scripts to the machines

3. Scan once script method - By manually starting (or via GPO) scripts on the machines

See the flowchart below to help you define the scan method for endpoints:



Note: management platform must be able to send and execute PowerShell scripts with system context on the endpoint.

The following paragraphs explain how to set up the CSAT endpoint scans via each of the methods.

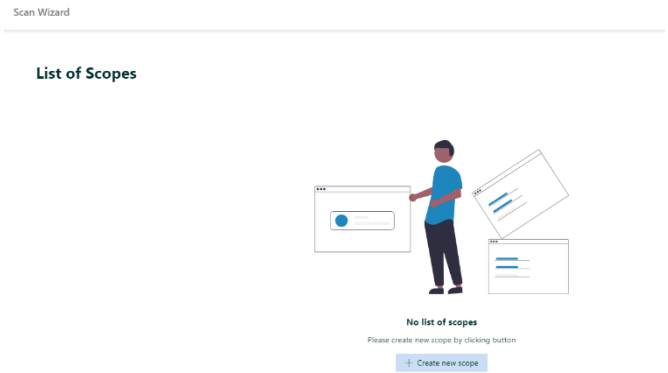
In an assessment, you can combine the methods to reach a variety of endpoints.

Scan scope method

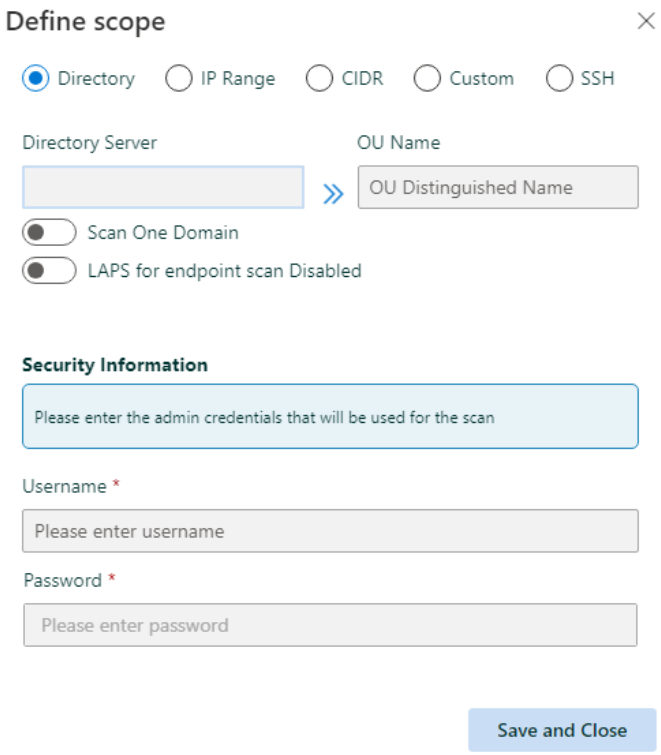
This method is used to scan Windows endpoints that are Domain joined, and it is used to scan Linux endpoints. The endpoints must be able to connect to the CSAT server.

To start an endpoint scan, a scope must be created. Multiple scan scopes can be set up if needed.

In the Scan Wizard page for Endpoints, click on 'Create new scope'.

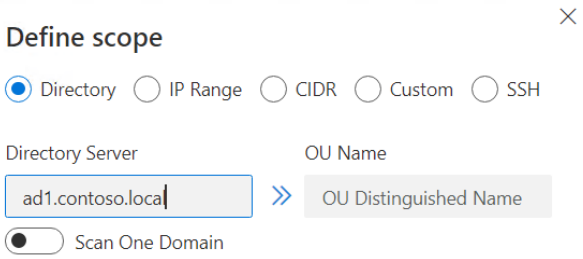


There are five ways to define a scope: 1. Directory, 2. IP Range, 3. CIDR, 4. Custom and 5. SSH.



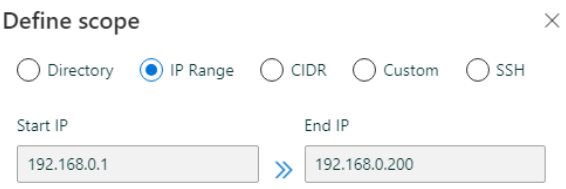
1. Directory

Enter the IP address or name of one of the domain controllers. If you want to limit the scope to only an Organizational Unit (OU), define the group under OU name. If you do not define a group in the OU name, the entire directory will be scanned. To only scan an Organizational Unit, specify the full distinguished name in the field 'OU name'.



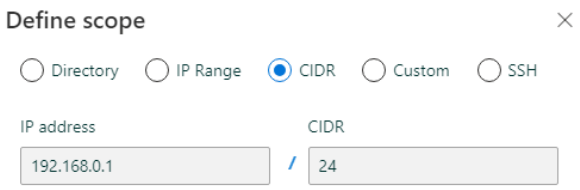
2. IP range

To scan machines within a certain IP range, enter the Start IP and End IP of the range you want to have in scope.



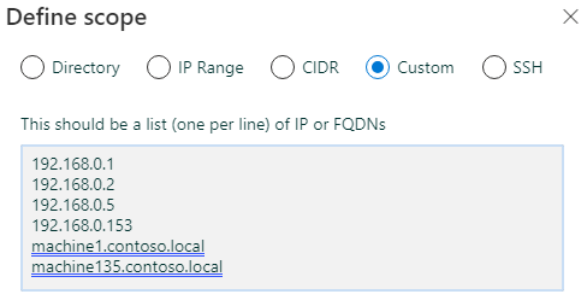
3. CIDR

You can also define the scope through a range of IP addresses with the CIDR networking prefix.



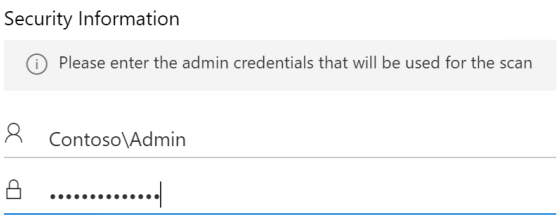
4. Custom

With this option you can define a scope by entering a FQDN or an IP address(es) you want to scan. You can enter multiple FQDN and IP addresses.

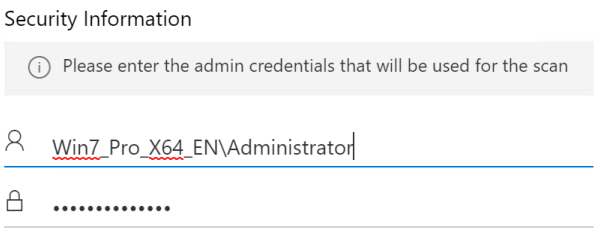


Windows Endpoint Credentials

Independent of the four ways above to define scan scopes, CSAT will need a Username and Password to run the scan. For Windows domain machines the username is Domain\Username.

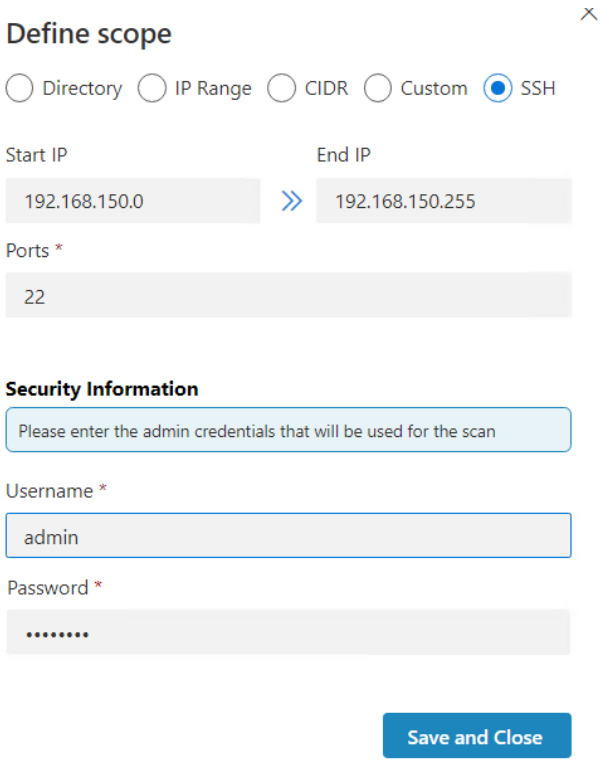


If you want to scan a non-domain joined endpoint, you need to enter 'device name\username' or '.\username'. For example:



5. SSH

The last option is SSH. This scan is used to scan Linux Operating Systems.



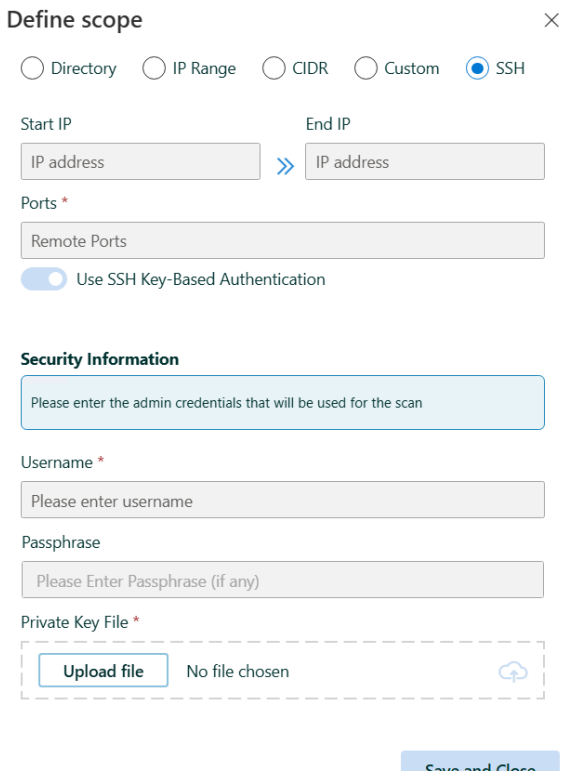
Linux machines can be scanned using SSH. The SSH scan can be configured directly from the CSAT interface. When you set up this scan, ensure that SSH is enabled on the devices in the scan scope. The default TCP port for SSH is 22.

Linux Endpoint Credentials

CSAT will need a Username and Password to run the scan on the Linux Endpoints. The specified account in the CSAT scan scope should be at least a member of the SUDO group. The reason is because certain used commands require the SUDO permissions.

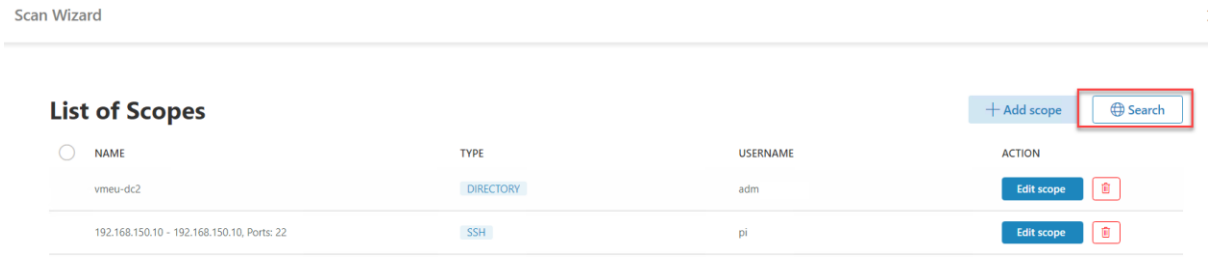
Linux certificate based authentication

The Linux SSH scan also supports certificate-based authentication. To use certificate-based authentication, ensure the certificate is installed on the machine that will be scanned and enable the option '' in CSAT. When you enable this option, a few fields will change. The password field will change to 'Passphrase' this field is optional and should be used if a password is required for certificate. The other field is and upload for the certificate that is used for authentication.

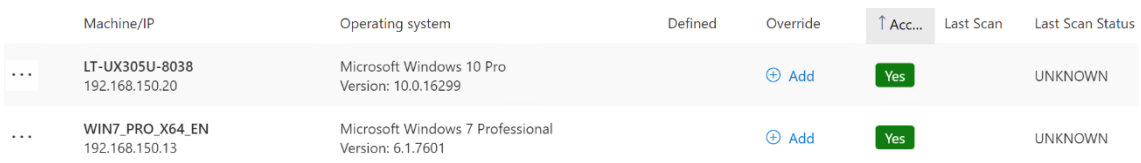


Discover the available endpoints

After you have defined the endpoint scan scopes, a discovery must be started. Click the 'Search' button in the top right of the screen. A notification will be shown if you want to start discovering the machines (Endpoints) that are in the selected scopes.

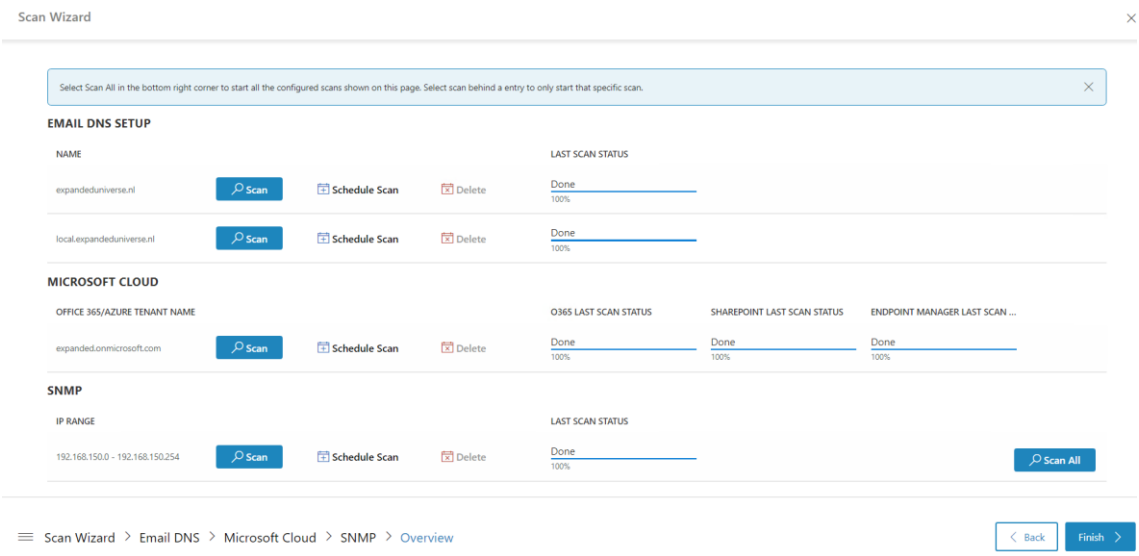


CSAT checks which machines within the defined scope are available and will provide feedback on the screen. Endpoint records with a green 'yes' in the accessible column, CSAT will be able to scan. If a grey 'No' is shown in the accessible column, the endpoint cannot be scanned. Examples of what could cause this are: wrong credentials, firewall ports that are not open. How you can solve these issues can be found in the document 'General Troubleshooting Document CSAT.pdf'



Overview page

The last page of the Scan wizard is the Overview page. On this page all scans that you have setup will be shown.



For all scans there is the option to set up a schedule. This schedule can be created by using the 'Schedule Scan' button. Use the 'Delete' button to delete a scan schedule. To start all the scans at once, click on 'Start all scans'. If you want to scan one single item, click the 'Scan' button in one of the entries.

Cloud scan script method

This paragraph describes how to set up the Endpoint scan via Microsoft Endpoint Manager or another MDM solution, by pushing a PowerShell script to the machines.

The Endpoint scan via PowerShell scripts in Microsoft Endpoint Manager can be used in cases where the endpoint cannot connect directly to the CSAT server. When employees are working from home or when endpoints are managed through Azure AD and Microsoft Endpoint Manager, you can use this method to run the Endpoint scan.

Prerequisites

- The customer must have an active Azure Subscription
- Customer must have Microsoft Endpoint Manager or another MDM solution with the ability to deploy PowerShell scripts to Windows endpoints. The scripts provided are designed and tested for Microsoft Endpoint Manager
- Windows endpoints that are actively running and managed by Microsoft Endpoint Manager or another MDM solution
- .NET Framework 4.7.2 or higher is required on the CSAT server

The following scripts are required to perform the scan with Microsoft Endpoint Manager:

- CSATServer_EnableEndpointCloudScan.ps1
- IME_Device_CSATCloudScan_Template.ps1

The scripts can be downloaded from the Settings/General Configurations page in CSAT (via the Gear icon).

Important: Place both files on the CSAT server in the same directory.

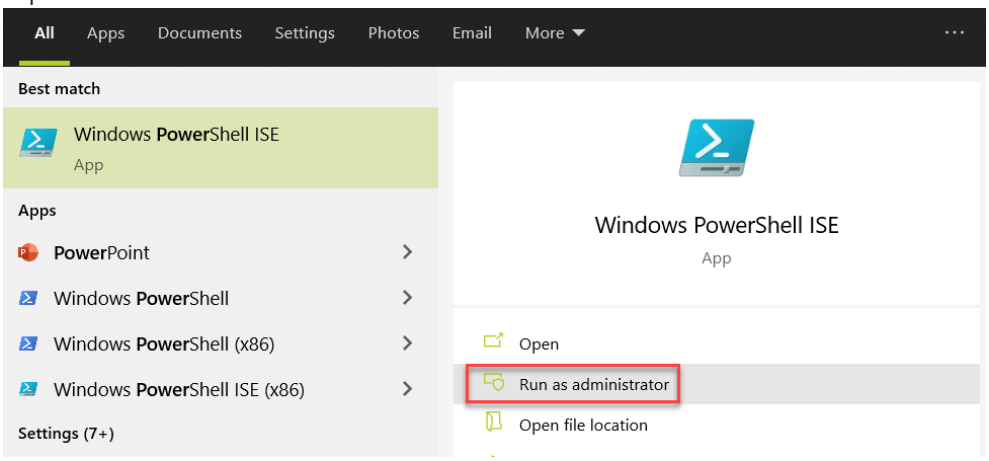
CSATServer_EnableEndpointCloudScan script

The CSATServer_EnableEndpointCloudScan script must be executed on the machine where CSAT is installed. This script will take the following steps:

- Create several directories in C:\Program Files\QS Solutions\CSAT
- Install and Import AZ module
- Login on the tenant of the customer
- Ask to select a subscription if there are more than one
- Create a resource group and storage account on the tenant
- Create two blob storages within the storage account, an upload, and a download blob
- Upload the CSAT dissolvable agent to the download blob
- Create a task scheduler which gathers the CSAT zip files from the upload blob every 10 minutes
- Reporting back the required keys of the newly created blobs

Follow the steps below to use this script.

1. Open a **PowerShell ISE session** with 'Run as administrator'

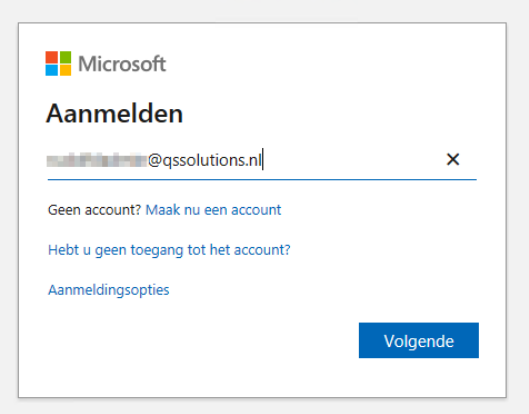


2. Open the **CSATServer_EnableEndpointCloudScan.ps1 script**.
3. Go to Line **100 # Script Specific**. The following lines need to be edited: Line 100, 101 and 102.
   Enter the data between the double quotes ("")
   - At Line 100 `$qAzureLocation` fill in the best supported location for the storage account (e.g., *westeurope*, *northeurope*, *centralus*)
   - At Line 101 `$qAzureRGName` fill in the name of the resource group that will be created
   - **Note: the default name is 'RGCSAT'.** Enter the customer's name behind the default name, for example: '**RGCSATQS'**
   - At Line 102 `$qAzureStorageAccountName` fill in the storage account name that will be created. **Note: This name must be unique in Azure worldwide and must be between 3 and 24 characters in length and use lower-case letters and numbers only.** For example: '**storcsatqs'**
   - In the example shown below, we have set the $AzureLocation to "*westeurope*", $RGName to "*RGCSATQS*" and $StorageAccountName to "*storcsatqs*"

```
# Script Specific
$qAzureLocation = "westeurope" #Please enter the best supported location for the storage account
$qAzureRGName = "RGCSATQS" #Default name RGCSAT put customerspefic behind it.
$qAzureStorageAccountName = "storcsatqs"| #Create unique name, this name must unique for Azure worldwide and must be between 3 and 24
```

4. When the required changes to the script have been made, it is now ready to be executed. Click on the **play button** ( ) or use the **F5 key** to run the script
5. Once the AZ module has been loaded, a login prompt will show. Login with the account of the customer on the Azure tenant, which has administrative privileges

on the Azure Subscription



6. In case there were more than one Azure subscription found, you will be asked to select a subscription. In this step, select the correct subscription by using the number keys
7. Wait a moment for the script to finish. The final output should be as follows:

```
CSAT Scan script template file IME_Device_CSATCloudScan_Template.ps1 found
and content imported
CSAT Microsoft Endpoint Manager Scan script file created
```

8. The server-side script is now finished. You can find the output file named **IME_Device_CSATCloudScan** in the same folder as the other scripts. This file is filled with the correct storage URLs and keys

IME_Device_CSATCloudScan script

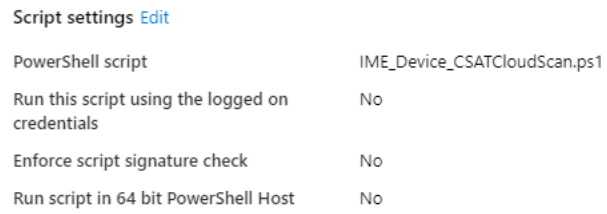
The IME_Device_CSATCloudScan script should be deployed by Microsoft Endpoint Manager to all the endpoints that you want to scan. This script will take the following steps:

- Download the CSAT dissolvable agent from the download blob storage and execute the CSAT endpoint scan
- Upload the scan results to the upload blob storage

To make sure that the script is working correctly, execute the script on the CSAT server (or another machine). Note: the script needs to be executed as local administrator.

Follow the steps below to deploy the script through **Microsoft Endpoint Manager.**

1. Go to the **Microsoft Endpoint Manager admin center**
2. Go to **Devices**
3. Go to **Scripts**
4. Click on **Add** and select **Windows 10**
5. Give the PowerShell Script a name (and description)
6. Upload the **IME_Device_CSATCloudScan.ps1 script** and use the script settings below



7. Assign the script to an Azure AD group
8. Review and add the script. The script will now be deployed to all endpoints in the included group(s). Note: It can happen that Microsoft Endpoint Manager will show that the script has failed, while the script has run successfully

Scan once script method

This paragraph describes how to scan endpoints by placing a script directly on the endpoint, or by deploying the script via a Group Policy.

A script must be executed on an endpoint. Running the script will have the endpoint connect to the CSAT server through port 8080, gathering the CSAT dissolvable agent and executing it, and sending the data back to the CSAT server through port 8080.

Prerequisites

- The endpoints on which the script is executed, must be able to connect to the CSAT server through port 8080

The following script is required to perform the endpoint scan:

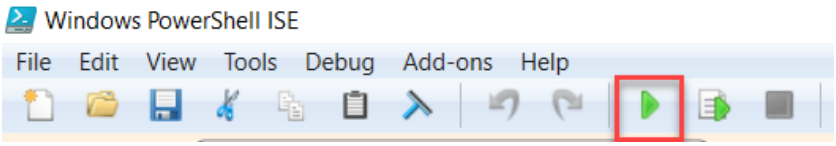
- IME_Device_CSATRunOnce.ps1

The script can be downloaded from the Settings/General Configurations page in CSAT (via the Gear icon).

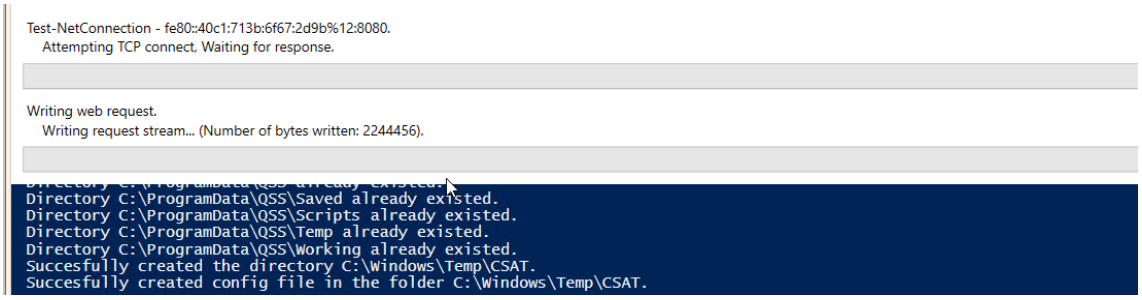
IME_Device_CSATRunOnce script

Open the script in PowerShell ISE as administrator to edit the script. Within the script you must change one variable. It is called `$qCSATServer,` by default it will be filled with `"[CSAT server name]"`.Replace this with the hostname of the CSAT server, make sure to keep the quotes (“”).

Save the script and run it on the endpoints you want to scan, start this process manually with the green button in PowerShell.



When the script has started, the endpoint will connect to the CSAT server, as shown in the following example:

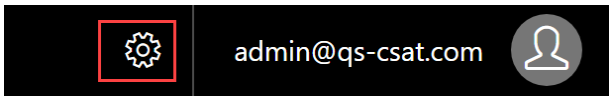


This can take up to 5 minutes to finish, the folder where we temporarily store the CSAT data will be automatically removed afterwards. When the script is finished you will see the endpoint show up in the endpoint overview on the CSAT server.

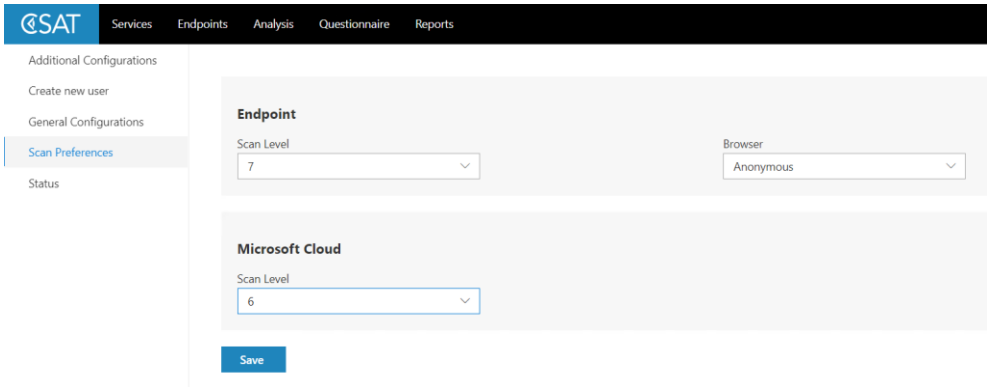
Optional scan settings: scan levels

Change the scan levels

Use the following steps to change the scan level(s). In CSAT, open the settings menu by clicking on the Gear icon in the top right corner next to the logged in username.



On the tab 'Scan Preferences' the scan levels and the browser scan option are shown. Here you can select the desired scan level and browser scan option. When the desired levels are set, click 'Save'.



See the following paragraphs for explanation of the Scan Preferences.

Endpoint Scan Level

In CSAT you can set the level of data that is collected from a Windows endpoint. With a lower level the scan will be faster, however less data is collected. With a higher level the scan will take more time and will collect more data from the endpoint. The default scan level is five. The details about what is scanned on the different levels are as follows:

Scan Level	Scanned features
1	Not used
2	CPU, Machine info, AV status, Local groups, and Local accounts
3	Scanned features from previous levels, Firewall, Registry keys, BitLocker, Installed applications and SQL instances
4	Scanned features from previous levels and Windows Updates, running services, Windows Activation, Shares, SMB version, Running applications and Local GPO
5 (default)	Scanned features from previous levels, hard disk type, hard disk size information and memory size
6	Scanned features from previous levels and Share permissions
7	Scanned features from previous levels, Executed applications and Application history
8	Scanned features from previous levels and Detailed Firewall rules
9	Scanned features from previous levels and Windows Services dependencies

The following chart is an indication of the agent's running duration and the size of data collected by the agent. The given numbers are intended to be used as an indication; your results may differ.

Client type	Scan level	Browser scan	Average scan time	Zip size
Windows Client OS	5	Off	2 min	0,2 MB
Windows Client OS	5	On	2 min 02 sec	1,2 MB
Windows Client OS	9	Off	2 min	0,4 MB
Windows Client OS	9	On	2 min 30 sec	1,5 MB
Windows Server OS	5	Off	1 min 10 sec	0,1 MB
Windows Server OS	9	Off	1 min 15 sec	0,2 MB

Browser Scan

With CSAT you can scan browser history of Chrome, Firefox, Edge Chromium, and Internet Explorer on the endpoints. You can disable or enable this scan, by default the browser scan is disabled. Before enabling the browser scan, ask the customer for consent.

There are three options for the browser scan: 'Off', 'Anonymous' and 'Full'.

With the option 'Off' the browser information is not scanned.
With the option 'Anonymous' the browser information is saved, however the information cannot be related to a specific endpoint.
With the option 'Full' all the information is saved, for example: which endpoint visited which URL.

Microsoft Cloud Scan Level

In CSAT you can set the level of data that is collected from the Microsoft Cloud scan and SharePoint on-premises.

Scan Level	Scanned features
5 (default)	Azure AD, Azure Subscription information, basic Azure Sentinel information, Azure AD conditional access, Azure networking, Microsoft Endpoint Manager, SharePoint (Online) information, Office 365 licenses and Microsoft and Cloud Secure Score
6	Scanned features from previous level, Total SharePoint Online Hubsites, OneDrive Default storage quota, SharePoint Online External Sharing capabilities, and SharePoint (Online) site collection Permissions, SharePoint Externally shared

When setting the scan level to 6, the Microsoft Entra ID scan application will need the 'SharePoint - Sites.FullControl.All' permissions. This is necessary because the API's needs those permissions to collect the data. With other permissions the CSAT PII scan will fail.

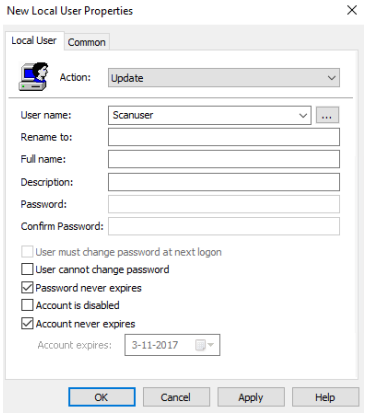
Optional: Add a GPO to create Scan User on endpoints

In case you are using a Domain Admin account to scan the endpoints, you can skip this step.

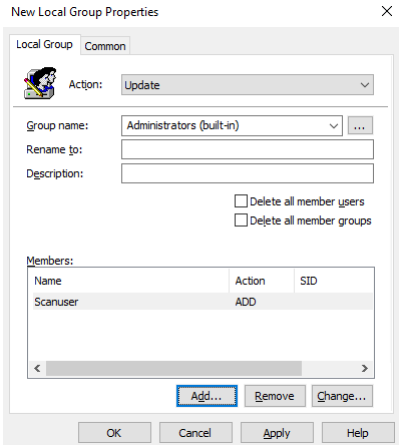
To execute the endpoint scan, a Scan User account is necessary that will be used by CSAT. This account can be either a Domain Admin account or a Local Administrator account on the endpoint.

In the following steps we will create a Group Policy Object (GPO) to create a local administrator account on the domain endpoints:

a. Launch the Group Policy Management Console on a domain controller
b. Right click the target domain that you want the GPO to apply to (Or each OU)
c. Select 'Create a GPO'
d. This will Launch Group Policy Editor
e. Navigate to: Computer Configuration\Preferences\Control Panel Settings\Local Users and Groups
f. Right Click in the blank area and select New – 'Local User'
g. Give your local admin a username. As an example, the name is set to 'Scanuser'
h. Make sure the Password and the Account never expire



a. Click on OK and right click again in the blank area. Select New – 'Local Group'
b. Select in Group name the group 'Administrators (built-in)' and in the members click 'Add'. Type the name of the user account created in step G and click on 'Add'



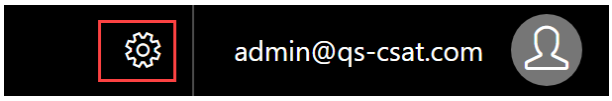
c. Select 'OK'. Now this GPO is connected to the endpoints where you want the Scan user to be available. The account will be created on the machines where this GPO is applied to
d. Note that it might take a reboot or up to a day before the GPO is applied to endpoints

Optional: Upload your own application classification file

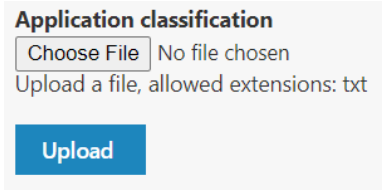
In the Analysis datasets of CSAT, there is information about the Installed Applications. The threat classification for the Installed Applications is based on certain keywords. There is an option to change the classification of the installed applications. The custom classification file must be of the extension 'txt'. An example of a custom application classification file is as follows:

```
#4
Java
Flash
Bittorrent
#3
Dropbox
Box
#2
Winrar
Adobe
```

When an entry is placed under the #2 the entry will be marked as 'Probably normal', when an entry is placed under the #3 the entry will be marked as 'Suspicious' and when an entry is placed under the #4 the item will be marked as 'Bad'. When you have created the text file, you need to upload the file on the CSAT server. To upload the application classification file, click on the Gear icon to open Settings.



After this click on 'Additional Configurations' and find the 'Application classification' part.



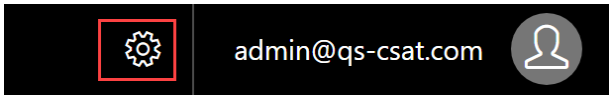
Click on 'Browse' and select your custom application classification text file. The last step is to click on 'Choose file' to upload the file to CSAT.

Optional: Upload your own Registry scan file

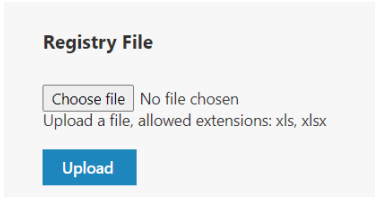
By default, CSAT will scan the endpoint for various registry keys on the Current user and Local machine hive. If you want, you can Upload your own Registry scan file to check your other registry keys. The custom registry file must be of the extension 'XLS' or 'XLSX'. The header rows must be 'Key' and 'Value'. An example of a custom registry Excel file is as follows:

	Key	Value
2	HKEY_CURRENT_USER\Control Panel\Desktop	ScreenSaverActive
3	HKEY_CURRENT_USER\Control Panel\Desktop	ScreenSaverIsSecure
4	HKEY_CURRENT_USER\Control Panel\Desktop	ScreenSaverTimeOut
5	HKEY_CURRENT_USER\SOFTWARE\Policies\Microsoft\Windows\Control Panel\Desktop	ScreenSaverActive
6	HKEY_CURRENT_USER\SOFTWARE\Policies\Microsoft\Windows\Control Panel\Desktop	ScreenSaverIsSecure
7	HKEY_CURRENT_USER\SOFTWARE\Policies\Microsoft\Windows\Control Panel\Desktop	ScreenSaverTimeOut
8	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\setup\recoveryconsol	SecurityLevel
9	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon	AutoAdminLogon
10	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon	CachedLogonsCount
11	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon	DefaultPassword

When you have created the Excel file, you need to upload the file on the CSAT server. To upload a registry file, go to the Settings screen.



After this click 'Additional Configurations', where you will see the option to upload the Registry File.



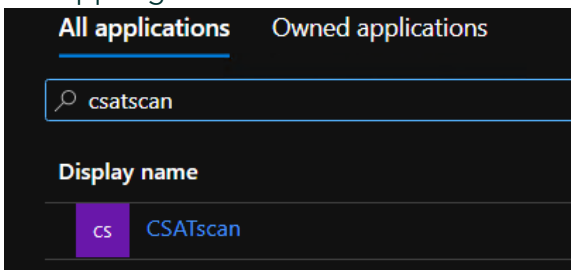
Click 'Choose file' and select your custom registry Excel file. As the last step click 'Upload' to upload the file to CSAT.

Uninstall CSAT and revoke permissions

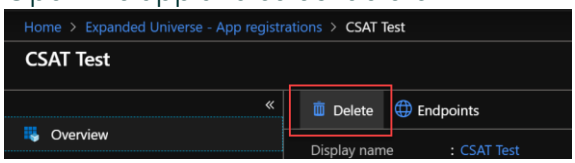
Delete Microsoft Cloud scan CSAT app

For security considerations, if you have finished the Microsoft Cloud scan and don't want to perform Microsoft Cloud scan anymore, it is advised to delete Azure Active Directory CSAT App that was created earlier.

a. To delete the Azure AD app, login on https://portal.azure.com/ with an account that is a global administrator on the Azure tenant, open the Azure AD and Open the App registrations and search for the 'CSATscan' app



b. Open the app and select delete



c. At that point you have deleted the CSAT scan app

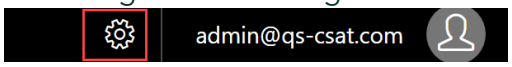
Delete scan account

If you have finished the CSAT scan and do not need the AD scan account or the local scan user account, it is recommended to delete the account(s). To delete the scan user created by GPO, you can change the account in GPO from 'Update' to 'Delete'.

Clear All Credentials from database

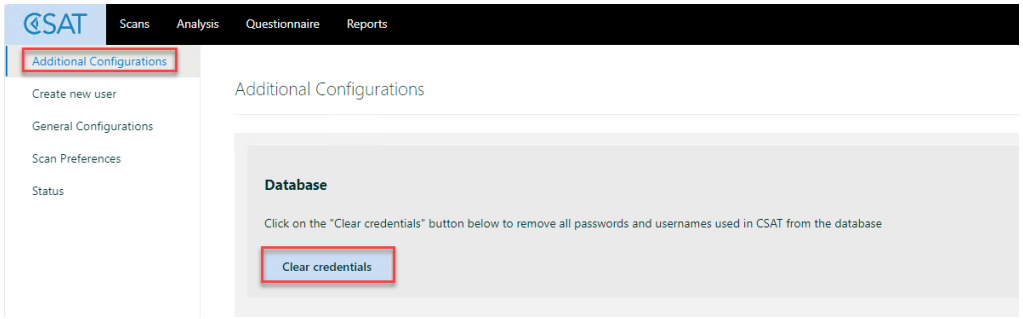
There is a Stored Procedure (SP) available, to purge the CSAT database of all setup scan credentials. For example, the passwords used for AD, endpoint scan, SharePoint On-Premises, and the Microsoft Cloud scan. To run this Stored procedure, use the following steps.

a. In CSAT go to the Settings screen



b. Open the page 'Additional Configurations'

c. Click on the button 'Clear credentials'



Remove VM

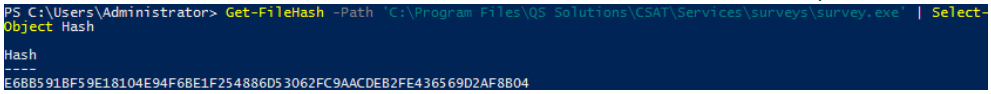
If you have finished the CSAT scan and do not need the Virtual Machine (VM) anymore (if you have used a VM for the CSAT server software), you can unjoin the VM from the domain and remove it.

Addendum

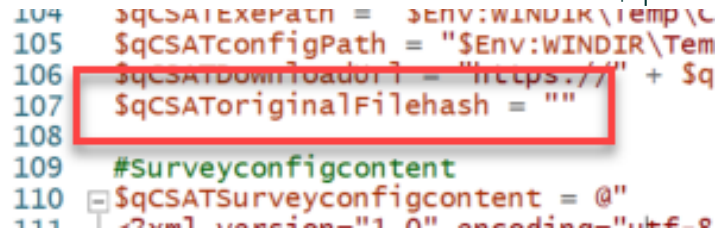
File hash check

In the Microsoft Endpoint Manager script, you can enable the file hash check. With this section you can do a file hash check on the downloaded CSAT.exe from the CSAT server. If the file hash from the CSAT.exe file does not match the script will stop. Use the following steps to enable this part of the script.

a. The first step is to get the File hash from the Survey.exe from the CSAT server. On the CSAT server open PowerShell and run the following command. Without the quotes
b. "Get-FileHash -Path 'C:\Program Files\QS Solutions\CSAT\Services\surveys\survey.exe' | Select-Object Hash"
c. This will show the file hash of the file on the screen. For example



d. Copy the hash value and open the Microsoft Endpoint Manager CSAT script. Paste the value between the "" in the variable $qCSAToriginalFilehash



e. The next step is to enable the file hash check. Set the variable $qCSATFilehashenabled to "Yes"

f. Save the script and upload the script to Microsoft Endpoint Manager

CSAT endpoint firewall rule explanation

CSAT uses the following firewall rules:

- "File and Printer Sharing (NB-Session-In)" with port 139 is used for the NetBIOS Session to the endpoint.
- "File and Printer Sharing (SMB-In)" with port 445 is used to send SMB data for the dissolvable agent to the endpoint(s).
- "Remote Scheduled Tasks Management (RPC)" with the RCP dynamic ports is used to send SMB data for the dissolvable agent to the endpoint(s). The RPC dynamic ports are 49152-65535.
- "Windows Management Instrumentation (DCOM-In)" is used for the initial WMI connection to the endpoint.
- "Windows Management Instrumentation (WMI-In)" is a random port. The port is used to send the CSAT dissolvable agent files to the endpoint. If you want you can change the WMI random port to a fixed port, use the following instruction to set a fixed WMI port on the endpoint "https://docs.microsoft.com/en-us/windows/win32/wmisdk/setting-up-a-fixed-port-for-wmi".
- TCP port 8080: The CSAT agent is undertaking several actions to collect data. After the agent has finished collecting, it sends the data back to the CSAT server. To

send said data the endpoint(s) must be allowed to communicate with the CSAT server over TCP 8080.

SharePoint Online rights

When you scan SharePoint Online with CSAT, Full Control permissions are granted for the application CSAT scans with. We often get the question why CSAT needs Full Control. We want to provide an answer why Full Control permissions are necessary.

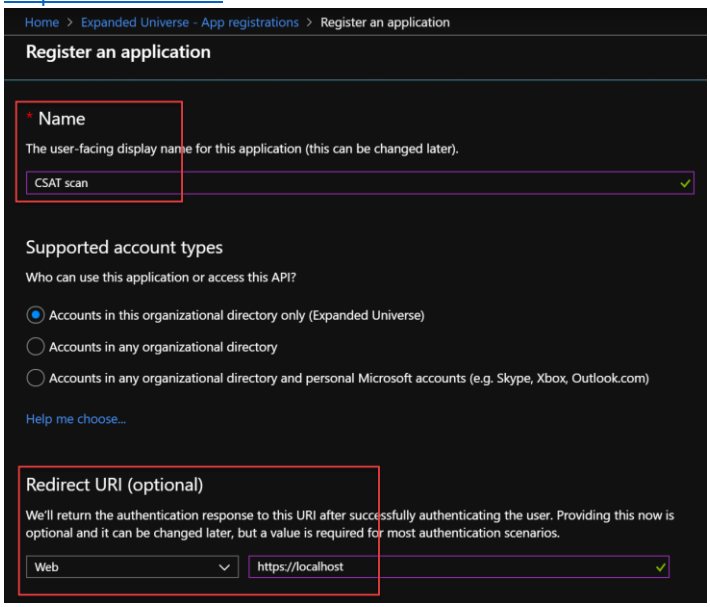
SharePoint Online has several parts. There are site collections, lists, search schema and many more. To each of these parts permissions can be applied. On some of the SharePoint Online parts, read permissions or write permissions can be assigned. There are also parts of SharePoint Online where you cannot give read permissions. CSAT makes use of several of the SharePoint Online parts for the scan, one of those is to query the search of SharePoint Online. To be able to query the SharePoint Online Search the application needs Full Control permissions.

Because CSAT needs full access permissions, we recommend that when the scan is done, the SharePoint Online app permissions are removed. How you can do this can be found in chapter 7.

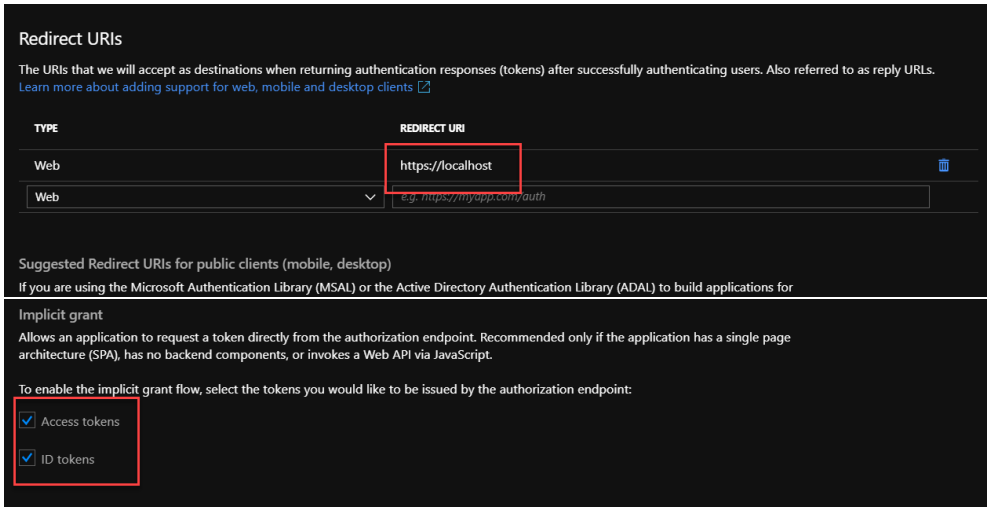
Create Microsoft Cloud Entra ID app manually

If necessary, you can use following steps to create the CSAT scan application manually.

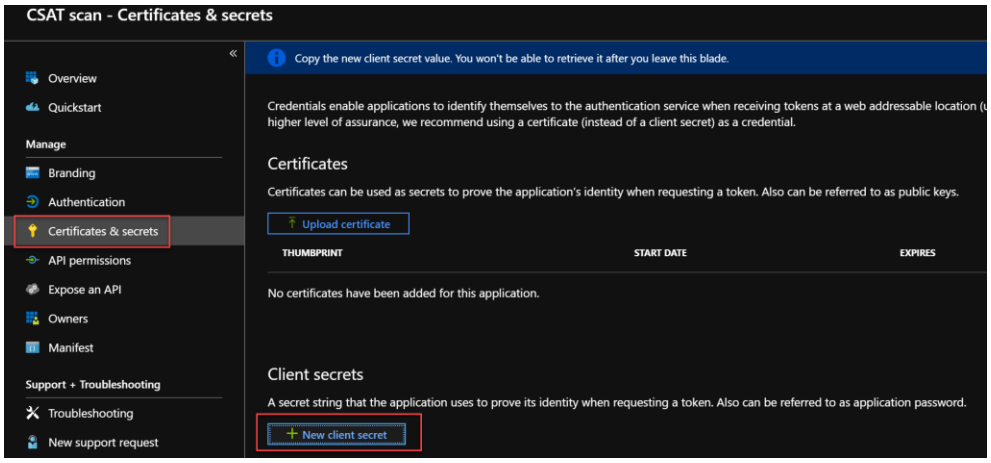
a. First you need to login into the Azure portal. Navigate to the Azure Active directory – App registrations and select 'Register an application'. The name of the app can be anything you like. We recommend using a name where you instantly can see that the app is for CSAT like 'CSAT scan'. Set the 'Redirection URI' to https://localhost



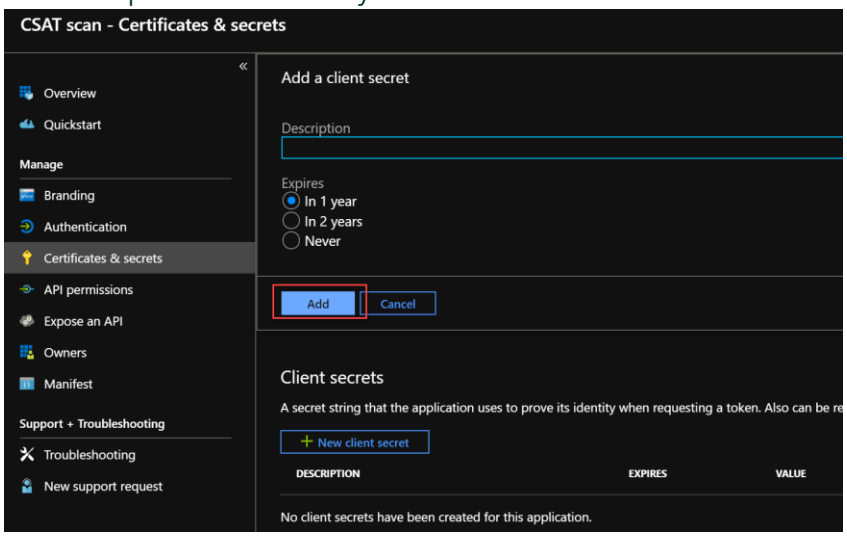
b. When the app has been created it will be opened on the 'Overview' page. Navigate to the 'Authentication' page and confirm that the 'Redirect URI' is set to https://localhost. Almost at the bottom of the page is the checkbox 'Access tokens' and 'ID Tokens', check these boxes and save the application



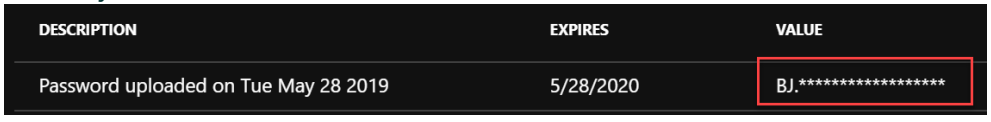
c. Go to the next page which is the 'Certificate & secrets' and create a new Client Secret



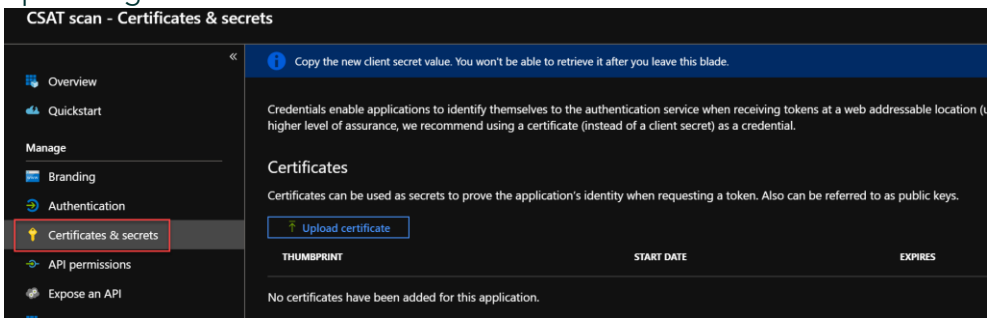
d. We recommend creating a secret with the shortest expiration value available. In the example below is 'In 1 year'. Click 'Add' to create a new secret



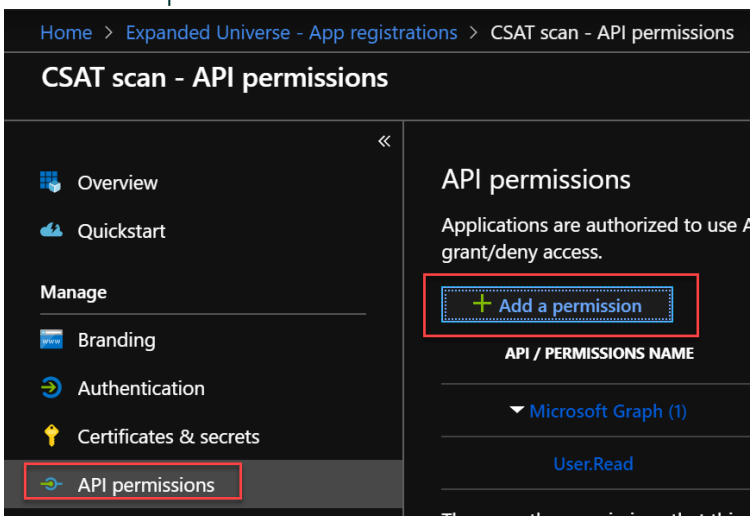
e. A new secret will be created. Save the Value of the app carefully because this value will only be shown once



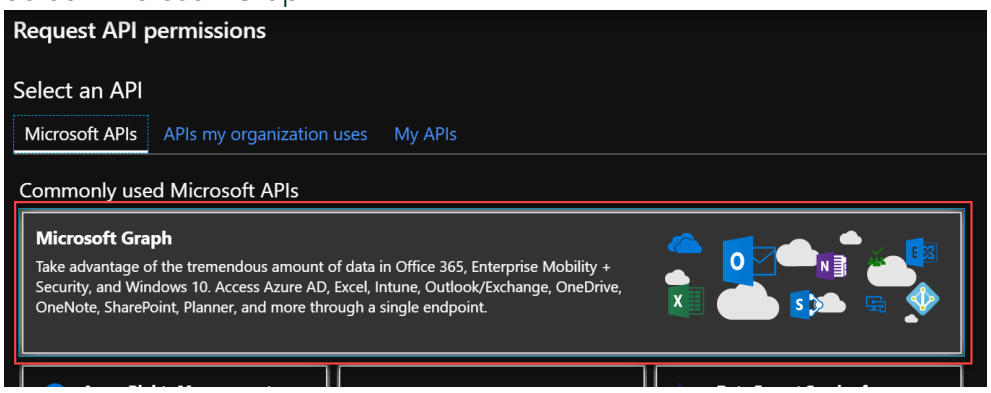
f. Then you need to upload a certificate, download the CSAT scan certificate from: https://csatrelease.blob.core.windows.net/release/CSATCert.cer then add that certificate on the Certificates and secrets page, by selecting Upload certificate and uploading the downloaded certificate.



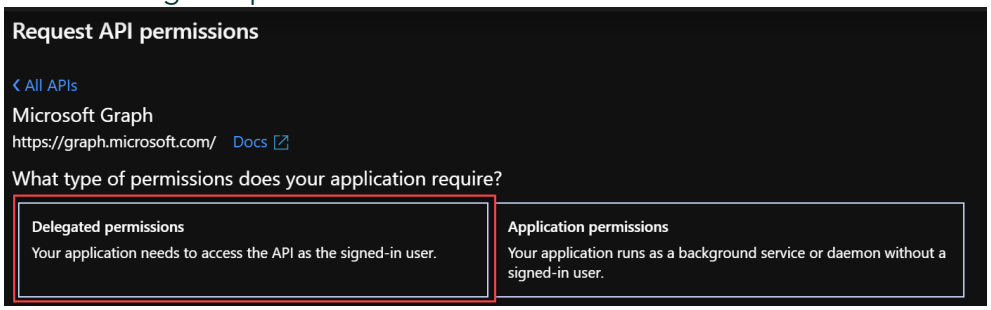
g. Permissions need to be added to the app. Go to the page 'API permissions' and click 'Add a permission'



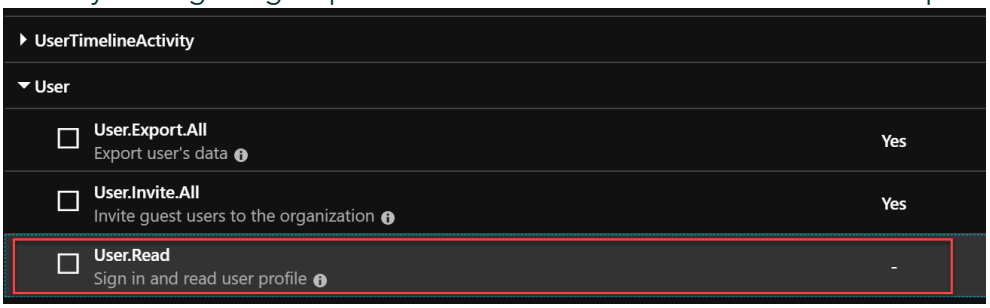
h. Select 'Microsoft Graph' API



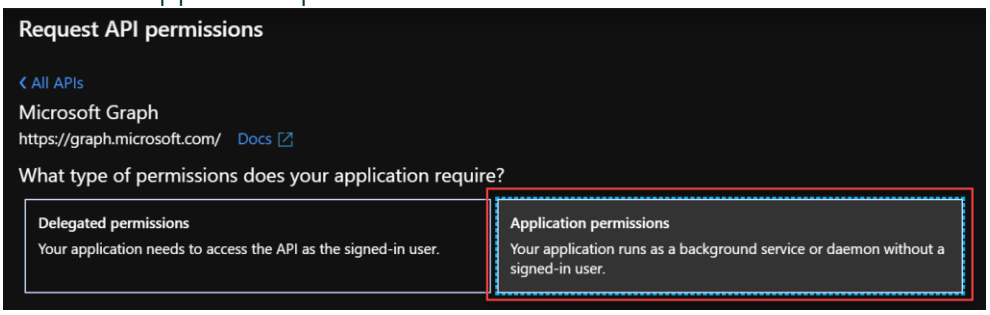
i. Select 'Delegated permissions'



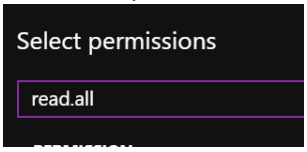
j. Start by finding the group 'User' and deselect the default 'User.Read' permission



k. Switch to 'Application permissions'



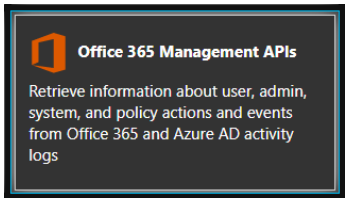
l. On the top bar filter on 'read.all'. At that point only the read permissions are shown



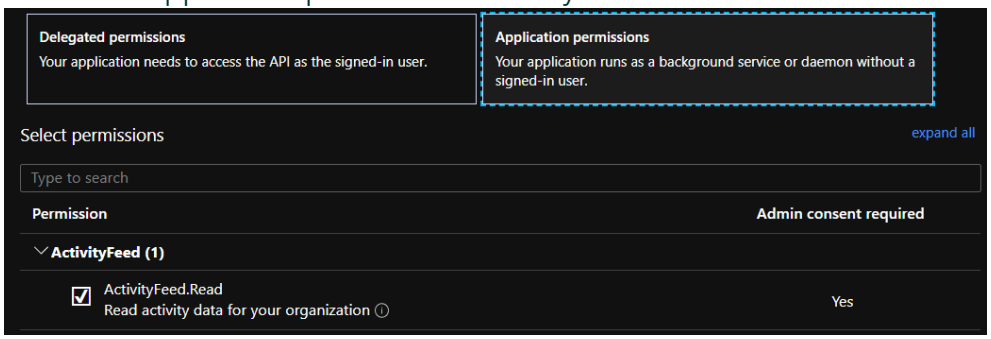
m. Select the following Application permissions:
    1. Application.Read.All
    2. AuditLog.Read.All
    3. DeviceManagementConfiguration.Read.All
    4. DeviceManagementDevices.Read.all
    5. Directory.Read.All
    6. Group.Read.All
    7. IdentityProvider.Read.All
    8. IdentityRiskEvent.Read.All [1]
    9. Policy.Read.All
    10. Reports.Read.All
    11. SecurityEvents.Read.All [1]
    12. Sites.Read.All [1]
    13. User.Read.All
    14. User_Impersonation
    15. RoleManagement.Read.Directory
    16. RoleManagement.Read.All
    17. InformationProtectionPolicy.Read.All

[1] In the 21Vianet tenants these permissions are not available.

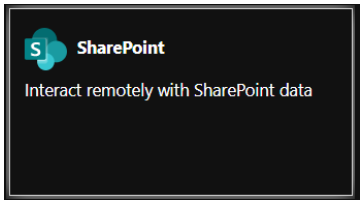
n. Permissions in the Office 365 management API must be added. On the Request API permissions page, select the 'Office 365 Management APIs' item



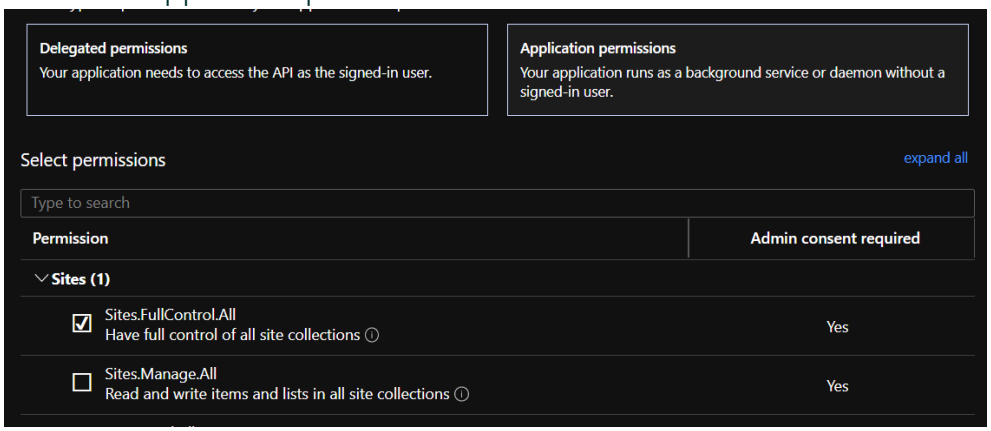
o. Select the Application permissions 'ActivityFeed.Read'



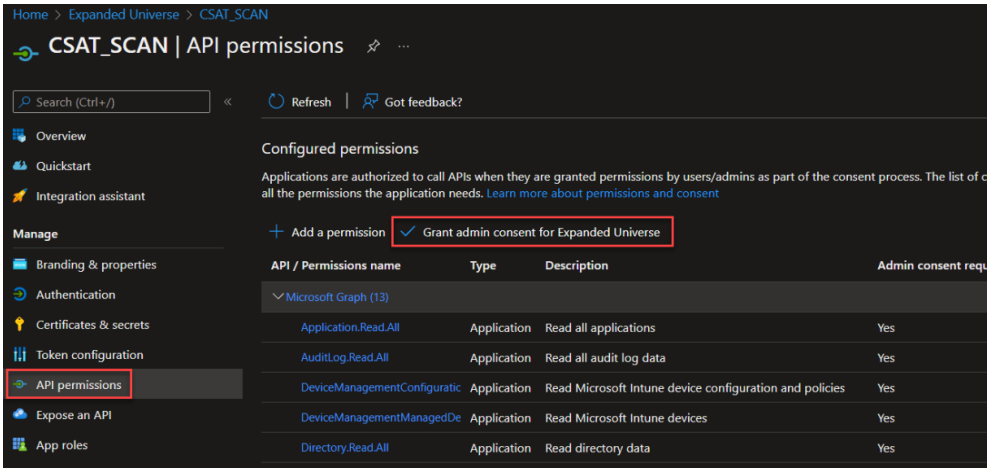
p. **When the Microsoft 'Scan Level' 6 is used**, the following permissions for SharePoint must be added. On the Request API permissions page, select the 'SharePoint' item



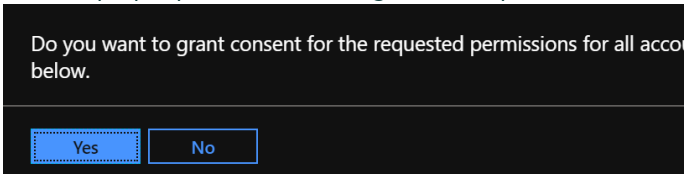
q. Select the Application permissions 'Sites.FullControl.All'



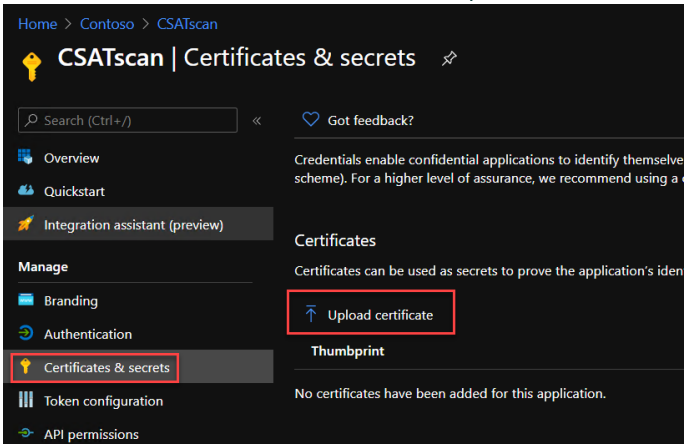
r. When you set the permissions on the app. click on the button 'Grant admin consent for [tenant name]'



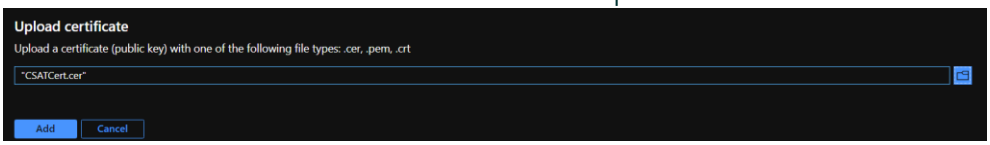
s. On the pop up click 'Yes' to grant the permissions



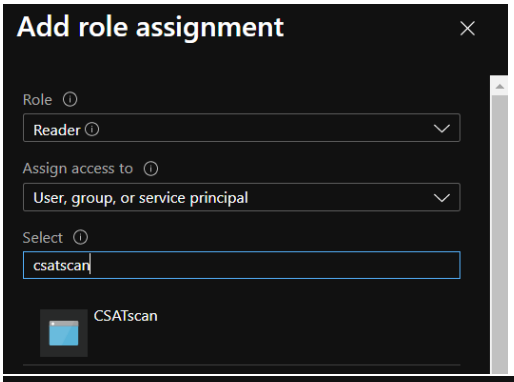
t. You need to place the downloaded certificate in the application. Open the page 'Certificates & secrets' and select 'Upload certificate'

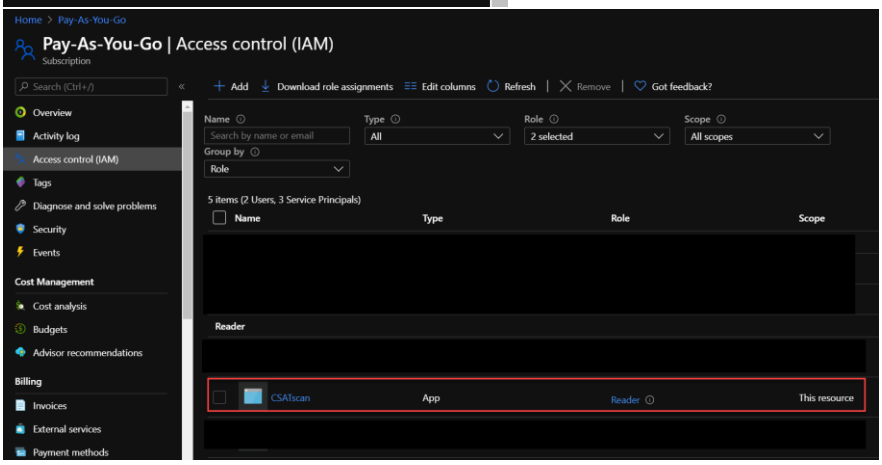


u. Browse to the downloaded certificate from step b and click 'Add'



v. With the Microsoft cloud scan, CSAT can also scan various parts of the Azure environment. If you have one or multiple Azure subscriptions, add the CSATscan application as a reader to the subscription(s). You can add the CSAT scan application by opening Azure subscription and via 'Access control (IAM)', select 'Add' button to add the CSAT application to the subscription as a reader

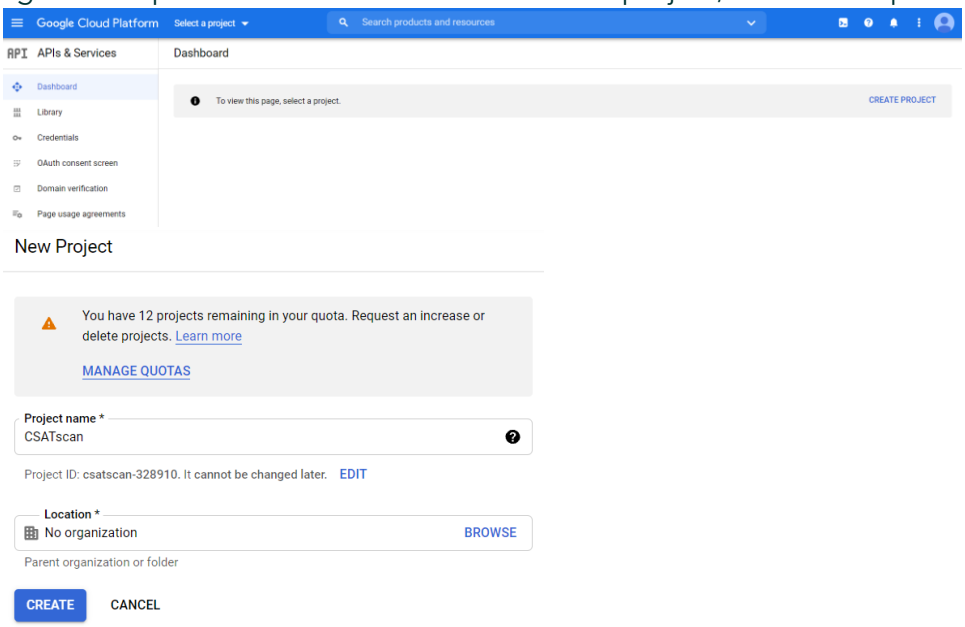




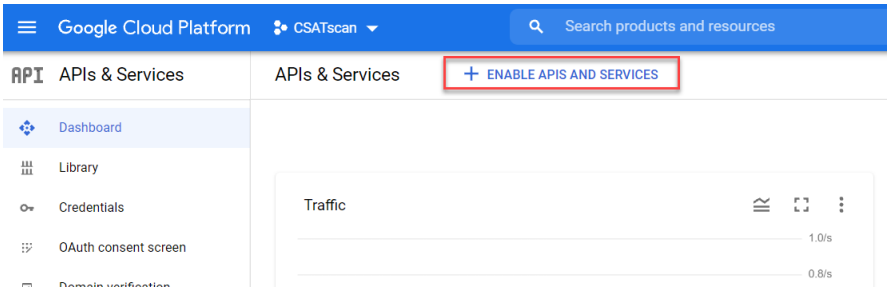
Create Google Workspace scan app manually

If necessary, you can use following steps to create the CSAT scan application manually.

a. To setup the Google Workspace scan, start by logging in to the developer's console of the Google Workspace: https://console.developers.google.com. Login with a Google Workspace admin account. Create a new project, in this example: 'CSATscan'

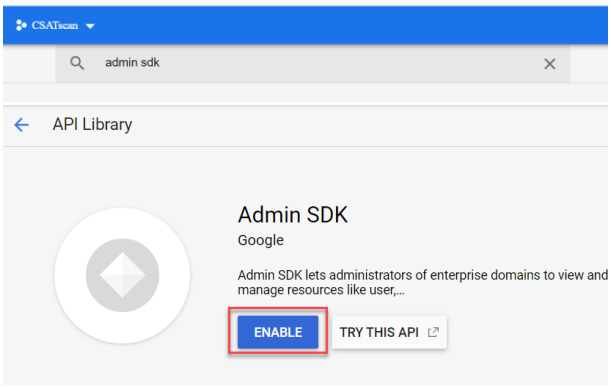


b. When the project is created, select in the top menu 'ENABLE APIS AND SERVICES'

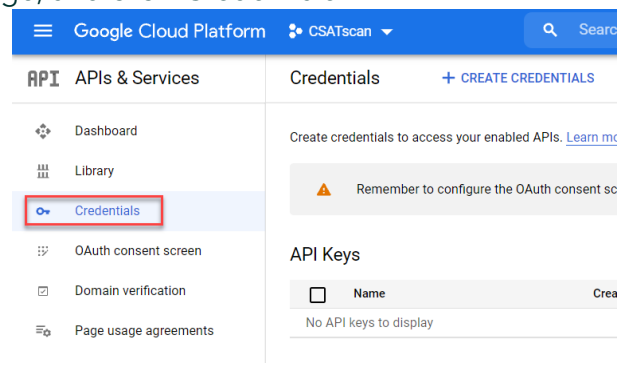


c. There are several API's that need to be enabled. These are:
    a. Admin SDK
    b. Cloud Resource Manager API
    c. Enterprise License Manager API
    d. Google Workspace Alert Center API
    e. Identity and Access Management (IAM) API

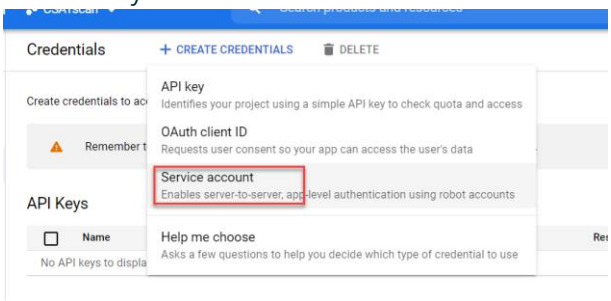
d. Search in the top bar for these API's. You can enable an API for a project by clicking on the API and click on 'Enable'

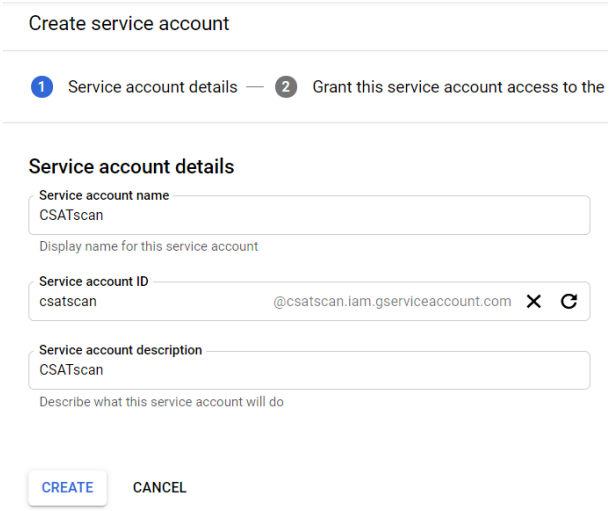


e. When the APIs are enabled, move back to the Google project API's and Services page, and click 'Credentials'

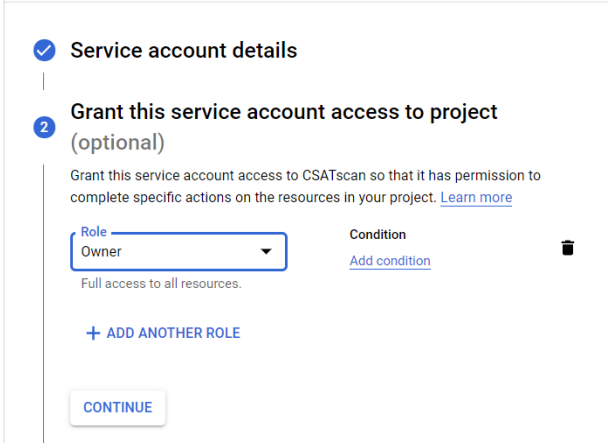


f. Choose the 'Service account' option. We recommend using a name for the service account that you can relate to the CSAT scan

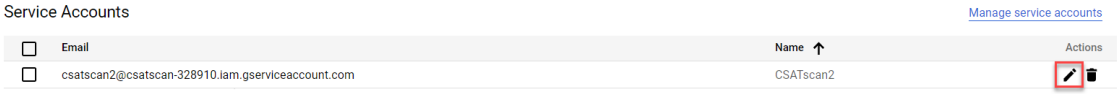




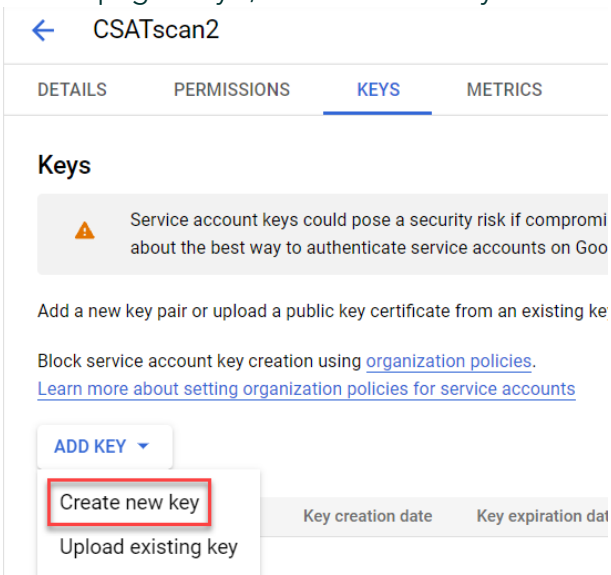
g. When you have entered the name and description click 'Create'. In the next screen you need to give the service account a role. Select the 'Owner' role. Click on 'Continue'. On the third screen click on 'Done'



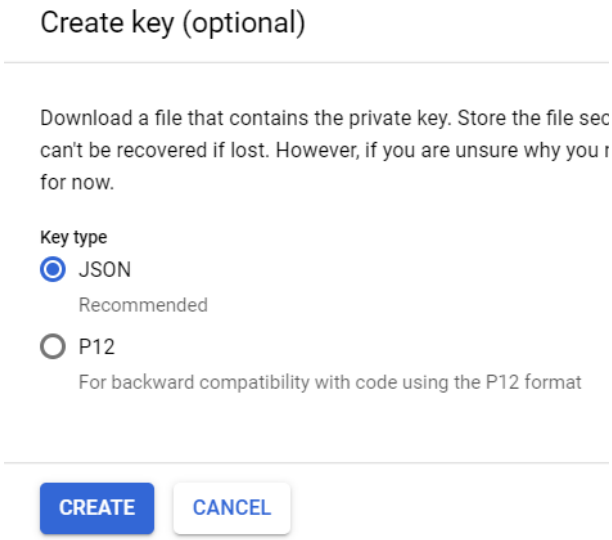
h. When the account is created, click on the pencil icon behind the account



i. Select the page 'Keys', click on 'Add Key' and select the option 'Create new Key'



j. Select either the JSON or the P12 file and click on 'Create'

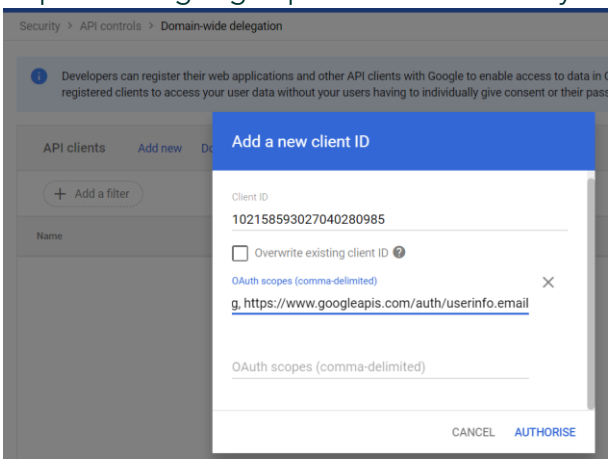


k. A file will be downloaded, save this JSON file since it is needed in a later step.

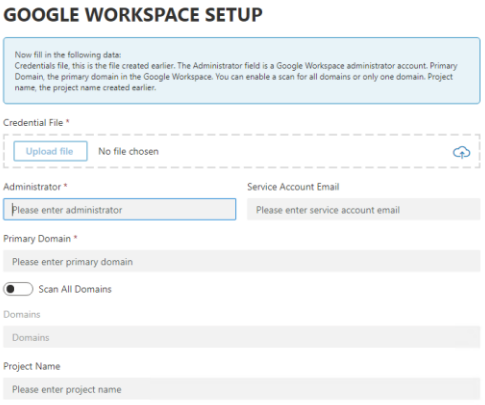
l. Switch over to the Google Workspace admin center, the link to this center is https://admin.google.com/. Click in the admin center Main menu - Security - Access and data control - API Controls. Scroll down to the 'Domain wide delegation pane' and select 'Manage Domain Wide Delegation' and click on 'Add New'. In the Client ID field, enter the Unique ID from the 'Service Account'. In the field 'OAuth scopes', enter the following data in one line and click 'Authorize'

https://www.googleapis.com/auth/admin.directory.customer.readonly,
https://www.googleapis.com/auth/admin.directory.device.mobile.readonly,
https://www.googleapis.com/auth/admin.directory.domain.readonly,
https://www.googleapis.com/auth/admin.directory.group.member.readonly,
https://www.googleapis.com/auth/admin.directory.group.readonly,
https://www.googleapis.com/auth/admin.directory.user.alias.readonly,
https://www.googleapis.com/auth/admin.directory.user.readonly,
https://www.googleapis.com/auth/apps.licensing,
https://www.googleapis.com/auth/userinfo.email,
https://www.googleapis.com/auth/cloud-platform.read-only,
https://www.googleapis.com/auth/admin.directory.rolemanagement.readonly,
https://www.googleapis.com/auth/cloud-platform,
https://www.googleapis.com/auth/apps.alerts,

https://www.googleapis.com/auth/identitytoolkit

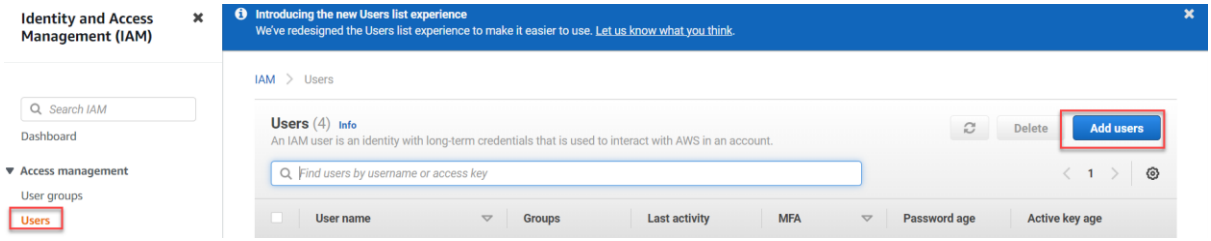


m. The next step is to enter the data in CSAT. Fill in the following data:
   a. Credentials file - The file created earlier
   b. Administrator is a Google Workspace administrator account
   c. Primary Domain - The primary domain in the Google Workspace
   d. You can enable a scan for all domains or only one domain
   e. Project name - the project name created earlier

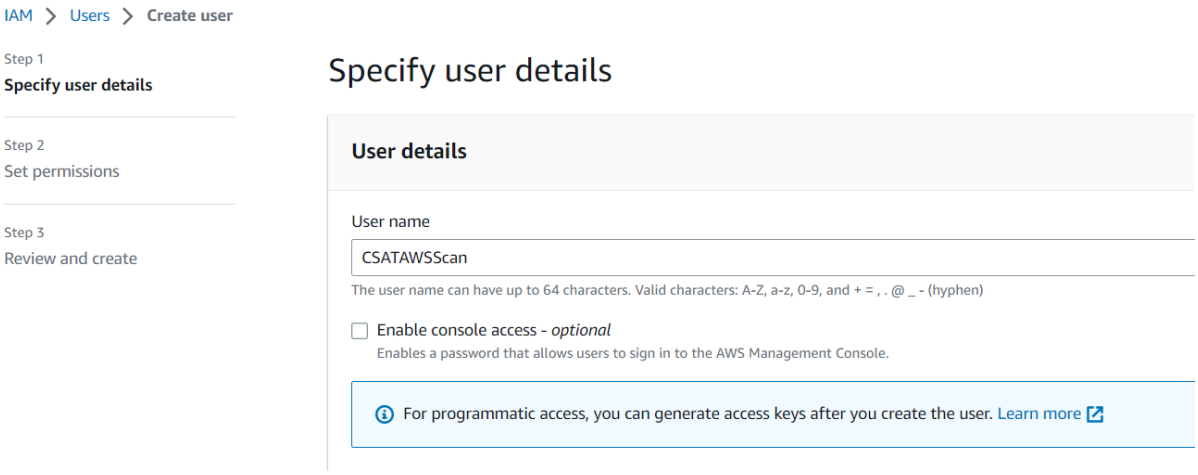


Create AWS scan app manually

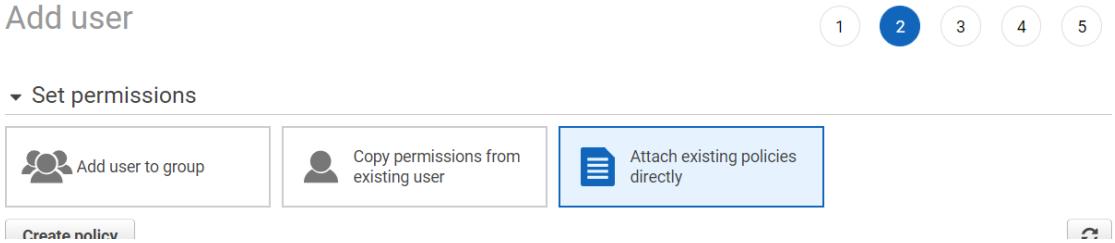
a. The Amazon Web Services scan is performed through the AWS API. An account needs to be created in the AWS environment to provide the necessary access for the CSAT scan. Login into your AWS console with an account that has the AdministratorAccess role. When logged in, open the 'IAM dashboard' and navigate to 'Users'. Click on 'Add users'



b. Give the new user a name and ensure the 'Enable console access' is not enabled

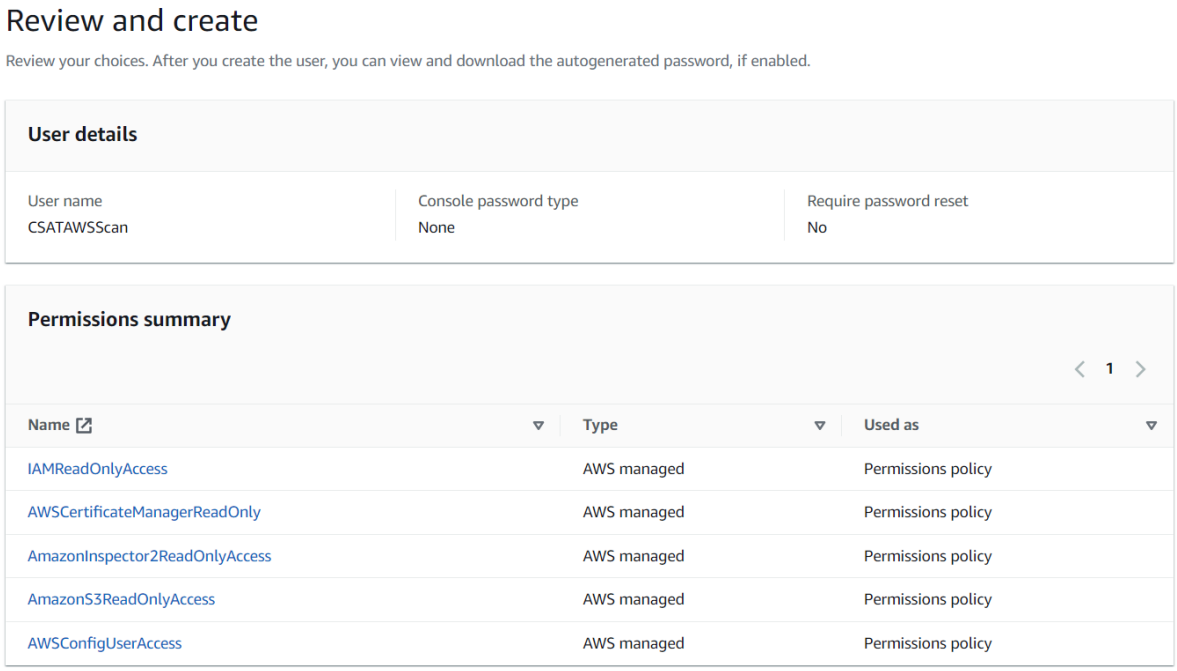


c. Click on next and on the permissions page, click on 'attach existing policies directly'

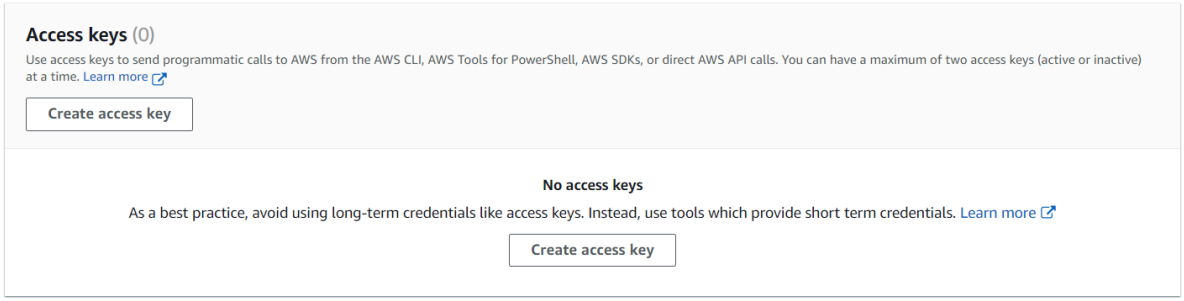


d. Add the following permissions
    a. IAMReadOnlyAccess
    b. AWSCertificateManagerReadOnly
    c. AWSConfigUserAccess
    d. AmazonInspector2ReadOnlyAccess
    e. AmazonS3ReadOnlyAccess

e. Click on next and add tags where necessary. On the review page you can see the account which will be created

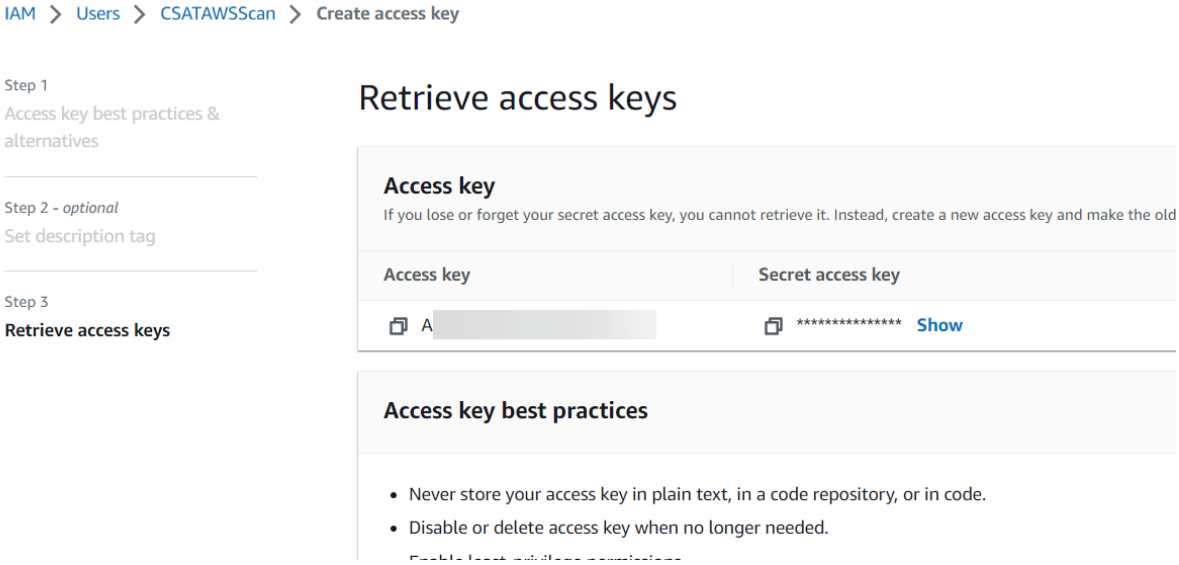


f. Click on ‘Create user’. Then the account will be created. Open the created account and navigate to the ‘Security credentials’. Under the selection ‘Access keys’ select the option ‘Create access key’.



g. On the screen ‘Access key best practices & alternatives’ select the option ‘Application running outside AWS’ and click on next. If necessary, you can enter a tag. Click on ‘create access key’ to continue.

h. A screen will open showing the 'Access key ID' and 'Secret access key'. Save both values carefully because these values need to be entered in CSAT. When the information is saved, switch back to the CSAT wizard.



i. On the AWS wizard page in CSAT enter the 'Access key ID' and 'Secret access key'.