HaloENGINE 6.8

Installation and Configuration Manual

Copyright

Contact

Secude Solutions AG

Landenbergstrasse 34

6005 Luzern

Switzerland

Tel: +41 41 510 70 70

Mail: info@secude.com

Support

Web: https://support.secude.com

Mail: support@secude.com

Table of Contents

1. INTRODUCTION 1

1.1. About this Manual 2

1.2. General Concepts of Classification 2

1.3. Quick Start Installation Summary 5

2. INSTALLING THE HALOENGINE SERVICE 7

2.1. Requirements 7

2.2. Prerequisites 9

2.2.1. Registering an Application in Microsoft Entra ID 9

2.2.2. Create and Configure the Sensitivity Labels 18

2.2.3. Others 18

2.3. HaloENGINE Service Installation Methods 19

2.3.1. Interactive Installation 19

2.3.2. Silent Installation 29

2.4. Configuring the Service 31

2.4.1. Administration Manager Tool 31

2.4.2. Registry Settings 36

2.4.3. Configuring Endpoint 38

3. INSTALLING THE HALOENGINE 43

3.1. System Requirements 43

3.2. Prerequisites 43

3.2.1. Obtain HaloENGINE License 43

3.2.2. Download SAP JCo (only for SAP clients) 45

3.2.3. User Management Settings 46

3.2.4. Forwarding Logs to Microsoft Sentinel 53

3.3. HaloENGINE Installation Methods 57

3.3.1. HaloENGINE Customer Modes 57

3.3.2. HaloENGINE With or Without Monitor Log Dashboard Integration 57

3.3.3. Interactive Installation 58

3.3.4. Silent Installation 67

3.4. Initial Configuration of HaloENGINE Admin Portal 69

3.4.1. Features 69

3.4.2. Reload and Restart....69
3.4.3. Welcome Page....70
3.4.4. Upgrading (Uploading Existing Configuration File)....71
3.4.5. Starting a New HaloENGINE....72
3.5. Setting Up Classification Engine....76
3.5.1. Quick Start Set Up....76
3.5.2. Logging into the Admin Portal....76
3.5.3. HaloENGINE Admin Portal Home Page....77
3.5.4. UI Elements Description....78
3.5.5. Phase 1. Certificate Configuration....80
3.5.6. Phase 2. Create Customer IDS (Only for Multi-Customer Mode)....94
3.5.7. Phase 3. Activate License (First time)....96
3.5.8. Phase 4. Register HaloENGINE Services....98
3.5.9. Phase 5. Configure Profiles and Classification....101
3.5.10. Phase 6. Service Mapping....135
3.5.11. Phase 7. Assign Systems....136
3.5.12. Phase 8. Configure HaloENGINE Features....139
3.5.13. Phase 9. Monitor Log Dashboard....152
3.5.14. Phase 10. Tenant Configuration....160
3.5.15. Phase 11. Monitor Log Validation....164
3.6. System Configuration....166
3.6.1. HaloENGINE Configuration....166
3.6.2. Import/Export Configuration....169
3.6.3. CAD File Types Configuration....170
3.6.4. Download Logs....172
3.6.5. HaloENGINE Admin Activities Log....172
3.6.6. Log Out....173
3.6.7. Change Password....174
3.6.8. Reset Administrator Password....174
3.6.9. Test the Configuration....175
3.6.10. How to Update?....175
3.6.11. HaloENGINE Service Monitor....181
3.6.12. Log Details....183
4. HALOENGINE API....184
4.1. About this Manual....185
4.2. Quick Start....186

4.3. Requirements 187
4.4. API Reference 187
4.4.1. Host/Base URL 187
4.4.2. GetVersion 188
4.4.3. GetRequiredMetaDataTypes 189
4.4.4. GetActionForm 190
4.4.5. ExecuteActionForm 196
4.4.6. DecryptFileAndFetchLabel 202
4.4.7. SendAuditLogData 206
4.5. Error Handling 215
5. TROUBLESHOOTING 216
5.1. HaloENGINE 216
5.1.1. Forgot your Admin Portal Password 216
5.1.2. Cannot Log in to Microsoft after Configuring the Tenant 216
5.1.3. Unable to Load the Admin Portal—Case 2 217
5.1.4. Unable to Load the Admin Portal or PDM Client could not Connect to HaloENGINE 218
5.1.5. Unable to Access Admin Portal on Localhost 219
5.1.6. Unable to Access the Admin Portal with FQDN 221
5.1.7. Protection Fails 221
5.1.8. Dashboard Fails to Load 223
5.2. HaloENGINE Service 224
5.2.1. Installation was Interrupted due to Certificate 224
5.2.2. Installation was Interrupted due to Improper Configuration 226
5.2.3. Network Related Issues 227
5.2.4. Initialization was Interrupted due to Incorrect Azure Details 228
5.2.5. HaloENGINE Service fails to Start 228
6. CUSTOMER SUPPORT AND FEEDBACK 230
6.1. Documentation Feedback 231
7. APPENDIX 232
7.1. Appendix 1 - SNC Configuration 232
7.2. Appendix 2 - Uninstalling the HaloENGINE 237
7.3. Appendix 3 - Uninstalling the HaloENGINE Service 239
7.4. Appendix 4 - Open-source Software (HaloENGINE) 240
7.5. Appendix 5 - Open-source Software (HaloENGINE Service) 248

Typographic Conventions

This guide uses the following typographic conventions to distinguish types of in-text information and icons to alert you to important information.

Convention	Description
Boldface type	• Items you must select, such as menu options, command buttons, or items in a list. • Titles of sections, sub-sections, etc.
Italic type	• To emphasize a word • Error messages • Table and Figure captions
`Consolas Font`	• Package names • Filenames and directory names • XML element names and attribute names • Parameters • File type • Code examples Example: `hesadm.exe start -user <domain\user> -pwd <password>`
Hyperlink	Provides quick and easy access to cross-referenced topics. Hyperlinks are highlighted in blue and underlined.
Admonitions	Note Contains detailed information about a topic and are of direct importance to the subject at hand. Warning Contains information about circumstances, parameters, and so on that MUST be fulfilled. Failure to comply will have consequences for the current operation. Tip Contains useful information about the operation of the application. Info Contains information, guidelines, or suggestions for performing tasks more effectively.

1. Introduction

HaloENGINE is a Java-based component that exposes a web service to HaloCAD for PLM and the HaloCORE SAP Add-On. Both HaloCORE and HaloCAD security solutions use it as a common component. Microsoft Purview Information Protection (MPIP) is seamlessly integrated into HaloCORE and HaloCAD solutions to ensure the protection of your sensitive documents.

HaloENGINE as a common component

HaloENGINE Features

1. Business logic: All business logic decisions are handled by this classification engine.
2. Logging the audit logs: Captures any file uploaded or downloaded, regardless of file protection.
3. Supports SIEM solutions such as Microsoft Azure Sentinel, Splunk, RSA, and others.
4. Halochain investigates the log file.
5. Dashboard: Displays important performance indicators and metrics, providing an overview of the company's data upload and download events.

About HaloENGINE

HaloENGINE is a Java-based component that classifies data into various groups based on defined parameters such as metadata. This classification engine houses any organization's business logic.

What is HaloENGINE Service?

The HaloENGINE Service is a Windows service that connects to the HaloENGINE over TCP/IP. It is the only component that directly communicates with the Azure Right Management Service (Azure RMS) to obtain the MPIP label required to protect a file. It actively listens to HaloENGINE decisions and encrypts and decrypts files based on them.

The rules are defined by the administrator in HaloENGINE based on the requirements of the organization, and the HaloENGINE Service then executes them to encrypt and decrypt files. The processing of PLM CAD and SAP data in HaloCORE and HaloCAD solutions relies heavily on the rules established in HaloENGINE.

1.1. About this Manual

This manual will guide you through the installation and configuration of the following components:

1. HaloENGINE
2. HaloENGINE Service
3. HaloENGINE API

This is the primary document that administrators must read before installing HaloCORE or HaloCAD. Following that, read the installation and operation manuals.

1.2. General Concepts of Classification

Sensitive Data Classification: This is the process of identifying and categorizing all the data in an organization depending on its sensitivity. When a systematic method of data classification is used, sensitive information is adequately protected and made accessible to those who need it. For example, more sensitive data, such as financial information, might be categorized in such a way that disclosure carries a higher risk. General information, such as those utilized for marketing, would be categorized as a lower risk. A higher level of protection is necessary for data identified as having a higher risk, whereas lower-risk data may need proportionately less protection. A data classification schema describes a specific approach to determining data classification levels.

Levels of Sensitive Data

Depending on sensitivity, data is typically categorized into several kinds.

1. **Public**: low data sensitivity
2. **Internal**: moderate data sensitivity
3. **Confidential**: high data sensitivity

You can take suitable action on the appropriate content in this situation with the use of Microsoft Purview's sensitivity labels. Sensitivity labels allow you to identify the level of sensitivity of data across your organization and impose protective settings that are appropriate for the sensitivity of that data.

How are labels created?

Through the Microsoft Purview portal, you can administer how labels are published to your users.

For more details, please refer to Microsoft online documentation.

Classification Scheme

It takes meticulous planning and preparation to define a classification scheme for an organization and set information types and labels. Each organization is unique, and there is no one-size-fits-all data protection rules. You could design your classification scheme based on the business context. Throughout this chapter, a basic-level scenario is used to demonstrate the configuration classification engine. Classifying data can be done in various ways, but most businesses prefer to use a three-level classification schema: Public, Internal, and Confidential.

Best Practices

Consider the following suggestions when creating classification labels:

1. Use existing classification schema (if any).
2. Use sub-labels for key departments. Some departments will have specific needs that require specific labels.
3. Use meaningful label names, it is recommended not to use acronyms as label names. Consider the names as follows for property Sensitivity.
   a. Personal - Non-business data, for personal use only.
   b. Public - Data that is specifically prepared for public consumption, such as marketing material or press announcements.
   c. Confidential - Sensitive business data that could cause damage to the business if shared with unauthorized people. Examples include contracts, security reports, and sales account data.
   d. Secret - Very sensitive business data that would cause damage to the business if it were shared with unauthorized people. Examples include customer information, contract letters, and pre-announced financial reports.

Classification Rule Engine

This is where HaloENGINE's business logic resides. It comprises the following:

1. **Classification Schema** - Defines which data categories will be used to categorize the organization's data.
2. **Classification Rules** - Rules are defined based on metadata and action rules to determine whether to block, label, protect, or decrypt a file.

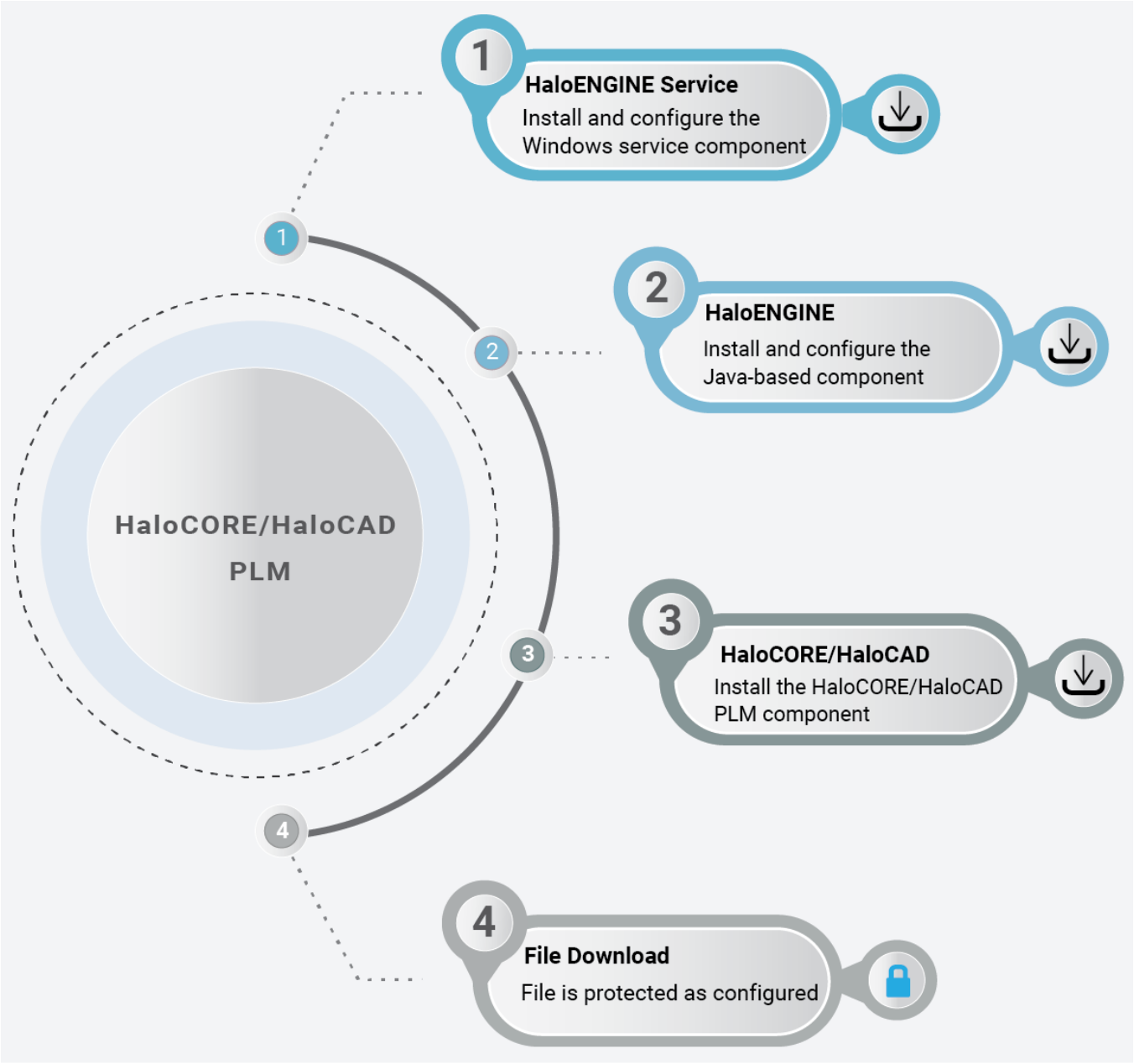
Use the table below to decide how you want to deploy the features.

Actions	Description
Monitor	File uploads and downloads are audited.
Block	File uploads and downloads are blocked.
Label/Protect	File uploads and downloads are classified. Using appropriate MPIP labels, classification labels are embedded in the file metadata.
Notify	Notifies about actions performed via the SAP front-end. Please note that 'Notify' is not supported by non-SAP clients.

Action description

1.3. Quick Start Installation Summary

The following visual illustrates the high-level concept of configuring HaloENGINE in HaloCORE and HaloCAD.



Quick start installation steps

Reference Manuals

The table below describes where to obtain information.

Component	Refer to
Step 1 – Install and configure the Windows Service component.	Refer to the section “Installing the HaloENGINE Service”.
Step 2 – Set up and configure the Java component.	Refer to the section “Installing the HaloENGINE”.
Step 3 – Install HaloCORE or HaloCAD.	Refer to the HaloCORE or HaloCAD manual.

Reference Manuals

2. Installing the HaloENGINE Service

This chapter details the necessary prerequisites for installing HaloENGINE Service.

2.1. Requirements

The following system requirements table specifies the minimum and recommended technical specifications, such as software and network resources, necessary to run HaloENGINE and HaloENGINE Service.

Components	Details
Operating System	HaloENGINE and HaloENGINE Service must be installed on the same server. **HaloENGINE** 1. MongoDB Compass 7.0.7 2. The most recent versions of Microsoft Edge, Chrome, and Firefox are supported by the HaloENGINE Admin portal. **HaloENGINE Service** 1. Supported only in Microsoft Windows Server 2022 and above. 2. Requires **.NET** Framework 4.6.2 and above. 3. Latest Windows system updates installed.
Office 365 Subscription	1. An Azure subscription is required to use Azure RMS and the MPIP functionality. 2. A working Microsoft Entra ID service must be available. 3. Microsoft Purview Information Protection must be fully configured. 4. A valid network path from the server, which will host the HaloENGINE Service, to the RMS service. HaloENGINE Service creates an outbound network communication with Microsoft Azure Services. 5. TLS 1.2 or higher must be enabled to ensure the use of cryptographically secure protocols. 6. Audit logging: Your Azure subscription must include Log Analytics on the same tenant as Microsoft Entra ID. 7. Register an application to get the Application (client) ID and Tenant ID in the Azure portal.

Requirements

Recommended URLs, Addresses, and Ports for MPIP

MIP SDK doesn't support the use of authenticated proxies. So, make sure you set the Microsoft 365 endpoints to bypass the proxy. View a list of endpoints at "Microsoft Online Documentation". However, Microsoft recommends the following:

Addresses	Ports
`*.protection.outlook.com` `40.92.0.0/15`, `40.107.0.0/16`, `52.100.0.0/14`, `52.238.78.88/32`, `104.47.0.0/17`, `2a01:111:f403::/48`	TCP 443
`*.aadrm.com`, `*.azurerms.com`, `*.informationprotection.azure.com`, `ecn.dev.virtualearth.net`, `informationprotection.hosting.portal.azure.net`,`*.office.com` (add `substrate.office.com` if you don't want to add all sub-domains), `crl3.digicert.com`, `crl4.digicert.com`.	TCP 443, 80
For event logging `*.events.data.microsoft.com`	TCP 443
National Cloud	**Microsoft Entra ID authentication endpoint**
Microsoft Entra ID for the US Government	`https://login.microsoftonline.us`
Microsoft Entra ID (global service)	`https://login.microsoftonline.com`

Recommended endpoints

2.2. Prerequisites

A few prerequisites must be met before installing the HaloENGINE Service.

2.2.1. Registering an Application in Microsoft Entra ID

This section will guide you through registering an application, obtaining the Client ID and Directory ID, and assigning permissions to the application.

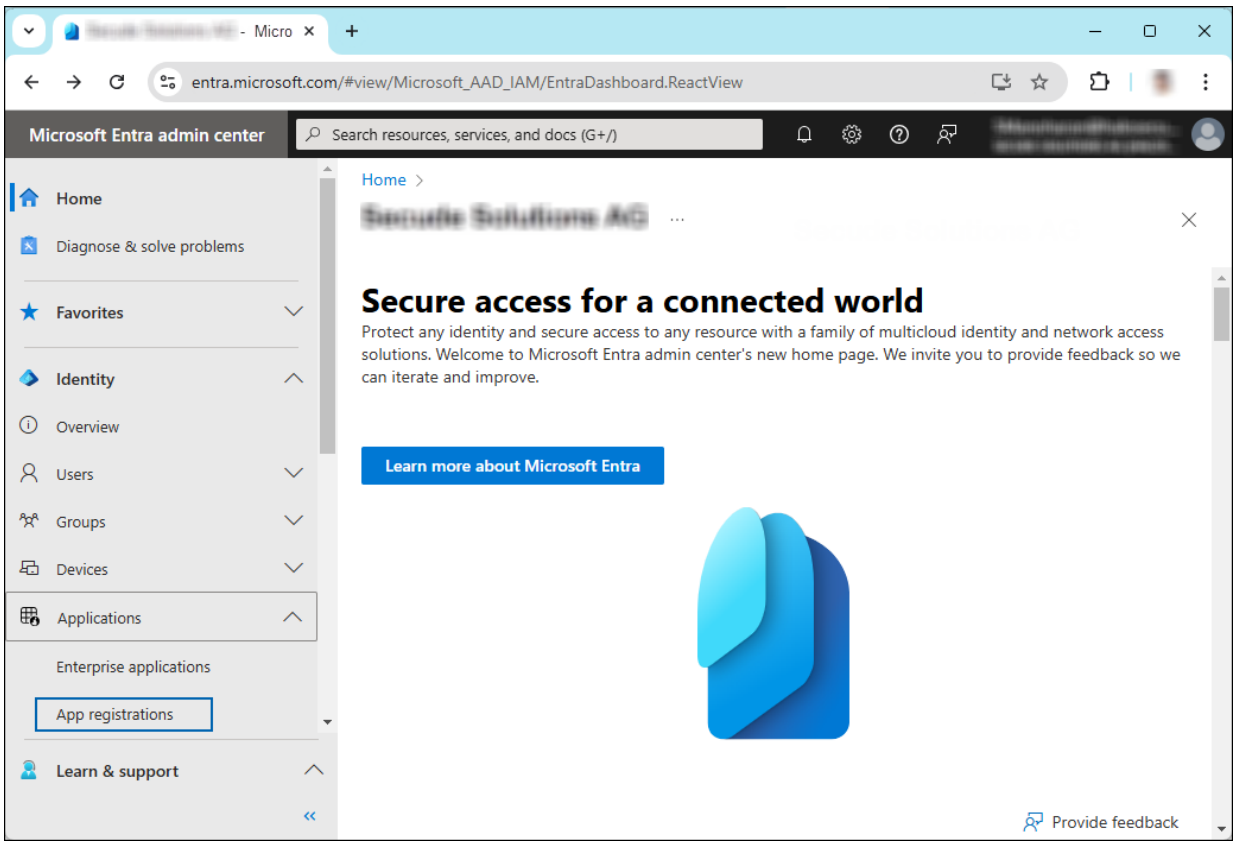
Microsoft documentation
Registering an application in Microsoft Entra ID establishes a trust connection between your application and the identity provider, the Microsoft identity platform.
The information in the Microsoft documentation overrides any information published in this section. For a comprehensive description, refer to Microsoft documentation.

Prerequisite: You must have sufficient permissions to register an application with your Microsoft Entra ID tenant.

2.2.1.1. Create an Application

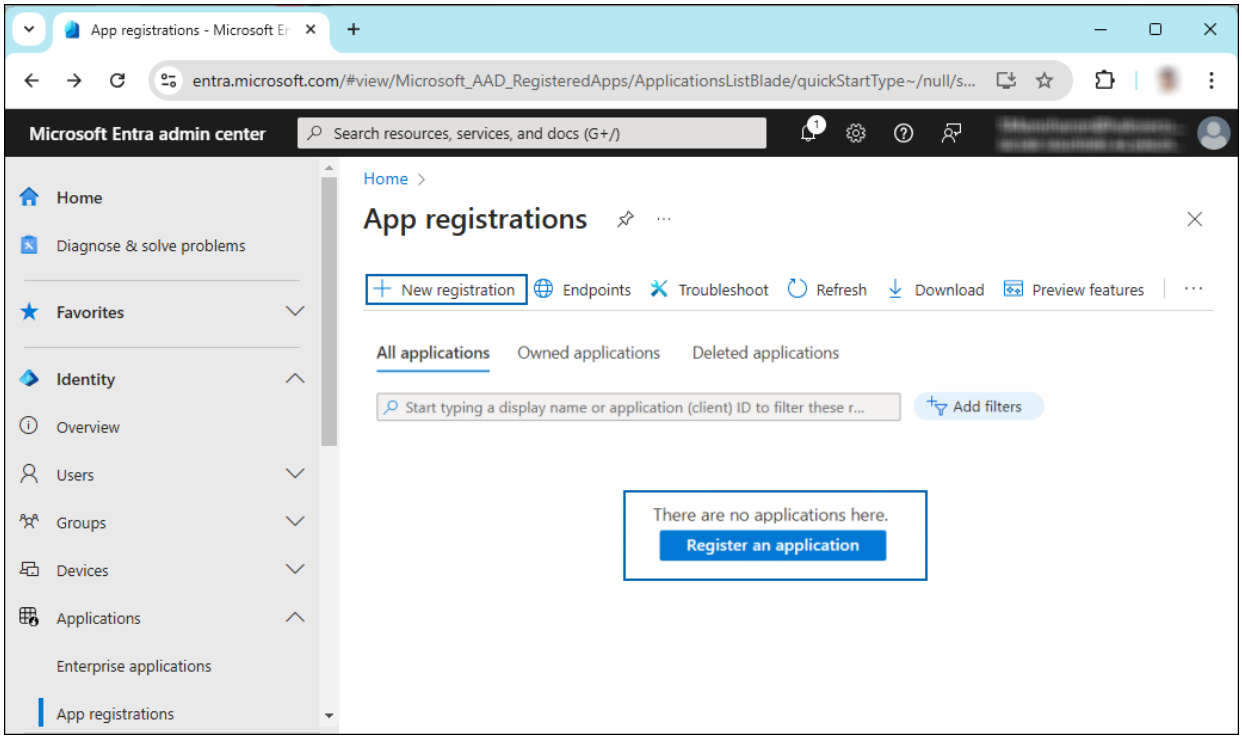
Follow these steps to register the application:

1. Log in to the Microsoft Entra admin center using an account that has administrator privileges.
2. If you have access to multiple tenants, click the Settings icon in the top menu and select the tenant for which you want to register the application from the **Directories + subscriptions** menu.
3. You will be directed to the homepage.



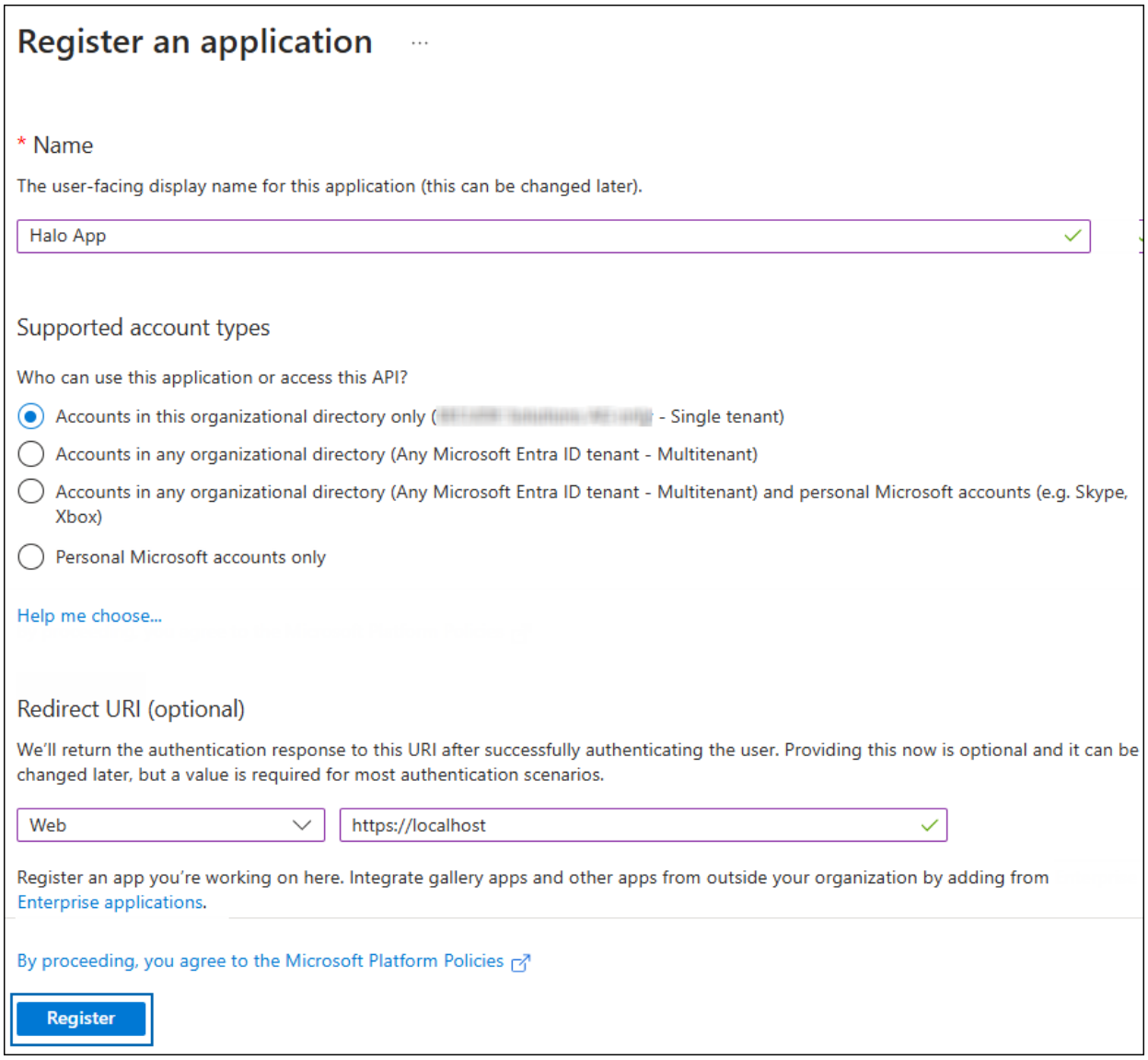
Selecting Microsoft Entra ID

1. Click **Identity** > **Applications** > **App registrations** on the left of the navigation pane.
2. On the **App registrations** page, click the **New registration** page or **Register an Application** button (this button appears only if no applications have already been created).



New application registration

3. On the **Register an application** page, enter the registration details for your application.



Application details

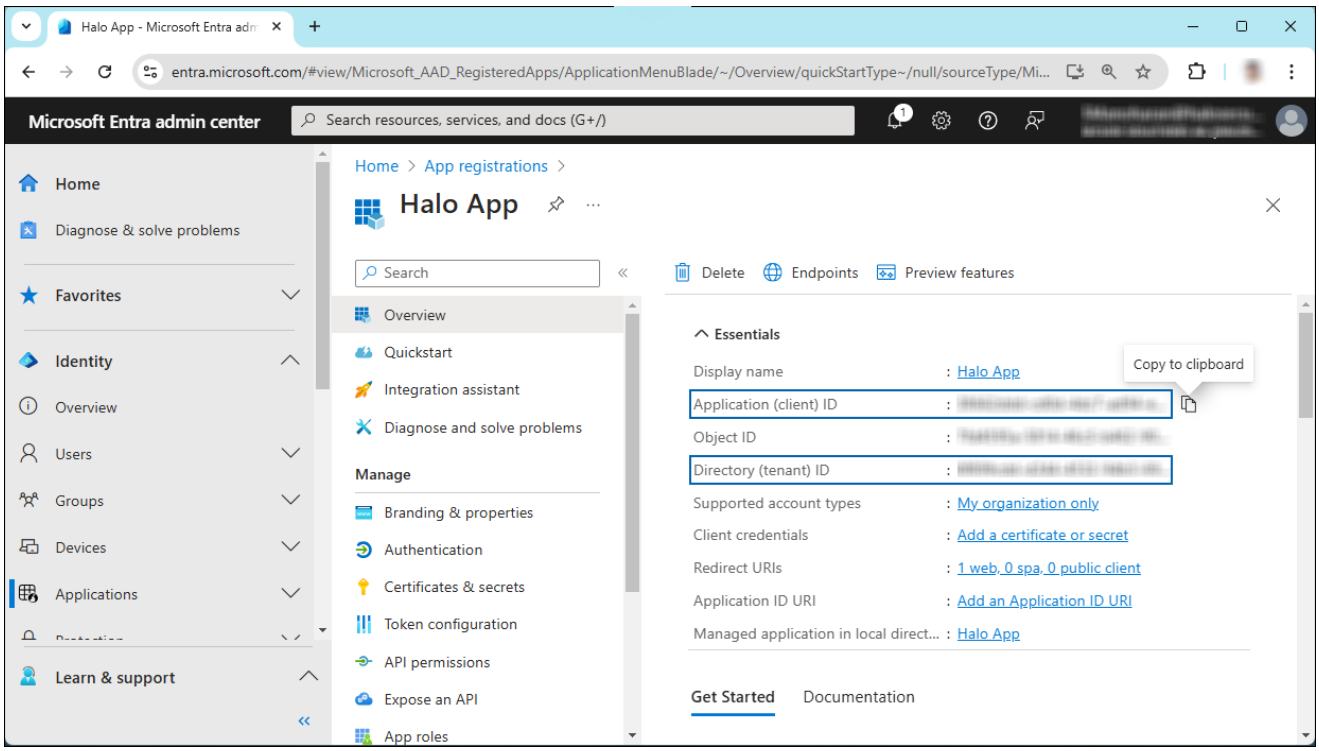
a. In the **Name** field, enter an appropriate application name.

b. Under **Supported account types**, select the option **Accounts in this organizational directory only (single tenant)**. As of now, the HaloENGINE Service only supports a single tenant.

c. Under **Redirect URI**: Select **Web**, and then type a valid redirect URI for your application. For example, `https://localhost`.

d. When finished, click **Register**.

4. The home page of the new application is created and displayed.



Application ID and Tenant ID

5. The following values are shown on the portal once registration is complete. To copy and save the ID value in a text editor, hover your cursor over it and click the **Copy to clipboard** icon.
   a. **Application ID** – It is also referred to as **Client ID**.
   b. **Directory ID** – It is also referred to as **Tenant ID**.

Save the authentication parameters

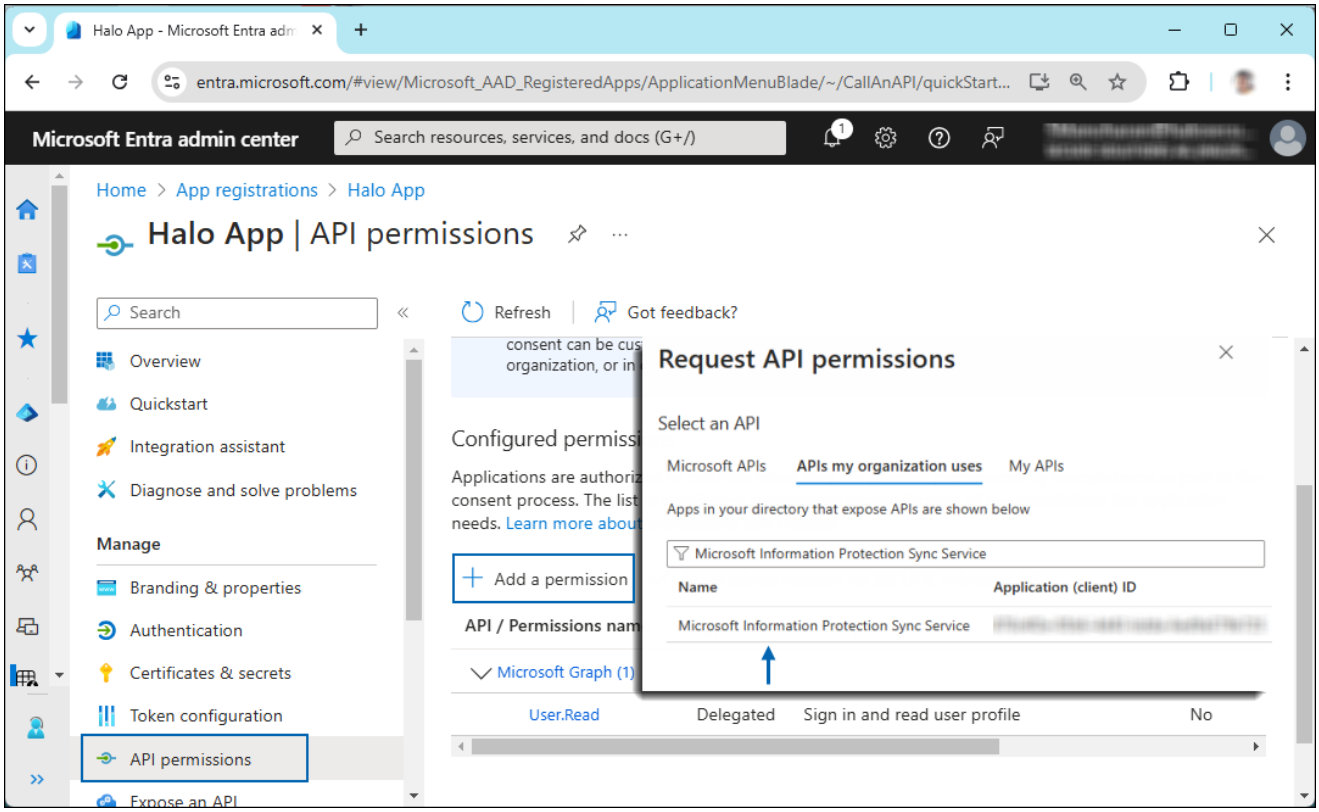
In a text editor (such as Notepad), copy the value of **Application (client) ID** and **Directory (tenant) ID**, and save it for initializing the HaloENGINE Service.

2.2.1.2. Add Required Permissions

To protect content with MIP SDK, you must provide the necessary API permissions to the application created in the previous section.

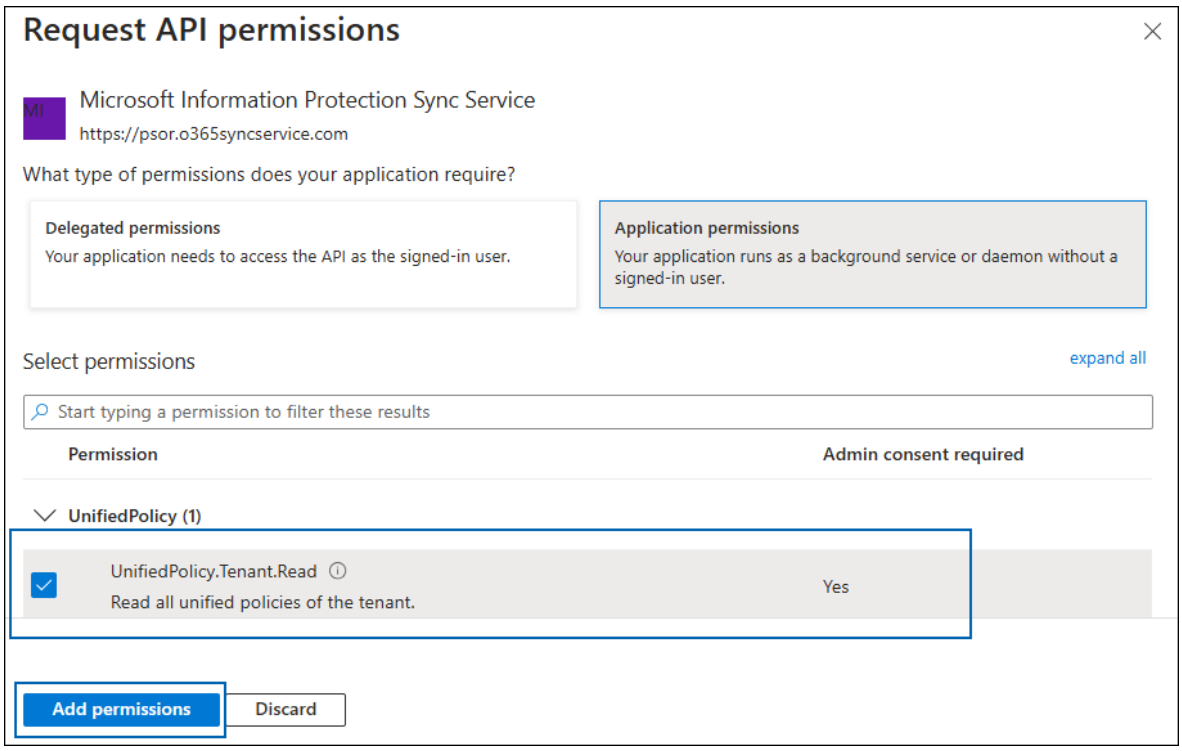
1. In the sidebar of the application page, select **API permissions**. The **API permissions** page for the new application registration page appears.
2. Click **Add a permission** button. The **Request API permissions** page appears.
3. Under the **Select an API** setting, select **APIs my organization uses**. A list appears containing the applications in your directory that expose APIs.
4. In the search box, type in the name of the permission indicated in the "Required Permissions" table below. Alternatively, you could scroll to find the API.

5. For example, type **Microsoft Information Protection Sync Service** into the search box. The following figure shows how the API is listed:



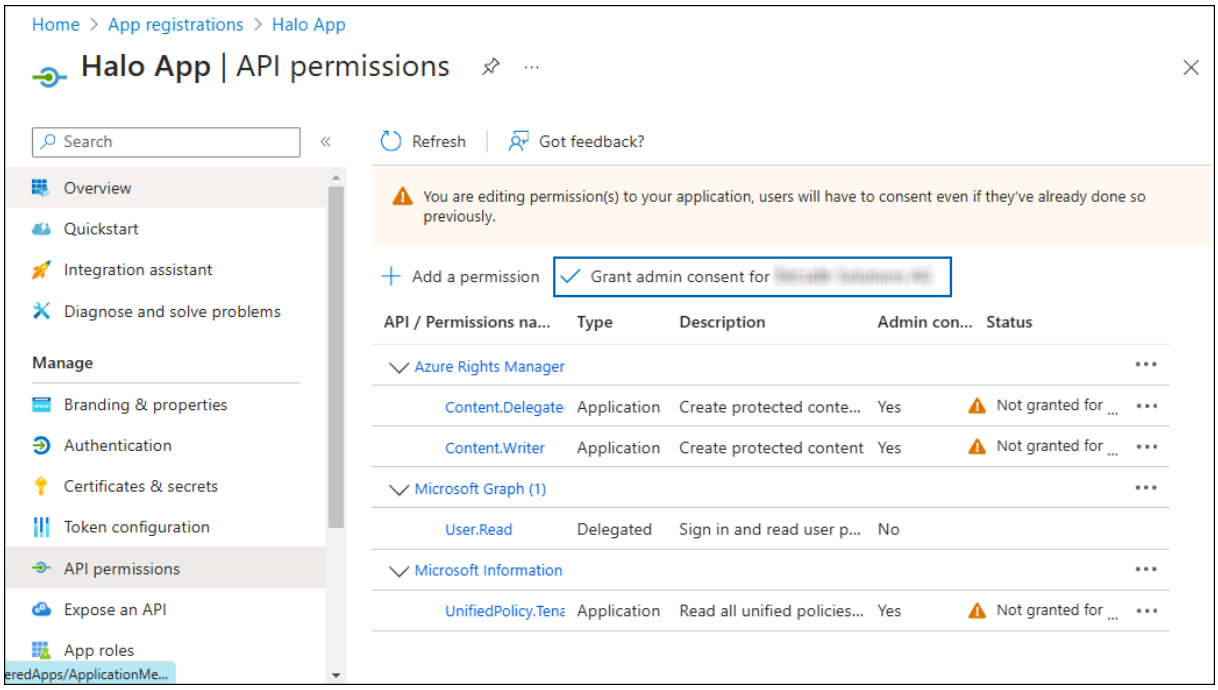
API selection

6. Now, click on the displayed API. You can see two permissions on the page – **Delegated permissions** and **Application permissions**.
7. Click **Application permissions** button and then under the **Permission** section, select the check box against "**Read all unified policies of the tenant**."



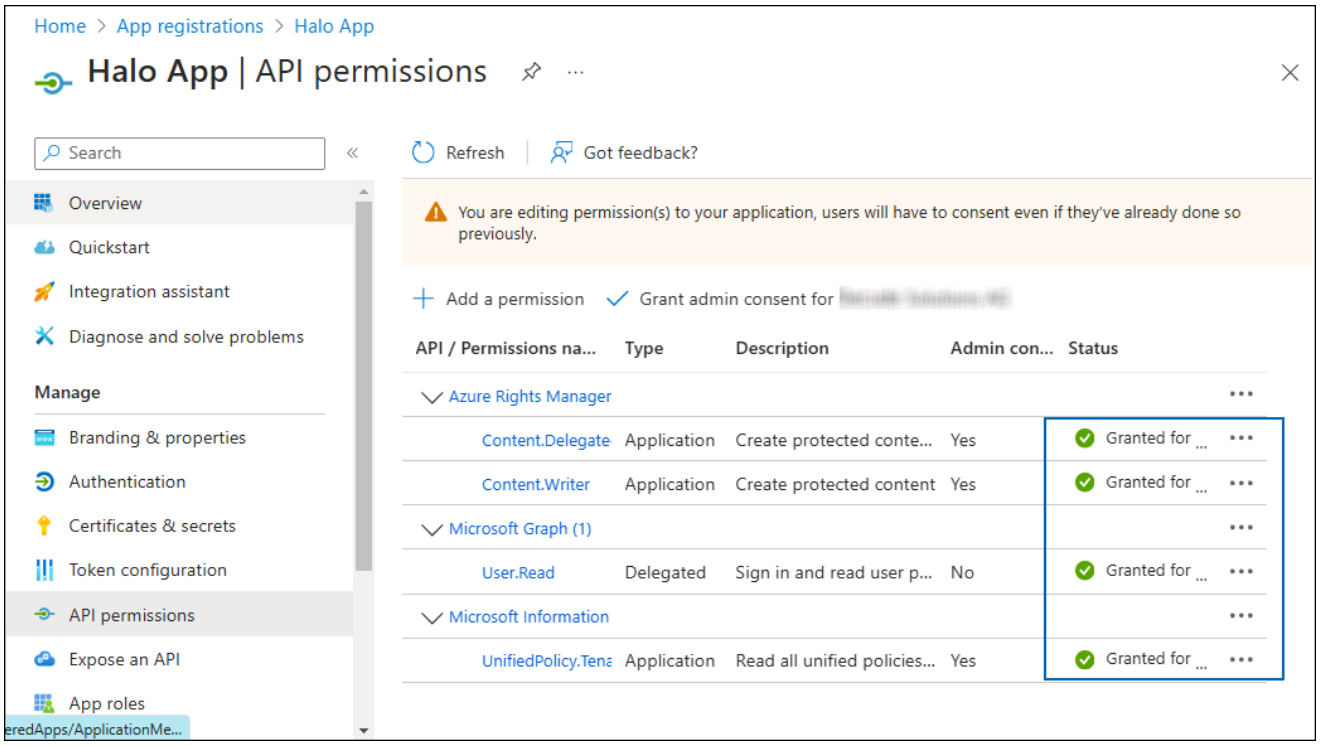
Adding permission

8. Click **Add permissions**.
9. Repeat the steps outlined above to add the other required permissions listed in the “Required permissions” table below.
10. You will be taken back to the **API permissions** page, where the permissions have been saved and added to the table with the status "**Not granted**."



Required API Permissions

11. Click **Grant admin consent for your company** button. You will be prompted to accept the consent confirmation; click **Yes** to the question.
12. After accepting the admin consent, the **Status** will change to "**Granted**."



API Permissions with admin consent

13. The following table lists the required permissions.

API / Permission Name	Display Name	Type	Description
Microsoft Graph	`User.Read`	Delegated	Sign in and read the user profile. This API permission is added by default, but it is not used by the HaloENGINE Service.
Azure Rights Management Services (Microsoft Rights Management Services)	`Content.DelegatedWriter`	Application	Create protected content on behalf of a user
	`Content.Writer`	Application	Create protected content
Microsoft Information Protection Sync Service	`UnifiedPolicy.Tenant.Read`	Application	Read all unified policies of the tenant

Required permissions #1

Additional Permission (Only for Decryption)

The above-mentioned permissions are adequate for applying the MPIP label to a file with the owner as SPN (Service Principal Name) ID or any user email ID. Additionally, the HaloENGINE Service requires the below-mentioned superuser privilege for the decryption function when the owner is not as SPN.

API / Permission Name	Display Name	Type	Description
Azure Rights Management Services (Microsoft Rights Management Services)	`Content.SuperUser`	Application	Read all protected content for this tenant in the Azure portal

Required permissions #2

2.2.1.3. Upload the Certificate in Azure Portal

HaloENGINE Service is based on certificate authentication, so you must enter your certificate information into the registered application.

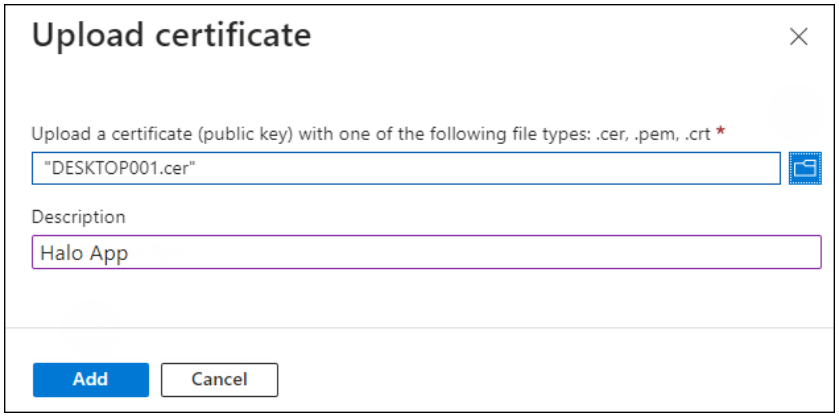
Prerequisites:

1. **Certificate**:
   a. Make sure to have a valid certificate that contains keys such as `-KeyExportPolicy Exportable` and `-KeySpec Signature`.
   b. And that can also be a self-signed certificate. Note: As a best practice and for security reasons, we recommend using a self-signed certificate in a test environment and NOT recommended for a production environment.
2. **Install the certificate**:
   a. Make sure to install this certificate on a Windows Server machine where the HaloENGINE Service is going to be installed.
   b. Certificate Store can either be **Current User** or **Local Computer**.
   c. If it is a self-signed certificate, then it should also be installed in “Trusted Root Certification Authorities”.
   d. If the certificate is signed, then the root CA authority and intermediate CA authority (if any) should also be installed in the respective trusted store.

To upload the public key of the certificate, follow the below steps:

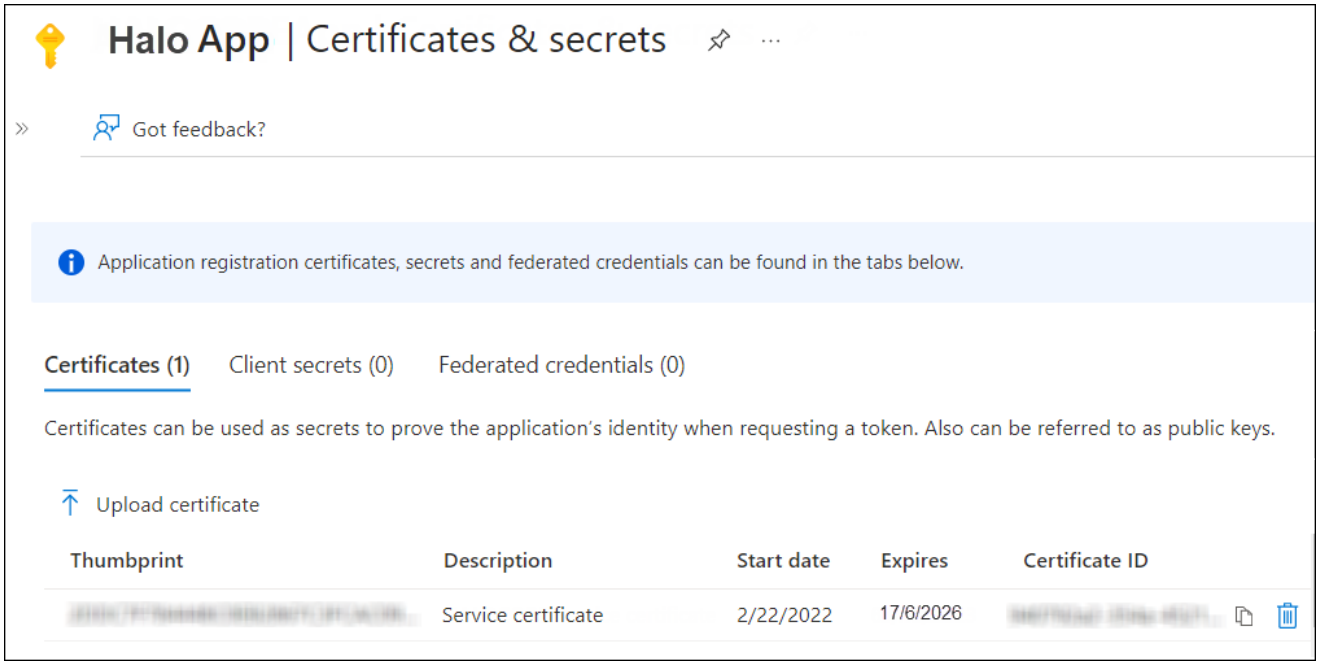
1. In the sidebar of the new application page, select **Certificate & secrets**.

2. Under the **Certificate** section, click **Upload certificate**. The **Upload certificate** dialog appears as shown in the below figure:



Upload certificate #1

3. Click on the folder icon to select the certificate and click **Open**. For illustration purposes, the file `DESKTOP001.cer` is used.
4. Now, click **Add**. The certificate will get uploaded and its thumbprint will be displayed on the page as shown in the below figure:



Upload certificate #2

5. You are now ready to install the HaloENGINE Service.

2.2.2. Create and Configure the Sensitivity Labels

As an administrator, you can create, configure, and publish sensitivity labels for various levels of content sensitivity based on your organization's classification taxonomy. Use names or terms that are familiar to your users. Consider starting with label names like Personal, Public, General, Confidential, and Highly Confidential if you don't already have a taxonomy in place. For more details, please refer to Microsoft online documentation.

2.2.3. Others

Before you begin, make sure that the following prerequisites are met in your system:

1. In case of silent installation, make sure to install Visual Studio Redistributable latest VS2015-2022 from the following link: https://aka.ms/vs/17/release/vc_redist.x64.exe (x64 version).
2. Make sure the user who is running the service or a specific group that the user belongs to is not to the **Deny log on as a service** policy (**Local Security Policy** > **Security Settings** > **Local Policies** > **User Rights Assignment**). If the user(s) exist, the **Error 1069: The Service did not start due to a logon failure** message will appear while running the HaloENGINE Service.

2.3. HaloENGINE Service Installation Methods

This chapter walks you through the steps of installing the Service using graphic and silent methods. By default, HaloENGINE Service is installed in Microsoft Purview Information Protection (MPIP) mode, which provides label-based protection. Note: Microsoft Purview Information Protection (formerly known as Microsoft Information Protection, MIP). Please note that the term "MIP" is still used in various places all across the manual. Both terminology MIP and MPIP are used interchangeably throughout this document.

You can install the add-on in the following modes:

1. **Graphical/Interactive Installation**
   Graphical mode installation is an interactive, graphical user interface-based method that is driven by a wizard.
2. **Silent Installation**
   Silent-mode installation is a non-interactive method of installing the add-on using command lines. If you want to run without a GUI, refer to the section “Silent Installation”.

2.3.1. Interactive Installation

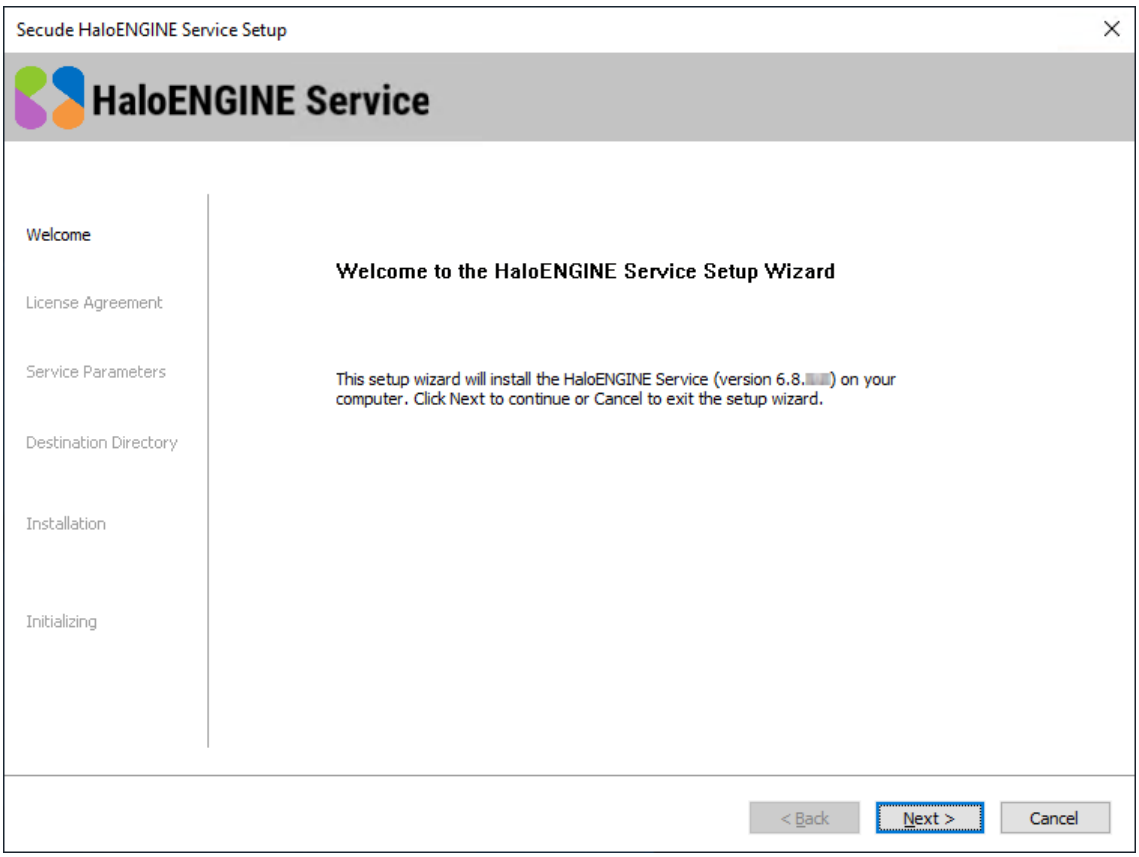
Prerequisites:

1. Azure application registration details. Please refer to the section "Registering an Application in Microsoft Entra ID".
2. A machine certificate, either a Root CA Signed Certificate or a Self-Signed Certificate.
3. Details of your cloud type.

Install HaloENGINE Service using the GUI-based setup program that is provided in the installation package. Make sure the user who installs the HaloENGINE Service has administrator rights. Follow the steps to install the HaloENGINE Service:

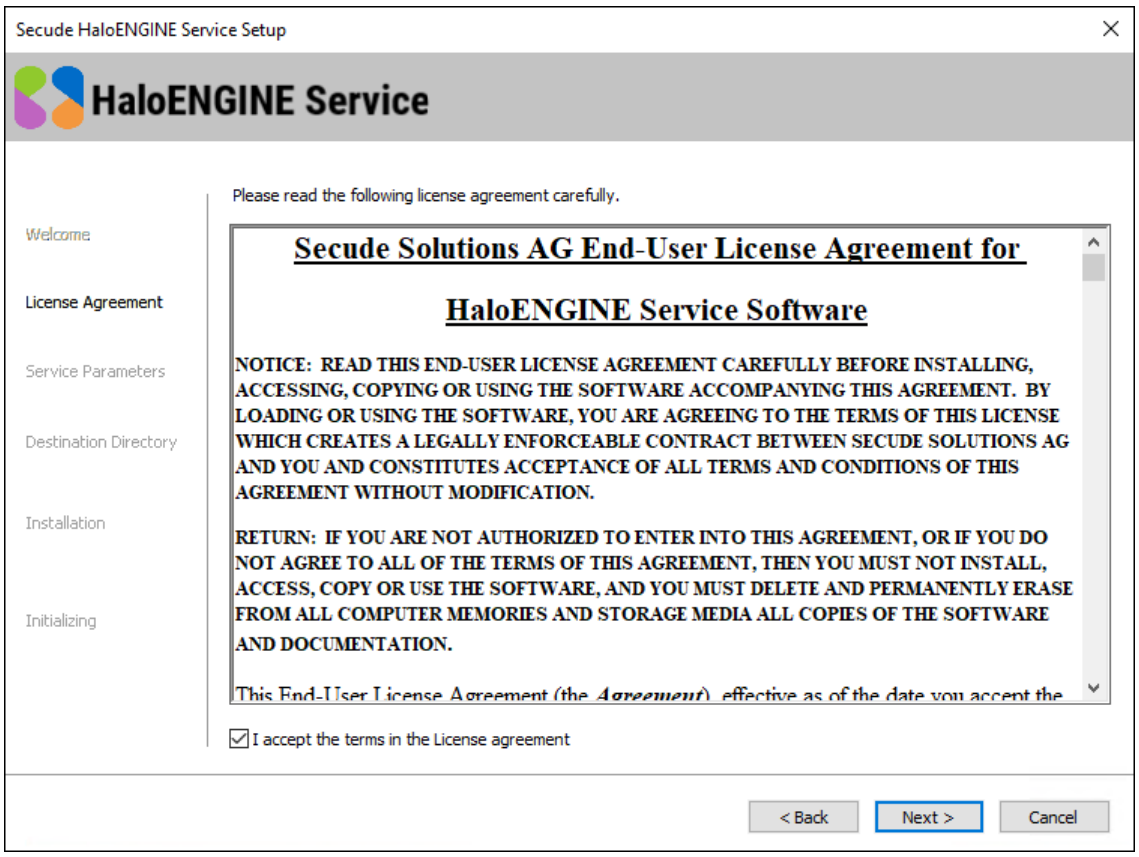
1. Navigate to the directory in which the HaloENGINE Service installation package is located and double-click the installer `HaloENGINE_Service_Setup.exe`.
2. Depending on your Windows security settings, you may get a warning such as "*Do you want to allow the following program to make changes to this computer?*". If you get this security warning, click the **Yes** button to continue the installation.
3. When the installer starts, you will see the startup dialog followed by the welcome dialog:

Startup dialog



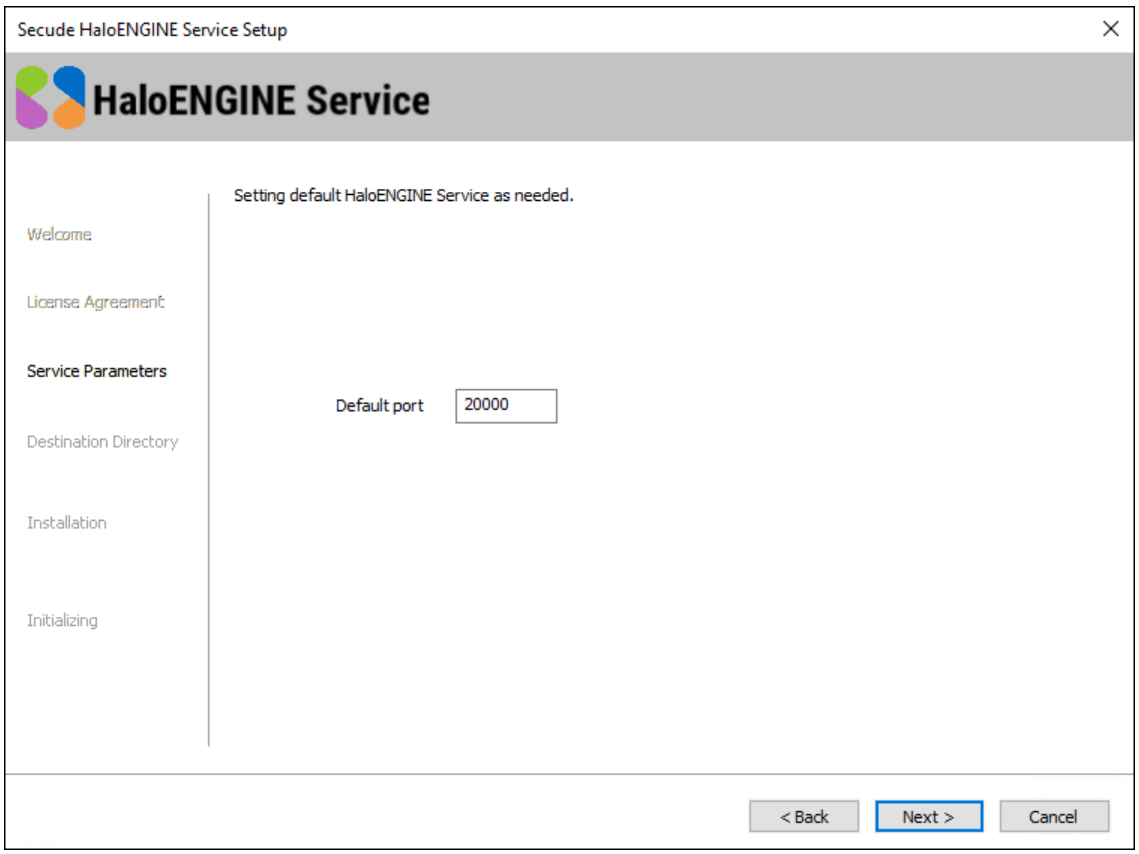
Welcome dialog

4. Click **Next** to continue the installation. The end-user license agreement dialog will appear:



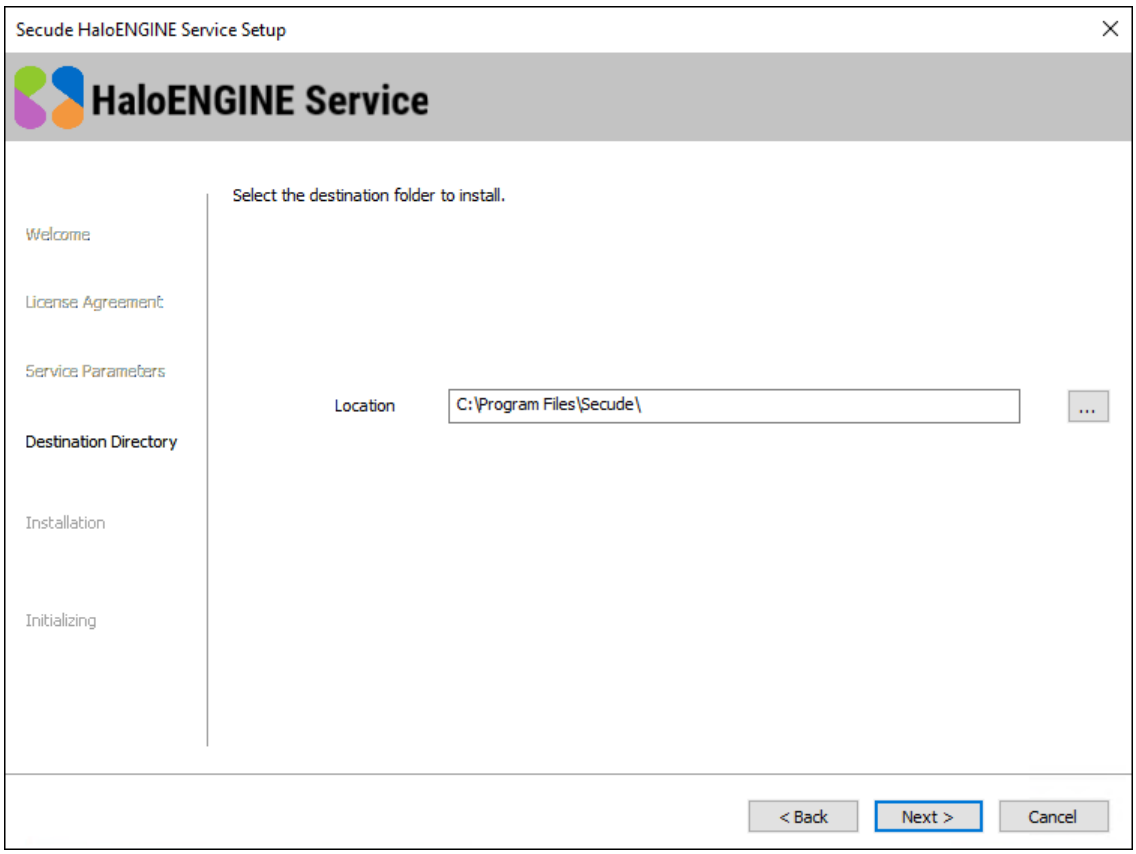
End-user License Agreement dialog

5. Read the End-User License Agreement. If you agree, select **I accept the terms in the License Agreement** and click **Next**. The default settings dialog will appear:



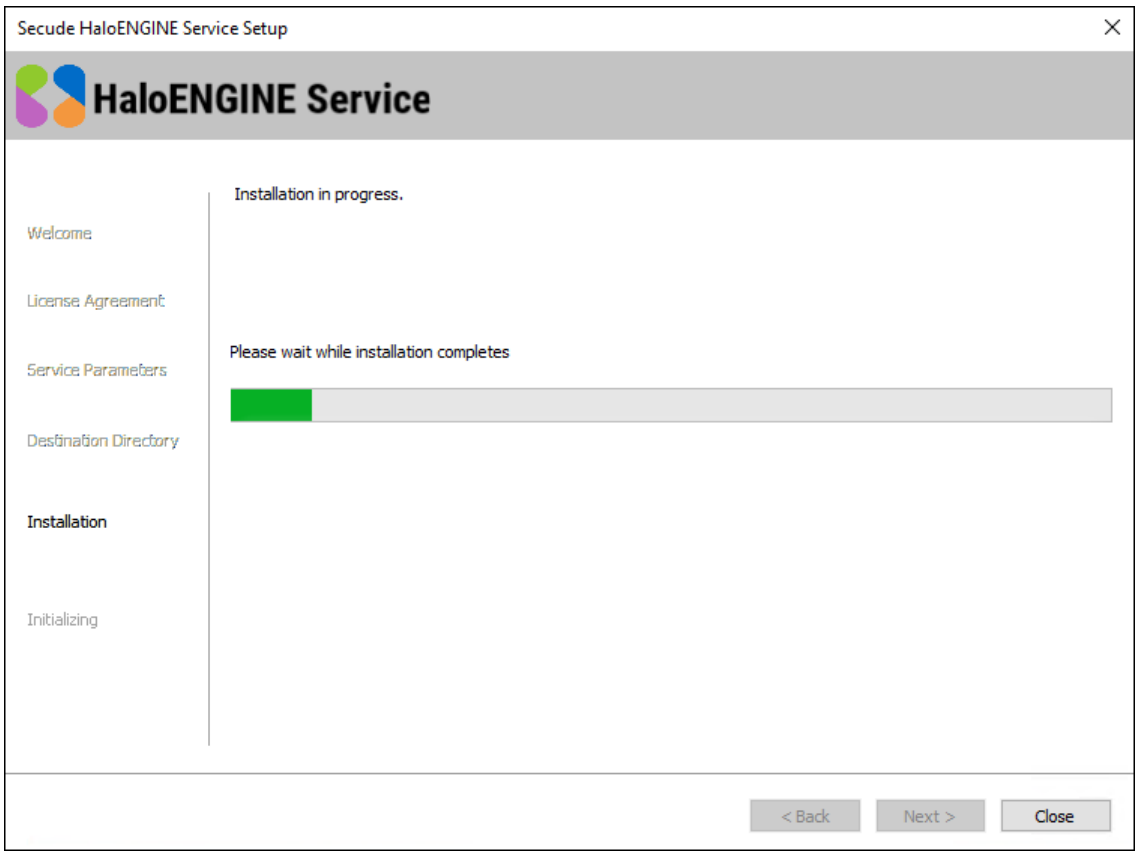
Default settings dialog

6. HaloENGINE Service is defaulted to port 20000, but the port range can be modified between 20000 to 65535 by editing the **Default port** text box.
7. Click **Next** to continue. The destination folder selection dialog will appear:



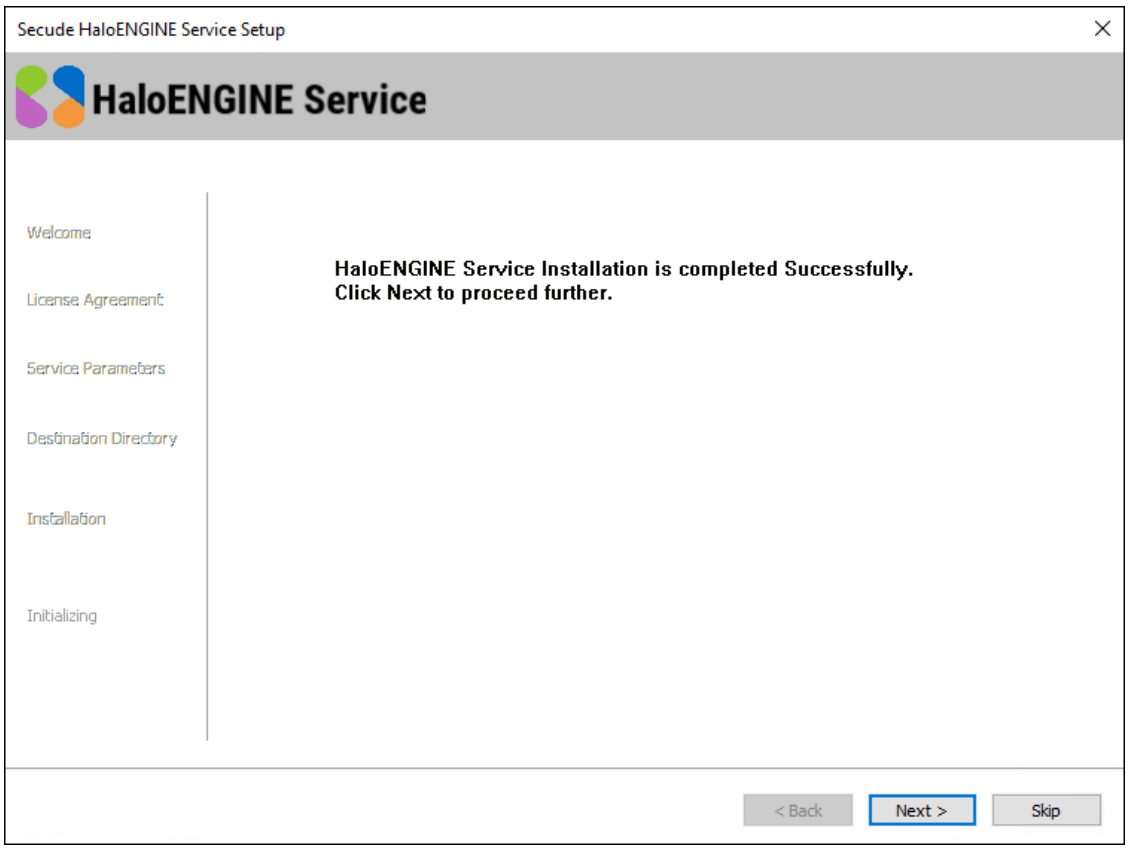
Destination folder selection dialog

8. By default, application files are stored in the program files directory (`C:\Program Files\Secude\`). If you would like to choose an alternate location, click the **Browse** button and select your location preference. When you are finished, click **Next**.
9. The installation begins and progress is shown in the dialog.



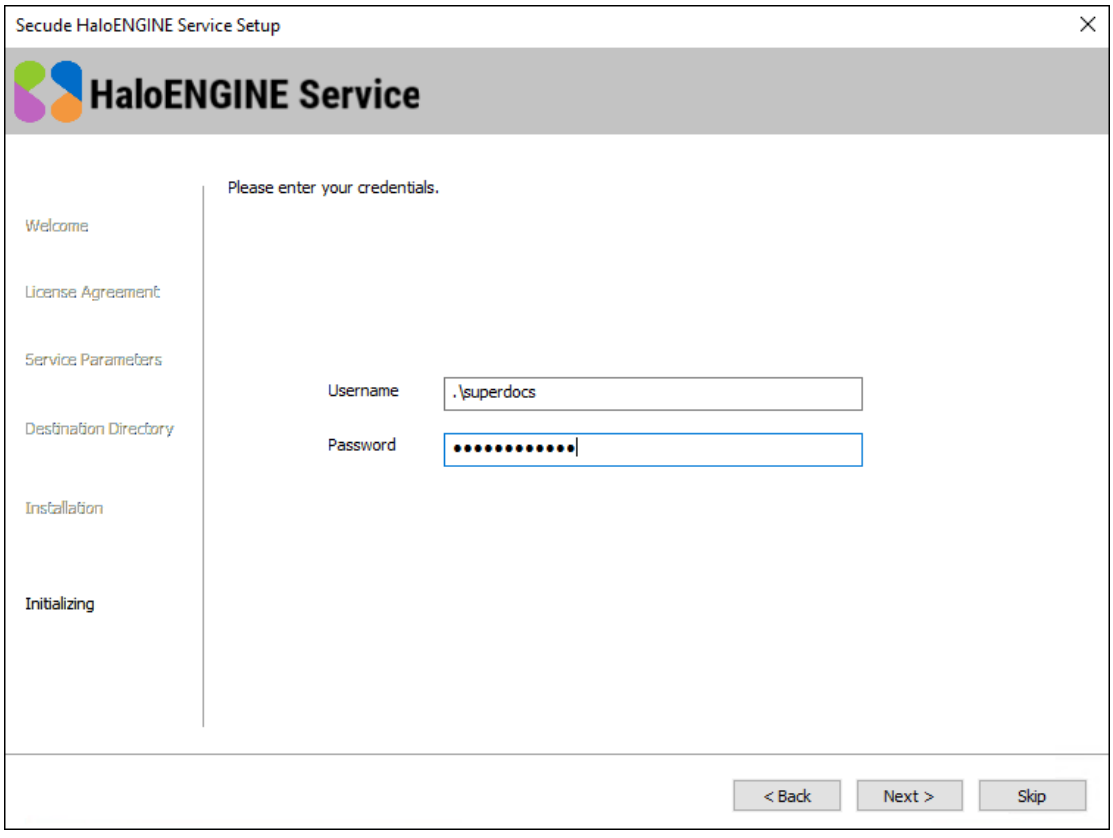
Installation progress dialog

10. When the installation is completed, you will see a message confirming that the HaloENGINE Service has been successfully installed.



Installation completed dialog

11. Click **Next**. The user credential dialog will appear:



User credential dialog

a. If the computer is connected to a domain and to run the HaloENGINE Service on it, you need to enter a domain user account and password. For example, `[domain]\[user]`, `hc.test\john`.

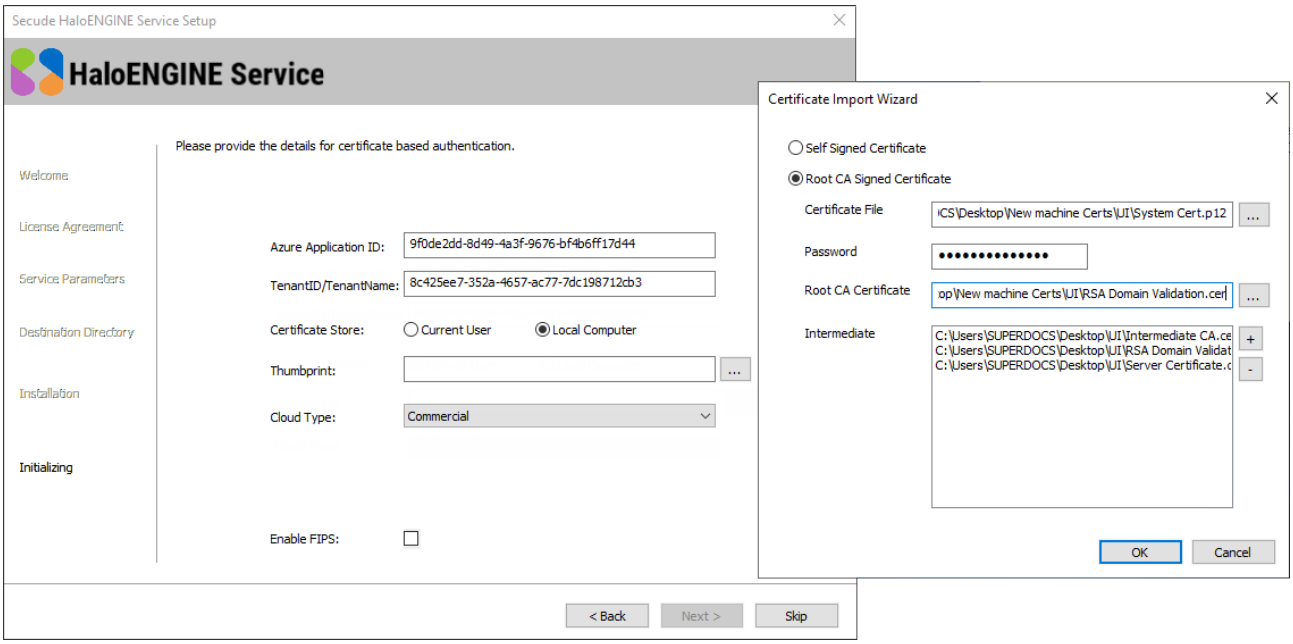
b. On a non-domain joined computer, you need to enter the username and password of a user. For example, `.\[user]`, `.\john`.

12. Click **Next**. The certificate-based authentication dialog will appear. To avoid errors, please ensure that you enter the correct Azure application registration details in the installation wizard.

a. **Azure Application ID**: Enter your application ID. For example, `9f0de2dd-8d49-4a3f-9676-bf4b6ff17d44`

b. **Tenant ID/Tenant Name**: Enter your Microsoft Entra tenant name (for example, `halosecude.onmicrosoft.com`) or its tenant ID (for example, `8c425ee7-352a-4657-ac77-7dc198712cb3`).

c. **Certificate Store Location**: Select a certificate store (**Current User** or **Local Computer**). When selecting Local Computer, ensure that the user running the service has at least local administrator rights.



Certificate-based authentication dialog

d. **Thumbprint**: If the certificate is already installed, you need to enter the thumbprint manually. If the certificate is not installed, click the **Browse** button to select the necessary certificates as explained below:

e. **Option 1: Self-Signed Certificate**—select this option if you have a self-signed certificate and this must be the certificate that is registered in the Azure portal. Click **Browse** button to select the certificate (`.pfx` or `.p12`) and type the password.

f. **Option 2: Root CA Signed Certificate**—select this option if you have a certificate that is signed by a CA. Click **Browse** button to select the signed certificate. The certificate path will appear in **Certificate File** field. Type its password in **Password** field. To select the Root CA (`.cer` / `.crt`), click **Browse** button in **Root CA Certificate** field. To select the intermediate CA certificates, click **Add** button in **Intermediate CA** field. In case, you want to remove a certificate from the "*Certificate Import Wizard*", click **Delete** button. Click **OK**, the thumbprint will be populated automatically.

g. **Cloud Type**: By default, Commercial will be set. However, based on your Azure subscription and configuration, you can change the cloud type from the list — Commercial / Custom / Germany / US_DoD / US_GCC / US_GCC_High / US_Sec / US_Nat / China_01. In the case of **Custom** cloud type, you need to enter the appropriate URLs in **Protection Cloud URL** (for example, `https://api.aadrm.com/`) and **Policy Cloud URL** (for example, `https://dataservice.protection.outlook.com/`).

h. **Enable Federal Information Processing Standards (FIPS):** If you want to utilize encryption algorithms that comply with FIPS standards, enable this option. By enabling the option, MPIP uses only FIPS-compliant encryption algorithms. If not, MPIP uses standard encryption algorithms. However, FIPS mode can be enabled at any moment using the Administration Manager Tool (`hesadm.exe`). For more details, please refer to MIP SDK Documentation "MIP SDK FIPS Compliance Statement".

i. Click **Next**.

13. Once the initialization is completed, you will get the success message as shown below.

Initialization completed dialog

14. Click **Close** to complete the installation.
15. Once you have set user credentials to initialize the service, you will be able to start and stop the service using Microsoft Services Control Manager (SCM) or the HaloENGINE Service Administration Manager Tool (`hesadm.exe`). Also, you can examine the state of the running "HaloENGINE Service" via SCM.
16. You have now successfully installed the HaloENGINE Service with the default settings.
17. Please refer to the section "Configuration of HaloENGINE Service" to know how to configure the other settings.

HaloENGINE Service startup after reboot

Since the HaloENGINE Service is installed as Automatic (Delayed Start), after a reboot or shutdown, the HaloENGINE Service will start after a delay of ~3 minutes. This is dependent on the machine, as a service marked as Automatic (Delayed Start) will be started shortly after all other services designated as Automatic have been started.

2.3.2. Silent Installation

Prerequisite: Make sure to install Visual Studio Redistributable latest VS2015-2022 from the following link - https://aka.ms/vs/17/release/vc_redist.x64.exe.

In addition to interactive installation, the HaloENGINE Service can be installed in silent mode and does not display a user interface or require user interaction. It is a convenient way to streamline installation using the command at once.

When running silent mode command lines, enclosing each parameter value with double quotation mark characters is recommended. For example: `hesadm.exe -sc start "HES"`

1. Open a command prompt and navigate to the directory of the installer.
2. To know the list of options available in silent mode, follow the steps given below:

   Type `HaloENGINE_Service_Setup.exe -help`

   Press Enter

   `[-extractinstaller <directory_to_extract>]`

   Output

   Type `HaloENGINE_Service_Setup.exe -extractinstaller "C:\Users\Administrator"`

   `C:\Users\Administrator`

   `Installer extracted successfully.`
3. You could see another HaloENGINE Service Setup `HaloENGINE_Service_Installer.exe` got extracted in the specified folder.
4. Now, navigate to the extracted setup and type: `HaloENGINE_Service_Installer.exe -help`

   Output

   ```
   [-install [-mpip] [-user <user id>] [-pwd <password>] [-port <port>] [-dir
   <destination_directory>]
   [(if -mpip) [<ApplicationID> <TenantID/Name> <CertificateStore ("Current User"|"Local
   Computer")> [<ThumbPrint> | <-selfsigned|-rootsigned>] [<-cloudtype>
   (Commercial|Custom|Germany|US_DoD|US_GCC|US_GCC_HIGH|US_Sec|US_Nat|China_01] [<-
   enablefips> ("true"|"false")]
    [(if -selfsigned) <Certificate File Path> <Certificate Password>]
    [(if -rootsigned) <Certificate File Path> <Certificate Password> <RootCertificate
   File Path> <Count of Intermediate Certificate> <Intermediate Certificate1>...] ] ]
    [(if cloudtype is Custom) <protectioncloudurl> <policycloudurl> ]
  [-uninstall -silent <true|false>]
   ```
5. The following is an example of installing the service in silent mode.

   Using the thumbprint Option with FIPS

   (Before using this command, you need to either manually install the root signed or self-signed

certificate in the particular store and have the details of the thumbprint)

```
HaloENGINE_Service_Installer.exe -install -mpip -user .\administrator -pwd Pa$wde@123
-port 20000 -dir "C:\Program Files\Secude" 90e42986-b044-y8a7-9a33-
a3114f71bd65 halosecude.onmicrosoft.com "Local Computer"
7bxvae61f9686c8c110ab350a28527ab4069515w -enablefips "true"
```

Using Self-Signed Certificate Option with Cloud Type

```
HaloENGINE_Service_Installer.exe -install -mpip -user .\administrator -pwd Pa$wde@123
-port 20000 -dir "C:\Program Files\Secude" r5352197-31e0-5rd2-8tfb-
0i0027b801fb halosecude.onmicrosoft.com "Current User" -selfsigned
"C:\Users\Administrator\cert\SELF-SIGNED.p12" Pa$wde@123 -cloudtype Commercial
```

Using Root CA Signed Certificate Option (WITHOUT an intermediate certificate)

```
HaloENGINE_Service_Installer.exe -install -mpip -user .\administrator -pwd Pa$wde@123
-port 20000 -dir "C:\Program Files\Secude" 12e42986-a044-48a7-8a33-
a3114f71bd65 halosecude.onmicrosoft.com "Local Computer" -rootsigned
"C:\Users\Administrator\cert\Signedcert.p12" Pa$wde@123
"C:\Users\Administrator\cert\Rootca.cer" 0 -cloudtype Commercial
```

Using Root CA Signed Certificate Option (WITH intermediate certificates)

```
HaloENGINE_Service_Installer.exe -install -mpip -user .\administrator -pwd Pa$wde@123
-port 20000 -dir "C:\Program Files\Secude" 12e42986-a044-48a7-8a33-
a3114f71bd65 halosecude.onmicrosoft.com "Local Computer" -rootsigned
"C:\Users\Administrator\cert\Signedcert.p12" Pa$wde@123
"C:\Users\Administrator\cert\Rootca.cer" 2 "C:\Users\Administrator\cert\Secude
Intermediate CA.cer" "C:\Users\Administrator\cert\Secude RSA Domain Validation.cer" -
cloudtype Commercial
```

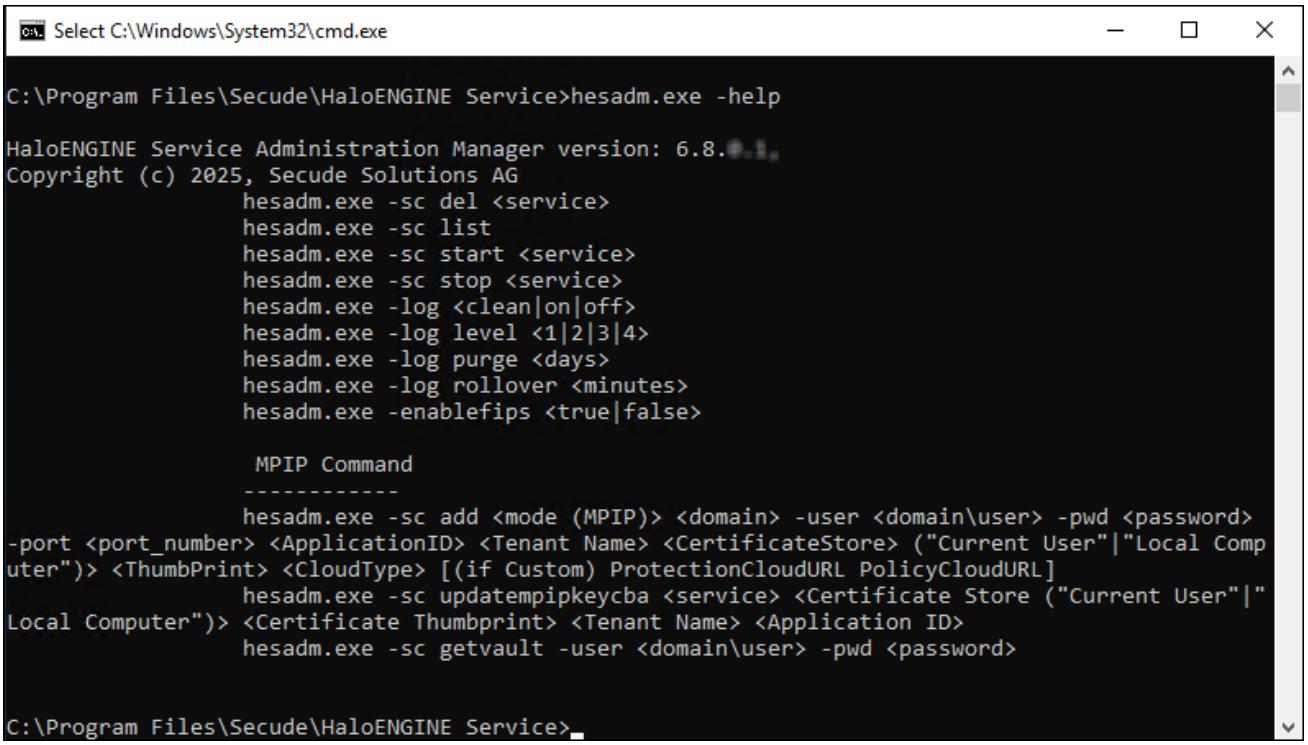
2.4. Configuring the Service

After installing the HaloENGINE Service, you may want to change the configuration. The Administration Manager tool (`hesadm.exe`) allows you to configure HaloENGINE Service.

Any changes to labels in the Microsoft Purview portal require restarting the HaloENGINE Service. If a MPIP label is added, removed, or modified in the Microsoft Purview portal, or if you change the HaloENGINE Service registry settings, the administrator must restart the HaloENGINE Service and HaloENGINE Tomcat service to ensure that the changes take effect. By doing this, labels are updated in HaloENGINE and synchronized with the Microsoft Purview portal.

2.4.1. Administration Manager Tool

The default location for the Administration Manager tool (`hesadm.exe`) is `%ProgramFiles%\Secude\HaloENGINE Service`.



hesadm.exe commands

Service Control Commands
`hesadm.exe -sc del <service>` Use this command to delete a service. For example,

```
hesadm.exe -sc del HES
```

```
hesadm.exe -sc list
```

Use this command to view the service.

Output

For a Domain User

```
Display Name: Secude HaloENGINE Service
Service Name: HES
Domain: HC.test
User Name: HC.test\administrator
Service Port: 20000
Service Mode: MPIP

Display Name: Secude HaloENGINE Service 1
Service Name: HES1
Domain: HC.test
User Name: HC.test\john
Service Port: 30000
Service Mode: MPIP
```

For a Non-Domain local user

```
Display Name: Secude HaloENGINE Service
Service Name: HES
Domain: .
User Name: .\superdocs
Service Port: 20000
Service Mode: MPIP
```

```
hesadm.exe -sc start <service>
```

Use this command to start the HaloENGINE Service. Note: This can be used only after setting user credentials to run HaloENGINE Service.

For example,

```
hesadm.exe -sc start HES
```

Output

```
Service Started successfully.
```

`hesadm.exe -sc stop <service>`

Use this command to stop the HaloENGINE Service.

For example,

```
hesadm.exe -sc stop HES
```

Output

```
Service Stopped successfully.
```

`hesadm.exe -log <clean|on|off>`

1. clean: removes all files from the logging directory.
2. on: enables the service logging.
3. off: disables the service logging.

For example,

```
hesadm.exe -log on
```

Output

```
Current log enabled, level = 3.

INFO,Log already on.
C:\Users\Administrator\AppData\Local\Secude\HaloENGINE Service\log\
```

`hesadm.exe -log level <1|2|3|4>`

1. Log level: 1: ERROR and INFO
2. Log level: 2: ERROR, WARNING, and INFO
3. Log level: 3: ERROR, WARNING, and INFO
4. Log level: 4: ERROR, WARNING, INFO, and DEBUG

For example,

```
hesadm.exe -log level 4
```

Output

```
Current log enabled, level = 3.

INFO,Logging enabled, level = 4.
```

`hesadm.exe -log purge <days>`

Use this command to set a time for log purging, i.e., the no. of day(s) by which the logs will be deleted.

For example,

```
hesadm.exe -log purge 2
```

Output

```
Current log enabled, level = 4.

INFO,Log files purge set to 2 day(s).
```

```
hesadm.exe -log rollover <minutes>
```

Use this command to set a log rollover time, i.e., the minute(s) by which a new log file will be generated.

For example,

```
hesadm.exe -log rollover 60
```

Output

```
Current log enabled, level = 4.

INFO,Log files rollover set to 60 minute(s).
```

```
hesadm.exe -enablefips <true|false>
```

Use this command to enable or disable the FIPS mode.

For example,

```
hesadm.exe -enablefips true
```

Output

```
Enabling FIPS module started.

Service Stopped successfully.

Extracting FIPS module files done.

Trying to Install FIPS modules for this PC.

fips modules configuration generated for this PC successfully.

Service Started successfully.
```

MPIP Mode Control Commands

Create a New Service

```
hesadm.exe -sc add <mode (MPIP)> <domain> -user <domain\user> -pwd <password> -port <port_number> <ApplicationID> <Tenant Name> <CertificateStore> ("Current User"|"Local Computer")> <ThumbPrint> <CloudType> [(if Custom) ProtectionCloudURL PolicyCloudURL]
```

Note:

1. If no cloud type is mentioned, the "Commercial" cloud type will be considered.
2. Protection Cloud URL and Policy Cloud URL are only applicable if you choose Custom cloudtype.

This command is used to create a new service.

Prerequisites:

- Be sure to use a different user other than an already initialized user.
- Be sure to use a port number from the range between 20000 to 65535.
- While creating multiple services, make sure to use a different port number other than an already used one.

For example,

For a Domain User

```
hesadm.exe -sc add MPIP hc.test -user hc.test\john -pwd #9y->\"raQ8< -port 30000 9496505e-f05a-4154-9d66-4f126cedf4b0 halosecude.onmicrosoft.com "Local Computer" 8713f14a4dd8d0c520f79e0416f33c745a3cbeaf https://api.aadrm.com https://dataservice.protection.outlook.com
```

For a Non-Domain local user:

```
hesadm.exe -sc add MPIP . -user .\user1 -pwd #9y->\"raQ8< -port 30000 9496505e-f05a-4154-9d66-4f126cedf4b0 halosecude.onmicrosoft.com "LocalComputer" 8713f14a4dd8d0c520f79e0416f33c745a3cbeaf
```

Output

```
Service created successfully.
```

Update MPIP Certificate

```
hesadm.exe -sc updatempipkeycba <service> <Certificate Store ("Current User"|"Local Computer")> <Certificate Thumbprint> <Tenant Name> <Application ID>
```

Use this command to update the new MPIP CBA (Certificate-Based Authentication) Keys.

For example,

```
hesadm.exe -sc updatempipkeycba HES "Current User"
6e9685132e2e86d1b0af75a848fcc7c0ec29839b halosecude.onmicrosoft.com u8352197-65e0-
4fd2-9efb-b90027b801fb
```

Output

```
MPIP Labels details retrieved successfully.

MPIP key updated successfully.
```

Display MPIP key

```
hesadm.exe -sc getvault -user <domain\user> -pwd <password>
```

Use this command to know your MPIP key information.

For example,

```
hesadm.exe -sc getvault -user .\administrator -pwd #9y->\"raQ8<
```

Output

```
Application ID: u8352197-65e0-4fd2-9efb-b90027b801fb

Tenant Name: halosecude.onmicrosoft.com

Certificate Store: LocalComputer

Certificate Thumbprint: 6e9685132e2e86d1b0af75a848fcc7c0ec29839b
```

Help Commands

2.4.2. Registry Settings

The following section explains how the registry is used to store service settings. To modify the registry value, open Registry Editor, navigate to this path `Registry Root Directory = HKEY_LOCAL_MACHINE\SOFTWARE\Secude\HaloENGINE Service`, and modify the Reg Key as you want. Any changes to the registry will require a restart of the HaloENGINE Service to take effect.

Name	Default value	Type	Description
dir_common	`common`	REG_SZ	The path to the directory where all the dependent DLL files are stored for the execution of HaloENGINE Service.

Name	Default value	Type	Description
dir_log	`log`	REG_SZ	Log files are generated in the service running the user's local profile i.e. in the following location `%LOCALAPPDATA%\Secude\HaloENGINE Service\log`.
dir_share	`share`	REG_SZ	This folder is for internal use only.
dir_tmp	`tmp`	REG_SZ	It stores the temporary files located at `%LOCALAPPDATA%\Secude\HaloENGINE Service\tmp`.
dir_vendor	`C:\Program Files\Secude\`	REG_SZ	This is the Secude's vendor directory under which Secude's components will get installed. For example, HaloENGINE Service.
enable_fips	`false`	REG_SZ	Enable or disable the FIPS mode. 1. true: By selecting this option, MPIP only uses FIPS-compliant encryption algorithms. 2. false: MPIP uses standard encryption algorithms.
log_enable	`on`	REG_SZ	Defines the status of the log. • On = Log file will be generated in the default location • Off = Log file will not be generated • Clean = Log files will be deleted. This parameter deletes only the logs and does not modify the log_enable to "Clean" from "on/off".
log_level	`3`	REG_SZ	• Log level 1: ERROR and INFO • Log level 2: ERROR, WARNING, and INFO • Log level 3: ERROR, WARNING, and INFO • Log level 4: ERROR, WARNING, INFO, and DEBUG

Name	Default value	Type	Description
log_purge	7	REG_SZ	It indicates removing files older than a defined time frame. By default, the log files older than 7 days will be deleted.
log_rollover	100	REG_SZ	Defines the log rollover time, i.e., a new log file will be generated based on the specified minute(s). By default, a new log file will be generated every 100 minutes.
templatefile_purge	1	REG_SZ	Defines the purge time of template files that are generated for every CAD assembly file (compound file) download. The default value set is one hour. For example, when a file is downloaded at 15:25 hours, the HaloENGINE Service creates a template file in the tmp\GUID folder (which can be located in the HaloENGINE Service user's profile folder). In the background, it examines and deletes the files which had reached the configured time i.e., after 16:25 hours. Note: This is only applicable in the event of CAD assembly file labeling.
version		REG_SZ	The version number of the installed service.

Configuration in the Registry

2.4.3. Configuring Endpoint

`Registry path of endpoint = HKEY_LOCAL_MACHINE\SOFTWARE\Secude\HaloENGINE Service\ep\HES`

Name	Default value	Type	Description
block_pii	false	REG_SZ	Enable or disable the visibility of Personally Identifiable Information (PII) in the MIP SDK logs. The MIP SDK logs are located at%LOCALAPPDATA%\Secude\HaloENGINE Service\log\mip_cache_storage\mip\logs\mip_sdk.miplog.

Name	Default value	Type	Description
			• false—PII will be visible in clear text in the MIP SDK logs. • true—PII will be masked with asterisks in the MIP SDK logs. This helps to protect the PII's confidentiality.
cachetype	1	REG_SZ	MPIP cache storage type used by the service. • In Memory—0, maintains the storage cache in memory in the application. • On Disk—1 (default storage type), stores the database (SQLite3) on disk in the directory provided in the settings object. The database is stored in plaintext. • On Disk Encrypted—2, stores the database (SQLite3) on disk in the directory provided in the settings object. The database is encrypted using OS-specific APIs.
cacheuserlicense	1	REG_SZ	• 0—false, End User License (EUL) will NOT be stored in the MPIP cache storage. • 1—true (default value), End User License (EUL) will be stored in the MPIP cache storage.
cloudtype		REG_SZ	User's Azure Cloud Type. For example Commercial.
credential		REG_SZ	Domain or computer name\name of the user under which HaloENGINE Service runs
databoundary	Default	REG_SZ	Audit and telemetry events are sent to the nearest collector, where these events are stored and processed. Other options: 1. Asia

Name	Default value	Type	Description
			2. Europe_MiddleEast_Africa 3. European_Union 4. North_America For example, if your AIP administrator sets North_America, the HaloENGINE Service forces all telemetry and audit data to go directly to North America.
domain		REG_SZ	Name of the domain.
enabledke	`0`	REG_SZ	Double Key Encryption • 0 (default value)—Disables the DKE functionality in the HaloENGINE Service. • 1 (On)—Enables the DKE functionality in the HaloENGINE Service. Please be aware that DKE labels are only visible when DKE functionality is enabled.
enablefiletracking	`0`	REG_SZ	To register register a protected file to track and revoke. • 0 (default value)—the protected file will not be registered for file tracking and access revocation. • 1—the protected file will be registered for file tracking and access revocation.
enableminimaltelemetry	`0`	REG_SZ	To transmit diagnostic information to Microsoft. • 0 (default value)—all diagnostic events are transmitted. • 1—minimum diagnostic events are transmitted.
MIPAuthType	`MSALCBA`	REG_SZ	Type of authentication method (MSALCBA).
mode	`MPIP`	REG_SZ	MPIP

Name	Default value	Type	Description
policycloudurl		REG_SZ	Policy Cloud URL. For example: `https://dataservice.protection.outlook.com`
port	`20000`	REG_SZ	Example port that the HaloENGINE Service used to communicate.
protectioncloudurl		REG_SZ	Protection Cloud URL. For example: `https://api.aadrm.com`
service	`HES`	REG_SZ	Name of the service. By default, it is “HES”. If you add more than one service, it will have HES1 and HES2 and so on.
streambuffersize	`10`	REG_SZ	It is a buffer size used for memory-based encryption with the MIP SDK. When the allotted buffer size is exceeded, an additional memory of stream buffer size is allocated, and this process is repeated until the encryption/decryption operation is completed. The default setting is 10MB.

Configuring Endpoint

Proxy Configuration

Many enterprises enforce a Group Policy Objects (GPO) that requires all outbound internet traffic routed through a proxy server. These proxy settings need to be used by both the MIP SDK and the MSAL library for MPIP authentication and functionalities. To use proxy settings for the MSAL library, we need to set the `msal_proxy_address` in `HKEY_LOCAL_MACHINE\SOFTWARE\Secude\HaloENGINE Service`.

Name	Type	Data
msal_proxy_address	REG_SZ	`<http://IP Address>`

Configuring MSAL proxy

If the above does not work for service-running users, in such cases, set the registry keys `ProxyServer` and `ProxyEnable` in `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings`.

Name	Type	Data
ProxyServer	REG_SZ	`<http://IP Address>`

ProxyEnable	REG_SZ	• 1 to enable. • 0 to disable.

Configuring proxy

To allow MIP SDK to use the proxy settings set up in your environment, follow the steps below:

Determine whether the proxy server has been properly set up by running the following command.

```
C:\Windows\system32>netsh winhttp show proxy

Current WinHTTP proxy settings:

Direct access (no proxy server).
```

If the response to the command is as shown above, it indicates that the proxy server has not been configured in the registry for winhttp.

To configure the proxy server for winhttp, use the following command:

Syntax: `C:\Windows\system32>netsh winhttp set proxy <proxyservername>:<portnumber>`

Example: `C:\Windows\system32>netsh winhttp set proxy 190.160.166.191:168`

In this case, the proxy server that has been set up with 190.160.166.191:168. Once this is executed successfully, the registry gets updated with the proxy server URL and HaloENGINE Service will make sure of the proxy settings.

What to do next?

The next step is to install and configure HaloENGINE after the service has been operational.

3. Installing the HaloENGINE

The requirements for installing HaloENGINE are detailed in this chapter.

3.1. System Requirements

The following table lists the requirements for the HaloENGINE.

Components	Details
Operating System	Installing HaloENGINE and HaloENGINE Service on the same server is necessary. Please refer to the HaloENGINE Service Requirements Table for further information about operating systems.
Supported browser version	The most recent versions of Microsoft Edge, Chrome, and Firefox are supported by the HaloENGINE Admin portal.

Requirements

3.2. Prerequisites

The prerequisites and dependencies for installing and configuring the HaloENGINE are summarized in this section.

3.2.1. Obtain HaloENGINE License

Before installing the HaloENGINE, we recommend obtaining the license file (`license.lic`) from Secude support to enable the HaloENGINE functionalities. The license file you received from Secude will include specific features and system types. This implies that only the system types that you have obtained in the license are accessible by their respective endpoints. After configuring the admin portal, import the license as instructed in the section "Phase 3. Activate License".

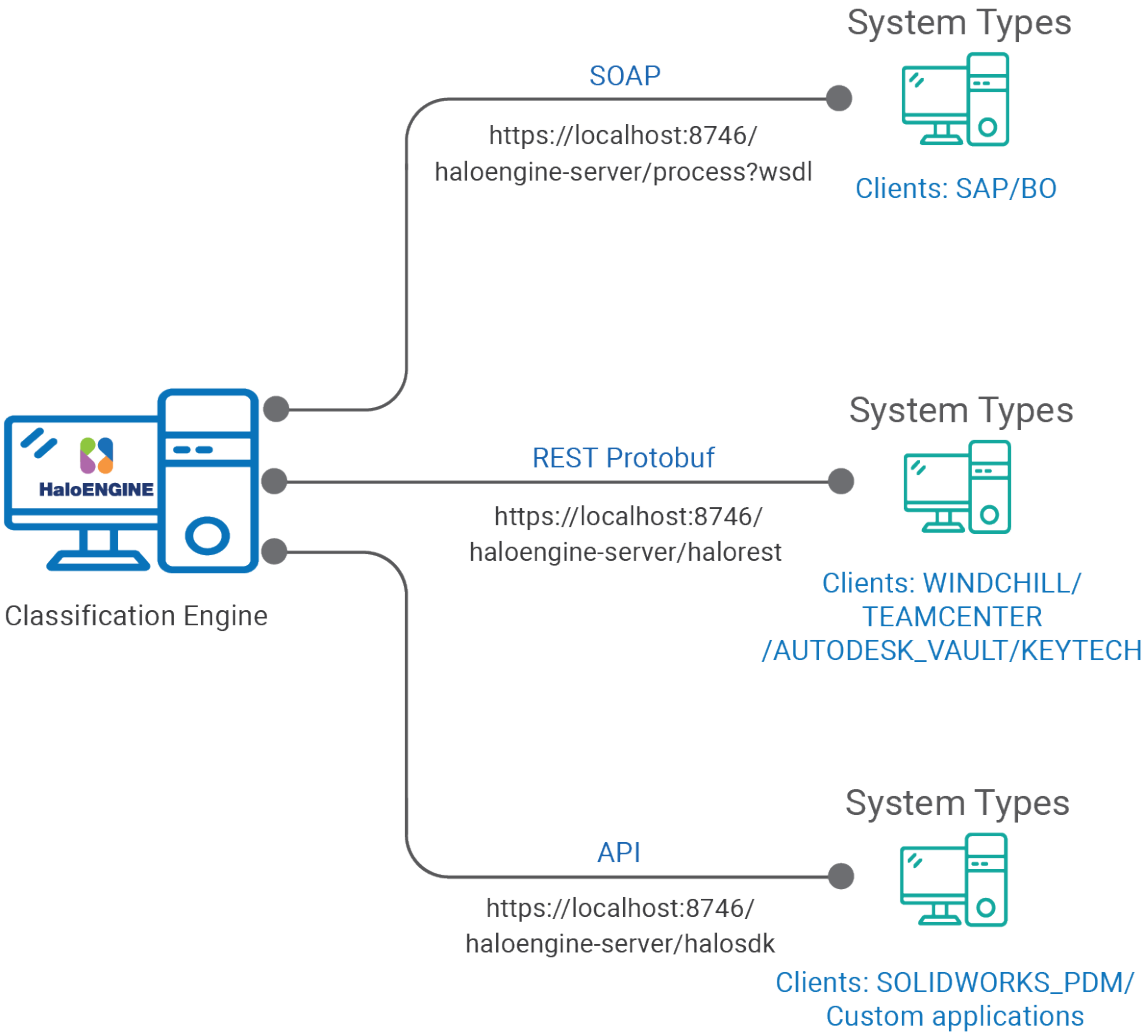
Avoid renaming the license file.
Once you have received the license file from Secude, use it exactly as is, without changing its name. Renaming the file prevents the license from activating.

For example,

Case 1: If your license file is enabled for feature Protect with the SAP system type, the SOAP interface is enabled internally, but access to the other endpoints (REST Protobuf and API) is restricted. Consequently, only Protect-related features are available on the HaloENGINE admin portal. However, the Monitor feature is included by default.

Case 2: If your licensing file includes the Protect and Block features for the system types Windchill, Teamcenter, and Autodesk Vault, the REST Protobuf interface is enabled internally, but the other endpoints (SOAP and API) are restricted. In this case, the HaloENGINE admin portal provides Protect and Block features. Additionally, the Monitor feature is enabled by default.

The following picture illustrates how the client communicates with the HaloENGINE.



System types and protocol

License File Per Customer

1. For Single Customer mode—you need to have one license file.
2. For Multi-Customer mode—you need to have license files as many 'customers' as you would create in the portal.
   For instance, if you intend to add three customer IDs to the portal, you will require three licensing files for each of them.
   a. Customer 1 (BM Automobile AG)—With one feature (e.g., Protect) in a single license file.
   b. Customer 2 (DELBONT Industries)—With one or two features (e.g., Protect and Block) in a single license file.
   c. Customer 3 (WHEELS INC)—With one feature (e.g., Block) in a single license file.

The table below will assist you in deciding the type of license you should obtain from Secude.

Customer Requirement	License Specification	Description
Monitor	Monitor	Customer environment that only needs the monitoring feature.
Block	Monitor + Block	Customer environment that just requires the blocking feature. However, monitoring is included as a standard feature.
Block and Protect	Monitor + Block + Protect	Customer environment that requires blocking and protecting features. A full license with all three features (Monitor, Block, and Protect) must be used.

Obtaining license

3.2.2. Download SAP JCo (only for SAP clients)

1. Go to https://websmp209.sap-ag.de/public/connectors, click on the **SAP Java Connectors** link, and select **Tools & Services** (you need a valid S-User from SAP).
2. Download the zip package as per your operating system (For example, Windows - x64 / x86 bit).
3. Extract the zipped folder.
4. **Related tasks**: After configuring the admin portal, import the files as instructed in the section "SAPJCo Configuration".

3.2.3. User Management Settings

Make a default (also known as regular) administrator account after installing the HaloENGINE component. This account is referred to as "Super Admin," and it has greater access than a typical administrator account. This account has full access to your HaloENGINE component.

3.2.3.1. User Accounts

User Account 1	User Account 2	User Account 3
Default Super Admin account	Customer_Admin	Customer_User
Role: ROLE_SUPER_ADMIN	Role: ROLE_CUSTOMER_ADMIN	Role: ROLE_CUSTOMER_USER
User validation: Locally validated	User validation: Microsoft Entra authentication	User validation: Microsoft Entra authentication

User Accounts

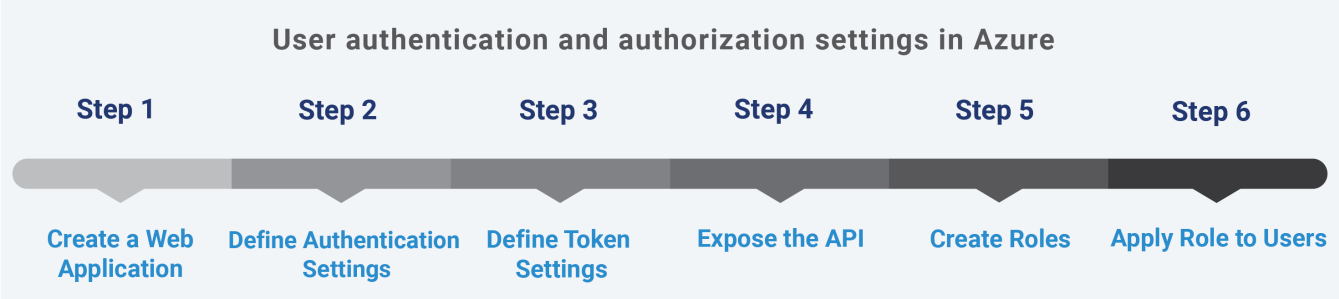
3.2.3.2. Settings in Azure Portal

User management is often included with Microsoft Azure and involves several request exchanges between the HaloENGINE Admin Portal and the identity provider, Microsoft Entra ID.

Microsoft documentation

Any application that wants to use Microsoft Entra ID for authentication must be registered in its directory. The information in the Microsoft documentation overrides any information published in this section. For a detailed explanation, please see the Microsoft documentation.

In the Azure portal, follow the steps below to configure user authentication and authorization settings.



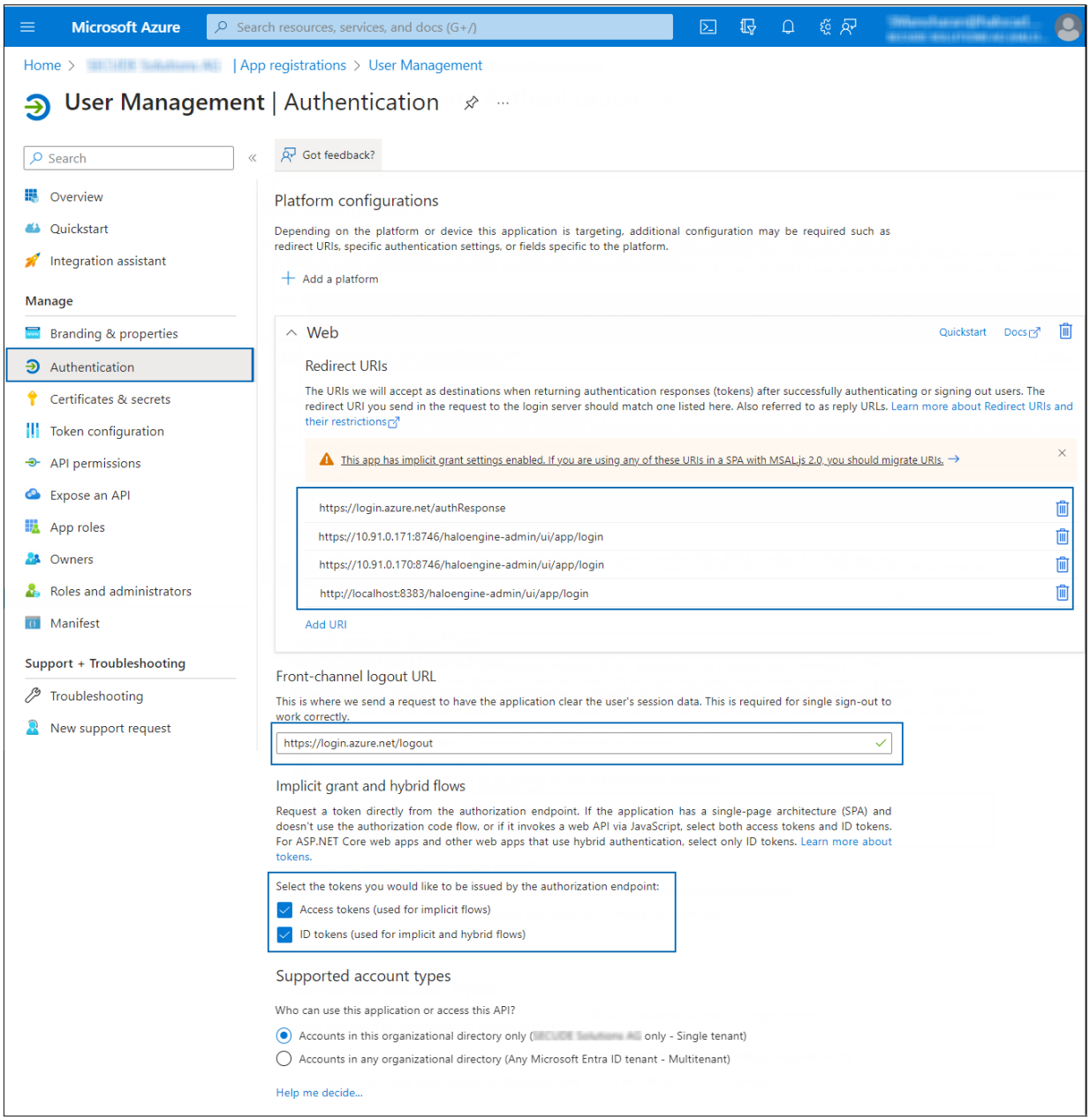
User authentication and authorization settings in Azure

3.2.3.2.1. Step 1: Create a New Web Application

1. You can either leverage an existing Web (Redirect URI) application or create a new one in Azure Portal. To serve as an example, the Web application **User Management** is created.
2. When registration is complete, the Overview page displays the **Application ID** and **Tenant ID** values. These values uniquely identify your application on the Microsoft identity platform. To preserve the values, copy them to the clipboard and paste them into a text editor (such as Notepad).

3.2.3.2.2. Step 2: Authentication Settings

1. In the left navigation pane, select **Authentication**.

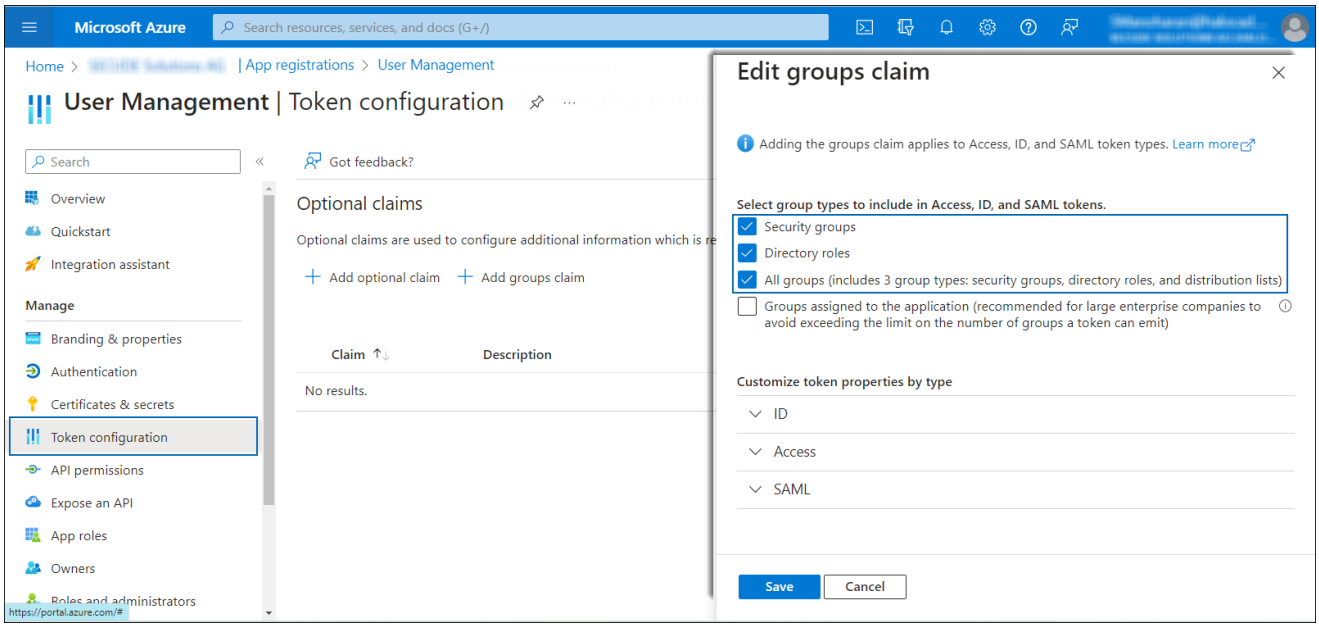


Authentication settings

2. Under the **Web** section, click **Add URI** and enter the following reply URLs one by one:
   a. `https://login.azure.net/authResponse`
   b. HaloENGINE Admin portal URL:
      - `https://<ip>:<port>/haloengine-admin/ui/app/login` (for example, `https://10.91.0.171:8746/haloengine-admin/ui/app/login`)
      - Or `http://<localhost>:<port>/haloengine-admin/ui/app/login` (for example, `http://localhost:8383/haloengine-admin/ui/app/login`)
3. Under **Front-channel logout URL** section, enter the URL – `https://login.azure.net/logout`.
4. Under the **Implicit grant and hybrid flows** section, select **Access tokens,** and **ID tokens** checkboxes.
5. Click **Save**.

3.2.3.2.3. Step 3: Token Settings

1. In the left navigation pane, select **Token configuration** and click **Add groups claim**.

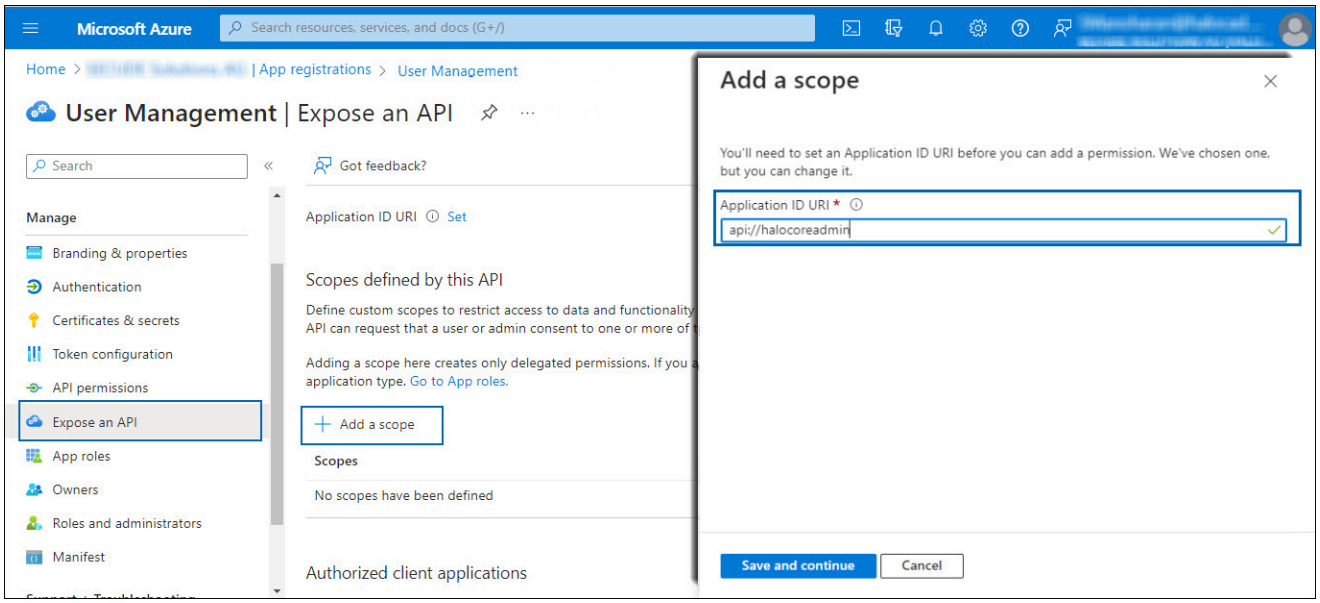


Token Settings

2. Select the following options:
   a. Security groups
   b. Directory roles
   c. All groups
3. Click **Save**.

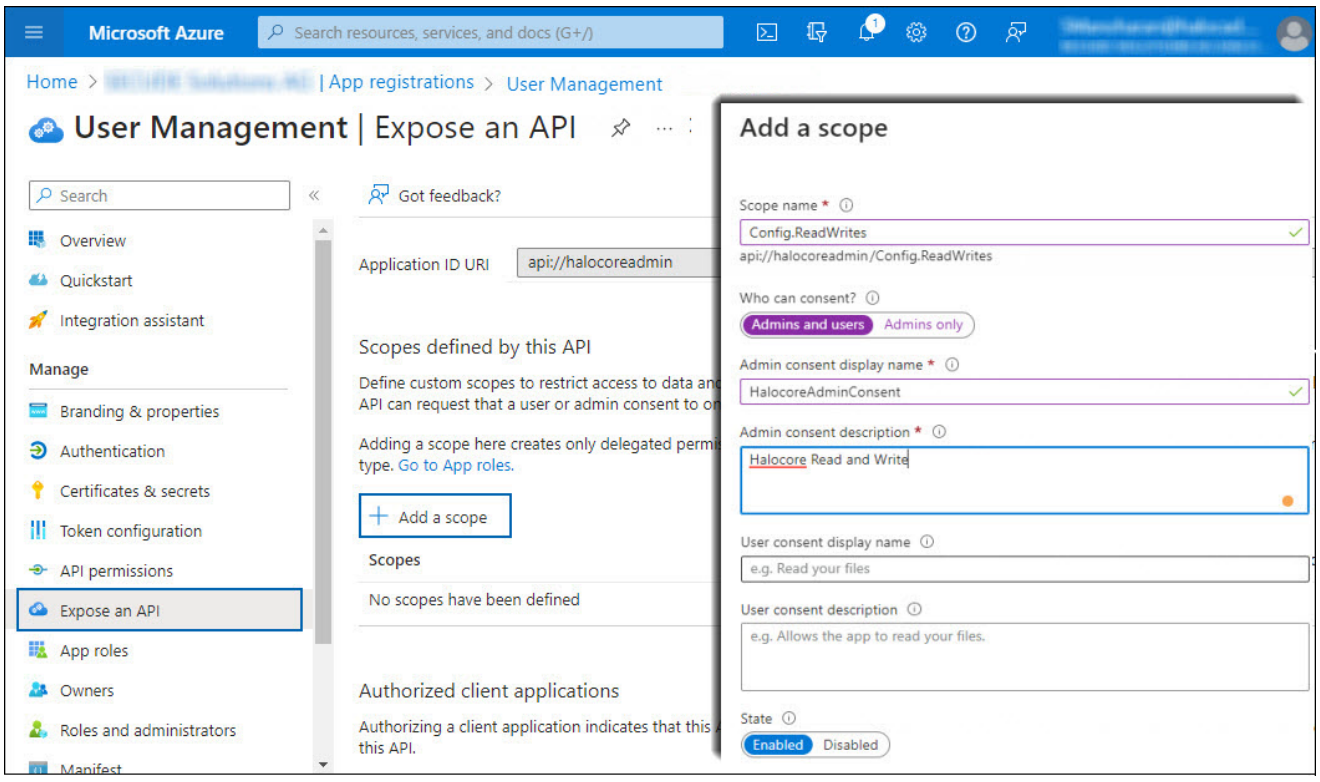
3.2.3.2.4. Step 4: Expose API

1. In the left navigation pane, select **Expose an API**.



Adding scope#1

2. Click **Add a scope** and enter the scope following `api://` in **Application ID URI**. In this example, `api://halocoreadmin` is used.
3. Click **Save and Continue**.
4. Again, click **Add a scope** and enter the following values:



Adding scope #2

a. **Scope name**: enter `Config.ReadWrites`

b. **Who can consent**?: select Admins and users

c. **Admin consent display name**: enter HalocoreAdminConsent

d. **Admin consent description**: enter Halocore Read and Write

e. **State**: select **Enabled**

5. Click **Add scope**. You can see the scope displayed in the UI.
6. Copy the generated scope `api://halocoreadmin/Config.ReadWrites` to the clipboard and save it in a text editor (such as Notepad).

3.2.3.2.5. Step 5: Create Roles

1. In the left navigation pane, select **APP roles**.
2. Click **Create app role** and enter the following values:

a. **Display name**: ROLE_CUSTOMER_ADMIN

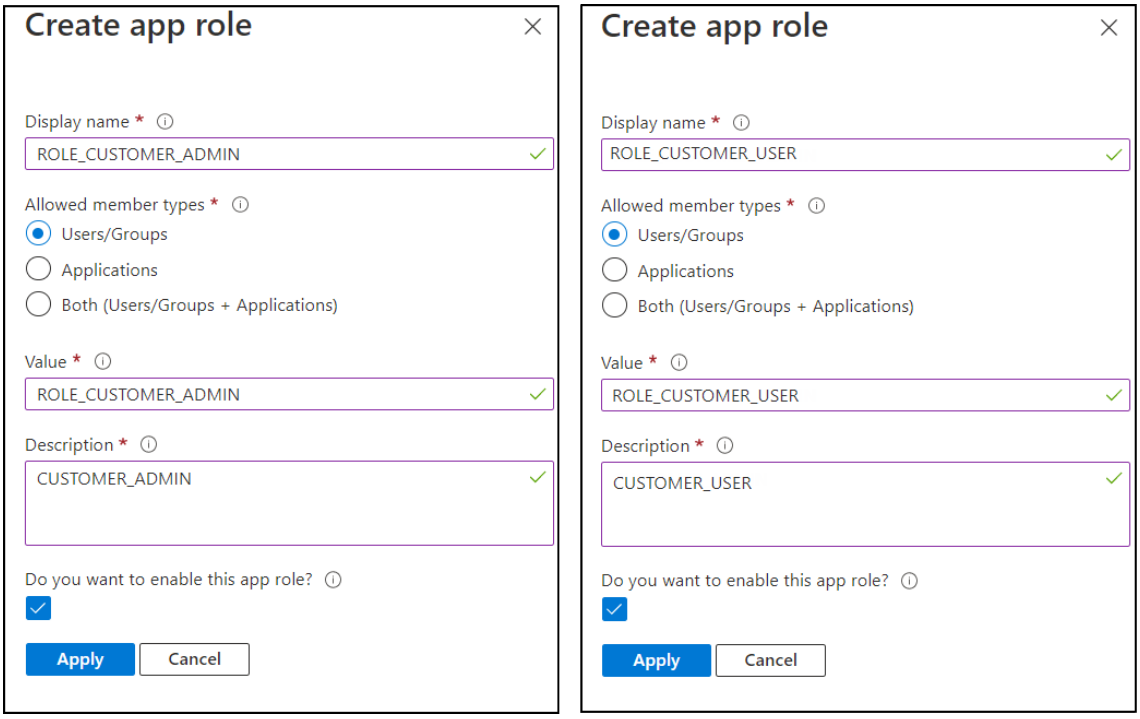
b. **Allowed member types**: select **Users/Groups**

c. **Value**: ROLE_CUSTOMER_ADMIN

d. **Description**: CUSTOMER_ADMIN

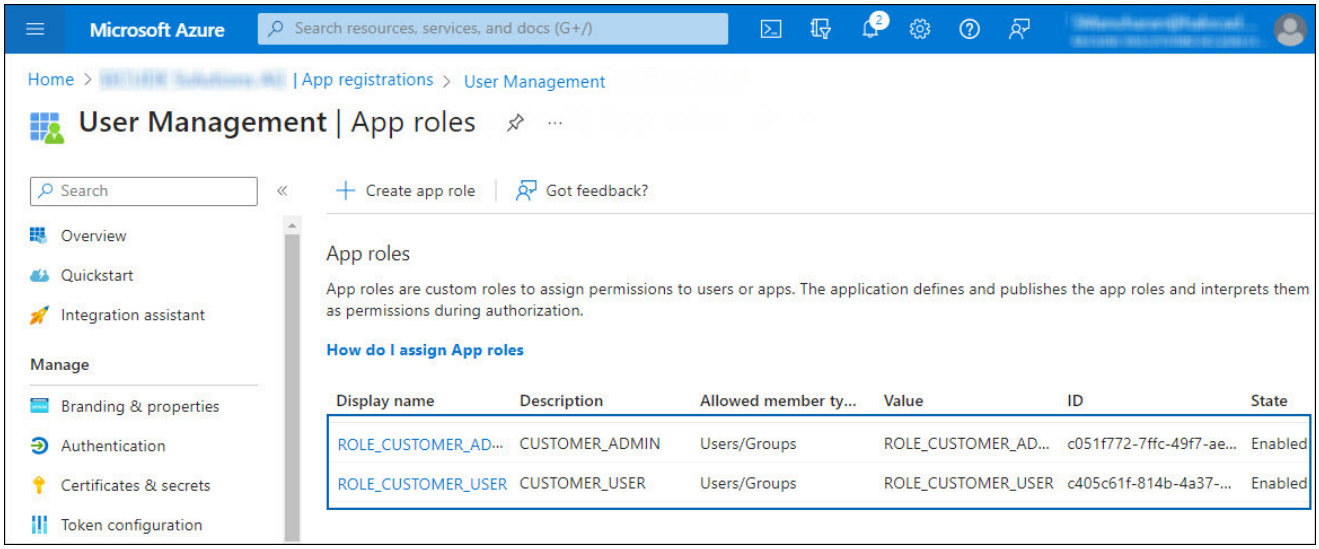
e. **Do you want to enable this app role?** – Select this option.

f. Repeat the above steps for the role **ROLE_CUSTOMER_USER**.



Adding Roles

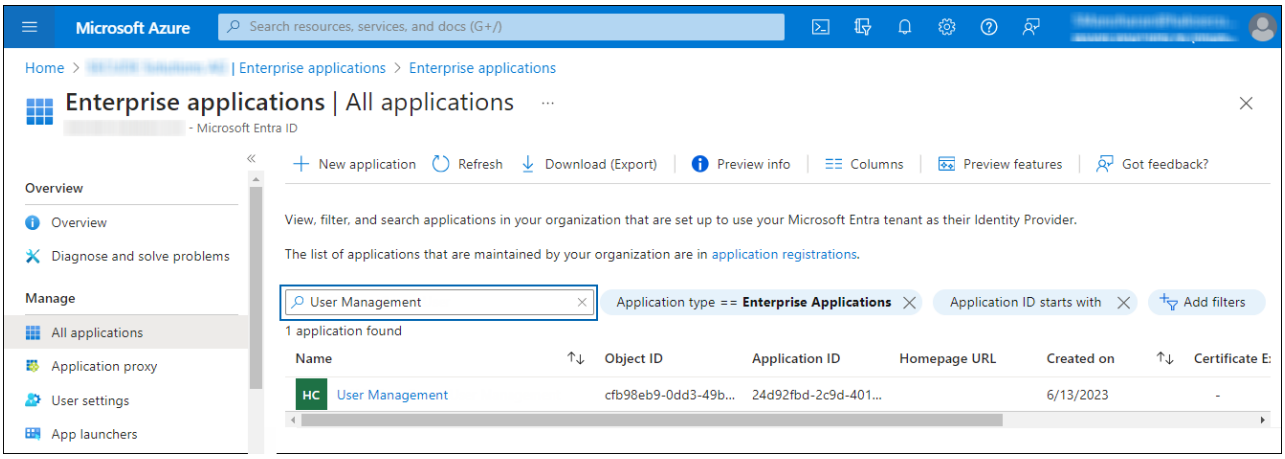
3. Click **Apply**.
4. The roles are added to the list.



Create Roles

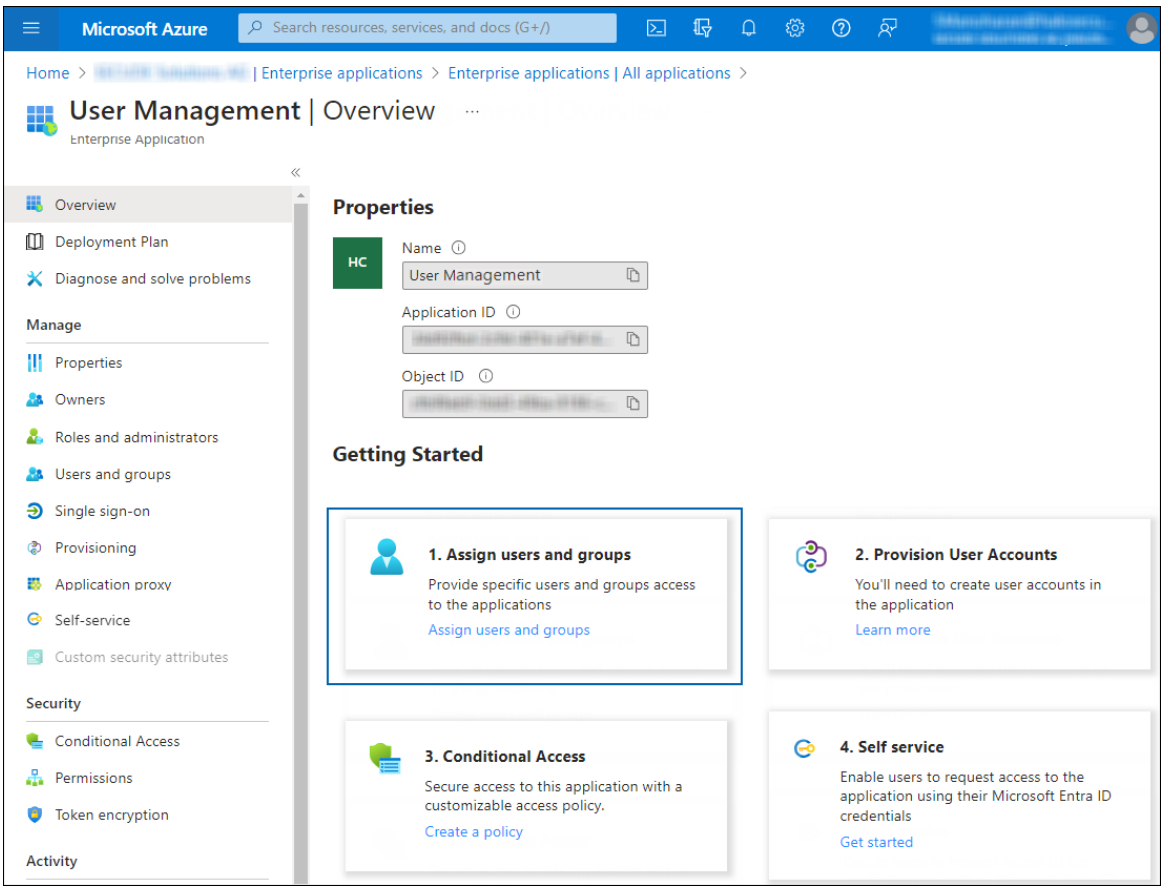
3.2.3.2.6. Step 6: Apply Role to Users

1. In the **Microsoft Entra ID** pane, select **Enterprise applications**.
   a. The **Enterprise Applications** page will appear with a list of existing Service Principals in your tenant.
   b. In the search box, enter your application name. In this example, **User Management** is entered in the search box.



Apply role to user #1

   c. The search result will be displayed.
   d. Now, click on the link from the list. The **Overview** page of the application will appear:



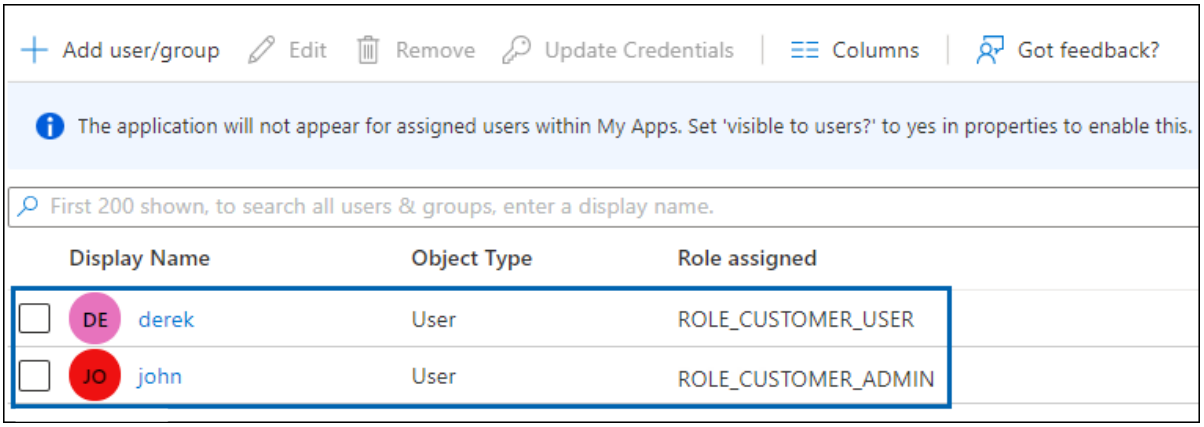
Apply role to user #2

e. Click **Assign users and groups**. The **Users and groups** page will appear.

f. On the **Users and groups** page, click **Add user/group**. The **Add Assignment** page will appear.

g. Under **Users and groups**:

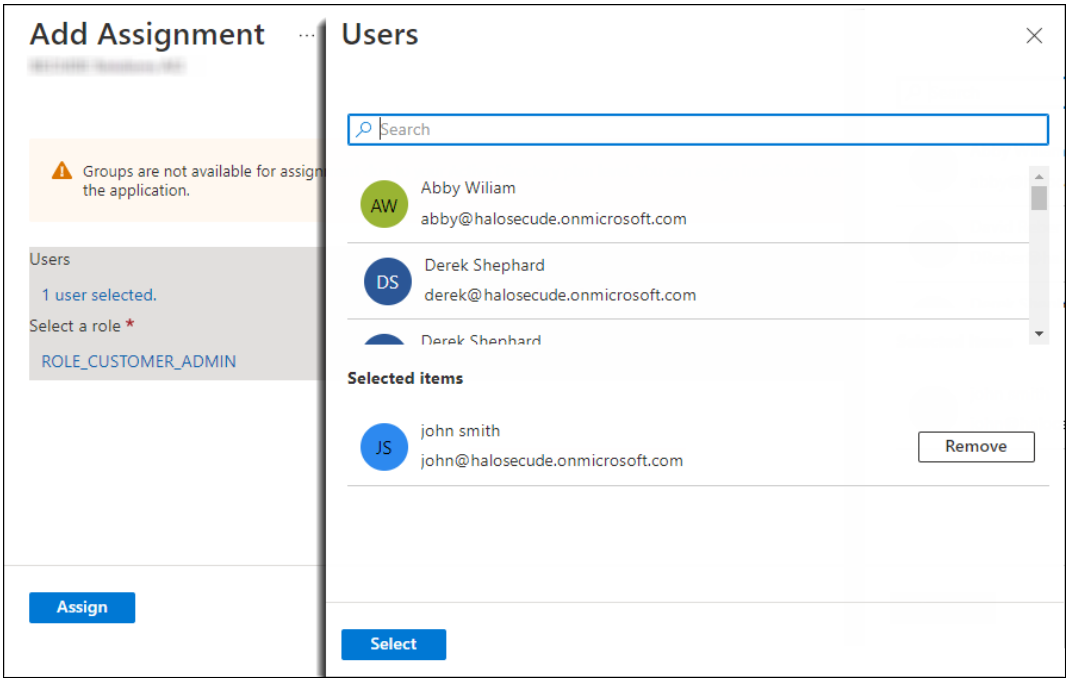
- Click **None Selected** and search for a user (for example, John).
- Click **Select** and **Assign**.



Adding users

h. Under **Select a role**:

- Click **None Selected** and search the role ROLE_CUSTOMER_ADMIN.
- Click **Select** and **Assign**.



Apply role to user #3

i. Repeat the above steps for the role ROLE_CUSTOMER_USER (for example, user Derek is assigned to this role).

2. **Related tasks**: After the initial configuration of the HaloENGINE Admin Portal, you need to use the above values to configure tenant details. Please refer to the section "Phase 10. Tenant Configuration".

3.2.4. Forwarding Logs to Microsoft Sentinel

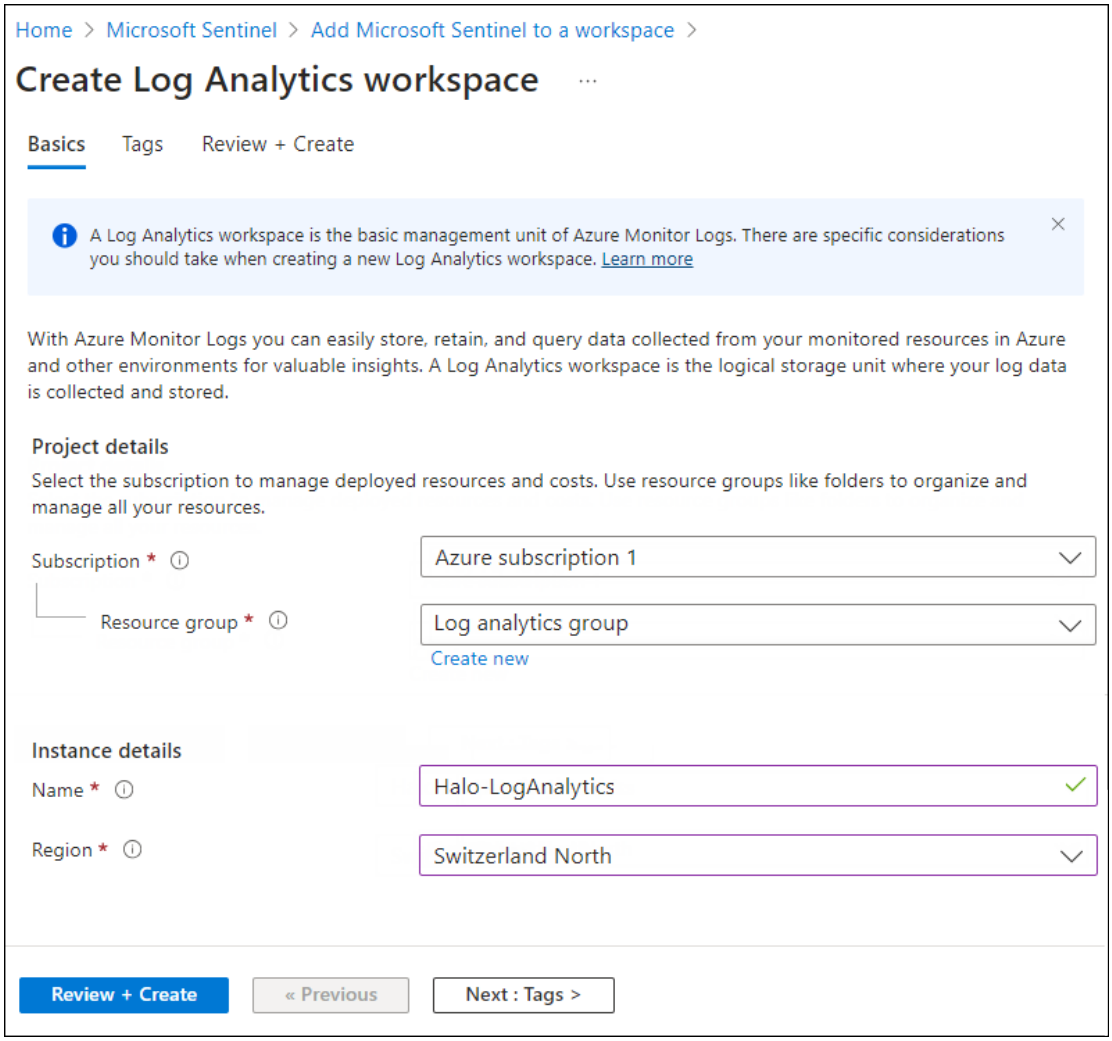
Microsoft Sentinel is a scalable, cloud-native security information and event management (SIEM) that delivers an intelligent and comprehensive solution for SIEM. Microsoft Sentinel provides cyberthreat detection, investigation, response, and proactive hunting, with a bird's-eye view across your enterprise. To begin using Microsoft Sentinel, the log analytics workspace must be configured.

3.2.4.1. Configuring Microsoft Sentinel

The explanation given in this section is only meant to serve as an example. Only the fundamental procedures for creating a workspace are shown in this section. Please refer to the Microsoft documentation for a detailed explanation of the configuration and settings. The information in the Microsoft documentation overrides any information published in this section.

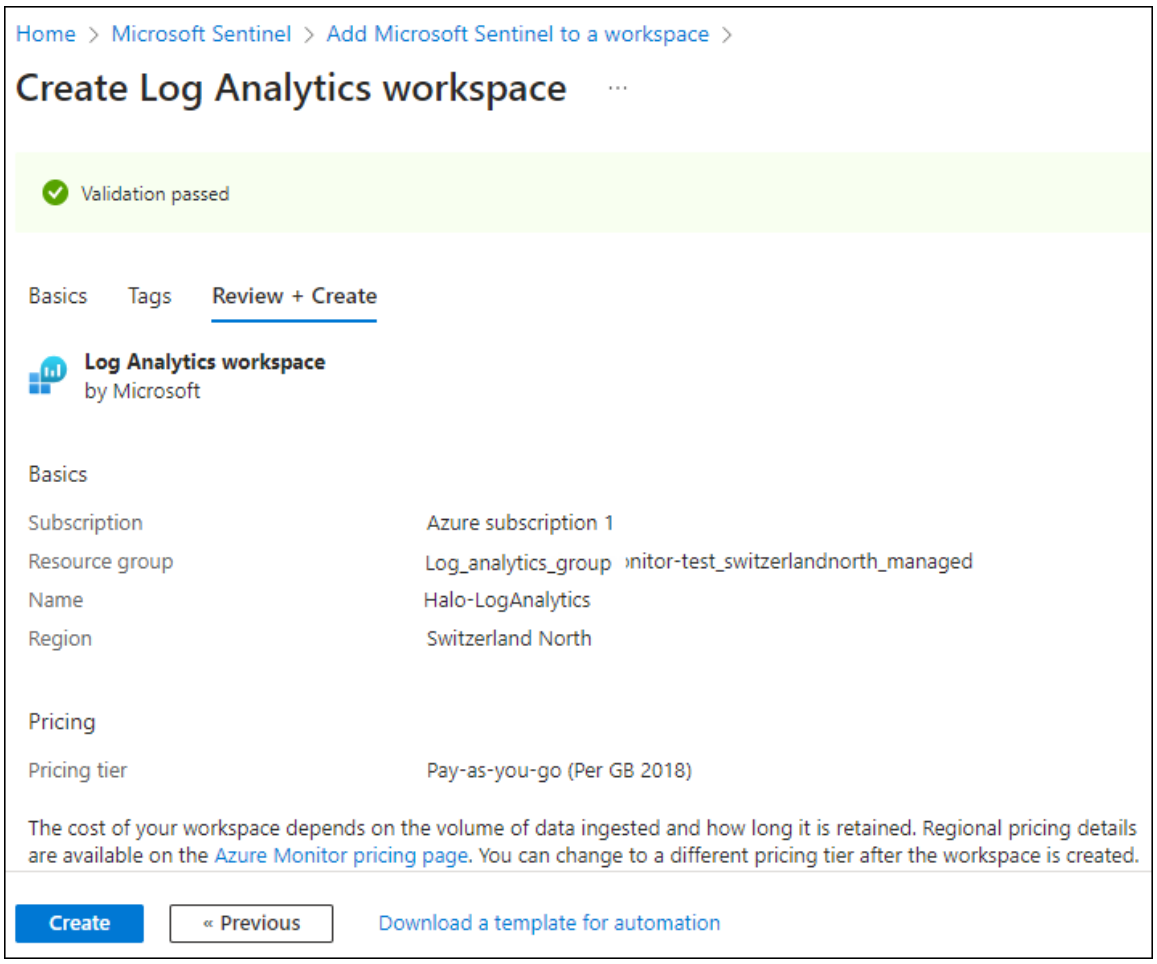
Prerequisite: Ensure that you have permission to perform this procedure.

1. Log in to the Microsoft Azure portal.
2. On the search bar, type **Microsoft Sentinel**. As you start typing, the list filters according to your input.
3. Select **Microsoft Sentinel** from the search results.
4. The **Microsoft Sentinel** page will appear. Here, you need to click **Create** from the top of the page.
5. On the **Add Microsoft Sentinel to a workspace** page, click **Create a new workspace**.
6. The **Create Log Analytics Workspace** page will appear as shown below, and you must enter the required details on this page.



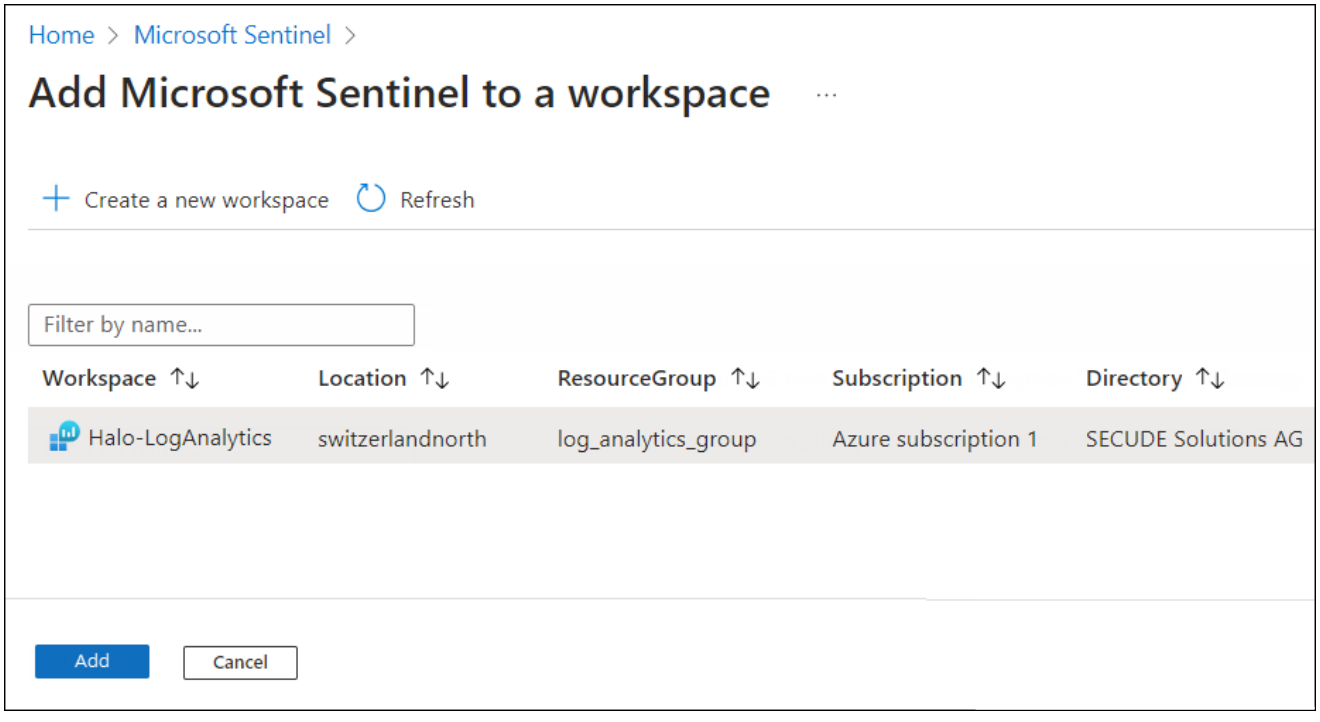
Workspace #1

7. Select a resource group from the list.
   a. Provide a name for your workspace.
   b. Choose a region from the list.
8. Once that is done, you can leave other options as-is, and then click on **Review + Create** and finally click on **Create** after the validation.



Workspace #2

9. The new workspace will be listed as follows:



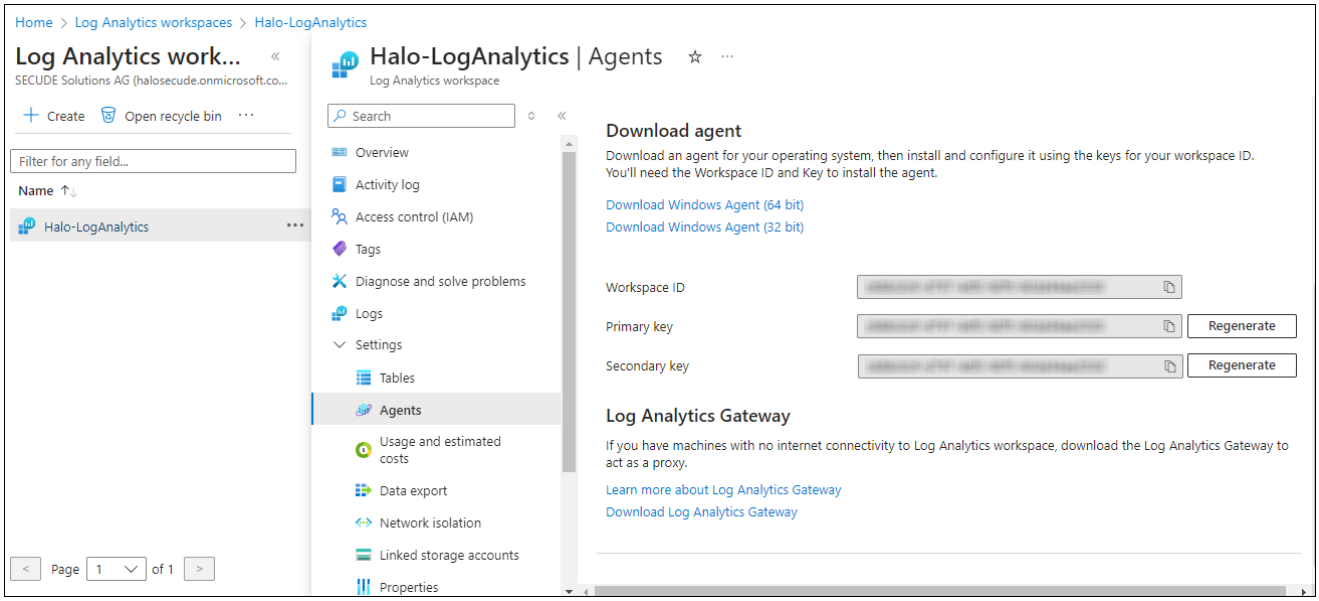
Workspace #3

10. Select the new workspace and click **Add**. The **Add** button will only be enabled if you have the required permission.
11. The connection between Microsoft Sentinel and Log Analytics is successfully created.

3.2.4.2. Fetching Key Details from Log Analytics Workspace

This section describes how to obtain the Log Analytics agent keys. Log Analytics agent keys are required to transfer logs from the HaloENGINE Admin portal to Microsoft Sentinel.

1. On the search bar, type **Log Analytics workspace**. As you start typing, the list filters according to your input.
2. Select **Log Analytics workspace** from the search results.
3. The **Log Analytics workspace** page now includes the new workspace you created in the previous section.
4. Select the new workspace.
5. In the menu, select **Settings** > **Agents**.
6. The page will provide the necessary information, including the **Workspace ID** and **Primary Key**.



Workspace #4

7. In a text editor (such as Notepad), copy the value of the **Workspace ID** and **Primary key** and save it for configuring the "Sentinel Log" in the HaloENGINE Admin portal.

3.3. HaloENGINE Installation Methods

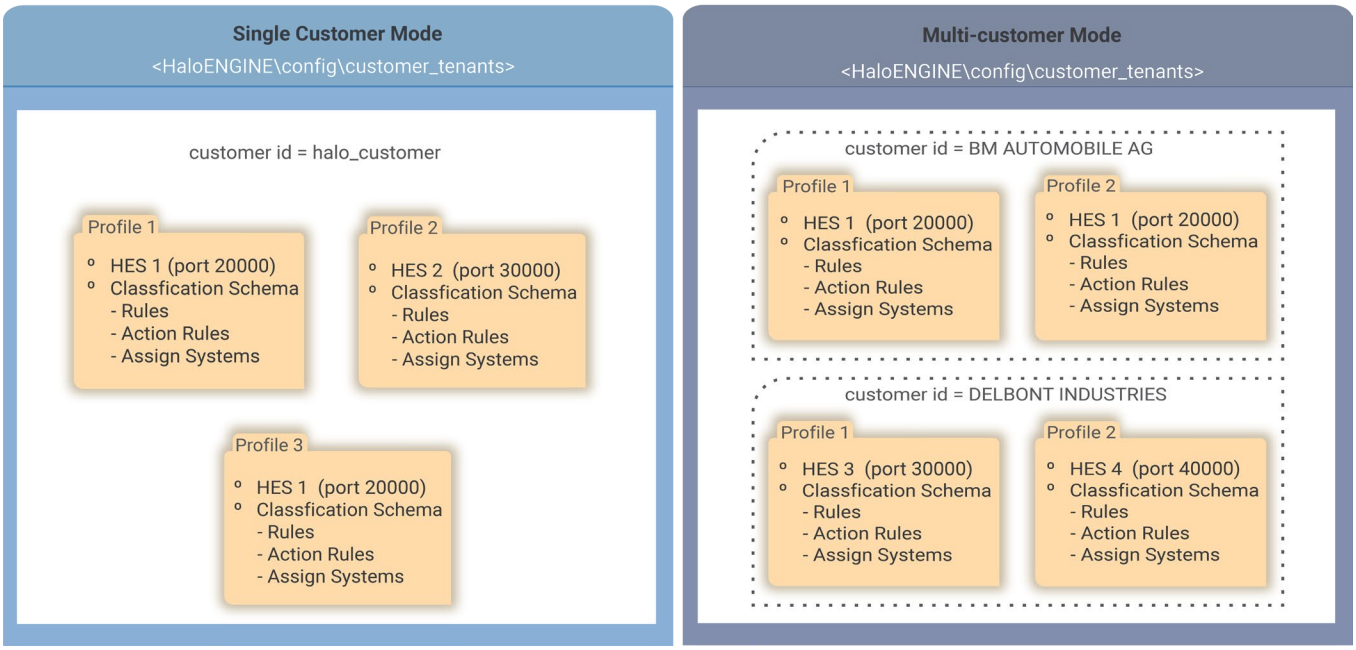
This chapter walks you through the steps of installing HaloENGINE using graphic and silent methods.

3.3.1. HaloENGINE Customer Modes

HaloENGINE can be deployed in two different modes.

1. Single Customer mode - Supports one customer with multiple tenants (HaloENGINE Services). By default, the customer ID **halo_customer** is used, but it can be modified.
2. In contrast to Single Customer, the Multi-Customer mode supports multiple customers with multiple tenants (HaloENGINE Services). It is designed in such a way that a HaloENGINE Service is targeted to a specific customer, thus other customers cannot gain access to any other HaloENGINE Service(s) of another customer.

The Single Customer and Multi-Customer folder structures after configuration are depicted in the figure below.



HaloENGINE Modes

3.3.2. HaloENGINE With or Without Monitor Log Dashboard Integration

It is necessary to know how you would like to install the HaloENGINE with the following options. HaloENGINE can be used with or without the Monitor Log Dashboard Integration.

Option 1: HaloENGINE with Monitor Log Dashboard

The Monitor Log Dashboard is connected to HaloENGINE through the MongoDB database. During the installation process, you have the option to choose from the following two depending on your database setup:

1. First-time installation of the MongoDB database.
   This applies to an environment without a MongoDB database. While installing HaloENGINE, select **Install MongoDB** in the UI. The dashboard can only be successfully started over this connection.
2. Use the existing MongoDB database.
   This applies to an environment where a MongoDB database has already been installed. To connect, all you need to do is use the current MongoDB connection string.

Option 2: HaloENGINE without Monitor Log Dashboard

If you do not want to integrate the dashboard, installing the MongoDB database is not necessary. At a later time, if you want to integrate with the dashboard, you need to uninstall and reinstall HaloENGINE with Option 1.

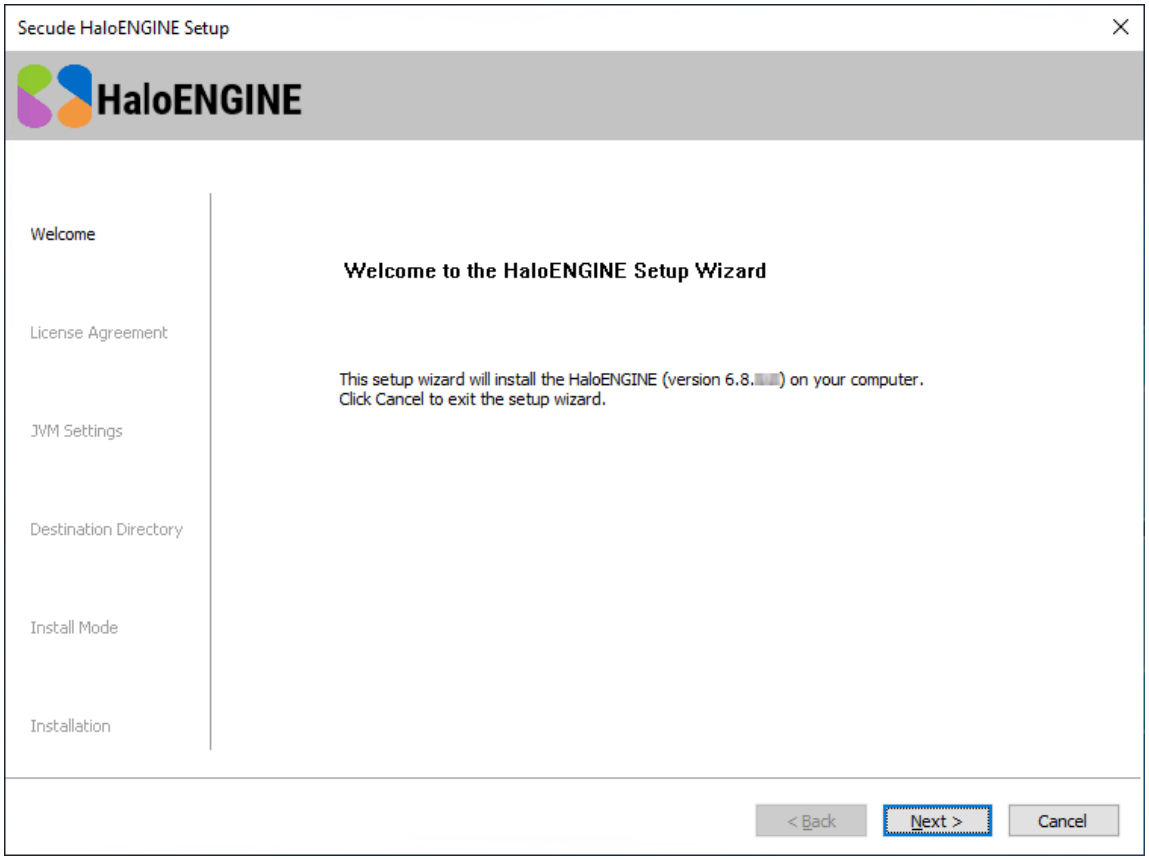
3.3.3. Interactive Installation

Use the GUI-based setup application included in the installation package to install HaloENGINE. If you want to run without a GUI, refer to the section "Silent Installation". Note: This version does not support silent installation for integrating HaloENGINE with the dashboard. If you want to integrate, use the GUI installer.

Installation Procedure

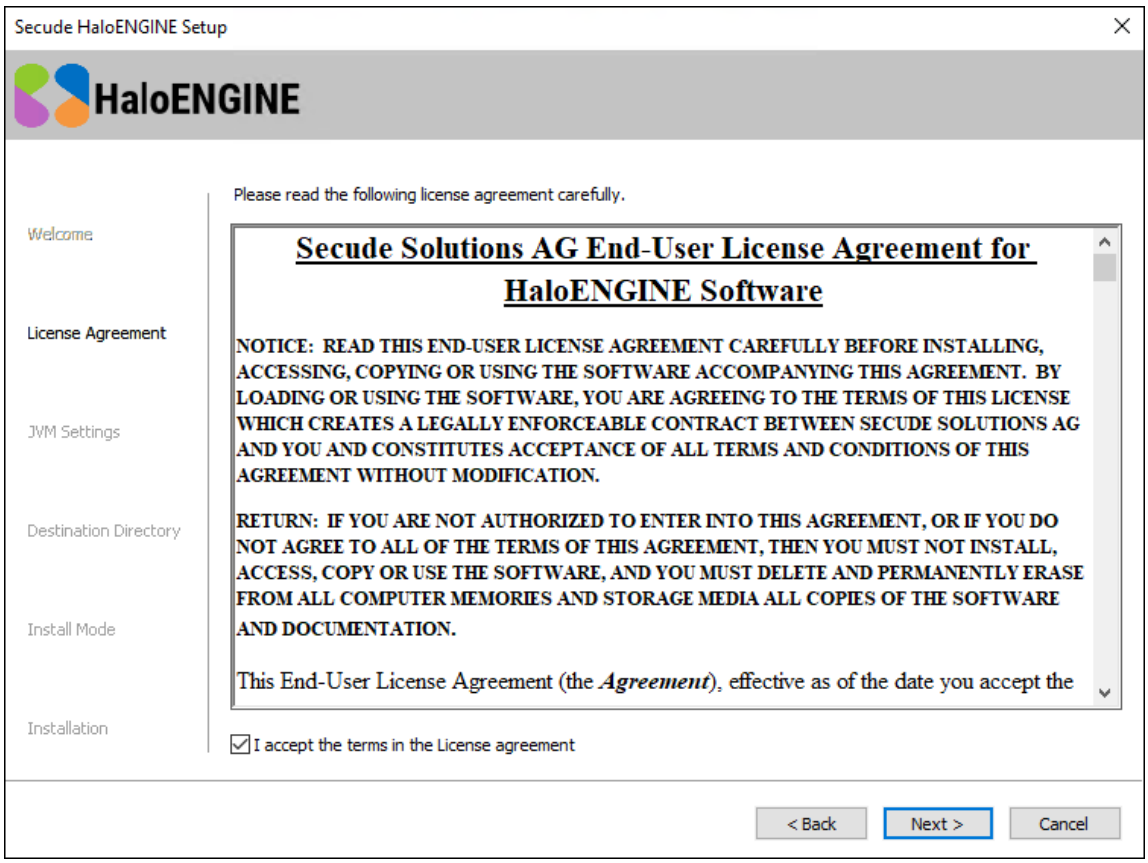
1. To begin the interactive installation, double-click the installer `HaloENGINE_Setup.exe` file. Depending on your Windows security settings, you may get a warning such as "*Do you want to allow the following program to make changes to this computer?*". If you get this security warning, click the **Yes** button to continue the installation.
2. When the installer starts, you will see the startup dialog followed by the welcome dialog:

Startup Dialog



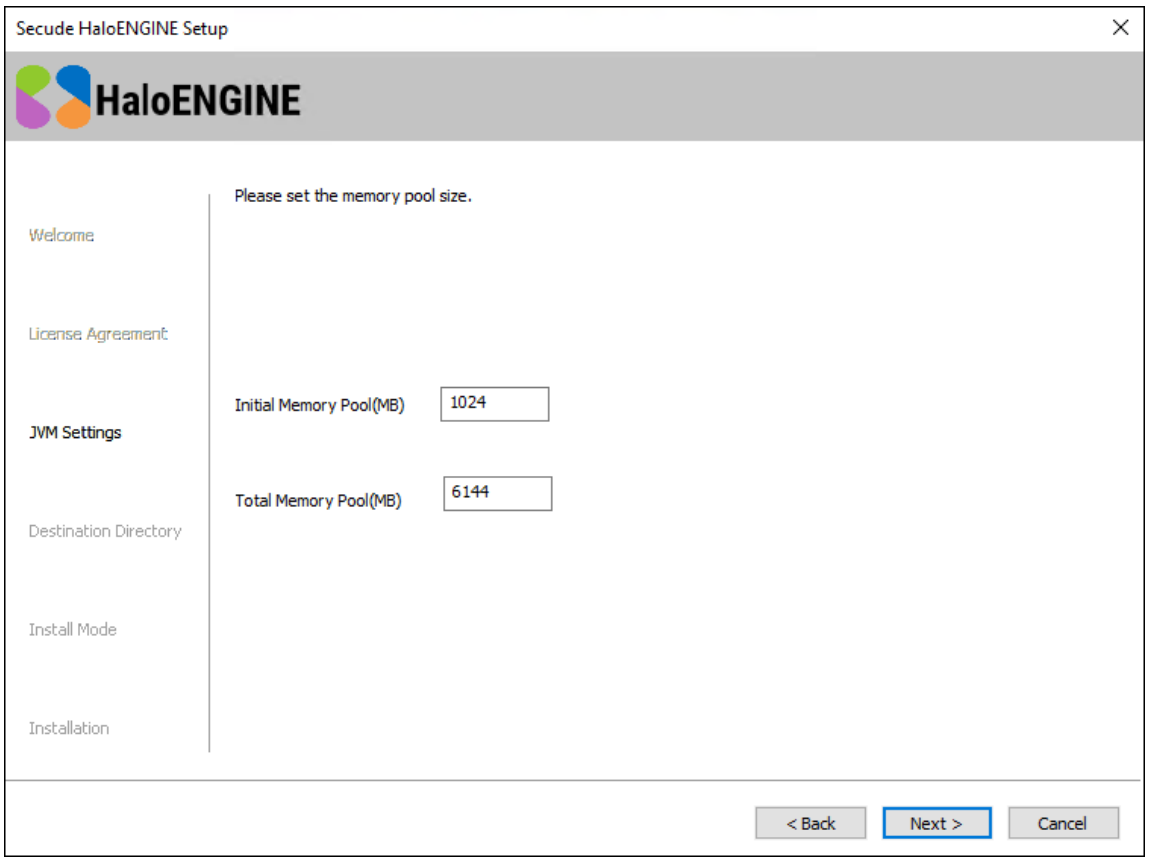
Welcome dialog

3. Click **Next** to continue the installation. The end-user license agreement dialog will appear:



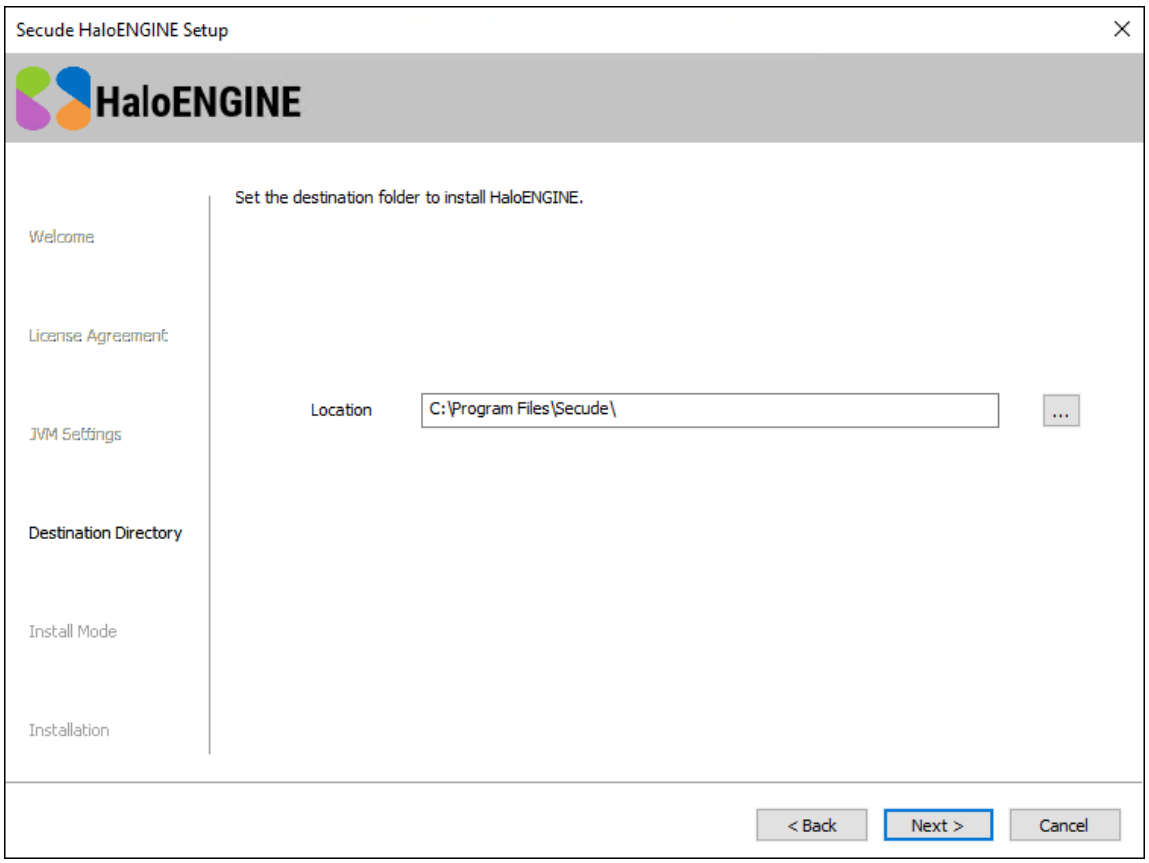
End-User License Agreement dialog

4. Read the End-User License Agreement. If you agree, select **I accept the terms in the License Agreement** and click **Next**. The Tomcat memory pool size configuration dialog will appear:



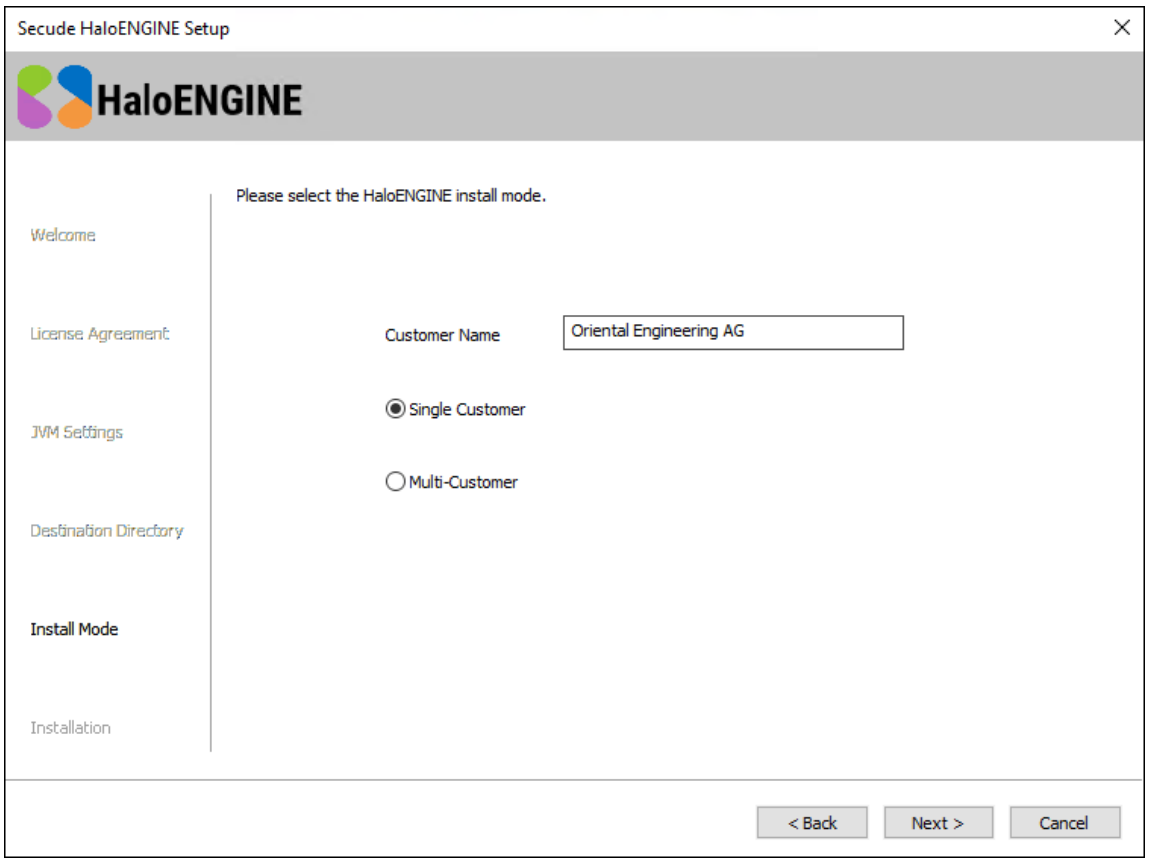
Tomcat pool size configuration dialog

5. If you want to change the default values of the **Initial Memory Pool** and **Total Memory Pool**, enter the amount of memory you want to allocate. Note: Ensure that the Total Memory Pool does not exceed the System's available 3/4th RAM.
6. Click **Next**. The destination folder selection dialog will appear:



Destination folder selection dialog

7. By default, application files are stored in the program files directory (`C:\Program Files\Secude\`). If you would like to choose an alternate location, click the **Browse** button and select your location preference. When you are finished, click **Next**.
8. The customer mode selection dialog will appear:

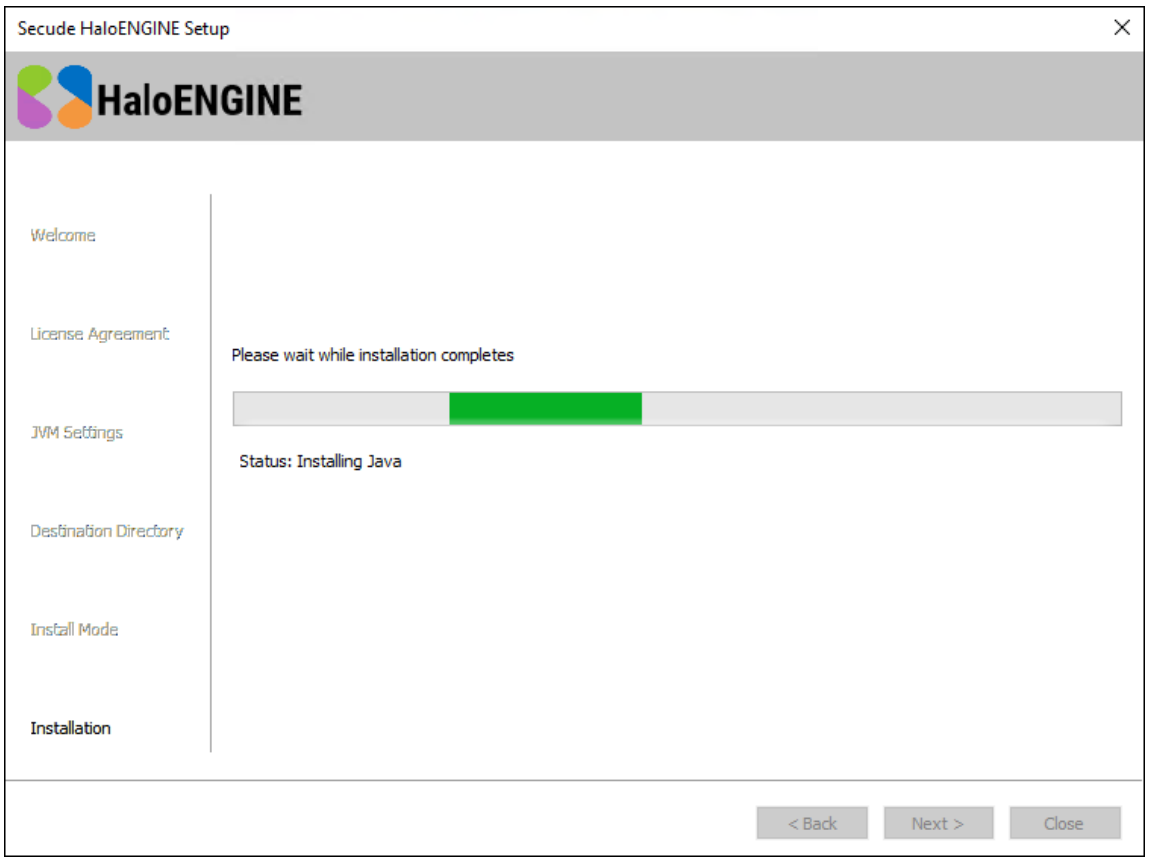


Customer mode selection dialog

a. Enter the name of the organization where HaloENGINE will be implemented. For instance, Oriental Engineering AG purchased HaloENGINE to use within their workplace.

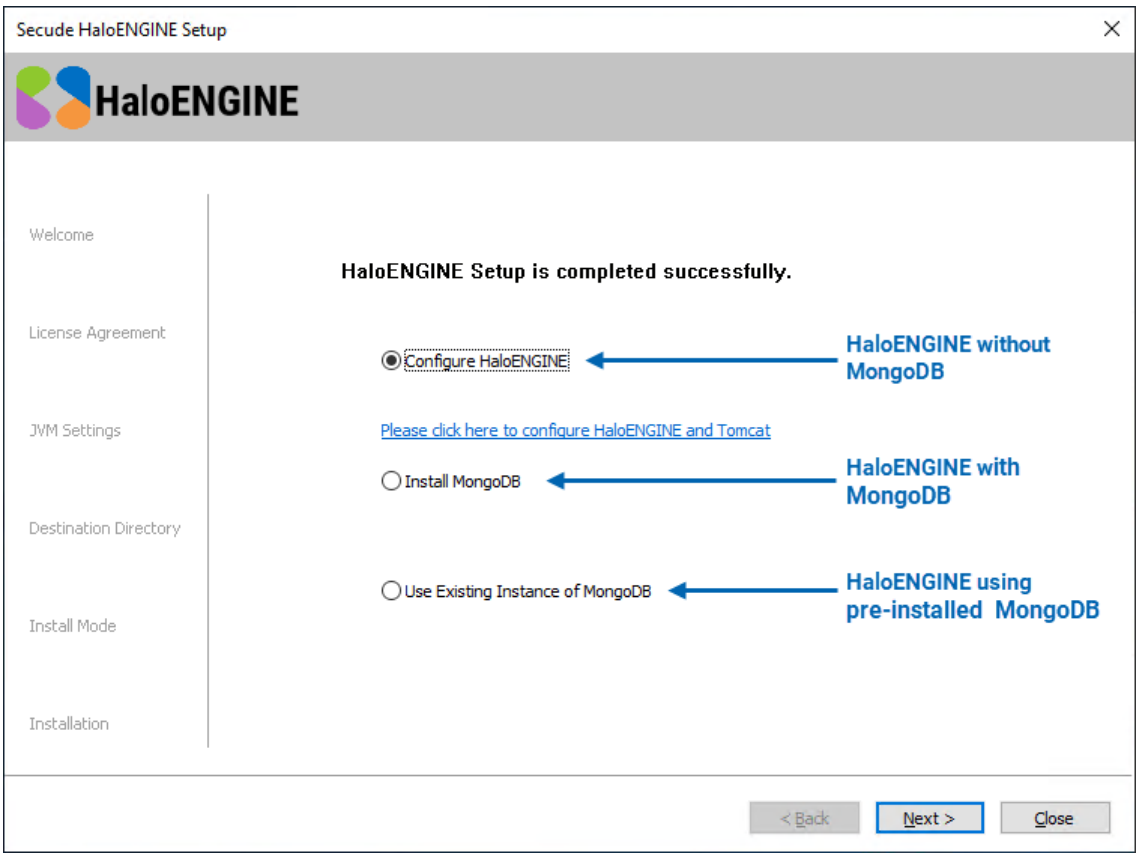
b. Select a mode (**Single Customer** or **Multi-Customer**), and click **Next**.

9. Please be patient as the installation will take some time. You can see the installation progress in the dialog:



Installation progress dialog

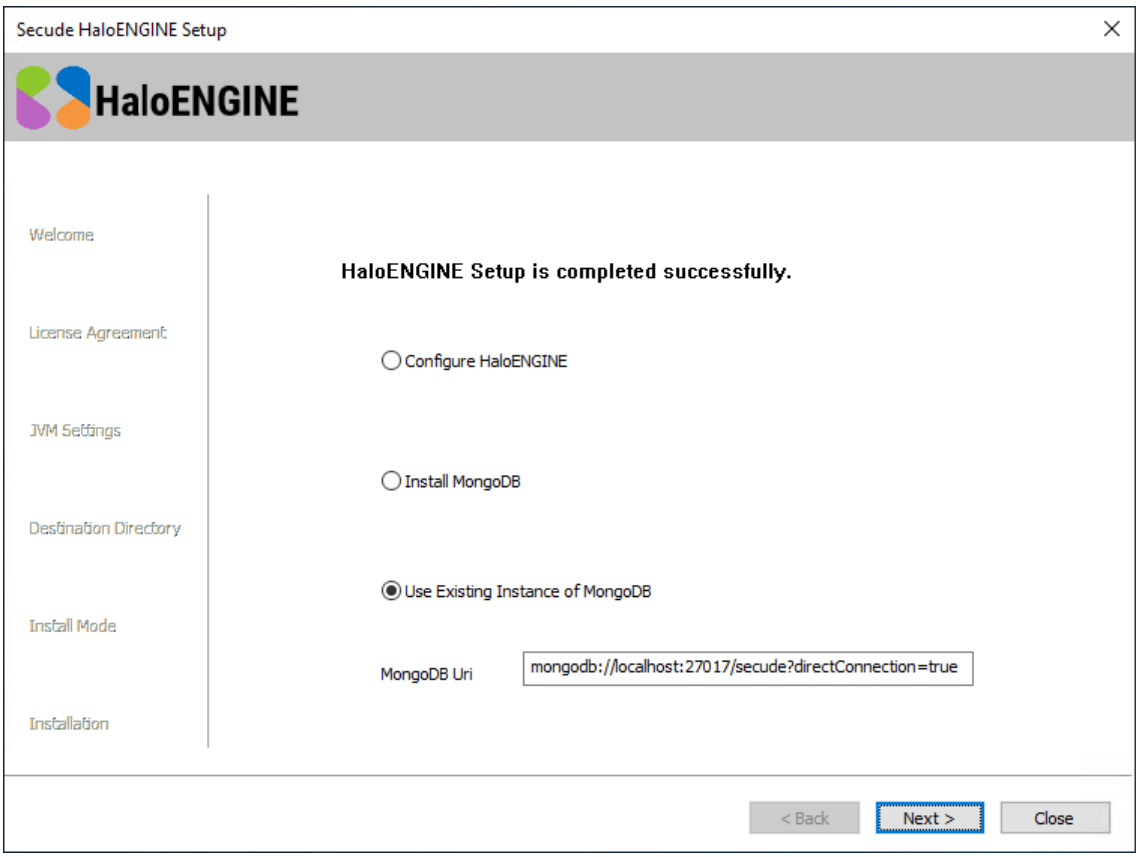
10. When the installation is completed, you will see a message confirming that the HaloENGINE Server has been successfully installed. Select one of the following options to configure the HaloENGINE Server.



HaloENGINE setup without MongoDB

a. HaloENGINE without MongoDB: Select the **Configure HaloENGINE** option if you do not want to integrate the dashboard. As shown above, the configuration screen will display a link. Click the link to access the HaloENGINE admin portal, then proceed with point 12.

b. HaloENGINE with MongoDB: Select the **Install MongoDB** option if MongoDB is not currently installed in your environment. Click **Next**. The installation starts by displaying a progress bar that indicates the progress of the process. Please be patient as this will take some time. After installing MongoDB, the configuration screen will display a link. Click the link to access the HaloENGINE admin portal, then proceed with point 12.



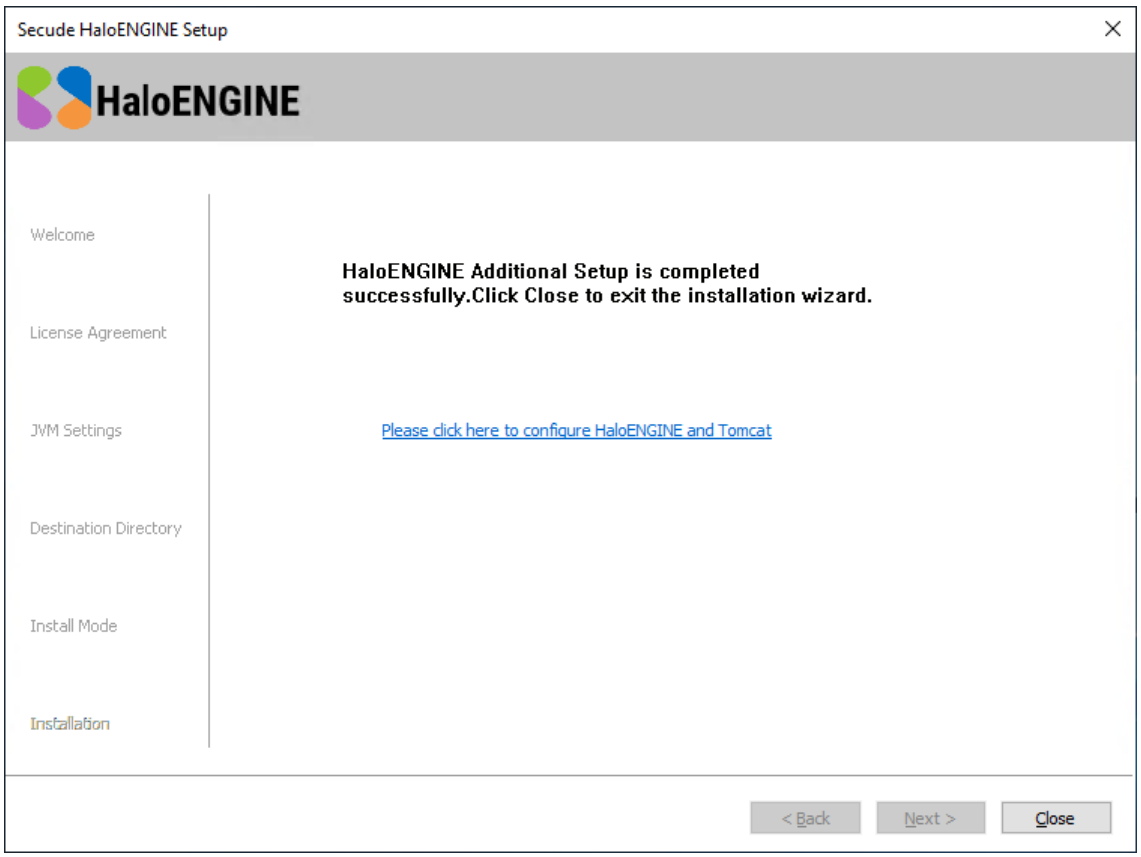
MongoDBHaloENGINE setup with pre-installed

c. HaloENGINE using pre-installed MongoDB: Select the **Use Existing Instance of MongoDB** option if the database already exists and then enter the MongoDB connection string in the **MongoDB Uri** field. The connection string varies depending on your configuration options.

   - With authentication, use the format `<mongodb>://<username>:<password>@<hostname>:<port>/<db_name>?authSource=admin>`. For example: `mongodb://myDatabaseUser:D1fficultP%40ssw0rd@cluster0.example.mongodb.net/?retryWrites=true&w=majority`
   - Without authentication, use the format `<mongodb>://<hostname>:<port>/<dbname>?directConnection=true>`. For example: `mongodb://localhost:27017/secude?directConnection=true`

d. Click **Next**,

11. The configuration screen will display a link. To access the HaloENGINE admin portal, click on the link.



HaloENGINE with additional setup completed successfully

12. Once you click the link, the admin portal will open in your default browser and you will notice a shortcut icon 

created on the desktop.

What to do next

1. Verify that the **Maximum memory pool size** in HaloENGINE Tomcat (…`bin/HaloENGINE_Tomcat9.exe`) does not exceed the system RAM. After setting up the HaloENGINE certificate, verify that the **maxSavePostSize** (bytes) from the Connector, which is SSLEnabled (in `server.xml`) and smaller than the "Maximum memory pool size".
2. If you want to send large files (2GB) forward and backward, make sure that the "Maximum memory pool size" is more than the maxSavePostSize (2GB, as specified above).
3. Please refer to the section "Initial Configuration of HaloENGINE Admin Portal" to know more about the initial configuration.

3.3.4. Silent Installation

Besides graphical mode, the HaloENGINE can be installed in silent mode, which does not require user involvement or display a user interface. It is a convenient way to streamline the installation process using the command at once.

1. Open a command prompt and go to the installer's location.
2. Follow the steps below to see the list of options present in silent mode:

   Type `HaloENGINE_Setup.exe -help`

   Press **Enter**

   Output

   ```
   ...
   HaloENGINE_Setup.exe -install -initmempool <Initial memory pool size in MB(s).
   Minimum size is 128 MB> -totalmempool <Total memory pool size in MB(s).
   Maximum size is 3/4 of total RAM size.> -dir <destination_directory> -installmode
   <SINGLE_CUSTOMER|MULTI_CUSTOMER> -customername <customer_name>
   HaloENGINE_Setup.exe -update -installmode <SINGLE_CUSTOMER|MULTI_CUSTOMER> -
   customername <customer_name>
   HaloENGINE_Setup.exe -uninstall -keepconfig <true|false>
   ```
3. The following are examples of silent mode installation:

   Install

   ```
   HaloENGINE_Setup.exe -install -initmempool 1024 -totalmempool 2048 -dir "C:\Program
   Files\Secude" -installmode SINGLE_CUSTOMER -customername "Oriental Engineering AG"
   ```

   Update

   ```
   HaloENGINE_Setup.exe -update -installmode SINGLE_CUSTOMER -customername "Oriental
   Engineering AG"
   ```

   (The current installer version must be greater; otherwise, an error notice will block the update)
4. Press **Enter**.
5. The installation process is complete, and you can access the HaloENGINE Admin portal.

3.4. Initial Configuration of HaloENGINE Admin Portal

This section describes the portal features and how to get started with the HaloENGINE Admin Portal.

3.4.1. Features

1. **Single Point Management**: You may manage all of your systems from the HaloENGINE Admin portal.
2. **Role-based access controls and security features**: The HaloENGINE Admin portal supports role-based authentication and authorization.
3. **User-Friendly UI**: The HaloENGINE Admin portaloffers a user-friendly user interface that is simple to understand with minimal knowledge of the platform.
4. **Business logic**: The classification engine makes all decisions in terms of business logic.
5. **Dashboard**: A business-friendly dashboard that displays high-level information in a single view, including live and historical log data from HaloENGINE monitor logs.

3.4.2. Reload and Restart

There will be references to both "reload" and "restart" throughout this manual. To avoid confusion, it's important to be familiar with these two terminologies.

What is meant by reload?

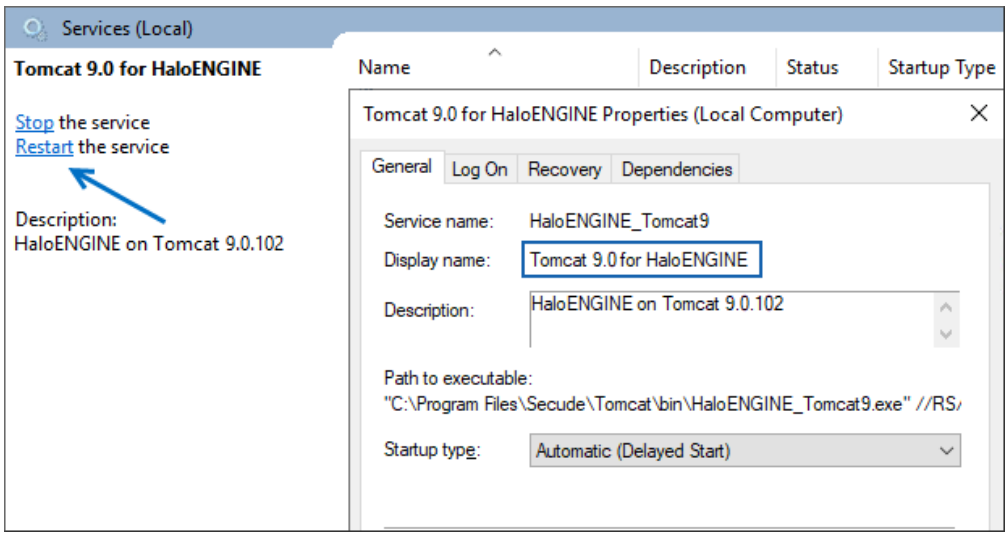
Reloading will instruct the service to reload its configuration files while leaving the current process running. It is considerably faster. When you make changes, such as updating or changing any rules, you must click the 'Reload Configuration' button for the change to take effect.

What is meant by restart?

A restart will instruct the service to stop operating completely and then resume. Restarting the HaloENGINE Tomcat service takes some time. The HaloENGINE Tomcat service must be restarted after any modification to the license activation, certificate, tenant configuration, SAPJCo update, import settings, or Remote Settings.

How to Restart the HaloENGINE Tomcat Service

1. Open the **Start** screen, type `services.msc`, and press **Enter** or **Press** the `Windows Key+R`, type in `services.msc`, and press **Enter**.
2. Locate the **Display Name** - **Tomcat 9.0 for HaloENGINE**.

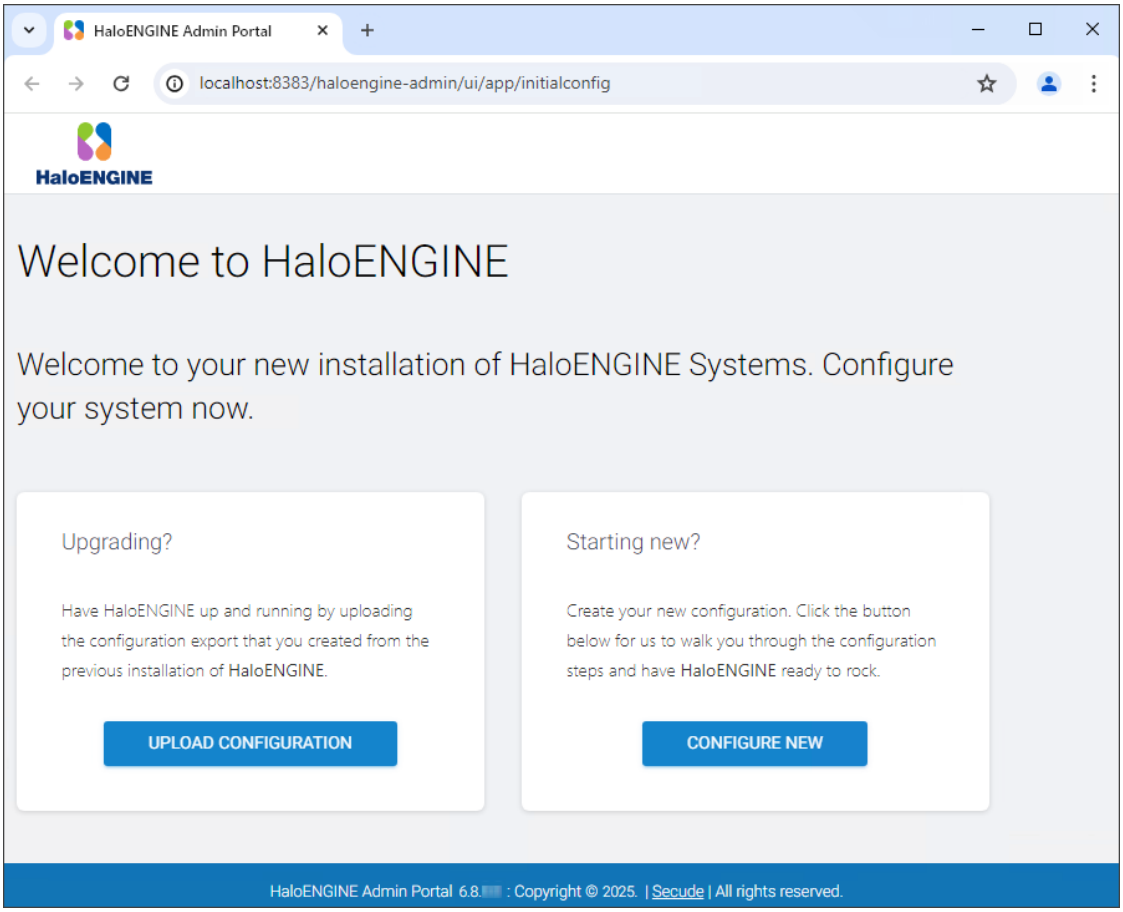


Restarting Tomcat Service

3. Click **Restart** and wait for a few minutes.

3.4.3. Welcome Page

A welcome page is displayed after clicking the installer link. It appears just the first time you configure the portal.



Welcome page

HaloENGINE provides the following options:

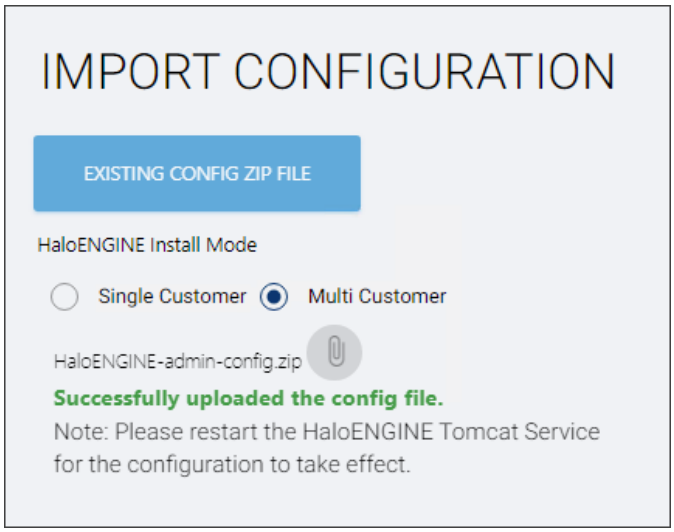
1. **Upgrade**: Moving to a newer version while keeping the existing configuration file. Please refer to the section "Upgrading (Uploading Existing Configuration File)".
2. **Starting new**: Creating a new configuration file to set up HaloENGINE. Please refer to the section "Starting a New HaloENGINE".

3.4.4. Upgrading (Uploading Existing Configuration File)

Prerequisite: Make sure you have exported the configuration zip file from the pre-existing HaloENGINE.

Follow the instructions below to upgrade:

1. Click **Upload Configuration** and then click **Existing Config Zip File**.
2. Select your installation mode – **Single Customer**/**Multi-Customer**.
3. You will notice that an attachment button appears to select the file.
4. Click the button and choose the `HaloENGINE-admin-config.zip` file from the **Open** Windows dialog box.
5. The name of the zip file is displayed on the page.



Uploading existing configuration file

6. You will receive a confirmation message after uploading the configuration file.
7. Restart the HaloENGINE Tomcat Service.
8. The next step is to set up the classification engine. Please refer to the section "Setting Up Classification Engine".

Reset Password

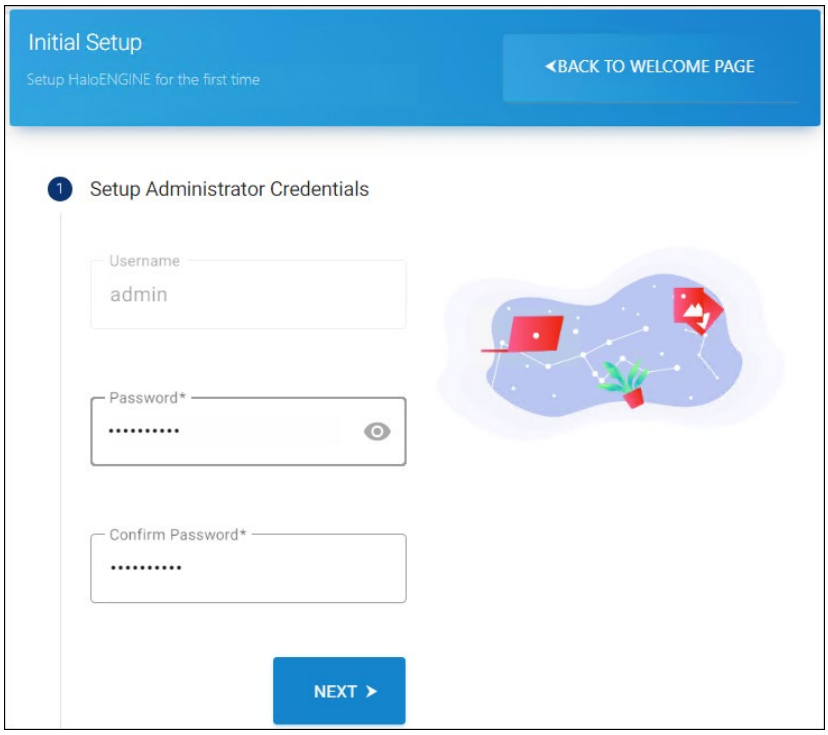
If your administrator password in the previous version is less than 12 characters, you must reset it according to the current password policy. To know how to reset the password, refer to the section "Reset Administrator Password".

3.4.5. Starting a New HaloENGINE

If this is your first time installing HaloENGINE, click **Configure** and proceed as instructed below:

3.4.5.1. Step 1. Logging into Portal for the First Time

1. On the *Initial Setup* page, you must create administrator credentials to access the HaloENGINE Admin Portal.



First time logging the page

2. As per policy, enter a strong password, then reenter it. The password-eye icon allows you to reveal or conceal your password.
3. Click **Next**.

Password Policy

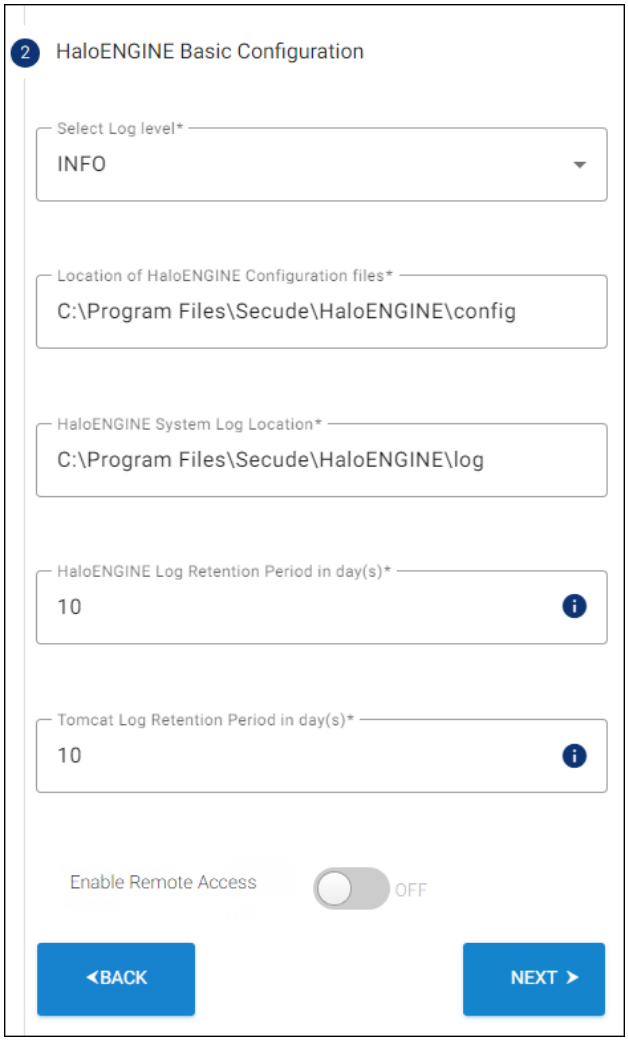
Be sure to use a strong, but memorable password. If you forget the password, HaloENGINE offers a way to reset it. To know how to reset the password, refer to the section "Reset Administrator Password".

- Passwords must be between **12** to **30 characters** long

- Password should not contain space
- A minimum of **1 uppercase** letter [A-Z]
- A minimum of **1 lowercase** letter [a-z]
- A minimum of **1 numeric character** [0-9]
- A minimum of **1 symbol** (@+%_-&#?|{}:;!*^$'[ ]" < > \ /)
  For example `HaloE$7Tg}@!`

3.4.5.2. Step 2. HaloENGINE Basic Configuration

1. The following page is used to configure the basic settings.



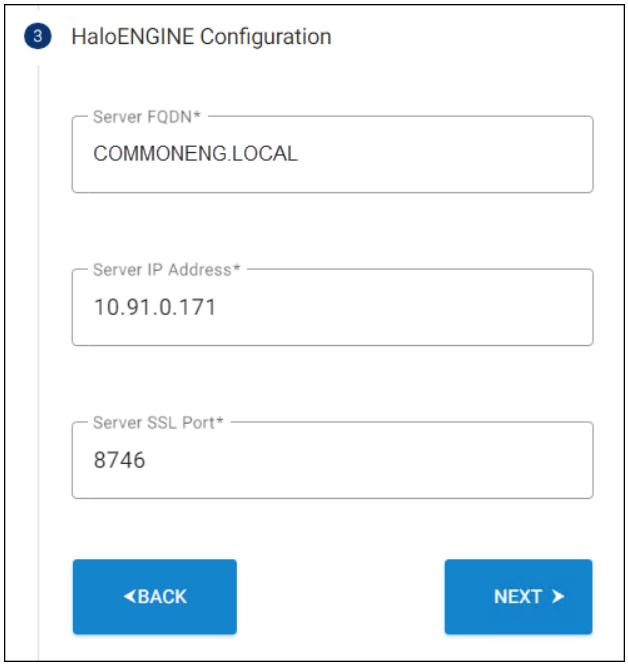
Basic Configuration Page

2. **Default Customer Name**—In single customer mode, the default customer name is `halo_customer`. After portal initialization, you can change this default customer name.
3. **Select Log level**—Choose a type of error log level (INFO/DEBUG/ERROR/WARN/ALL).
4. **Location of HaloENGINE Configuration Files**—Enter the configuration file's path. The default path is `C:\Program Files\Secude\HaloENGINE\config`.

5. **HaloENGINE System Log Location**—Enter the file path for the HaloENGINE system log. The default path is `C:\Program Files\Secude\HaloENGINE\log`.
6. **HaloENGINE Log Retention Period in day(s)**—Set the duration for which the HaloENGINE logs should be available. The log retention period is determined by the days you specify here. Log files older than the retention period will be deleted. For example, if you specify it as 10, log files older than 10 days are deleted. Range: 0 to 90 days.
7. **Tomcat Log Retention Period in day(s)**—Specify how long the Tomcat logs should be available. Range: 0 to 90 days.
8. **Enable Remote Access**—To enable access to configure the HaloENGINE Admin portal remotely (via IP), click on the slider button. Note: Please restart the HaloENGINE Tomcat service if you have made changes in the **Configure Remote Access** property.
9. Click **Next**.

3.4.5.3. Step 3. HaloENGINE Configuration

1. Your server's details, such as the fully qualified domain name, IP address, and default port number, will be filled in automatically on this page. If needed, you can modify the port number. Note: Once the port has been configured, it cannot be changed. Therefore, kindly make the necessary modifications. If you still want to modify the port, back up the configuration and then remove the HaloENGINE. Reinstall the HaloENGINE, then modify the port.

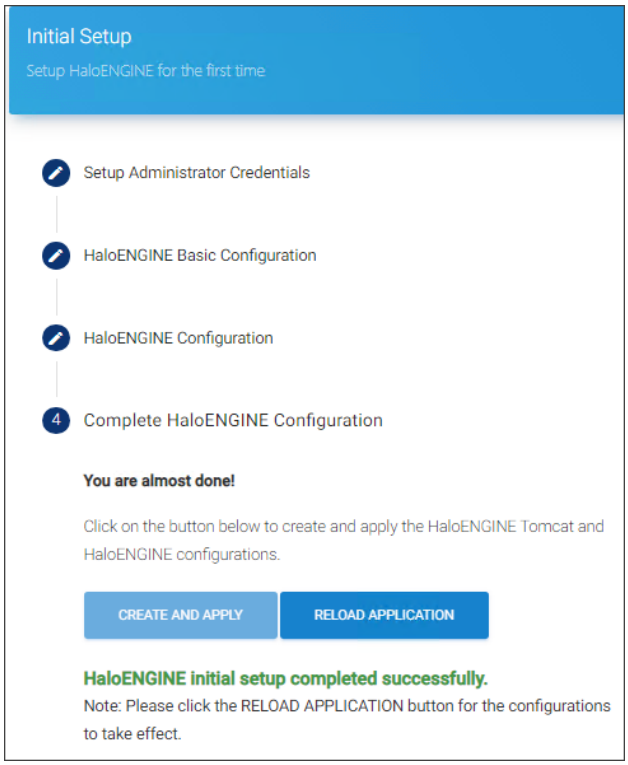


Configuration page

2. Click **Next**.

3.4.5.4. Step 4. Completion Page

1. This is the final page of the configuration.



Final configuration page

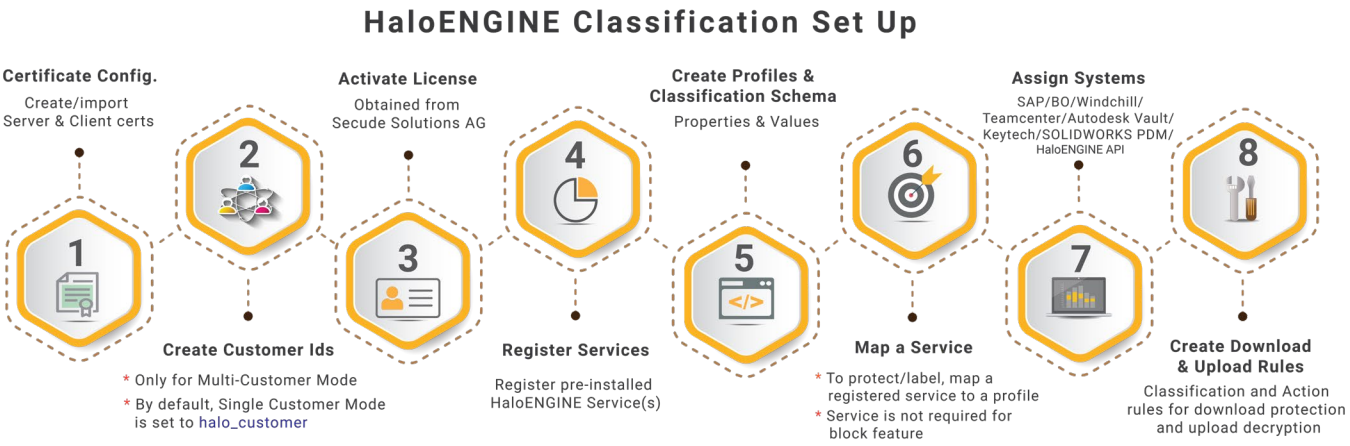
2. Click **Create and Apply** to create `config.properties` file and update the `hc-servlet.xml` file.
3. Click **Reload Application** to update the changes done. After reloading, the page will redirect to the login page.
4. These settings can always be changed through the portal as detailed in the section "System Configuration".

3.5. Setting Up Classification Engine

This chapter describes how to set up HaloENGINE.

3.5.1. Quick Start Set Up

The process of configuring the Classification Engine is shown in high-level detail in the figure below.



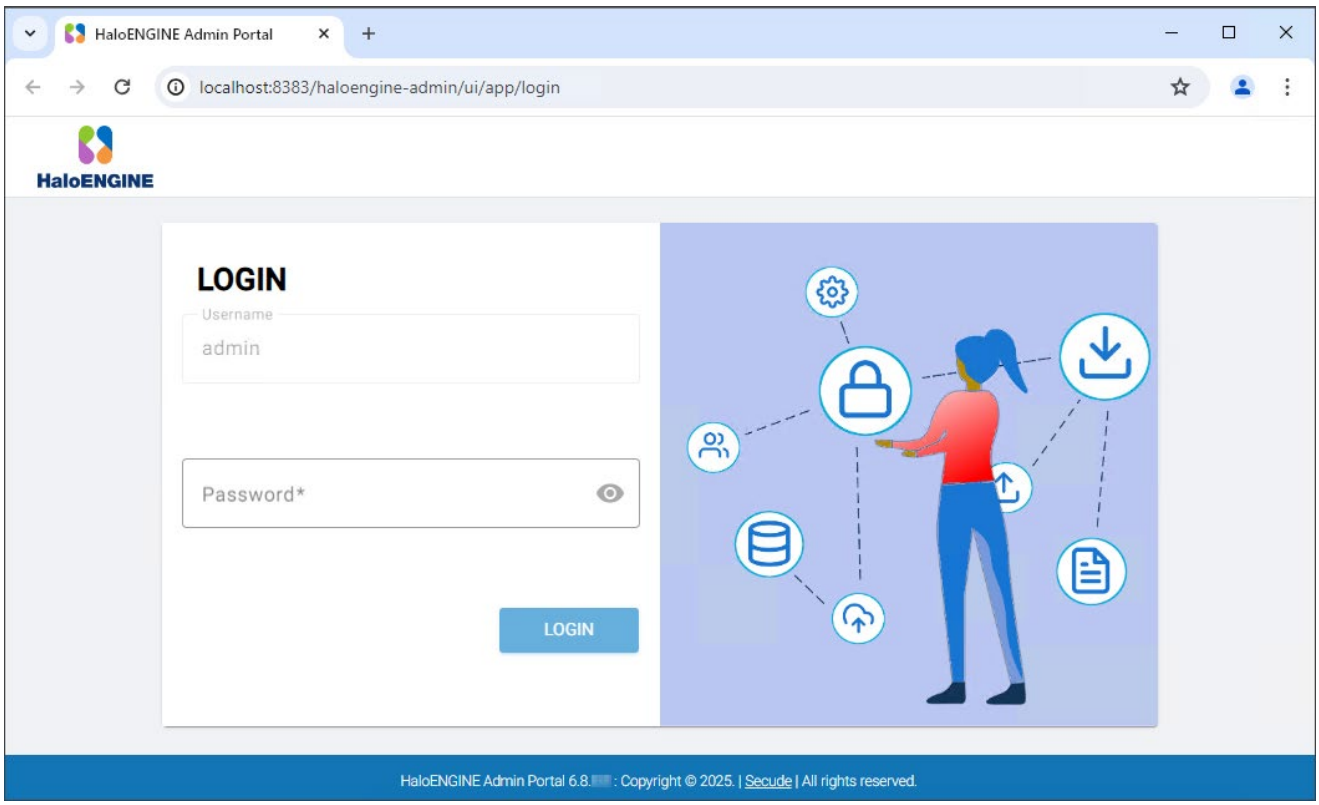
Setting up Classification Engine

The license file you obtained from Secude will contain specific features and system types. This implies that only the system types that you have obtained in the license are accessible by their respective endpoints. This chapter covers all feature sets (Monitor, Block, and Protect) that are common to all system types, including BO, SAP, Windchill, Teamcenter, Keytech, Autodesk_Vault, SOLIDWORKS_PDM, and HaloENGINE_API. However, for visual representation purposes, only one system type (SAP) is shown. Refer to the HaloCAD PLM/PDM Operations Manual if you would like to view the metadata, log, and user interface for a particular system type.

3.5.2. Logging into the Admin Portal

Follow the steps below to configure the HaloENGINE features and classification properties:

1. After reloading, you will be directed to the login screen, as seen in the figure below.



Login page after initial configuration

2. Enter the password that was assigned in the initial configuration. Note: Copy and paste are not allowed in this field.

   Results:

   a. The HaloENGINE Admin Home page is the first page you view after logging into the portal.

   b. Please refer to the following section.

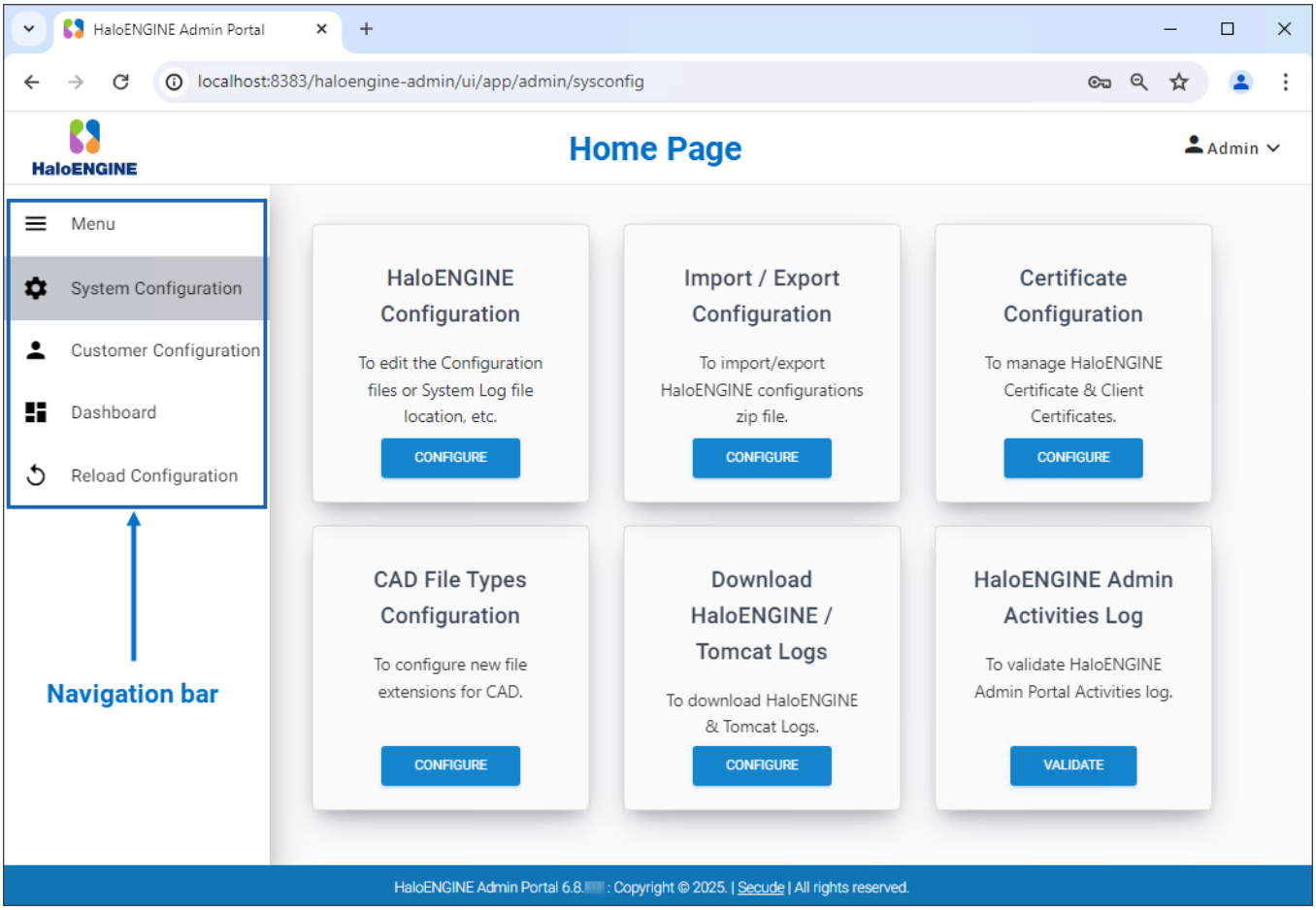
Invalid credentials or the number of sessions exceeded

You might occasionally receive the message "*Invalid credentials or number of sessions exceeded*" while attempting to enter the admin portal. One of two things could be the cause of this message:

1. Entered an invalid password.
2. Opened a second session, or even suddenly ended the current one by closing the tab rather than logging out of the application (wherein the session remains internally active). You might need to clear the browser cache in this case.

3.5.3. HaloENGINE Admin Portal Home Page

When an administrator logs into the admin portal, the homepage is the landing page. This page contains options that will assist you in managing the admin portal. It is beneficial to understand the fundamental portal elements and how to connect with them. The home page will appear as depicted in the following figure.



Home page

Directory Access

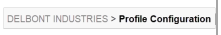
After completing the configuration, there will be a set of folders with essential files created on the HaloENGINE installed location. The default location is `C:\Program Files\Secude`. It is recommended to ensure that `C:\Program Files\Secude\HaloENGINE\config` directory allows accessing it in your system. To allow access, you can assign folder permissions to "ALL APPLICATION PACKAGES".

3.5.4. UI Elements Description

Each UI element is briefly described in the following table.

S.No	Elements	Description
1		Use this icon to create a customer ID, profile, property, rule, client, and create (server or self-signed) certificate.

S.No	Elements	Description
2	 	Use this icon to edit an existing customer ID, profile, property, rule, and client.
3		Use this icon to view the details of the customer, profile, property, service, and rule.
4		Use this icon to copy an existing profile, property, and rule. For example: Select an existing profile > Click **Copy** icon > Modify the name > Click **Save**.
5	 	Use this icon to delete an existing profile, property, rule, client, and Keystore.
6		Use this icon to move a rule to the top.
7		Use this icon to move a rule to the bottom.
8		Use this icon to revert to the previous settings.
9		Use this icon to save the current settings.
10		Use this icon to export a certificate/profile and download service logs.
11		Use this icon to import a certificate/profile. For example: Click **Import Profile** icon > Click **Select Profile zip file** > Select the file > Click **Import**.

S.No	Elements	Description
12		Use this slider button to enable/disable a setting.
13		Use this button to attach a file.
14		Breadcrumb This UI pattern is a secondary navigation link that helps users track of their location within the application.
15		Extended Tags Use this icon to include additional metadata while downloading a file from SAP.

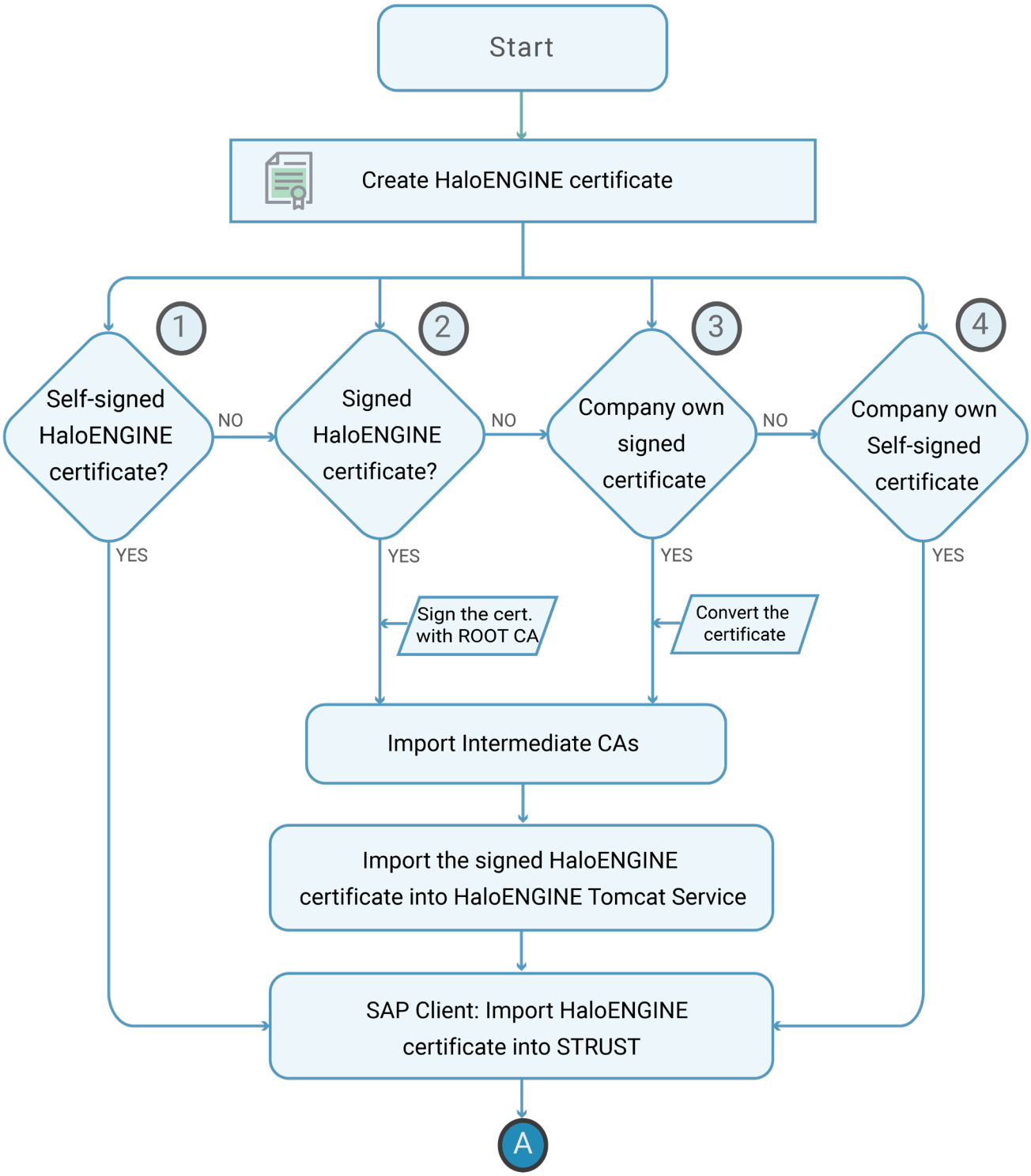
Elements Description

3.5.5. Phase 1. Certificate Configuration

The HaloENGINE Admin portal includes a reliable approach for dealing with certificates. It provides two approaches for dealing with a server certificate:

1. A self-signed server certificate is generated by the server itself.
2. Or using the organization's own certificate.

The figure below depicts the high-level steps involved in administering the server certificate.



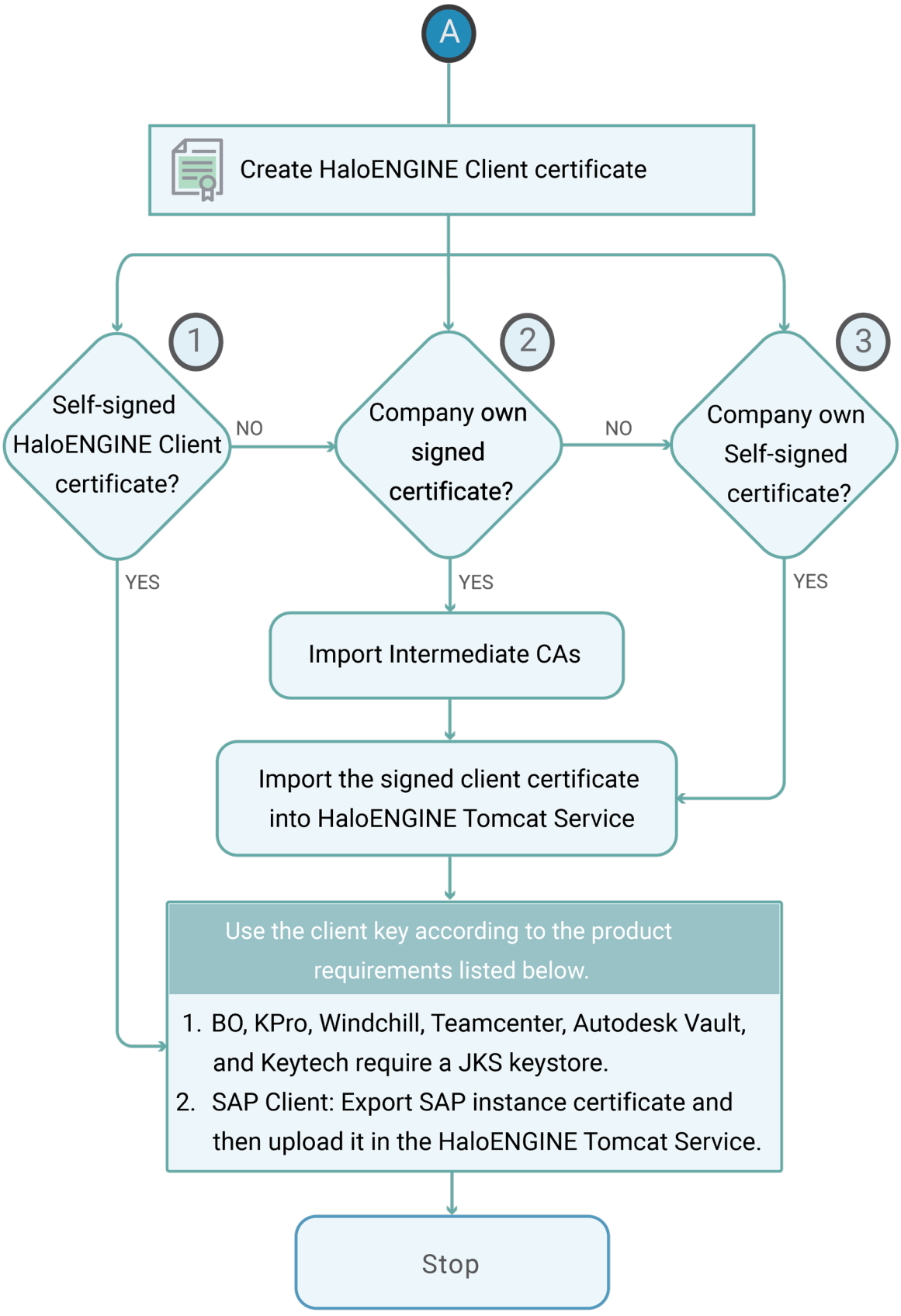
HaloENGINE Certificate

HaloCAD for SOLIDWORKS PDM client relies on server certificate authentication, therefore, you can use either a self-signed certificate (`HaloENGINEServer.cer`) or a company-owned signed certificate.

Change of server certificate name

If you want to continue using the older certificate version, rename `HalocoreServer.cer` to `HaloENGINEServer.cer` and use it.

The figure below depicts the high-level steps involved in administering the client certificate.

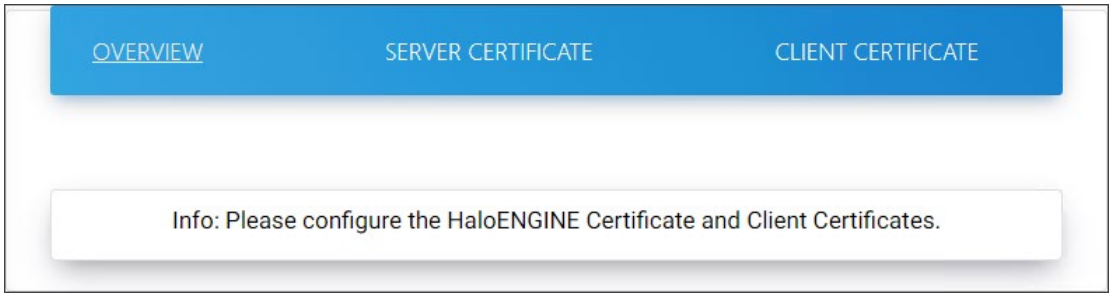


HaloENGINE Client Certificate

3.5.5.1. Step 1. Use Server Certificate Generated by HaloENGINE Admin Portal (Option 1)

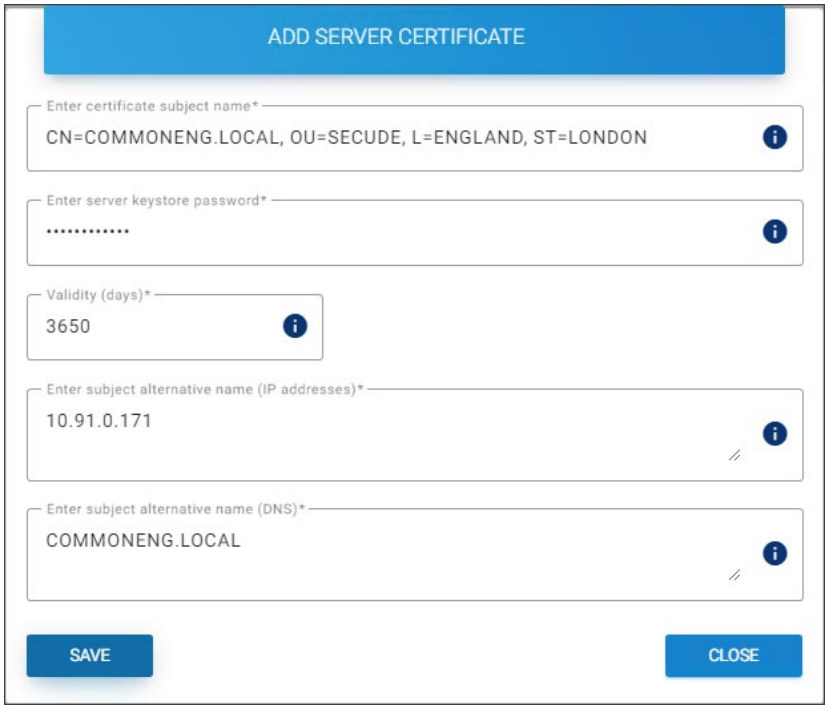
Step 1a. Create a Self-Signed HaloENGINE (Server) Certificate

1. On the left navigation bar, click **System Configuration**, and then on the **Certificate Configuration** tab, click **Configure**.
2. The *Overview* page will appear as shown in the figure below:



Default Certificate Page

3. Click **Server Certificate** and then click **Create Certificate** button.
4. The **Add Server Certificate** page will appear as shown in the figure below:



Creating a server certificate

5. **Enter certificate subject name** – Enter a subject name. For example: `CN=COMMONENG.LOCAL, OU=SECUDE, L=ENGLAND, ST=LONDON`.
6. **Enter server keystore password** – Enter a server Keystore password. For example, `HaloENGINE_1`. Note: Copy and paste are not allowed in this field. Please refer to the section "Keystore password policy".
7. **Validity (days)** – Enter certificate validity in days (1 to 5475). The default value is 3650.

8. **Enter subject alternative name (IP addresses)** – Enter the server IP address. For example, `10.91.0.171`.
9. **Enter subject alternative name (DNS)** – Enter an alternative subject name (FQDN). For example, `COMMONENG.LOCAL`.
10. Click **Save**.

    Results:

    a. You can see a confirmation message after updating the certificate successfully.

    b. A self-signed server certificate (`HaloENGINEServer.cer`) is generated along with two other files (`HaloENGINEServer.csr, serverKeystore.jks`) in `...Tomcat\conf\cert`.

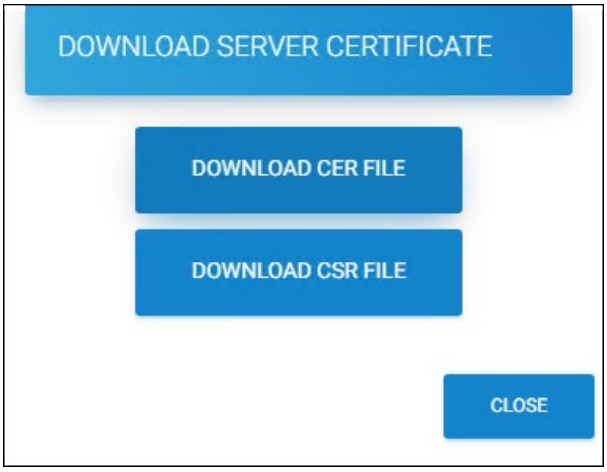
    c. The page will display server certificate information.

    What to do next

    a. In the case of other client systems, refer to Step 4 to create a client certificate.

    b. In the case of the SAP client, the next step is to download the self-signed certificate (`HaloENGINEServer.cer`) and import it into the SAP System.

    c. Click the download icon and on the **Download Server Certificate** dialog, click **Download CER File**. A copy of the self-signed server certificate `HaloENGINEServer.cer` will be downloaded.



Download Server Certificate

11. Click **Close** to close the dialog.

Keystore Password Policy

Before creating the password, make sure to follow the policies listed below:

- The password must be between **6** to **30 characters** long
- The password should not contain a space
- The first letter should be an alphabetic character [**upper** or **lower** case letter]

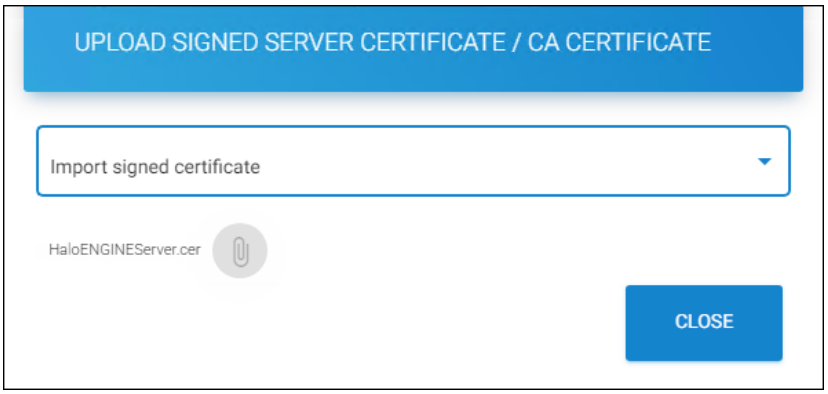
- It must contain at least **1 numerical** character [0-9]
- It must contain at least **1 symbol** [$ _ #]

  For example: **HaloCORE_1**

Step 1b. For a CA-Signed HaloENGINE Certificate

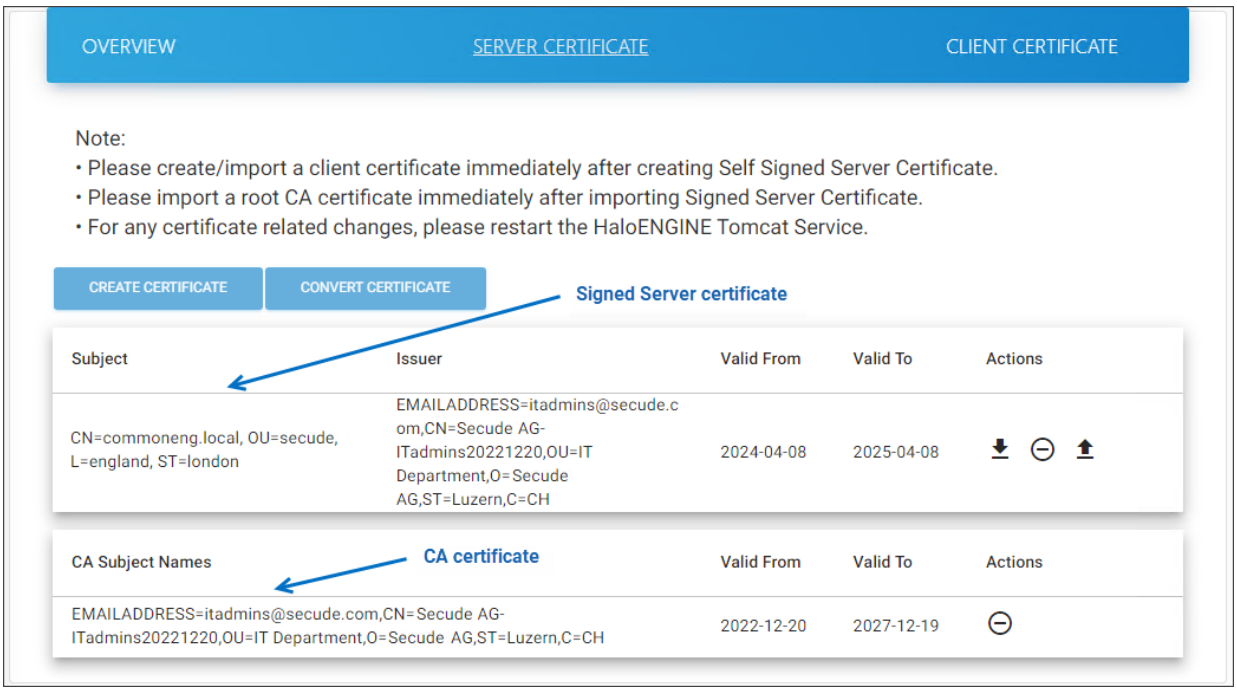
You can convert the self-signed certificate created in Step 1a into a CA-Signed certificate by signing it with your Certificate Authority (CA).

1. Click the download icon and on the **Download Server Certificate** dialog, click **Download CSR File**. A Certificate Signing Request (CSR) `HaloENGINEServer.csr` will be downloaded.
2. Submit the `HaloENGINEServer.csr` file to your Certificate Authority and get the signed certificate as `HaloENGINEServer.cer`.
3. Import the CA - refer to Step 3. Please note that a signed certificate cannot be imported before uploading its corresponding CA.
4. As the certificate (`HaloENGINEServer.cer`) is signed now, you need to import it into the HaloENGINE Tomcat Service.
5. **Import Signed Certificate:**
   a. After importing the CA (in Step 3. Import Intermediate CAs), continue to import the signed certificate.
   b. From the list, choose **Import signed certificate**.
   c. Click on the attachment button and select the signed `HaloENGINEServer.cer` certificate from the **Open** Windows dialog.



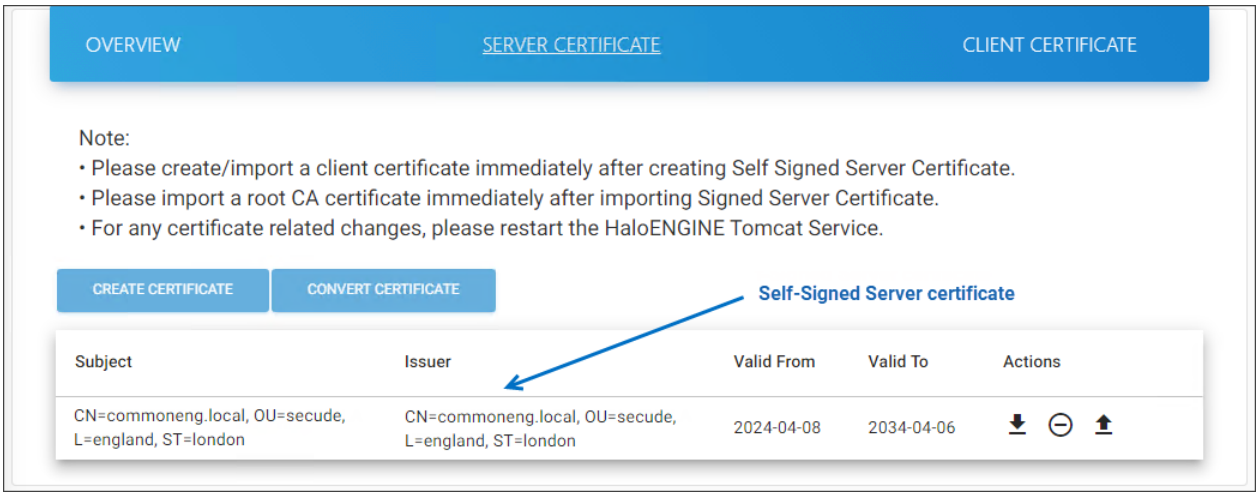
Importing the signed HaloENGINEServer.cer certificate

Results: The name of the certificate will be displayed on the screen, and you will receive a confirmation message after uploading the certificate. To close the dialog, click Close. The Server Certificate page appears as shown in the figure below when you upload your certificate:



Signed Server certificate and Root CA #1

Illustration for the self-signed certificate.



Self-Signed Server certificate #2

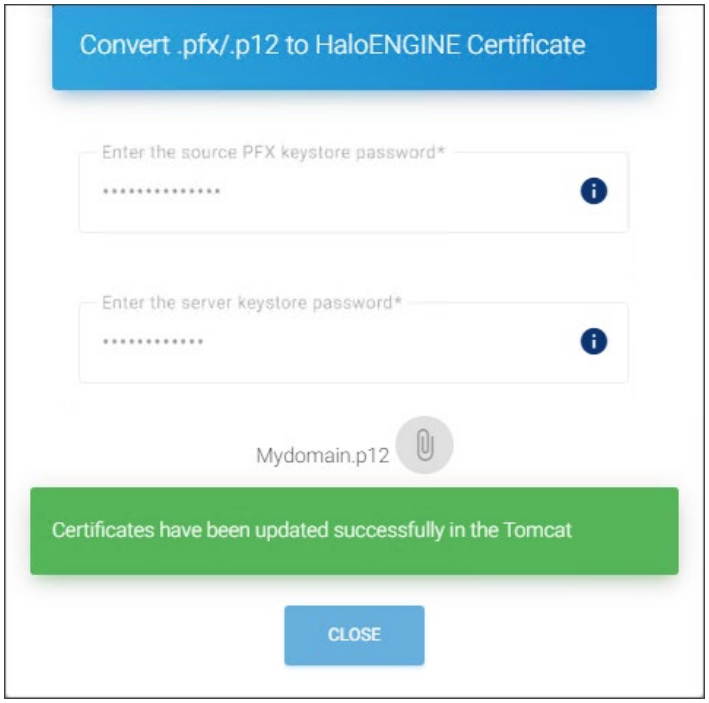
6. **What to do next**: Continue from Step 4.

Step 2. Use Company Own Certificate as Server Certificate (Option 2)

Alternatively, if you already have a certificate for your company, you can use it with the HaloENGINE Admin Portal. However, the company's own certificate must be converted in order to work with HaloENGINE. Conversion is as simple as uploading to the admin portal and downloading it as `HaloENGINEServer.cer`.

To convert the company's own certificate, follow the steps below:

1. On the left navigation bar, click **System Configuration**, and then on the **Certificate Configuration** tab, click **Configure**.
2. Click **Server Certificate** and then click on **Convert Certificate**.
3. The **Convert .pfx/.p12 to HaloENGINE Certificate** dialog will appear.
4. Enter the source password for the PFX/P12 file you want to convert. Note: Copy and paste are not allowed in this field.
5. Enter the server keystore password. Please refer to the section "Keystore password policy".
6. Click on the attachment button and select the PFX/P12 file from the **Open** Windows dialog.



Convert the existing certificate into HaloENGINE certificate

7. The certificate's name is displayed on the page.

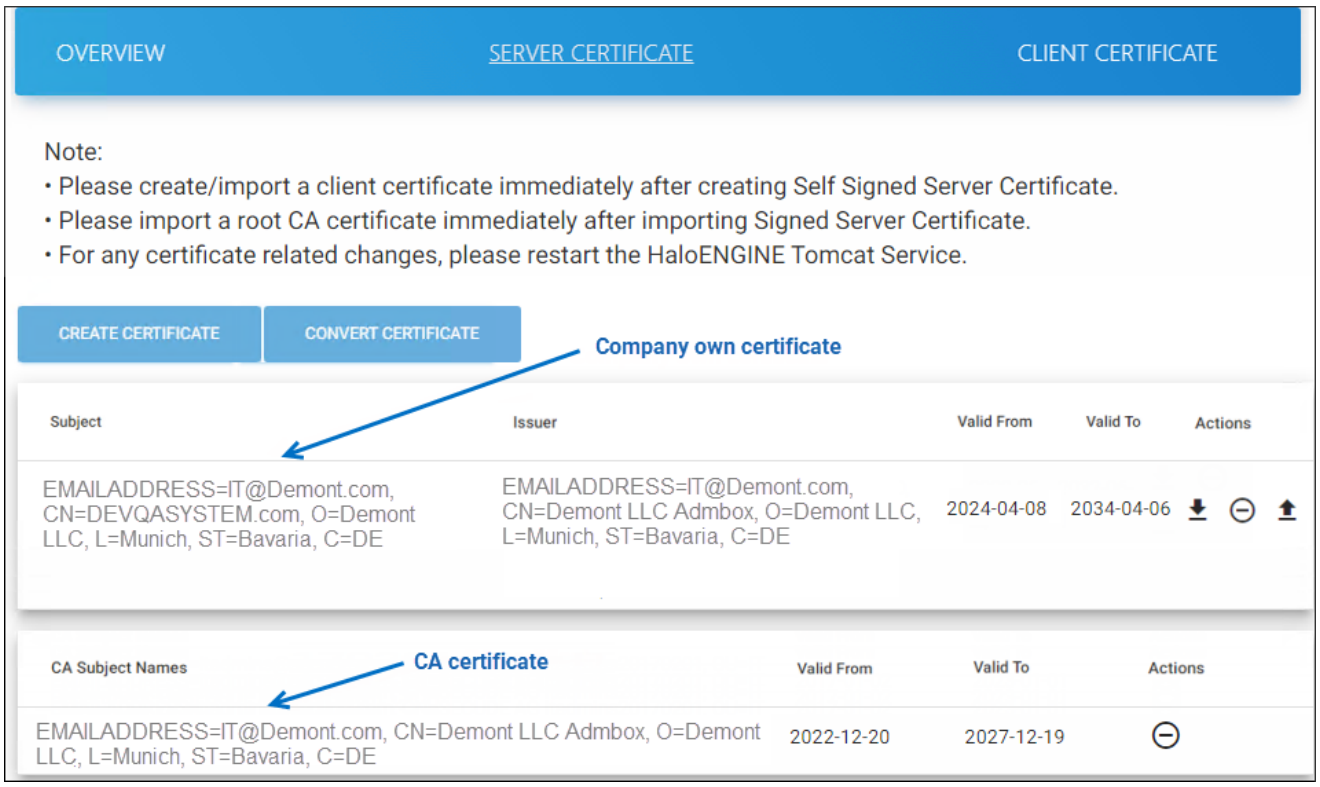
   Results:

   a. You will receive a confirmation message after uploading the certificate.

   b. Click **Close** to close the dialog.

What to do next

1. Import the CA - refer to Step 3. Please note that a signed certificate cannot be imported before uploading its corresponding CA.
2. If your certificate is signed, you need to import it into the HaloENGINE Tomcat Service - refer to Step 1b.
3. After uploading your certificates, the *Server Certificate* page looks as shown in the figure below:



Company own certificate and its Root CA

4. Continue from Step 4.

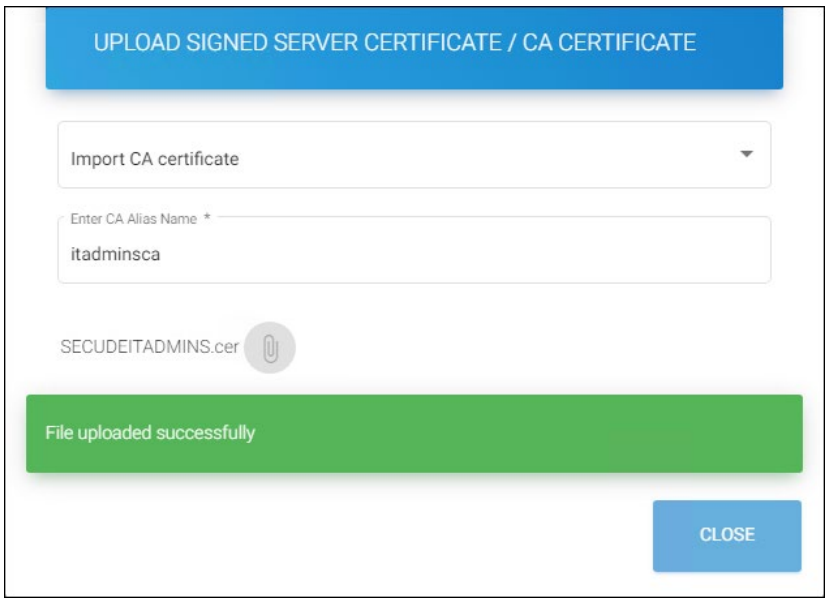
3.5.5.2. Step 3. Import Intermediate CAs

To evaluate a system's overall security level, the HaloENGINE needs a root CA or intermediate CA. You must include all intermediate CAs in the following cases:

1. If an intermediate CA has signed `HaloENGINEServer.cer` - Step 1b.
2. If you use the company's own certificate, which is signed by an intermediate CA - Step 2.
3. If an intermediate CA has signed your client's (SAP/BO) certificate.

To upload the CA Certificate, follow the steps below:

1. Click the upload icon and a pop-up window **Upload Signed Server Certificate / CA Certificate** will appear.
2. From the list, choose **Import CA certificate** and enter an alias name of your choice for Root CA (e.g., `itadminsca`).
3. Click on the attachment button and select your root CA from the **Open** Windows dialog box.



Importing CA certificate

4. The name of the certificate appears on the page.

   Results:

   a. You will receive a confirmation message after uploading the certificate.

   b. Repeat the steps above to add all intermediate CAs.

For SAP client

If you are using a self-signed certificate, you must import the `HaloENGINEServer.cer` certificate into your SAP client machine using STRUST. This ensures that the HaloENGINE and the SAP system are properly connected.

1. Import HaloENGINE Certificate into SAP System - For further details, please refer to the section "Importing the HaloENGINE Certificate into ABAP System" in the HaloCORE Installation Manual.
2. Export and install the SAP system's certificate into HaloENGINE - refer to Step 5.

3.5.5.3. Step 4. Use Client Cert from Admin Portal (Option 1 - For Non-SAP Clients Only)

Similar to how the Server certificate is handled, HaloENGINE provides two ways to handle a client certificate:

1. A self-signed client certificate is generated by the server - see Step 4a.
2. Or use the company's own certificate - refer to Step 5 (Note: For an SAP client, also need to refer to Step 5)

Step 4a. For a Self-Signed HaloENGINE Client Certificate

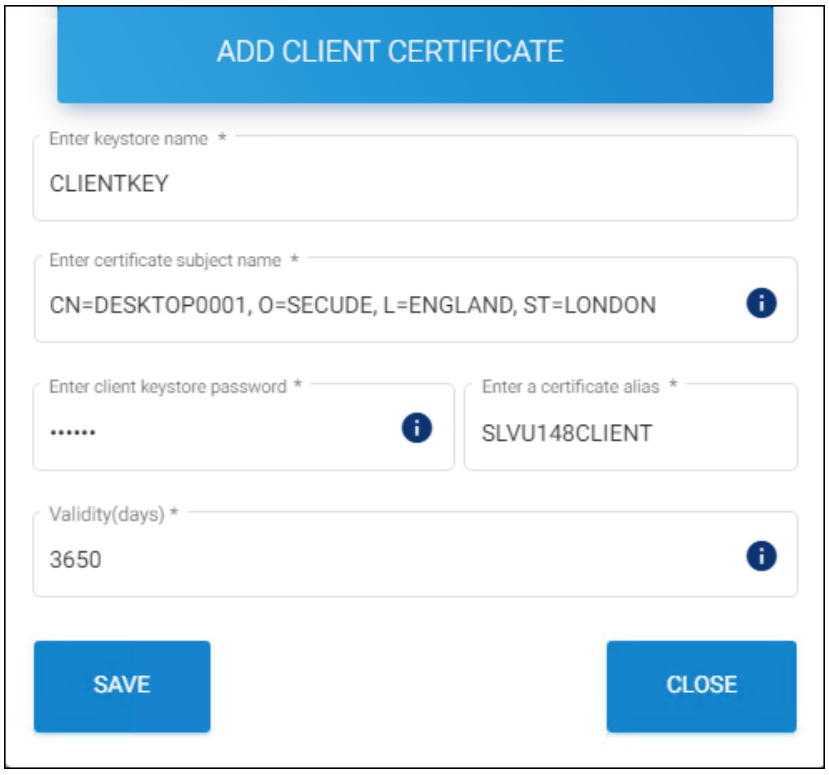
This instruction applies to the clients listed below. Note: Self-signed client certificates can be generated using the HaloENGINE. At the time of creation, it will be added to the client Keystore.

Client systems	Required Keystore format
BO	`.jks`
KPro	`.jks`
Windchill	`.jks`
Teamcenter	`.jks`
Keytech	`.jks`
Autodesk_Vault	`.jks`

Client Keystore

Follow the steps below to create a self-signed client certificate:

1. On the left navigation bar, click **System Configuration**, and then on the **Certificate Configuration** tab, click **Configure**.
2. Click **Client Certificate** and then click **Create Certificate** button.
3. The **Add Client Certificate** page will appear as shown in the figure below:



Creating a client certificate

4. **Enter keystore name** – Enter a Keystore name for the client. For example: `CLIENTKEY`.
5. **Enter certificate subject name** – Enter a subject name. For example: `CN=DESKTOP0001, O=SECUDE, L=ENGLAND, ST=LONDON`. **Enter client keystore password** – Enter a client Keystore password. For

example: `ckpass1#`. Note: Copy and paste are not allowed in this field. Please refer to the section "Keystore password policy".

6. **Enter a certificate alias** – Enter an alias name. For example: `SLVU148CLIENT`.
7. **Validity (days)** – The default period is 3650 days.
8. Click **Save**.

   Results:

   a. You can see a confirmation message after adding the client's certificates successfully.

   b. A self-signed (`CLIENTKEY.cer`) certificate is generated along with two other files (`CLIENTKEY.pfx`, `CLIENTKEY.jks`) in `...Tomcat\conf\cert`. The user-specified Keystore name is used as the filenames.

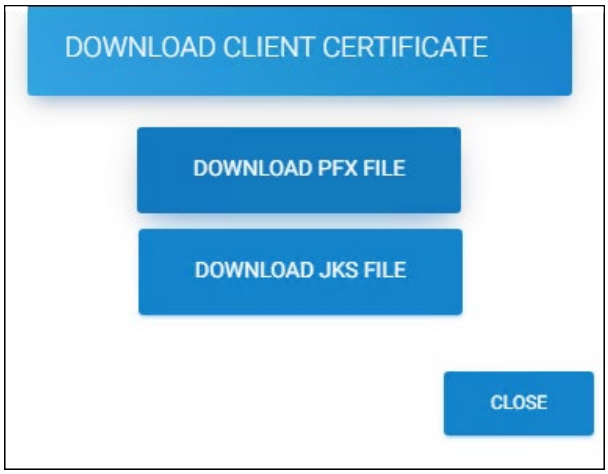
   c. Click **Close** to close the page.

   d. The client certificate is generated and installed into the HaloENGINE Tomcat Service.

What to do next: Download the HaloENGINE Client Certificate.

To establish the connection between the client and server, you need to download this certificate/Keystore and add the client machine

1. Click the download icon, and the **Download Client Certificate** dialog will appear.
2. HaloENGINE client systems such as BO, KPro, Windchill, Autodesk_Vault, and Teamcenter require a JKS Keystore to operate. Hence, click **Download JKS File** to download a copy of the JKS file. As per the above example, a file named `CLIENTKEY.jks` will be downloaded.



Downloading the client certificate

3. Click **Close** to close the page.

3.5.5.4. Step 5. Use Company's Own Certificate as Client Certificate (Option 2)

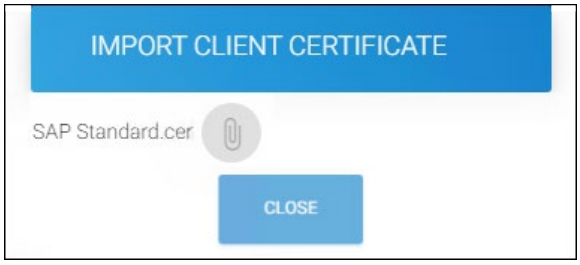
If you want to use your company's certificate, you must add it to the HaloENGINE Tomcat Service. For SAP, choose this option.

Prerequisites:

1. In the case of a SAP client, export the SAP system's certificate (SSL System Client SSL client). Please refer to the section "Exporting the SAP Certificate" in the HaloCORE Installation Manual to learn how to obtain your SAP certificate.
2. In the case of other clients, have client certificates ready in advance.
3. If your client certificate is signed by an intermediate CA, you must upload it as described in section Step 3.

To upload an existing client certificate, follow the steps below:

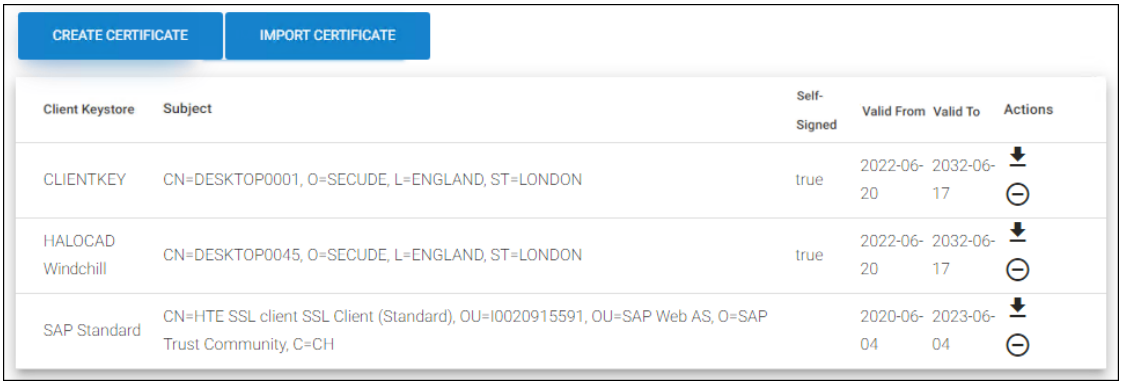
1. Click **Import Certificate**.
2. The **Import Client Certificate** dialog will appear.
3. Click on the attachment button and select the client certificate from the **Open** Windows dialog box. (For example, SAP instance certificate, `SAP Standard.cer`).
4. Perform the same steps to upload other client certificates as well.



Uploading existing client certificates

5. Click **Close** to close the dialog.

Results: After uploading your certificates, the *Client Certificate* page looks as shown in the figure below:



Uploaded client certificates

3.5.5.5. How to Delete the HaloENGINE Client Certificate?

To remove the client certificate, perform the following steps:

1. On the left navigation bar, click **System Configuration**, and then on the **Certificate Configuration** tab, click **Configure**.
2. Click **Client Certificate** in the right corner.
3. Now, select the client certificate and click the delete icon under the **Actions** column.
4. To the question *"Are you sure to delete ?"*, answer **OK**.
5. By clicking **OK**, you agree to delete the client certificate permanently.
   Results: You can see a confirmation message after deleting the certificates successfully.

3.5.5.6. How to Delete the HaloENGINE Certificate?

Please be aware that removing the server certificate will also permanently remove all other certificates (including client and CA certificates). Upon deleting the certificates, the admin portal will not load. To access the admin portal, manually change the protocol to HTTP and the port number to 8383. Additionally, clear browsing data.

CA Certificate(s)

To remove the CA certificate(s), perform the following steps:

1. On the left navigation bar, click **System Configuration**, and then on the **Certificate Configuration** tab, click **Configure**.
2. Click **Server Certificate** in the center.
3. Now, select the CA certificate and click the delete icon under the **Actions** column.
4. To the question *"Are you sure to delete server CA certificate?"*, answer **Yes**.
5. By clicking **Yes**, you agree to delete the *CA* certificate from the Keystore.
   Results: You can see a confirmation message after deleting the certificates successfully.

Server Certificate

To remove the server certificate, follow these instructions:

1. On the left navigation bar, click **System Configuration**, and then on the **Certificate Configuration** tab, click **Configure**.
2. Click **Server Certificate** in the center.
3. Now, select the server certificate and click the delete icon under the **Actions** column.
4. To the question *"Are you sure to delete the HaloENGINE Certificate?"*, answer **OK**.

5. By clicking **OK**, you agree to delete the Server and the Client certificates from the Keystore permanently.

   Results: You can see a confirmation message after deleting the certificates successfully.

Restart the HaloENGINE Tomcat service

Restart the HaloENGINE Tomcat service after making all necessary certificate-related adjustments.

3.5.6. Phase 2. Create Customer IDS (Only for Multi-Customer Mode)

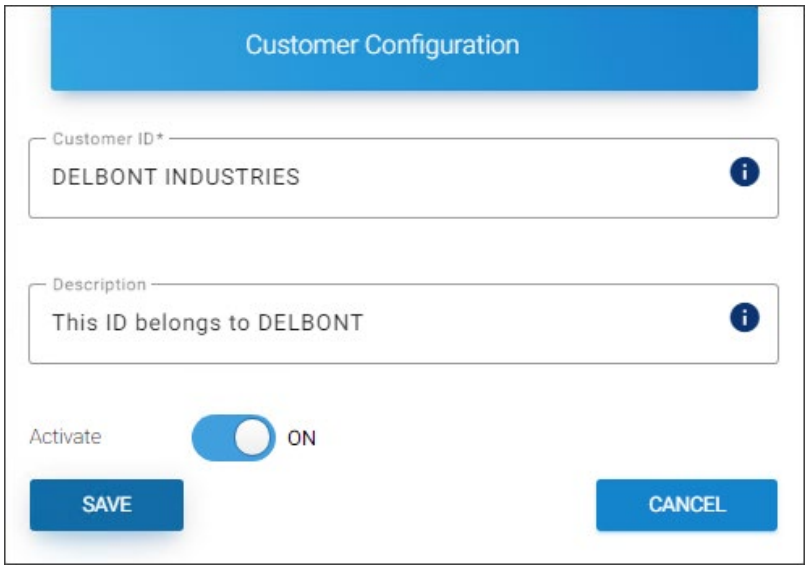
UI Variation in Single Customer and Multi-Customer pages

The HaloENGINE pages will differ slightly depending on the installed mode (single or multi).

1. Single Customer UI: Here, you can notice the default **Customer ID: halo_customer** in breadcrumb navigation.
2. Multi Customer UI: Depending on your customer (ID) creation, the ID gets displayed on top of **Customer Configuration** pages. For example, if you have created a customer as "DELBONT INDUSTRIES", then you can notice **Customer ID: DELBONT INDUSTRIES** in breadcrumb navigation.

To manage your customers, use the Customer Management page. If you have selected Single-Customer mode, proceed with Phase 3. Activate License (First time).

1. On the left navigation bar, click **Customer Configuration**.
2. Click on the plus icon, and the *Customer Configuration* page will appear as shown in the figure below:



Customer ID creation

3. Enter the following details:

a. **Customer ID** – Enter a customer ID.

b. **Description** – Enter a description for it (optional).

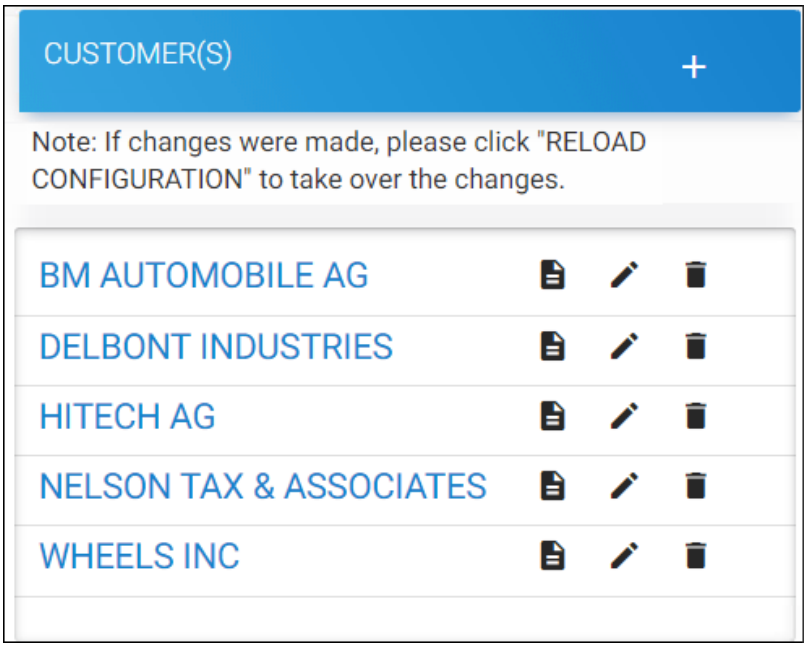
c. **Activate** – The current Customer ID is automatically enabled by default. However, you can deactivate it by clicking the **Activate** slider button.

4. Click **Save**.
5. Repeat the above steps to generate additional customer IDs.
6. The default **Customer ID** for Single Customer mode is `halo_customer`. By using the edit icon, the name can be modified.

   Results:

   a. You will receive a confirmation message after successfully enrolling a customer.

   b. The new customer ID is added to the **Customer IDs** list as shown in the figure below:



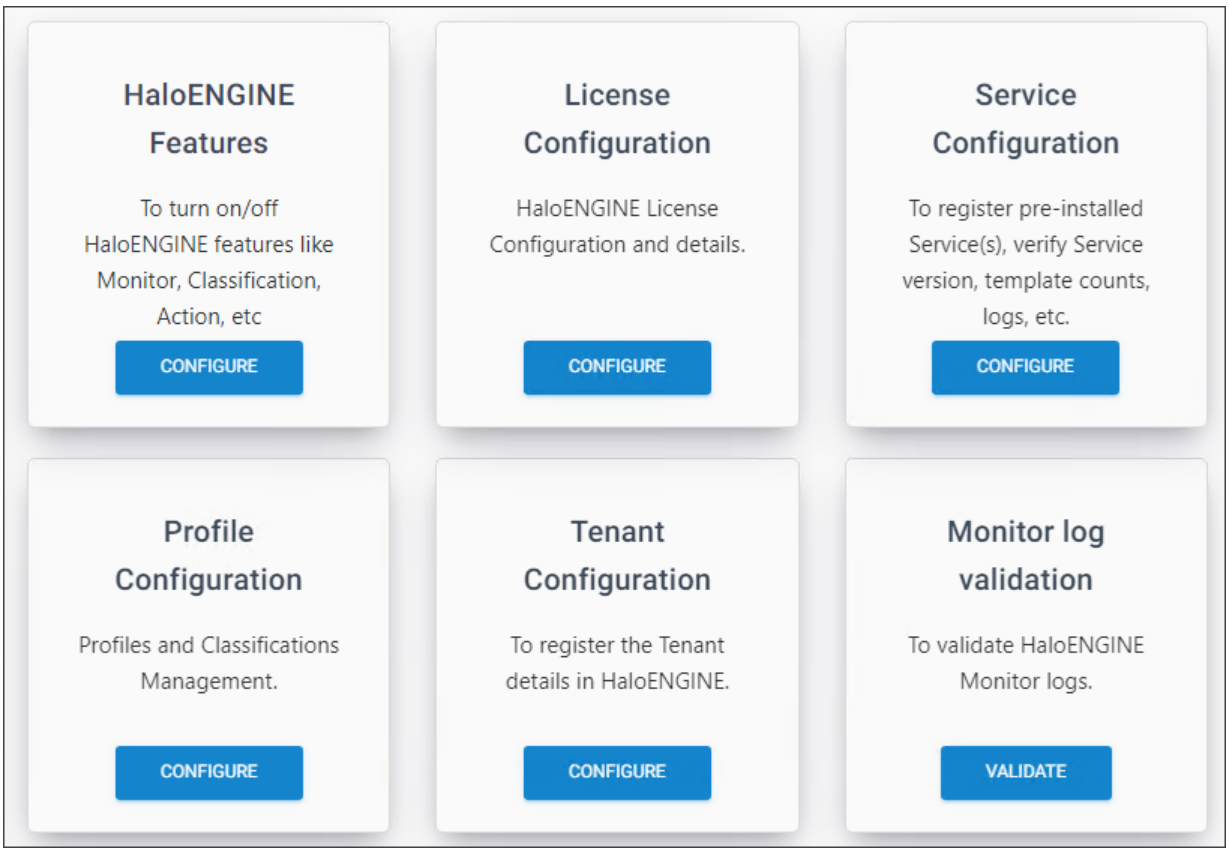
Customer IDs in the list

Related tasks:

1. You can manage the Customer IDs by using the edit/delete icons.
2. You can view customer details by clicking the **Customer Details** icon.

What to do next

1. Select a customer ID from the list and the following page will appear for the specific ID.



Customer-specific configuration

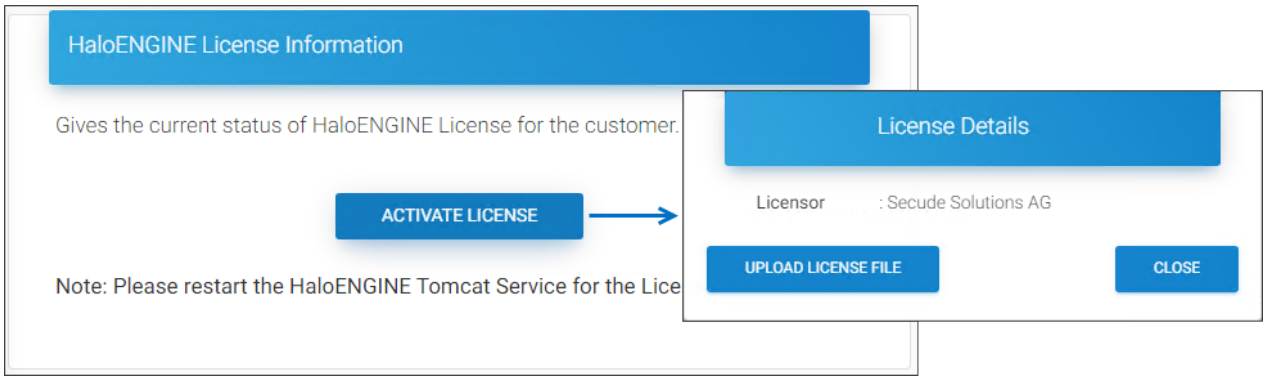
2. To configure the chosen customer ID, click on the tabs. Please see the sections that follow.

3.5.7. Phase 3. Activate License (First time)

Prerequisite: Make sure you have a license file from Secude.

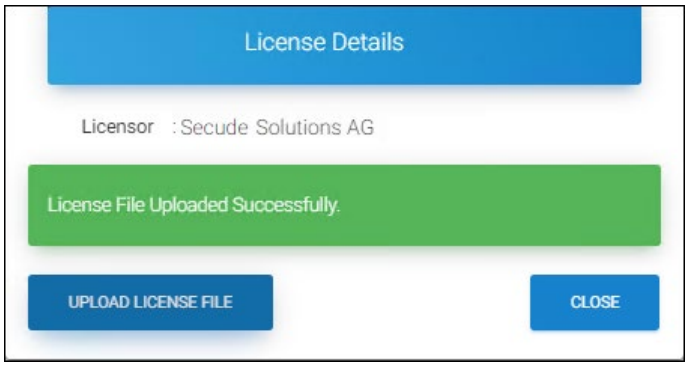
To activate the license, follow the steps outlined below:

1. On the left navigation bar, click **Customer Configuration**, and then from the **Customers** list, select one of them.
2. On the **License Configuration** tab, click **Configure**.
3. The *HaloENGINE License Information* page will appear as shown in the figure below:



License activation page #1

4. Click **Activate License** and then on the *License Details* page, click **Upload License File**.



License activation page #2

5. Select the `license.lic` file from the **Open** Windows dialog.

   Results:

   a. You will get a confirmation message after the file upload is successful.

   b. Click **Close** to close the dialog.

   c. Restart the HaloENGINE Tomcat service for the license file change to take effect.

   d. In Multi-Customer mode, repeat the above steps for additional customer IDs.

What to do next: Login to the admin portal and follow the steps below to check the license details or renew it.

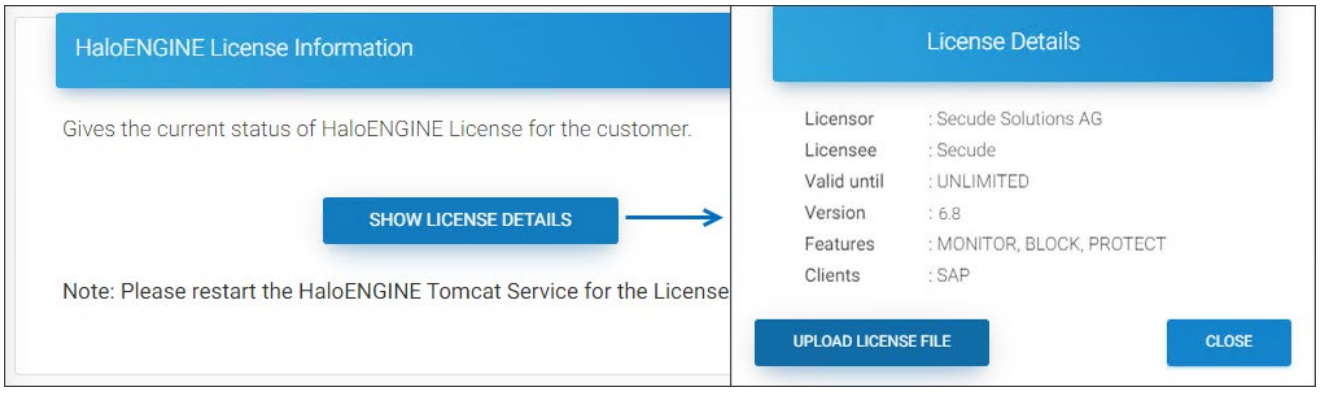
Check License Details / Renew License

This page is also useful for the following reasons:

1. To verify license information such as validity and activated features.
2. The current license has expired; in this case, you must renew it from Secude.

To check the license details:

1. Click the **Show License Details** button. Note: The **Show License Details** button will be enabled only after the first activation.



Renew/check license dialog

Results: The license details will be displayed.

2. Click **Close** to close the dialog.

To renew the license:

Click **Upload License File** and select the new `license.lic` file from the **Open** Windows dialog.

Results:

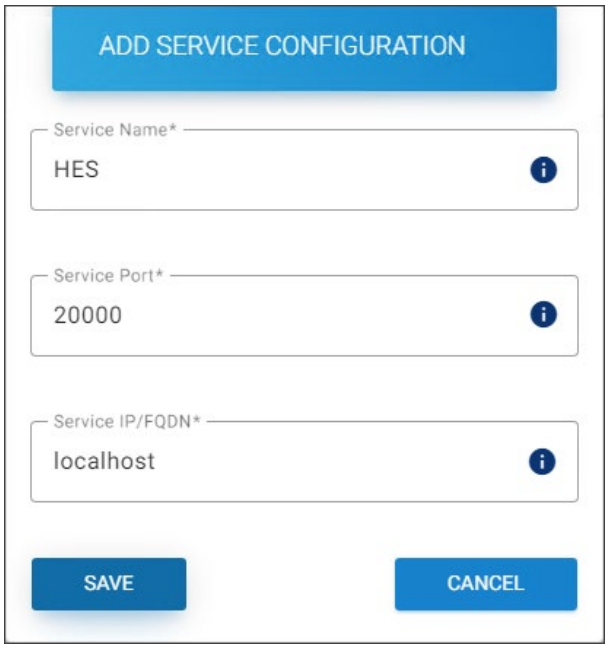
1. You will get a confirmation message after the file upload is successful.
2. Click **Close** to close the dialog.
3. Restart the HaloENGINE Tomcat service for the license file change to take effect.

3.5.8. Phase 4. Register HaloENGINE Services

Prerequisite: Make sure that the HaloENGINE Service is installed. The default name of the service is “HES”. Note: To add more services, use the Administration Manager (`hesadm.exe`) tool. For more details, please refer to the section "Configuration of HaloENGINE Service".

Follow the below steps to register HaloENGINE Service(s) in the admin portal.

1. On the left navigation bar, click **Customer Configuration**, and then from the **Customers** list, select one of them.
2. On the **Service Configuration** tab, click **Configure**.
3. Click on the plus icon, and the *Add Service Configuration* page will appear as shown in the figure below:



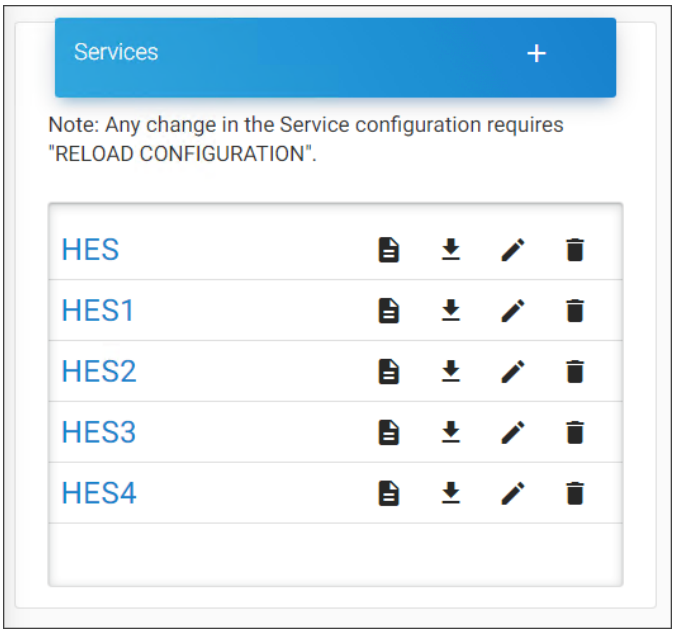
HaloENGINE Service details

4. **Service Name** – Enter a name for the service.

5. **Service Port** – Enter the service port number.
6. **Service IP/FQDN** – Enter `localhost` or `127.0.0.1`.
7. Click **Save**.

   Results:

   a. You will receive a confirmation message after successfully registering the service.



Service Configuration

   b. Reload the HaloENGINE Admin portal after registering a service.

   c. You can now see the registered service listed on the **Service Map** page.

   d. The following error messages could appear: If the wrong port number was entered; if you are trying to register a service that does not exist; or if you are trying to register a service that is already registered with another customer.

Related tasks

1. Using the appropriate icons, you can also edit or delete a service or view service details.
2. Repeat the above steps to create multiple services.
3. To go back to the previous page, use the breadcrumb navigation.

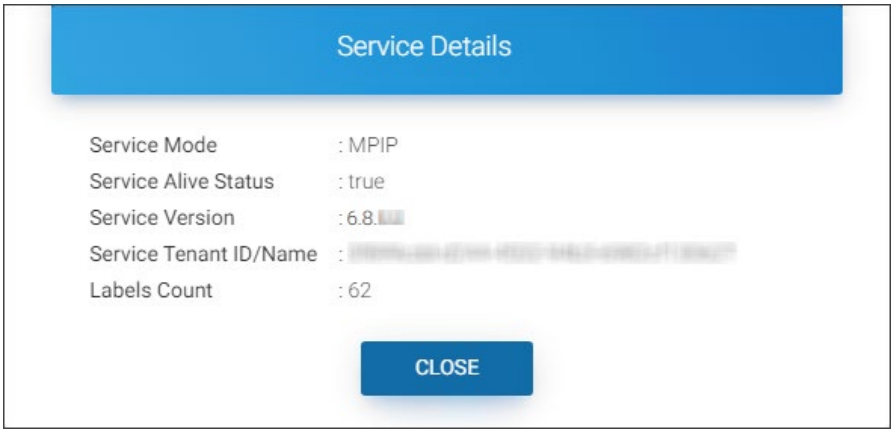
3.5.8.1. Check the Status of the HaloENGINE Service

Follow the steps below to check the status of a service.

1. Select the profile as you wish.
2. Click on the registered service.

Results:

a. The status of the selected service will be displayed as shown in the figure below:

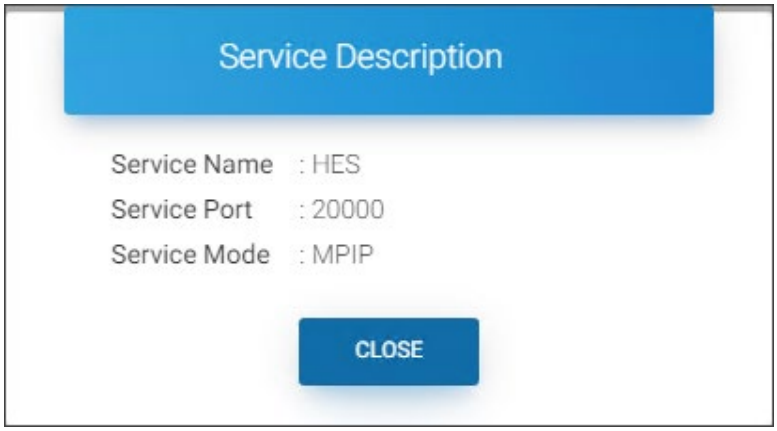


HaloENGINE Service Status

b. Click **Close** to close the dialog.

Related tasks

1. To view the service description, click the **Service Description** icon.
2. The description will appear as shown in the figure below:



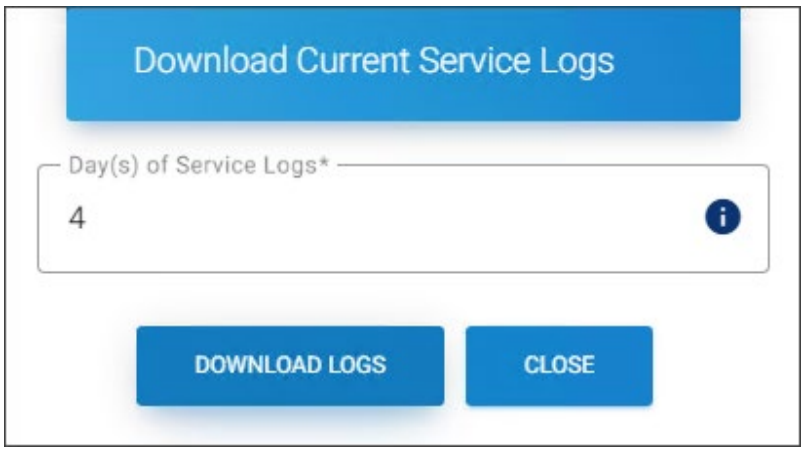
Service Description

3. Click **Close** to close the dialog.

3.5.8.2. Download the HaloENGINE Service Logs

Follow the procedures below to retrieve the service logs.

1. Select a registered service and then click the **Download Service Logs** icon.
2. The **Download Current Service Logs** dialog will appear as shown in the figure below:



Download Service Logs

3. Enter the number of days (minimum 1 day and maximum 90 days) and then click **Download Logs**.
4. Make sure that the entered value does not exceed the “log purge” set in the HaloENGINE Service.

   Results: A zip file named in the registered service will be downloaded to the default download location. For example, `HES.zip` file.

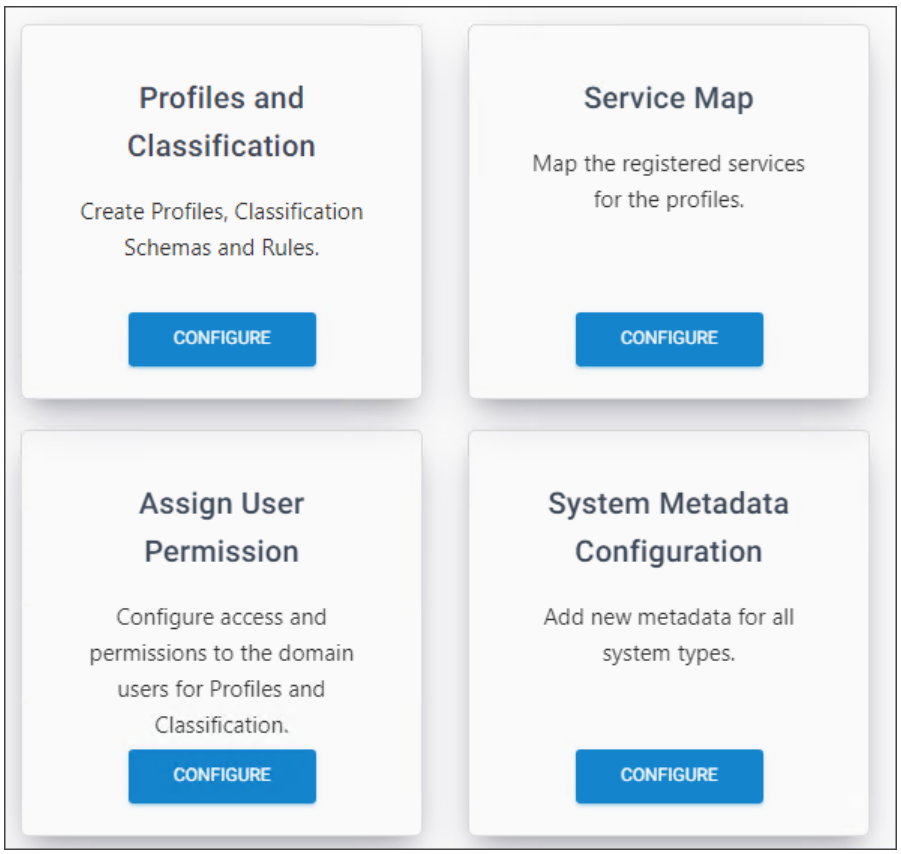
3.5.9. Phase 5. Configure Profiles and Classification

A profile is a repository for all details relating to classification settings.

Prerequisite: Make sure to register the HaloENGINE Services as mentioned in the section "Phase 4. Register HaloENGINE Services". Note: Blocking does not require HaloENGINE Service Registration.

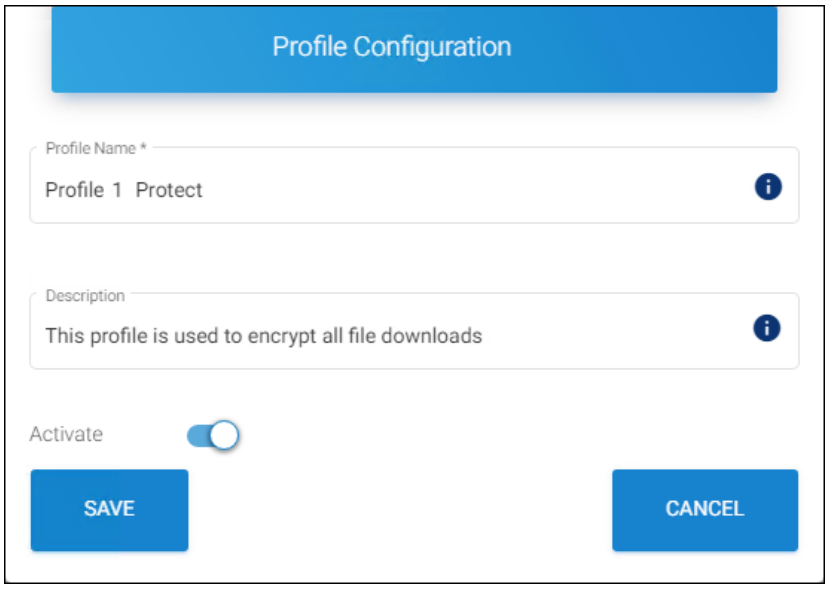
Follow the below procedure to configure the Profile:

1. On the left navigation bar, click **Customer Configuration** and then select a customer ID from the list. On the **Profile Configuration** tab, click **Configure**. The following page will appear, as shown in the figure below:



Profile Configuration page #1

2. On the **Profiles and Classification** tab, click **Configure**.
3. Click the plus icon on the *Classification Profiles* page and then enter the following details:



Profile Configuration page #2

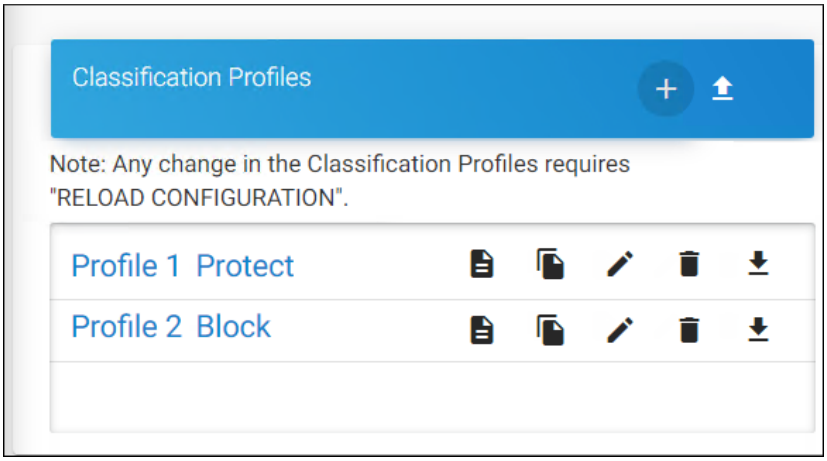
4. **Profile Name** – Enter a name for the new profile. Note: A profile name cannot contain any of the following characters "< >: " / \ |? * ` ~" and can contain "- _"
5. **Description** – Enter a description for the new profile (optional).

6. **Activate** – The current profile is automatically enabled by default. However, you can deactivate it by clicking the **Activate** slider button.
7. Click **Save**.
8. Repeat the above steps to create multiple profiles.

   Results:

   a. You will receive a confirmation message after successfully saving the profile.

   b. The new profile is added to the **Classification Profiles** list.



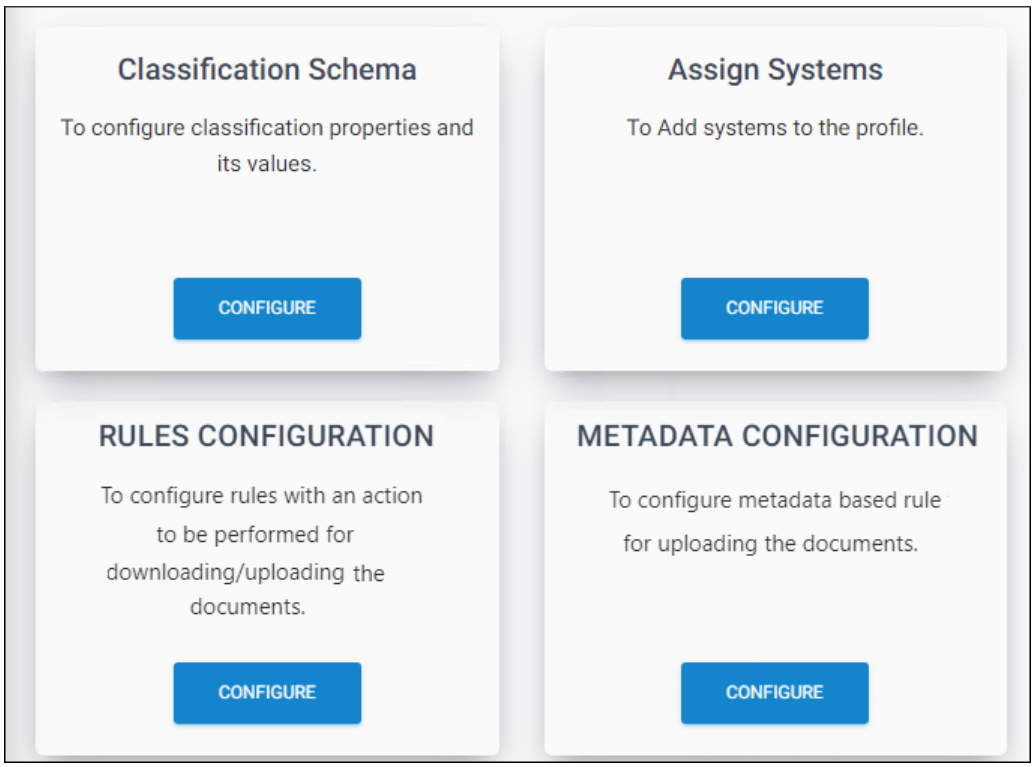
Profile list

Related tasks

1. You can manage the Classification Profiles by using the copy, edit, delete, download, and import icons.
2. If you want to view the profile details, click the **Profile Details** icon.

What to do next:

1. Select a classification profile from the displayed list. The *Classification Configuration* page will appear as shown in the figure below:



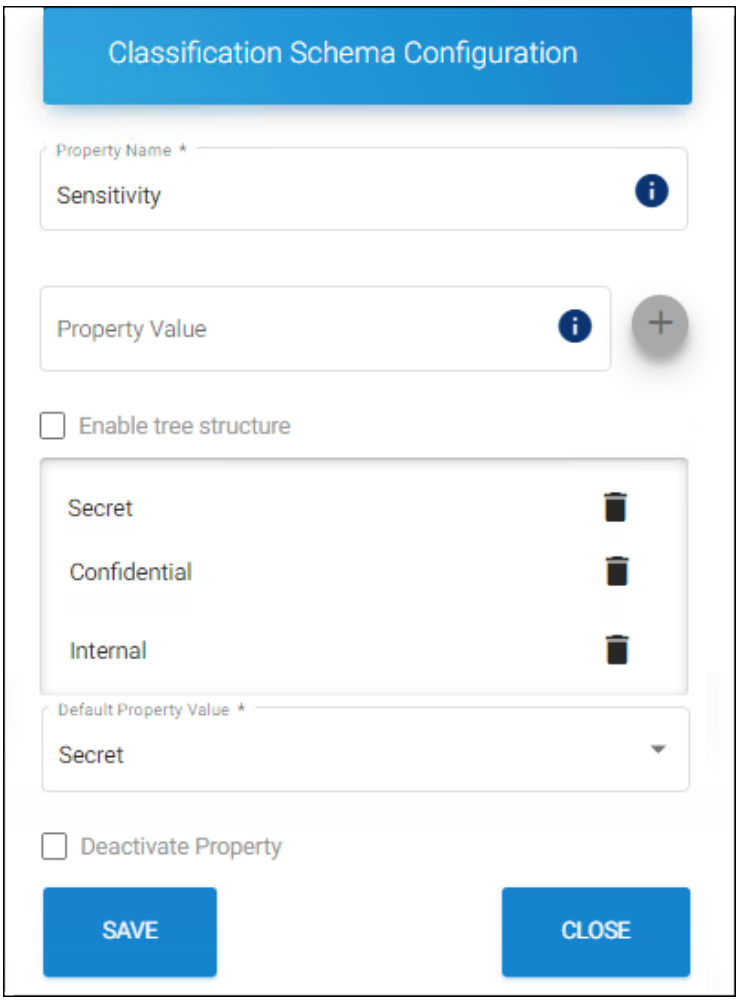
Classification Configuration

2. Refer to the following sections to create a classification schema, rules (download and upload), configure metadata, and assign systems for each profile.

3.5.9.1. Create Classification Schema

Classification Schema contains properties and their values.

1. On the **Classification Schema** tab, click **Configure**.
2. Click on the plus icon and enter the following details:
   a. **Property Name** – Enter a name for the new property (maximum 20 characters and case sensitive). For example, sensitivity.
   b. **Property Value** – Enter a value for the property (maximum 20 characters and case sensitive) and click the plus icon on the right. The value is added to the list. For example, Secret, Confidential, and Internal.



Classification Schema Configuration

3. The first entry (e.g., Secret) will be taken as the default value, but you can modify it using the **Default** dropdown menu. The words `default`, `group`, `multiple`, `if`, `tree`, `hierarchy`, and `return` are reserved keywords that are used for internal processes. Therefore, it should not be used as a **Property Name** or **Property Value**. Using the keyword will result in a compile-time error.
4. Add as many values as you wish to add.
5. Click **Save**.

   Results:

   a. You will receive a confirmation message after successfully saving the Classification Schema.

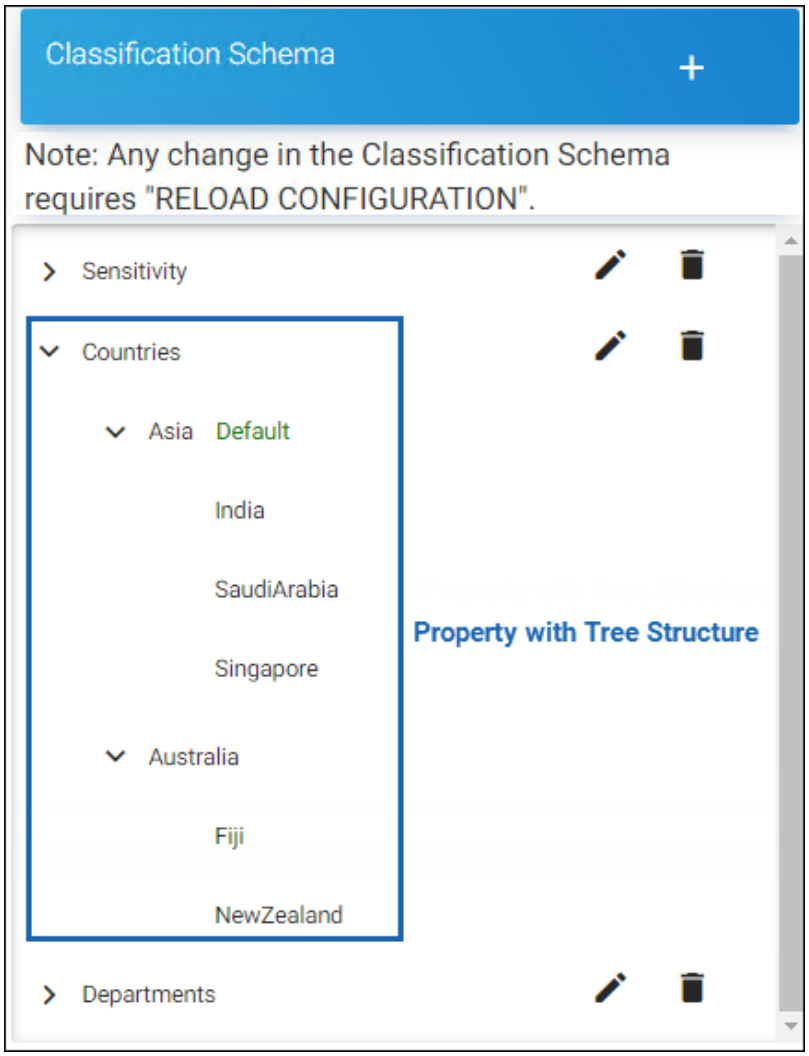
   b. The property name and its values get added as a node.

   c. Similarly, you can add many nodes by using the plus icon.

6. **Enable tree structure**: To have a tree structure view of information, where each item can have several multiple children, select the Property Value (e.g., Asia) and enter a value in the property value field (e.g., India), and then select **Enable tree structure** check box and add the child node using the

plus icon. In this illustration, the **Property Value** “Asia” contains three child nodes - India, Saudi Arabia, and Singapore.

7. Click **Close** to close the page.



Classification Schema list

Related tasks

1. By default, the current Property will be activated. You can deactivate it by using the **Deactivate Property** check box.
2. You can manage the classification profiles by using the edit and delete icons.

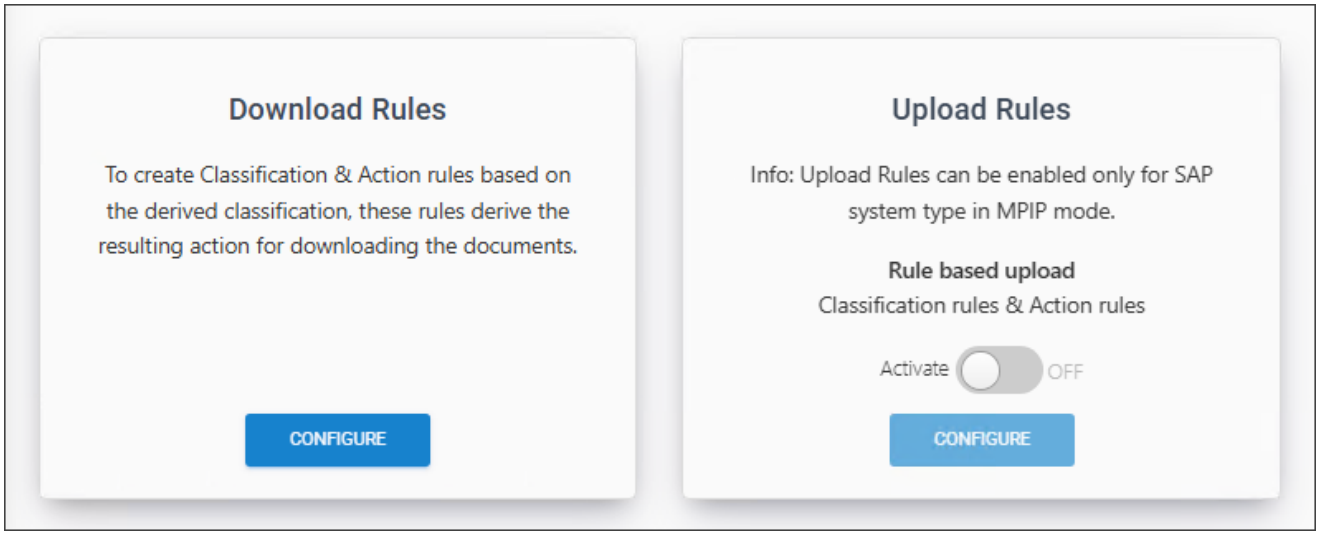
3.5.9.2. Create Download Classification Rules

Download rules define classification rules based on metadata types and Pre-Expression and action rules decide whether to block/protect/notify/exclude when a file is downloaded.

3.5.9.2.1. Personally Identifiable Information (Pre-Expression)

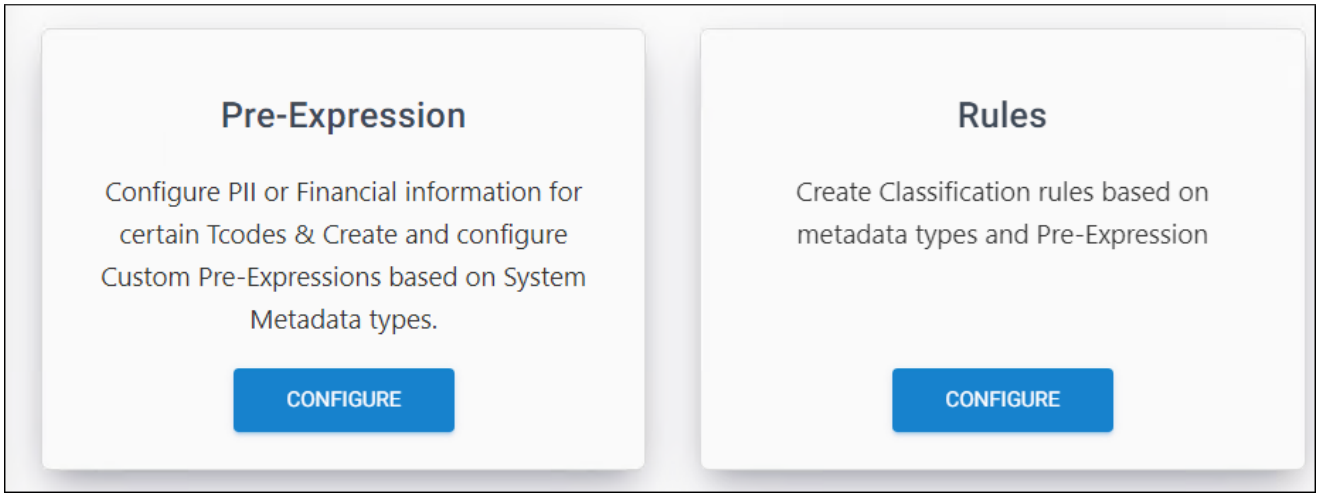
HaloENGINE provides a predefined list of pre-expression for Personally Identifiable Information (PII) contained in tcodes. Personally identifiable information is only applicable to the SAP system type.

1. On the **Rules Configuration** tab, click **Configure** and the following page will appear as shown in the figure below:



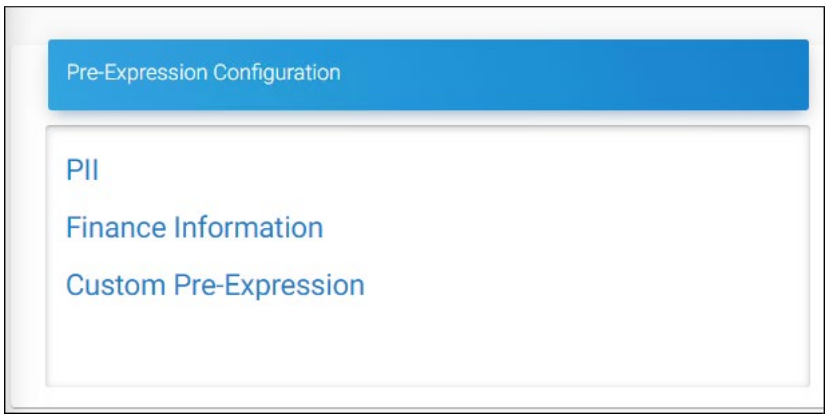
Rules Configuration

2. On the **Download Rules** tab, click **Configure** and then on the **Classification Rules** tab, click **Configure** and the following page will appear as shown in the figure below:



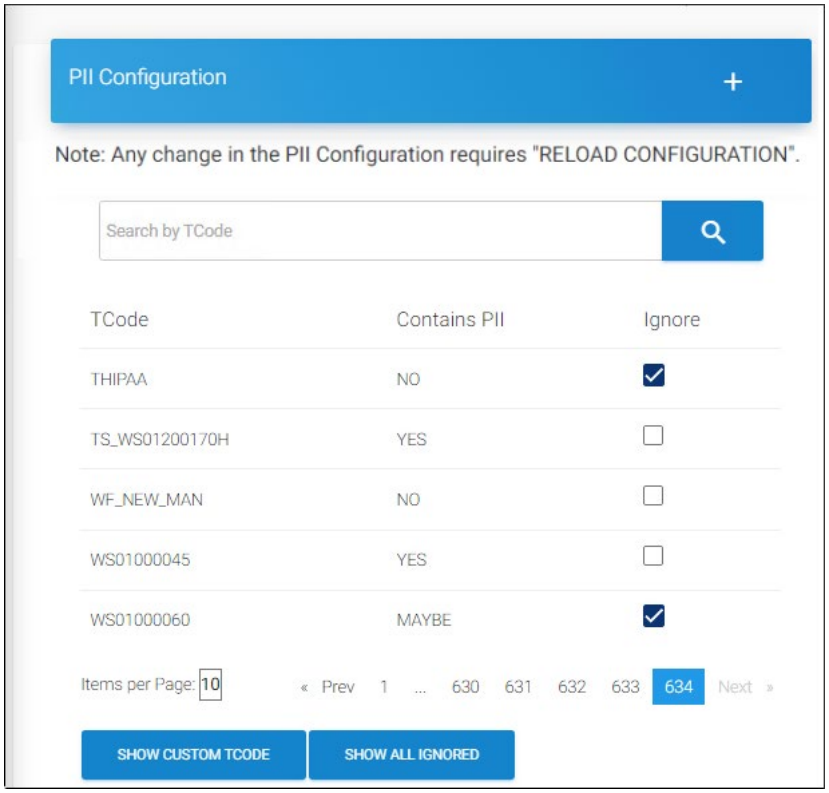
Classification rules

3. On the **Pre-Expression** tab, click **Configure** and the following *Pre-Expression Configuration* page will appear as shown in the figure below:



Pre-Expression Configuration

4. Click **PII** from the list. The *PII Configuration* page will appear as shown in the figure below:



PII configuration

5. The value of the tcodes are indicated by the following options:
   - YES = it contains PII
   - NO = it does not contain PII
   - MAYBE = It might contain PII
6. If you want to ignore a tcode, select **Ignore** check box against it.
7. These values of the tcode have no relationship with the Ignore check box.
8. To find a tcode, enter the name in the **Search by TCode** text box.

   Results: The search results will be shown automatically.

To add custom tcode(s)

1. Click on the plus icon. The **Add Custom PII** dialog will appear.
2. Enter your custom tcode and choose one of the following values from the list (**YES**/**NO**/**MAYBE**).
3. Click **Save**.

   Results: You will receive a confirmation message on adding the tcode.

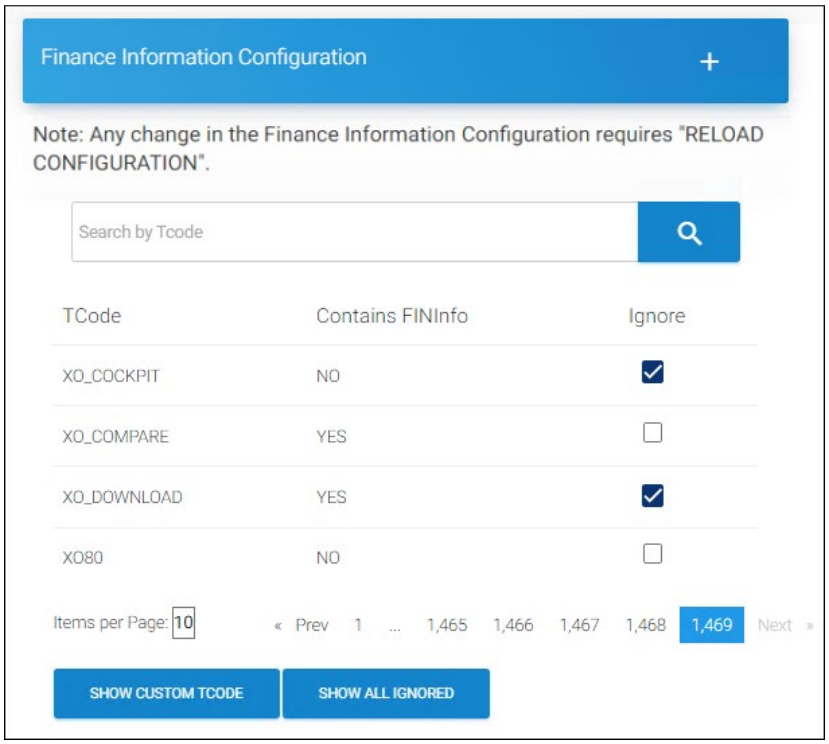
Related tasks

1. To view the list of custom tcode(s) added, click **Show Custom Tcode**.
2. If you wish to remove the tcode(s) from the list, click the **Delete** icon.
3. To view only ignored tcode(s), click **Show All Ignored**.
4. To view all (including ignored), click **Show All**.

3.5.9.2.2. Finance Information (Pre-Expression)

HaloENGINE Server provides a predefined list of pre-expression for Finance Information contained in tcodes. Finance Information is only applicable to the SAP system type.

1. On the **Pre-Expression Configuration** page, click **Finance Information**.
2. The *Finance Information Configuration* page will appear as shown in the figure below:



Finance configuration

3. The value of the tcodes are indicated by the following options:
   - YES = it contains finance information

- NO = it does not contain financial information
- MAYBE = It might contain financial information

4. If you want to ignore a tcode, select **Ignore** check box against it.
5. These values of the tcode have no relationship with the Ignore check box.
6. To find a tcode, enter the name in the **Search by TCode** text box.

   Results: The search results will be shown automatically.

To add custom tcode(s)

1. Click on the plus icon. The **Add Custom Finance Info** dialog will appear.
2. Enter your custom tcode and choose one of the following values from the list (**YES**/**NO**/**MAYBE**).
3. Click **Save**.

   Results: You will receive a confirmation message on adding the tcode.

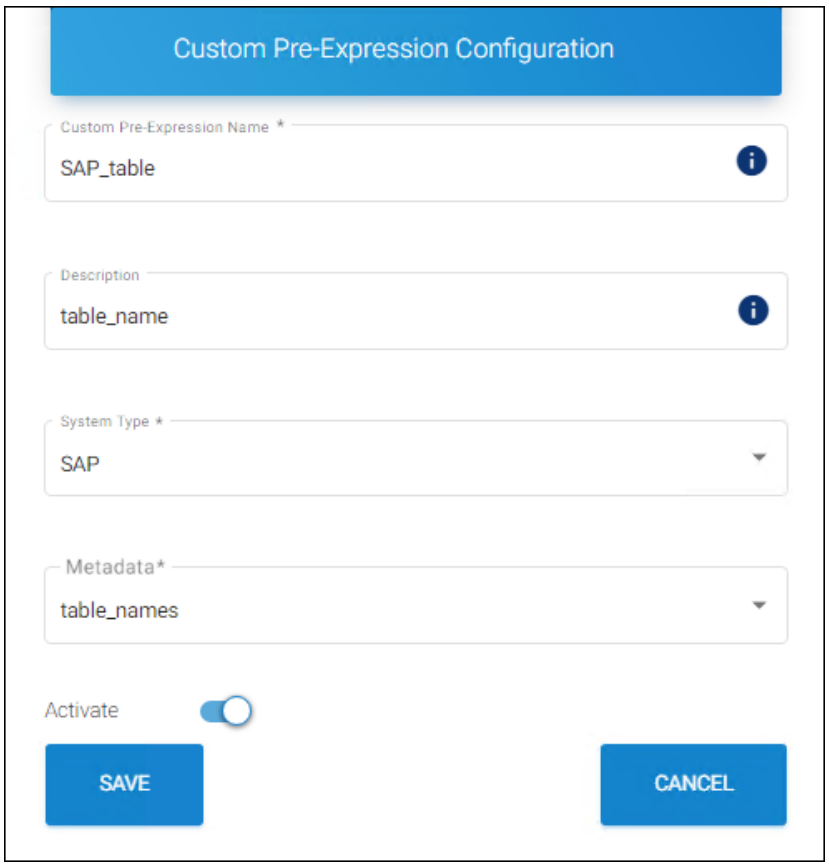
Related tasks

1. To view the list of custom tcode(s) added, click **Show Custom Tcode**.
2. If you wish to remove the tcode(s) from the list, click **Delete icon**.
3. To view only ignored tcode(s), click **Show All Ignored**.
4. To view all (including ignored), click **Show All**.

3.5.9.2.3. Custom Pre-Expression

This page allows you to create custom pre-expressions depending on the system types for which you have been licensed. This is available for all systems, including BO, SAP, Windchill, Teamcenter, Keytech, Autodesk_Vault, SOLIDWORKS_PDM, and HaloENGINE_API.

1. On the **Pre-Expression Configuration** page, click **Custom Pre-Expression**.
2. Click on the plus icon on the *Custom Pre-Expression* page and enter the following details:



Custom Pre-Expression #1

3. **Custom Pre-Expression Name** – Enter a name for the new custom pre-expression entry. Note: only '**alphabet**', '**numbers**', '**_**' and '**-**' characters are supported.
4. **Description** – Enter a description of the new custom pre-expression (optional).
5. **System Type** – HaloENGINE supports the following system types: BO, SAP, Windchill, Teamcenter, Keytech, Autodesk_Vault, SOLIDWORKS_PDM, and HaloENGINE_API. Based on your license, select your system type.
6. **Metadata** – Select a metadata from the list.
7. **Activate** – The current Custom Pre-Expression is automatically enabled by default. However, you can deactivate it by clicking the **Activate** slider button.
8. Click **Save**.

   Results:

   a. You will receive a confirmation message after adding the Custom Pre-Expression.

   b. The new custom pre-expression is added to the list.

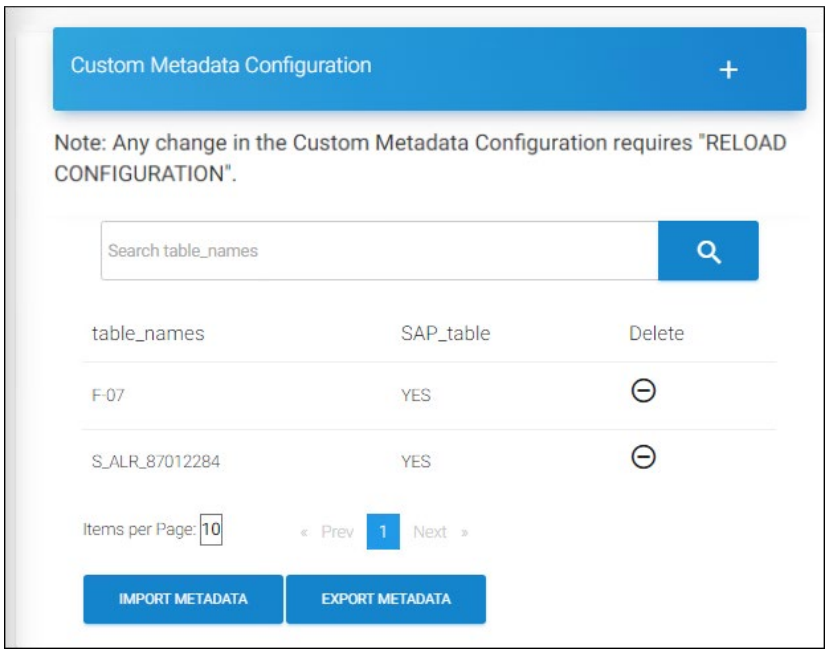
Reference Manuals: For more information about metadata description, please refer to the relevant HaloCAD PLM/PDM Installation Manual.

1. SAP – HaloCORE Installation Manual
2. Autodesk Vault – HaloCAD for Autodesk Vault Installation Manual

3. Teamcenter – HaloCAD for Teamcenter Installation Manual
4. Windchill – HaloCAD for Windchill Installation Manual
5. SOLIDWORKS PDM – HaloCAD for SOLIDWORKS PDM Installation Manual
6. Keytech – HaloCAD for Keytech Installation Manual
7. BO – HaloCORE BO Installation Manual
8. HaloENGINE API – There is no built-in metadata for REST SDK, so Custom metadata can be used to generate new metadata for the HaloENGINE API system type. Please refer to the section "Custom Metadata".

To add custom metadata configuration

1. Now, select a custom pre-expression from the list and the *Custom Metadata Configuration* page will appear, as shown in the figure below:
2. For illustration, a new custom pre-expression "F-07" is added to the list.



Custom Pre-Expression #2

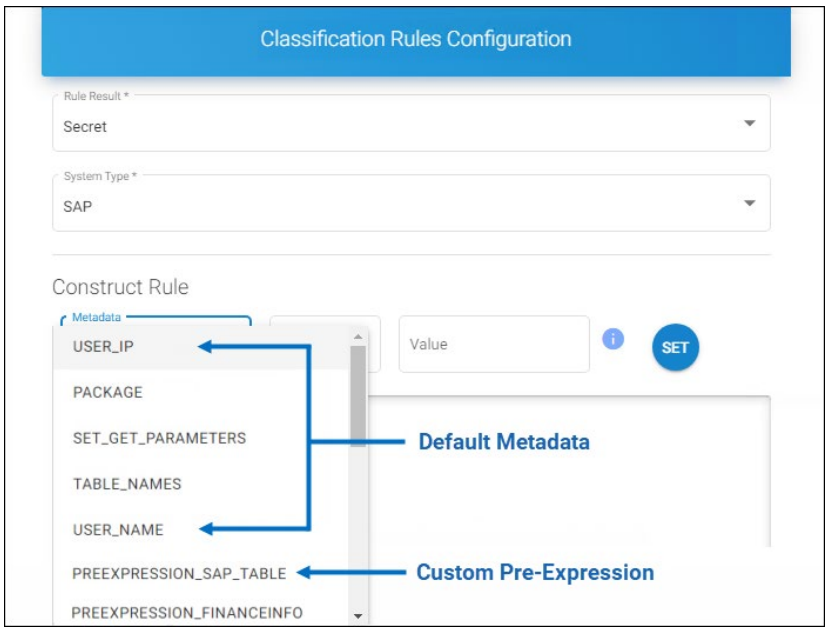
3. Click on the plus icon. The **Add Custom Metadata Values** dialog will appear.
4. Enter a value and select any one of the following options:
   a. YES = it contains specified metadata information
   b. NO = it does not contain the specified metadata information
   c. Click **Save**.

Results:

a. You will receive a confirmation message on saving the Custom Metadata.
b. The new metadata value is added to the list.

Related tasks

1. To find a metadata value, enter the name in the **Search Metadata** text box. The search results will be shown.
2. If you want to remove custom metadata from the list, click the **Delete** icon against the metadata.
3. **To Import Custom Metadata:** If you wish to add your own metadata, click **Import Metadata.**
   The **Import Custom Metadata** dialog will appear. Click on the button and select the metadata file (`.csv, xls, .xlsx`) from the **Open** Windows dialog.
4. **To Export Custom Metadata:** If you wish to export the existing metadata, click **Export Metadata**. An Excel file will be downloaded. The new custom pre-expression is displayed and available for user selection in the **Classification Rule UI** as metadata as shown in the below example:



Example for Custom Pre-Expression #3

5. You can manage the Custom Pre-Expressions by using the edit or delete icons.

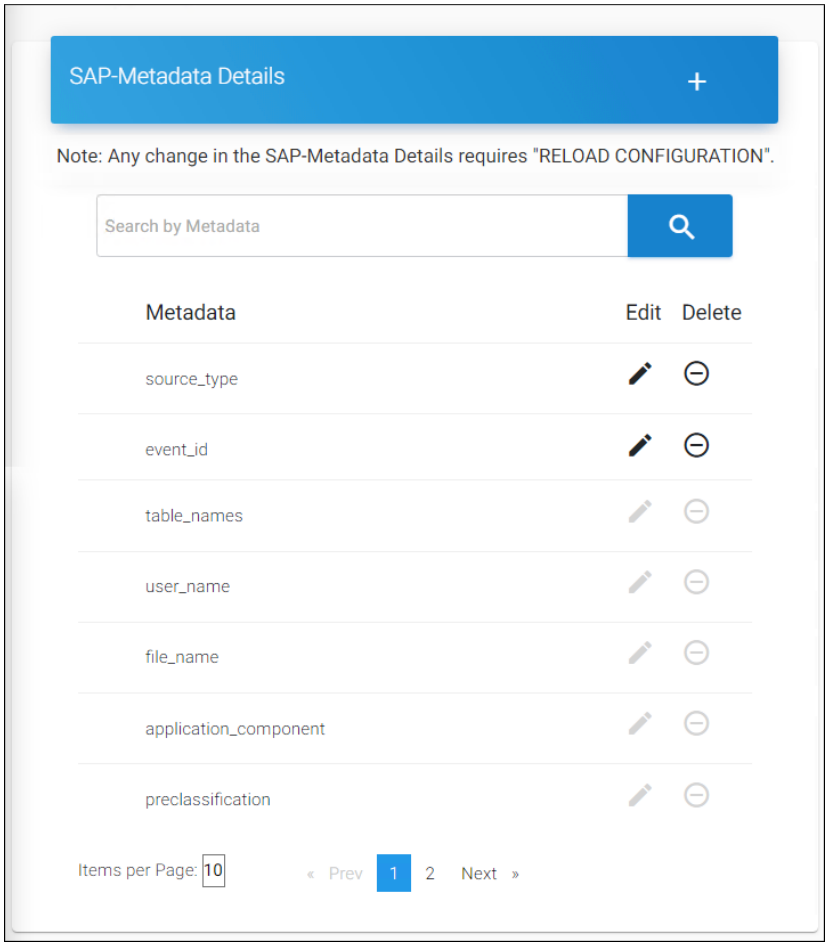
3.5.9.2.4. Custom Metadata

For data classification and secure file downloads, the HaloENGINE admin portal uses the default metadata. However, depending on the needs of each organization, the admin portal allows them to add their own metadata. Note: Metadata can be configured for PLM clients who do not want schema or rule-based decryption. For more information, refer to the section "Metadata Configuration".

Follow the below procedure to create custom metadata for System types:

1. On the left navigation bar, click **Customer Configuration** and then select a customer ID from the list.
2. On the **Profile Configuration** tab, click **Configure** and then on the **System Metadata Configuration** tab, click **Configure**.

3. Click on the System Type (for example, SAP), and the *SAP-Metadata Details* page will appear as shown in the figure below:



Metadata details page

4. Click on the plus icon. The **Add Custom Metadata** dialog will appear.
5. Enter a name and click **Save**.

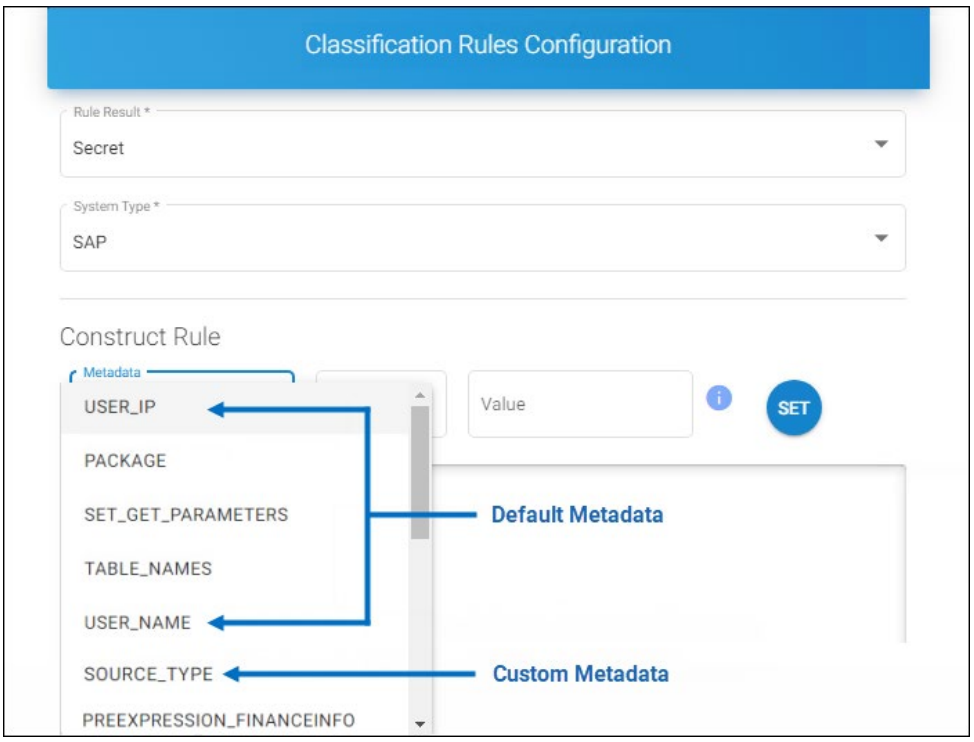
   Results:

   a. You will receive a confirmation message on saving the Custom Metadata.

   b. The new metadata name is added to the list.

Related tasks

1. If you want to edit/remove a newly added custom metadata from the list, click the **Edit**/**Delete** icon against the metadata.
2. To search metadata by name, use the text box labeled **Search by Metadata**. Your search results will be displayed.
3. The new custom metadata is displayed and available for user selection in the **Classification Rule UI** as shown in the below example:



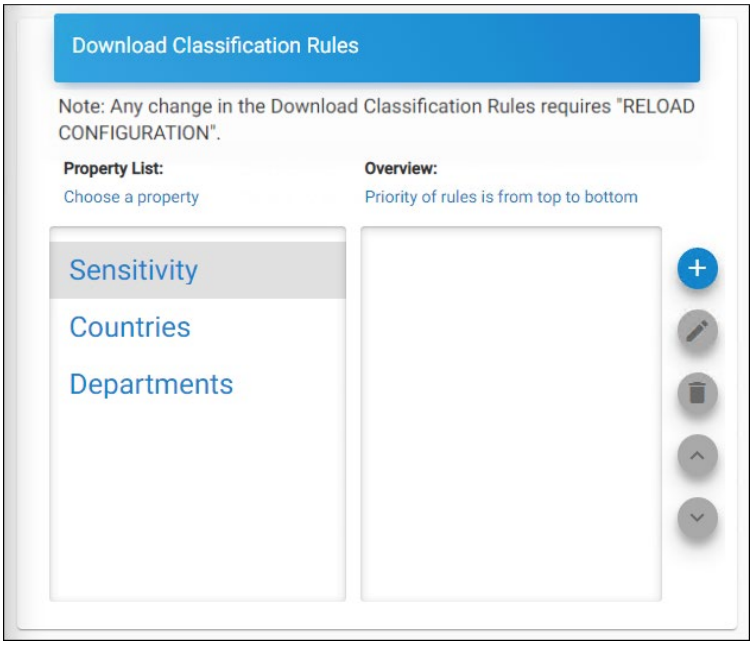
Example for Custom Metadata

3.5.9.2.5. Create Download Rules

Prerequisite: Make sure that classification properties and their values are configured.

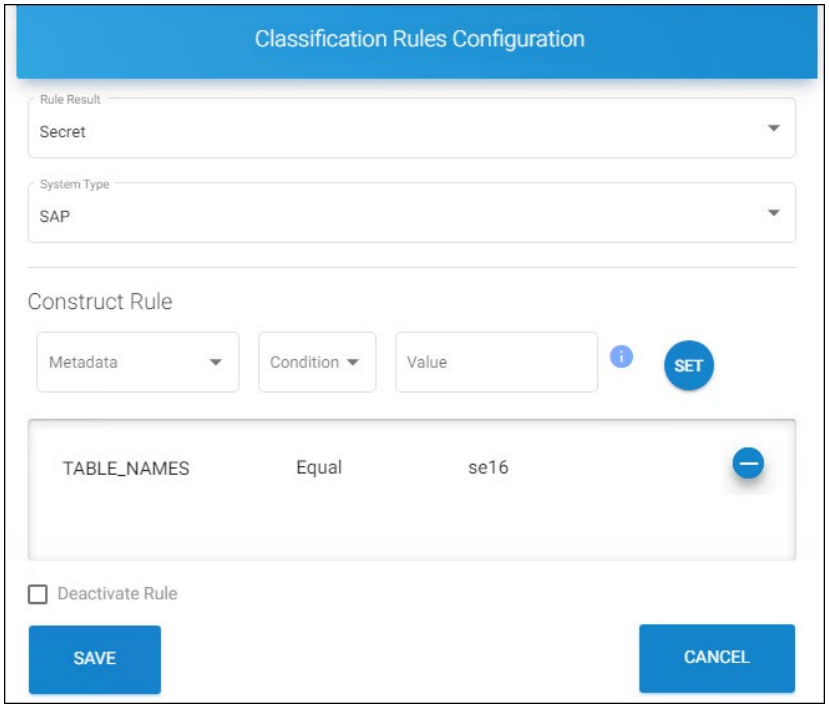
Classification Rules define one or more classifications based on metadata types and pre-expressions.

1. On the **Rules** tab, click **Configure**.
2. The *Download Classification Rules* page will appear as shown in the figure below:



Download classification rules page

3. Select a property from the **Choose a Property** table and then click on the plus icon.
4. The *Classification Rules Configuration* page will appear as shown in the figure below:

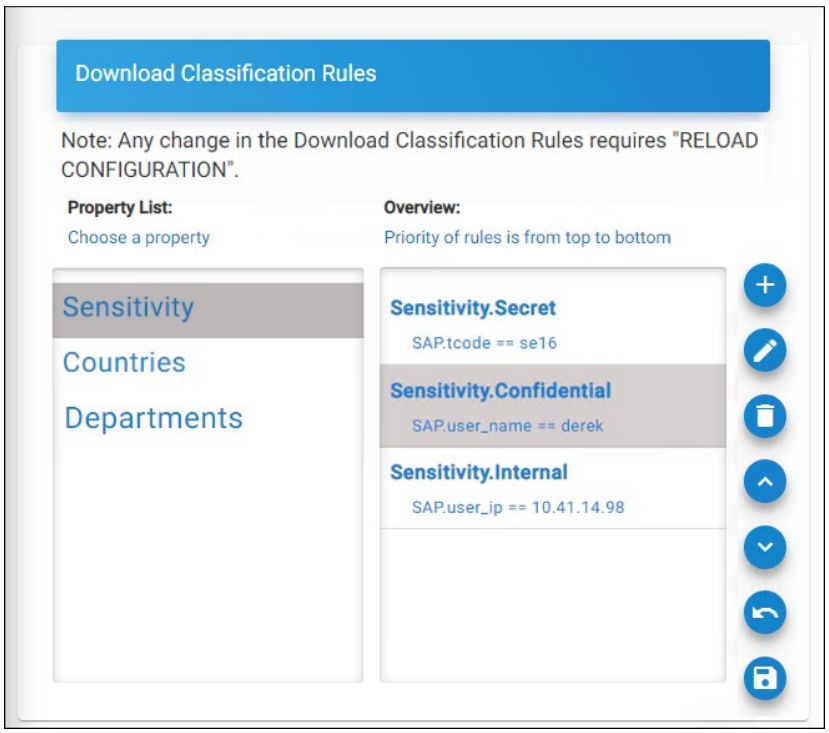


Classification rules configuration

5. Enter the values for the following:
   a. **Rule Result** – Select a value from the list.
   b. **System Type** – HaloENGINE supports the following system types: BO, SAP, Windchill, Teamcenter, Keytech, Autodesk_Vault, SOLIDWORKS_PDM, and HaloENGINE_API. Based on your license, your system type will be displayed by default.
   c. **Metadata** – Select a value from the list.
   d. **Condition** – Select a condition (Equal/Not Equal) from the list.
   e. **Value** – Enter a value for the selected metadata (case-sensitive).
6. Click **Set** to apply the rules.
7. The selected metadata and its condition will be added to the list.
8. Click **Save**.

Results:

1. You will receive a confirmation message after adding or updating the rule.
2. The rule is added to the list under the **Overview** table as shown in the figure below:



Classification rules page after configuration

Related tasks

1. By default, the current rule will be activated. However, you can turn off the rule by selecting the **Deactivate Rule** check box.
2. If you wish to increase/decrease the priority of a rule, you can do so by selecting the rule and then clicking on the respective up arrow/down arrow icon.
3. You can reverse the priority changes you have made by clicking the **Restore the priority changes** icon.
4. To save your priority changes, click **Save the priority changes** icon.

Reference Manuals:

For more information about metadata description, please refer to the relevant HaloCAD PLM/PDM Installation Manual.

1. SAP – HaloCORE Installation Manual
2. Autodesk Vault – HaloCAD for Autodesk Vault Installation Manual
3. Teamcenter – HaloCAD for Teamcenter Installation Manual
4. Windchill – HaloCAD for Windchill Installation Manual
5. SOLIDWORKS PDM – HaloCAD for SOLIDWORKS PDM Installation Manual
6. Keytech – HaloCAD for Keytech Installation Manual
7. BO – HaloCORE BO Installation Manual

8. HaloENGINE API – There is no built-in metadata for REST SDK, so Custom metadata can be used to generate new metadata for the HaloENGINE API system type. Please refer to the section “Custom Metadata”.

3.5.9.2.6. Add Action Rules

Action rules specify when a file download should be blocked, labeled, protected, or excluded.

Simulation Mode

1. In Simulation Mode, you can observe the runtime behavior of the label/protect/block/exclude process. The file will be downloaded without being labeled or blocked.
2. Additionally, the event is logged as an actual file download.
3. This feature is only applicable to SAP clients.

Prerequisite:

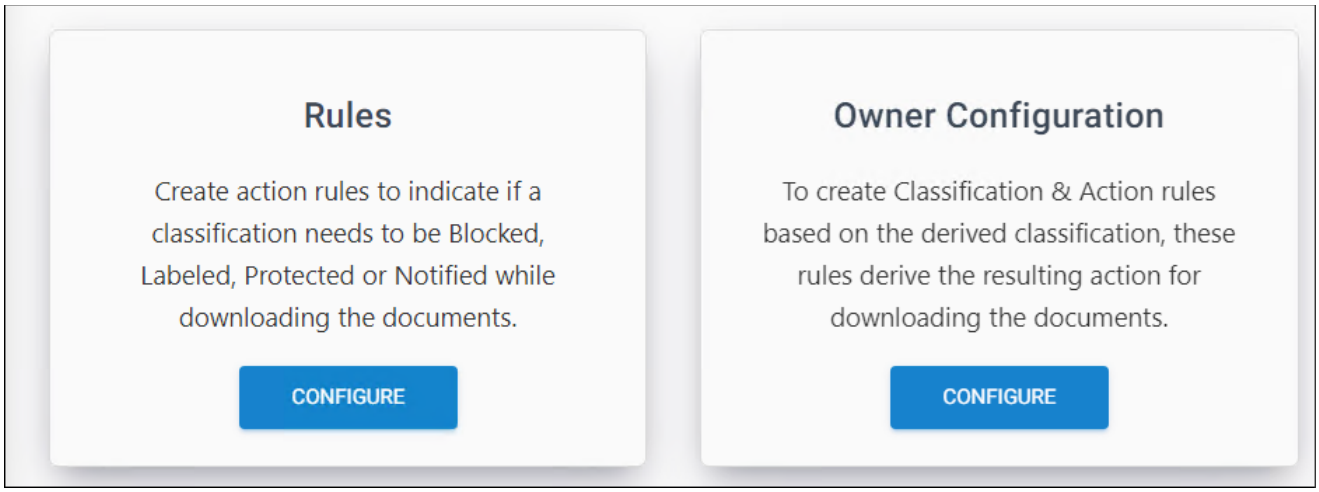
Based on the features you choose (as indicated in the table below), you must map the profile to a registered HaloENGINE Service as described in the section "Phase 4. Register HaloENGINE Services".

Action Rules	HaloENGINE Service
Protect/Label	Is needed for protection
Block	Not required

Action rules and HaloENGINE Service

Follow the below procedure to add Action Rules:

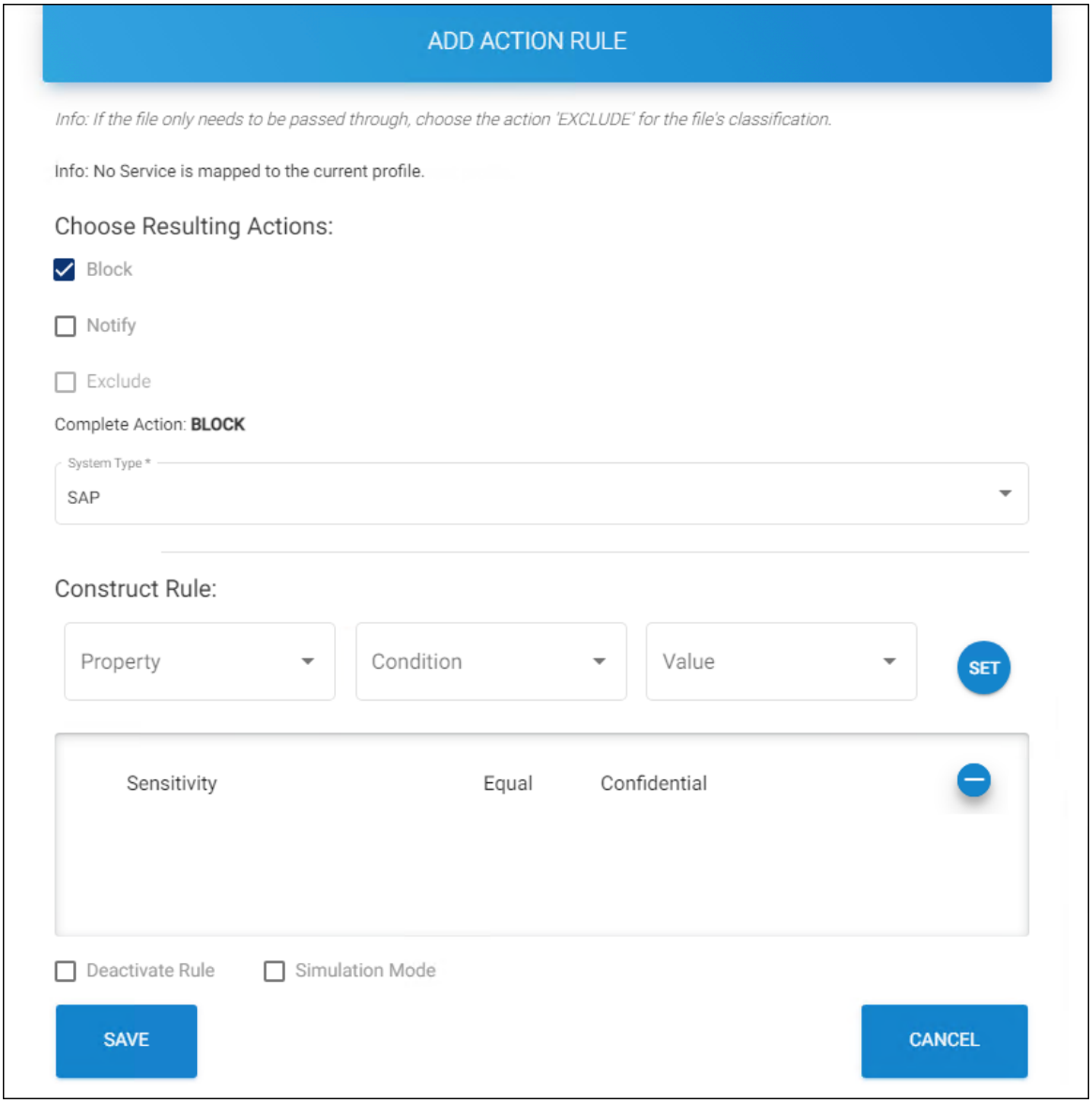
1. On the **Action Rules** tab, click **Configure** and the following page will appear, as shown in the figure below:



Action Rules

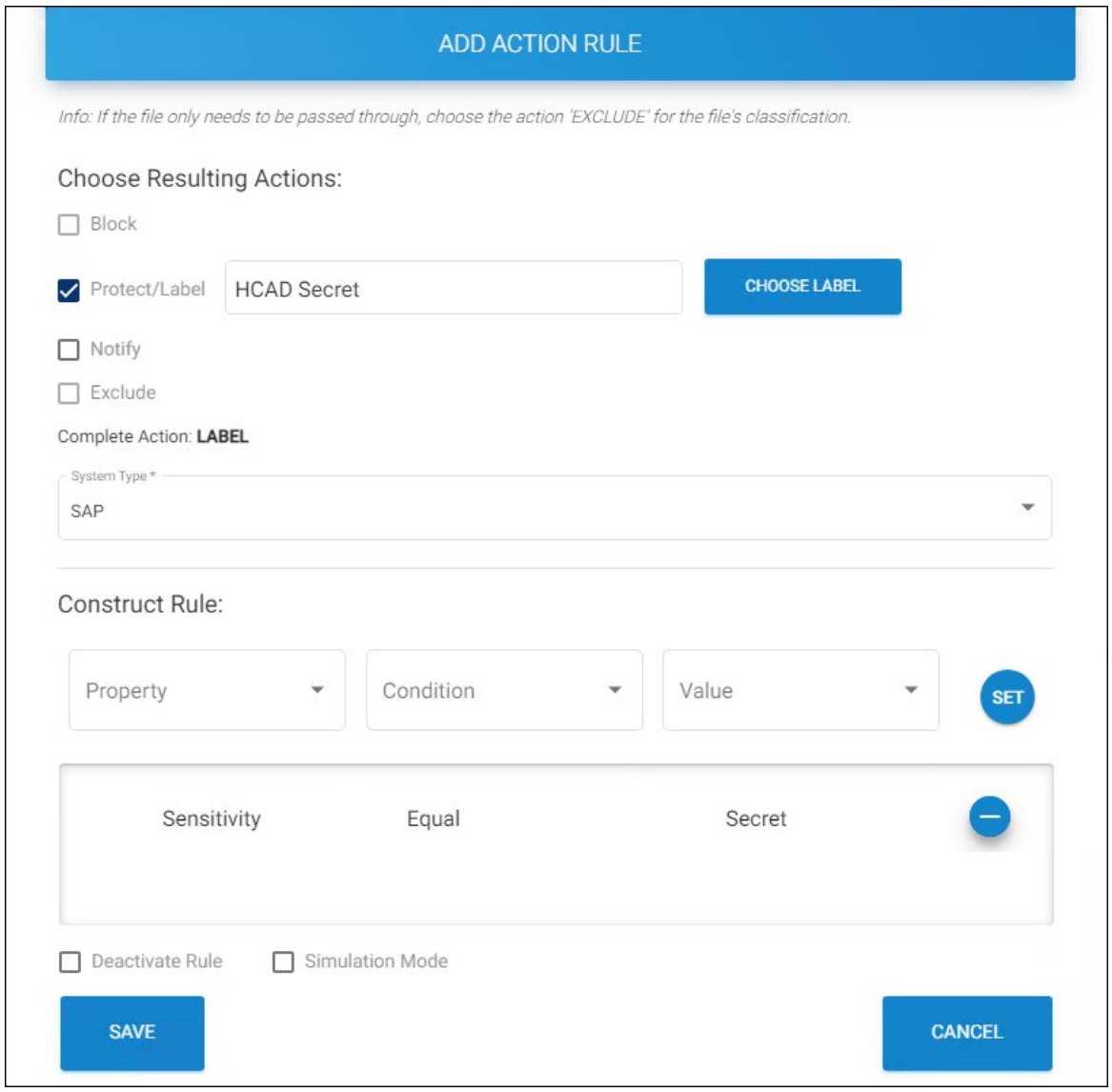
2. On the **Rules** tab, click **Configure**.

3. On the *Action Rules for Download* page, click on the plus icon.
4. The *Add Action Rule* page will appear.
5. Under **Choose Resulting Actions** select any one of the actions:
   a. To block a file download, select the **Block** check box and proceed to point 6.



Action rule for block

   b. To protect a file download, select the **Protect/Label** check box. Click **Choose Label** to select a label from the list. Note: The labels are automatically retrieved from Azure RMS by the HaloENGINE Service. Proceed to point 6.



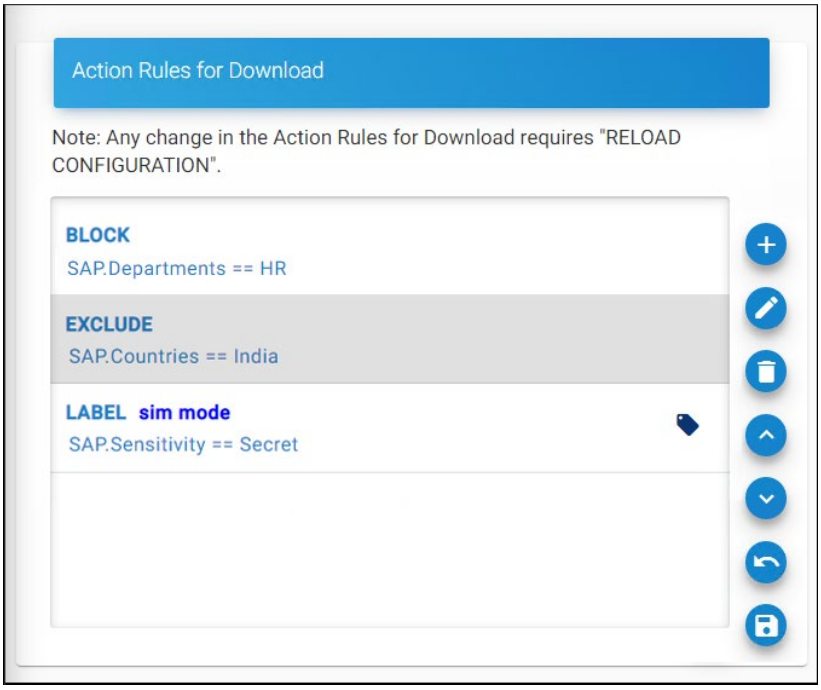
Action rule for protection

c. **Exclude** – Allows suppressing actions such as monitor, block, notify, label, or protect during a file download by selecting the "**Exclude**" action based on the configured metadata (e.g., user_name) or Pre-expression. If selected, other options will be disabled. Proceed to point 6.

d. **Notify** – Notifies of a file download. You can choose to notify from the four choices listed above. Note: HaloCORE's Notify (alert) mechanism allows organizations to proactively detect security and compliance risks via real-time reporting. All download and data extraction activities in SAP are reviewed, and alerts are raised using the GRC mechanism. During a download, the HaloENGINE determines whether a notification must be sent or not based on the classification rules and actions. If action = Notify, the HaloENGINE requests the NetWeaver client (BAdI) to send a notification. A GRC alert is triggered "as implemented in the enhancement spot /SECUDEGC/ES_ALERT". Please note this mechanism is not yet implemented in HaloCORE for GRC. It will be implemented in a future release.

6. **System Type**
   a. Supported system types for protection: BO, SAP, Windchill, Teamcenter, Keytech, Autodesk_Vault, SOLIDWORKS_PDM, and HaloENGINE_API. Based on your license, your system type will be displayed by default.
   b. Supported system types for blocking: BO, SAP, Windchill, Teamcenter, Autodesk_Vault, and SOLIDWORKS_PDM, Based on your license, your system type will be displayed by default.
7. Enter the values for the following under **Construct Rules**:
   a. **Property** – Select a value from the list.
   b. **Condition** – Select a condition (Equal/Not Equal) from the list.
   c. **Value** – Select a value from the list.
   d. **Deactivate Rule** – If you want to deactivate a rule, select **Deactivate Rule** check box.
   e. **Simulation Mode** – If you want to perform the exact actions without processing the file, select the Simulation Mode check box.
8. Click **Set** to set up the rule. The selected property and its condition will be added to the list.
9. Click **Save**.

   Results:
   a. You will receive a confirmation message after adding or updating the action rule.
   b. The rule is added to the list.



List of action rules

Related tasks

1. You can manage the Action Rule by using the edit/delete icons.
2. If you wish to increase/decrease the priority of a rule, you can do so by selecting the rule and then clicking on the respective up arrow/down arrow icon.
3. You can reverse the priority changes you have made by clicking the **Restore the priority changes** icon.
4. To save your priority changes, click **Save the priority changes** icon.

Action Rule priorities

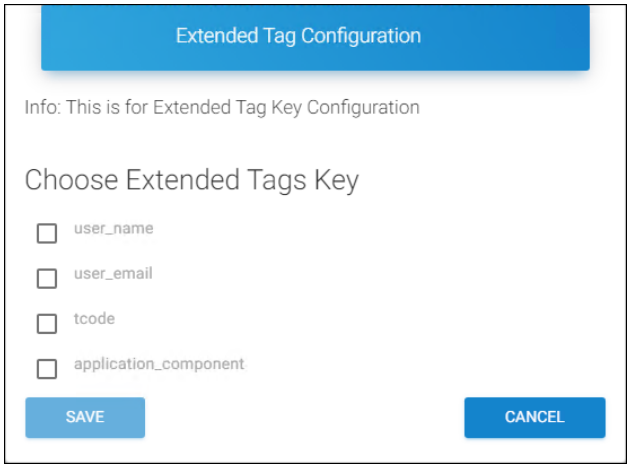
When there are several classification rules, the HaloENGINE prioritizes them from top to bottom. For instance, if Rule 1, Rule 2, Rule 3, and Rule 4 are present in the Classification Engine.

1. The Classification Engine starts verifying the topmost rule "Rule 1" first. If all classification expressions are correct, the first action rule is applied.
2. If not, it moves on to "Rule 2" and does more verification.
3. This verification process continues until a classification expression with the correct classification expression is found, or none apply.

Extended Tags Configuration (Only for SAP)

Besides MPIP metadata, some users may wish to add additional metadata while downloading a file from SAP. In such cases, the user should add an extended key and value.

1. After saving the rule for SAP, you can see the **Extended Tags Configuration** icon on the **Action Rules for Download** page.
2. Adding an extended tags feature is only applicable to the SAP Client type. Extended tag configuration is not available in case of block or exclude action.
3. Click on the tag icon, and the *Extended Tag Configuration* page will appear as shown in the figure below:



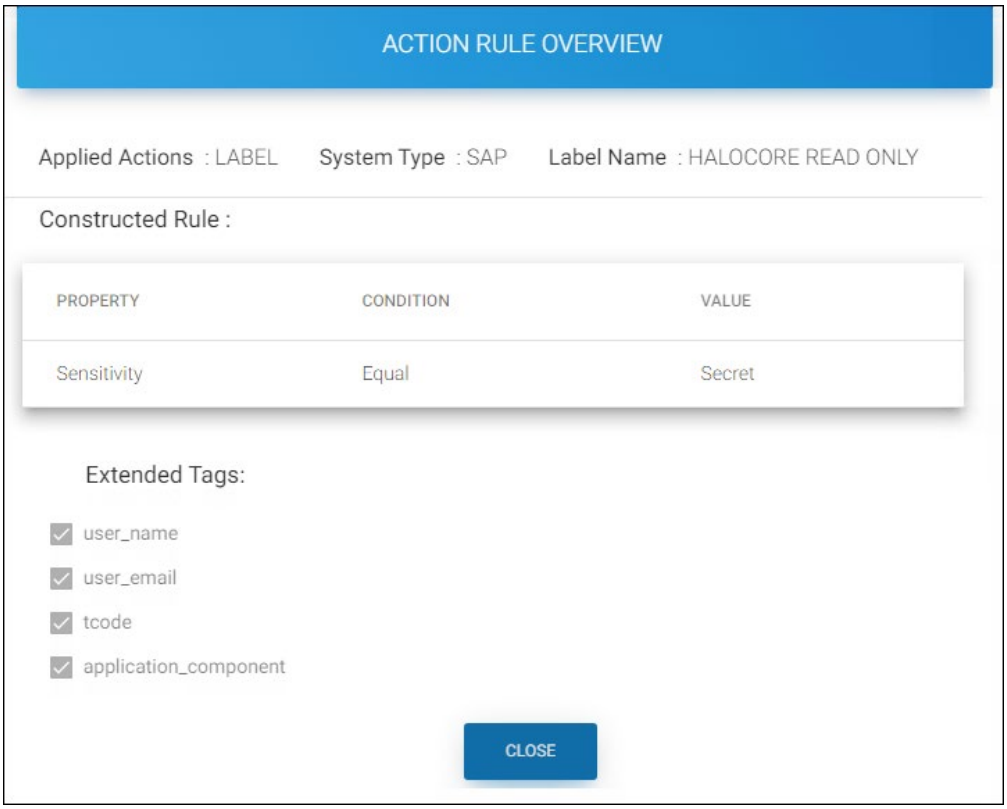
Extended tag configuration page

4. Select one or more tags (user_name, user_email, tcode, application_component) from the list.
5. Click **Save** to save the setting.

   Results:

   a. You will receive a confirmation message after adding or updating the tags.

   b. Double-click on the Action Rule and the *Action Rule Overview* page will appear as shown in the figure below:



Overview page

6. Click **Close** to close the page.

Owner Configuration (Optional)

This feature defines how a user can be determined as an owner of exported documents.

Supported client systems

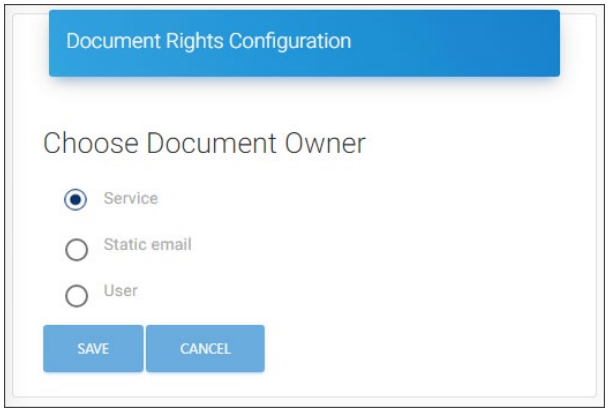
1. Supported in SAP, Teamcenter, Windchill, and Autodesk_Vault systems.
2. Not supported in the BO system.

Prerequisites:

1. Make sure the HaloENGINE Service is installed.
2. Make sure to map a HaloENGINE Service to a profile.

Follow the below steps to configure owner rights:

1. On the **Owner Configuration** tab, click **Configure**.
2. The *Document Rights Configuration* page will appear as shown in the figure below:



Owner rights

3. Select one of the following three options:
   a. **Service** (default) – The Application ID that is used to initialize the HaloENGINE Service will be the owner of the document.
   b. **Static email** – The email address entered in the text box will be considered the owner of the document.
   c. **User** – The mail address is derived from the Client (For example, `SAP User ID`).
4. Click **Save** to save the rule.
   Results: You will receive a confirmation message after updating the assigned rights.

3.5.9.3. Create Upload Classification Rules

Upload rules define classification rules based on metadata types and action rules decide how a file must be decrypted when uploading a file. These two rules derive the resulting action for uploading the documents.

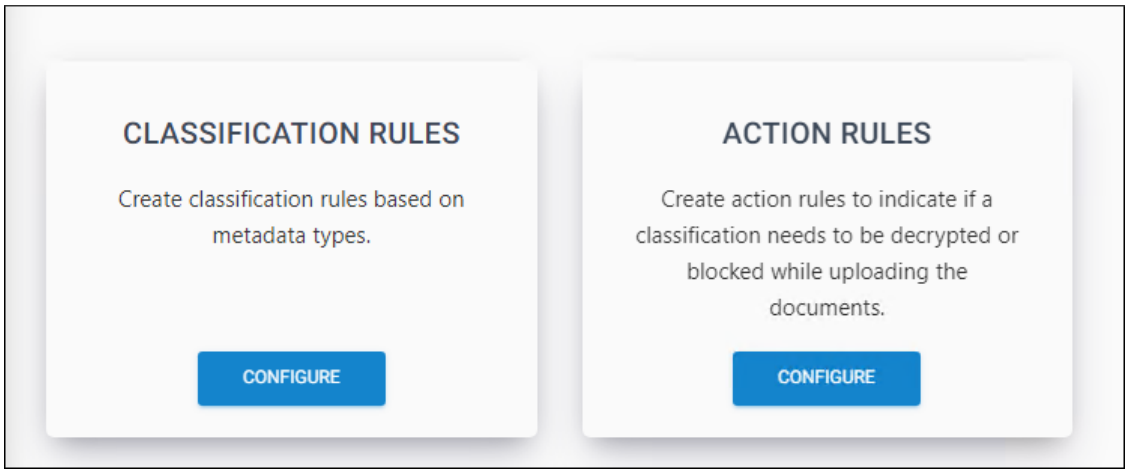
Prerequisites:

1. Make sure that the HaloENGINE Service is installed.
2. Make sure that the profile is mapped to a registered HaloENGINE Service. For more details, please refer to the section "Phase 4. Register HaloENGINE Service".

Follow the below procedure to enable the upload rules:

1. To create classification and action rules for file uploads, you need to enable **Upload Rules** first.
2. On the **Upload Rules** tab, turn on the **Activate** button as shown in the image "Classification Configuration".

3. To the question, *Would you like to Enable/Disable Upload configuration? Upload Configuration will be Enable*d, answer **Yes**.
4. You will receive a confirmation message on changing the upload switch for decryption.
5. Now, click **Configure**, *Upload Rules Configuration* page will appear as shown in the figure below:

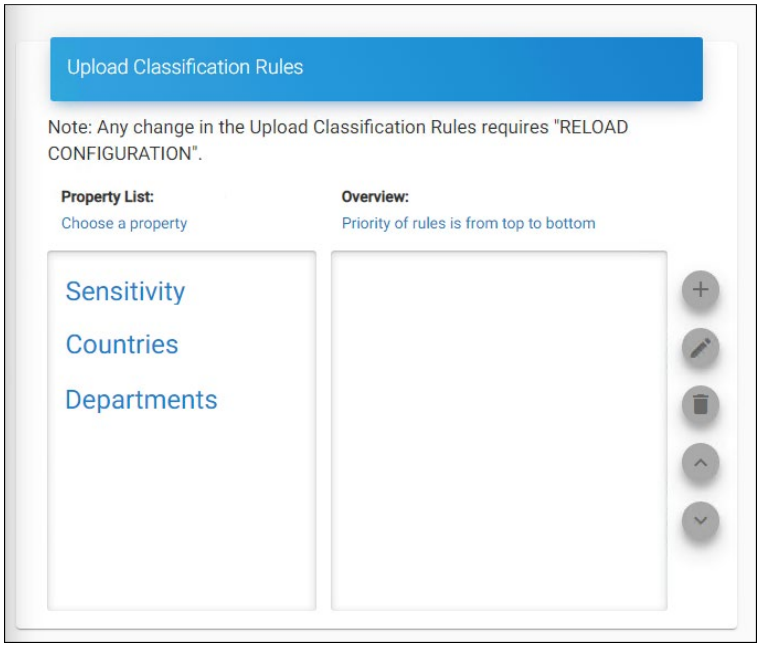


Upload rules configuration page

3.5.9.3.1. Create Upload Rules

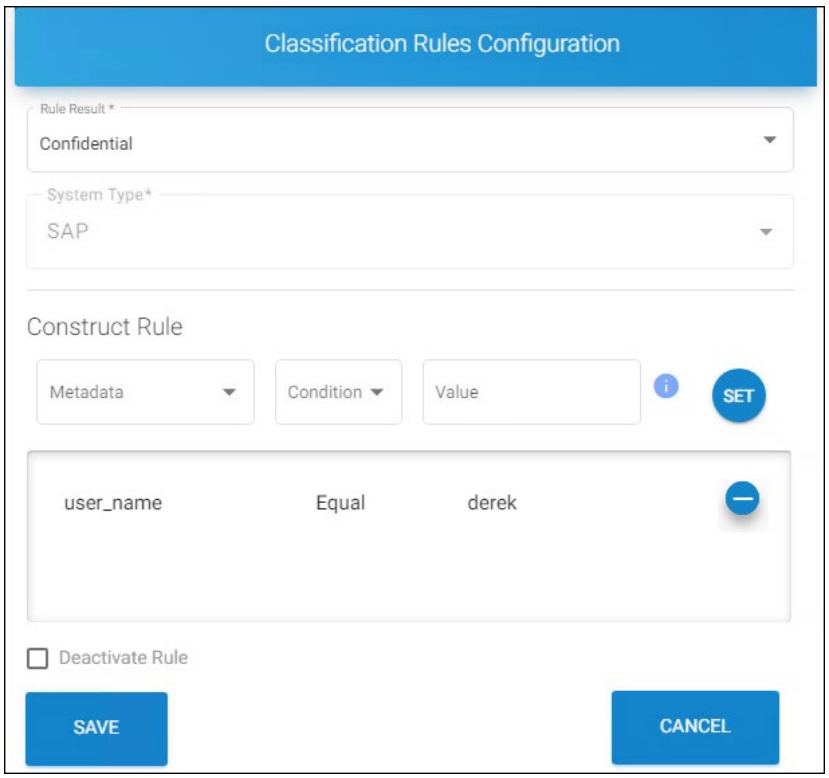
Classification rules can be created based on metadata types.

1. On the **Classification Rules** tab, click **Configure**.
2. The *Upload Classification Rules* page will appear as shown in the figure below:



Upload classification rules page

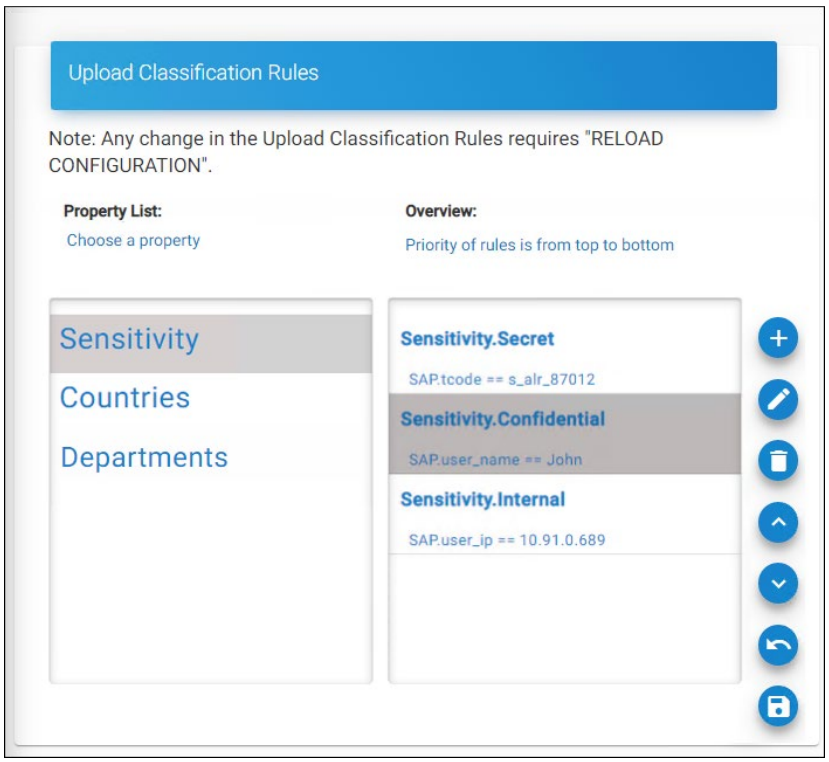
3. Select a property from the **Choose a property** table and then click on the plus icon.
4. The *Classification Rules Configuration* page will appear as shown in the figure below:



Upload Classification Rules Configuration #1

5. On the **Classification Rules Configuration** page, enter the values for the following:
   a. **Rule Result** – Select a value from the list.
   b. **System Type** – SAP will be displayed by default. Currently supported only for SAP system type.
   c. **Metadata** – Select a value from the list.
   d. **Condition** – Select a condition (Equal/Not Equal) from the list.
   e. **Value** – Enter a value for the selected metadata (case-sensitive).
   f. **Deactivate Rule** – By default, the current rule will be activated. However, you can turn off the Rule by selecting the **Deactivate Rule** check box.
6. Click **Set** to apply the rules. The selected metadata and its condition will be added to the list.
7. Click **Save**.

   Results:
   a. You will receive a confirmation message after adding or updating the rule.
   b. Please note that it is not possible to add the same rule that already exists in Download Rules.
8. The rule is added to the list under the **Overview** table as shown in the figure below:



Upload Classification Rules Configuration #2

Related tasks

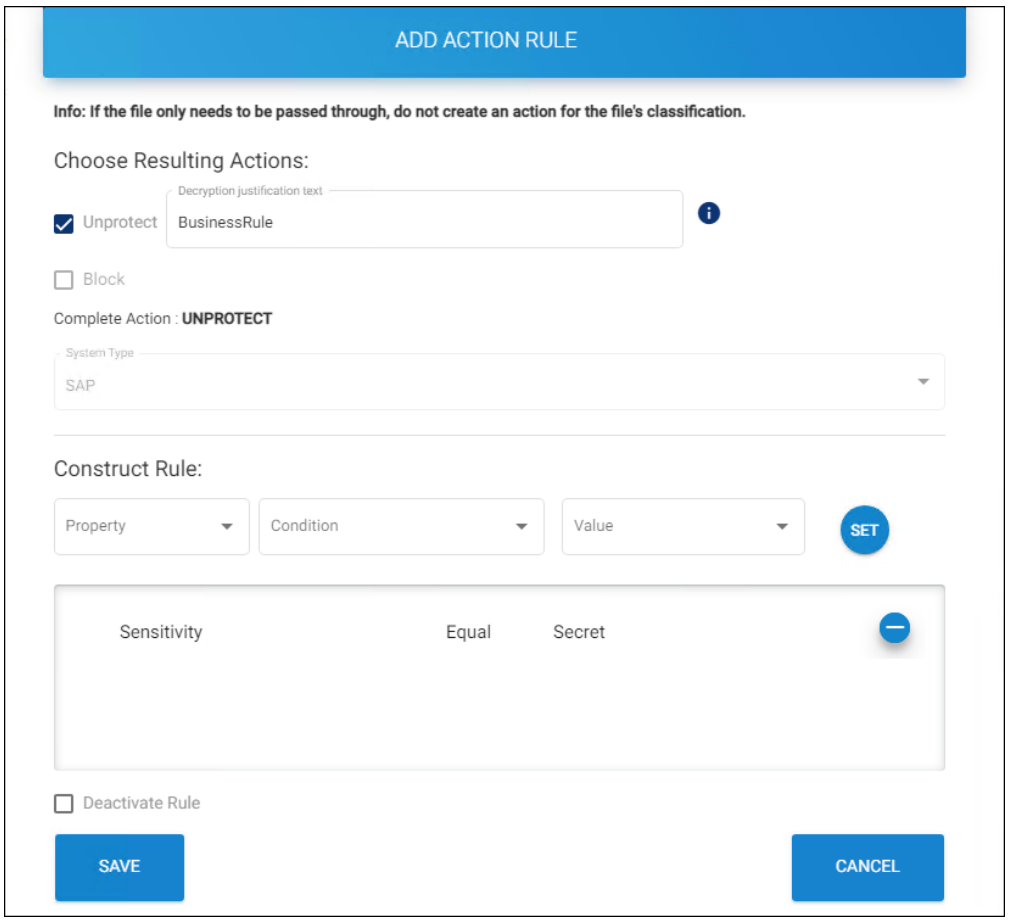
1. You can manage the action rule by using the edit/delete icons.
2. If you wish to increase/decrease the priority of a rule, you can do so by selecting the rule and then clicking on the respective up arrow/down arrow icon.
3. You can undo the priority changes you have made by clicking the **Restore the priority changes** icon.
4. To save your priority changes, click **Save the priority changes** icon.

3.5.9.3.2. Add Action Rules

Action rules are created to apply decryption while uploading the documents.

Follow the below procedure to configure rules to unprotect:

1. On the **Action Rules** tab, click **Configure**.
2. Click on the plus icon on the *Action Rules for Upload* page.
3. The *Add Action Rule* page will appear as shown in the figure below:



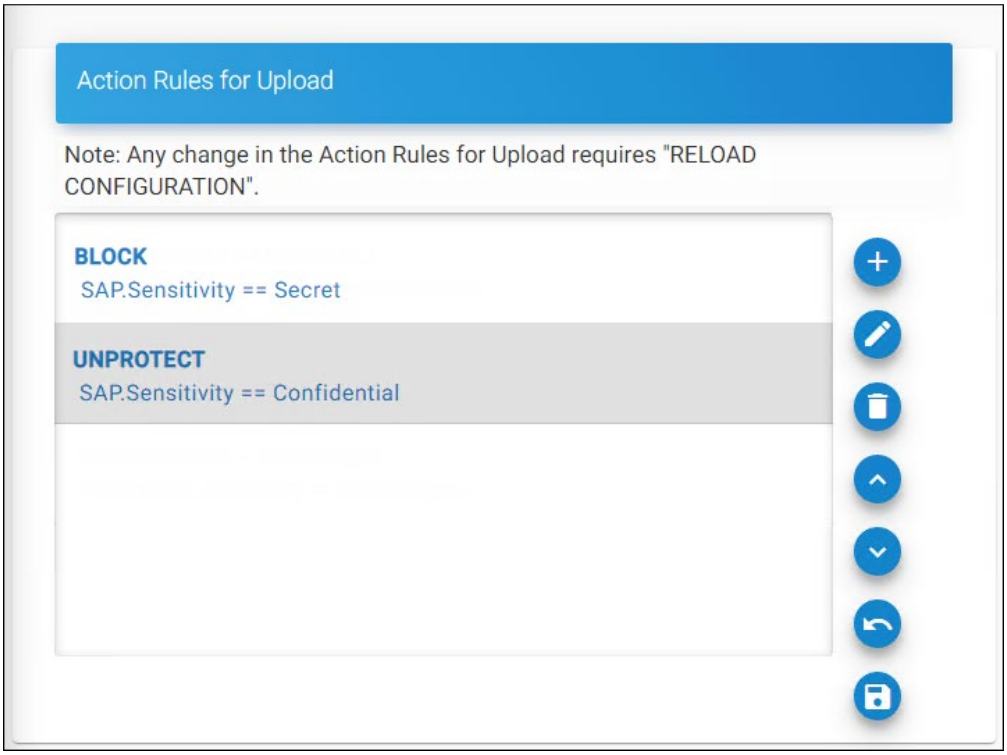
Add action rule page

4. Under **Choose Resulting Actions** select any one of the actions:
   a. **Unprotect** – Select the check box, if the uploaded file needs to be decrypted and enter a justification message or you can leave it blank in the **Decryption justification text** box. The justification text can be up to 15 characters without space or special characters. Proceed to point 6.
   b. **Block** – Select the check box, if the uploaded file needs to be blocked. Proceed to point 6.
5. **System Type** – SAP will be displayed by default. Currently supported only for SAP system type.
6. Enter the values for the following under **Construct Rules**:
   a. **Property** –Select a value from the list.
   b. **Condition** – Select a condition (Equal/Not Equal) from the list.
   c. **Value** – Select a value from the list.
   d. **Deactivate Rule** – By default, the current rule will be activated. However, the admin portal allows you to turn off the Rule by selecting the **Deactivate Rule** check box.
7. Click **Set** to set up the rules. The selected property and its condition will be added to the list.
8. Click **Save**.

Results:

a. You will receive a confirmation message after adding or updating the rule.

b. The rule is added to the *Action Rules for Upload* page as shown in the figure below:



Action rules for upload

Related tasks

1. The rule is added to the list. If you wish to increase/decrease the priority of a rule, you can do so by selecting the rule and then clicking on the respective up arrow/down arrow icon. However, a rule with more conditions cannot be moved below the rule with fewer conditions.
2. You can reverse the priority changes you have made by clicking the **Restore the priority changes** icon.
3. To save your priority changes, click **Save the priority changes** icon.

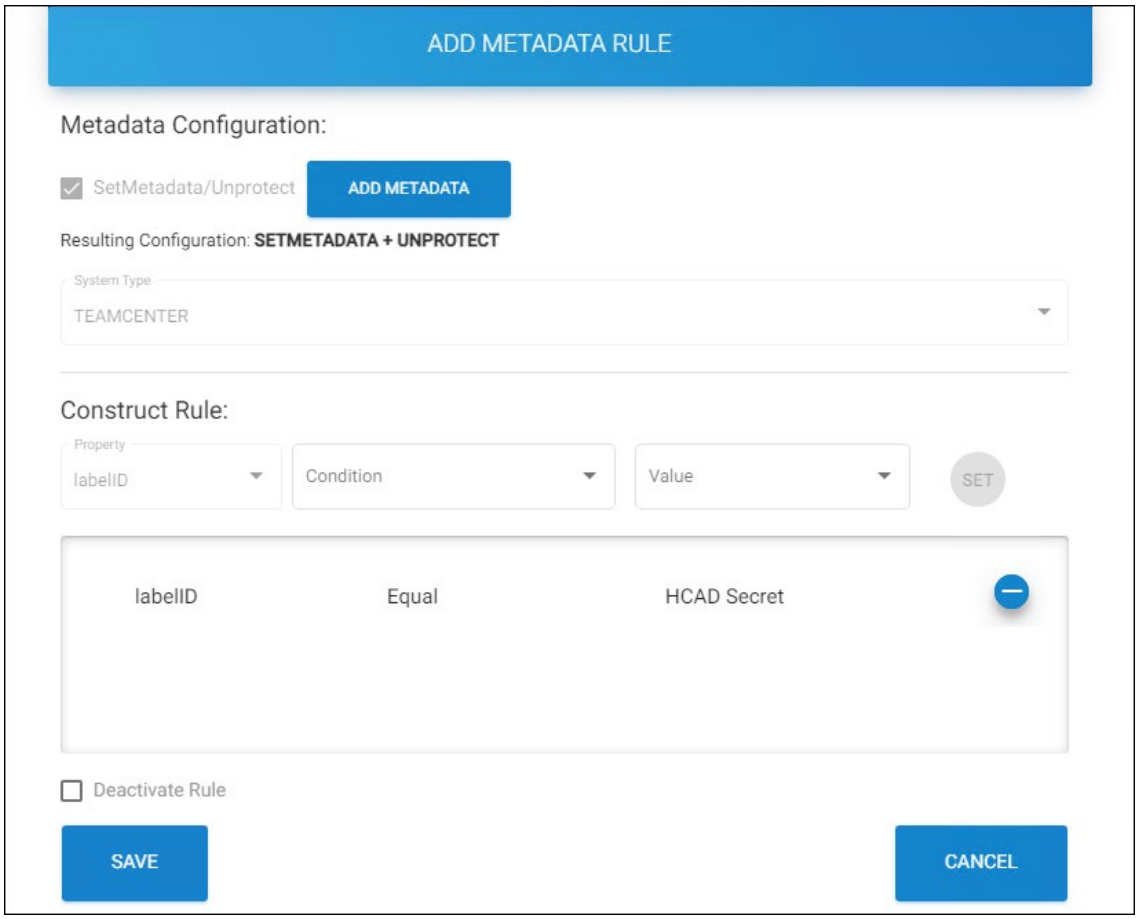
3.5.9.4. Metadata Configuration

SetMetadata/Unprotect Action (only for Teamcenter): It allows you to set existing metadata back onto the file while checking-in, based on the MPIP label. This aids in the consistency of file classification. As an example, for Teamcenter **IP_Classification** values can be returned. Note: It is not currently supported by other PLMs.

Follow the below steps to configure metadata:

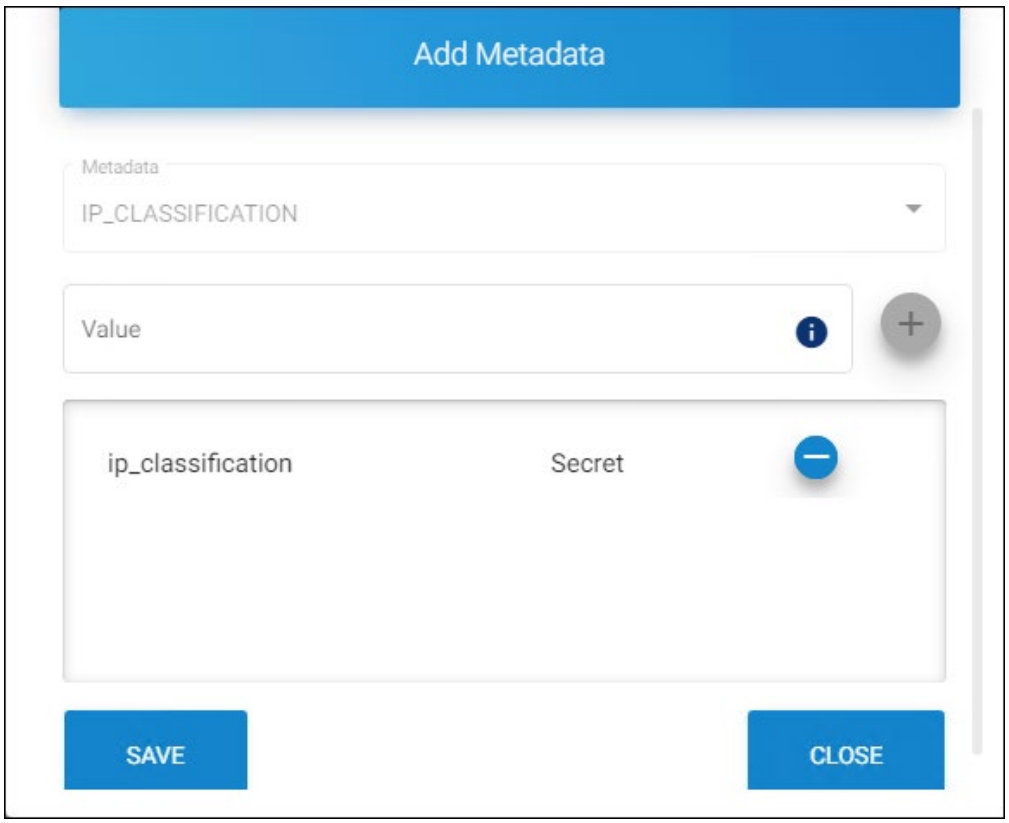
1. On the **Metadata Configuration** tab, click **Configure**.

2. Click on the plus icon, and the *Add Metadata Rule* page will appear as shown in the figure below:



Add metadata rule

3. By default, **SetMetadata/Unprotect** option will be selected.
4. Click **ADD METADATA**.
5. The *Add Metadata* page will appear as shown in the figure below:



Add metadata page

a. **Metadata** – IP_CLASSIFICATION will be displayed by default. Currently supported only for **ip_classification** metadata.

b. **Value** – Enter the metadata that is used during encryption (minimum of 3 characters, maximum of 30 characters, and case sensitive.)

c. Click on the **plus** icon to apply the rules. The selected metadata and its condition will be added to the list.

d. Click **Save**.

6. **System Type** – Teamcenter will be displayed by default. Currently supported only for Teamcenter system type.
7. Enter the values for the following under **Construct Rules**:

a. **Property** – labelID will be displayed by default. Currently supported only for labelID.

b. **Condition** –Select a condition (Equal/Not Equal) from the list.

c. **Value** – Select a label from the list.

d. Click **Set** to set up the rules. The selected property and its condition will be added to the list.

e. **Deactivate Rule** – By default, the current rule will be activated. However, the admin portal allows you to turn off the Rule by selecting the **Deactivate Rule** check box.

8. Click **Save**.

   Results: You will receive a confirmation message after adding or updating the rule.

The table below outlines the key attributes that are allowed on each system type.

Profile Configuration								
System Types	**Download Rules (default)**	**Upload Rules**	**PII and Fin. Info.**	**Cust. Pre-Exp.**	**Owner Config.**	**Metadata Config.**	**Sys. Metadata Config.**	**Auth./Comm. Endpoint**
SAP	Yes	Opt.	Yes	Opt.	Opt.	N/A	Opt.	Mutual
HaloCORE BO	Yes	N/A	N/A	Opt.	Opt.	N/A	Opt.	Mutual
Teamcenter	Yes	N/A	N/A	Opt.	Opt.	Opt.	Opt.	Mutual
Autodesk_Vault	Yes	N/A	N/A	Opt.	Opt.	N/A	Opt.	Mutual
Windchill	Yes	N/A	N/A	Opt.	Opt.	N/A	Opt.	Mutual
Keytech	Yes	N/A	N/A	Opt.	Opt.	N/A	Opt.	Mutual
SOLIDWORKS PDM	Yes	N/A	N/A	Opt.	Opt.	N/A	Opt.	Supports mutual and server-side
HaloENGINE_API	Yes	N/A	N/A	Opt.	Opt.	N/A	Opt.	Supports mutual and server-side

Key attributes of each system type

Abbreviations used in the above table

1. N/A - Not Applicable
2. Opt. - Optional
3. Fin. Info. - Finance Information
4. Cust. Pre-Exp. - Custom Pre-Expression
5. Owner Config. - Owner Configuration
6. Metadata Config. - Metadata Configuration (Profile Configuration > Profile Classification > Classification Configuration > METADATA CONFIGURATION)

7. Sys. Metadata Config. - System Metadata Configuration (Profile Configuration > System Metadata Configuration)
8. Auth. - Authentication
9. Comm. - Communication

3.5.9.5. Assign User Permission

HaloENGINE uses three roles—**ROLE_SUPER_ADMIN**, **ROLE_CUSTOMER_ADMIN**, and **ROLE_CUSTOMER_USER**—for authentication and authorization. These roles are set up and managed through the Azure portal. For more details, please refer to the section "User Management Settings". The **Assign User Permission** page allows you to add users who have been assigned to the role **ROLE_CUSTOMER_USER**.

The following configurations are possible for the ROLE_CUSTOMER _USER. Using these read-and-write permissions, a user can manage multiple profiles.

For example,

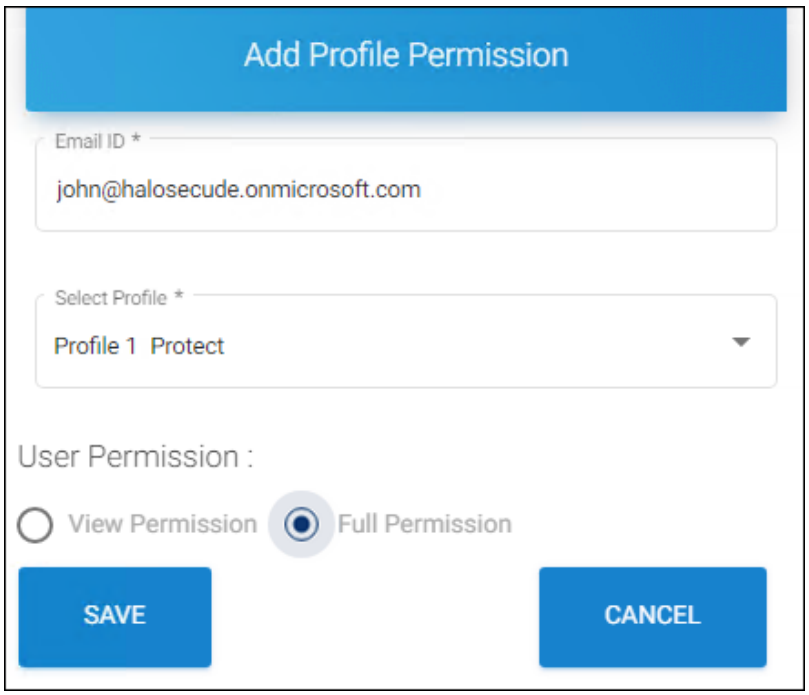
1. User 1 - assigned with full rights as an admin user. So he could access the entire portal without any limitations.
2. User 2 - assigned with read-only access. This user can view the configuration of a particular profile but is restricted to changing the settings.
3. User 3 - assigned with write access. This user is allowed to change the configuration of a particular profile.

User accounts

1. Administrator with Super User role—Granted, the highest level of access to the entire HaloENGINE component.
2. Domain Users with Customer_Admin roles—Have fewer admin privileges than Super User.
3. Domain Users with Customer_User roles must be configured with access. Access to this user is granted by either Customer_Admin or Super User.

Follow the below procedure to configure user access:

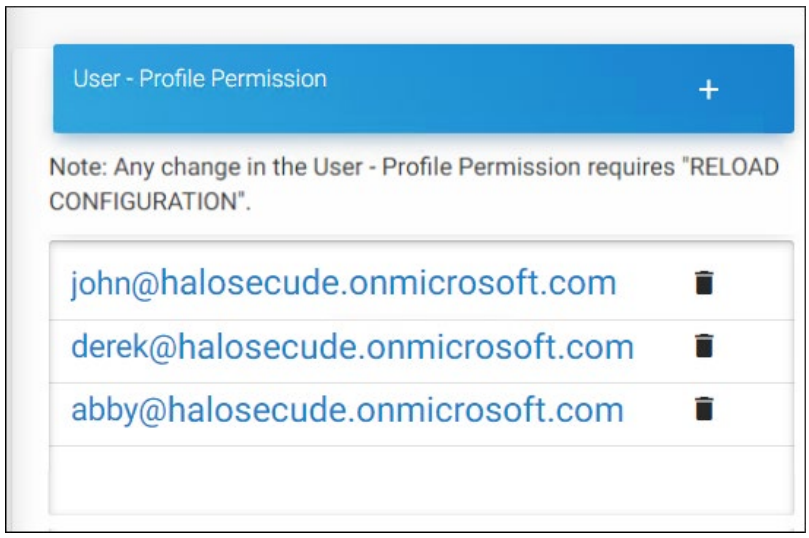
1. On the **Assign User Permission** tab, click **Configure**. The *User - Profile Permission* page will appear.
2. Click on the plus icon and enter the following details on the *Add Profile Permission* page.



Adding a user page

3. Enter the following details:
   a. **Email ID** - Enter the email ID, which is mapped to the role ROLE_CUSTOMER_ADMIN/ROLE_CUSTOMER_USER in the Azure portal. For more details, please refer to the section "User Management Settings".
   b. **Select Profile** - Select a profile from the list.
   c. **User Permission** - Select either View Permission or Full Permission for the user.
4. Click **Save**.

   Results:
   a. You will receive a confirmation message after adding the user permission.
   b. The Email ID will be added to the list as shown in the figure below:

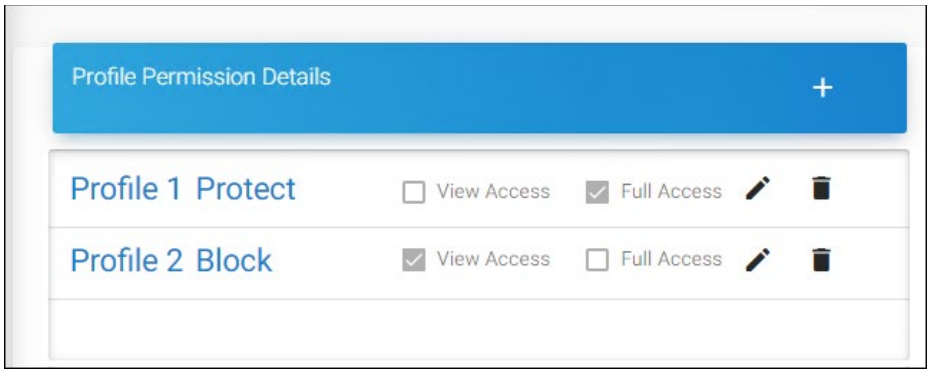


User profile permission #1

Related tasks

To know the details of a user.

1. Click on the user email id. The *Profile Permission Details* page will appear as shown in the figure below:



User profile permission #2

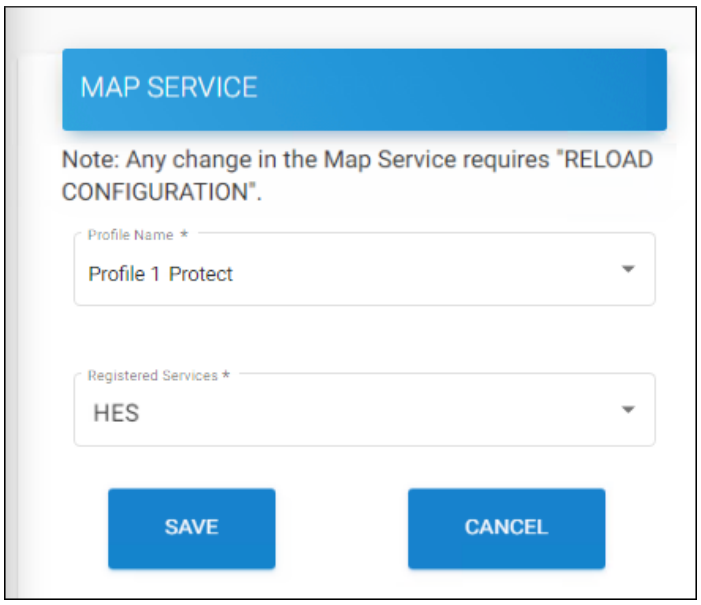
2. You can manage the permission by using the edit/delete icons.

3.5.10. Phase 6. Service Mapping

To encrypt files, you must assign a HaloENGINE Service to a profile.

Prerequisite: Make sure that the HaloENGINE Service is installed and registered in the admin portal. For more details, please refer to "Phase 4. Register HaloENGINE Services".

1. On the left navigation bar, click **Customer Configuration** and then select a customer ID from the list. On the **Profile Configuration** tab, click **Configure**, and then on the **Service Map** tab, click **Configure**. The *Map Service* page will appear as shown in the figure below:



Service mapping page

2. **Profile Name** – Select a profile name from the list.
3. **Registered Services** – Select a registered service from the list.
4. Click **Save**. Repeat the same procedure to map other HaloENGINE Services.

   Results:

   a. You will receive a confirmation message after mapping the service.

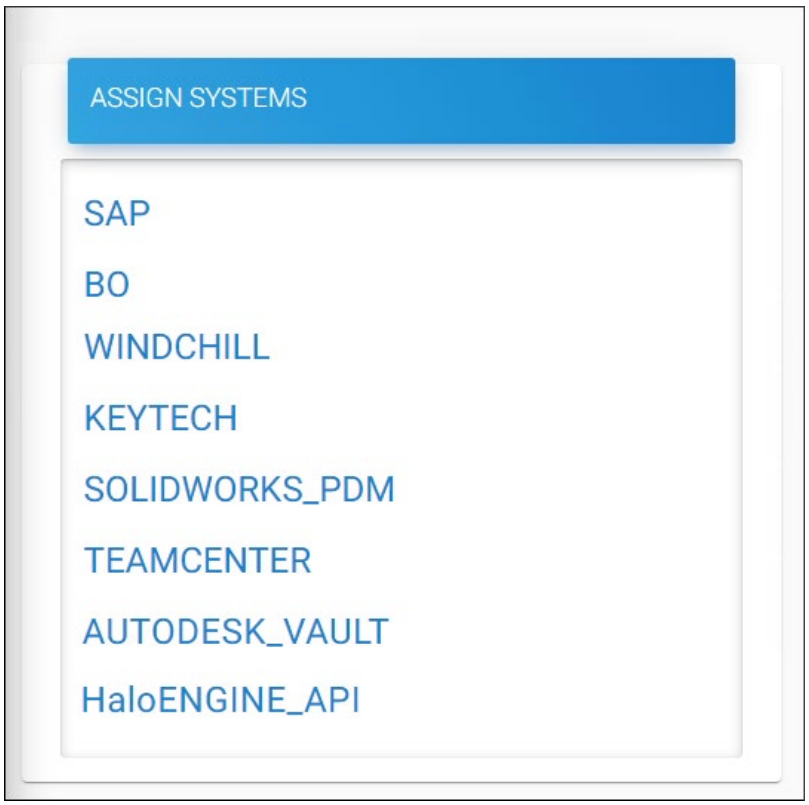
   b. Please be aware that adding the same service that is already mapped to another customer ID is not possible.

3.5.11. Phase 7. Assign Systems

The client systems that must communicate with HaloENGINE should be registered in the admin portal using a unique ID. Please note that if you enable the monitor without configuring a System Unique ID in Assign Systems, the Monitor log in HaloENGINE will not be updated.

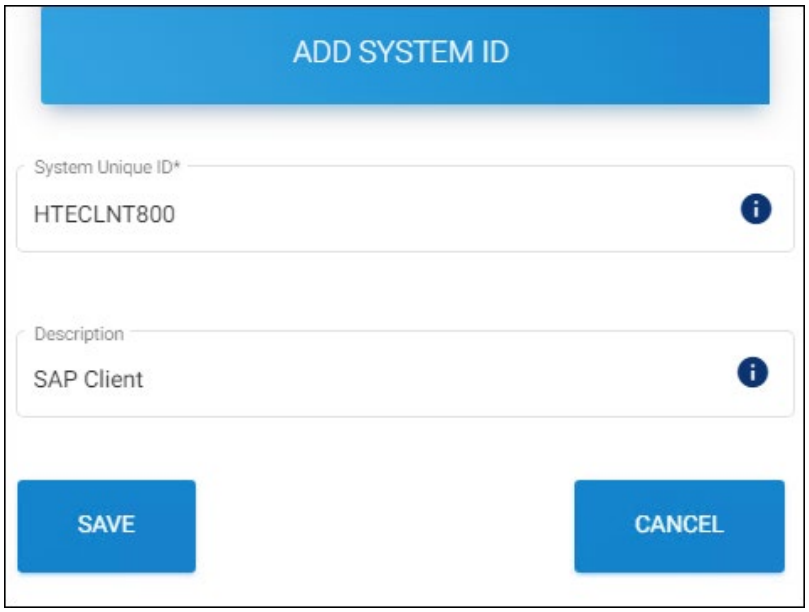
Follow the below procedure to add a system type:

1. On the left navigation bar, click **Customer Configuration** and then select a customer ID from the list.
2. On the **Profile Configuration** tab, click Configure and then on the **Profiles and Classification** tab, click **Configure**. From the profile list, click on a profile, and on the **Assign Systems** tab, click **Configure**.
3. To illustrate and showcase the list of system types available in the portal, a license generated with all client types is uploaded. However, in a typical business environment, you may only have one or a few system types depending on the environment. That implies that by default, only the systems that you have licensed will be displayed.



Assign systems page #1

4. Click on a system type. For illustration, the SAP system is selected.
5. Click on the plus icon and enter the following details on the *Add System ID* page.



Assign systems page #2

6. **System Unique ID** – Enter your system's **System Unique ID**. For information on how the System Unique ID is created, please refer to the section below referred to "Creating a System Unique ID for Clients".
7. **Description** – Enter a description (optional).

8. Click **Save**. Repeat the same steps for other systems.

   Results: You will receive a confirmation message after adding or updating the system ID.

Related tasks

1. You can manage the systems by using the edit/delete icons.
2. You can view the system details by clicking the **Assign System Details** icon.
3. Whenever you make changes to the classification engine, make sure to click **Reload Configuration** for the configuration to take effect. The page will be redirected to the login page once the reload completes.
4. Please be aware that two profiles cannot have the same System Unique ID.

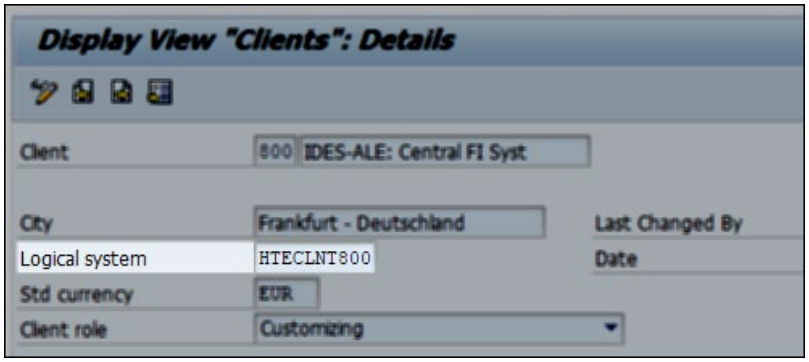
Creating a System Unique ID for Clients

Please make sure the names are case-sensitive when using the System Unique ID in Assign Systems and Client Systems.

HaloCORE SAP Add-on

For an SAP system, the System Unique ID can be either a Logical system name or a new identifier.

1. Method #1 - The Logical system name can be retrieved by using the tcode, **SCC4 - Client Administration**.



Sample system unique ID in SAP instance

2. Method #2 - New identifier. Please refer to the section "HaloENGINE Connection Parameters" in the HaloCORE Installation Manual.

HaloCORE BO

For example, if you specify the **System Unique ID** as **BOCLNT01**, then the same must be entered in the configuration file `ClientUID=BOCLNT01`.

HaloCAD for Teamcenter

Here, the **System Unique ID** must be the Teamcenter Server's hostname that is added as the FMS target in the proxy configuration. For example, if your Teamcenter Server's hostname is TEAMCENTER01, the **System ID** must also be **TEAMCENTER01** when configuring it with the HaloCAD Configuration Tool. The

same name must also be supplied in the System Unique ID field.

HaloCAD for Windchill

Here, the hostname of the Windchill Server that is specified during HaloCAD for Windchill configuration must be the **System Unique ID**. For example, if your Windchill Server's hostname is **WINDCHILL01**, the **System ID** must also be WINDCHILL01 when configuring it with the HaloCAD Configuration Tool. The same name must also be supplied in the System Unique ID field.

HaloCAD for Keytech

For example, if you specify the **System Unique ID** as **KEYTECH01**, then the same ID must be used in the HaloCAD Configuration Tool (System ID=KEYTECH01) while configuring its properties.

HaloCAD for Autodesk Vault

Here, the hostname of the Vault Server that is specified during HaloCAD for AutoDesk configuration must be the **System Unique ID**. For example, if your Vault Server's hostname is **VAULTCLNT01**, the **System ID** must also be VAULTCLNT01 when configuring it with the HaloCAD Configuration Tool. The same name must also be supplied in the System Unique ID field.

HaloCAD for SOLIDWORKS PDM

For example, if you specify the **System Unique ID** as **SWDPDM01**, then the same ID must be used while executing the installer (System ID=SWDPDM01).

HaloENGINE_API

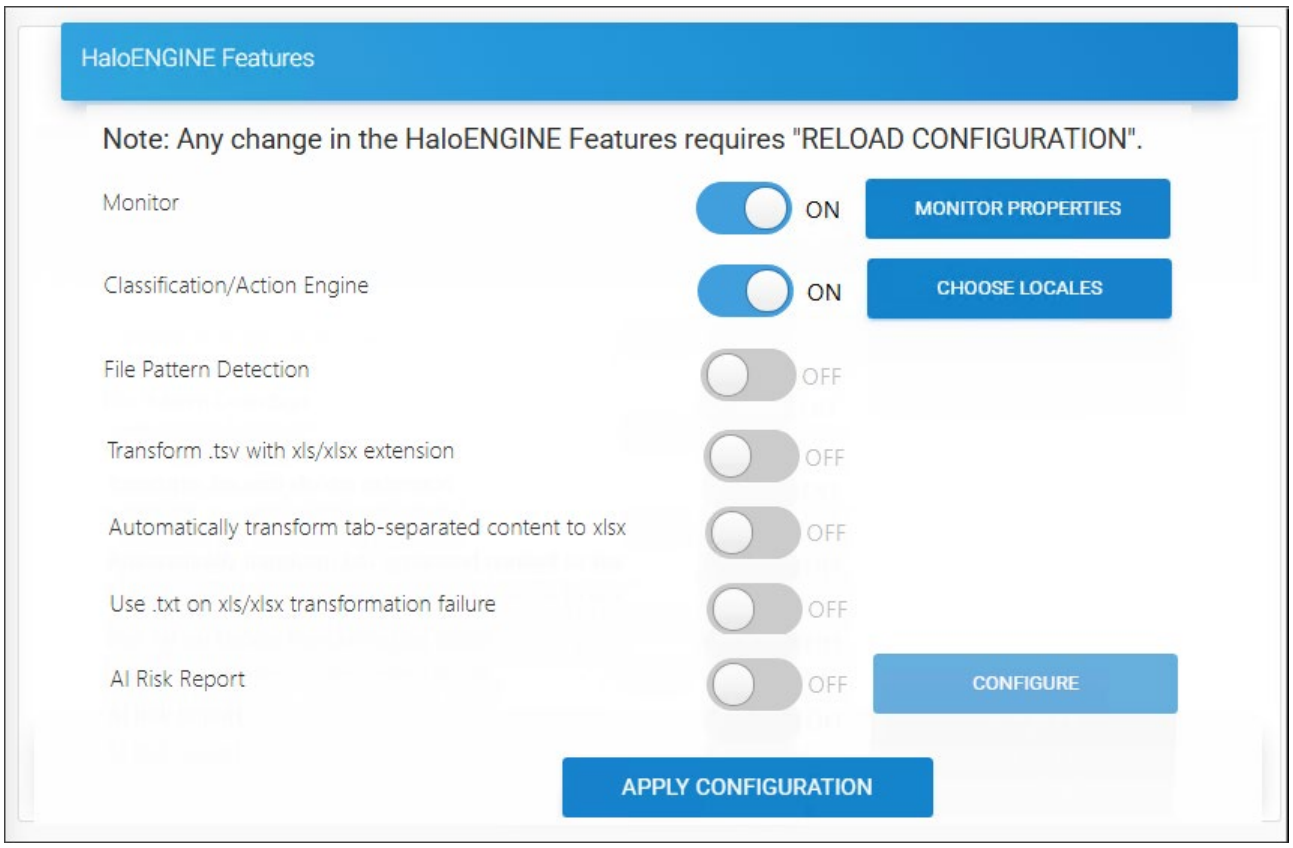
For example, if you set the System Unique ID to **RESTclient** (System ID=RESTclient), the same ID must be used when calling the APIs.

3.5.12. Phase 8. Configure HaloENGINE Features

For any type of licensed system, the first step is to enable the monitor.

Prerequisite: Verify that the HaloENGINE license is active. Refer to the section "Phase 3. Activate License (First time)".

1. On the left navigation bar, click **Customer Configuration**, and then from the **Customers** list, select one of them.
2. On the **HaloENGINE Features** tab, click **Configure**. The *HaloENGINE Features* page will appear as shown in the figure below:



Enable Monitor

3. Enabling the Monitor is the first step.
4. Click on the slider button to enable **Monitor** and then click **Apply Configuration**.

   Results:

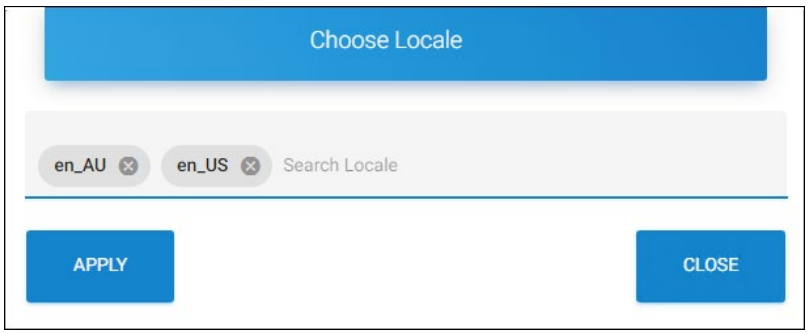
   a. You will receive a confirmation message after changing the default configuration.

   b. Click **Reload Configuration** to make the changes take effect.

3.5.12.1. Enable Classification/Action Engine

Follow the steps below to enable the classification engine:

1. Click on the slider button to enable/disable **Classification/Action Engine**.
2. The **Choose locales** button will be enabled automatically.
3. Click **Choose locales**, *Choose Locale* page will appear as shown in the figure below:



Locales

4. Search and select one or more texts for translation. For example, en_US.
5. Click **Apply**.

   Results:

   a. The chosen texts for translation are added to the list.

   b. You can either press **Apply Configuration** now and then reload configuration to let the changes take effect, or you can configure further settings and then press **Apply Configuration**.

3.5.12.2. Enable File Pattern Detection

Click the slider button to enable **File Pattern Detection**. Once enabled, it will automatically identify the file type by analyzing its structure, format, or extension.

Assume that a Word file is uploaded and downloaded. When a Word file `Sample.docx` is renamed to `Sample.txt` and the File Pattern Detection option is enabled, HaloENGINE will check and transmit the result to the HaloENGINE Service that the file pattern is Word, but the extension is different. Thus, it is protected as Sample.docx by HaloENGINE Service.

On the other hand, HaloENGINE will simply send the file to HaloENGINE Service without examining it if File Pattern Detection is turned off. Thus, HaloENGINE Service will protect it as `Sample.ptxt.`

3.5.12.3. Enable Excel Conversion

Note: If you only have a license for the **Block** and **Monitor** feature, the following options will be disabled.

Follow the steps below to configure an Excel file download:

1. **Transform `.tsv` with xls/xlsx extension** – To transform tab-separated text files (`.tsv`) named as `.xls/xlsx` to proper `.xls` /`.xlsx` files, click on the slider button.
2. **Automatically transform tab-separated content to xlsx** – To transform tab-separated text files (`.tsv`) independent of the extension and convert to XLSX automatically, click on the slider button.
3. **Use .txt on xls/xlsx transformation failure** – If the conversion of a `.tsv/.txt` file to a native XLS/XLSX file fails, the exported file will get labeled as `.txt`.

4. When you complete the HaloENGINE configuration, click **Apply Configuration**.
5. **What to do next**: Click **Reload Configuration** for the changes to take effect. The page will be redirected to the login page once the reload completes.

Dependencies among features

1. It is possible to enable other HaloENGINE features only if **Monitor** is enabled.
2. Similarly, it is possible to enable "File Pattern Detection", "Automatically transform tab-separated content to xlsx", "Transform `.tsv` with `xls/xlsx` extension" and Use `.txt` on `xls/xlsx` transformation failure options, only if **Classification/Action Engine** is enabled.
3. Also, please note that activating the "Automatically transform tab-separated content to xlsx" option or Use `.txt` on `xls/xlsx` transformation failure will automatically activate the "Transform `.tsv` with `xls/xlsx` extension" option.
4. And deactivating "Transform `.tsv` with `xls/xlsx` extension" option will automatically deactivate the "Automatically transform tab-separated content to xlsx" option and use `.txt` on `xls/xlsx` transformation failure option.
5. Meanwhile, the "Transform `.tsv` with `xls/xlsx` extension" option can be stand-alone activated.

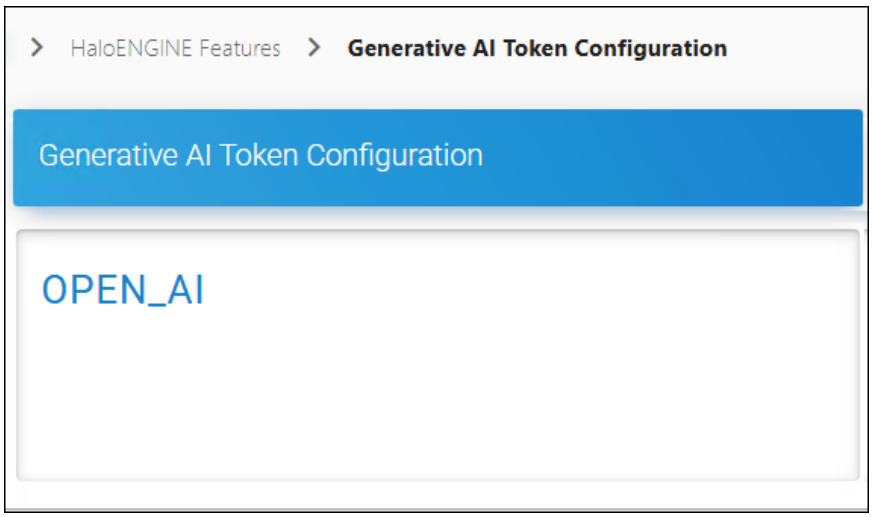
3.5.12.4. Generate Risk Reports

HaloCORE and HaloENGINE extend their support for generating risk reports based on user prompts, integrating with the OpenAI API. This is a licensed functionality that is currently only available on SAP.

Prerequisite: Ensure that you have an account on this platform https://platform.openai.com/docs/overview and get a key. This API key is required for communication between HaloENGINE and OpenAI.

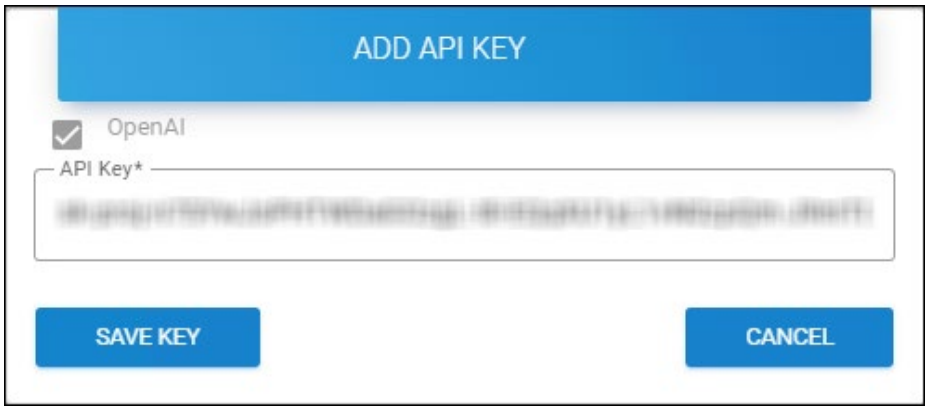
Follow the steps below to create a risk report:

1. Click on the slider button to activate the **AI Risk Report**. You will note that the **Configure** button is also enabled.
2. Click the **Configure** button.
3. The *Generative AI Token Configuration* page will appear as illustrated in the figure below.



Generative AI Token Configuration page

4. Click **Open AI**.
5. Click on the plus icon, and the *Add API Key* page will appear as shown in the figure below:



Adding the API key

6. Enter the registered key and click **Save** Key.

   Results:

   a. You will receive a confirmation message after successfully saving the key.

   b. Using the appropriate icons, you can also edit or delete the key.

   c. Reload the HaloENGINE Admin portal after registering the key.

   d. Please refer to the HaloCORE manual for more information on how to download the risk report.

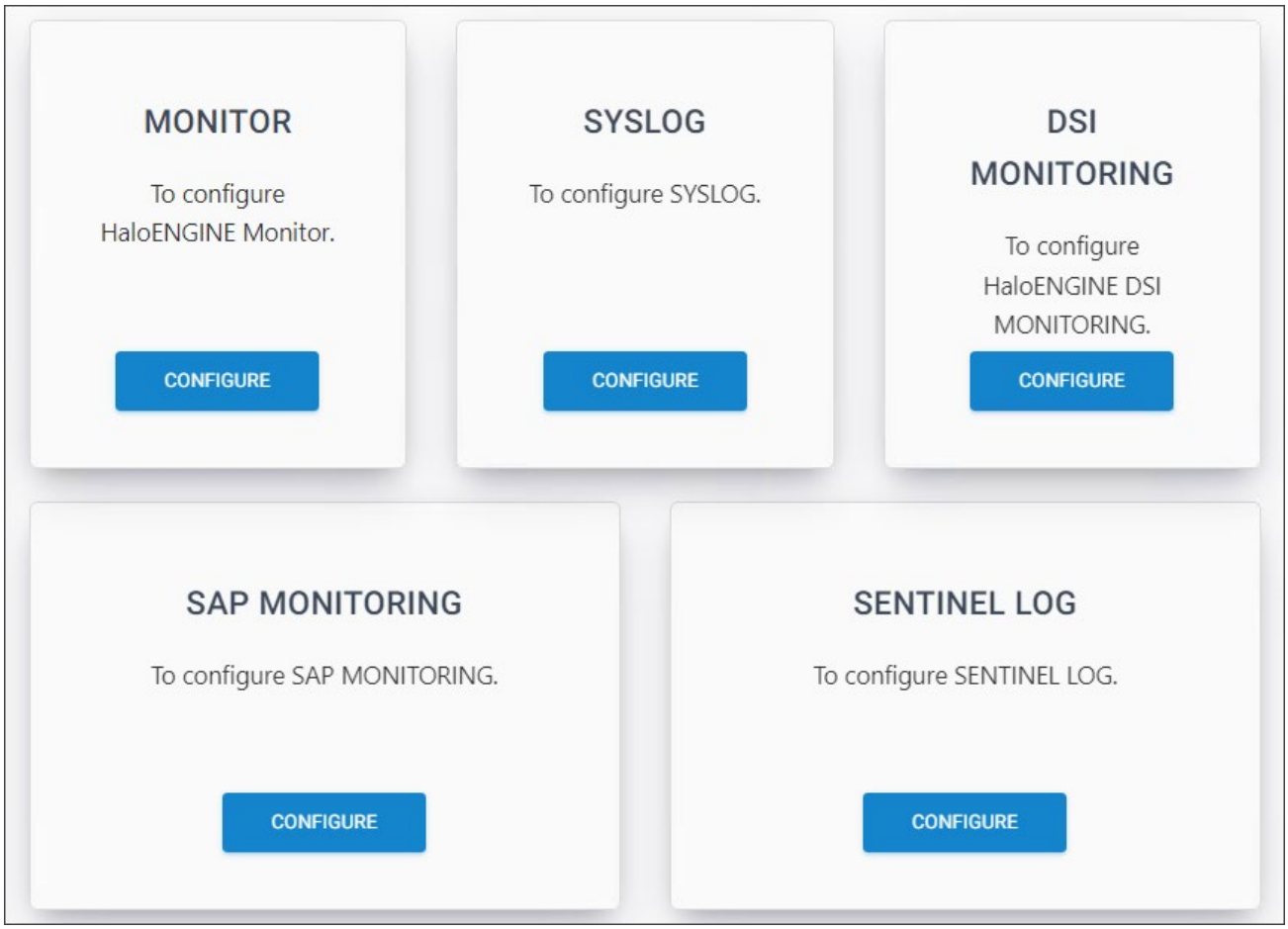
3.5.12.5. Monitor Configuration

Prerequisite: As mentioned in the section above, ensure that Monitor is enabled.

Note: SAP Monitoring and Sentinel Log options are only applicable to SAP system types. This means that if you are licensed for other system types, these two options will be disabled.

Follow the steps below to configure the Monitor:

1. On the *HaloENGINE Features* page, click **Monitor Properties**.
2. The *Monitor Configuration* page will appear as shown in the figure below:



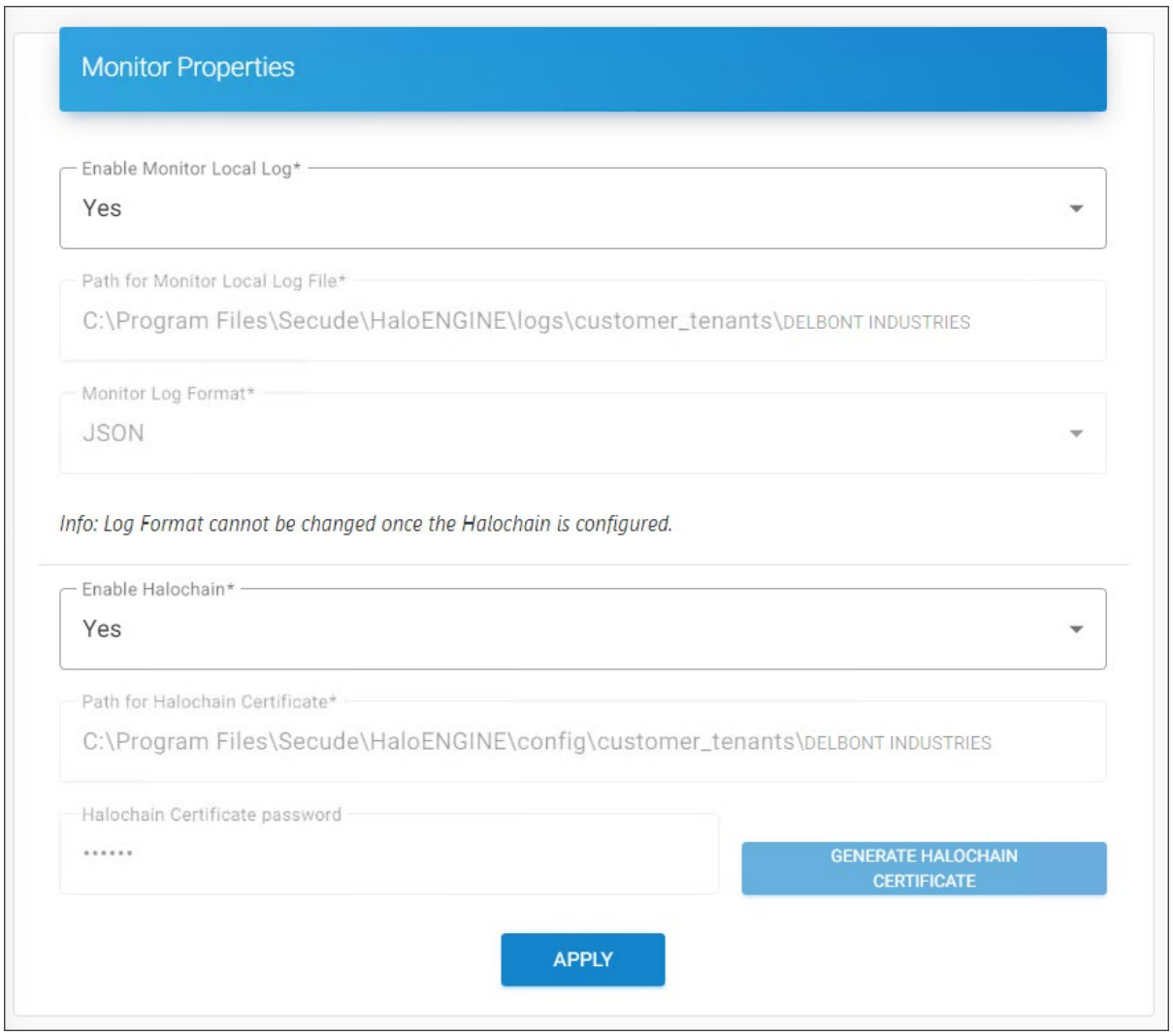
Monitor Configuration

3. You need to configure Monitor, Syslog, DSI Monitoring, SAP Monitoring, and Sentinel Log one by one, by referring to the following sections.

3.5.12.5.1.Monitor Properties

Follow the below steps to configure the monitor properties:

1. On the **Monitor** tab, click **Configure** and then enter the following details on the *Monitor Properties* page as shown in the figure below:



Monitor Log Configuration

2. **Enable Monitor Local Log** – Choose **Yes**/**No** to enable/disable the local monitor log. If enabled, the default path for **Single Customer** – `C:\Program Files\Secude\HaloENGINE\logs\customer_tenants\halo_customer` and for **Multi-Customer** – The path varies based on the customer IDs. For example: `C:\Program Files\Secude\HaloENGINE\logs\customer_tenants\DELBONT INDUSTRIES`.
3. **Monitor Log Format** – Choose one of the following monitor log formats (CEF/LEEF/JSON). Please note that it is not possible to change the log format once the Halochain is configured and the field will be disabled once you enable Halochain.
4. **Enable Halochain** – Choose **Yes**/**No** to enable/disable the **Halochain** feature. If enabled, the default Halochain certificate path for **Single Customer** – `C:\Program Files\Secude\HaloENGINE\config\customer_tenants\halo_customer` and **Multi-Customer** – The path varies based on the customer IDs. For example: `C:\Program Files\Secude\HaloENGINE\config\customer_tenants\DELBONT INDUSTRIES`.

5. **Halochain Certificate Password** – Enter a password for Halochain and click **Generate Halochain Certificate**. You will receive a confirmation message on creating a certificate.
6. Click **Apply**.

   Results: You will receive a confirmation message after successfully updating the properties.

3.5.12.5.2.Syslog Properties

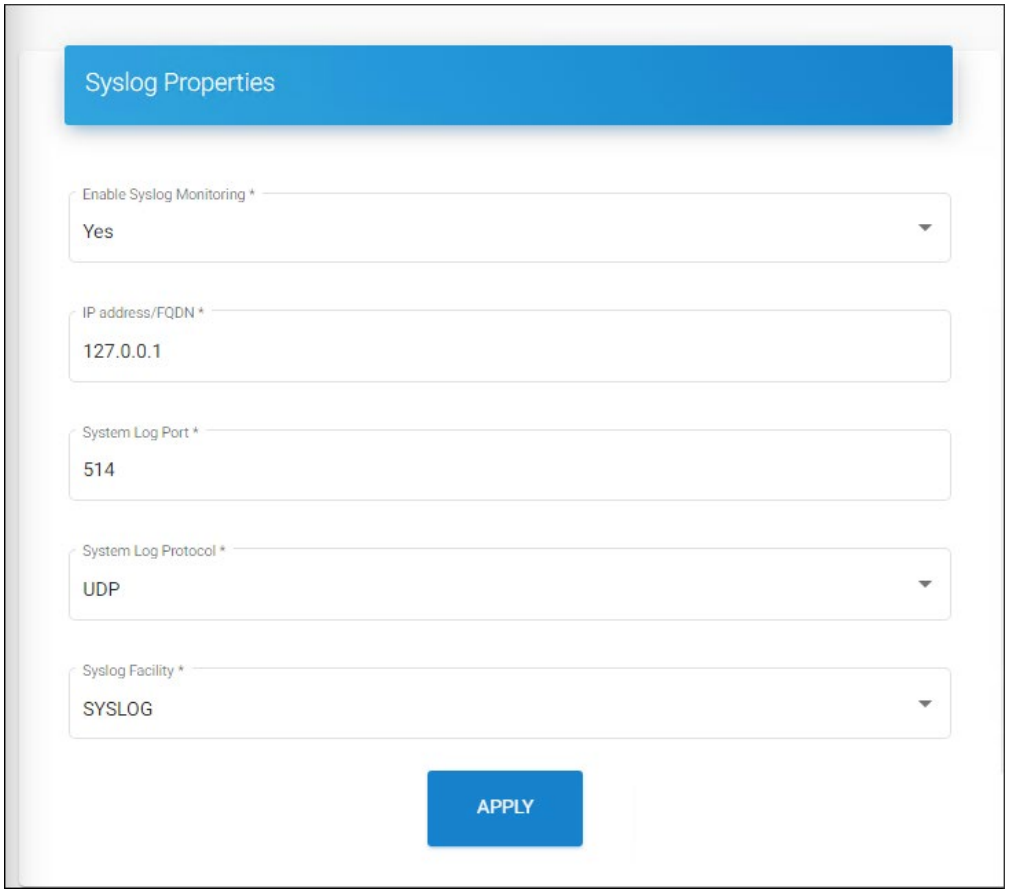
Syslog Requirements

Please make sure that the following requirements are met:

1. UDP/TCP enabled.
2. The firewall accepts UDP/TCP packets on the configured port.
3. To forward audit logs to SPLUNK/RSA, you need to configure the audit Syslog accordingly.

Follow the below steps to configure the Syslog properties:

1. On the **Syslog** tab, click **Configure** and then enter the following details on the **Syslog Properties** page as shown in the figure below:



Syslog Properties

2. **Enable Syslog Monitoring** – Choose **Yes**/**No** to enable/disable Syslog.

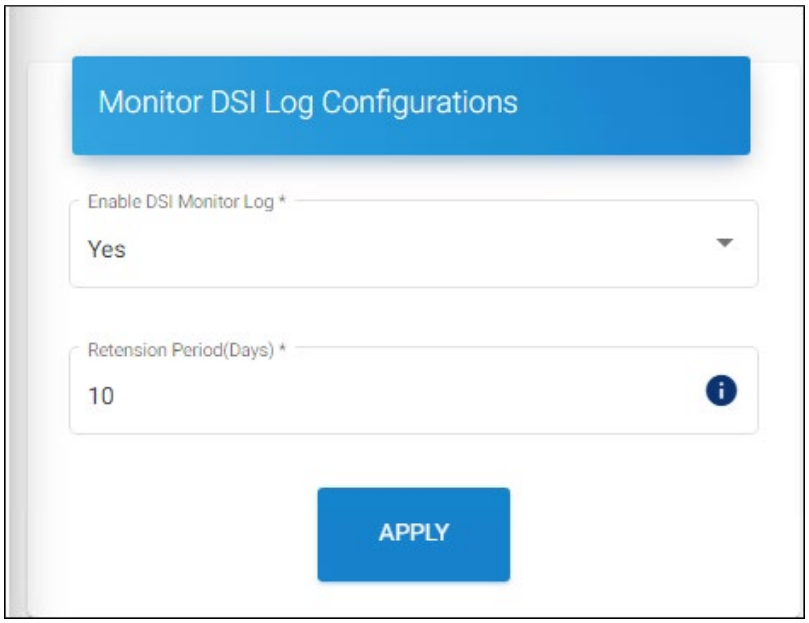
3. **IP Address/FQDN** – If enabled, enter the IP address/FQDN.
4. **System Log Port** – Enter the system log port number. The default port is 514.
5. **System Log Protocol** – Enter the system log protocol (UDP/TCP). The default protocol is UDP.
6. **Syslog Facility** – Enter the Syslog facility (KERN/USER/SYSLOG/AUDIT). The default facility is SYSLOG.
7. Click **Apply**.

   Results: You will receive a confirmation message after successfully updating the properties.

DSI Monitoring

Follow the below steps to configure the DSI monitoring properties:

1. On the **DSI Monitoring** tab, click **Configure** and then enter the following details on the *Monitor DSI Log Configurations* as shown in the figure below:



DSI Monitoring

2. **Enable DSI Monitor Log** – Choose **Yes**/**No** to enable/disable the DSI Monitor log.
3. **Retention Period (Days)** – Specify how long the logs should be available.
4. Forwarded DSI logs from SAP are stored in the `HaloENGINE_DSI.log` file.
5. Click **Apply**.

   Results: You will receive a confirmation message after successfully updating the properties.

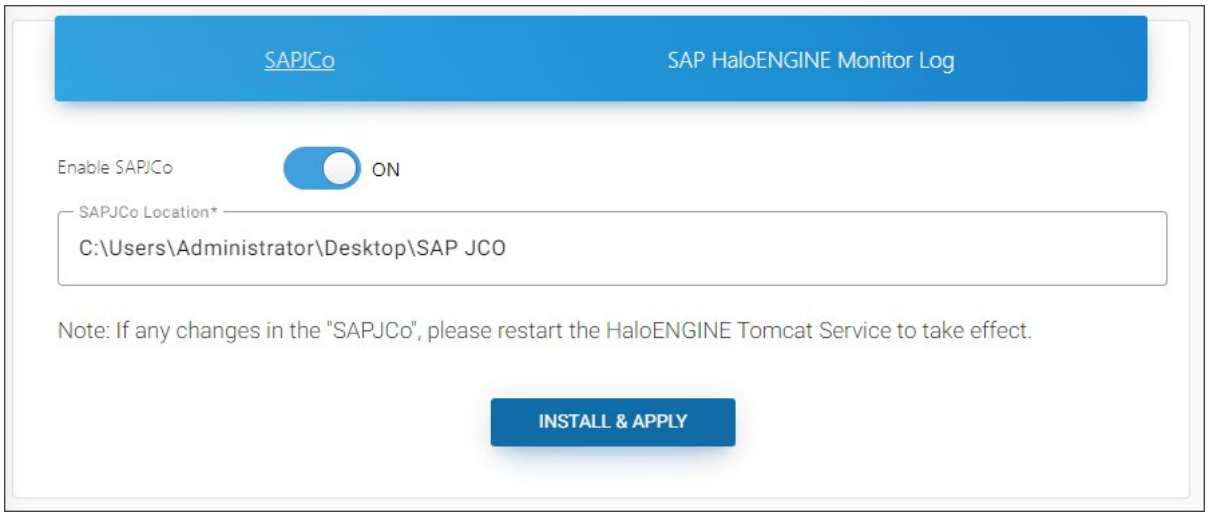
3.5.12.5.3.SAP Monitoring

SAP Monitoring applies to SAP system types and allows you to configure monitor features.

SAPJCo Configuration

SAPJCo is the component that connects HaloENGINE with your SAP instance.

1. Select the **SAP Monitoring** tab to install or update SAPJCo.



SAPJCo configuration page

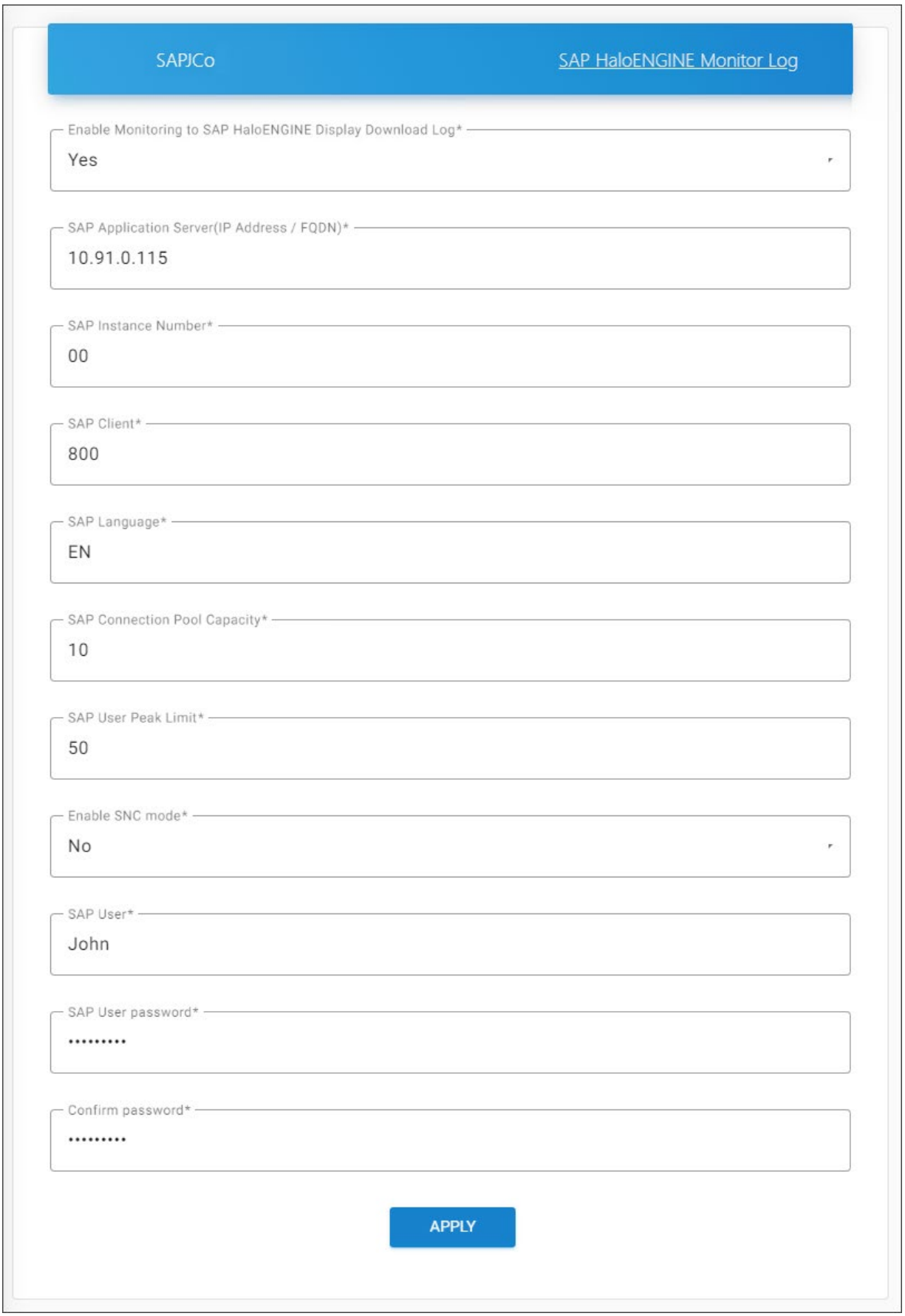
2. **To Install**: Click on the slider button and enter the file path of SAP JCo files.
3. **To update**: Disable the slider button and then enable it. Now, specify the new file path.
4. Click **Install & Apply.**

   Results: You will receive a confirmation message after successfully updating the properties.

SAP HaloENGINE Monitor Log

Follow the below steps to configure the SAP monitoring properties:

1. Click the **SAP Monitoring** tab and enter the following details on the **SAP HaloENGINE Monitor Log** page, as shown in the figure below:



SAP Monitoring

2. **Enable Monitoring to SAP HaloENGINE Display Download Log** – Choose **Yes/No** to enable/disable SAP HaloENGINE Monitor Log.
3. **SAP Application Server (IP Address / FQDN)** – Enter the SAP application server name. For example, `10.91.0.115` or `SLUV0001.secude-sap.com`
4. **SAP Instance Number** – Enter the SAP instance number. The default number is 00.
5. **SAP Client** – Enter the SAP client. The default client is 800.
6. **SAP Language** – Enter the SAP language. The default language is EN.
7. **SAP Connection Pool Capacity** – Enter the SAP pool capacity. The default capacity is 10.
8. **SAP User Peak Limit** – Enter the SAP user peak limit. The default limit is 50.
9. **Enable SNC mode** – If SNC is disabled, you need to specify the SAP User password and confirm it. If SNC is enabled, you need to specify the following details:
10. Enter **SNC Initiator Name (SNC_MYNAME)**. Based on the certificate details, your default name will be populated automatically. For example, `p:CN=HCCS, O=SECUDE, C=CH`
11. Enter **Communication Partner (SNC_PARTNERNAME)**. For example, `p:CN=SAP, O=SECUDE, C=CH`
12. Enter **External Security Library Path (SNC_LIB)**. Please note that the environment variable must be set manually. For more details, please refer to the section "Appendix 1 - SNC Configuration (Step 4)".
13. Choose any one of the **Quality of Protection Level (SNC_QOP)** settings. (1 - Authentication only, 2 - Integrity protection, 3 - Privacy protection, 8 - Protection (default), 9 - Maximum protection)
14. Click **Apply**.

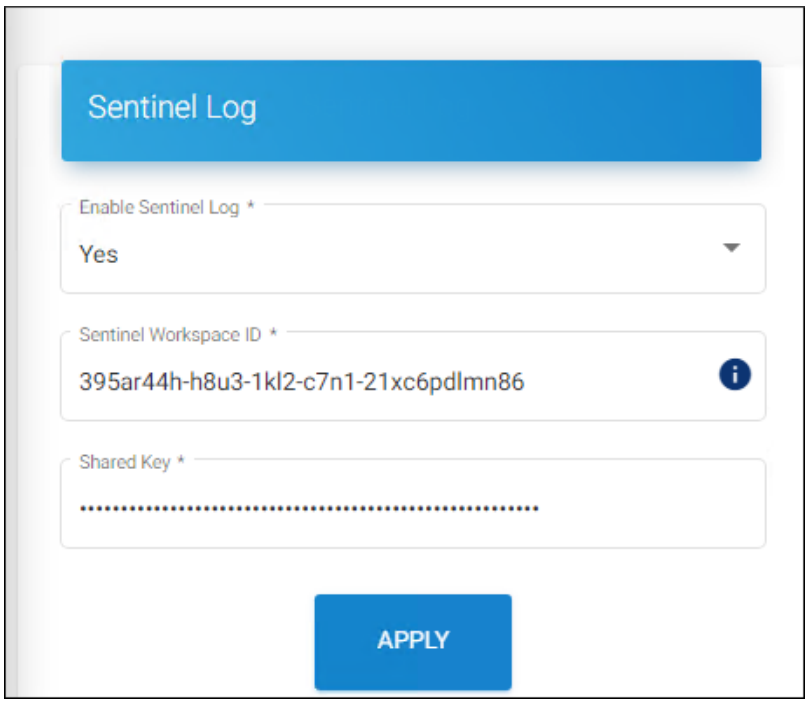
    Results: You will receive a confirmation message after successfully updating the properties.

3.5.12.5.4.Sentinel Log

Prerequisite: Microsoft Sentinel must be configured. Please refer to the section "Forwarding Logs to Microsoft Sentinel".

Follow the below steps to configure the Sentinel log properties:

1. Click the **Sentinel Log** tab and enter the following details in the **Sentinel Log** dialog as shown in the figure below:



Sentinel Log

2. **Enable Sentinel Log** – Choose **Yes/No** to enable/disable Sentinel Log.
3. **Sentinel Workspace ID** – Enter the **Workspace ID** of your Microsoft Entra ID. For example, `395ar44h-h8u3-1kl2-c7n1-21xc6pdlmn86`.
4. **Shared Key** – Enter the **Primary Key** of your **Workspace ID.** For example, `/mjnjgjbKIUTv5M/FJDBFDmdfnidfidi8ujsasusd09uu=ndhdihdkij`.
5. Click **Apply**.

   Results: You will receive a confirmation message after successfully updating the properties.

What to do next

Test the log after configuration.

Prerequisites:

1. Make sure that the HaloENGINE admin portal is restarted after configuring Sentinel properties.
2. Make sure that actions like uploading and downloading take place after the admin portal has been configured so that a sufficient number of logs can be obtained and forwarded.

Follow the steps to obtain logs in Microsoft Sentinel.

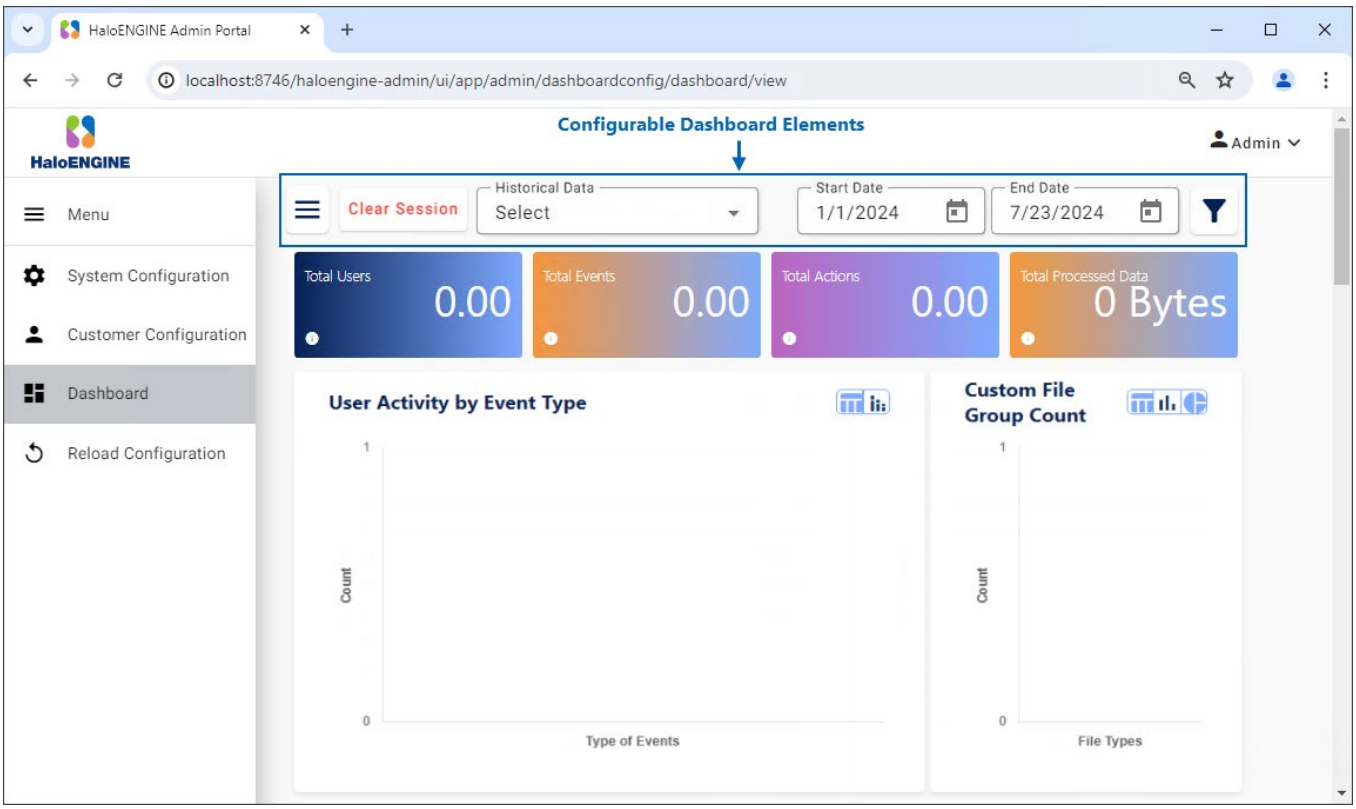
1. Log in to the Microsoft Azure portal.
2. On the search bar, type **Microsoft Sentinel**. As you start typing, the list filters according to your input.
3. Select **Microsoft Sentinel** from the search results.
4. The **Microsoft Sentinel** page will appear. Here, you need to click **Create** from the top of the page.
5. The page displays available workspaces.

6. Select your workspace.
7. Navigate to **General** > **Logs**. Forwarded logs will be stored in the `HALOCORE_CL` table.
8. Type `HALOCORE_CL` in the right-side query panel. As you start typing, the list filters based on your input.
9. Select the table `HALOCORE_CL` and choose the appropriate query to fetch the logs. For example. where `action_s contains ""`
10. Run it to get the results.
11. Based on the query applied, logs will be retrieved.

3.5.13. Phase 9. Monitor Log Dashboard

The HaloENGINE dashboard is an information management tool that visually monitors and displays important performance indicators and metrics, providing an overview of your company's data upload and download events. It uses tables, graphs, charts, and other visual components to display data. HaloENGINE may be viewed and updated in real-time, giving users accurate and up-to-date information when they need it. It is also possible to load a previously generated log file into the dashboard to get a visual picture.

As a prerequisite, make sure the database connection has been established. On the left navigation bar, click **Dashboard**. The following page is the default view. Note: If you receive a "*Failed to get data*" connection error, MongoDB may not have been installed or started yet. In that case, install MongoDB and/or start it manually.



Default dashboard view

You can use several elements available in the dashboard user interface to personalize how your data is presented. The dashboard allows you to see both persistent and non-persistent logs.

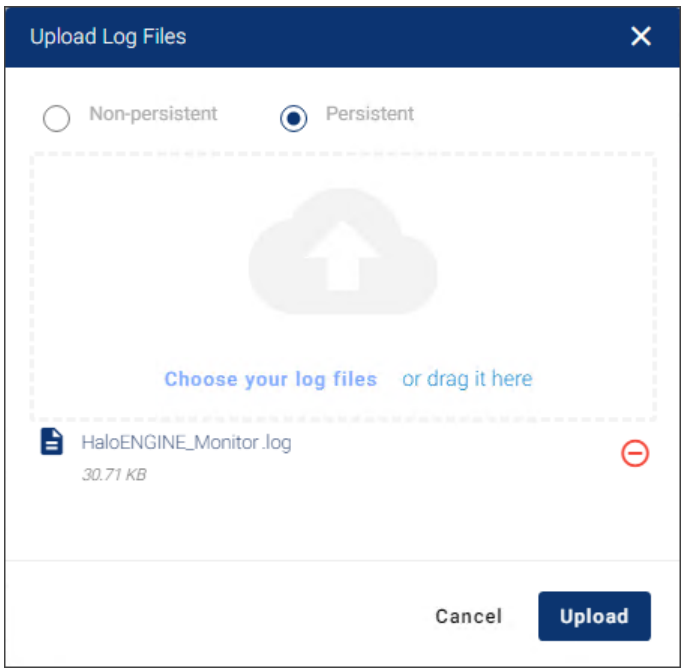
Persistent log: This is real-time log data obtained directly from the HaloENGINE log files. If you want to review a log file permanently, you can upload it using the **Upload Logs** option. These logs are then displayed in the Historical Data section.

Non-persistent log: This option is useful when you need to access a previously saved log file or a log file from another HaloENGINE. Such log files can be uploaded using the **Upload Logs** option.

3.5.13.1. Upload Logs

Follow the steps below to upload a log file for both persistent and non-persistent options.

1. Click the **Menu** icon and then **Upload Logs**.
2. The *Upload Log Files* page will appear as shown in the figure below:



Upload log files

3. Select either the **Non-persistent** or **Persistent** option.
4. Upload or drag your log files to the page.
5. The name of the uploaded log files will appear in the list. If you want to remove an uploaded file, click the **Remove this file** icon.
6. Click **Upload**.

   Results:

   a. You will receive a confirmation message after successfully uploading the logs.

   b. The dashboard presents the uploaded log file with visual features.

   c. The populated data can be filtered by Historical Data, Products, and Date Range.

3.5.13.2. Customization

Dashboard logs allow users to customize the layout, design, and information based on their preferences. You can change the chart's layout or style by clicking on the Grid, Bar, or Pie elements.

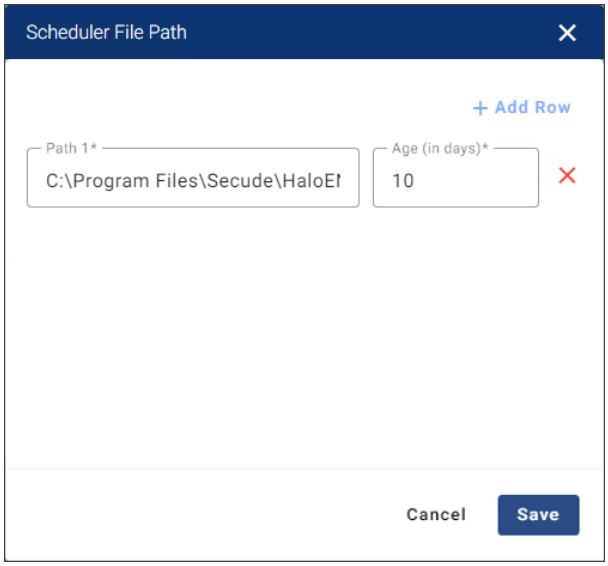
1. The uploaded log IDs will appear in the list of **Historical Data**. By selecting one ID, the dashboard will automatically visualize the specified log entry. If you want to remove the uploaded data, click the **Delete** icon.
2. By selecting the **Start Date** and **End Date** in the calendar, the logged items will be displayed within that timeframe.
3. By clicking the **More Filters** icon, you can filter the Products, Events, Actions, Source Type, and Sensitivity Labels.

4. If you want to clear the filtered/selected data, click the **Clear Filters** button.
5. If you want to remove the uploaded Non-persistent log data, click the **Clear Session** button.

3.5.13.3. Scheduler

This option allows you to define the number of days the logs in the specified path should be maintained. Upon reaching a specified number of days, the logs will be automatically deleted from the MongoDB database.

1. Click on the **Scheduler**, the *Scheduler File Path* page will appear as shown in the figure below:



Scheduler file path

2. Click **+Add Row**, the fields will be visible on the page.
3. Enter the log path in **Path**. For example: `C:\Program Files\Secude\HaloENGINE\logs\customer_tenants\DELBONT INDUSTRIES`
4. Enter the number of days in **Age** that the log should be kept. For example: 10
5. Click **Save**.

   Results:

   a. You will receive a confirmation message after successfully configuring the scheduler.

   b. The logs will be cleared after 10 days.

   c. To add additional paths, click **+Add Row** and enter the information described above.

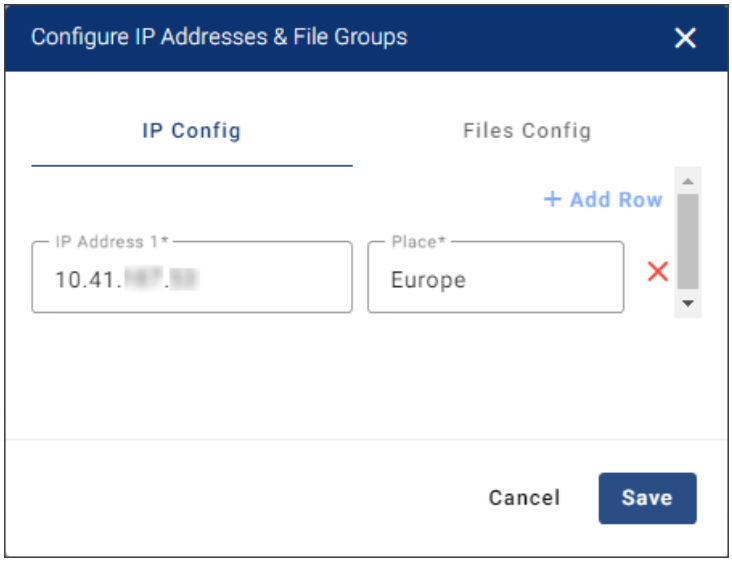
   d. To remove a path, click the remove “X” icon.

3.5.13.4. Configure IP and Files

IP Config

This option allows you to specify the geographical location of the log entries. For example, if the U.S. is specified, log items associated with that region will be highlighted.

1. Click on the **Configure IP and Files**, and the *Configure IP Address & File Groups page* will appear as shown in the figure below:



IP Config

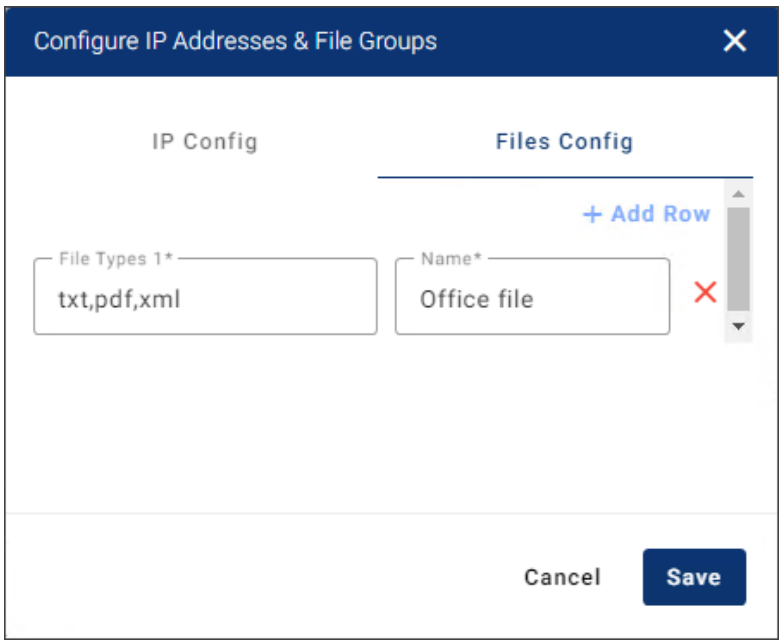
2. Click **+Add Row**, the fields will be visible on the page.
3. Click the **IP Config** tab and enter the IP address and place. For Example:
   a. **IP Address**: `10.41.*.*`
   b. **Place**: `Europe`
4. Click **Save**.

   Results:
   a. The IP Address data will be shown on the dashboard based on the provided log files.
   b. To enter more IP addresses, click **+Add Row** and enter the details as above.
   c. To remove an IP address, click the **Remove** icon.

Files Config

This option allows you to define file types. For example, if pdf is specified, log items that correspond to this file type will be highlighted.

1. Click on the **Configure IP and Files**, and select the **Files Config** tab.



Files Config

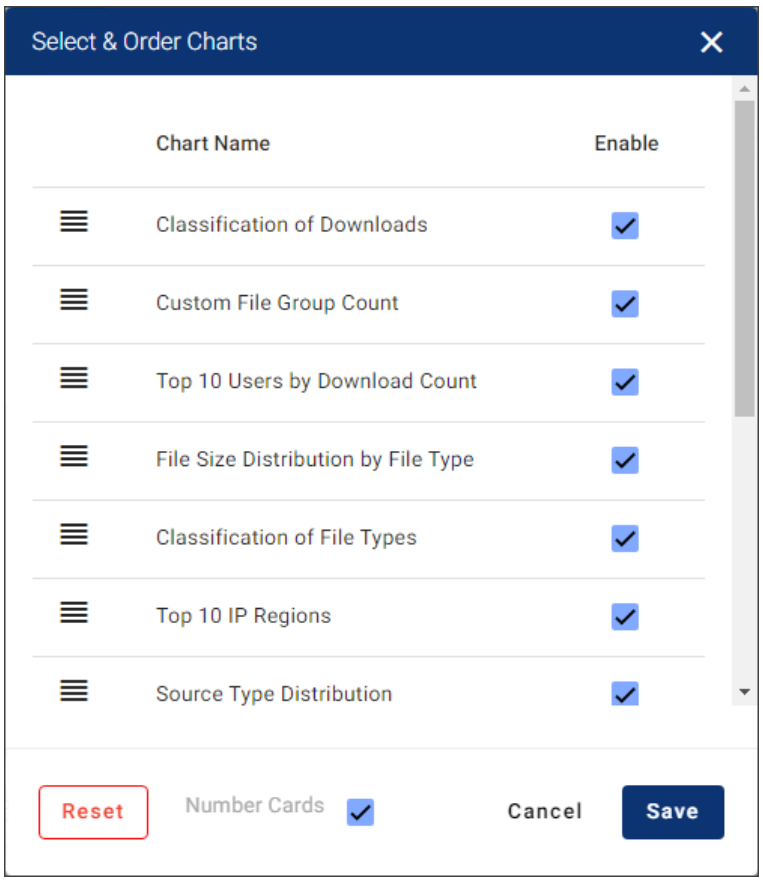
2. Click **+Add Row**, the fields will be visible on the page.
3. Enter the file types and name of the file types. For Example:
   a. **File Types**: `txt`, `pdf`, `xml`
   b. **Name**: Office file
4. Click **Save**.

   Results:
   a. The file type data will be shown on the dashboard based on the provided log files.
   b. To enter more file types, click **+Add Row** and enter the details as above.
   c. To remove file types, click the **Remove** icon.

3.5.13.5. Select Charts

This option allows you to enable/disable the charts that will appear on the dashboard. You can rearrange the charts by dragging them in any order you prefer.

1. Click on the **Select Charts**, and the *Select & Order Charts* page will appear as shown in the figure below:



Select charts

2. Select the **Enable** checkbox next to each chart you want to appear on the dashboard, and then drag and drop them into the order you want them to appear.
3. Click **Save**.

   Results:

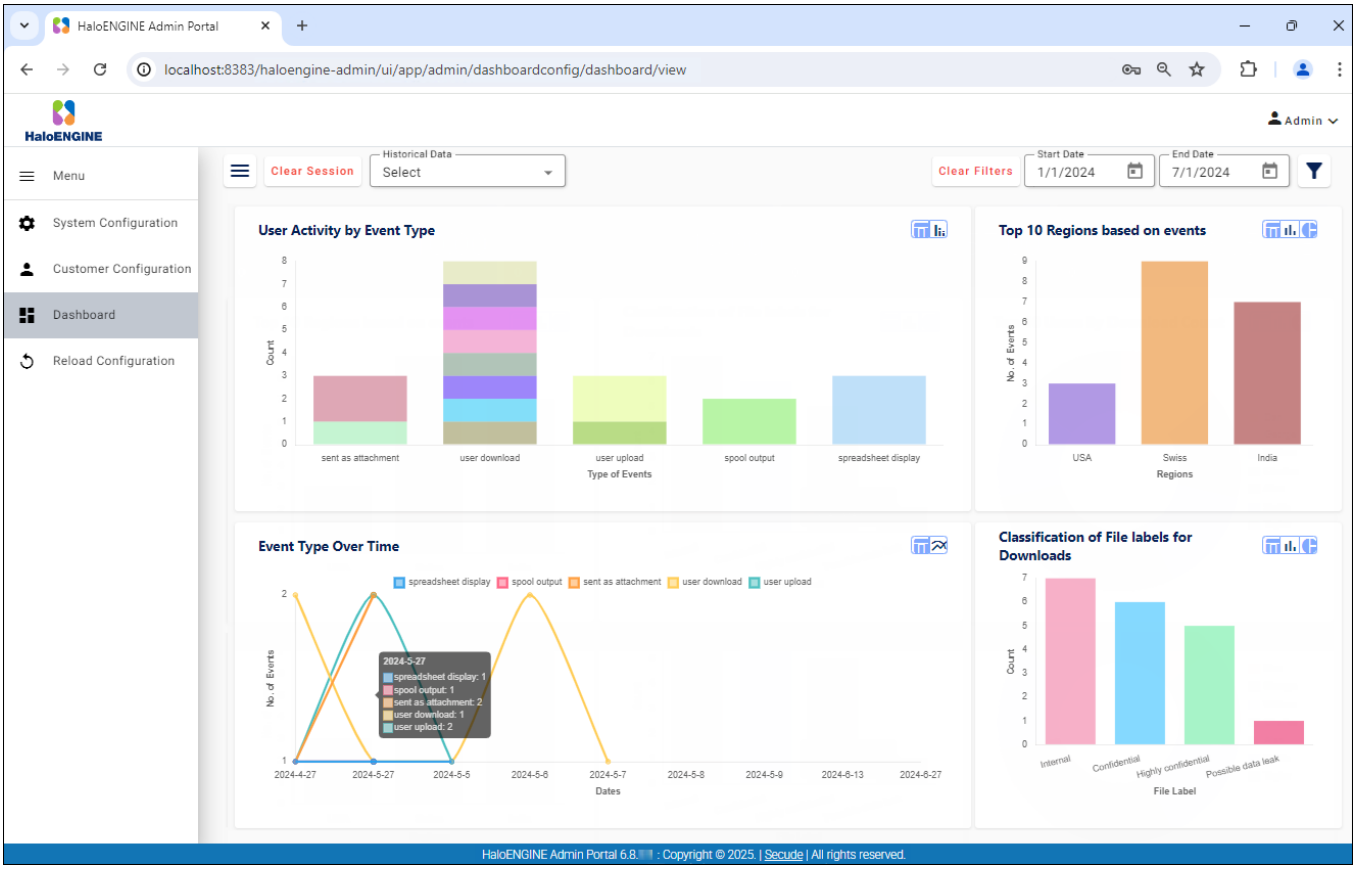
   a. You will receive a confirmation message after successfully configuring the chart order.

   b. The charts will be displayed in the given order.

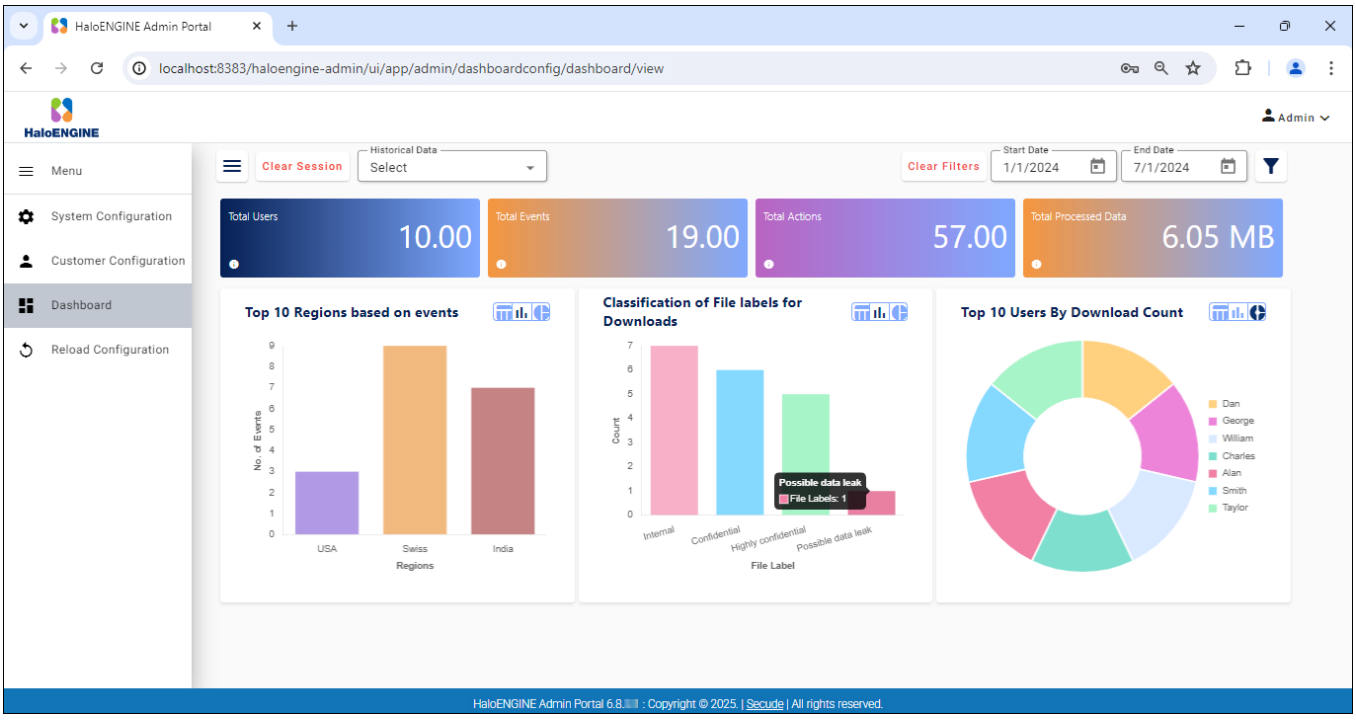
   c. To restore the charts to the default view, click **Reset**. You will receive a confirmation message saying "*Are you sure you want to reset to default*" click **Yes** to confirm.

   d. Number Cards are displayed at the top of the dashboard to show the records. Key metrics such as total users, total events, total actions, and total processed data are displayed. Select the **Number Cards** check box to display the cards, or uncheck it to hide them.

3.5.13.6. Sample Screens



Sample 1



Sample 2

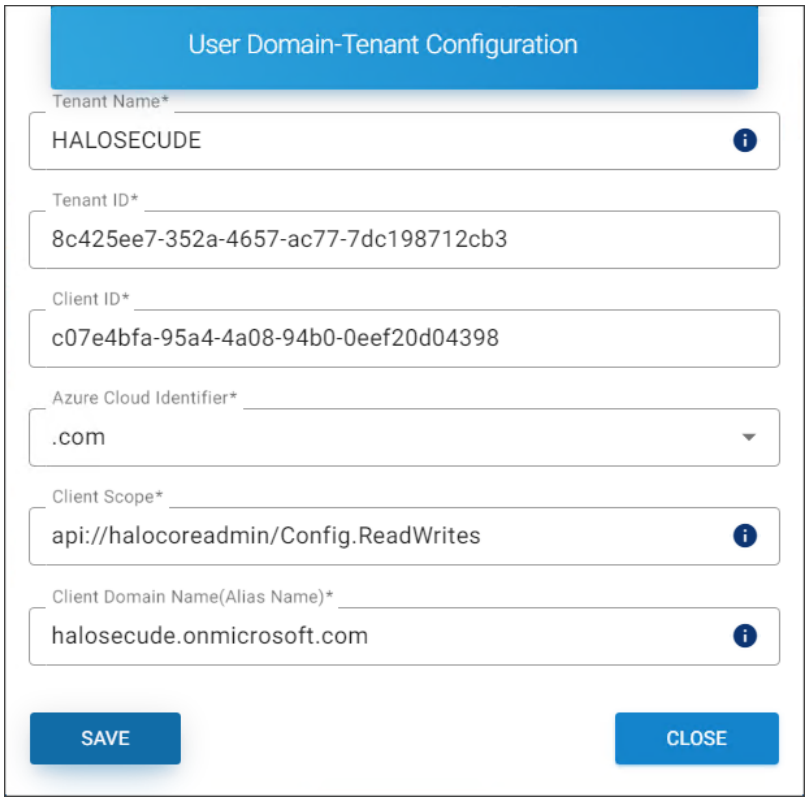
3.5.14. Phase 10. Tenant Configuration

Prerequisite: Make sure that you have configured the required details as described in the section "Settings in Azure Portal".

For user authentication and validation, you need to register the domain details as instructed below:

1. On the left navigation bar, click **Customer Configuration**, and then from the **Customers** list, select one of them.
2. On the **Tenant Configuration** tab, click **Configure**.
3. Click the plus icon, and the *User Domain-Tenant Configuration* page will appear as shown in the figure below:

   Note: The values displayed on the example screen are altered for security reasons.



Registering a domain page

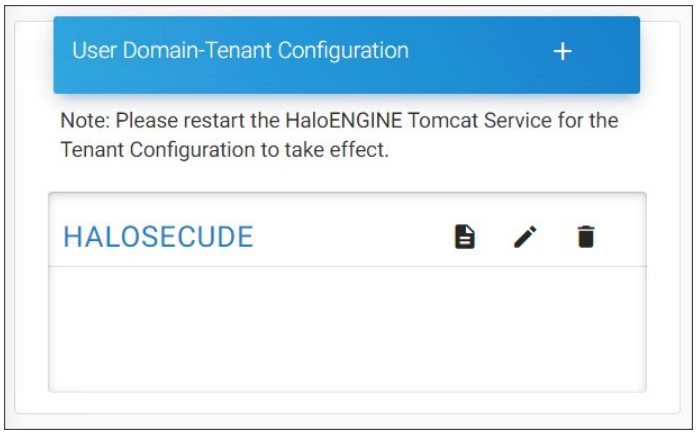
4. **Tenant Name** – Enter the name of your Microsoft Entra tenant. Note: Maximum 30 characters, alphanumeric characters, hyphen, and underscore are only allowed. For example, `HALOSECUDE`
5. **Tenant ID** – Enter the unique identifier of your Microsoft Entra ID instance. For example, `8c425ee7-352a-4657-ac77-7dc198712cb3`
6. **Client ID** – Enter the identifier that is assigned when registering the application. For example, `c07e4bfa-95a4-4a08-94b0-0eef20d04398`
7. **Azure Cloud Identifier** – Select the identifier from the list. For example: `.com`, `.us`

8. **Client Scope** – Enter the scope assigned to the application. For example, `api://halocoreadmin/Config.ReadWrites`
9. **Client Domain Name (Alias Name)** – Enter an alias name for your domain. For example, `halosecude.onmicrosoft.com`.
10. Click **Save** and repeat the above steps to register other tenants.

Results: You will receive a confirmation message after successfully registering the user domain.

Related tasks:

1. Using the appropriate icons, you can also edit or delete a tenant.
2. If you want to view the tenant details, click the **Tenant Details** icon.
3. You can now see the registered tenants listed under the **User Domain-Tenant Configuration page**.



Registered user domain page

What to do next:

1. Restart the HaloENGINE Tomcat service for the configuration change to take effect.
2. Login using the admin account or user account.

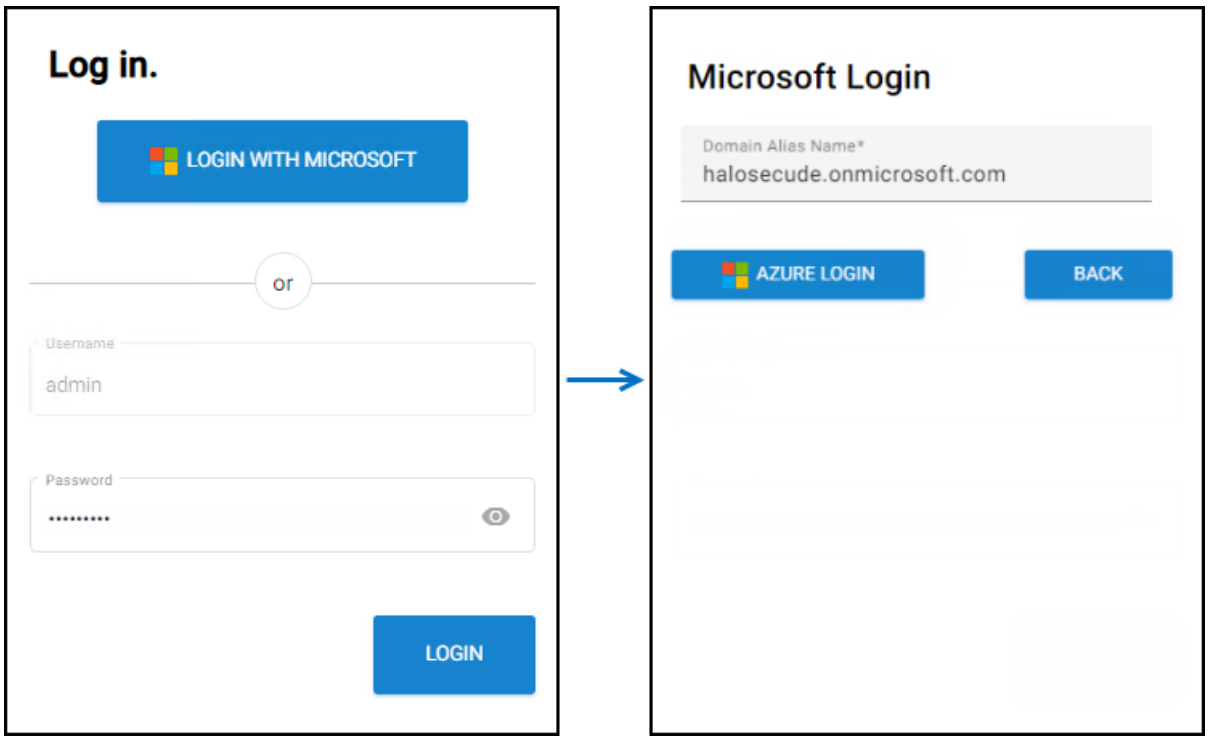
3.5.14.1. User Login (Super Admin / Azure Users)

Once tenant configuration is done and reload is completed, the page will be redirected to the login page. You can select either one of the following options to log in to the portal.

Option 1 – Default Super Admin Account

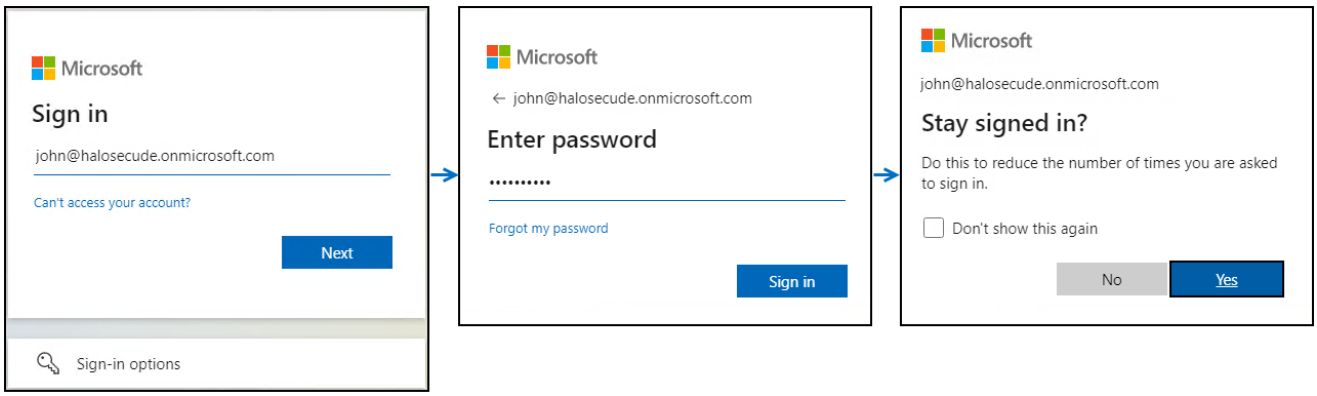
Option 2 – Microsoft account (log in using user account - Customer_Admin or Customer_User)

1. Click on the button **Continue with Microsoft**.



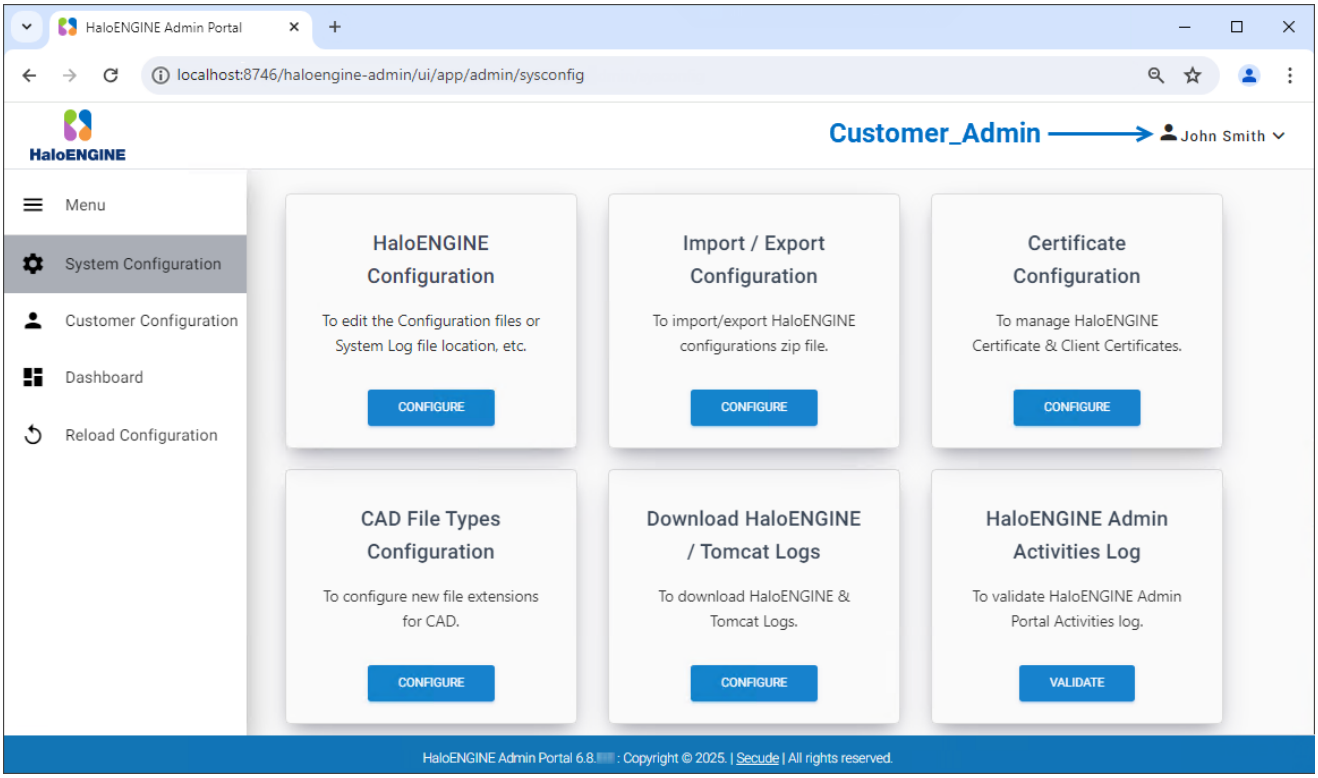
Microsoft Azure Login #1

2. Enter the alias name that is entered in the HaloENGINE Admin Portal and click **Azure Login**.
3. Microsoft Sign-In Assistant requests you to enter the user credentials.
4. Enter your Azure credentials and click **Sign-in**.

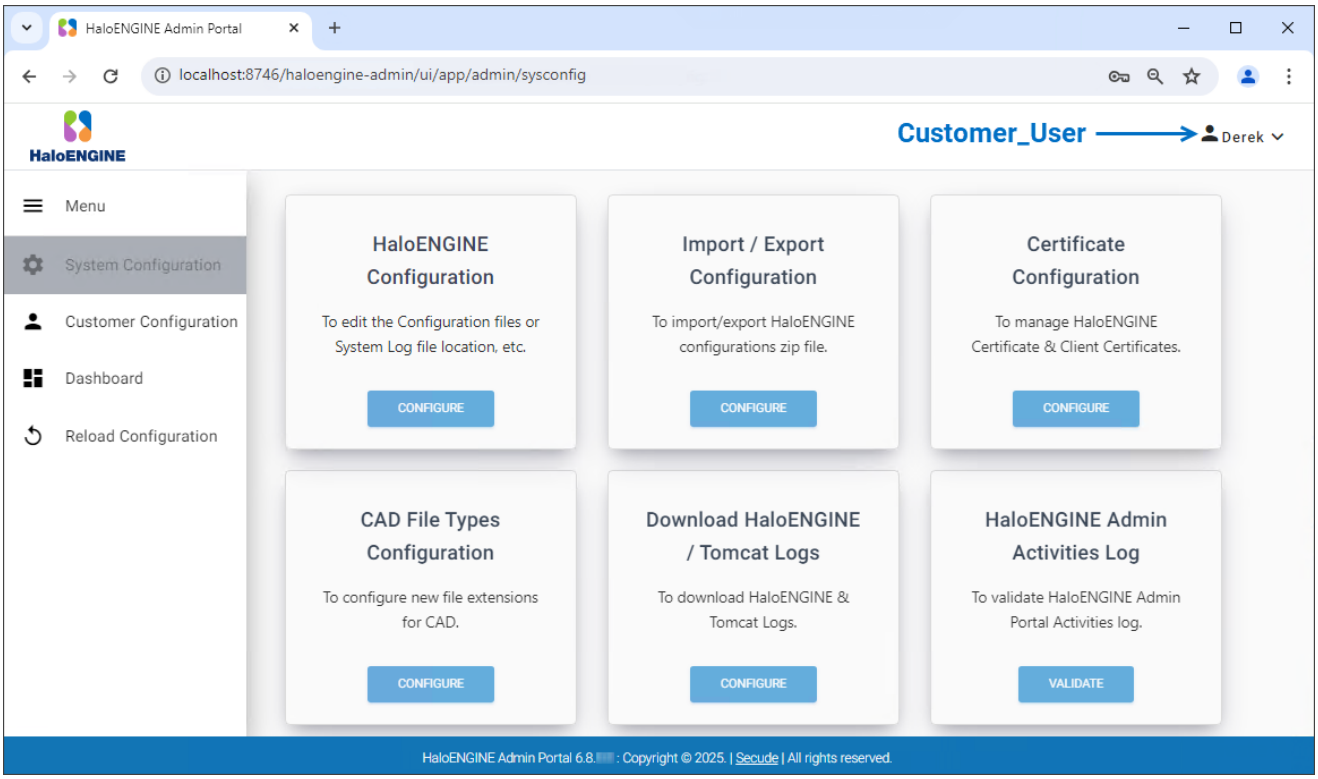


Microsoft Azure Login #2

5. To the question "*Stay signed in?*" click **No**/**Yes** based on your need.
6. After the successful authentication, you will be logged into the portal. Please note that if a user logs into the HaloENGINE Admin Portal using the Azure user account, the access token issued remains valid for a period. Therefore, even if you close the browser, and re-open it or refresh the page, you do not need to enter the credentials again to sign in. However, to enforce the user login, the user must first sign out from the Azure portal.
7. For illustration purposes, user accounts are shown in the below images:



Admin account



User account

Methods to log in admin portal

1. If you are using the Remote Desktop Protocol (RDP) to connect to your HaloENGINE system and log into the Admin Portal, you need to use the default admin account.
2. Alternatively, if you have enabled “Configure Remote Access” you could sign in via the Microsoft Sign option and with the default admin account. Use the following URL:
   a. `http://<ip>:<port>/haloengine-admin/ui/app/login`
   b. For example, `https://10.41.14.69:8746/haloengine-admin/ui/app/login`

3.5.15. Phase 11. Monitor Log Validation

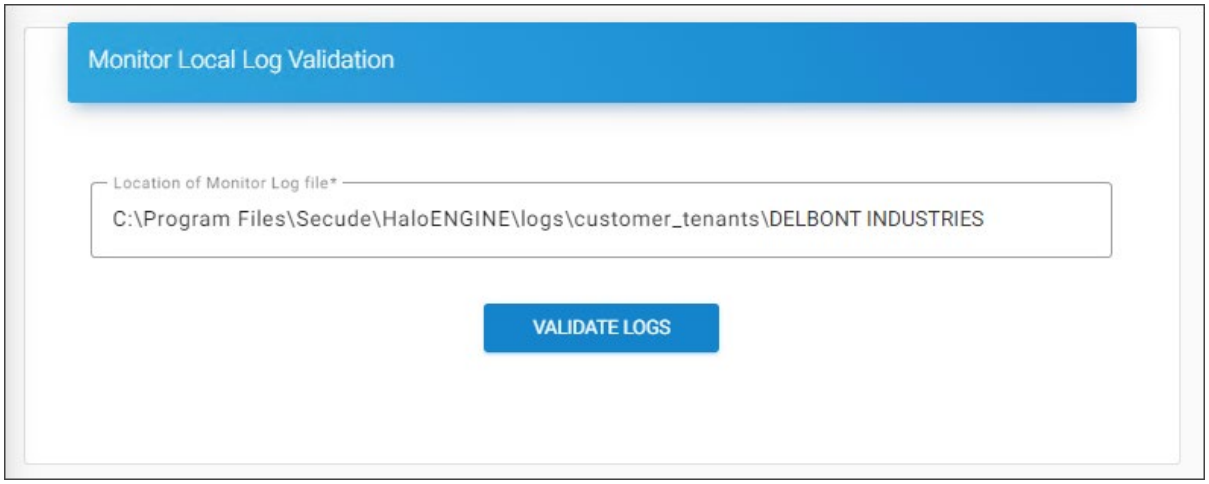
Halochain is a powerful feature that scrutinizes audit log files such as `HaloENGINE_Monitor.log` and `HaloENGINE_Admin_Activities.log` for any manipulation.

Prerequisites:

1. Make sure that you have enabled Halochain in Monitor Properties.
2. It is recommended to enable the Halochain feature during the initial configuration of the HaloENGINE. This is because Halochain is designed to work with a fresh `HaloENGINE_Monitor.log` file. In case, you enable it at a later stage, you need to back up the `HaloENGINE_Monitor.log` file and then delete or empty the log file to start the validation.

Follow the below procedure to validate the audit log file:

1. On the left navigation bar, click **Customer Configuration**, and then from the **Customers** list, select one of them.
2. On the **Monitor Log Validation** tab, click **Configure**.
3. The *Monitor Local Log Validation* page will appear:



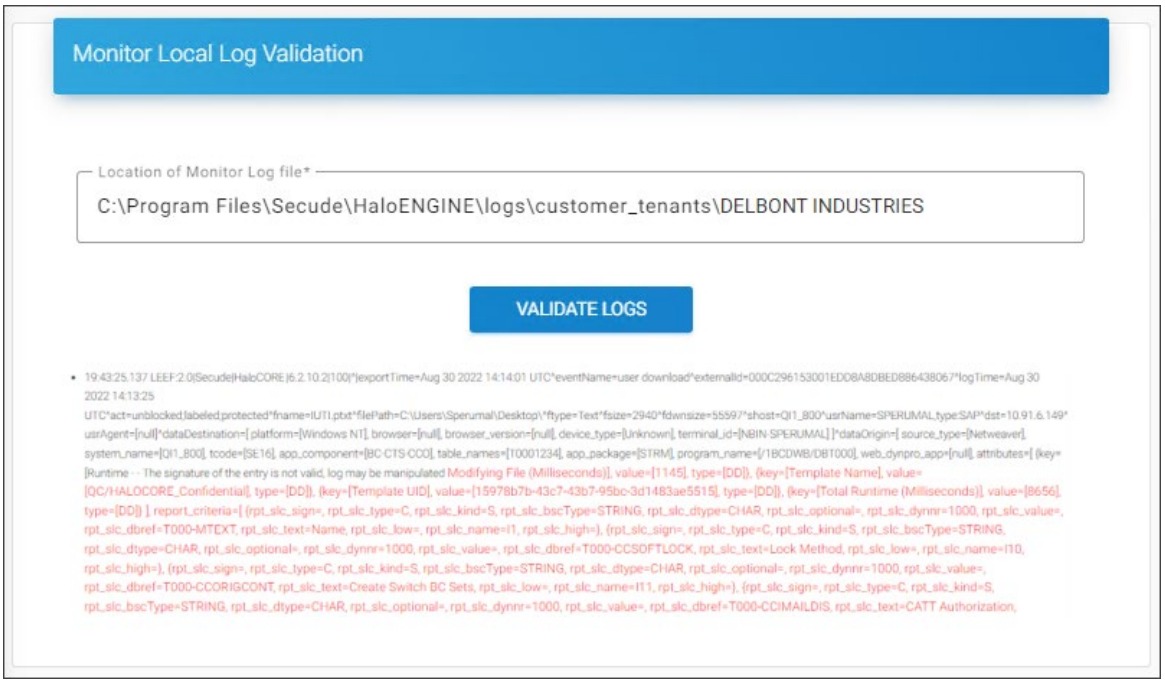
Monitor log validation

4. Click **Validate Logs**.

Results:

a. You will receive the message "*The log file has been validated and no manipulated entries found.*", if no manipulation is identified,

b. If manipulation is detected, you will obtain the following output:



Halochain output

3.6. System Configuration

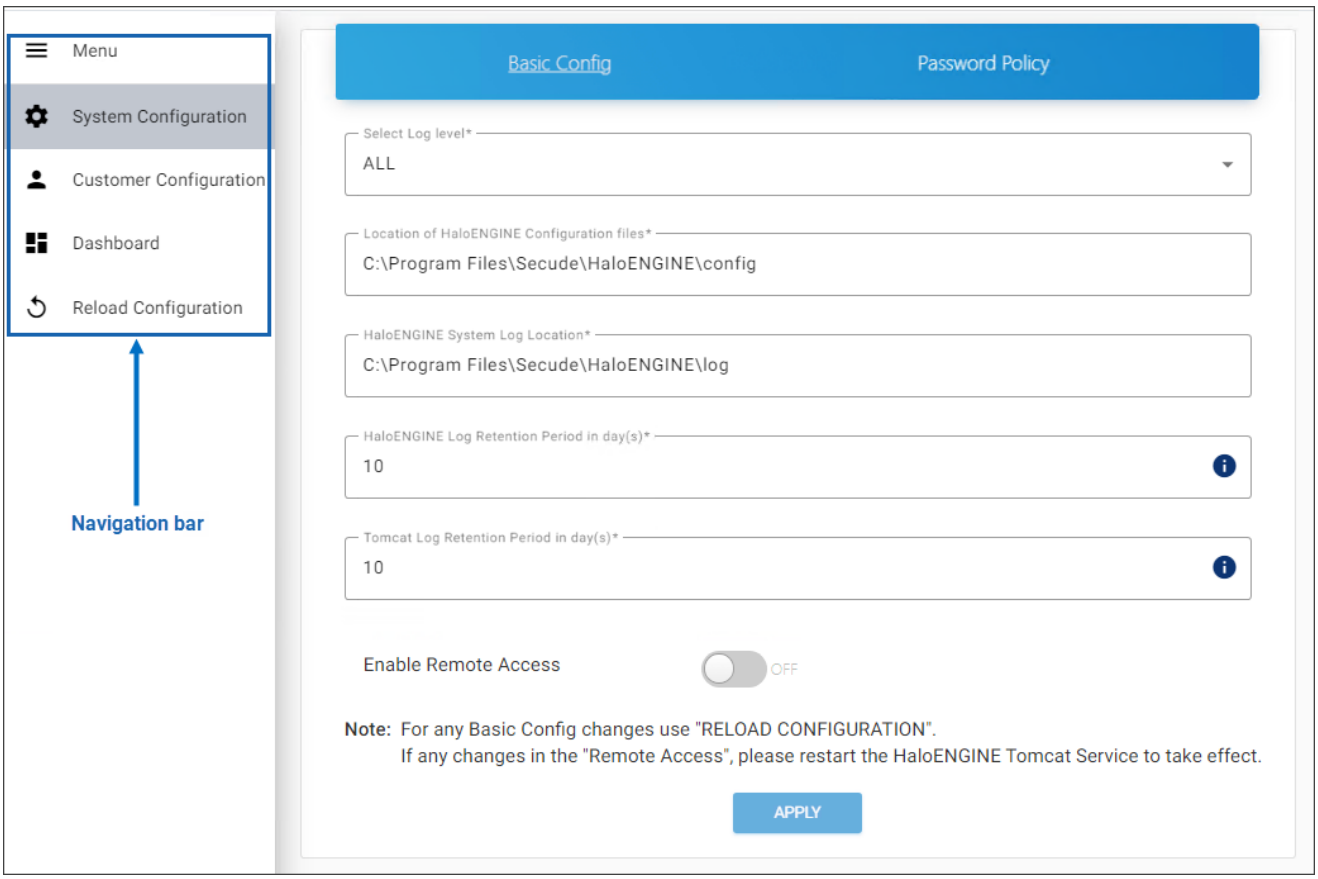
The initial configuration settings on the System Configuration page can be updated at any time. This page also handles certificate and password management. You can set a password policy if necessary for your business environment, but it is not mandatory.

3.6.1. HaloENGINE Configuration

Basic Configuration

Follow the below steps to update the basic HaloENGINE configuration:

1. Login admin portal.
2. On the left navigation bar, click **System Configuration,** and then on the **HaloENGINE Configuration** tab, click **Configure**.
3. Update the following:
   a. Log level
   b. Path for HaloENGINE configuration files
   c. Path for HaloENGINE system log
   d. Retention period of HaloENGINE log
   e. Retention period of Tomcat log
   f. Enable/disable remote access
4. To make basic configuration changes take effect, click **Apply** and then click **Reload Configuration** in the left navigation bar.



HaloENGINE Configuration

Results:

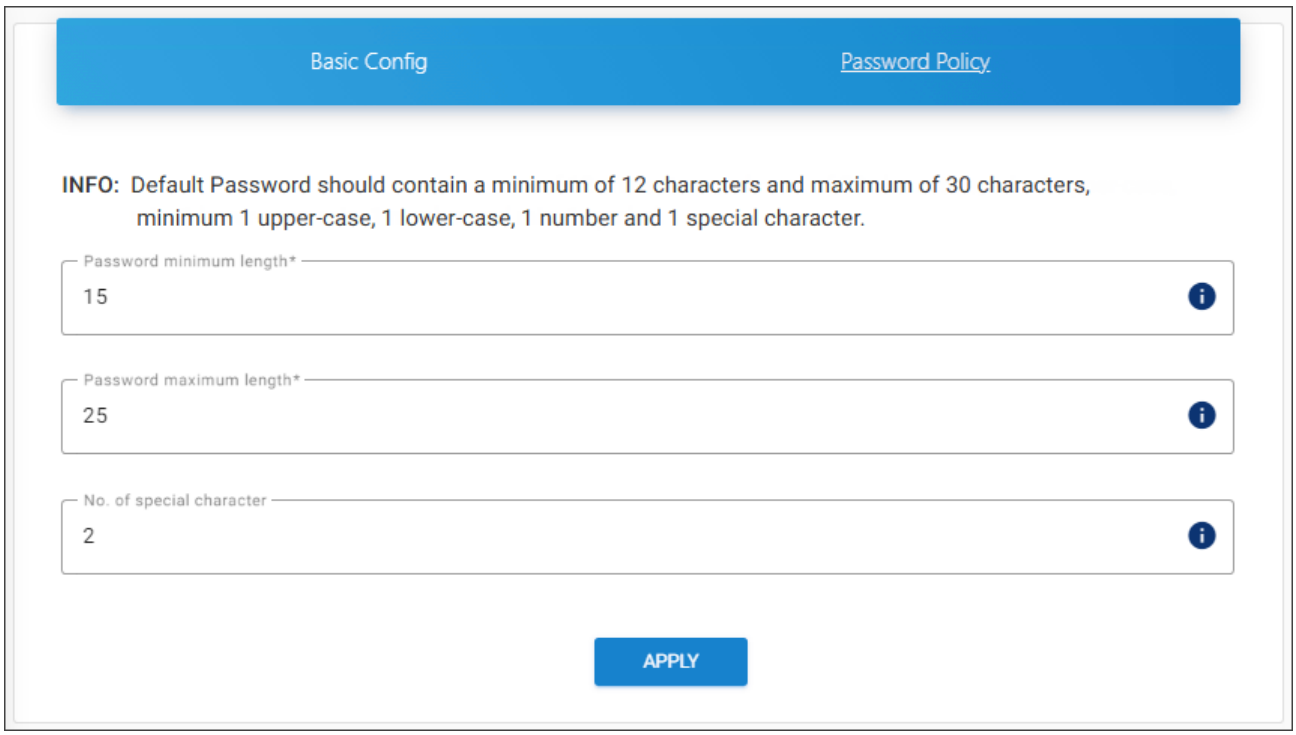
a. The page will be directed to the login page once the reload is done.

b. If any changes are made to Remote Settings please restart the HaloENGINE Tomcat service.

Password Policy

HaloENGINE's password policy requires a minimum of 12 characters and a maximum of 30 characters to increase security. However, the length of a company's password policy is determined by security requirements, regulatory obligations, and industry best practices. Therefore, you can configure or update your length seamlessly on this page.

1. Select the **Password Policy** tab and enter the following details as shown in the figure below:



Password policy configuration

2. **Password minimum length** – Enter the minimum number of characters required for your password. The default setting allows more than 12 characters.
3. **Password maximum length** – Enter the maximum number of characters required for your password. The default setting allows up to 30 characters.
4. **No. of special character** – Enter the number of special characters that should be included in your password. The default setting requires at least one special character. Note: If you set a Password Policy that includes more than one special character, you must input the password continuously. For example, if you set the **No. of special character** to 2, input them one after the other (for example, Pass234567!$). Entering special characters apart (for example, Pass!234567$) in the new password field will not be accepted.
5. Click **Apply**.

   Results:

   a. You will receive a confirmation message after successfully updating the password policy followed by a warning message as "*Please change your Password.*"

   b. On the warning message screen, click **Change Password**. The **Change Admin Password** screen will appear.

   c. Enter your current password, create a new password, and confirm it in the text boxes provided. For more details, please refer to the section "Change Password".

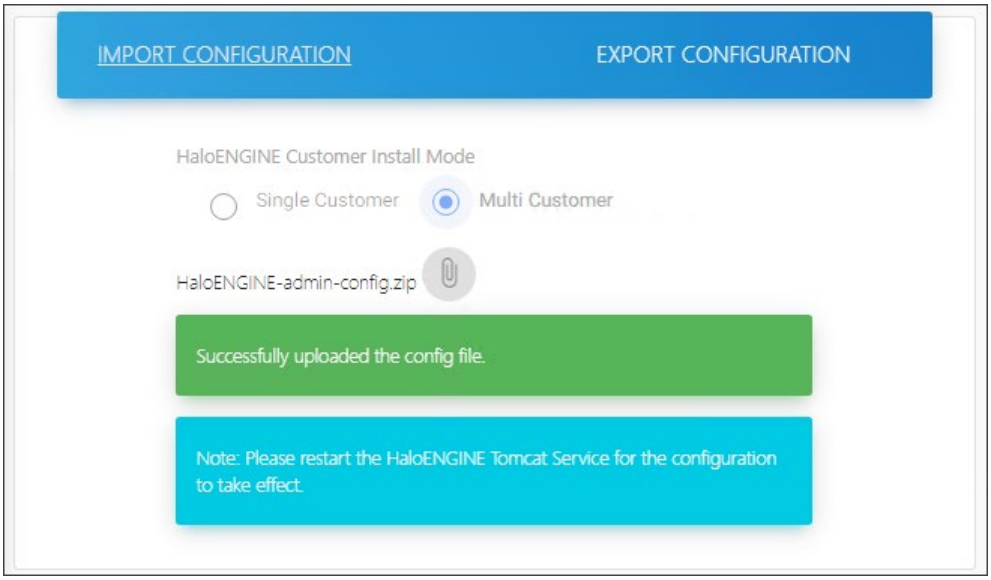
   d. The admin portal will restart automatically and you must enter the new password to access it.

e. Please note that it is not allowed to use the current password as your new password.

3.6.2. Import/Export Configuration

Follow the below steps to update the import/export configuration:

1. On the left navigation bar, click **System Configuration**, and then on the **Import/Export Configuration** tab, click **Configure**.
2. To import:
   a. Select the mode of installation - **Single Customer** or **Multi Customer**. You can notice an attachment button gets enabled for file selection.
   b. Click on the button and select the `HaloENGINE-admin-config.zip` file from the **Open** Windows dialog.
   c. **Results**: You can see the name of the zip file displayed on the page.



Import Configuration

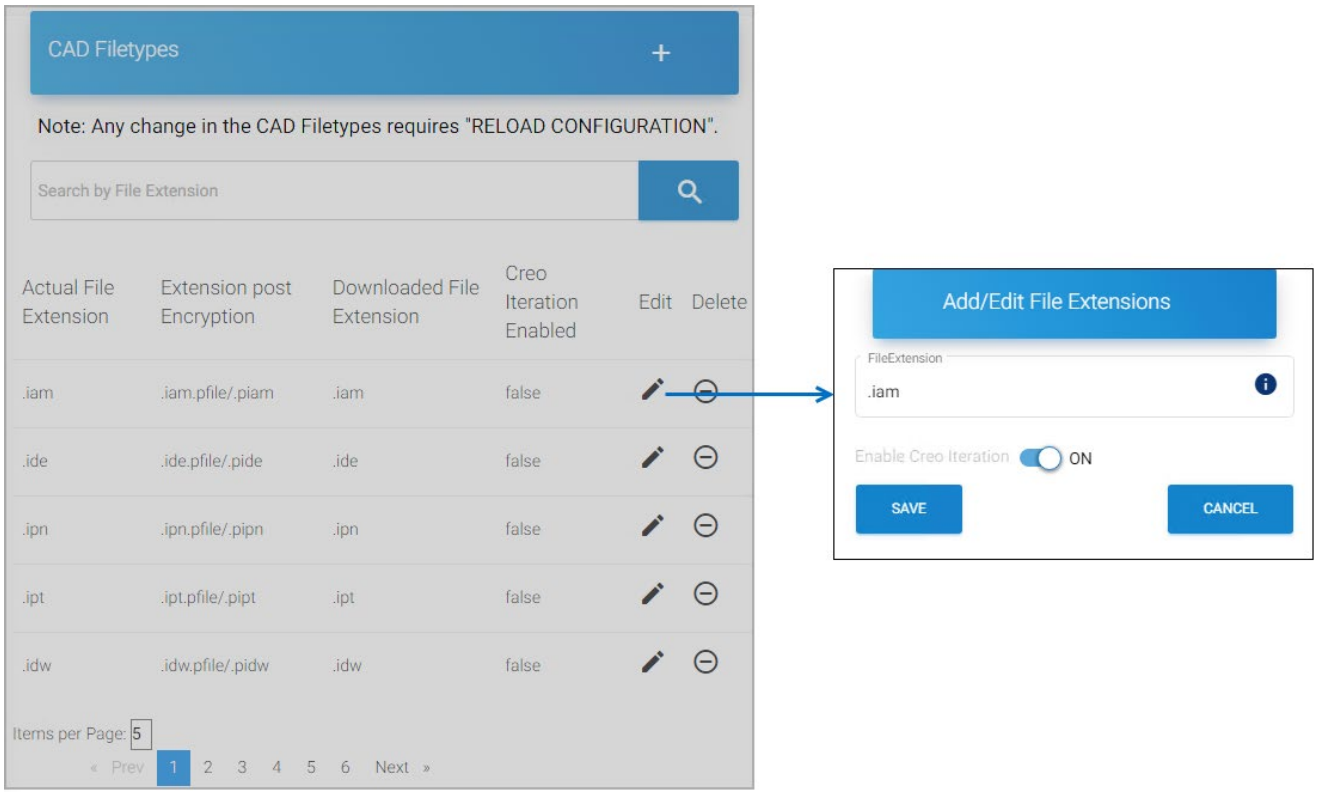
3. **What to do next:** Restart the HaloENGINE Tomcat service for the configuration update to take effect.
4. To export:
   a. Click **Export Configuration** and then click **Export Config** button.
   b. Please wait while the file `HaloENGINE-admin-config.zip` is downloaded.

3.6.3. CAD File Types Configuration

Use this page to add a new CAD file extension that will enable encryption and decryption for CAD-compatible file formats.

To add a new file extension, follow the steps below:

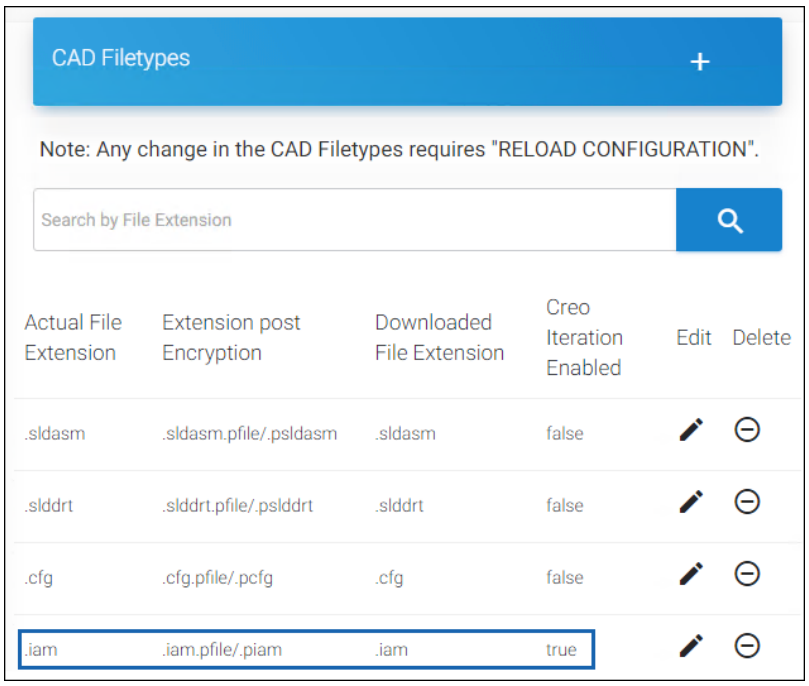
1. On the left navigation bar, click **System Configuration**, and then on the **CAD File Types Configuration** tab, click **Configure**.
2. The *CAD Filetypes* page will appear as shown in the figure below:



CAD File Types Configuration

3. **Option 1**: To change the Creo Iteration of a file type from the existing list.
   a. Turn ON the slider button **Enable Creo Iteration** against the file type.
   b. In this example, `.iam` is enabled with Creo Iteration.
4. Click **Save**.

   Results: You can see a confirmation message after saving the file type. In the below example, the `.iam` row gets appended to the end of the list with **Creo Iteration Enabled = true**.



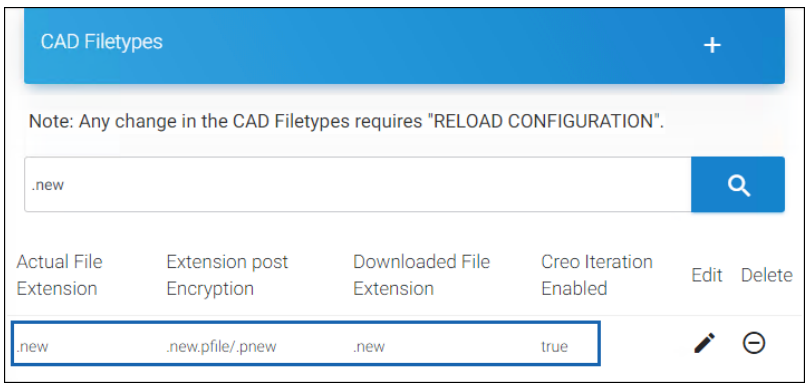
Creo Iteration Enabled

5. **Option 2**: To add a new file extension.
   a. Click on the plus icon and enter the file extension along with Creo Iteration Enabled = true/false status.
   b. Click **Save**.

   Results: You can see a confirmation message after saving the file type and the new entry is appended to the list's end.

6. **To find a file extension:**
   a. Click **Search File Extension**. The **Search File Extension** page will appear.
   b. Enter the file extension in **Search File Extension** and click **Search**.

   Results: The results of the search will be automatically listed. You can manage the file extension file using the **Edit** or **Delete** icon.

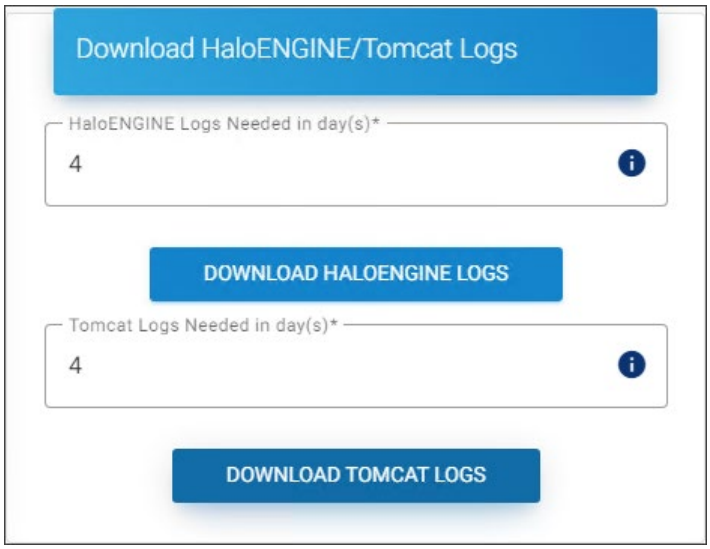


Search File Extension

3.6.4. Download Logs

The HaloENGINE logs and Tomcat logs can be downloaded via the admin portal using the following procedure:

1. On the left navigation bar, click **System Configuration**, and then on the **Download HaloENGINE/Tomcat Logs** tab, click **Configure**.
2. The *Download HaloENGINE/Tomcat Logs* page will appear as shown in the figure below:



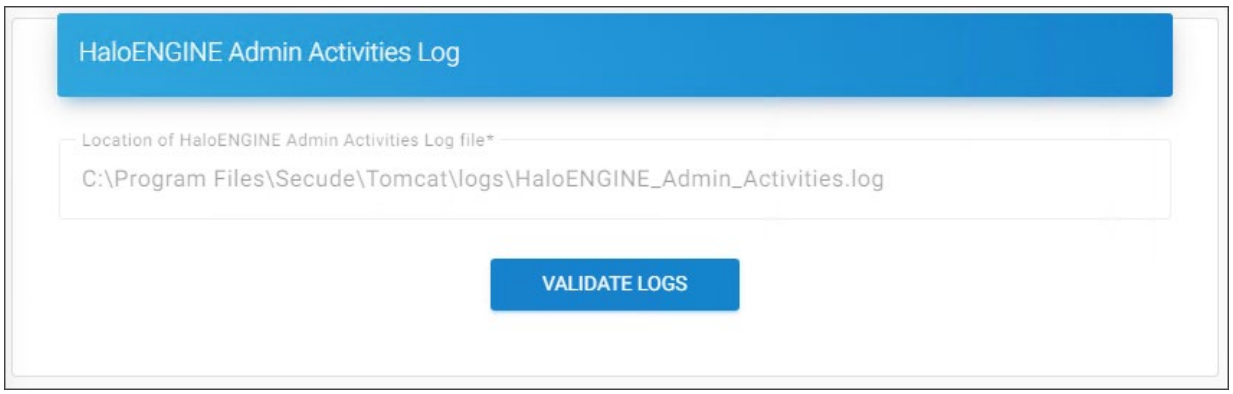
HaloENGINE and Tomcat logs

3. To download the HaloENGINE logs:
   a. Enter the number of days and then click **Download HaloENGINE Logs**.
   b. **Results**: A zip file (`HaloENGINE-Log`) will be downloaded to the default download location.
4. To download the Tomcat logs:
   a. Enter the number of days and then click **Download Tomcat Logs**.
   b. **Results**: A zip file (`tomcat-Log`) will be downloaded to the default download location.
5. Please note that you can only enter the value within the range that is defined on the *HaloENGINE Configuration* page for HaloENGINE log retention and Tomcat log retention.

3.6.5. HaloENGINE Admin Activities Log

Halochain scrutinizes the log file `HaloENGINE_Admin_Activities.log` for any modification and shows the results.

1. On the left navigation bar, click **System Configuration**, and then on the **HaloENGINE Admin Activities Log** tab, click **Validate**.
2. The *HaloENGINE Admin Activities Log* page will appear as shown in the figure below:



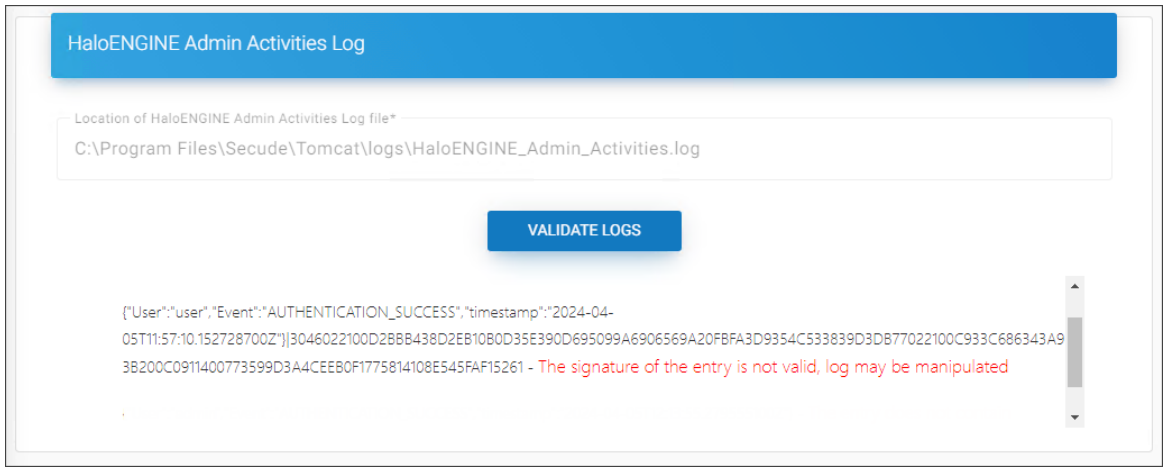
Admin Activities log

3. Click **Validate Logs**.

   Results:

   a. You will receive the message "*The log file has been validated and no manipulated entries found.*", if no manipulation is identified,

   b. If manipulation is detected, you will obtain the following output:



Halochain output

3.6.6. Log Out

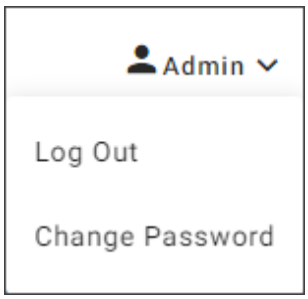
Logging out means terminating the current user's access to the portal. When the **Log Out** button is pressed, the portal is notified that the current user intends to terminate the login session.

A logged-in user's login session expires after 20 minutes. The user will no longer be able to use the portal after this period has passed. The user will be automatically logged out and redirected back to the login screen.

3.6.7. Change Password

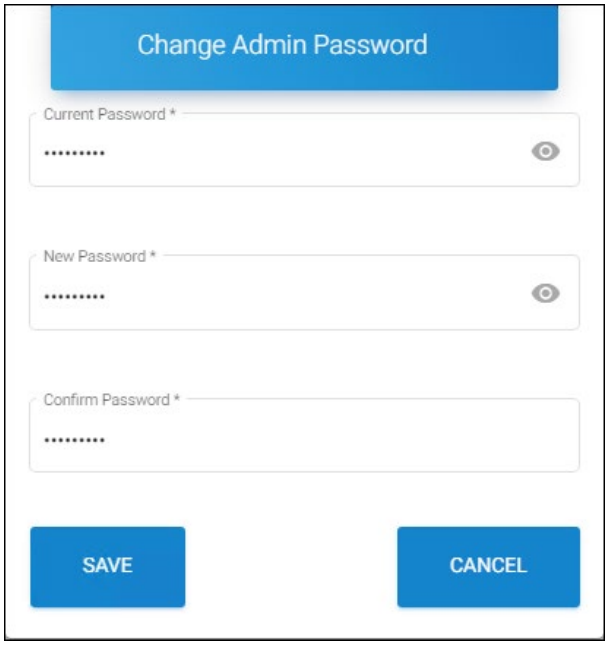
You can change your password for security concerns by following the steps below:

1. Click **Change Password** on the top right corner.



Change login password #1

2. The *Change Admin Password* dialog will appear as shown in the figure below:



Change login password #2

3. Enter the current password.
4. Enter your new password and re-enter again.
5. Click **Save**.

3.6.8. Reset Administrator Password

Use the following procedure to reset, update, or change your administrator password.

1. Copy `haloengine-password-config-<version>.zip` file to the desktop and extract it.
2. Open Command Prompt with administrator rights and change directory to `haloengine-password-config-<version>\bin`.

3. Type `haloengine-password-config.bat -h` to display the help information.

   For example:

   ```
   haloengine-password-config.bat -confPath <Full path of HaloENGINE config directory> -newPwd <new password for the login>
   haloengine-password-config.bat -confPath "C:\Program Files\Secude\HaloENGINE\config" -newPwd TestHalo!2345
   ```

When to reset and change the password?

HaloENGINE Admin portal provides the option of either changing or resetting your password. You can change the password when you know the current password. If you have forgotten the current password, you could reset (create a new) password using the tool.

3.6.9. Test the Configuration

1. Restart the HaloENGINE Tomcat service.
2. If you have configured the HaloENGINE properly, the following URLs must be resolved. URL resolves within the machine when you use `localhost`. Where localhost is the fully qualified hostname or IP address of the HaloENGINE installed machine.
   a. Process URL: `http://localhost:8383/haloengine-server/process?wsdl`
   b. Monitor URL: `http://localhost:8383/haloengine-server/monitor?wsdl`
   c. Stateful Process URL: `http://localhost:8383/haloengine-server/stateful_process?wsdl`
3. To access from other machines, use the IP address of the HaloENGINE.
   a. `http://10.41.14.69:8383/haloengine-server/process?wsdl`
   b. `http://10.41.14.69:8383/haloengine-server/monitor?wsdl`
   c. `http://10.41.14.69:8383/haloengine-server/stateful_process?wsdl`

   What to do next: Install the SAP add-on, and use the above URLs to create logical ports for processing the file and monitoring the downloads.

3.6.10. How to Update?

This section describes how to update HaloENGINE from previous versions to the latest version.

3.6.10.1. Update from HALO Core Server to HaloENGINE

This section is for users who are using previous versions of HALO Core Server (for example, <6.6) and want to update to HaloENGINE 6.8.

Update password

If your administrator password in the previous version is less than 12 characters, you must reset it according to the current password policy. To know how to reset the password, refer to the section "Reset Administrator Password".

1. **Step 1: Export admin file from HALO Core Server**
   a. Export the `halocore-admin-config.zip` file using the **Export Configuration** option.
   b. Uninstall HALO Core Server version 6.5 using the installer `SECUDE_HALO_CORE_SERVER_X64.EXE`.
   c. When prompted "*Do you want to keep the HALO Core Server configuration files?*" during the removal process, select **Yes**. The Tomcat files and configuration will be saved as a result.
2. **Step 2: Install the new version (HaloENGINE 6.8)**
   a. Install the HaloENGINE using `HaloENGINE_Setup.exe`.
   b. At this moment, do not launch the portal to configure it. The reason for this is to use the previously stored files from Step 1.
   c. Create a system variable `JAVA_HOME` and copy the `HaloENGINE_HOME` value. For example, e.g: `JAVA_HOME = D:\test\Secude\secude-jre`
3. **Step 3: Run the batch file**
   a. Open a command prompt and navigate to the folder where `HaloENGINEMigrationFor67.bat` is available in the product package.
   b. Execute the batch file as shown below:

```
HaloENGINEMigrationFor67.bat <path to the old zip file>\ <zip file name> <name
   of the new zip file>
For example:
HaloENGINEMigrationFor67.bat D:\Office\admin_zip_files\  halocore-admin-
   config.zip  HaloENGINE-admin-config-new.zip
```

   c. The new configuration zip file will be generated at `D:\Office\admin_zip_files`. Note: Make sure the folder name has no spaces.
   d. Now launch the portal and import the new zip file using the **Import Configuration** option.
4. **Step 4: Replace XML files**

   To use the previous versions (<6.6) of the server certificate `HalocoreServer.cer`, simply rename it to `HaloENGINEServer.cer`.

   Case 1: If you have chosen the default installation folder (`C:\Program Files\Secude`), you can skip this step.

Case 2: If you have chosen a location (`D:\sample\Secude`) other than the default installation folder, follow the steps below.

a. Replace the [`server.xml`, `tomcat-users.xml`, `cert` folder] files that were saved in Step 1 in the installation folder.

b. From the above location, edit the `server.xml`.

```
<Connector SSLEnabled="true" maxSavePostSize="2147483640"
  maxThreads="200" port="8746" protocol="org.apache.coyote
  .http11.Http11NioProtocol" scheme="https" secure="true"
  sslImplementationName="org.apache.tomcat.util.net.jsse
  .JSSEImplementation">
<SSLHostConfig certificateVerification="optional" ciphers
  ="TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
  ,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
  ,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
  ,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
  ,TLS_RSA_WITH_AES_128_CBC_SHA256
  ,TLS_RSA_WITH_AES_128_CBC_SHA
  ,TLS_RSA_WITH_AES_256_CBC_SHA256
  ,TLS_RSA_WITH_AES_256_CBC_SHA" protocols="TLSv1.2"
  sslProtocol="TLSv1.2" truststoreFile="C:\Program
  Files\Secude\Tomcat\conf\cert\serverKeystore.jks"
  truststorePassword="Test123$" truststoreType="PKCS12">
<Certificate certificateKeyAlias="serverkey"
  certificateKeystoreFile="C:\Program
  Files\Secude\Tomcat\conf\cert\serverKeystore.jks"
  certificateKeystorePassword="Test123$"
  certificateKeystoreType="PKCS12"/>
</SSLHostConfig>
</Connector>
```

Server XML

c. Replace the current HaloENGINE installation location (`D:\sample\Secude`) in two places where you see `serverKeystore.jks` and `certificateKeystore.jks`.

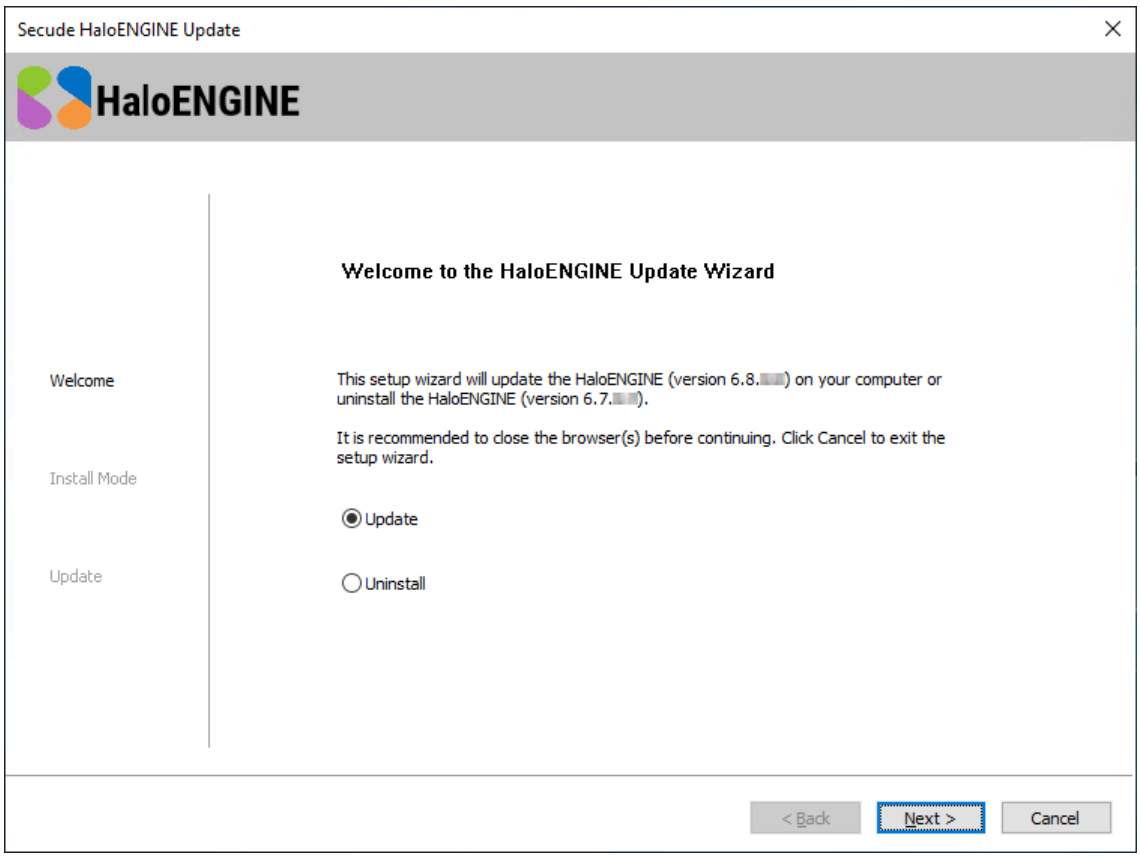
d. For example, `D:\sample\Secude\Tomcat\conf\cert\serverKeystore.jks` and `C:\Program Files\Secude\Tomcat\conf\cert\serverKeystore.jks`.

e. Save it and start the Tomcat Service.

f. Launch the admin portal.

3.6.10.2. Update of HaloENGINE from Version 6.7.x.x to 6.8.x.x

1. Navigate to the directory in which the HaloENGINE installation package is located and double-click the `HaloENGINE_Setup.exe`. The installation begins with the following dialog:

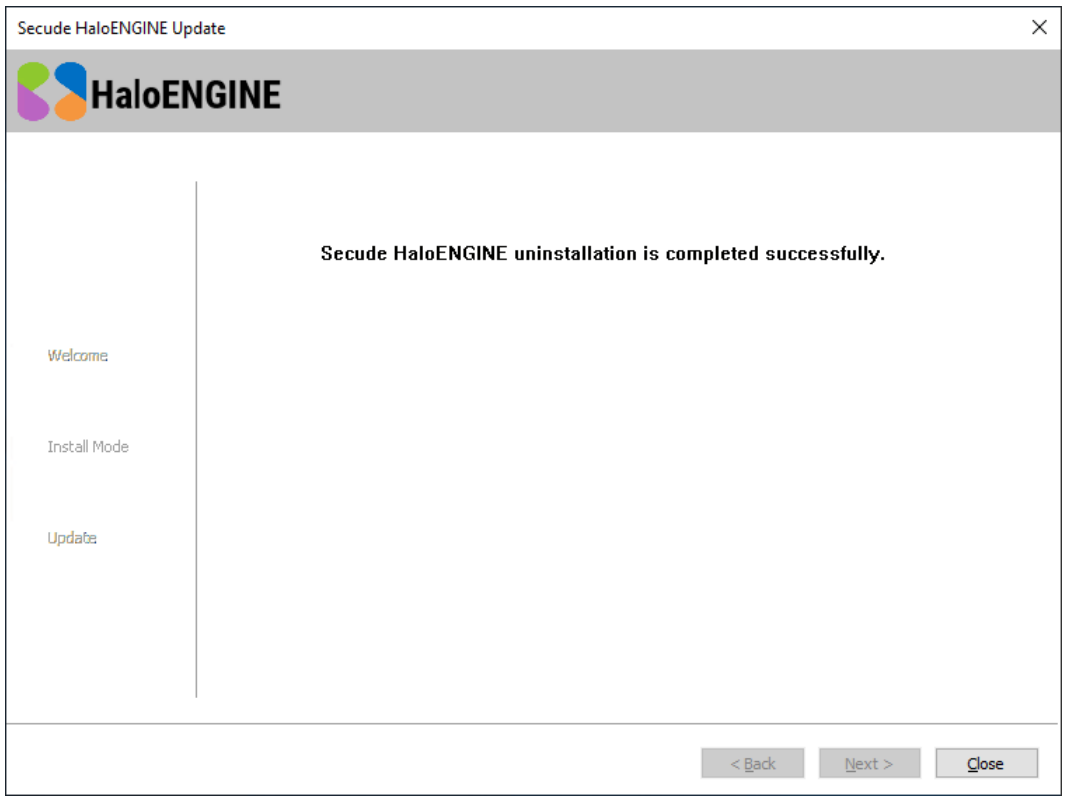


Update screen #1

2. Select either **Update** or **Uninstall**.

   a. **Uninstall:** If you wish to uninstall the server component, select **Uninstall** and click **Next**.

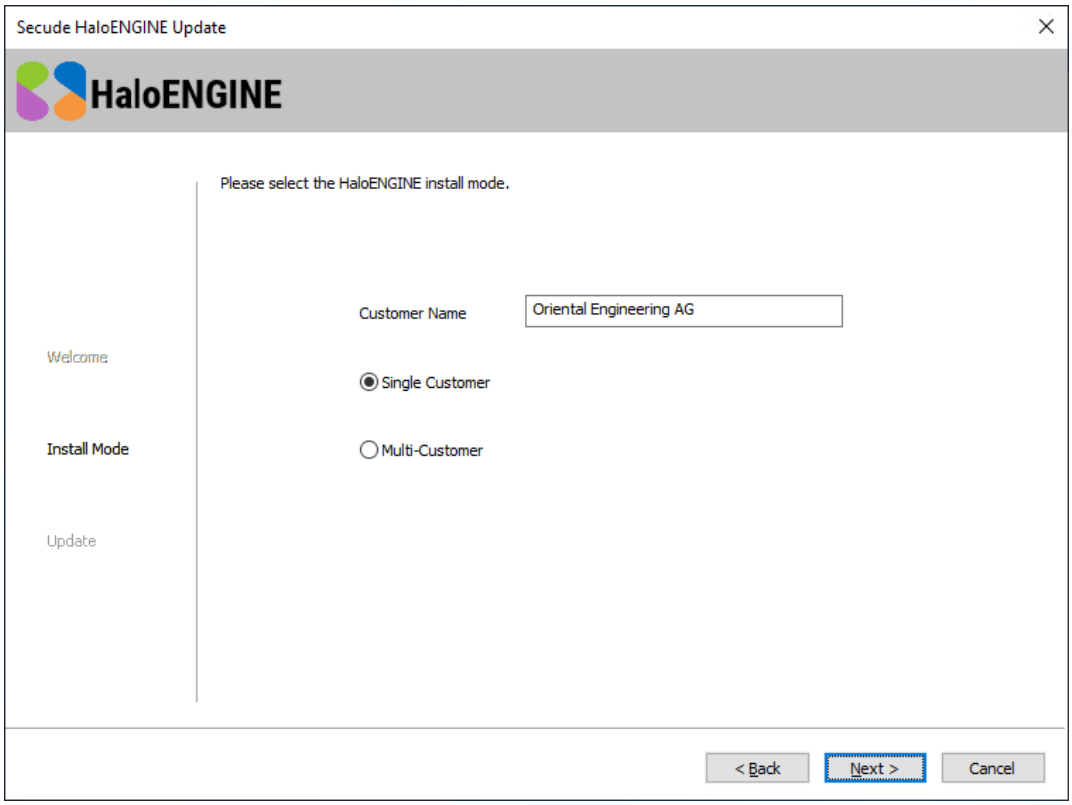
      - To the question, *"You are about to uninstall the HaloENGINE. Are you sure you want to uninstall the application?"*, answer **Yes**.
      - To the question, *"Do you want to keep the HaloENGINE configuration files?"*, answer **Yes** to save and then continue the installation or answer **No** to continue uninstallation without saving.
      - On completing the uninstall process, the following screen will appear. Click **Close** to close the wizard.



Uninstall dialog

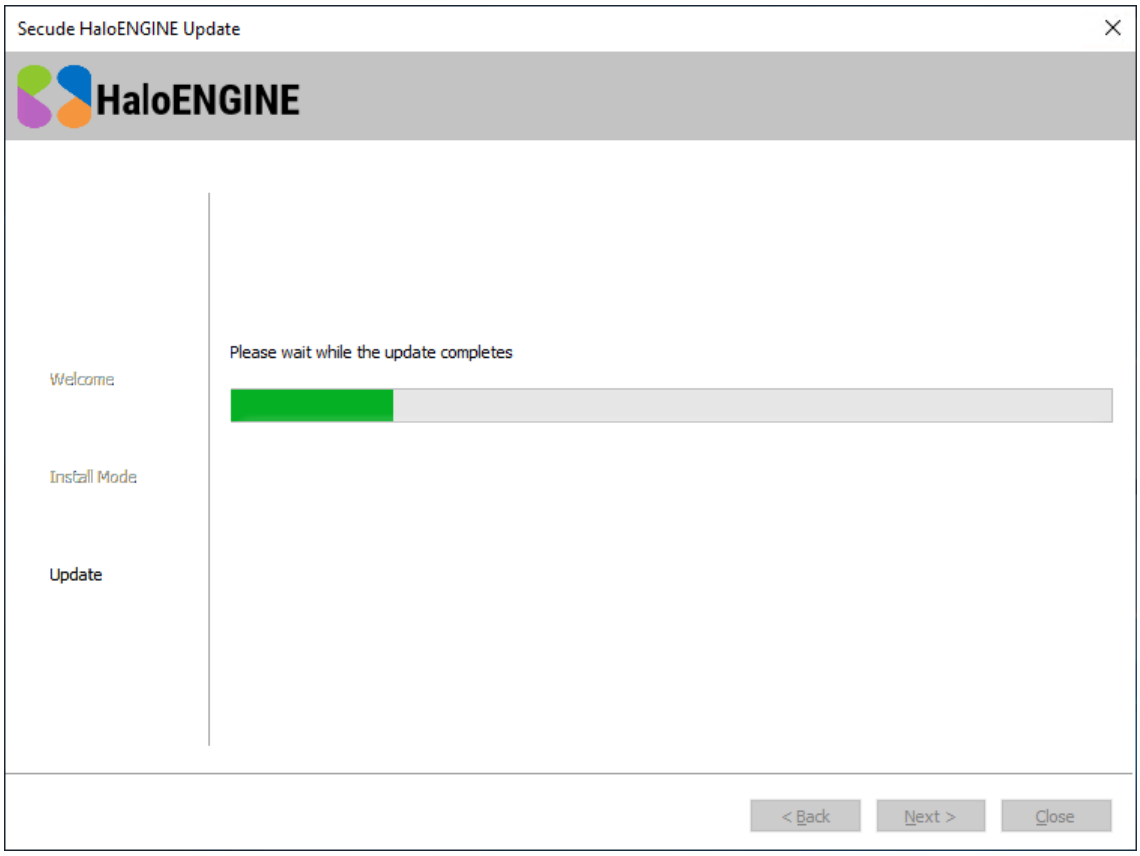
b. **Update:** If you wish to update, select **Update** and click **Next**.

3. The Customer mode selection dialog will appear:



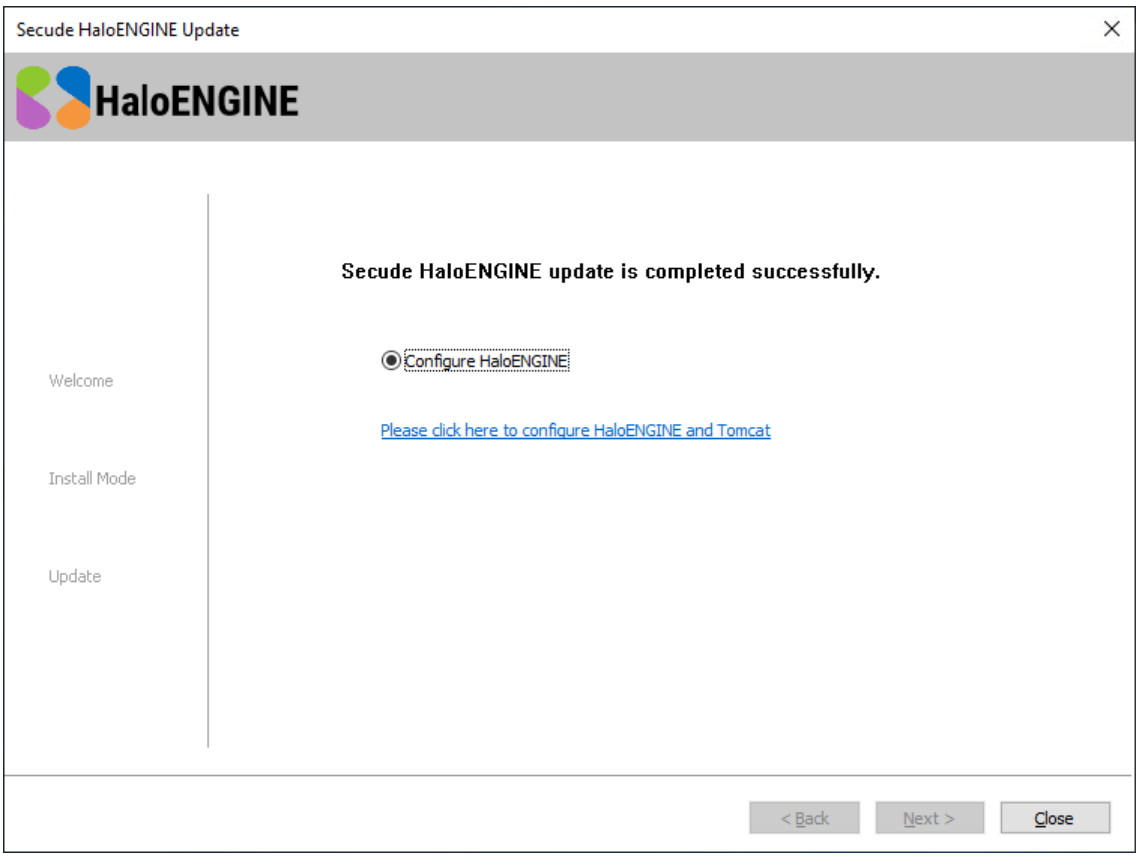
Update screen #2

4. Select a mode (**Single Customer** or **Multi-Customer**), and click **Next**.
5. The update begins, and progress is shown in the dialog. Please be patient, as this will take some time.



Update screen #3

6. Once the update is completed, the HaloENGINE configuration dialog will appear.



Update screen #4

7. When you select **Configure HaloENGINE**, a link will appear on the configuration screen.
8. Run the batch file as described in the "**Step 3: Run the Batch File**" section above.
9. Click on the link to access the HaloENGINE admin portal.
10. Note: To use the previous versions (<6.6) of the server certificate `HalocoreServer.cer`, simply rename it to `HaloENGINEServer.cer`.

3.6.11. HaloENGINE Service Monitor

HaloENGINE Service Monitor displays HaloENGINE Service and Azure Connection information and verifies that the protection is properly applied.

Prerequisites:

1. HaloENGINE Service must be installed.
2. HaloENGINE must be installed.

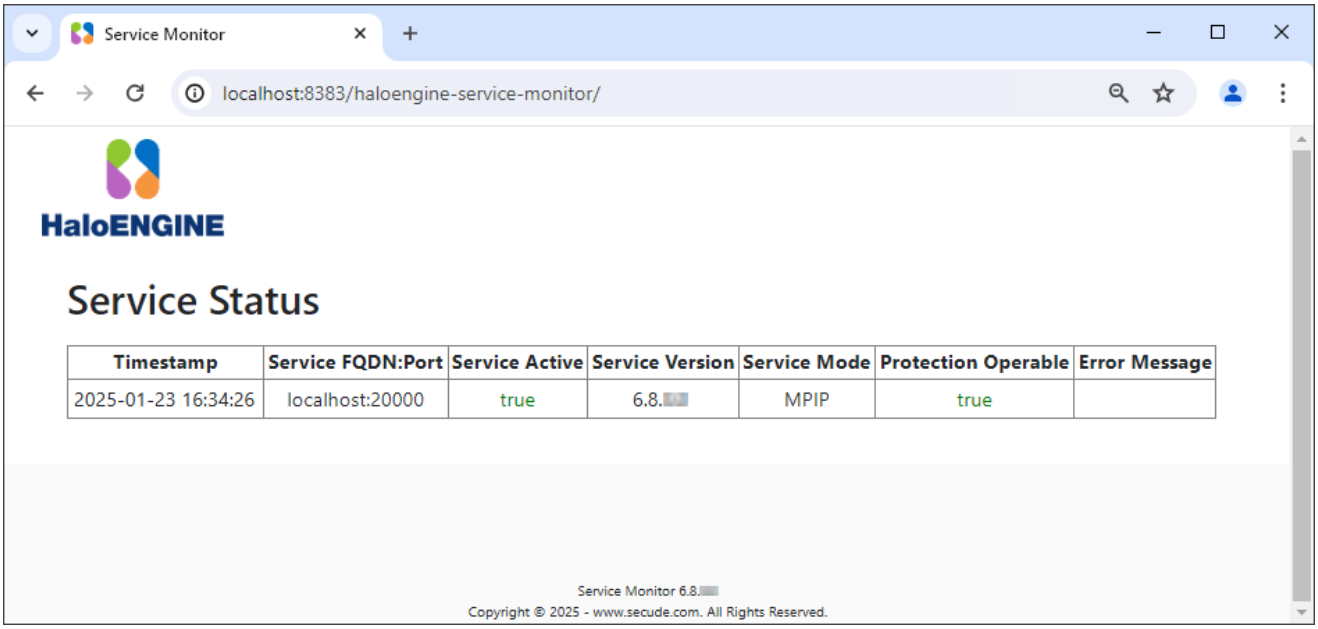
Follow the steps to display the HaloENGINE Service Monitor page:

1. Stop HaloENGINE Tomcat Service.
2. Navigate to the installer package and edit `HCSRVNodes.json` file.
3. Enter the following details:

If MPIP mode, enter the author (e-mail address) and a `label ID`.

```
[ {
"author":"john@halosecude.onmicrosoft.com",
"template_ID":"",
"label_ID":"{cec0887a-07de-4dde-a67f-23edcf22395e}"
} ]
```

4. **Save** the file.
5. Place the `HCSRVNodes.json` in the HaloENGINE installed directory.
   a. The default location is `...Secude\ServiceMonitor\config`
   b. User-defined location e.g., `D:\Secude\ServiceMonitor\config`
6. Start HaloENGINE Tomcat Service.
7. Access HaloENGINE Service Monitor with the following URL: `http://localhost:8383/haloengine-service-monitor/`



HaloENGINE Service status

3.6.12. Log Details

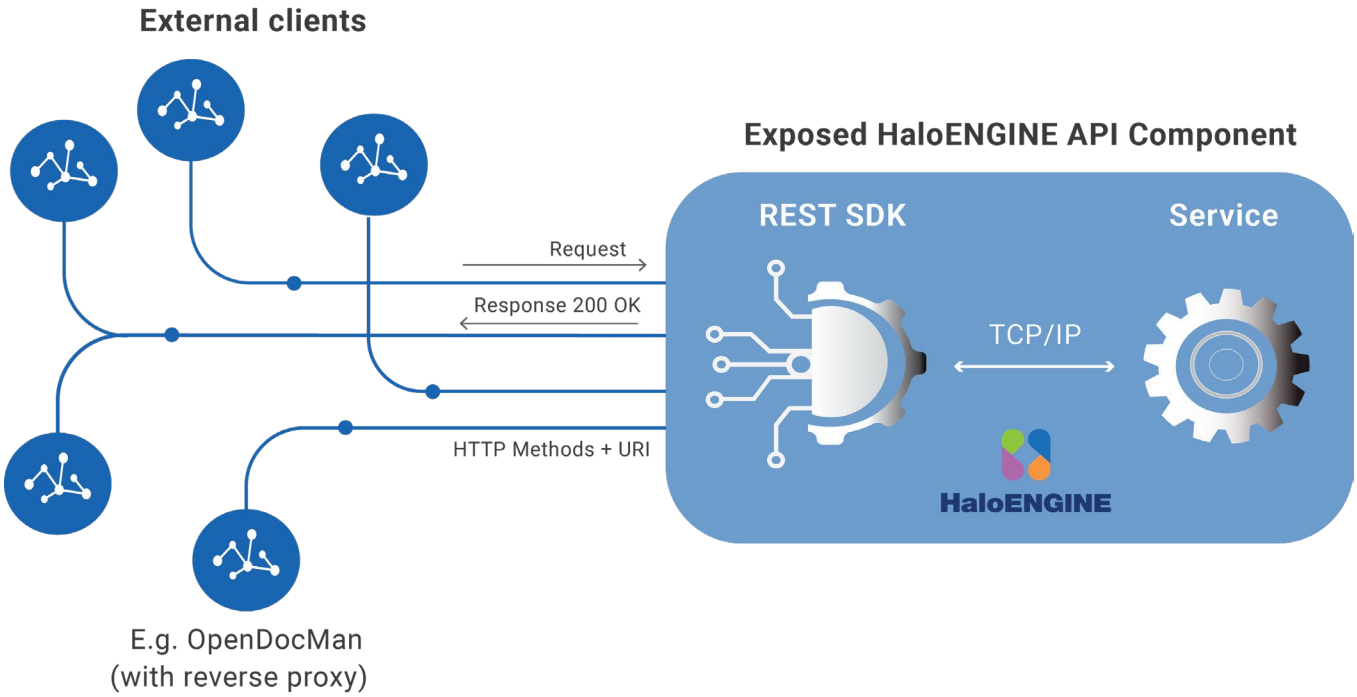
The following table lists the HaloENGINE log files.

Filename	Location	Description
`HaloENGINE.log`	`<installed path>\Secude\HaloENGINE\log`	HaloENGINE's activities are logged into this file, such as connection, file process, and so on.
`HaloENGINE_Monitor.log`	1. **Single customer mode** – `<installed path>\Secude\HaloENGINE\logs\customer_tenants\halo_customer` 2. **Multi-customer mode** – The path varies based on the customer IDs. For example: a. `<installed path>\Secude\HaloENGINE\logs\customer_tenants\BMAUTOMOBILE AG` b. `<installed path>\Secude\HaloENGINE\logs\customer_tenants\DELBONT INDUSTRIES`	The tenant's download activities are logged into this file.
`HaloENGINE_DSI.log`	Same as above	DSI logs are forwarded from SAP and are logged into this file.
`Service_Monitor.log`	`<installed path>\Secude\ServiceMonitor\logs`	HaloENGINE Service health check status logged into this file.

Log Details

4. HaloENGINE API

Secude's HaloENGINE API architecture aims to streamline underlying MPIP functionalities such as file protection and audit log export. The HaloENGINE API enables MPIP capabilities by seamlessly integrating with existing business applications.



HaloENGINE API

What can be expected when using the API?

1. It streamlines web-based application interaction via HTTP methods.
2. The end consumer can protect files with their own rule engine or business logic.
3. This will extend to any existing or customized data portal within the organization that must be scrutinized and protected against data leaks.

The usage of this information, as well as the implementation of any of these APIs, is the responsibility of the customer and is dependent on their abilities to evaluate and incorporate them into their place of business.

4.1. About this Manual

This document demonstrates how to successfully call the HaloENGINE API from your application and use it for your business needs. It assumes you are familiar with REST API calls. It provides a clear and comprehensive background to the REST SDK, including endpoints, parameters, response types, and any other information that developers should be aware of. It also explains how the resources work and provides examples that should help you get started.

> Please be aware that the examples in this document are meant only as guidance and should not be applied in a production environment.

Use case illustration

To demonstrate a real-world example, OpenDocMan and HaloENGINE API are used, and requests and responses are shown in the API method section. In this manual, each method is outlined briefly, and its requests and responses are captured using the Postman tool.

OpenDocMan, an open-source document management system (DMS), communicates with the HaloENGINE API using a reverse proxy. However, depending on the business requirements, you can integrate your Document Management System using an intermediate reverse proxy, customization, or middleware application (such as MuleSoft). Using the HaloENGINE API methods, a file is encrypted when downloaded from OpenDocMan and decrypted when uploaded to OpenDocMan.

4.2. Quick Start

The following high-level steps describe how to get started with HaloENGINE and expose the APIs.

1. **Step 1**: Install and configure the HaloENGINE and HaloENGINE Service as described in the following chapters “Installing the HaloENGINE Service” and “Installing the HaloENGINE”.
2. **Step 2**: Import the license with the HaloENGINE API enabled in the admin portal.
3. **Step 3:** Server Certificate Authentication. Select one of the following approaches for authentication.
   Self-signed Certificate: A minor configuration change is necessary on the client side. Download the server certificate (`HaloENGINEServer.cer`) from the HaloENGINE Admin portal and manually install it on the client machine in the Trusted Root Certification Authorities.
   Company Owned Signed Certificate: If you already have a certificate, you can import it into the admin portal. Make sure your company's Root CA is installed in Trusted Root Certification Authorities. In this case, there is no need to install the server certificate (`HaloENGINEServer.cer`) on your client machine. For more details, please refer to the section “Phase 1. Certificate Configuration”.
4. **Step 4:** Set classification engine. This step comprises creating profiles, schema, and action rules based on the needs of your business. Please refer to the chapter “Setting Up Classification Engine”.

4.3. Requirements

The HaloENGINE requirements are listed in the table below.

Components	Details
Operating System	1. Supported only in Microsoft Windows Server 2022 and above. 2. Latest Windows system updates installed.
Supported browser version	The most recent versions of Microsoft Edge, Chrome, and Firefox are supported by the HaloENGINE Admin portal.

Requirements

4.4. API Reference

4.4.1. Host/Base URL

Base URL	`https://{servername}:{port}/haloengine-server`
Endpoint description	`https://{servername}:{port}/haloengine-server/halosdk`

Base URL

Using the above URL, the "halosdk" API is accessible.

The following variables should be replaced with values for your system.

1. {`server`} corresponds to the server's name or IP address of your server.
2. {`port`} is the port number on which the server runs.

Resource Methods Description

Typically, an API will have multiple endpoints associated with the same resource. Every resource is exposed via a URL. You can obtain the URL of every resource by obtaining access to the API Root Endpoint.

Method	URL
GET	`/GetVersion`
POST	`/GetRequiredMetaDataTypes`
POST	`/GetActionForm`
POST	`/ExecuteActionForm`
POST	`/DecryptFileAndFetchLabel`

Method	URL
POST	`/SendPLMAuditLogData`

Endpoints

4.4.2. GetVersion

Purpose	Gets information about the HaloENGINE version installed on a server at the client site.
Request method	GET
Input Request	`https://{servername}:{port}/haloengine-server/halosdk/GetVersion`

GetVersion details

4.4.2.1. Postman Example

The following example is demonstrated using Postman tool and the HaloENGINE API to obtain data.

4.4.2.1.1. Request

```
GET https://10.41.14.69:8746/haloengine-server/halosdk/GetVersion
```

4.4.2.1.2. Response

A successful request returns the following information: Status code: 200. The response body is in plain text format containing the version number of the HaloENGINE.

```
6.8.0.0
```

The response indicates that the HaloENGINE is alive and its version is `6.8.0.0`.

4.4.2.2. OpenDocMan Example

The following example is demonstrated using OpenDocMan through a reverse proxy with the HaloENGINE API, with the results displayed in Postman tool.

4.4.2.2.1. Request

```
GET https://10.41.14.69:8746/haloengine-server/halosdk/GetVersion
```

4.4.2.2.2. Response

```
6.8.0.0
```

The response indicates that HaloENGINE is alive and its version is `6.8.0.0`.

4.4.3. GetRequiredMetaDataTypes

Purpose	Retrieves the necessary metadata types configured on the server in the customer environment.
Request method	POST
Input Request	`https://{servername}:{port}/haloengine-server/halosdk/GetRequiredMetaDataTypes`

GetRequiredMetaDataTypes details

4.4.3.1. Postman Example

The following example is demonstrated using Postman tool and the HaloENGINE API to obtain data.

Prerequisite: The HaloENGINE API system type does not currently have any built-in metadata; hence, new metadata can be created using Custom metadata. Please refer to the section "Custom metadata".

4.4.3.1.1. Request

The request is sent in the Body-XML format with the following parameters:

1. `customer_id` - Indicates which customer ID the HaloENGINE is using.
2. `system_id` - Indicates the unique system ID of a client system.
3. `system_type` - Indicates the client system type.

```
<id>
    <customer_id>HaloAPI</customer_id>
    <system_id>RESTclient</system_id>
    <system_type>HaloENGINE_API</system_type>
</id>
```

4.4.3.1.2. Response

A successful request returns the following information: Status code: 200

Response to this request:

In the response, the metadata added in the HaloENGINE admin portal will be displayed.

```
[user_group, work_in_progress, folder, review, release, project]
```

4.4.3.2. OpenDocMan Example

The following example is demonstrated using OpenDocMan through a reverse proxy with the HaloENGINE API, with the results displayed in Postman tool.

4.4.3.2.1. Request

The request is sent in the Body-XML format with the following parameters:

```
<id>
    <customer_id>halo_customer</customer_id>
    <system_id>HaloengineClient</system_id>
    <system_type>HaloENGINE_API</system_type>
</id>
```

4.4.3.2.2. Response

A successful request returns the following information: Status code: 200

Response to this request:

```
[file_type, folder_name, lifecycle_name]
```

4.4.4. GetActionForm

There are three options in "Owner Configuration": Service (default), Static email, and User. You can set it up on the HaloENGINE admin portal. Note: In the case of static email, enter the user's email address in the admin portal. To learn how to configure **Owner Configuration**, refer to the section "Owner Configuration".

Owner Configuration - User option

When you choose User in the HaloENGINE admin portal, the request results in true (`<user_email_needed>true</user_email_needed>`), therefore when executing `ExecuteActionForm`, you must enter the author's email ID.

Purpose	Determine whether to encrypt or decrypt a file.
Request method	POST
Input Request	`https://{servername}:{port}/haloengine-server/halosdk/GetActionForm`

GetActionForm details

4.4.4.1. Postman Example

The following example is demonstrated using Postman tool and the HaloENGINE API to obtain data.

4.4.4.1.1. Request

A multipart/form-data request is sent with the following parameters:

Key: `customerIdentification` (Text as Type)

Description: Indicates the customer's details (`customer_id`, `system_id`, and `system_type`) that HaloENGINE uses.

Value: The value should look similar to the following:

```
<id>
    <customer_id>HaloAPI</customer_id>
    <system_id>RESTclient</system_id>
    <system_type>HaloENGINE_API</system_type>
</id>
```

Key: `metadata` (Text as Type)

Description: Indicates the metadata provided to decide the appropriate action.

Value: The value should look similar to the following.

```
<metadata>
    <!--Optional:-->
    <general_metadata>
        <!--Optional:-->
        <simple_value>
            <!--Zero or more repetitions:-->
            <entry>
                <!--Optional:-->
                <key>user_name</key>
                <!--Zero or more repetitions:-->
                <value>john</value>
            </entry>
        </simple_value>
        <!--Optional:-->
        <complex_value>
            <!--Zero or more repetitions:-->
            <entry>
                <type>data</type>
                <key>project</key>
                <!--1 or more repetitions:-->
                <values>?</values>
            </entry>
        </complex_value>
    </general_metadata>
</metadata>
```

4.4.4.1.2. Response

A successful request returns the following information: Status code: 200

Response to this request:

```
--uuid:3c3e23eb-0225-4b65-893c-677e8ff8b10d
Content-Type: text/plain
Content-Transfer-Encoding: binary
Content-ID: <simMode>
Content-Disposition: form-data; name="simMode"

false
--uuid:3c3e23eb-0225-4b65-893c-677e8ff8b10d
Content-Type: text/plain
Content-Transfer-Encoding: binary
Content-ID: <labelVendor>
Content-Disposition: form-data; name="labelVendor"
```

```
NONE
--uuid:3c3e23eb-0225-4b65-893c-677e8ff8b10d
Content-Type: application/xml
Content-Transfer-Encoding: binary
Content-ID: <action>
Content-Disposition: form-data; name="action"



            <?xml version="1.0" encoding="UTF-8" standalone="yes"?>
            <ns2:action xmlns:ns2="http://interfaces.central.halocore.secude.com">
                <value>LABEL</value>
                <value>AUDIT</value>
            </ns2:action>
--uuid:3c3e23eb-0225-4b65-893c-677e8ff8b10d
Content-Type: application/xml
Content-Transfer-Encoding: binary
Content-ID: <authorMode>
Content-Disposition: form-data; name="authorMode"



                <?xml version="1.0" encoding="UTF-8" standalone="yes"?>
                <ns2:author_mode
xmlns:ns2="http://interfaces.central.halocore.secude.com">
                    <user_email_needed>false</user_email_needed>
                    <static_email></static_email>
                </ns2:author_mode>
--uuid:3c3e23eb-0225-4b65-893c-677e8ff8b10d
Content-Type: text/xml
Content-Transfer-Encoding: binary
Content-ID: <classification>
Content-Disposition: form-data; name="classification"



                    <?xml version="1.0" encoding="UTF-8" standalone="yes"?>
                    <classification version="1.0">
                        <class name="Default">
                            <displayNames>
                                <displayName locale="en_US" name="Default"/>
                            </displayNames>
                            <properties>
                                <property name="Sensitivity" dataType="listValue">
                                    <displayNames>
                                        <displayName locale="en_US" name="Sensitivity"/>
                                    </displayNames>
```

```
                                    <values>
                                        <listValue name="Secret">
                                            <displayNames>
                                                <displayName locale="en_US"
name="Secret"/>
                                            </displayNames>
                                        </listValue>
                                    </values>
                                </property>
                            </properties>
                        </class>
                    </classification>

--uuid:3c3e23eb-0225-4b65-893c-677e8ff8b10d
Content-Type: application/xml
Content-Transfer-Encoding: binary
Content-ID: <template>
Content-Disposition: form-data; name="template"



                        <?xml version="1.0" encoding="UTF-8" standalone="yes"?>
                        <ns2:template
xmlns:ns2="http://interfaces.central.halocore.secude.com">
                            <guid>99f1473d-74f4-47ca-9843-e735f94fa797</guid>
                            <template_name>HCAD Secret</template_name>
                        </ns2:template>
--uuid:3c3e23eb-0225-4b65-893c-677e8ff8b10d--
```

4.4.4.2. OpenDocMan Example

The following example is demonstrated using OpenDocMan through a reverse proxy with the HaloENGINE API, with the results displayed in Postman tool.

4.4.4.2.1. Request

A multipart/form-data request is sent with the following parameters:

Key: `customerIdentification` (Text as Type)

Description: Indicates the customer's details (`customer_id`, `system_id`, and `system_type`) that HaloENGINE uses.

Value: The value should look similar to the following:

```
<id>
    <customer_id>halo_customer</customer_id>
    <system_id>HaloengineClient</system_id>
    <system_type>HaloENGINE_API</system_type>
</id>
```

Key: `metadata` (Text as Type)

Description: Indicates the metadata provided to decide the appropriate action.

Value: The value should look similar to the following.

```
<metadata>
    <general_metadata>
        <simple_value

            <entry>
                <key>user_name</key>
                <value>john</value

            </entry>
        </simple_value>
        <complex_value>
            <entry

                <type>data</type>
                <key>project</key>
                <values>?</values>
            </entry>
        </complex_value>
    </general_metadata>
</metadata>
```

4.4.4.2.2. Response

A successful request returns the following information: Status code: 200

Response to this request:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:template xmlns:ns2="http://interfaces.central.halocore.secude.com">
        <guid>d7e95033-e7f1-4218-8941-7d60d8e9cf69</guid>
        <template_name>CADSecured</template_name>
</ns2:template>
```

4.4.5. ExecuteActionForm

Purpose	Executes the determined action retrieved by GetActionForm.
Request method	POST
Input Request	`https://{servername}:{port}/haloengine-server/halosdk/ExecuteActionForm`

ExecuteActionForm details

4.4.5.1. Postman Example

The following example is demonstrated using Postman tool and the HaloENGINE API to obtain data.

4.4.5.1.1. Request for Encryption

Prerequisite: When you select the **User** option in "Owner Configuration", you must input an email address in the author field.

A multipart/form-data request is sent with the following parameters:

Key: `customerIdentification` (Text as Type)

Description: Indicates the customer's details (`customer_id`, `system_id`, and `system_type`) that HaloENGINE uses.

Value: The value should look similar to the following.

```
<id>
    <customer_id>HaloAPI</customer_id>
    <system_id>RESTclient</system_id>
    <system_type>HaloENGINE_API</system_type>
</id>
```

Key: `action` (Text as Type)

Description: Indicates what action should be taken on the file (LABEL/UNPROTECT/AUDIT).

Value

```
<action>
    <!--Zero or more repetitions:-->
    <value>LABEL</value>
</action>
```

Key: `template` (Text as Type)

Description: If the action is to label, it indicates the template to use.

Value: The value should look similar to the following.

```
<template>
    <!--Optional:-->
    <guid>99f1473d-74f4-47ca-9843-e735f94fa797</guid>
    <template_name>HCAD Secret</template_name>
</template>
```

Key: `extendedTags` (Text as Type)

Description: Indicates additional metadata that can be included while downloading a file.

Value: The value should look similar to the following.

```
<extended_tags>
    <!--Zero or more repetitions:-->
    <extended_tags>
        <key></key>
        <!--Optional:-->
        <value>username</value>
    </extended_tags>
</extended_tags>
```

Key: `author` (Text as Type)

Description: This indicates who owns the exported document. This field is applicable only when the User option is selected in the admin portal. Note: If you selected User in the admin portal, please provide the author's email address. The following is an example of the default Service option. Thus, no author is added.

Value: The value should look similar to the following.

```
<author>?</author>
```

Key: `file_size` (Text as Type)

Description: Indicates the file size in bytes.

Value: The value should look similar to the following.

```
5462
```

Key: `file` (File as Type). Browse and choose a file.

Description: Indicates which file is currently being used.

Value: The value should look similar to the following.

```
BOM.txt
```

Key: `classification` (Text as Type)

Description: Indicates the sensitivity setting.

Value: The value should look similar to the following.

```
<classification>?<classification>
```

4.4.5.1.2. Response for Encryption

A successful request returns the following information: Status code: 200

Response to this request: Protected content will also be included in the response body.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:applied_action
    xmlns:ns2="http://interfaces.central.halocore.secude.com">
    <fileProtected>true</fileProtected>
    <fileLabeled>true</fileLabeled>
    <fileDecrypted>false</fileDecrypted>
    <already_protected>false</already_protected>
</ns2:applied_action>
```

The `.pfile` extension shows that the action was successfully performed on the file.

4.4.5.1.3. Request for Decryption

To decrypt a file, use the same parameters as in the Request for Encryption, with the exception that the “action key” must be "Unprotect" and the “file key” must be a protected file, as shown below.

Key: `action` (Text as Type)

Description: If the action is to unprotect, it specifies which template should be used.

Value: The value should look similar to the following.

```
<action>
    <!--Zero or more repetitions:-->
    <value>UNPROTECT</value>
</action>
```

Key: `file` (File as Type). Browse and choose a protected file.

Description: Indicates which file is currently being used.

Value: The value should look similar to the following.

```
BOM.ptxt
```

4.4.5.1.4. Response for Decryption

Response to this request: Unprotected content will also be included in the response body.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:applied_action
    xmlns:ns2="http://interfaces.central.halocore.secude.com">
    <fileProtected>false</fileProtected>
    <fileLabeled>false</fileLabeled>
    <fileDecrypted>true</fileDecrypted>
    <already_protected>true</already_protected>
</ns2:applied_action>
```

The protected file has been decrypted successfully in the above example.

4.4.5.2. OpenDocMan Example

The following example is demonstrated using OpenDocMan through a reverse proxy with the HaloENGINE API, with the results displayed in Postman tool.

4.4.5.2.1. Request for Encryption

A multipart/form-data request is sent with the following parameters:

Key: `customerIdentification`(Text as Type)

Description: Indicates the customer's details (`customer_id`, `system_id`, and `system_type`) that HaloENGINE uses.

Value: The value should look similar to the following:

```
<id>
    <customer_id>halo_customer</customer_id>
    <system_id>HaloengineClient</system_id>
    <system_type>HaloENGINE_API</system_type>
</id>
```

Key: `action` (Text as Type)

Description: Indicates what action should be taken on the file (LABEL/UNPROTECT/AUDIT).

Value: The value should look similar to the following.

```
<action>
    <!--Zero or more repetitions:-->
    <value>LABEL</value>
</action>
```

Key: `template` (Text as Type)

Description: If the action is to label, it indicates the template to use.

Value: The value should look similar to the following

```
<template>
    <!--Optional:-->
    <guid>d7e95033-e7f1-4218-8941-7d60d8e9cf69</guid>
    <template_name>CADSecured</template_name>
</template>
```

Key: `extendedTags` (Text as Type)

Description: Indicates additional metadata that can be included while downloading a file.

Value: The value should look similar to the following.

```
<extended_tags>
    <key/>
    <value>""</value>
</extended_tags>
```

Key: `author`(Text as Type)

Description: The following is an example of the default Service option. Thus, no author is added.

Value: The value should look similar to the following.

```
<author>?</author>
```

Key: `file_size`(Text as Type)

Description: Indicates the file size in bytes.

Value: The value should look similar to the following.

```
9521
```

Key: `file` (File as Type)

Description: Indicates which file is currently being used.

Value: The value should look similar to the following.

```
Checklist.txt
```

Key: `classification`(Text as Type)

Description: Indicates the sensitivity setting.

Value: The value should look similar to the following.

```
<classification>?<classification>
```

4.4.5.2.2. Response for Encryption

A successful request returns the following information: Status code: 200

Response to this request: Protected content will also be included in the response body.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:applied_action
    xmlns:ns2="http://interfaces.central.halocore.secude.com">
    <fileProtected>true</fileProtected>
    <fileLabeled>true</fileLabeled>
    <fileDecrypted>false</fileDecrypted>
    <already_protected>false</already_protected>
</ns2:applied_action>
```

The `.pfile` extension shows that the action was successfully performed on the file.

4.4.5.2.3. Request for Decryption

To decrypt a file, use the same parameters as in the Request for Encryption, with the exception that the action key must be "Unprotect" and the file key must be a protected file, as shown below.

Key: `action` (Text as Type)

Description: If the action is to unprotect, it specifies which template should be used.

Value: The value should look similar to the following.

```
<action>
    <!--Zero or more repetitions:-->
    <value>UNPROTECT</value>
</action>
```

Key: `file` (File as Type)

Description: Indicates which file is currently being used.

Value: The value should look similar to the following.

```
Checklist.ptxt
```

4.4.5.2.4. Response for Decryption

Response to this request: Unprotected content will also be included in the response body.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:applied_action
    xmlns:ns2="http://interfaces.central.halocore.secude.com">
    <fileProtected>false</fileProtected>
    <fileLabeled>false</fileLabeled>
    <fileDecrypted>true</fileDecrypted>
    <already_protected>true</already_protected>
</ns2:applied_action>
```

The protected file has been decrypted successfully in the above example.

4.4.6. DecryptFileAndFetchLabel

Purpose	Decrypts an encrypted file and returns the label information that was used to encrypt the file.
Request method	POST
Input Request	`https://{servername}:{port}/haloengine-server/halosdk/DecryptFileAndFetchLabel`

DecryptFileAndFetchLabel details

Let's imagine a business use case in which a watermark needs to be added to a protected file.

The process of adding a watermark to a protected file involves decrypting it and then applying the same label. This can be achieved by using this method to identify the label applied to the file and then decrypting it.

4.4.6.1. Postman Example

The following example is demonstrated using Postman tool and the HaloENGINE API to obtain data.

4.4.6.1.1. Request for Decryption

A multipart/form-data request is sent with the following parameters:

Key: `customerIdentification` (Text as Type)

Description: Indicates the customer's details (`customer_id`, `system_id`, and `system_type`) that HaloENGINE uses.

Value: The value should look similar to the following.

```
<id>
    <customer_id>HaloAPI</customer_id>
    <system_id>RESTclient</system_id>
    <system_type>HaloENGINE_API</system_type>
</id>
```

Key: `metadata` (Text as Type)

Description: Indicates the metadata provided to decide the appropriate action.

Value: The value should look similar to the following.

```
<metadata>
    <!--Optional:-->
    <general_metadata></general_metadata>
</metadata>
```

Key: `file_size` (Text as Type)

Description: Indicates the file size in bytes.

Value: The value should look similar to the following.

```
5462
```

Key: `file` (File as Type). Browse and choose a file.

Description: Indicates which file is currently being used.

Value: The value should look similar to the following.

```
BOM.ptxt
```

Key: `classification` (Text as Type)

Description: Indicates the sensitivity setting.

Value: The value should look similar to the following.

```
<classification>?<classification>
```

4.4.6.1.2. Response for Decryption

Response to this request: Unprotected content and label information will be sent in the response body as multipart/form-data.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:applied_action
    xmlns:ns2="http://interfaces.central.halocore.secude.com">
    <fileProtected>false</fileProtected>
    <fileLabeled>false</fileLabeled>
    <fileDecrypted>true</fileDecrypted>
    <already_protected>true</already_protected>
</ns2:applied_action>

---
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:template
    xmlns:ns2="http://interfaces.central.halocore.secude.com">
    <guid>99f1473d-74f4-47ca-9843-e735f94fa797</guid>
    <template_name>HCAD Secret</template_name>
</ns2:template>
```

The protected file has been decrypted successfully in the above example.

4.4.6.2. OpenDocMan Example

The following example is demonstrated using OpenDocMan through a reverse proxy with the HaloENGINE API, with the results displayed in Postman tool.

4.4.6.2.1. Request for Decryption

A multipart/form-data request is sent with the following parameters:

Key: `customerIdentification` (Text as Type)

Description: Indicates the customer's details (`customer_id`, `system_id`, and `system_type`) that HaloENGINE uses.

Value: The value should look similar to the following.

```
<id>
    <customer_id>halo_customer</customer_id>
    <system_id>HaloengineClient</system_id>
    <system_type>HaloENGINE_API</system_type>
</id>
```

Key: `metadata` (Text as Type)

Description: Indicates the metadata provided to decide the appropriate action.

Value: The value should look similar to the following.

```
<metadata>
    <!--Optional:-->
    <general_metadata></general_metadata>
</metadata>
```

Key: `file_size` (Text as Type)

Description: Indicates the file size in bytes.

Value: The value should look similar to the following.

```
9521
```

Key: `file` (File as Type). Browse and choose a file.

Description: Indicates which file is currently being used.

Value: The value should look similar to the following.

```
Checklist.ptxt
```

Key: `classification` (Text as Type)

Description: Indicates the sensitivity setting.

Value: The value should look similar to the following.

```
<classification>?<classification>
```

4.4.6.2.2. Response for Decryption

Response to this request: Unprotected content and label information will be sent in the response body as multipart/form-data.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:applied_action
    xmlns:ns2="http://interfaces.central.halocore.secude.com">
    <fileProtected>false</fileProtected>
    <fileLabeled>false</fileLabeled>
    <fileDecrypted>true</fileDecrypted>
    <already_protected>true</already_protected>
</ns2:applied_action>

---
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:template
    xmlns:ns2="http://interfaces.central.halocore.secude.com">
    <guid>99f1473d-74f4-47ca-9843-e735f94fa797</guid>
    <template_name>CADSecured</template_name>
</ns2:template>
```

The protected file has been decrypted successfully in the above example.

4.4.7. SendAuditLogData

Purpose	Sends audit log to the server.
Request method	POST
Input Request	`https://{servername}:{port}/haloengine-server/halosdk/SendAuditLogData`

SendAuditLogData details

The following example is demonstrated using Postman and the HaloENGINE API to obtain data.

4.4.7.1. Request

A multipart/form-data request is sent with the following parameters:

Key: `customerIdentification` (Text as Type)

Description: Indicates the customer's details (`customer_id`, `system_id`, and `system_type`) that HaloENGINE uses.

Value: The value should look similar to the following.

```
<id>
    <customer_id>HaloAPI</customer_id>
    <system_id>RESTclient</system_id>
    <system_type>HaloENGINE_API</system_type>
</id
```

Key: `logInfo` (Text as Type)

Description: Indicates the timestamp when the event occurred.

Value: The value should look similar to the following.

```
<log_info>
    <utc_time_stamp>2021-02-23T23:01:00+05:00</utc_time_stamp>
    <!--Optional:-->
    <time_zone>-1</time_zone>
    <!--Optional:-->
    <logID>loginID1</logID>
</log_info>
```

Key: `userInfo` (Text as Type)

Description: Indicates the user details.

Value: The value should look similar to the following.

```
<user_info>
    <user_name>john</user_name>
    <!--Optional:-->
    <user_type>john</user_type>
    <user_email>john@halosecude.onmicrosoft.com</user_email>
</user_info>
```

Key: `fileInfo` (Text as Type)

Description: Indicates the file details.

Value: The value should look similar to the following.

```
<file_info>
    <!--Optional:-->
    <file_name></file_name>
    <!--Optional:-->
    <file_path>C:\</file_path>
    <!--Optional:-->
    <file_type>txt</file_type>
    <file_protected_before>false</file_protected_before>
    <size_original>4445</size_original>
    <size_download>444448</size_download>
</file_info>
```

Key: `resultedDecision` (Text as Type)

Description: Indicates the action that was taken on the file.

Value: The value should look similar to the following.

```
<resulted_decision>
    <fileBlocked>false</fileBlocked>
    <fileLabeled>false</fileLabeled>
    <fileProtected>false</fileProtected>
    <unprotected>true</unprotected>
    <fileBlocked>true</fileBlocked>
    <unlabeled>true</unlabeled>
    <!--Optional:-->
    <policy_name>HCAD Secret</policy_name>
    <!--Optional:-->
    <policy_id>99f1473d-74f4-47ca-9843-e735f94fa797</policy_id>
    <!--Optional:-->
    <classification>
        <by_user>
            <?xml version="1.0" encoding="UTF-8"?>
            <classification version="1.0">
                <class name="DB">
                    <displayNames>
                        <displayName locale="en_US" name="Local Configuration"/>
                    </displayNames>
                    <properties>
                        <property name="C_IPADDR" dataType="stringValue"
valueType="simple">
                            <displayNames>
                                <displayName locale="en_US" name="IP Address"/>
                            </displayNames>
                            <values></values>
```

```
                        </property>
                        <property name="C_LOGID" dataType="stringValue"
valueType="simple">
                            <displayNames>
                                <displayName locale="en_US" name="Log ID"/>
                            </displayNames>
                            <values></values>
                        </property>
                        <property name="C_TABS" dataType="stringValue"
valueType="simple">
                            <displayNames>
                                <displayName locale="en_US" name="Table/View Names"/>
                            </displayNames>
                            <values></values>
                        </property>
                        <property name="C_TSTMP" dataType="stringValue"
valueType="simple">
                            <displayNames>
                                <displayName locale="en_US" name="Time Stamp"/>
                            </displayNames>
                            <values></values>
                        </property>
                        <property name="C_TCODE" dataType="stringValue"
valueType="simple">
                            <displayNames>
                                <displayName locale="en_US" name="Transaction Code"/>
                            </displayNames>
                            <values></values>
                        </property>
                        <property name="C_UNAME" dataType="stringValue"
valueType="simple">
                            <displayNames>
                                <displayName locale="en_US" name="User Name"/>
                            </displayNames>
                            <values></values>
                        </property>
                        <property name="C_WDAPPL" dataType="stringValue"
valueType="simple">
                            <displayNames>
                                <displayName locale="en_US" name="WD Application"/>
                            </displayNames>
                            <values></values>
                        </property>
                        <property name="SENS" dataType="listValue" valueType="simple">
```

```
                            <displayNames>
                                <displayName locale="en_US" name="Sensitivity_1"/>
                            </displayNames>
                            <values>
                                <listValue name="CONF">
                                    <displayNames>
                                        <displayName locale="en_US" name="Confidential"/>
                                    </displayNames>
                                </listValue>
                            </values>
                        </property>
                        <property name="DOM" dataType="listValue" valueType="simple">
                            <displayNames>
                                <displayName locale="en_US" name="Domain"/>
                            </displayNames>
                            <values>
                                <listValue name="LOG">
                                    <displayNames>
                                        <displayName locale="en_US" name="Logistics"/>
                                    </displayNames>
                                </listValue>
                            </values>
                        </property>
                    </properties>
                </class>
            </classification>
        </by_user>
        <by_system>
            <?xml version="1.0" encoding="UTF-8"?>
            <classification version="1.0">
                <class name="DB">
                    <displayNames>
                        <displayName locale="en_US" name="Local Configuration"/>
                    </displayNames>
                    <properties>
                        <property name="C_IPADDR" dataType="stringValue"
valueType="simple">
                            <displayNames>
                                <displayName locale="en_US" name="IP Address"/>
                            </displayNames>
                            <values></values>
                        </property>
                        <property name="C_LOGID" dataType="stringValue"
valueType="simple">
```

```
                            <displayNames>
                                <displayName locale="en_US" name="Log ID"/>
                            </displayNames>
                            <values></values>
                        </property>
                        <property name="C_TABS" dataType="stringValue"
valueType="simple">
                            <displayNames>
                                <displayName locale="en_US" name="Table/View Names"/>
                            </displayNames>
                            <values></values>
                        </property>
                        <property name="C_TSTMP" dataType="stringValue"
valueType="simple">
                            <displayNames>
                                <displayName locale="en_US" name="Time Stamp"/>
                            </displayNames>
                            <values></values>
                        </property>
                        <property name="C_TCODE" dataType="stringValue"
valueType="simple">
                            <displayNames>
                                <displayName locale="en_US" name="Transaction Code"/>
                            </displayNames>
                            <values></values>
                        </property>
                        <property name="C_UNAME" dataType="stringValue"
valueType="simple">
                            <displayNames>
                                <displayName locale="en_US" name="User Name"/>
                            </displayNames>
                            <values></values>
                        </property>
                        <property name="C_WDAPPL" dataType="stringValue"
valueType="simple">
                            <displayNames>
                                <displayName locale="en_US" name="WD Application"/>
                            </displayNames>
                            <values></values>
                        </property>
                        <property name="SENS" dataType="listValue" valueType="simple">
                            <displayNames>
                                <displayName locale="en_US" name="Sensitivity_1"/>
                            </displayNames>
```

```
                            <values>
                                <listValue name="CONF">
                                    <displayNames>
                                        <displayName locale="en_US" name="Confidential"/>
                                    </displayNames>
                                </listValue>
                            </values>
                        </property>
                        <property name="DOM" dataType="listValue" valueType="simple">
                            <displayNames>
                                <displayName locale="en_US" name="Domain"/>
                            </displayNames>
                            <values>
                                <listValue name="LOG">
                                    <displayNames>
                                        <displayName locale="en_US" name="Logistics"/>
                                    </displayNames>
                                </listValue>
                            </values>
                        </property>
                    </properties>
                </class>
            </classification>
        </by_system>
    </classification>
    <aborted_by_system>false</aborted_by_system>
    <aborted_by_user>false</aborted_by_user>
    <error>false</error>
    <!--Optional:-->
    <sim_mode>false</sim_mode>
    <!--Zero or more repetitions:-->
    <extended_tags>
        <key>Key1</key>
        <!--Optional:-->
        <value>Value1</value>
    </extended_tags>
</resulted_decision>
```

Key: `plmContextInfo` (Text as Type)

Description: Indicates the PLM server information (source).

Value: The value should look similar to the following.

```
<plm_context_info>
    <!--Optional:-->
    <event_type>user download</event_type>
    <browser_client>false</browser_client>
    <!--Zero or more repetitions:-->
    <pre_process_info>
        <!--Optional:-->
        <type>sample</type>
        <key>ABC</key>
        <value>12345</value>
    </pre_process_info>
    <!--Zero or more repetitions:-->
    <attributes>
        <!--Optional:-->
        <type>Attr1</type>
        <key>project_name</key>
        <value>CMS_Turbo_Engine</value>
    </attributes>
    <!--Optional:-->
    <document_id>1222</document_id>
    <!--Optional:-->
    <document_number>222</document_number>
    <!--Optional:-->
    <document_type>1</document_type>
    <!--Optional:-->
    <document_part>j</document_part>
    <!--Optional:-->
    <document_version>00</document_version>
    <!--Optional:-->
    <view_only>false</view_only>
    <!--Optional:-->
    <dms_process>false</dms_process>
</plm_context_info>
```

Key: `plmDestInfo` (Text as Type)

Description: Indicates the destination, such as which client the data was downloaded from.

Value: The value should look similar to the following.

```
<plm_destination_info>
    <!--Zero or more repetitions:-->
    <destination_attributes>
        <!--Optional:-->
        <type>Dest</type>
        <key>client_ip</key>
        <value>10.41.14.69</value>
    </destination_attributes>
    <!--Optional:-->
    <browser>Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/112.0.0.0 Safari/537.36</browser>
    <!--Optional:-->
    <hostname>ABC</hostname>
    <!--Optional:-->
    <ipaddress>10.41.14.69</ipaddress>
    <!--Optional:-->
    <operating_system>WIN10</operating_system>
</plm_destination_info>
```

4.4.7.2. Response

A successful request returns the following information: Status code: 200

Response to this request: In boolean value

```
true
```

The log is sent to the server.

4.5. Error Handling

An unsuccessful request returns a response code other than 200. If you receive a null response, you may need to review the input.

Status Code	Sample Message	Description
400 `BAD_REQUEST`	Monitor feature is not enabled	The Monitor feature is not activated in the portal.
401 `UNAUTHORIZED`	Unauthorized client attempting to access the endpoint. The page cannot be viewed because the client type is not licensed for it. Please contact the administrator.	Attempted to connect to an unlicensed endpoint.
`406` `NOT_ACCEPTABLE`	The System type is wrong. Please contact the administrator.	When any of the values, such as customer ID, system ID, or system type, are incorrect it will be stated in the error message.

Error Codes

5. Troubleshooting

This page will help you through the most common problems that may arise during the installation and configuration of the HaloENGINE and Service, which are described below.

5.1. HaloENGINE

As the first step in troubleshooting, make sure that your HaloENGINE version is up to date. Each release of HaloENGINE adds new features and fixes many problems. Installing the latest version may clear any problems without the need for further troubleshooting.

5.1.1. Forgot your Admin Portal Password

Symptoms

Login fails with the error message "*Invalid credentials*".

Background

Entered the wrong password to access the HaloENGINE Admin Portal.

Probable Cause

No matter how careful you are, there may be times when you are unable to access the admin portal because you can't remember your password.

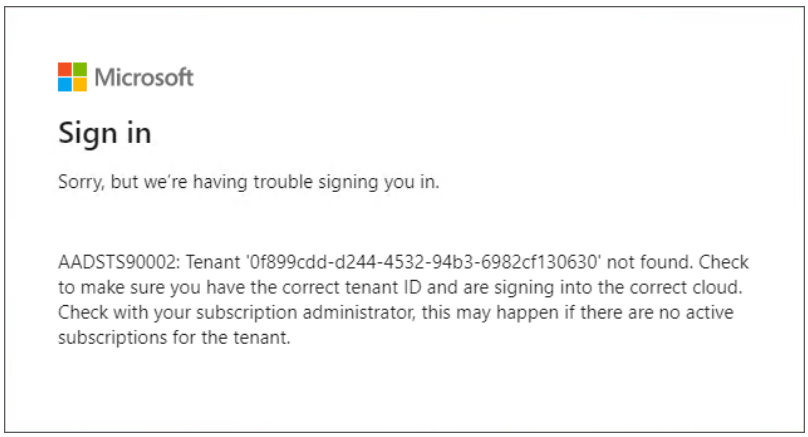
Recommended Action

1. Run Command Prompt as an administrator.
2. Type `haloengine-password-config.bat -h` to reset the password.
3. Log in with the new password.

5.1.2. Cannot Log in to Microsoft after Configuring the Tenant

Symptoms

The user login fails with the following error message.



Microsoft Sign-in error message

Background

The above error occurs when a user logs in to a HaloENGINE Admin Portal using Microsoft Sign-In.

Probable Cause

The Tenant ID/Client ID you entered on the *User Domain-Tenant Configuration* page is either incomplete or incorrect.

Recommended Action

1. Check that the Tenant ID/Client ID given on the *User Domain-Tenant Configuration* page is correct.
2. Log in to the admin portal.

5.1.3. Unable to Load the Admin Portal—Case 2

Symptoms

Error message #1 occurs in the browser when trying to open the HaloENGINE Admin Portal in the HTTPS protocol.

Background

The above-mentioned message appears when the user deletes the server and client certificates.

Probable Cause

Removing the server certificate permanently removes all other certificates (including client and CA certificates) and causes the admin portal to operate via the HTTP protocol only. This is expected behavior.

Recommended Action

1. Manually change the protocol from HTTPS to HTTP and the port to 8383.
2. Clear your web browser's HTTP Strict Transport Security (HSTS) settings. Please see this link for additional details: How to clear HSTS settings in Chrome and Firefox.

5.1.4. Unable to Load the Admin Portal or PDM Client could not Connect to HaloENGINE

Symptoms

1. Error message #1 occurs in the browser when opening the HaloENGINE Admin Portal.
2. HaloCAD for SOLIDWORKS PDM client cannot connect to HaloENGINE.

Background

The above-mentioned error occurs when the admin portal is attempted to open via `https://[server_IP]:8746/haloengine-admin/` but does not open. When a client attempts to connect to the portal, it is unable to connect.

Probable Cause

The HaloENGINE's IP address was modified after it was initially configured. It indicates that HaloENGINE attempts to run with the old IP address.

Recommended Action

Action 1: Use a static IP address

It is not recommended to frequently change the IP address of systems in a large network. Changing HaloENGINE's IP address affects communication with the PDM Client.

Action 2: Update the IP address in `hc-servlet.xml`

Proactive action: Make sure that the FQDN is used to generate the HaloENGINE server certificate instead of the system IP address.

In some circumstances, a strategic change in IP addresses is required due to network restructuring, security incidents, or significant infrastructure upgrades. In this circumstance, follow the steps below:

1. Locate the XML file in `C:/Program Files/Secude/Tomcat/webapps/haloengine-server/WEB-INF/hc-servlet.xml`.
2. Open the XML file and update the `publishedEndpointUrl` with the new IP address.

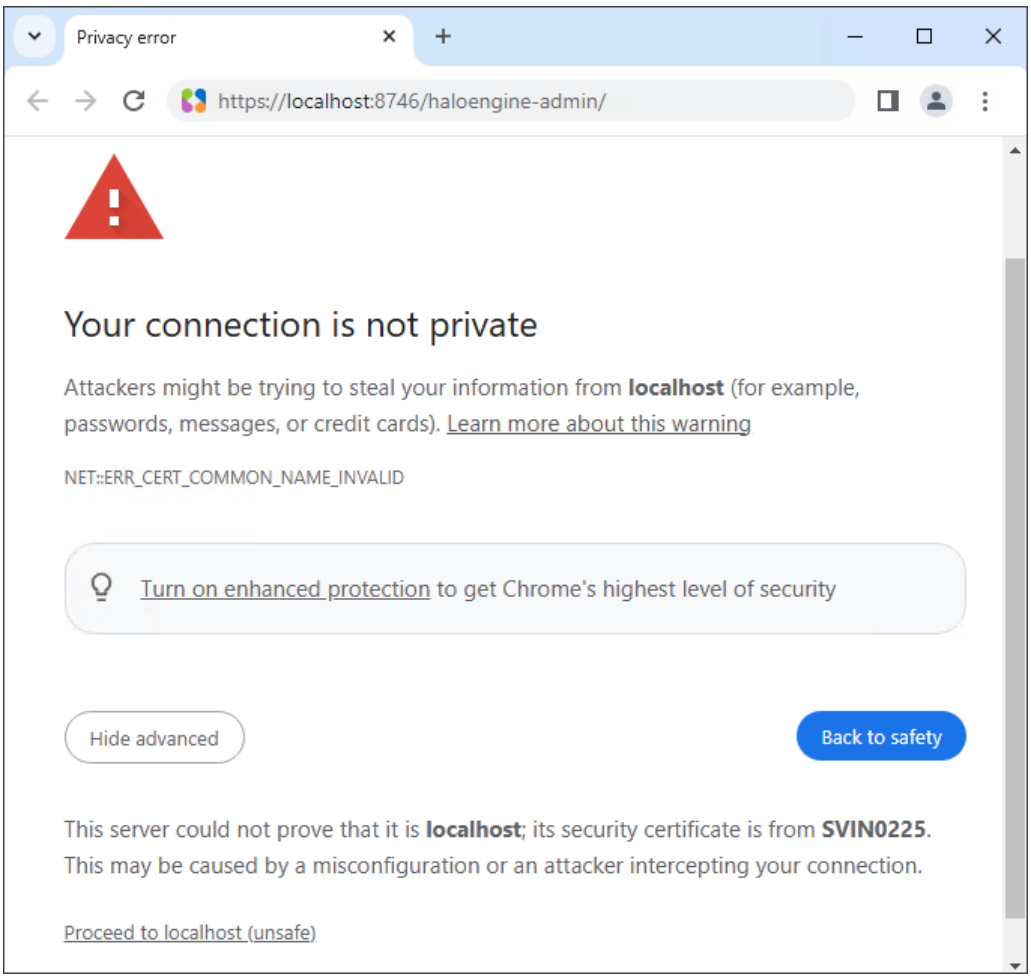
```
    <jaxws:endpoint id="HaloEngineProcessInterface"
        implementor="com.secude.haloengine.server.impl.HaloEngineProcessPortImpl"
        wsdlLocation="WEB-INF/haloengine-server-process.wsdl" address="/process"
        publishedEndpointUrl = "https://19.41.14.188:8746/haloengine-
server/process" />

    <jaxws:endpoint id="HaloEngineMonitorEndpoint"

implementor="com.secude.haloengine.server.interfaces.audit.HaloEngineServerMonitor
PortImpl"
        wsdlLocation="WEB-INF/haloengine-server-monitor.wsdl" address="/monitor"
        publishedEndpointUrl = "https://19.41.14.188:8746/haloengine-
server/monitor" />

    <jaxws:endpoint id="HaloEngineStatefulEndpoint"

implementor="com.secude.haloengine.server.interfaces.stateful.HaloEngineStatefulPo
rtImpl"
        wsdlLocation="WEB-INF/haloengine-stateful-process.wsdl"
address="/stateful_process"
        publishedEndpointUrl = "https://19.41.14.188:8746/haloengine-
server/stateful_process" />
```

3. Save the document.
4. Restart the Tomcat service.
5. Launch the admin portal via `https://[new_server_IP]:8746/haloengine-admin/`
6. HaloENGINE now runs on the new IP address, and other clients can communicate with it.

5.1.5. Unable to Access Admin Portal on Localhost

Symptoms

The following error message (`NET::ERR_CERT_COMMON_NAME_INVALID`) appears in the browser when attempting to load the HaloENGINE Admin Portal.



Privacy error message

Background

The above-mentioned issue occurs when the admin portal is attempted to open on localhost - `https://localhost:8746/haloengine-admin/`.

Probable Cause

After restarting the Tomcat service, the admin portal runs on localhost via HTTPS, and the browser displays an error message `NET::ERR_CERT_COMMON_NAME_INVALID`. This indicates that the certificate's common name does not match.

Recommended Action

1. Open a new browser.
2. Enter the HaloENGINE server's FQDN manually in the browser instead of using localhost. For example: `https://SVIN0225:8746/haloengine-admin/`.

5.1.6. Unable to Access the Admin Portal with FQDN

Symptoms

HaloENGINE Admin Portal cannot launch properly.

Background

When attempting to access the admin portal via `https://FQDN:8746/haloengine-admin/`, it does not open.

Probable Cause

The IP address of the HaloENGINE-installed server machine can change after the initial configuration.

Recommended Action

By default, the HaloENGINE server's Fully Qualified Domain Name (FQDN) is automatically configured in the `hc-servlet.xml` file, preventing dynamic IP issues. However, if you are still unable to access the admin portal, please add an entry to your hosts file that links your dynamic IP address to the appropriate FQDN. Furthermore, whenever your IP address changes, you must update the hosts file with the new address and the associated FQDN.
For example: "`<current_ip_address> <FQDN>`".

5.1.7. Protection Fails

Symptoms

Protection does not happen, or protection fails.

Background

When a user downloads a file, no protection is applied to the chosen file.

- For office files, the label is applied, and the file opens unprotected.
- For non-native files, no label is applied, and an error appears.

Probable Cause

This problem happens when one or more of the following conditions are met:

1. **Case 1**: If the Classification Engine is turned off.
2. **Case 2**: If the HaloENGINE Service is not registered and mapped to the current profile.
3. **Case 3**: If no Action/Classification rules are configured under Download Rules.
4. **Case 4:** If the HaloENGINE Service/HaloENGINE Tomcat Service stops unexpectedly.
5. **Case 5**: If the certificate used by the HaloENGINE Service has expired.
6. **Case 6:** If the System Unique ID on the Admin Portal does not match the System ID on the client system.

7. **Case 7** (only for SAP clients):
   a. HaloENGINE Server certificate is not imported into STRUST, or it was imported, but is no longer valid or has expired.
   b. HaloENGINE (Server) connection is not alive when connected with an SAP instance.
   c. If the **HaloENGINE Connection Parameters** are incorrectly set.

Recommended Action

1. **Case 1**: Check that the **Classification Engine** is turned on.
2. **Case 2**: Make sure that a registered HaloENGINE Service is mapped to an appropriate profile (**Customer ID**).
3. **Case 3**: Make sure to include an appropriate classification rule, followed by a suitable action rule.
4. **Case 4**: Check that the HaloENGINE Service is running; if not, restart it manually and then restart the HaloENGINE Tomcat Service. Note: It is recommended to restart the HaloENGINE whenever the HaloENGINE Service is restarted.
5. **Case 5**: Make sure to upload the same valid certificate that is already installed on the Windows Server machine where the HaloENGINE Service is installed.
6. **Case 6:** Check that the name entered in the admin portal's **System Unique ID** field matches the name entered in the **System ID** (in configuration properties). Also, make sure the names are case-sensitive. Make sure that the client system name matches the name entered in the admin portal's **System Unique ID** field. Also, make sure the names are case-sensitive. For example, if your client system name is 'MYDESKTOP', but you enter 'mydesktop' in the **System Unique ID** field, you will receive an error due to case sensitivity.
7. **Case 7** (only for SAP clients):
   a. If you are using a self-signed certificate, import a valid `HaloENGINEServer.cer` into STRUST.
   b. Check that the HaloENGINE connection is **Alive**.
   c. On the **HaloENGINE Connection Parameters** screen, be sure you select the option **Activate HaloENGINE** and enter the current profile that you are using in **Customer ID**.
8. Re-try downloading now.

5.1.8. Dashboard Fails to Load

Symptom

The dashboard window displays the error message "*Failed to get data*".

Background

HaloENGINE is installed in a custom location with an inbuilt MongoDB option during installation. After initializing the HaloENGINE admin portal, the Monitor log dashboard fails to load.

Probable Cause

HaloENGINE is installed in the Desktop location path.

Recommended Action

As a best practice, it is not recommended to install it on the HaloENGINE desktop location. However, if you install it on a desktop location, you will encounter this type of error. To resolve it, you need to grant sufficient permission to the Network Service.

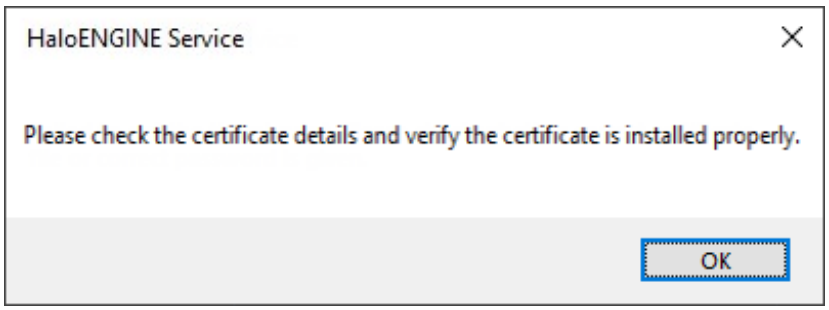
5.2. HaloENGINE Service

As the first step in troubleshooting, make sure that your HaloENGINE Service version is up to date. Each release of HaloENGINE Service adds new features and fixes many problems. Installing the latest version may clear any problems without the need for further troubleshooting.

5.2.1. Installation was Interrupted due to Certificate

Symptom

Error message: "*Please check the certificate details and verify the certificate is installed properly.*"



Certificate error message

Background

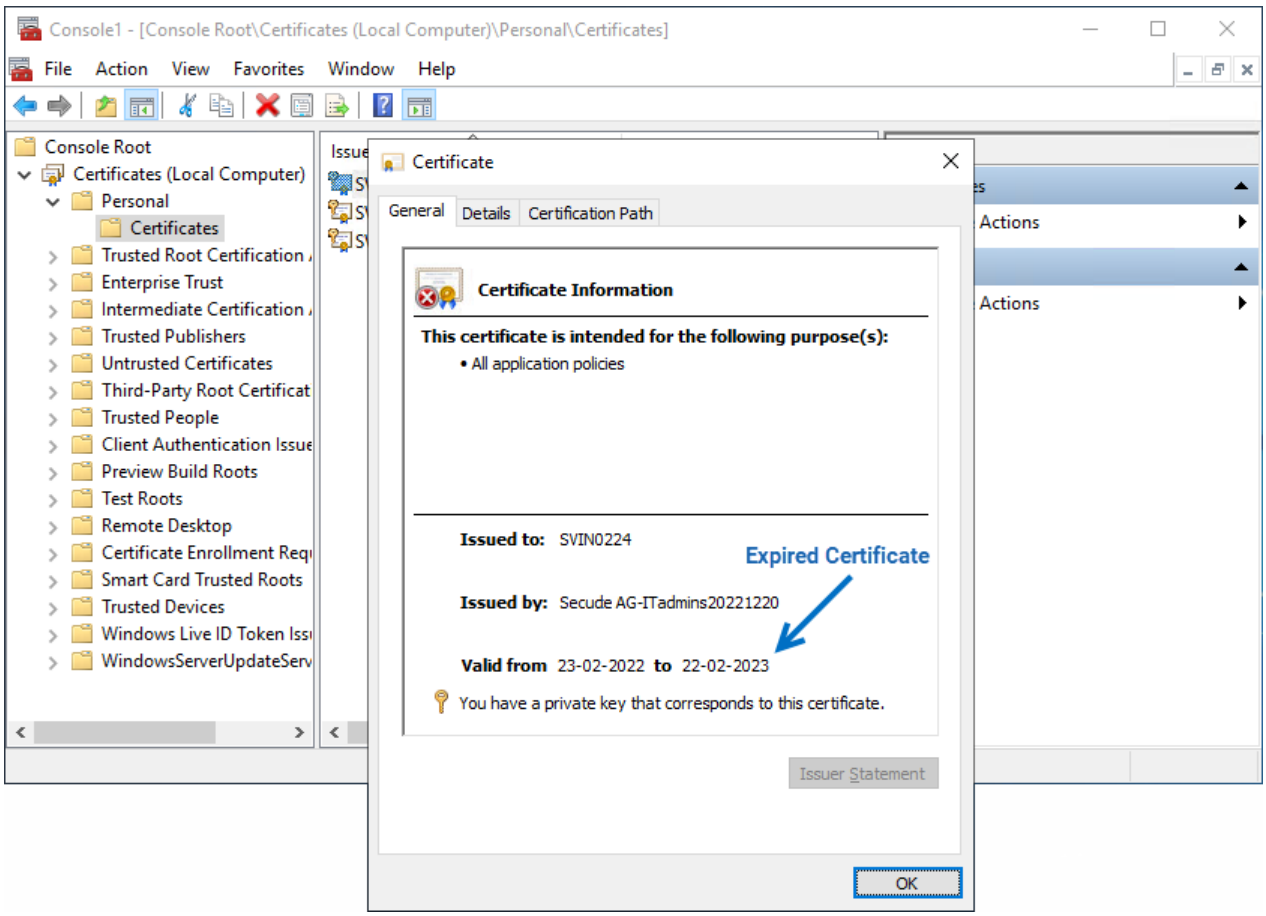
HaloENGINE Service installation in MPIP results in the error message shown above.

Probable cause

The certificate that you installed in the Certificate Store (Current User or Local Computer) has expired.

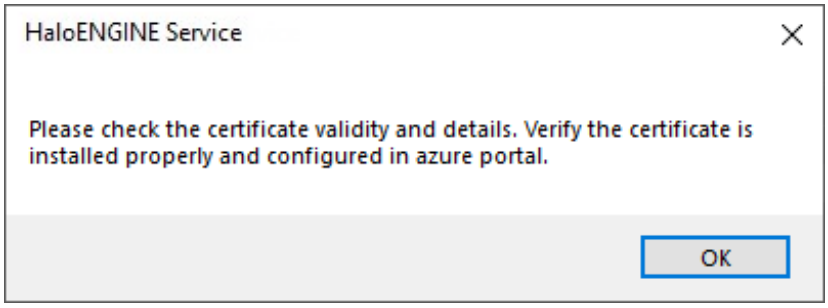
Recommended Action

1. Verify the certificate using the Microsoft Management Console (MMC) snap-in.



Certificate in MMC

2. If the certificate is invalid, add a new certificate.
3. If you proceed to install HaloENGINE Service at this point, you will receive the following message:



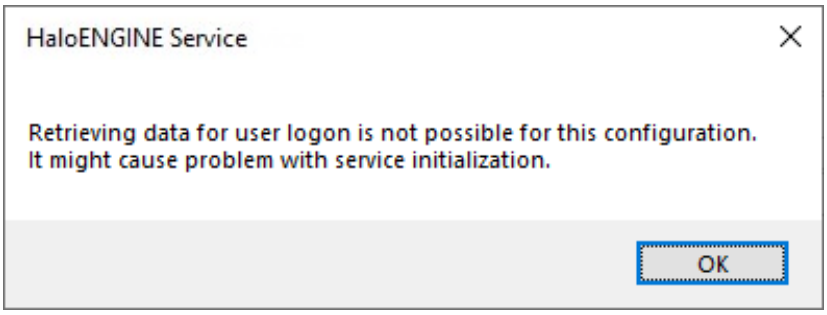
Mismatch of Certificate

4. Make sure that the same certificate is updated on the Azure portal (under the **Certificate** section > click **Upload certificate**).
5. Continue with the installation now.

5.2.2. Installation was Interrupted due to Improper Configuration

Symptom

Error message: "*Retrieving data for user logon is not possible for this configuration. It might cause problem with service initialization.*"



User login / RMS issue

Background

The error message given above appears while installing the HaloENGINE Service.

Probable cause

The username and domain were entered in the improper format.

Recommended Action

1. Enter the user's name in the proper format.
   a. To operate the HaloENGINE Service on a computer that is linked to a domain, you must input a domain user account and password. For example, `[domain]\[user]`, `hc.test\john`.
   b. On a non-domain linked machine, you must input a user's username and password. For example, `.\[user]`, `.\john`
2. Continue with the installation.

5.2.3. Network Related Issues

Symptom

Case 1

```
Something bad happened: Failed to send HTTP request with error code 'system:0' Inner
exception:
[http_exception:'SSL error: WINHTTP_CALLBACK_STATUS_FLAG_CERT_REV_FAILED failed to check
revocation status.'],
NetworkError.Category=Unknown, HttpRequest.SanitizedUrl=
https://api.aadrm.com/my/v2/publishinglicenses,
HttpRequest.Id=bbb8ae75-baba-4da5-ae6b-8d1e38d6f7fd, CorrelationId=90a5e1a4-914b-49c5-
851f-897aff78ef82,
CorrelationId.Description=ProtectionEngine, CorrelationId=106b4179-e86a-4681-86ef-
3bbaa05f9041,
CorrelationId.Description=FileHandler. Exiting
```

Case 2

```
"HTTP operation 5928aaf8-7b55-4bcb-bee3-be2a3dde2746 failed: Failed with:
[NetworkError: 'Failed to send HTTP request with error code 'system:0' Inner exception:
[http_exception: 'SSL error: WINHTTP_CALLBACK_STATUS_FLAG_CERT_REV_FAILED failed to
check revocation status. WINHTTP_CALLBACK_STATUS_FLAG_INVALID_CA SSL invalid CA. '],
NetworkError.Category=Unknown, HttpRequest.SanitizedUrl=https://api.aadrm.com/my/v2/
publishinglicenses, HttpRequest.Id=5928aaf8-7b55-4bcb-bee3-be2a3dde2746']"
`anonymous-namespace'::LogHttpOperationDetails
```

Background

File download/installation fails in MPIP mode, with any of the errors listed in the `MIP.log` file.

Probable cause

Case 1: Required endpoints stated in (row 125) Microsoft documentation are not permitted in network settings on ports 80 and 443.

Case 2: The problem was caused by an SSL proxy that was configured on the network.

Recommended Action

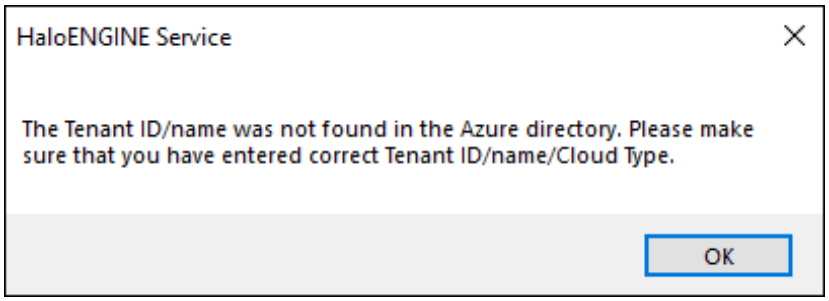
Case 1: Verify that both ports 80 and 443 on the network settings are open for the URL listed in row 125.

Case 2: Make sure that the SSL proxy's Root CA is installed on the PC that is running the HaloENGINE Service.

5.2.4. Initialization was Interrupted due to Incorrect Azure Details

Symptom

Error message: "*The Tenant ID/name was not found in the Azure directory. Please make sure that you have entered the correct Tenant ID/name/Cloud Type.*"



Invalid Azure details

Background

This error message appears during the initialization of the HaloENGINE Service.

Probable cause

The Azure information you provided is inaccurate.

Recommended Action

1. Make sure your Azure tenant ID or name is correct.
2. Choose the suitable cloud type.
3. Continue the installation.

5.2.5. HaloENGINE Service fails to Start

Symptom

The error appears as "*Process finished with error. Please check logs for more details*."

The HaloENGINE Service log shows the following error.

```
Cannot establish access to the shared memory [Global\0150B81D-A6E6-4EFD-B1FA-97172AD05C44HCS].

(hr = 0x80070005)

Access is denied.
```

Background

The error messages mentioned above appear while initializing the HaloENGINE Service.

Probable cause

This is because the **Administrators** rights have been removed from the **Create Global Objects** settings under **User Rights Assignment**.

Recommended Action

Add the following registry key `ipc_enable_file` in `HKEY_LOCAL_MACHINE\SOFTWARE\Secude\HaloENGINE Service` and reinitialize the service.

Name	Type	Data
ipc_enable_file	REG_SZ	on

Configuring registry entry

6. Customer Support and Feedback

Please be ready with the below-listed information before contacting our team to help you with the issue you are experiencing. The data that you provide will help us to serve you better.

1. Full contact details.
2. HaloENGINE and HaloENGINE Service build version.
3. Date, time, and description of the error (if possible, provide screenshots).
4. What (if any) third-party products (software or other) were used in conjunction with our product?
5. Any other information necessary to reproduce the error.

Secude offers help and support through

1. Technical support email: support@secude.com
   If you choose the email option to contact us, please provide your company details with a detailed description of the issue and attach the log file (if any). Our representative will respond to your email inquiry.
2. Phone support: Call +41 41 510 70 70 to talk to our representative to diagnose and resolve the technical problem.

Other resources

Please visit https://secude.com to know about upcoming events, press releases, and to download whitepapers.

6.1. Documentation Feedback

Secude understands the importance of technical content when attempting to gain product knowledge and strives to continuously improve product documentation to ensure that users receive the information they want. To provide feedback on the documentation, please send an email to documentation@secude.com. Please include the following details in your feedback:

1. Product name and version
2. Documentation topic
3. Details of the suggestion or error

The technical documentation team will consider your feedback and address it in future documentation updates.

7. Appendix

This section contains supplementary information.

7.1. Appendix 1 - SNC Configuration

Secure Network Communication (SNC) protects the logical link between the endpoints of a communication. To have a secure connection between the components, you need to enable SNC. The module SAPJCo is used to send data from the HaloENGINE to the AS ABAP. This communication uses the protocol RFC and needs to be protected with SAP Secure Network Communications (SNC).

> The explanation presented in this section is solely for purposes of illustration. For details regarding the setup and configuration of SNC in AS ABAP, please refer to the SAP Online Help (http://help.sap.com) to find an authoritative source of content.

Step 1: Enable SNC in AS ABAP

Before you start the enabling process in HaloENGINE, make sure that the following requirements are met in your SAP AS ABAP system:

1. Configured and started with SNC enabled.
2. An RFC user with access rights to the HaloENGINE audit Log.
3. The SNC-Name of the RFC user is set in the AS ABAP user management.
4. The PSE file with the client X.509 certificate of the RFC user and the PSE file password are available.

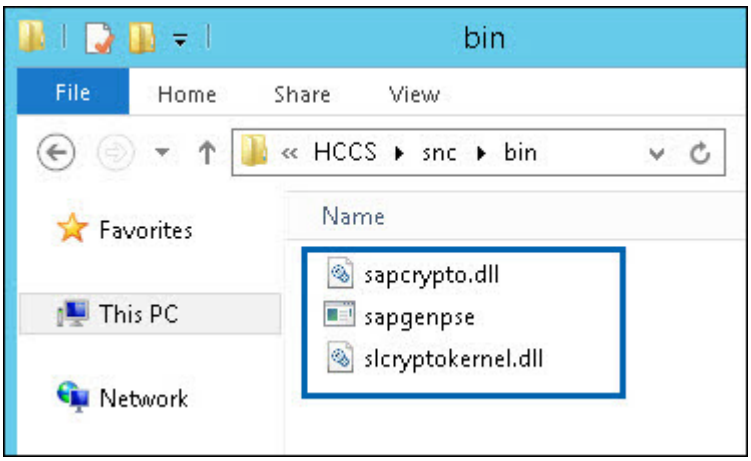
Step 2: Create folder structure in HaloENGINE

Create the following folder structure:

1. `\<path>\snc\bin`
2. `\<path>\snc\sec`

Step 3: Download and Install CommonCryptoLib in HaloENGINE

1. Login to "SAP Software-Downloads".
2. Navigate to "By Category -> SAP Cryptographic Software -> SAPCRYPTOLIB -> COMMONCRYPTOLIB 8 -> Downloads".
3. Select your operating system e.g., "WINDOWS ON X64 64BIT".
4. Download the latest version of SAPCRYPTOLIB.
5. Extract the archive via SAPCAR.
6. Copy the following files to `\<path>\snc\bin\`.

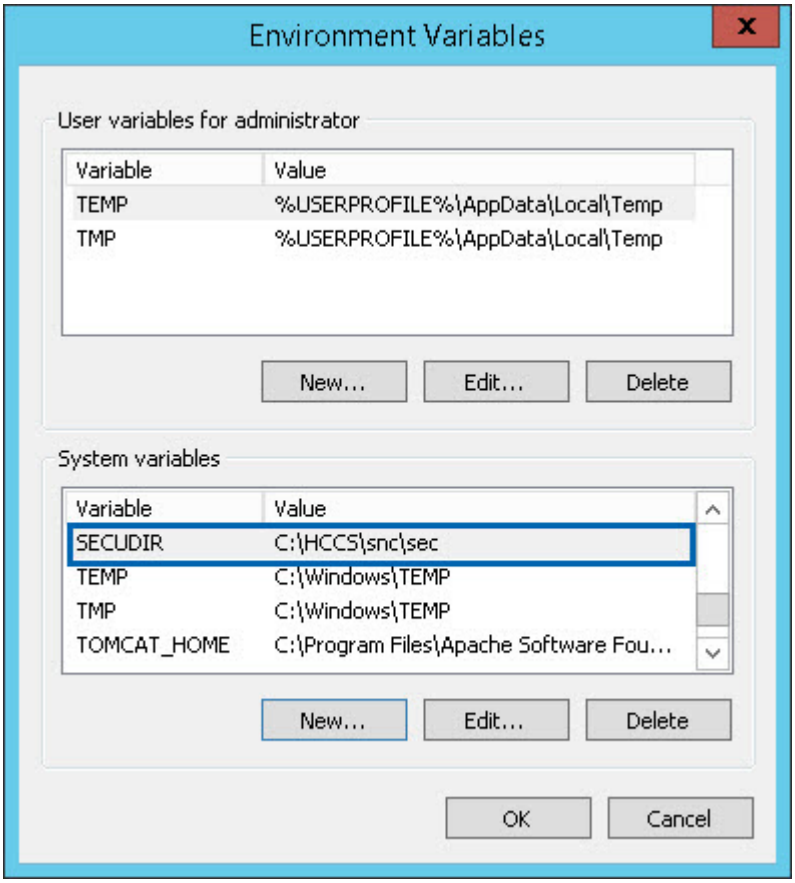


CommonCryptoLib files

Step 4: Set Environment Variable SECUDIR in HaloENGINE

The **CommonCryptoLib** uses the Environment Variable **SECUDIR** to access the PSE files and the Credentials.

1. Set the System Environment variable `SECUDIR to \<path>\snc\sec`.



Environment Variable SECUDIR

2. Restart the computer to make your system aware of these changes.

Step 5: Create PSE for the Client (HaloENGINE)

1. Execute the following command to generate the PSE.
2. In this step, a text file with certificate details will be generated.
3. This text file must be signed by your CA before you go to step 5a.

```
Run:
"\<path>\snc\bin\sapgenpse" get_pse -p "\<path>\snc\sec\<client>.pse" -x <password>
 -r \<path>\snc\sec\<client>.txt "CN=<distinguishedname>, O=<companyname>, C=<name>



Output would look similar to this example below:
Certificate Request
 Signed Part
 Subject :CN=JCOSNC, O=SECUDE, C=IN
 Key
 Key type :rsaEncryption (1.2.840.113549.1.1.1)
 Key size :2048
 Attributes
 Signature
 Signature algorithm :sha256WithRsaEncryption (1.2.840.113549.1.1.11)
 Signature (size="2048") :<Not displayed>
```

Step 5a: Import Root/Issuing CA certification into PSE

1. Make sure you have the Root CA.cer and signed `client.cer` in `\<path>\snc\sec\`.
2. Execute the following command to import the Certificate Authority.

```
Run:
"\<path>\snc\bin\sapgenpse" import_own_cert -p "\<path>\snc\sec\<client>.pse" -x
 <password> -c "\<path>\snc\sec\<client>.cer" -r "\<path>\snc\sec\ROOTCA.cer"



Output:
CA-Response successfully imported into PSE "C:\HCCS\snc\sec\jcosnc.pse"
```

Step 5b: Check the configuration

To check the configuration, run the following command:

```
Run:
"\<path>\snc\bin\sapgenpse" get_my_name -p "\<path>\snc\sec\<client>.pse" -x <password> -
v

Output would look similar to this example below:
Retrieving my certificate... ok.
Getting requested information... ok.
.
.
.
MY Certificate:
-------------------------------------------------------------------------------
Subject : CN=JCOSNC, O=SECUDE, C=IN
Issuer : EMAIL=itadmins@secude.com, CN=itadmins20110916, OU=IT Department, O=Secude AG,
SP=Nid walden, C=CH
.
.
.
-------------------------------------------------------------------------------
No additional forward certificate path (CA certificates).
Root Certificate:
-------------------------------------------------------------------------------
Subject : EMAIL=itadmins@secude.com, CN=itadmins20110916, OU=IT Department, O=Secude AG,
SP=Nid walden, C=CH
Issuer : EMAIL=itadmins@secude.com, CN=itadmins20110916, OU=IT Department, O=Secude AG,
SP=Nid walden, C=CH
.
.
.
-------------------------------------------------------------------------------
```

Note:

- Check whether the version of CommonCryptoLib is 8.5.10 or higher.
- Check whether the Environment Variable $SECUDIR points to \<path>\snc\sec.

Step 5c: Generate Credentials

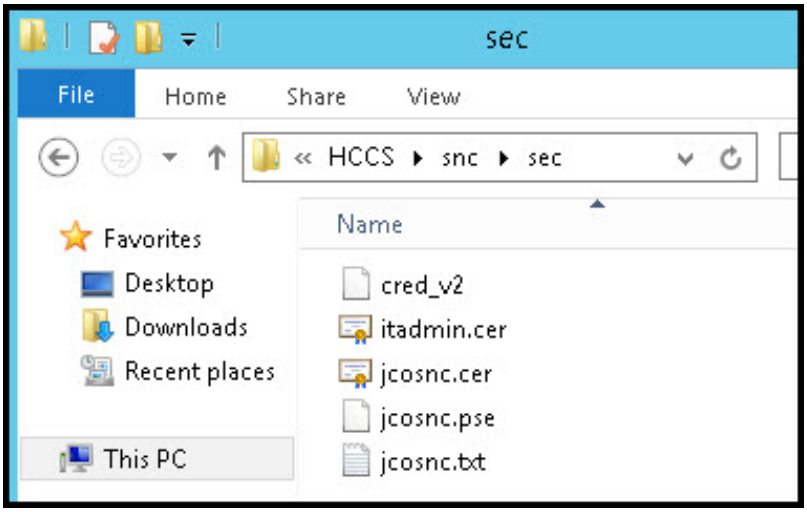
The PSE file is protected with the PSE file password. To give access to the PSE file, the Credentials file (cred_v2) needs to be created. The Credentials file contains the path and the password of the PSE file. To create the Credentials file, run the following command:

```
 Run:
"\<path>\snc\bin\sapgenpse" seclogin -p "\<path>\snc\sec\<client>.pse" -x <password> -O
SYSTEM


Output would look similar to this example below:
running seclogin with USER="Administrator"
 creating credentials for well-known group "NT AUTHORITY\SYSTEM" ...
 Adjusting credentials and PSE ACLs to include "NT AUTHORITY\SYSTEM"...
   C:\HCCS\snc\sec\cred_v2  ... ok.
   C:\HCCS\snc\sec\jcosnc.pse  ... ok.
 Added SSO-credentials for PSE "C:\HCCS\snc\sec\jcosnc.pse"
```

Note: If you run the CMD with the account which is used by the SAP JCo to access the Credentials file, then the option -O need not be given.

Step 5d: Check the content of the folder:

Your "sec" directory should contain the following files.



Folder content

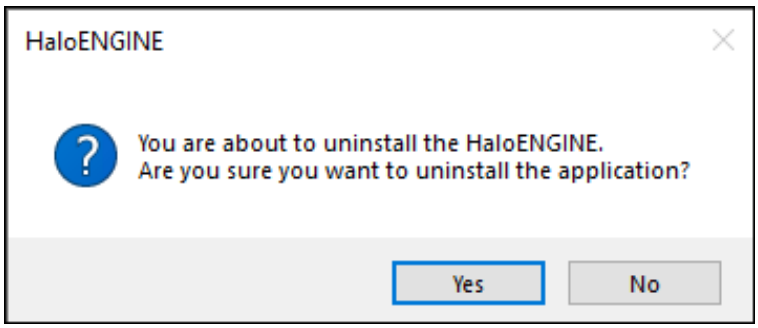
HaloENGINE SNC configuration is done, now the SAP JCo should be able to protect the RFC communication to the AS ABAP with SNC.

7.2. Appendix 2 - Uninstalling the HaloENGINE

Method #1

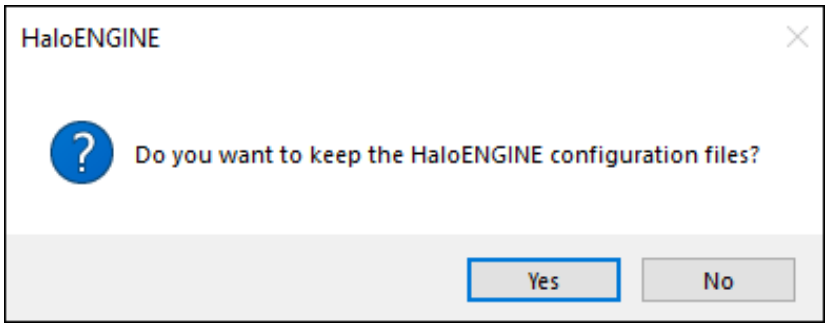
When you no longer use the service, you may uninstall the application. Uninstalling removes all files and registry settings that were added to your computer during the initial installation.

1. Click **Start** menu > go to **Control Panel** > **Programs** > **Programs and Features** > **Uninstall a Program** > select **HaloENGINE** application from the list > right-click and select **Uninstall** option or double-click on the installer `HaloENGINE_Setup.exe`.
2. Depending on your Windows security settings, you may get a security warning as "*Do you want to allow the following program to make changes to this computer*?". If you get this security warning, click the **Yes** button to confirm that you want to uninstall the application.
3. The following confirmation message will appear:



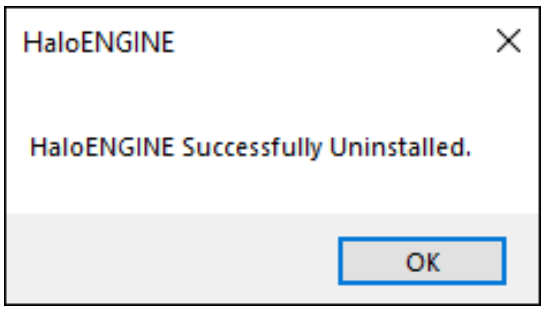
Uninstall message #1

4. Click **Yes** to confirm that you want to remove it from the computer.
5. You will be prompted to save a backup of the configuration files.



Uninstall message #2

6. Click **Yes** to save and continue with the uninstallation (The previous configuration files will be kept in the same location) or choose **No** to proceed with the uninstallation without saving.



Uninstall message #3

7. Click **OK** to close the message.

Method #2

The application can be removed using the command line, as illustrated in the sample below.

1. Open a command prompt.
2. Navigate to the application installer's directory.
3. Use the following commands to uninstall:

   Example #1: uninstall and keep the configuration files

   ```
   HaloENGINE_Setup.exe -uninstall -keepconfig true
   ```

   Example #2: uninstall and delete the configuration files

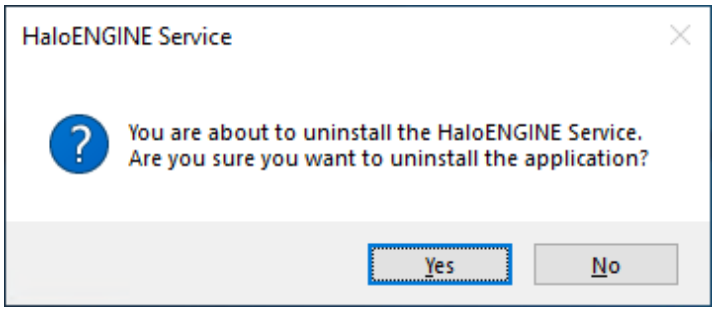
   ```
   HaloENGINE_Setup.exe -uninstall -keepconfig false
   ```

7.3. Appendix 3 - Uninstalling the HaloENGINE Service

When you no longer use the service, you may uninstall the application. Uninstalling removes all files and registry settings that were added to your computer during the initial installation.

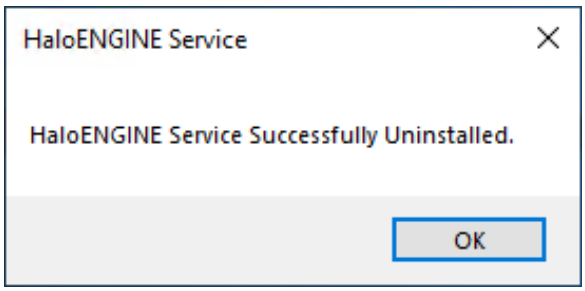
Method #1

1. Click **Start** menu > go to **Control Panel** > **Programs** > **Programs and Features** > **Uninstall a Program** > select **HaloENGINE Service** from the list > right-click and select **Uninstall** option.
2. Depending on your Windows security settings, you may get a security warning as "*Do you want to allow the following program to make changes to this computer*?". If you get this security warning, click the **Yes** button to confirm that you want to uninstall the add-on.
3. The following confirmation message will appear.



Uninstall message #1

4. Click **Yes** to confirm that you want to remove it from the computer.
5. The service is uninstalled successfully. Click **OK** to close the dialog.



Uninstall message #2

Method #2

Follow the below procedure to uninstall the service using a command.

1. Open a command prompt.
2. Navigate to the installation directory where the setup `exe` was extracted.
3. Use the following command to uninstall:

   Example:

   ```
   HaloENGINE_Service_Installer.exe -uninstall -silent true
   ```

7.4. Appendix 4 - Open-source Software (HaloENGINE)

Third-party software/code is included or bundled with Secude's products according to its appropriate license. Secude conducts testing to make sure the third-party products are compatible with and perform as intended with Secude applications.

The third-party libraries and dependencies used by HaloENGINE are shown in the table below.

Library	Version	Source Code	License Name	License Link
javax.xml.bind:jaxb-api	2.3.1	https://github.com/javaee/jaxb-v2	CDDL-1.0	https://javaee.github.io/glassfish/LICENSE
javax.xml.ws:jaxws-api	2.3.1	https://github.com/javaee/jax-ws-spec	CDDL-1.0	https://javaee.github.io/glassfish/LICENSE
javax.xml.soap:javax.xml.soap-api	1.4.0	https://github.com/javaee/javax.xml.soap	CDDL-1.0	https://github.com/javaee/javax.xml.soap/blob/master/LICENSE
javax.annotation:javax.annotation-api	1.3.2	https://github.com/javaee/javax.annotation	CDDL-1.0	https://github.com/javaee/javax.xml.soap/blob/master/LICENSE
com.sun.activation:javax.activation-api	1.2.0	https://repo1.maven.org/maven2/javax/activation/javax.activation-api/1.2.0/	CDDL-1.0	https://github.com/javaee/activation/blob/master/LICENSE.txt
com.sun.activation: jakarta.activation	1.2.2	https://github.com/javaee/activation	CDDL-1.0	https://javaee.github.io/glassfish/LICENSE
org.slf4j:slf4j-api	1.7.36	http://www.slf4j.org/download.html	MIT	http://www.slf4j.org/license.html
com.sun.xml.bind:jaxb-impl	2.3.5	https://github.com/javaee/jaxb-v2	CDDL-1.1	https://github.com/javaee/jaxb-v2/blob/master/LICENSE
jakarta.xml.bind:jakarta.xml.bind-api	2.3.3	https://github.com/eclipse-ee4j/jaxb-api	BSD 3	https://github.com/eclipse-ee4j/jaxb-api/blob/master/LICENSE.md

Library	Version	Source Code	License Name	License Link
joda-time:joda-time	2.12.7	https://github.com/JodaOrg/joda-time	Apache 2.0	https://github.com/JodaOrg/joda-time/blob/master/LICENSE.txt
net.iharder:base64	2.3.9	http://iharder.sourceforge.net/current/java/base64/	Public Domain	http://iharder.sourceforge.net/current/java/base64/
org.graylog2:syslog4j	0.9.61	https://github.com/graylog-labs/syslog4j-graylog2	LGPL 2.1	https://github.com/graylog-labs/syslog4j-graylog2/blob/master/LICENSE
ch.qos.logback:logback-classic	1.2.14	https://github.com/qos-ch/logback	LGPL 2.1	https://github.com/qos-ch/logback/blob/master/LICENSE.txt
ch.qos.logback:logback-core	1.2.14	https://github.com/qos-ch/logback	LGPL 2.1	https://github.com/qos-ch/logback/blob/master/LICENSE.txt
com.googlecode.json-simple:json-simple	1.1.1	https://github.com/fangyidong/json-simple	Apache 2.0	https://github.com/fangyidong/json-simple/blob/master/LICENSE.txt
org.apache.commons:commons-lang3	3.13	https://github.com/apache/commons-lang	Apache 2.0	https://github.com/apache/commons-lang/blob/master/LICENSE.txt
nl.basjes.parse.useragent:yauaa	5.23	https://github.com/nielsbasjes/yauaa	Apache 2.0	https://github.com/nielsbasjes/yauaa/blob/master/LICENSE
org.eclipse.persistence:org.eclipse.persistence.moxy	2.7.9	https://github.com/eclipse-ee4j/eclipselink/tree/master/moxy	EPL 2.0	https://github.com/eclipse-ee4j/eclipselink/blob/master/LICENSE.md

Library	Version	Source Code	License Name	License Link
com.google.guava:guava	33.0.0-jre.jar	https://github.com/google/guava	Apache 2.0	https://github.com/google/guava/blob/master/COPYING
org.apache.logging.log4j:log4j-api	2.20.0	https://github.com/apache/logging-log4j2	Apache 2.0	https://github.com/apache/logging-log4j2/blob/release-2.x/LICENSE.txt
com.javax0.license3j:license3j	3.2.0	https://github.com/verhas/License3j	Apache 2.0	https://github.com/verhas/License3j/blob/master/LICENSE.txt
javax.servlet:javax.servlet-api	4.0.1	https://github.com/javaee/servlet-spec	CDDL-1.0	https://github.com/javaee/servlet-spec/blob/master/LICENSE
org.apache.poi:poi-ooxml	5.2.3	https://github.com/apache/poi	Apache 2.0	https://www.apache.org/licenses/LICENSE-2.0
com.univocity:univocity-parsers	2.9.1	https://github.com/uniVocity/univocity-parsers	Apache 2.0	https://www.apache.org/licenses/LICENSE-2.0
com.opencsv:opencsv	5.9	https://github.com/cygri/opencsv	Apache 2.0	https://github.com/cygri/opencsv/blob/master/LICENSE
com.ibm.icu:icu4j	70.1	https://github.com/unicode-org/icu	ICU license	https://github.com/unicode-org/icu/blob/main/icu4c/LICENSE
com.fasterxml.jackson.core:jackson-databind	2.18.1	https://github.com/FasterXML/Jackson-databind	Apache 2.0	https://github.com/FasterXML/jackson-databind/blob/2.13/LICENSE
com.datastax.oss:java-driver-core	4.17.0	https://github.com/datastax/java-driver	Apache 2.0	https://github.com/datastax/java-driver/blob/4.x/LICENSE
com.datastax.oss:java-driver-query-builder	4.17.0	https://github.com/datastax/java-driver	Apache 2.0	https://github.com/datastax/java-driver/blob/4.x/LICENSE

Library	Version	Source Code	License Name	License Link
com.datastax.oss:java-driver-mapper-runtime	4.17.0	https://github.com/datastax/java-driver	Apache 2.0	https://github.com/datastax/java-driver/blob/4.x/LICENSE
org.json:json	20211205	https://github.com/vogella/org.json/tree/master/src	org.JSON	https://github.com/vogella/org.json/tree/master/src
org.apache.httpcomponents:httpclient	4.5.14	https://github.com/apache/httpcomponents-client	Apache 2.0	https://github.com/apache/httpcomponents-client/blob/master/LICENSE.txt
com.google.protobuf:protobuf-java	3.21.12	https://github.com/protocolbuffers/protobuf	BSD 3-Clause	https://github.com/protocolbuffers/protobuf/blob/master/LICENSE
org.apache.cxf:cxf-rt-frontend-jaxws	3.5.8	https://github.com/apache/cxf	Apache 2.0	https://github.com/apache/cxf/blob/master/LICENSE
org.apache.cxf:cxf-rt-rs-security-cors	3.5.8	https://github.com/apache/cxf	Apache 2.0	https://github.com/apache/cxf/blob/master/LICENSE
org.apache.cxf:cxf-rt-ws-rm	3.5.8	https://github.com/apache/cxf	Apache 2.0	https://github.com/apache/cxf/blob/master/LICENSE
com.sun.xml.ws:rt	2.3.0	https://jar-download.com/artifacts/com.sun.xml.ws/rt/2.3.0/source-code	EDL 1.0	https://javaee.github.io/metro-jax-ws/LICENSE
org.springframework: spring-context	5.3.33	https://github.com/spring-projects/spring-framework/tree/main/spring-context	Apache 2.0	https://github.com/spring-projects/spring-framework/blob/main/src/docs/dist/license.txt

Library	Version	Source Code	License Name	License Link
org.springframework:spring-web	5.3.33	https://github.com/spring-projects/spring-framework/tree/main/spring-web	Apache 2.0	https://github.com/spring-projects/spring-framework/blob/main/src/docs/dist/license.txt
org.codehaus.woodstox:stax2-api	3.1.4	https://github.com/FasterXML/woodstox	Apache 2.0	https://github.com/FasterXML/woodstox/blob/master/LICENSE
org.springframework.boot:spring-boot-starter-web	2.7.18	https://github.com/spring-projects/spring-boot	Apache 2.0	https://github.com/spring-projects/spring-boot/blob/main/LICENSE.txt
org.springframework.boot:spring-boot-starter-security	2.7.18	https://github.com/spring-projects/spring-boot	Apache 2.0	https://github.com/spring-projects/spring-boot/blob/main/LICENSE.txt
org.springframework.security:spring-security-jwt	1.1.1.RELEASE	https://github.com/spring-projects/spring-security-oauth	Apache 2.0	https://github.com/spring-projects/spring-security-oauth/blob/main/license.txt
o.jsonwebtoken:jjwt	0.9.1	https://github.com/jwtk/jjwt	Apache 2.0	https://github.com/jwtk/jjwt/blob/master/LICENSE
javax.resource:javax.resource-api	1.7.1	https://github.com/javaee/javax.resource	CDDL-1.0	https://github.com/javaee/javax.resource/blob/master/LICENSE
commons-io:commons-io	2.5	https://github.com/apache/commons-io	Apache 2.0	https://github.com/apache/commons-io/blob/master/LICENSE.txt
commons-fileupload:commons-fileupload	1.2.1	https://github.com/apache/commons-fileupload	Apache 2.0	https://github.com/apache/commons-fileupload/blob/master/LICENSE.txt

Library	Version	Source Code	License Name	License Link
commons-beanutils:commons-beanutils	1.9.4	https://github.com/apache/commons-beanutils	Apache 2.0	https://github.com/apache/commons-beanutils/blob/master/LICENSE.txt
org.springframework.boot:spring-boot-gradle-plugin	2.7.18	https://github.com/spring-projects/spring-boot/tree/main/spring-boot-project	Apache 2.0	https://github.com/spring-projects/spring-boot/blob/main/LICENSE.txt
org.springframework.batch:spring-batch-core	4.3.10	https://github.com/spring-projects/spring-batch	Apache 2.0	https://github.com/spring-projects/spring-batch/blob/main/LICENSE.txt
org.springframework.batch:spring-batch-infrastructure	4.3.7	https://github.com/spring-projects/spring-batch	Apache 2.0	https://github.com/spring-projects/spring-batch/blob/main/LICENSE.txt
org.springframework.boot:spring-boot-starter-actuator	2.7.18	https://github.com/spring-projects/spring-boot/tree/main/spring-boot-project	Apache 2.0	https://github.com/spring-projects/spring-boot/blob/main/LICENSE.txt
org.springframework.hateoas:spring-hateoas	1.4.1	https://github.com/spring-projects/spring-hateoas	Apache 2.0	https://github.com/spring-projects/spring-hateoas/blob/main/LICENSE
org.jolokia:jolokia-core	1.7.2	https://github.com/rhuss/jolokia	Apache 2.0	https://github.com/rhuss/jolokia/blob/master/LICENSE
org.dizitart:nitrite	3.2.0	https://github.com/nitrite/nitrite-java	Apache 2.0	https://github.com/nitrite/nitrite-java/blob/develop/LICENSE.md

Library	Version	Source Code	License Name	License Link
com.microsoft.azure:msal4j	1.7.1	https://github.com/AzureAD/microsoft-authentication-library-for-java	MIT	https://github.com/AzureAD/microsoft-authentication-library-for-java/blob/dev/LICENSE
org.springframework.boot:spring-boot-starter-oauth2-resource-server	5.8.2	https://github.com/spring-projects/spring-boot/tree/main/spring-boot-project	Apache 2.0	https://github.com/spring-projects/spring-boot/blob/main/LICENSE.txt
org.springframework.security:spring-security-oauth2-jose	5.8.2	https://github.com/spring-projects/spring-security	Apache 2.0	https://github.com/spring-projects/spring-security https://github.com/spring-projects/spring-security/blob/main/LICENSE.txt
org.springframework.security.oauth:spring-security-oauth2	2.5.2.RELEASE	https://github.com/spring-projects/spring-security	Apache 2.0	https://github.com/spring-projects/spring-security - https://github.com/spring-projects/spring-security/blob/main/LICENSE.txt
org.springframework.security:spring-security-oauth2-client	5.8.2	https://github.com/spring-projects/spring-security	Apache 2.0	https://github.com/spring-projects/spring-security - https://github.com/spring-projects/spring-security/blob/main/LICENSE.txt

Library	Version	Source Code	License Name	License Link
org.springframework.security.oauth.boot:spring-security-oauth2-autoconfigure	2.6.8	https://github.com/spring-projects/spring-security	Apache 2.0	https://github.com/spring-projects/spring-security - https://github.com/spring-projects/spring-security/blob/main/LICENSE.txt
Tomcat	9.0.102	https://github.com/apache/tomcat	Apache 2.0	https://github.com/apache/tomcat/blob/main/LICENSE
Java	11	https://github.com/adoptium/jdk	-	https://www.eclipse.org/legal/epl-2.0/
MongoDB	7.0.7	https://fastdl.mongodb.org/windows/mongodb-windows-x86_64		

Open-source software

7.5. Appendix 5 - Open-source Software (HaloENGINE Service)

Third-party software/code is included or bundled with Secude's products according to its appropriate license. Secude conducts testing to make sure the third-party products are compatible with and perform as intended with Secude applications.

The third-party libraries and dependencies used by the HaloENGINE Service are shown in the table below.

Library	Version	Source Code	License Link
Boost Library	1.85.0	https://archives.boost.io/release/1.85.0/source/	https://www.boost.org/LICENSE_1_0.txt
Protobuf Library	5.26.1	Release v5.26.1 · protocolbuffers/protobuf · GitHub	https://github.com/protocolbuffers/protobuf/blob/master/LICENSE
WTL	9.0	https://github.com/wxWidgets/wxWidgets	https://en.wikipedia.org/wiki/Common_Public_License
Rapidxml	1.13	https://sourceforge.net/projects/rapidxml/files/latest/download	http://rapidxml.sourceforge.net/license.txt
MIP SDK	1.16.126	https://learn.microsoft.com/en-us/information-protection/develop/version-release-history	https://docs.microsoft.com/en-us/information-protection/develop/

Open-source software

www.secude.com

About Secude

Secude, a Microsoft and SAP Partner, is a global leader for Zero Trust Data-centric security and Enterprise Digital Rights Management (EDRM) solutions.

For more than 25 years Secude has been trusted by many Fortune 500 and DAX-listed companies for architecting, implementing, and protecting their data. Our data-centric security professionals apply their passion and deep domain expertise to provide a holistic approach to protect priceless Intellectual Property (IP) in CAD & SAP based collaborations and supply chains.

With branches in Europe, North America and Asia, Secude supports customers with the implementation of IT security strategies through a global network.