Secude

HaloENGINE

Installation and Configuration Manual

Version 6.10

Copyright

Contact

Secude Solutions AG

Murbacherstrasse 19

6003 Luzern, Switzerland

Mail: info@secude.com

Support

Web: https://support.secude.com

Mail: support@secude.com

Table of Contents

Typographic Conventions

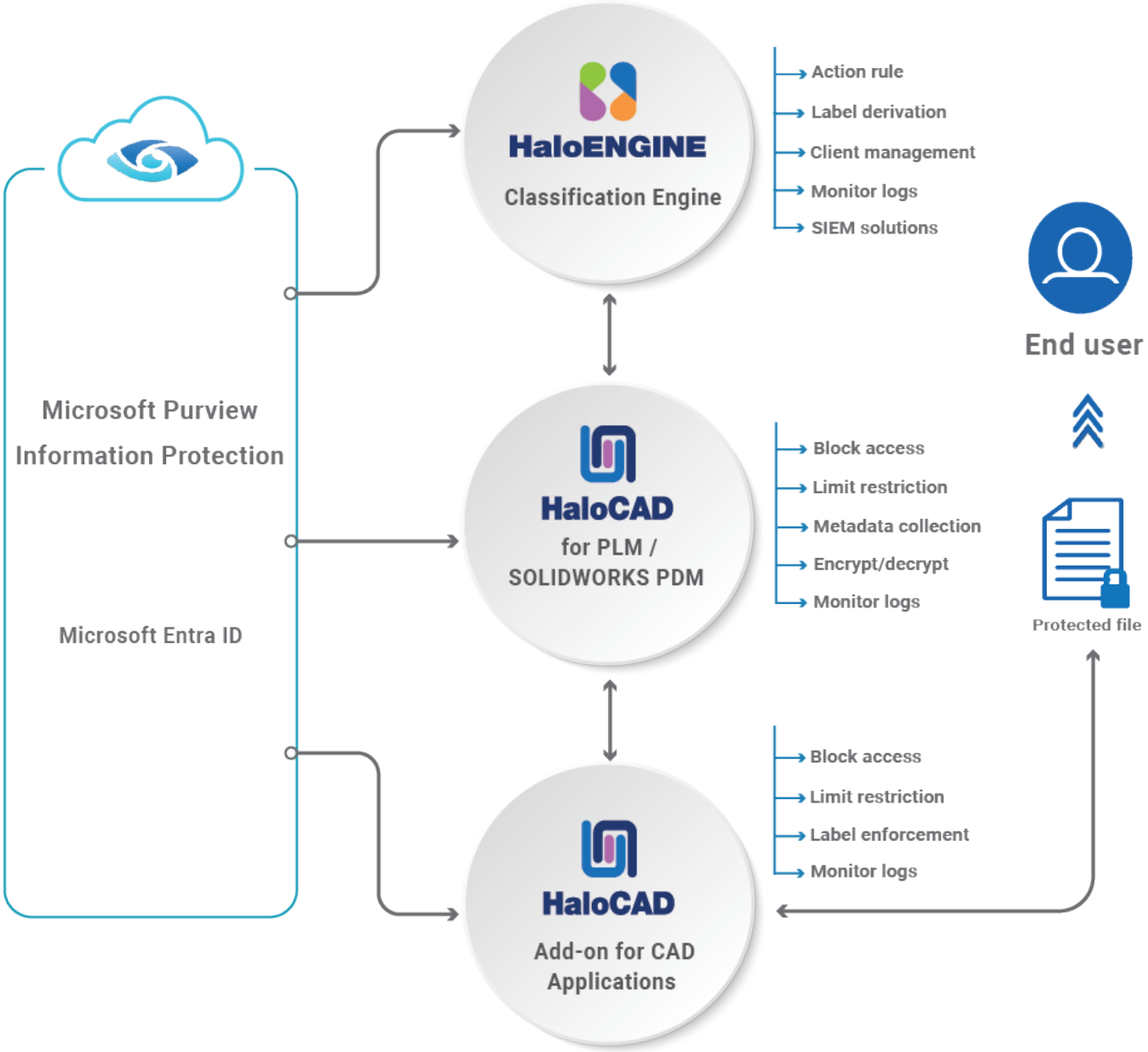
This guide uses the following typographic conventions to distinguish types of in-text information and icons to alert you to important information.

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 classification engine that applies business logic and integrates with the Microsoft Purview Information Protection service to fetch the sensitivity labels for configuration in the admin portal. Using metadata, it classifies and organizes data while enforcing schemas and action rules, serving as the core component that works with the HaloCAD for PLM/PDM solution to protect data.

The HaloCAD for PLM solution integrates with the PLM application, includes HaloCAD PROTECT and HaloCAD MONITOR features, and leverages Microsoft Purview Information Protection (MPIP), formerly Microsoft Information Protection (MIP), to provide Enterprise Digital Rights Management (EDRM). During file download, HaloENGINE receives relevant metadata from HaloCAD for PLM/PDM, determines the appropriate action based on the configured rules, and forwards the label and action information to HaloCAD for PLM/PDM for file processing (encryption).



HaloENGINE integrated with HaloCAD for PLM/PDM solution

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, including Microsoft Azure Sentinel, Splunk, RSA, and others.
4. Halochain: Verifies whether the log file has been tampered with or not.
5. Dashboard: Displays important performance indicators and metrics, providing an overview of the company's data upload and download events.

1.1. About this Manual

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

1. HaloENGINE
2. HaloENGINE API

About the Term “HaloENGINE Tomcat Service”

The HaloENGINE Tomcat Service is a common component used in both the HaloENGINE and HaloCAD products. Since it was initially developed for HaloENGINE and later adopted across HaloCAD, all Tomcat instances in Secude appear under the name “HaloENGINE Tomcat Service.”

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 that 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 appropriate action on the relevant content in this situation using 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's 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 are 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

When creating classification labels, consider the following recommendations:

1. **Leverage existing classification schemas (if available):**
   Reuse established frameworks within your organization to maintain consistency and reduce redundancy.
2. **Use sub-labels for key departments:**
   Certain departments may have unique classification requirements. Create sub-labels to address these specific needs. For example, Finance-Confidential, HR-Confidential.
3. **Choose meaningful label names:**
   Avoid using acronyms or ambiguous terms. Ensure label names clearly reflect their purpose and meaning.

Classification Rule

Rules are defined based on metadata and action rules to determine whether to block, label, protect, or decrypt a file.

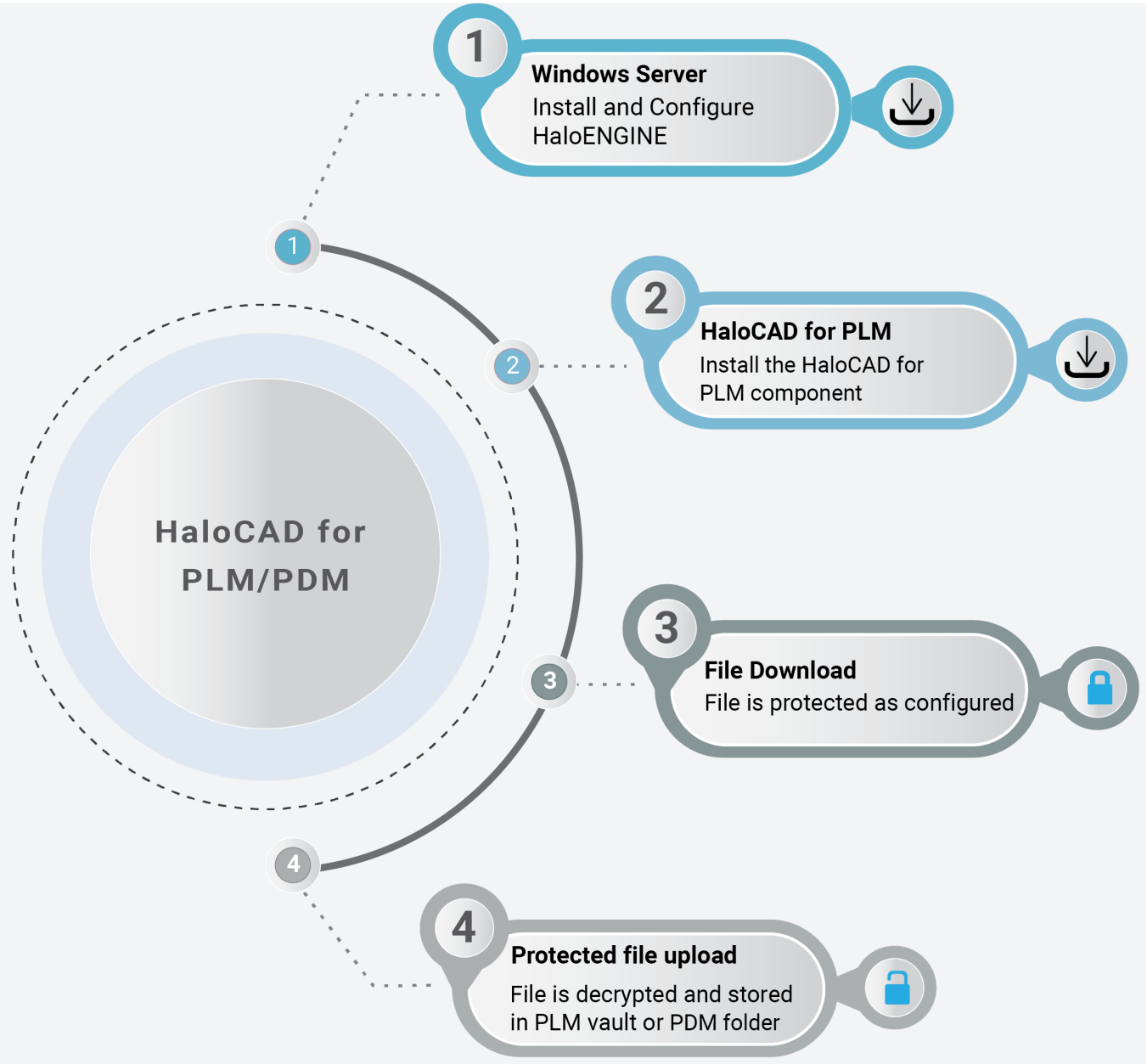
Use the table below to decide how you want to deploy the features.

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.

Action description

2. Quick Start Installation Summary

The following visual illustrates the high-level concept of configuring HaloENGINE with HaloCAD.



Quick start installation steps

Reference Manuals

The table below describes where to obtain information.

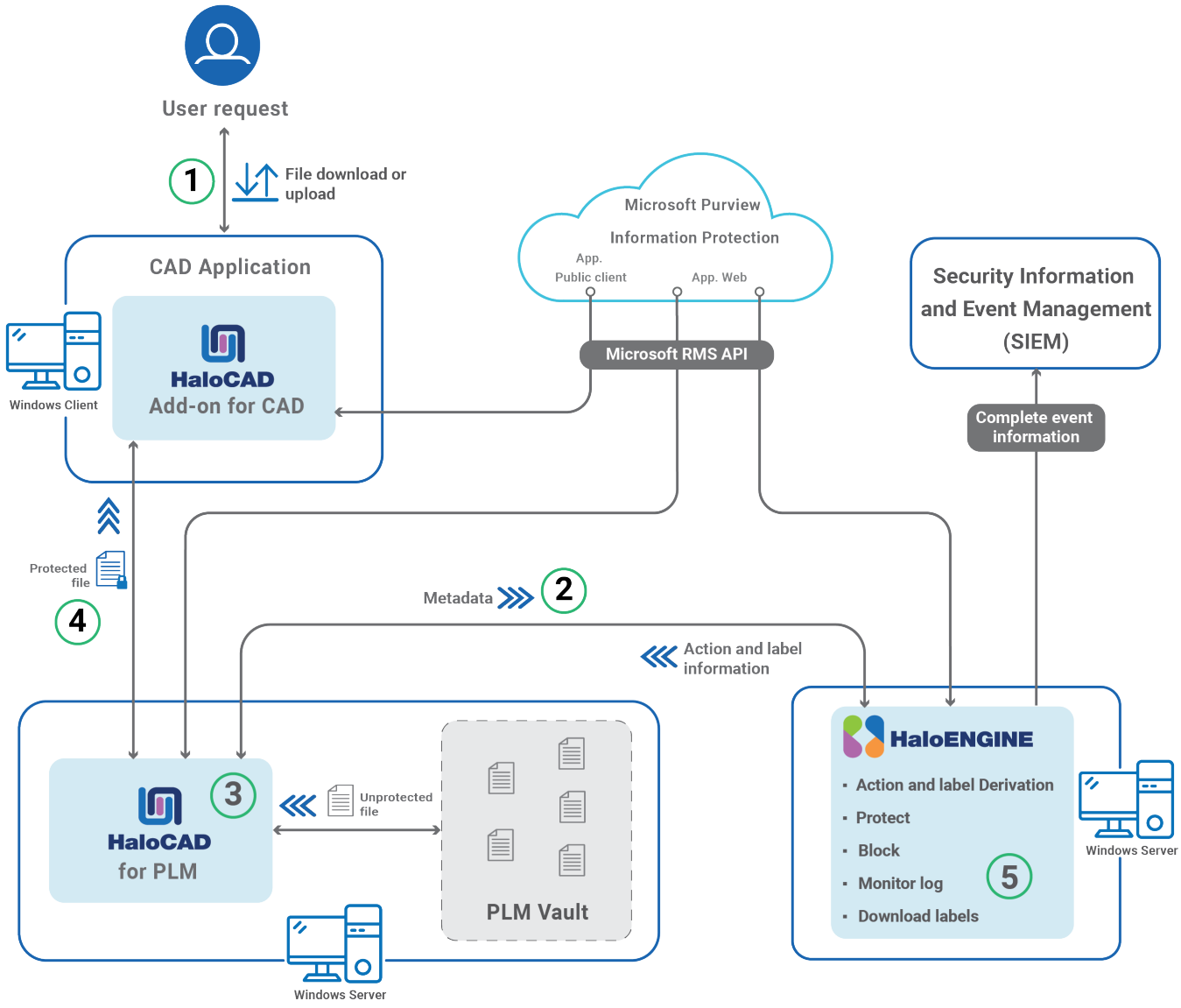
Component	Refer to
Step 1 – How to install and configure HaloENGINE.	Refer to the current manual.

Component	Refer to
Step 2 – How to install HaloCAD for PLM/PDM.	Please refer to the respective HaloCAD for the PLM/PDM Installation Manual you have purchased
Steps 3 and 4 – Workflow illustrating protection and decryption	Please refer to the respective HaloCAD for the PLM/PDM Operations Manual you have purchased

Reference Manuals

3. How does it work?

At a high level, the workflow between HaloCAD for PLM and HaloENGINE is illustrated in the following steps:



Integration Workflow: HaloCAD for PLM and HaloENGINE

1. The user performs a check-out (download) or check-in (upload) action.
2. HaloCAD for PLM fetches the user-selected file and collects its metadata. The metadata is sent to the HaloENGINE, where the appropriate action and label information are derived and provided back to HaloCAD for PLM.
3. HaloCAD for PLM executes actions based on the derived action and label information:
   a. If no valid action is available, the file is downloaded without modification.

b. During check-in, if a valid action with a label is found, HaloCAD for PLM removes the label and stores the decrypted file in PLM.

c. During check-out, if a valid action with a label is found, HaloCAD for PLM applies the label.

d. If a block action rule is configured in HaloENGINE, HaloCAD for PLM prevents file downloads.

4. The protected file is returned to the user.
5. HaloCAD for PLM captures the event details and forwards them to the HaloENGINE monitor log for auditing.

4. System Requirements

This section describes the minimum and recommended system requirements for installing and running the application. It specifies the software dependencies, operating systems, and network prerequisites. Ensuring that the target environment meets these requirements is essential for a successful deployment, optimal performance, and reliable operation of the system.

Components	Details
Operating System	Supported only on Microsoft Windows Server 2022 or later with the latest system updates installed.
Applications	1. MongoDB Compass 7.0.7 2. Requires **.NET** Framework 4.6.2 and above. 3. The HaloENGINE Admin portal supports the most recent versions of Microsoft Edge, Chrome, and Firefox.

Requirements

5. Prerequisites

This chapter describes the prerequisites that must be completed before installing and configuring HaloENGINE. These steps ensure that the product integrates smoothly with your organization's security and compliance infrastructure. The following setup tasks are required:

1. Register an application in Microsoft Entra ID.
2. Provide Microsoft Office 365 subscription details.
   - Create and configure sensitivity labels.
   - Configure recommended URLs, addresses, and ports for MPIP.
   - Enable support for TLS 1.2 at the client workstation for Microsoft Entra ID.
3. Ensure HaloENGINE Tomcat service runtime conditions are met.
4. Obtain the HaloENGINE license.
5. Configure User Management Settings in the Azure portal.
6. Set up Microsoft Sentinel.

Completing these prerequisites in advance helps streamline the deployment process and ensures that HaloENGINE functions as intended within your environment.

5.1. Register 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.

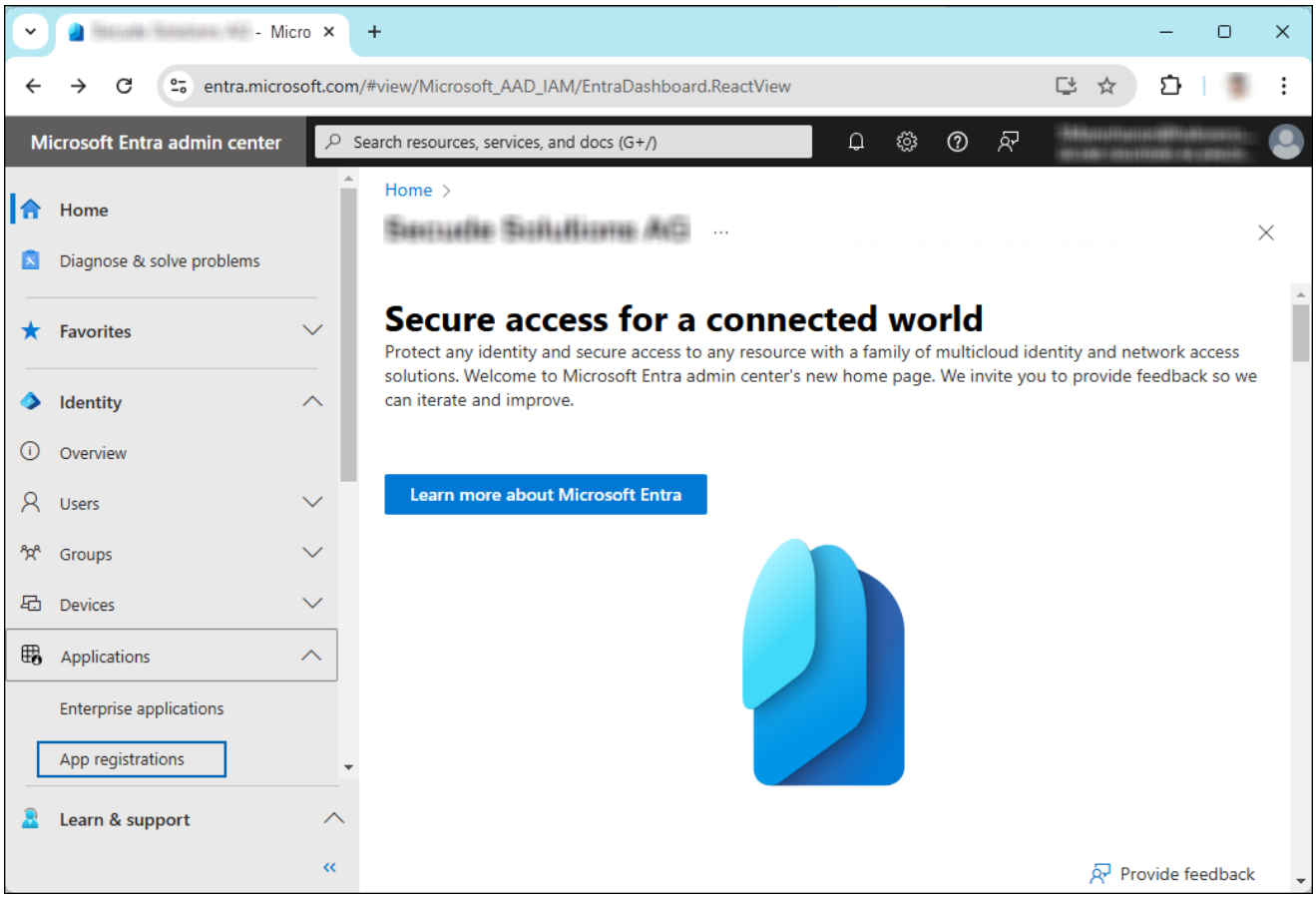
Prerequisite: You must have sufficient permissions to register an application with your Microsoft Entra ID tenant.

5.1.1. Create an Application

Follow these steps to register the application:

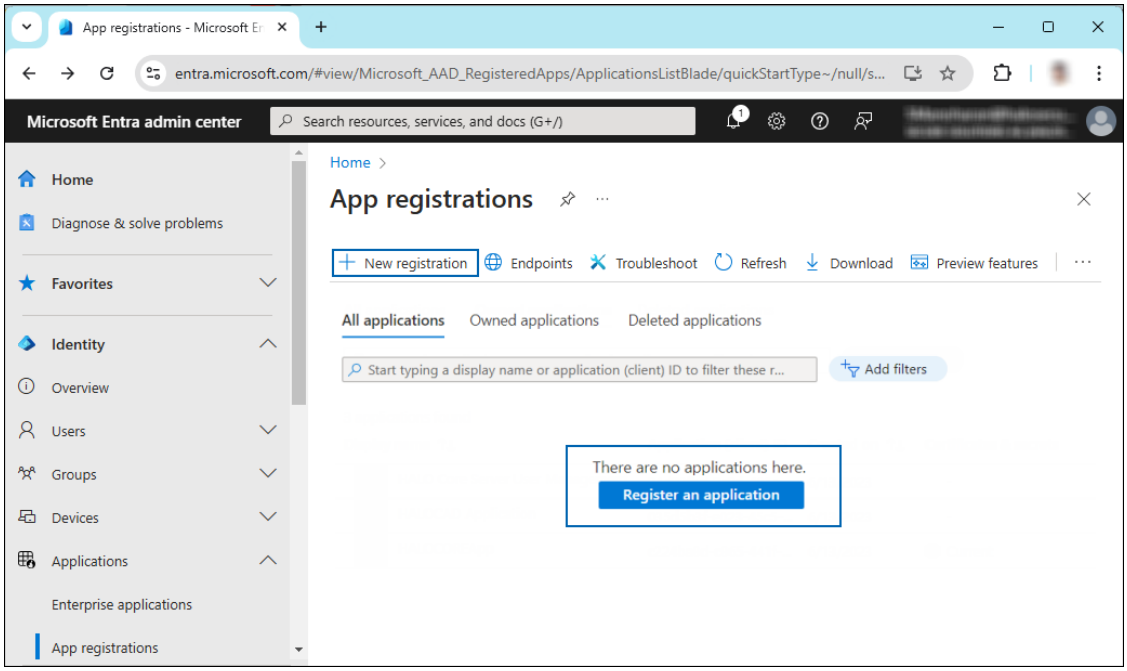
1. Log in to the Microsoft Entra admin center using an account that has administrator privileges.

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.



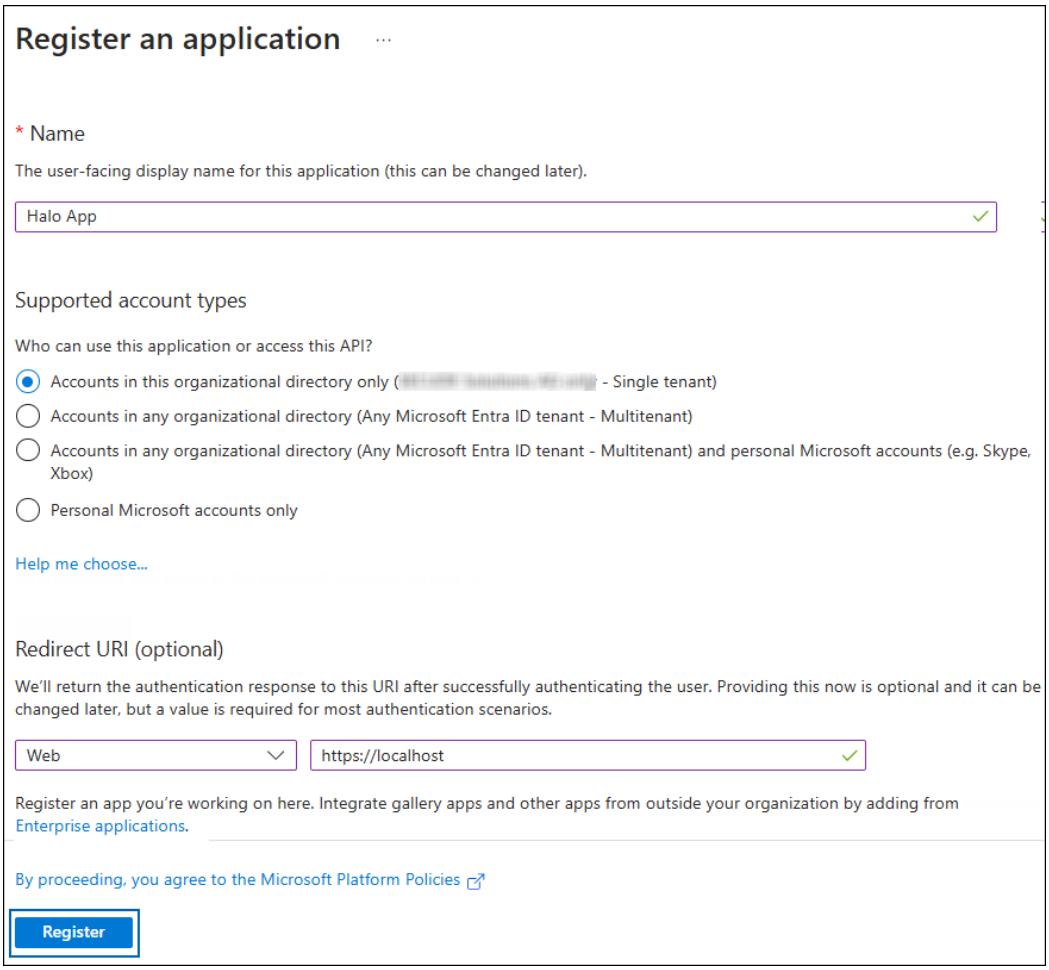
Selecting Microsoft Entra ID

4. Click **Identity** > **Applications** > **App registrations** on the left of the navigation pane.
5. 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

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



Application details

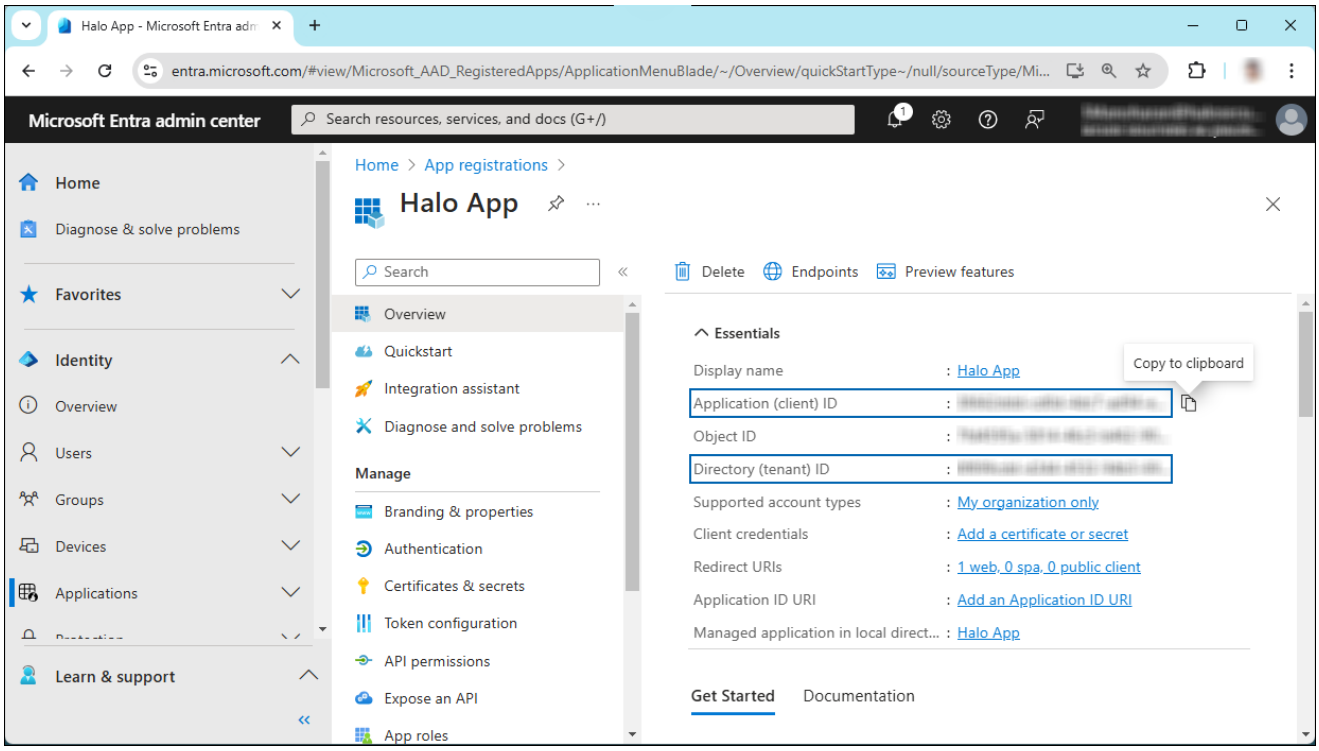
a. In the **Name** field, enter an appropriate application name.

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

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



Application ID and Tenant ID

8. 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**.

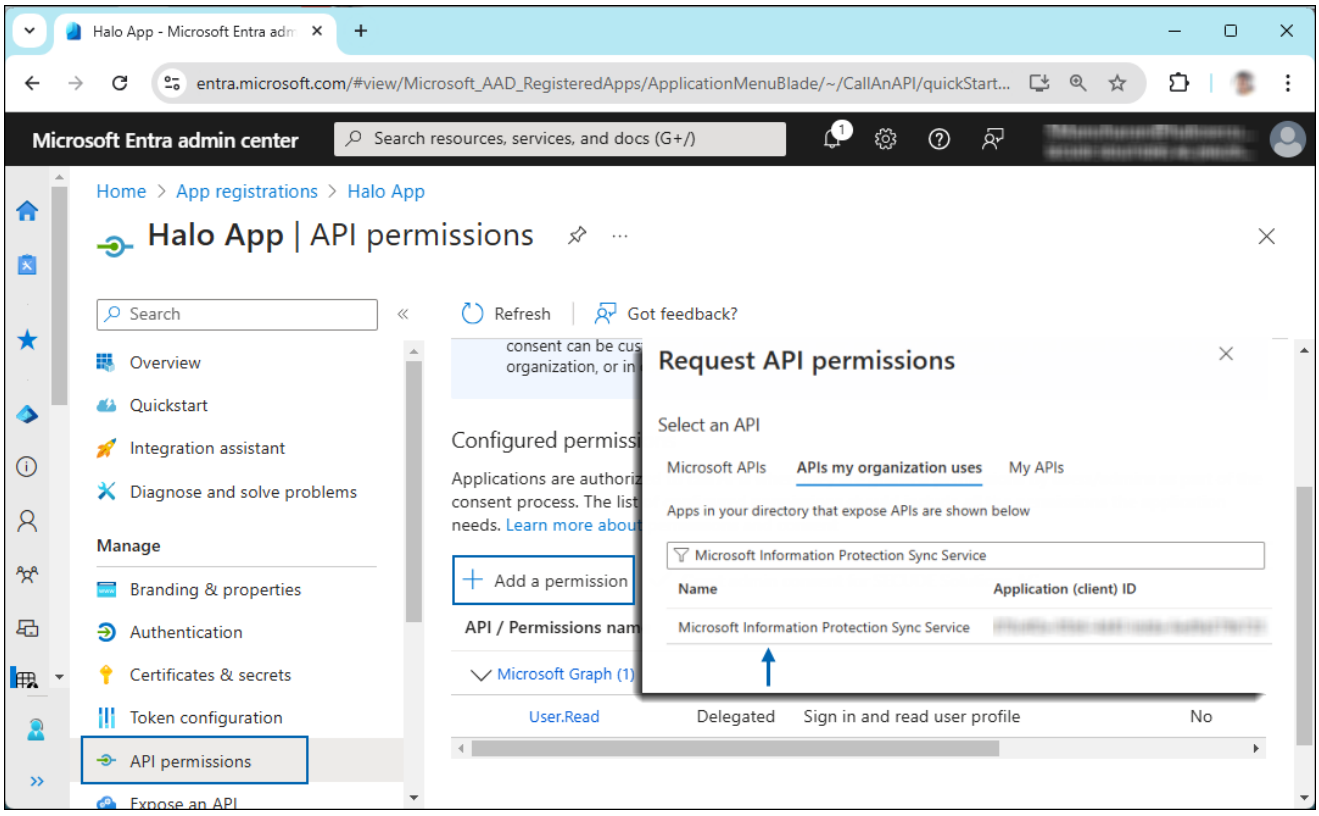
Save the authentication parameters

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 Tomcat Service.

5.1.2. Add Required Permissions

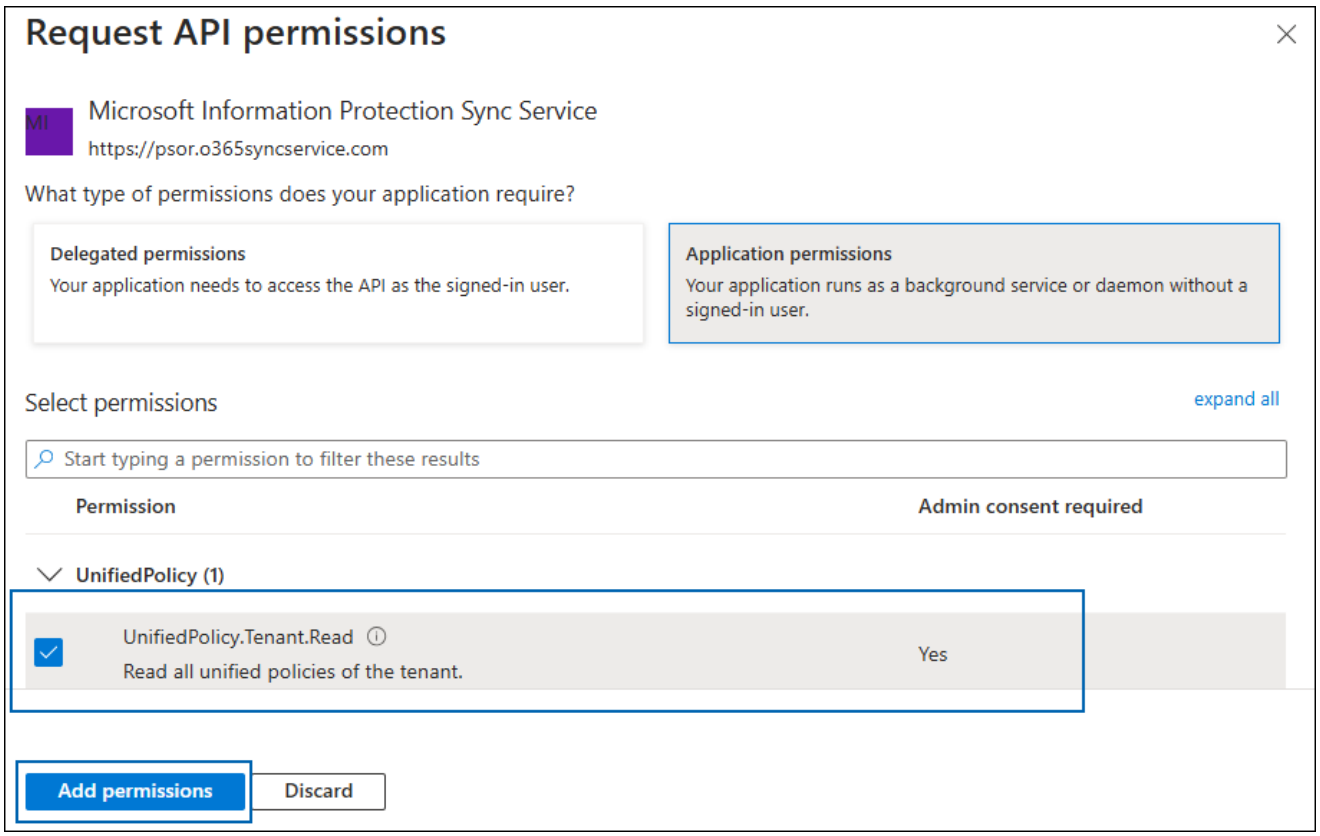
To protect content with MIP SDK, you must provide the necessary API permissions to the application created in the previous section.

1. In the sidebar of the application page, select **API permissions**. The **API permissions** page for the new application registration 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:



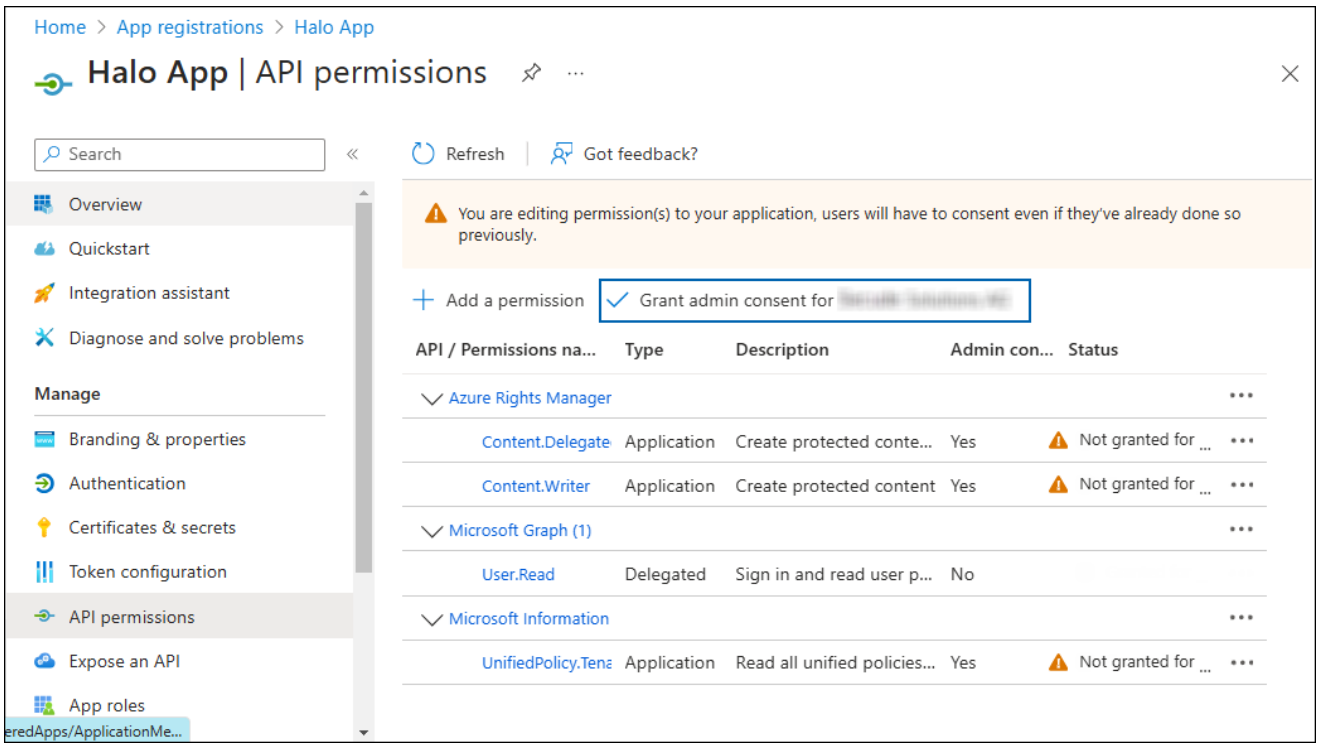
API selection

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 near "**Read all unified policies of the tenant**."



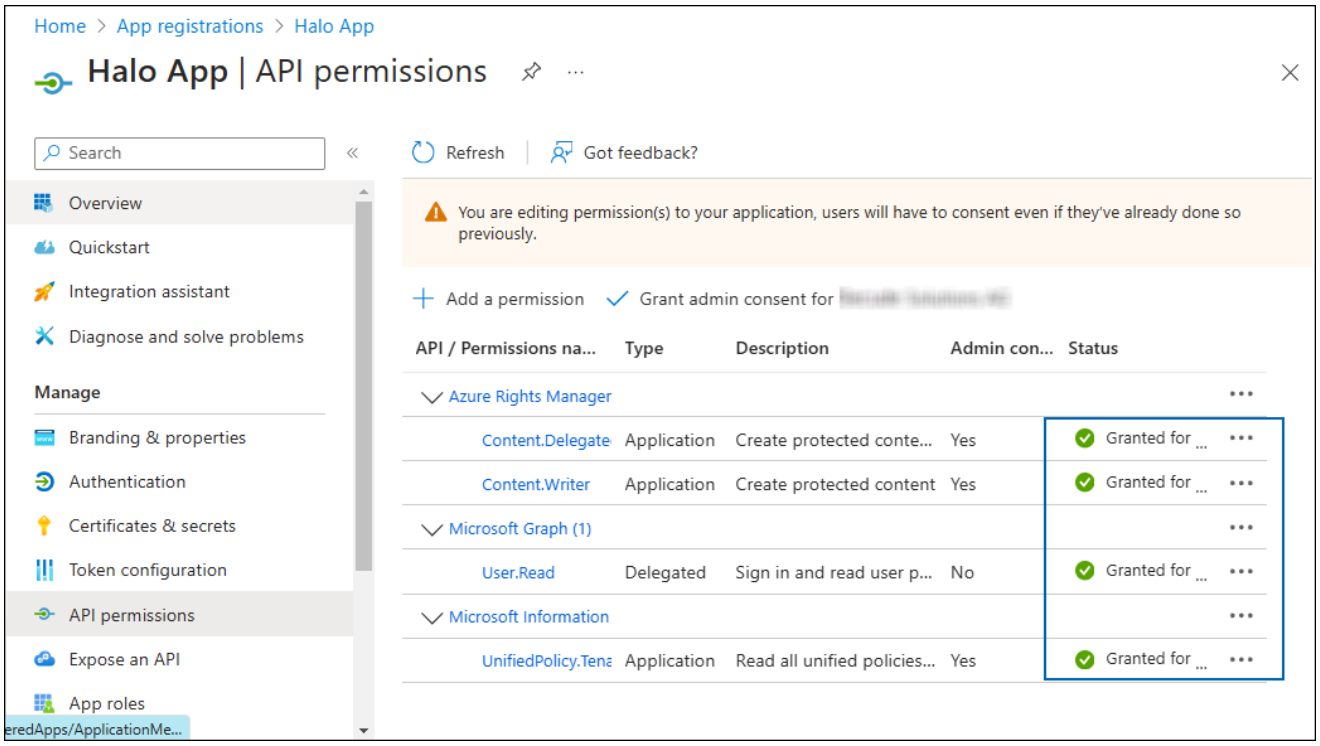
Adding permission

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 the HaloENGINE Tomcat Service does not use it.
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 permissions mentioned above 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 Tomcat Service requires the following 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

5.1.3. Upload the Certificate in the Azure Portal

The HaloENGINE Tomcat Service relies on certificate-based authentication to access MPIP services. Therefore, you must enter your certificate information in the registered application before proceeding with the configuration.

Prerequisites:

1. **Certificate**:

a. Ensure that you have a valid certificate containing the following key properties: `-KeyExportPolicy Exportable` and `-KeySpec Signature`.

b. The certificate can also be self-signed. Note: As a best practice and for security reasons, use a self-signed certificate only in a test environment. It is not recommended for production environments.

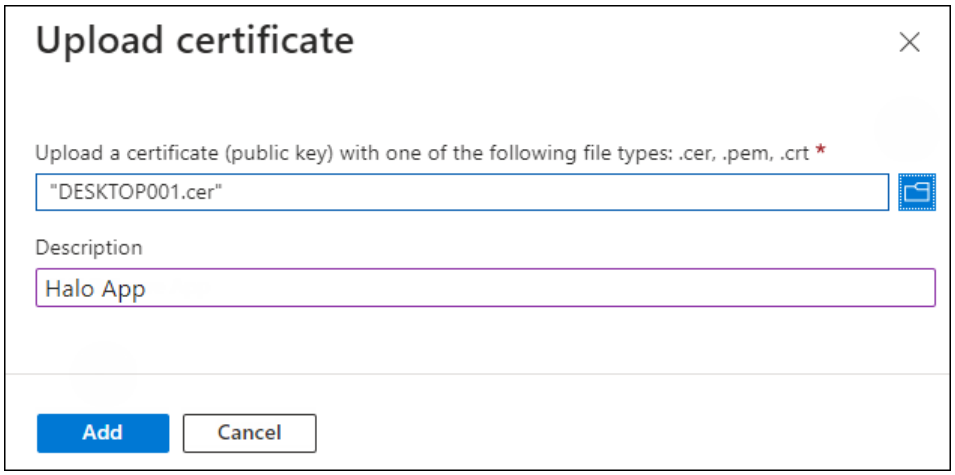
2. **Local Computer** certificate store: The certificate required for MPIP authentication must be installed in the Local Computer certificate store, along with the Root CA and Intermediate CA certificates.

   a. If the certificate is CA-signed, install all related certificates in their respective stores (Root, Intermediate, and Personal).

   b. If the certificate is self-signed, install it in both the Trusted Root Certification Authorities and Personal stores of the Local Computer.

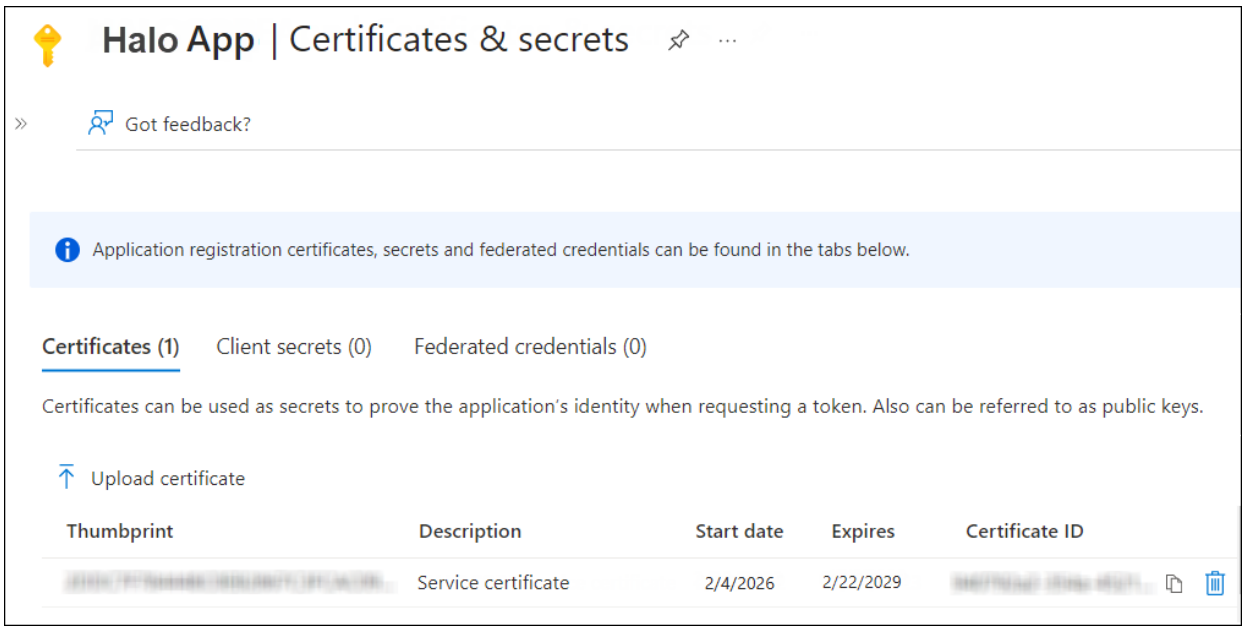
To upload the public key of the certificate, follow the steps below:

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 figure below:



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 figure below:



Upload certificate #2

5.2. Office 365 Subscription Details

1. Fully configured Microsoft Purview Information Protection.
2. An Azure subscription is required to use Azure RMS and the MPIP functionality.
3. A working Microsoft Entra ID service must be available.
4. Transport Layer Security (TLS) 1.2 or higher must be enabled to ensure the use of cryptographically secure protocols at all client workstations. Please refer to the section "Enable Support for TLS 1.2 at the Client Workstation for Microsoft Entra ID".
5. Audit logging: Your Azure subscription must include Log Analytics on the same tenant as Microsoft Entra ID.

5.2.1. Create and configure 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.

5.2.2. Recommended URLs, Addresses, and Ports for MPIP

MIP SDK doesn't support the use of authenticated proxies. Therefore, ensure that 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) For details on Microsoft Entra ID endpoints, please refer to "Microsoft Online Documentation".	`https://login.microsoftonline.com`

Recommended endpoints

5.2.3. Enable Support for TLS 1.2 at the Client Workstation for Microsoft Entra ID

To improve the security posture of the tenant and to remain in compliance with industry standards, Microsoft Entra ID stopped supporting the following Transport Layer Security (TLS) protocols and ciphers:

1. TLS 1.1

2. TLS 1.0
3. 3DES cipher suite (TLS_RSA_WITH_3DES_EDE_CBC_SHA)

In order for the HaloCAD for CAD add-on to be able to authenticate to Microsoft Entra ID, TLS 1.2 must be activated on the respective client workstation. Please see this Microsoft article to enable TLS 1.2.

Microsoft documentation

The information in the Microsoft documentation overrides any information published in this section.

Secude is not liable for changes to the content of this section because it was extracted from the Microsoft article at the time when the HaloCAD manual was prepared. Do check the most recent updates in this regard from the Microsoft documentation.

In summary, the following steps must be performed:

1. Update the Windows Operating System
2. Update .NET Framework
3. Set the following registry settings:

S.No	Windows Registry	Values
1	[HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\.NETFramework\v4.0.30319]	"SystemDefaultTlsVersions"=dword:00000001 "SchUseStrongCrypto"=dword:00000001
2	[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319]	"SystemDefaultTlsVersions"=dword:00000001 "SchUseStrongCrypto"=dword:00000001

Registry entries

5.3. Conditions for Running the HaloENGINE Tomcat Service

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

Deny log on as a service policy

If the service is running under a specific user or a specific group, ensure that the user is not restricted by 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 appears while running the HaloENGINE Tomcat service.

Allow non-admin users to access a private key (without full admin rights)

During installation, the HaloENGINE gets the required Microsoft Entra ID application details and certificate thumbprint. When the HaloENGINE Tomcat service starts, it tries to connect to the MPIP services using the details entered during installation. As part of this process, it validates the certificate thumbprint against the certificate installed in the **Local Computer** certificate store. The thumbprint entered in the installation wizard must match the one available in the Local Computer certificate store.

If the service runs under a non-administrative user account, the user may not have sufficient permissions to access the certificate's private keys when the certificate is installed in the Local Computer store. This restriction prevents successful authentication with MPIP services. To resolve this issue, grant the user **Read** permission to access the certificate's private key by following the steps listed below.

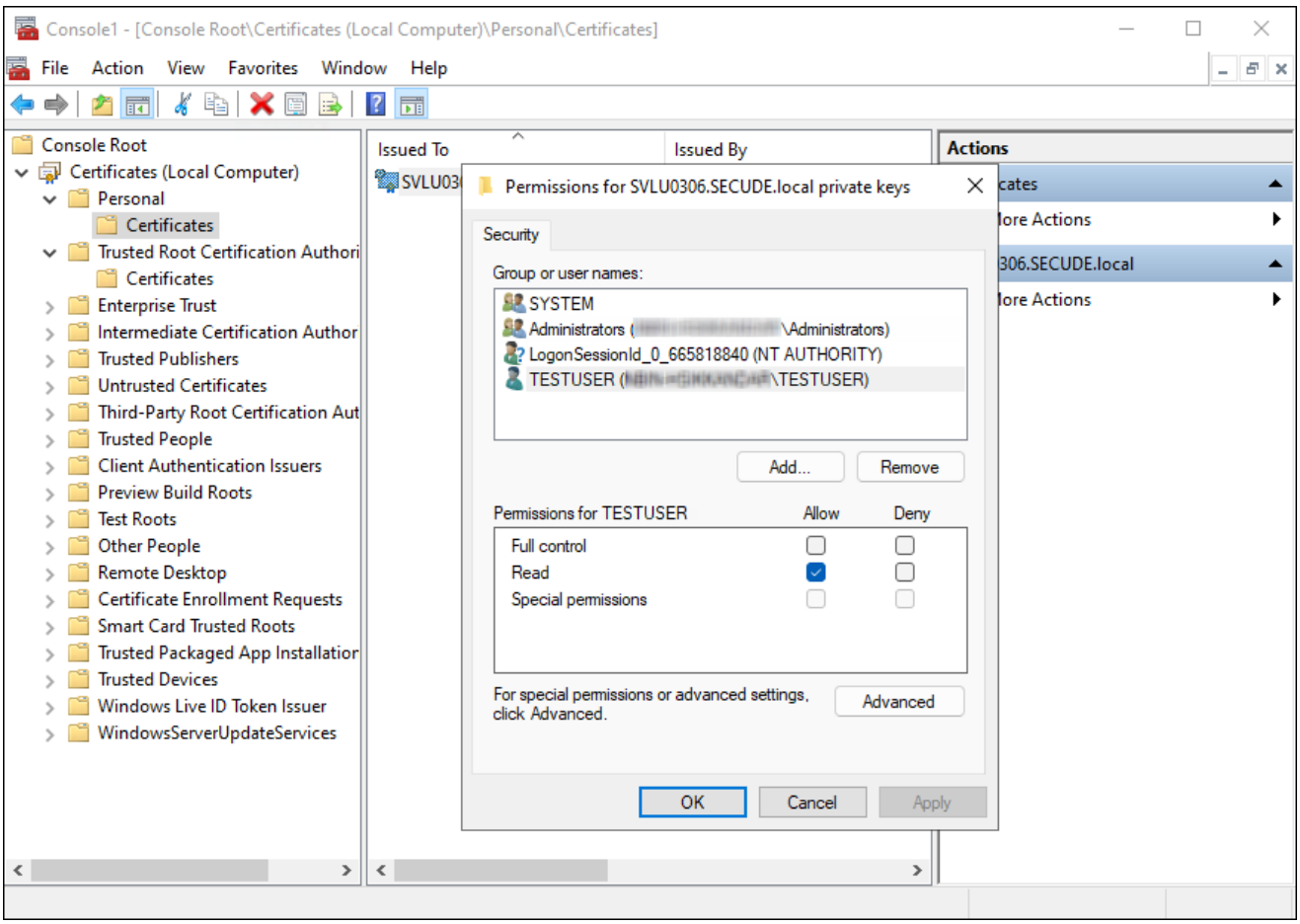
Any errors encountered during this process are recorded in the log file. If the verification succeeds, the service proceeds with initialization.

Prerequisites

1. The required certificates (machine certificate, root CA, and intermediate CA) are already installed.
2. The private key is stored in the **Windows Certificate Store** under **Local Computer**.
3. You have administrative rights to perform the setup.

Follow the procedure below to grant read access:

1. Open **Certificate Manager** as Administrator.
2. Press **Win + R**, type mmc, and press **Enter**.
3. In the console, go to **File** and select **Add/Remove Snap-in**.
4. Select **Certificates** from the list and click **Add**.
5. Choose the **Computer account**, then click **Next**, followed by **Finish**, and then **OK**.
6. In the left panel, expand **Certificates (Local Computer)**, expand **Personal**, and select **Certificates**.
7. Identify the certificate that contains the private key.
8. Right-click the certificate, select **All Tasks**, and then select **Manage Private Keys**.
9. In the **Permissions** window, click **Add** and enter the non-admin username (for example, TESTIL) and click **OK**.
10. Select the **Read** permission, click **Apply**, and then click **OK**.



Granting private key access to a non-admin user

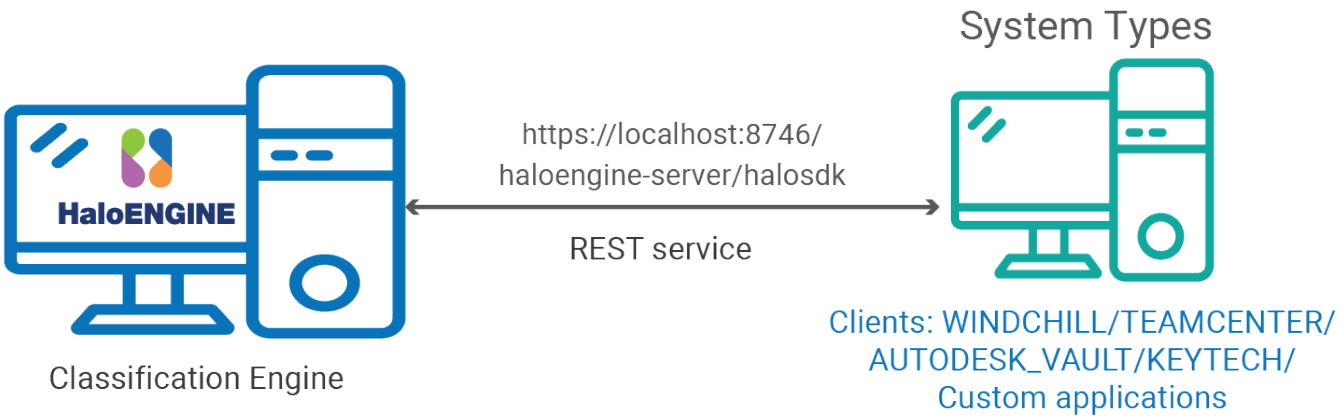
5.4. Obtain the HaloENGINE License

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 specified in the license are accessible via their respective endpoints.

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.

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



System types and protocol

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

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

Obtaining license

5.5. 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.

5.5.1. 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

5.5.2. 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.

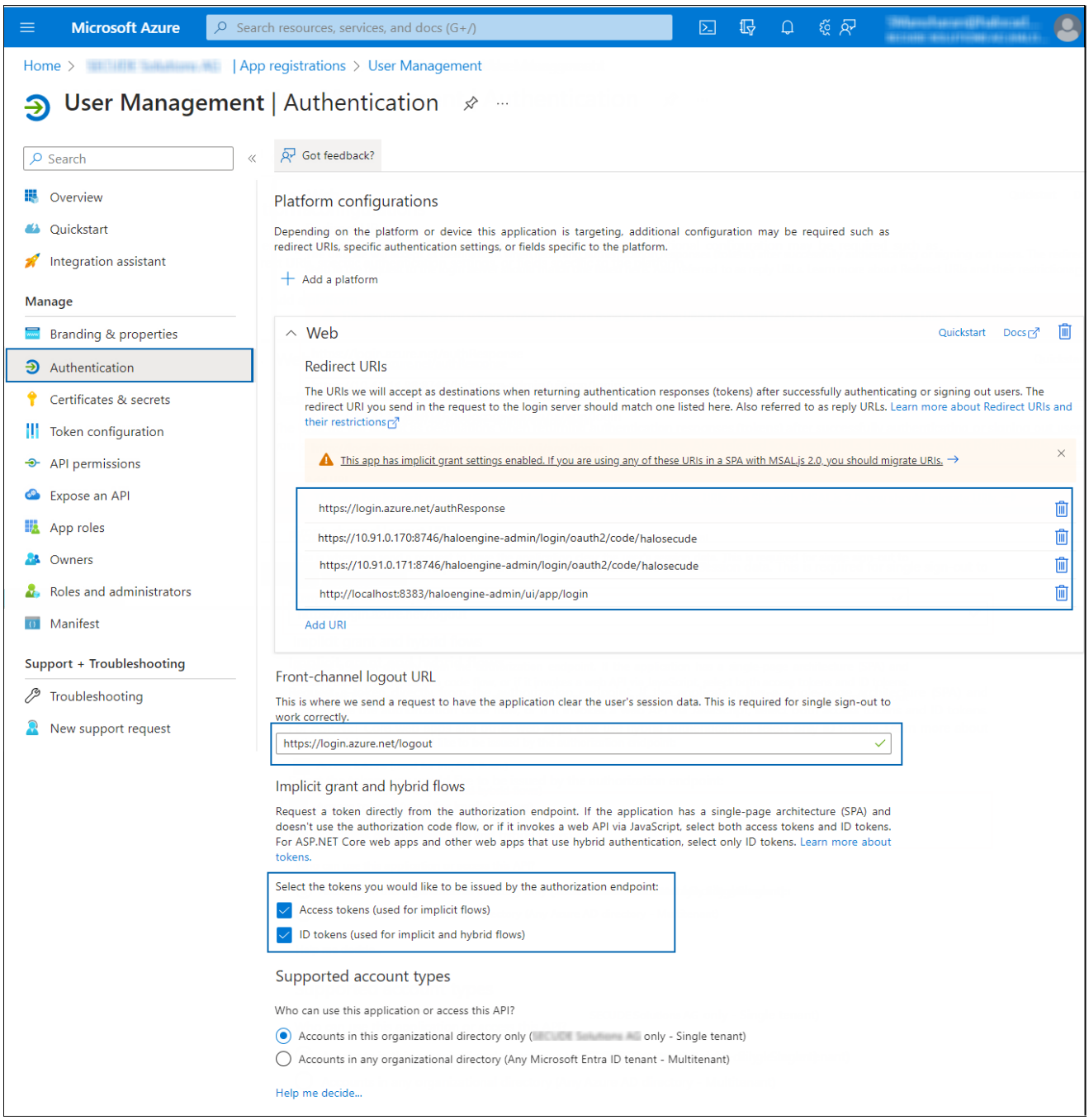
In the Azure portal, follow the steps below to configure user authentication and authorization settings.

5.5.2.1. 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).

5.5.2.2. 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:

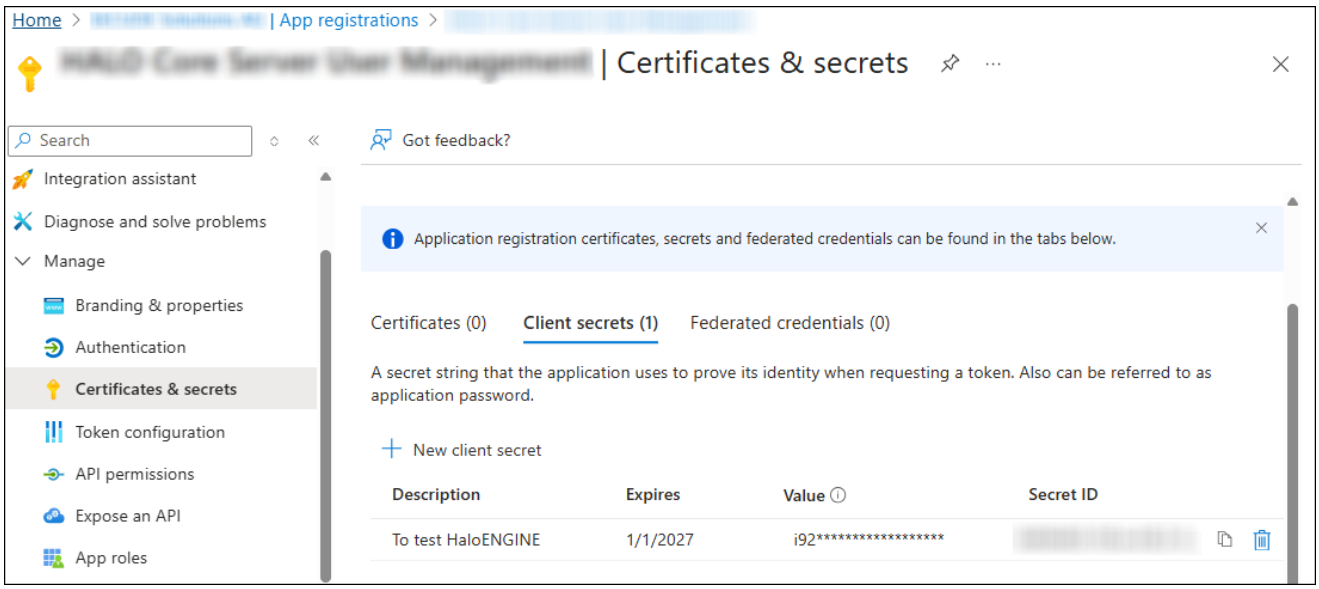
      - `https://<ip>:<port>/haloengine-admin/login/oauth2/code/<tenant name>` (for example, `https://10.91.0.65:8746/haloengine-admin/login/oauth2/code/halosecude`)

- Or `http://<localhost>:<port>/haloengine-admin/login/oauth2/code/<tenant name>` (for example, `http://localhost:8383/haloengine-admin/login/oauth2/code/halosecude`)

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**.

5.5.2.3. Step 3: Certificates & Secrets

1. In the left navigation pane, click **Certificates & secrets**.
2. Under **Client secrets**, click **+ New client secret**.
3. On the **Add a client secret** page, enter a **Description**, choose the **validity period** under **Expires**, and click **Add**.
4. After clicking **Add**, a new row appears under **Client secrets**.

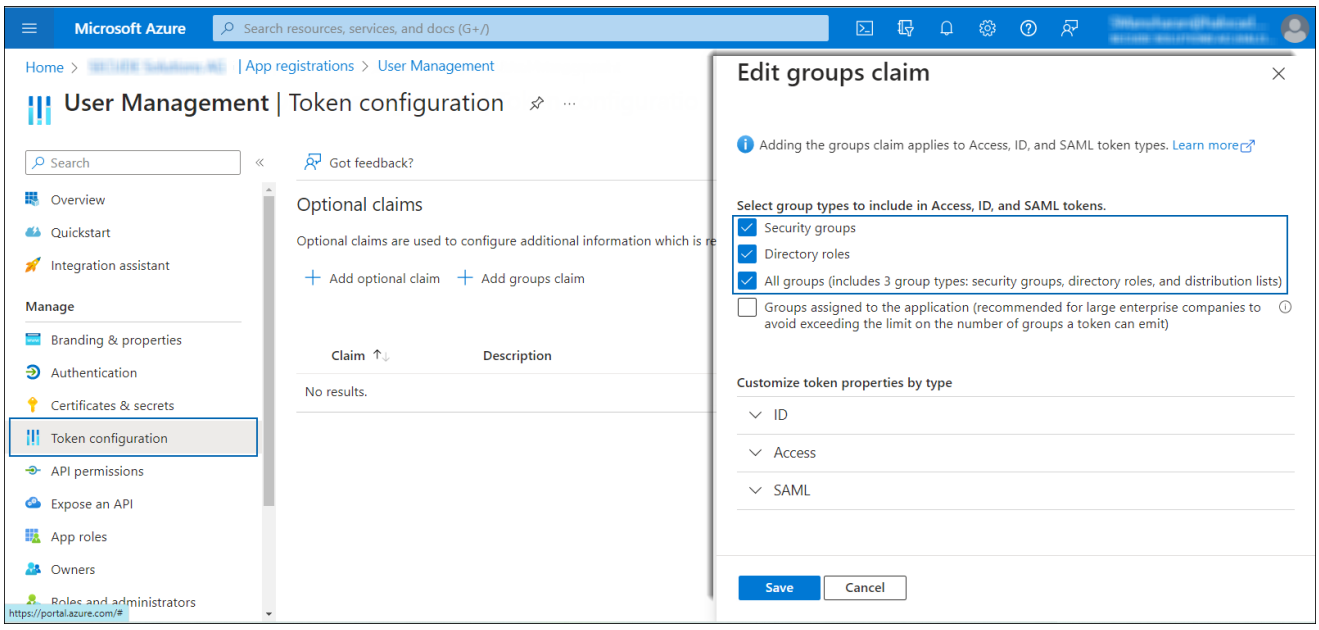


Client secret value

5. Copy the **Value** field immediately, as it will only be displayed once.
6. Store this value securely and use it for Tenant Configuration.

5.5.2.4. Step 4: 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

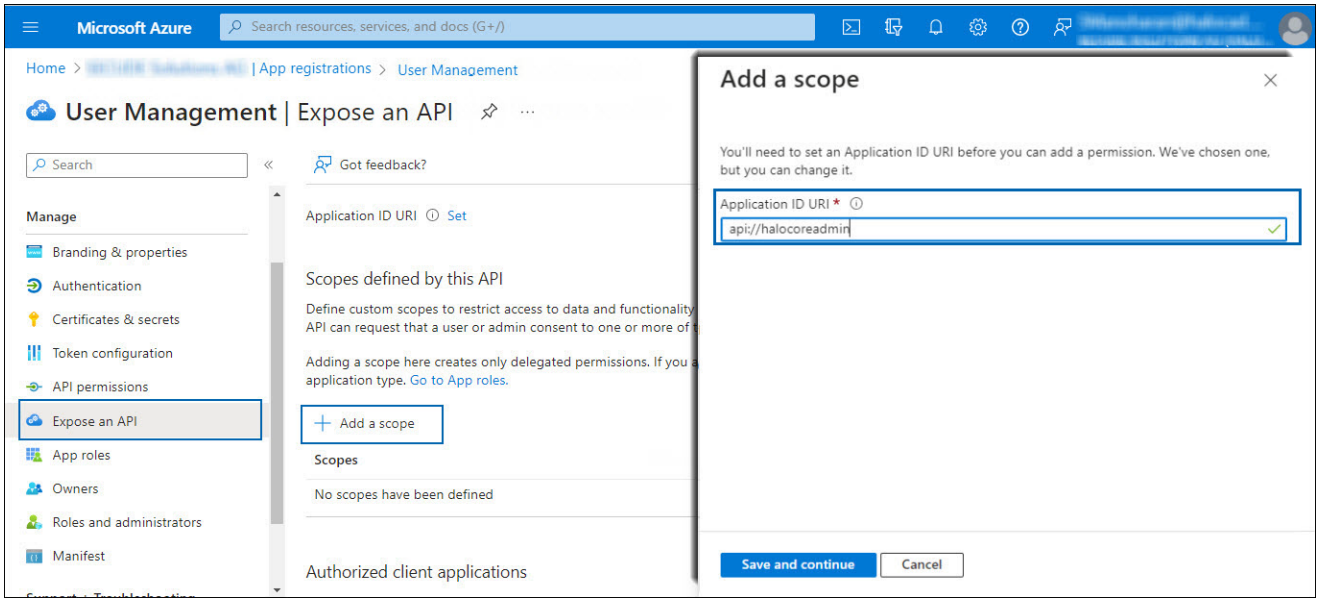
   b. Directory roles

   c. All groups

3. Click **Save**.

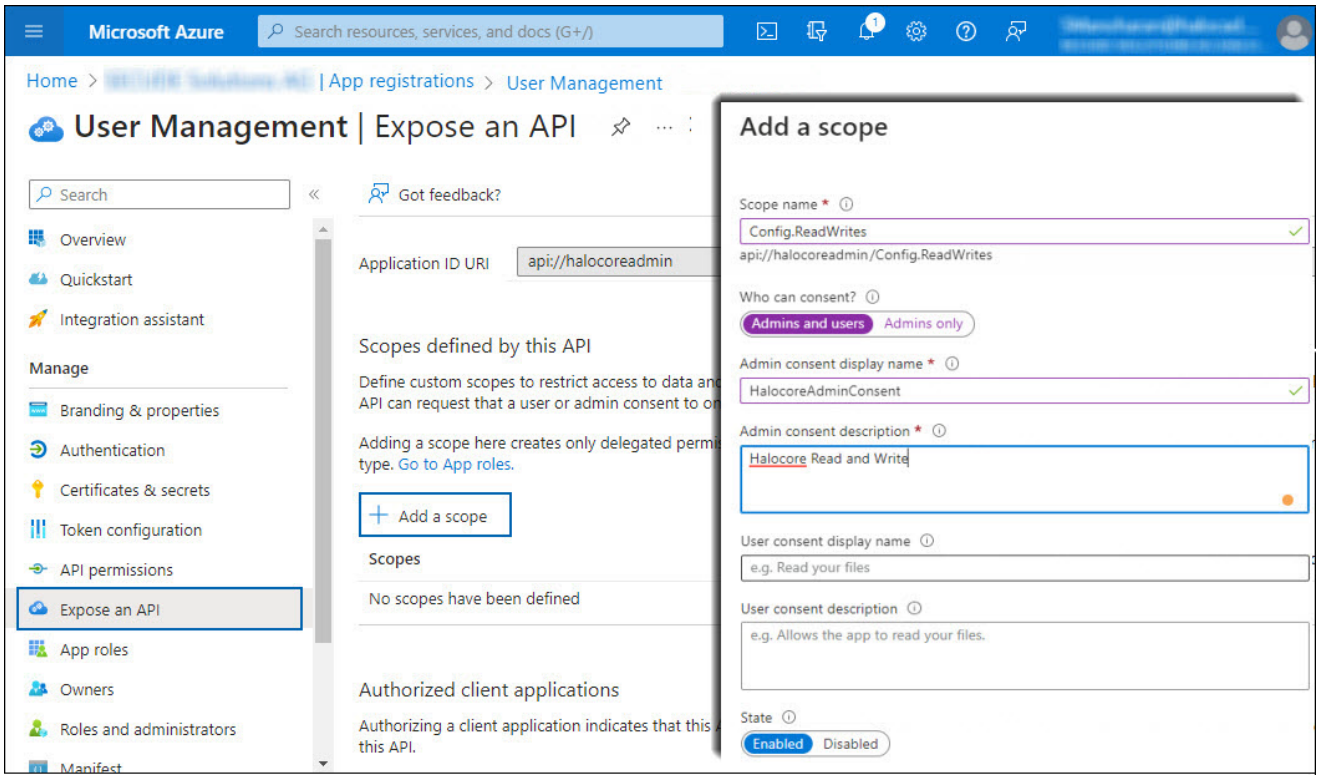
5.5.2.5. Step 5: Expose API

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).

5.5.2.6. Step 6: 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

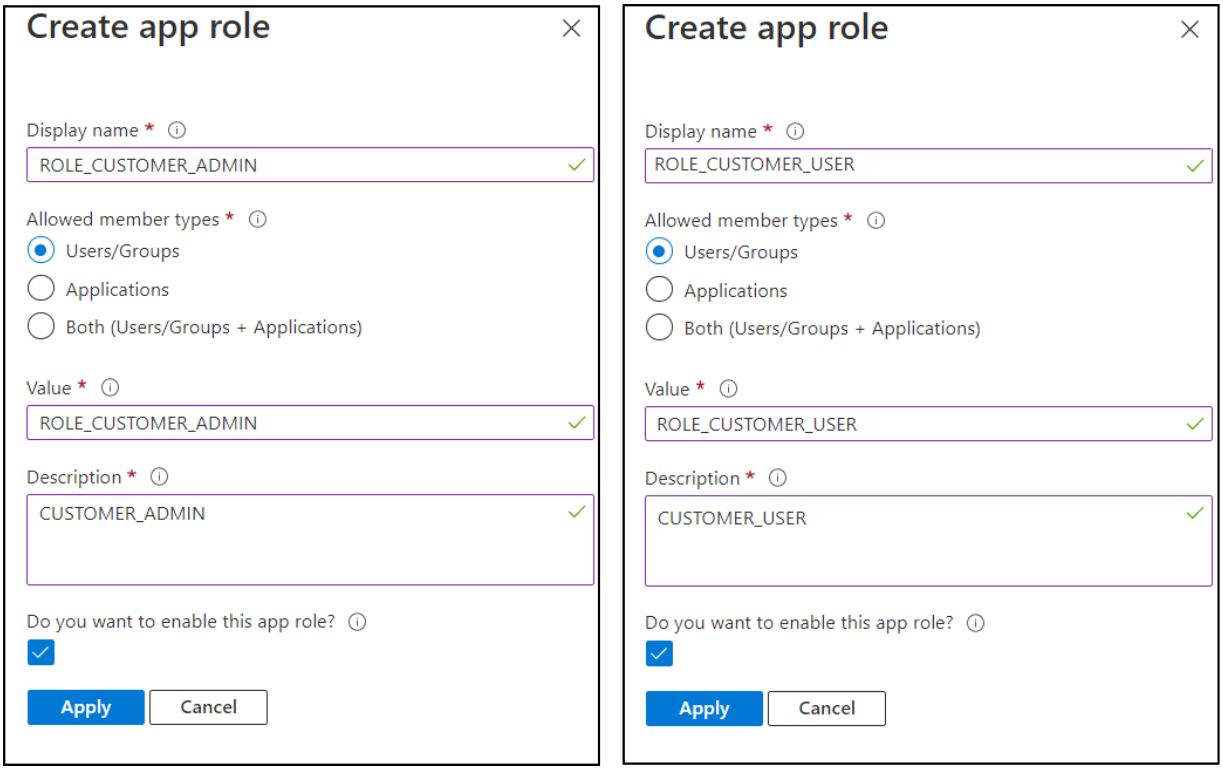
b. **Allowed member types**: select **Users/Groups**

c. **Value**: ROLE_CUSTOMER_ADMIN

d. **Description**: CUSTOMER_ADMIN

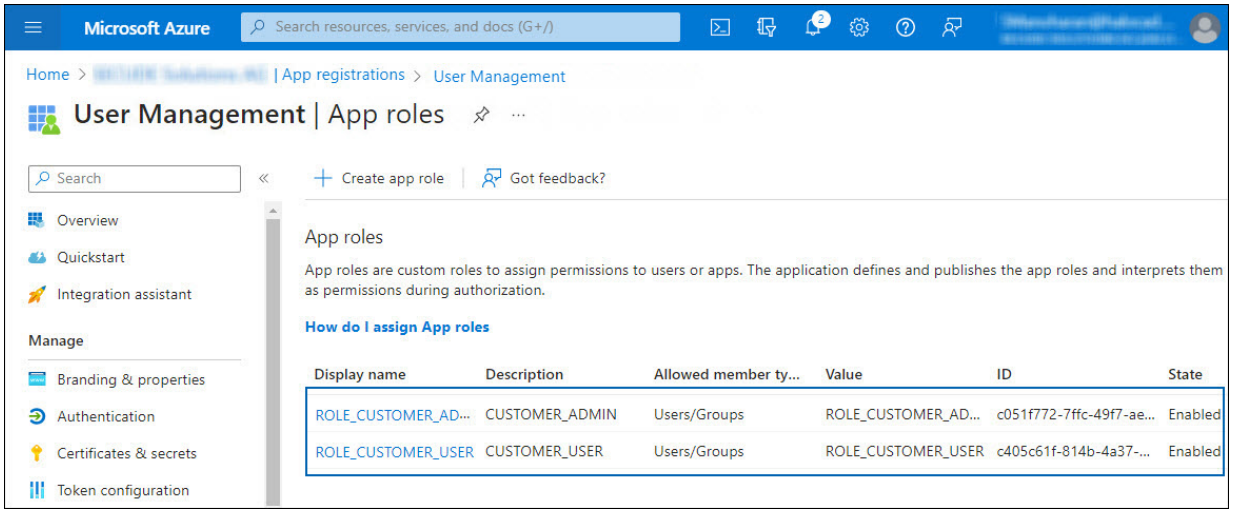
e. **Do you want to enable this app role?** – Select this option.

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



Adding Roles

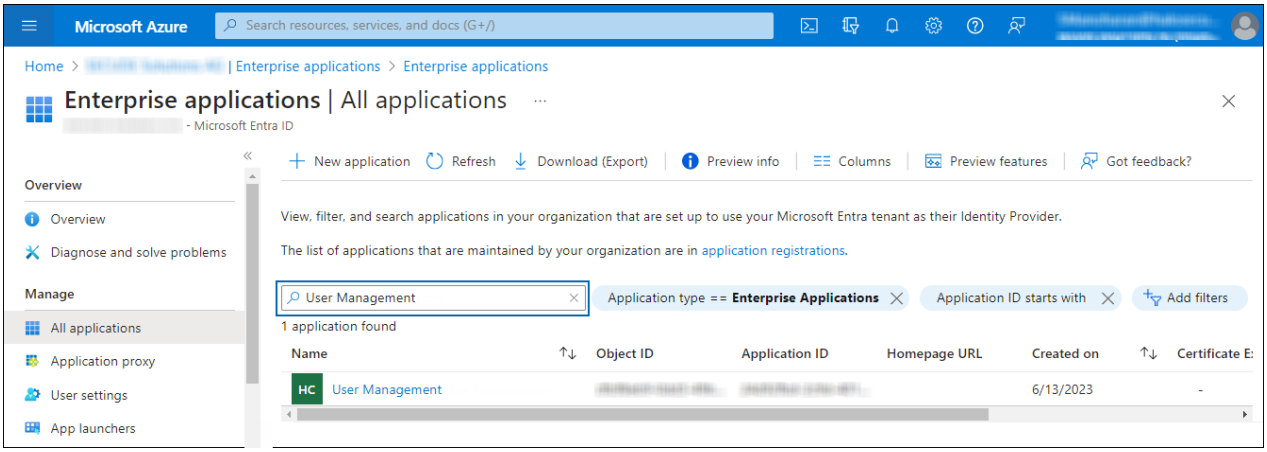
3. Click **Apply**.
4. The roles are added to the list.



Create Roles

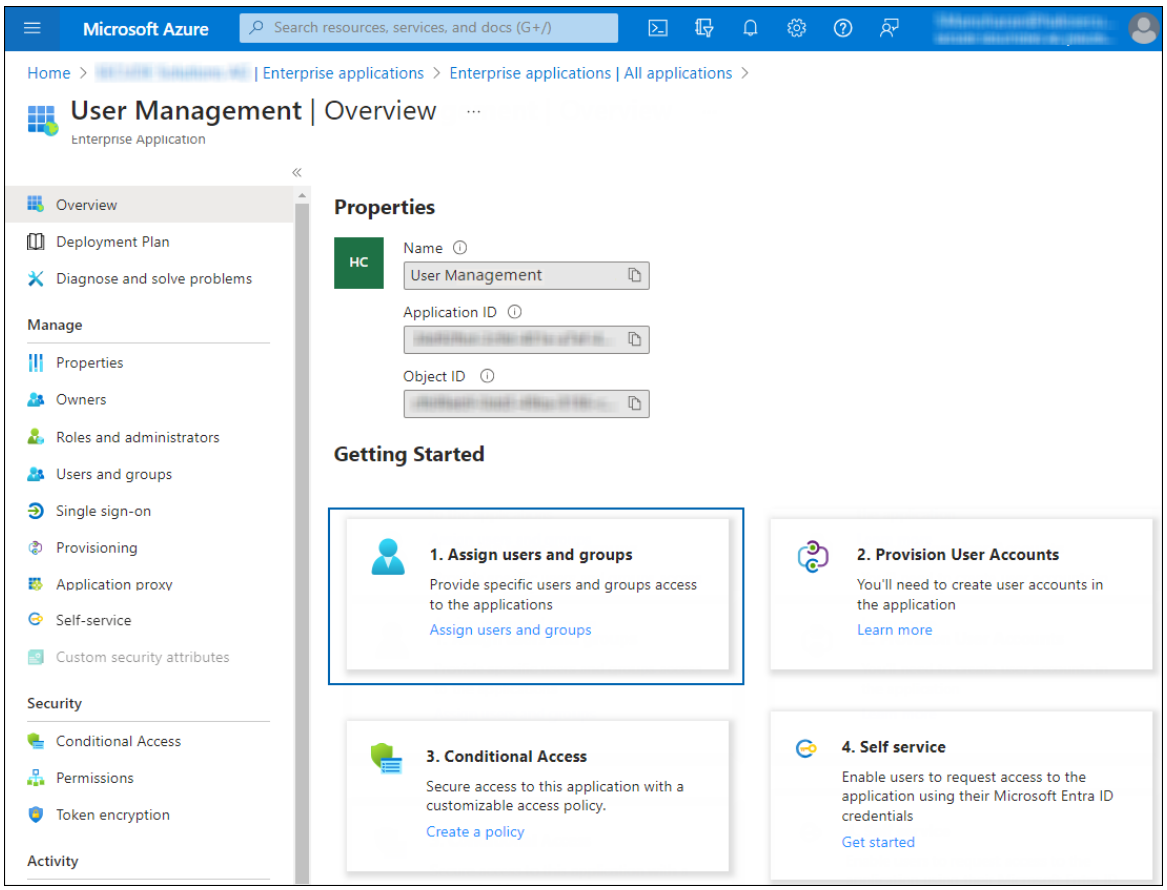
5.5.2.7. Step 7: Apply Role to Users

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:



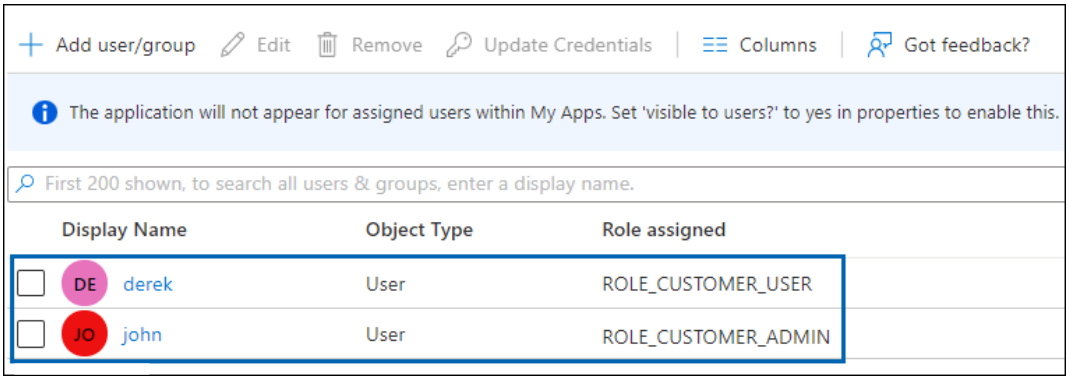
Apply role to user #2

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**.

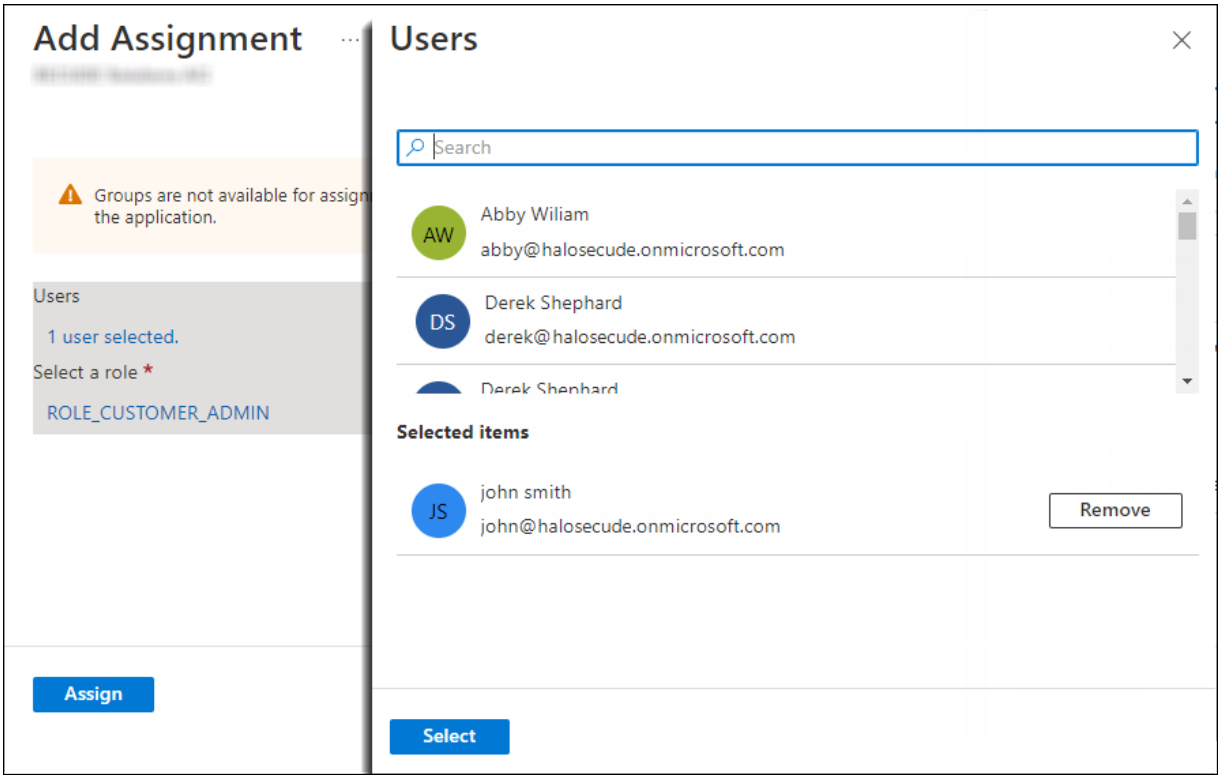


Adding users

h. Under **Select a role**:

- Click **None Selected** and search for 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 7. Tenant Configuration".

5.6. Forward Logs to Microsoft Sentinel

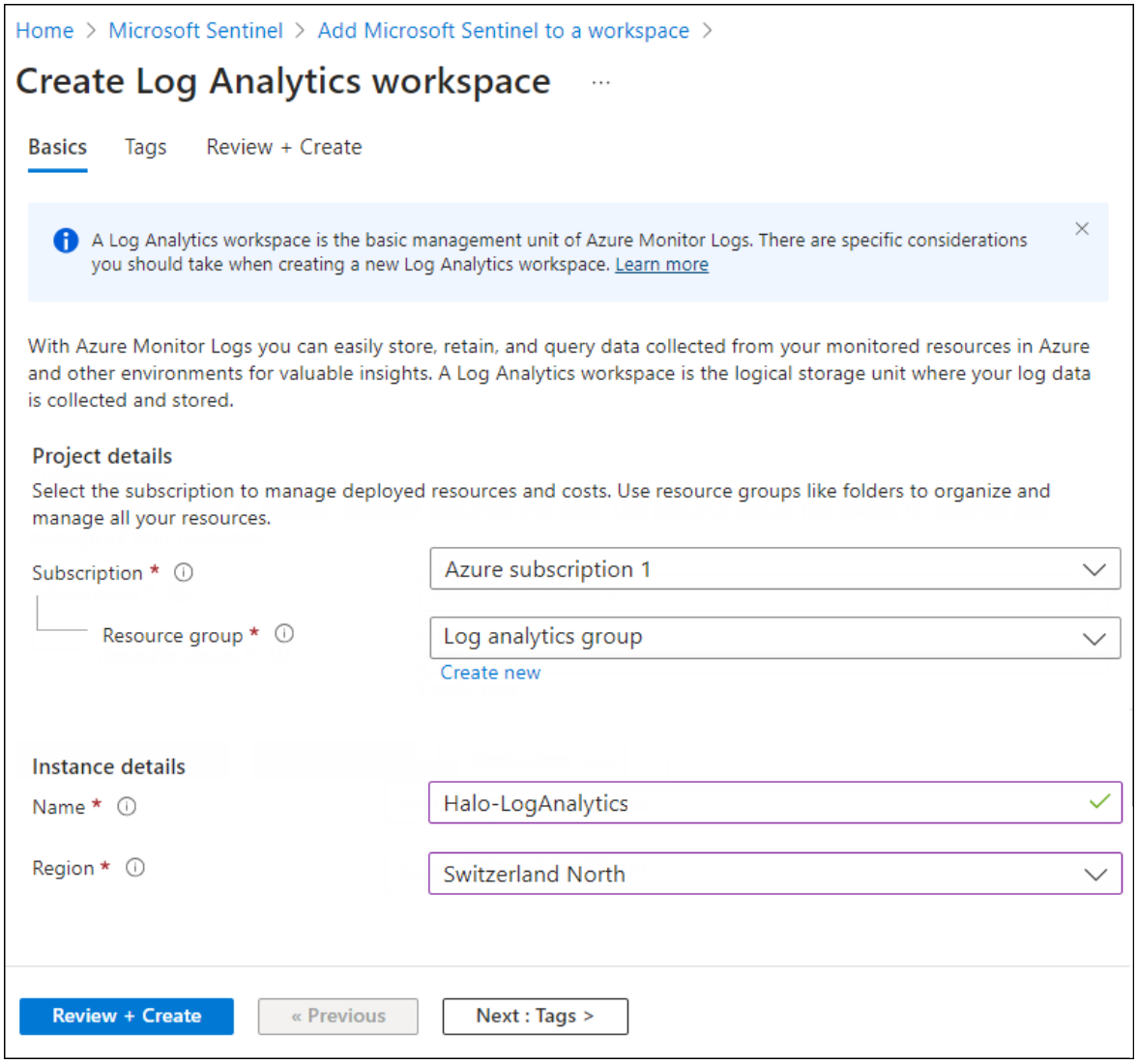
Microsoft Sentinel is a scalable, cloud-native security information and event management (SIEM) that delivers an intelligent and comprehensive solution for SIEM. Microsoft Sentinel provides cyberthreat detection, investigation, response, and proactive hunting, with a bird's-eye view across your enterprise.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

5.6.1. Configure 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.

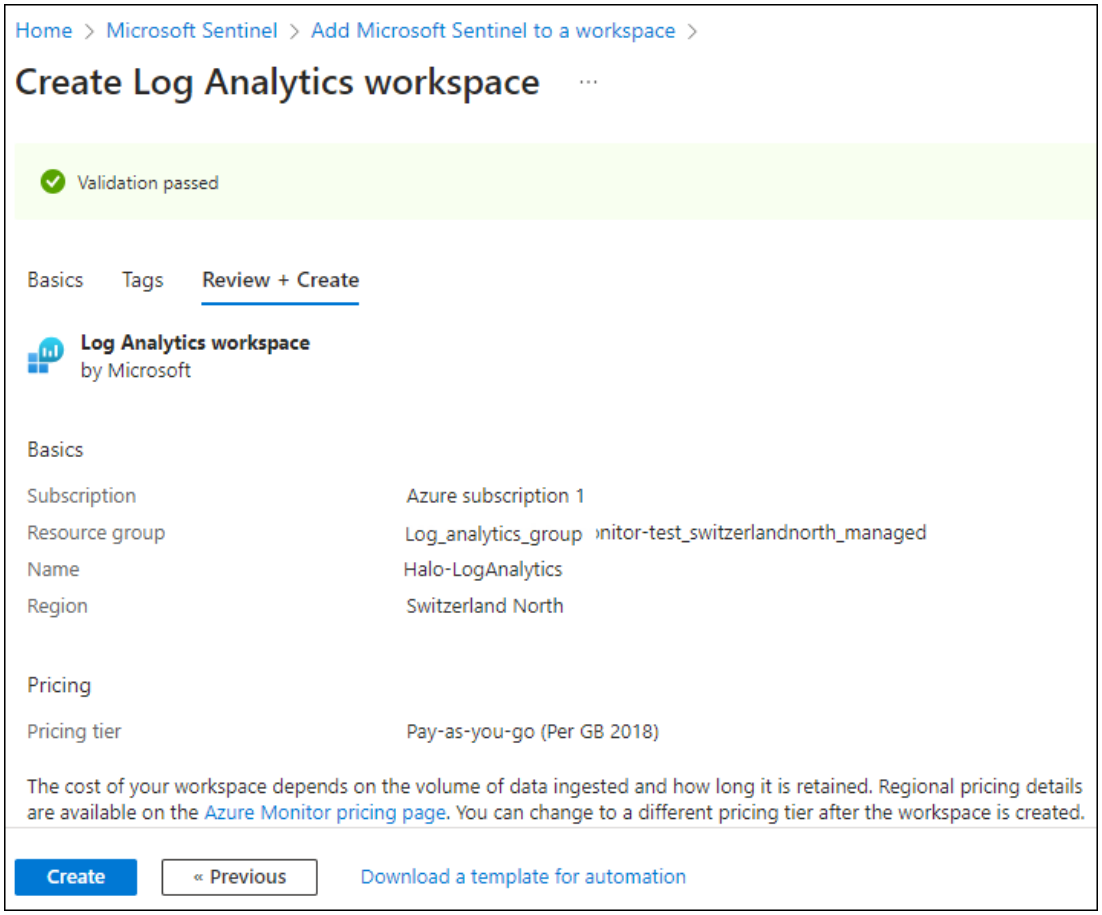
1. Log in to the Microsoft Azure portal.
2. In the search bar, type **Microsoft Sentinel**. As you start typing, the list filters according to your input.
3. Select **Microsoft Sentinel** from the search results.
4. The **Microsoft Sentinel** page will appear. Here, you need to click **Create** at the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

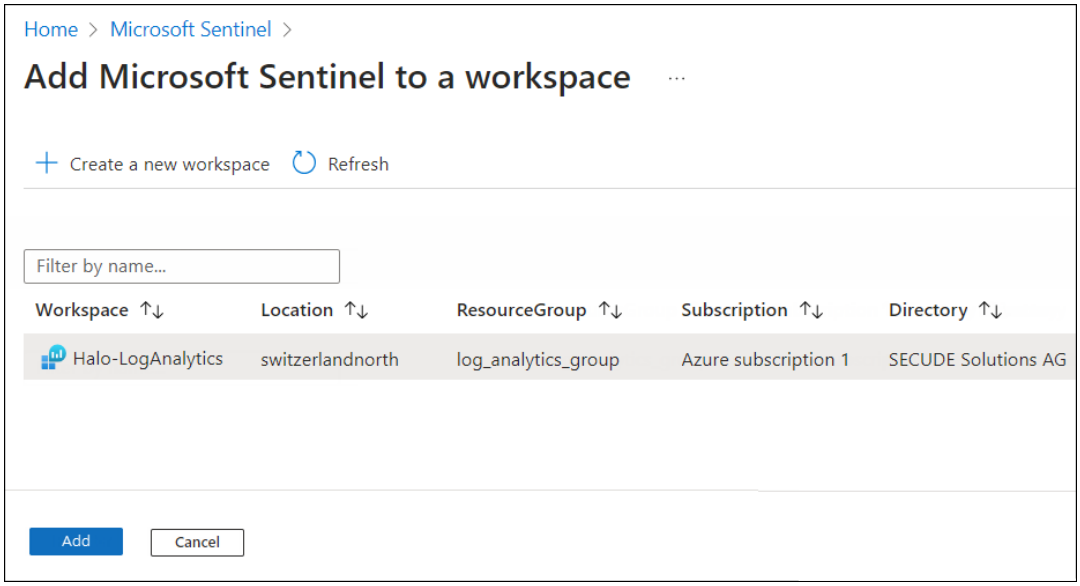
7. Select a resource group from the list.
   a. Provide a name for your workspace.
   b. Choose a region from the list.

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:



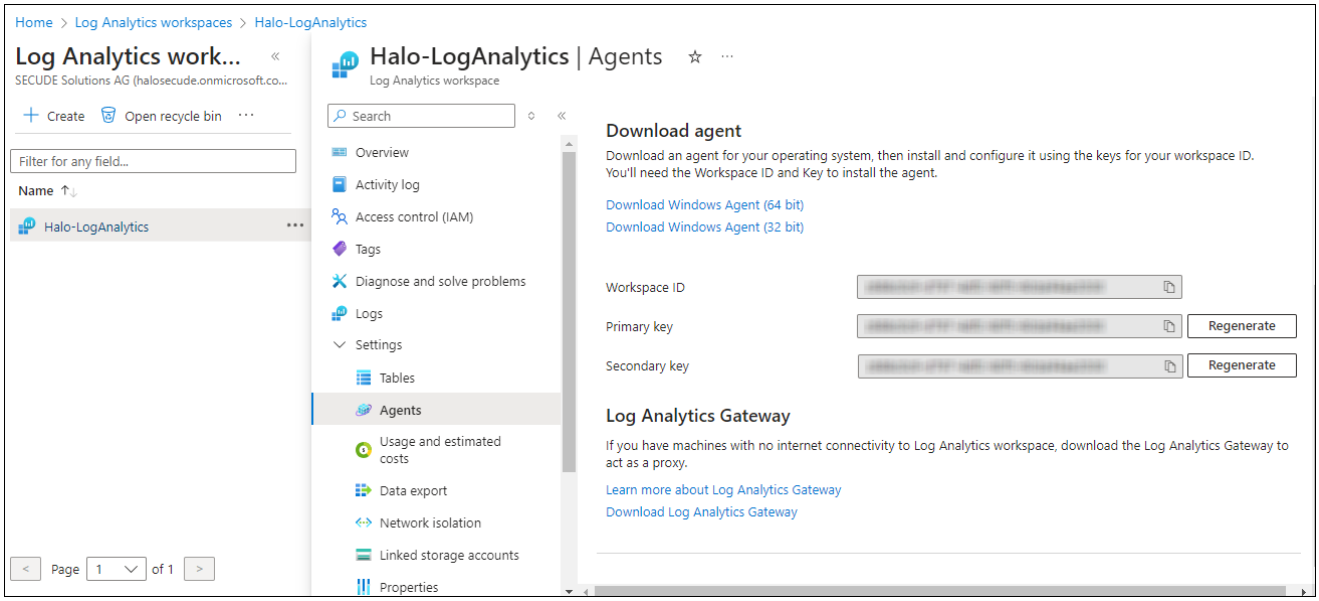
Workspace #3

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.

5.6.2. Fetch 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.

6. Installing the HaloENGINE

This chapter walks you through the steps of installing HaloENGINE using graphical and silent methods. By default, HaloENGINE 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 terminologies, MIP and MPIP, are used interchangeably throughout this document.

6.1. 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 wish to integrate with the dashboard, you will need to uninstall and reinstall HaloENGINE using Option 1.

6.2. 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 combine, use the GUI installer.

Prerequisites

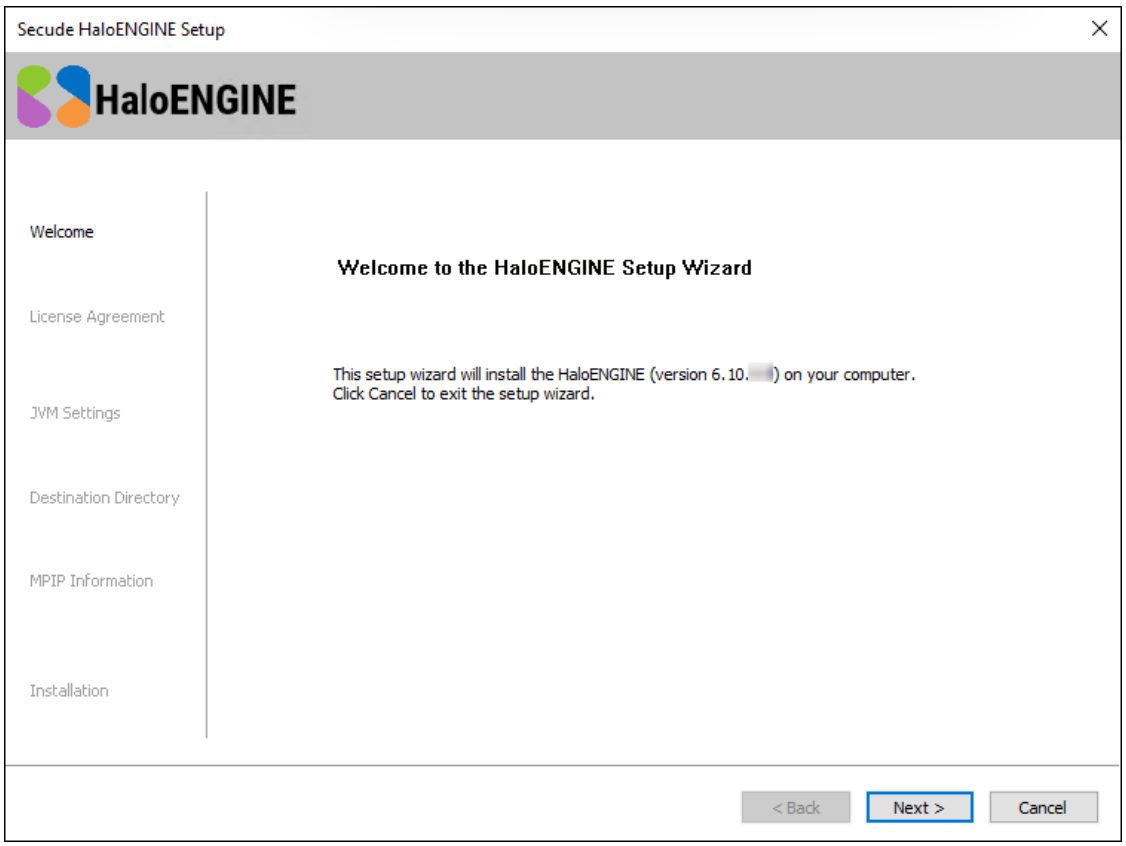
Before installing HaloENGINE, ensure that the following requirements are met:

1. Ensure that the previously installed HaloENGINE Service is completely uninstalled.
2. Azure application registration details: Refer to the section “Registering an Application in Microsoft Entra ID”.
3. The certificate required for MPIP authentication must be installed in the Local Computer certificate store, along with the Root CA and Intermediate CA certificates.
   - If the certificate is CA-signed, install all related certificates in their respective stores (Root, Intermediate, and Personal).
   - If the certificate is self-signed, install it in both the Trusted Root Certification Authorities and Personal stores of the Local Computer.
4. Administrator rights: The user performing the HaloENGINE installation must have administrator privileges.

Installation Procedure

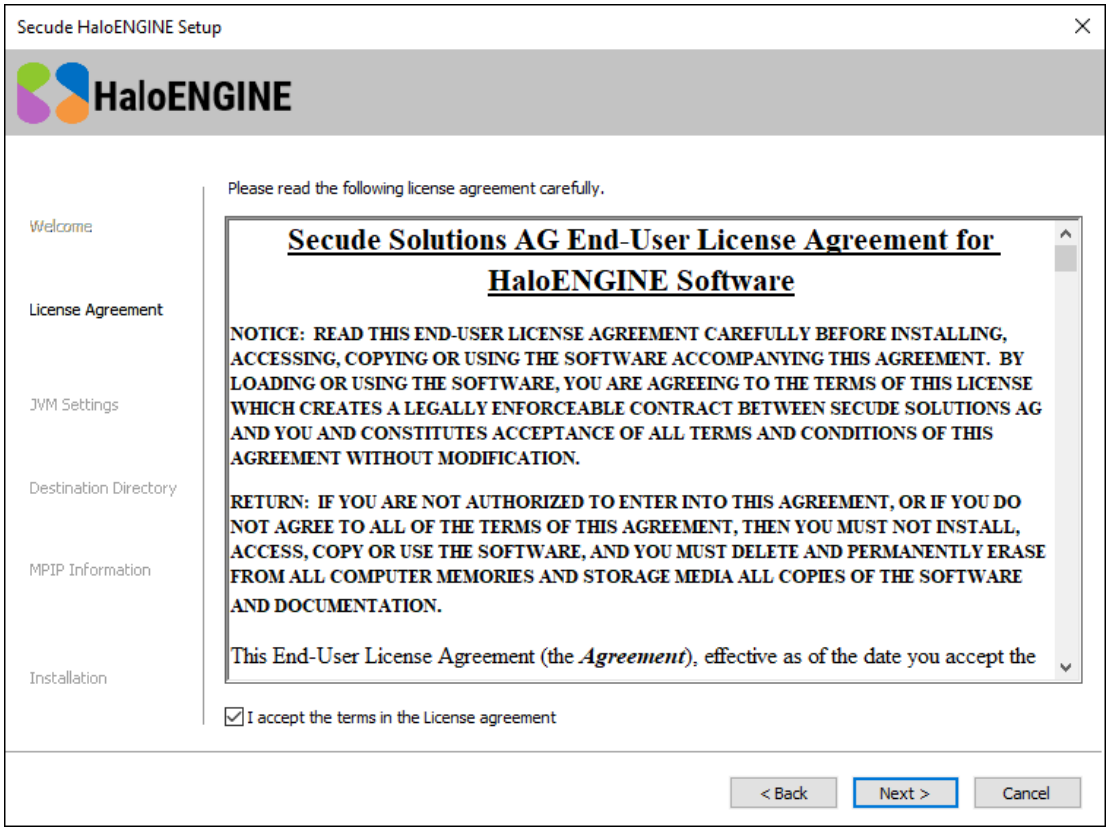
1. To begin the interactive installation, double-click the installer `HaloENGINE_Setup.exe` file. Depending on your Windows security settings, you may get a warning such as "*Do you want to allow the following program to make changes to this computer?*". If you get this security warning, click the **Yes**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

Startup Dialog



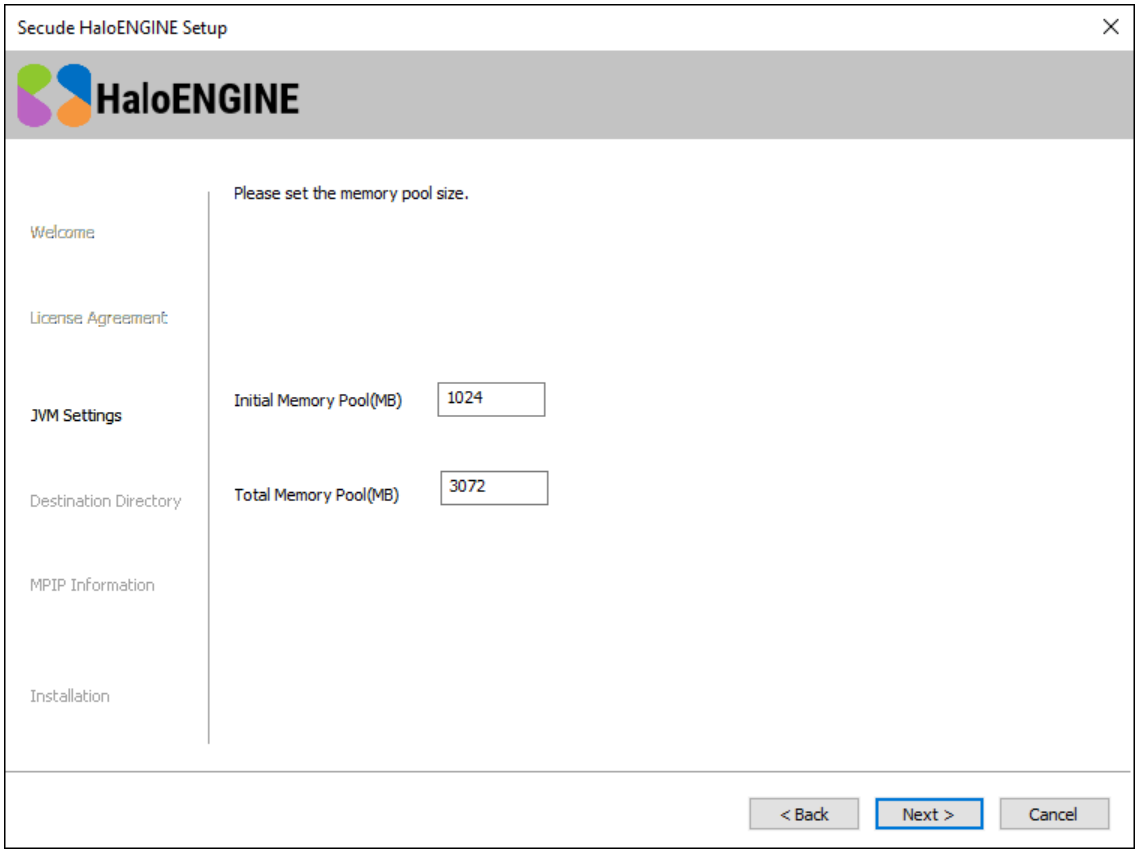
Welcome dialog

3. Click **Next** to continue the installation. The **End-User License Agreement (EULA)** dialog appears.



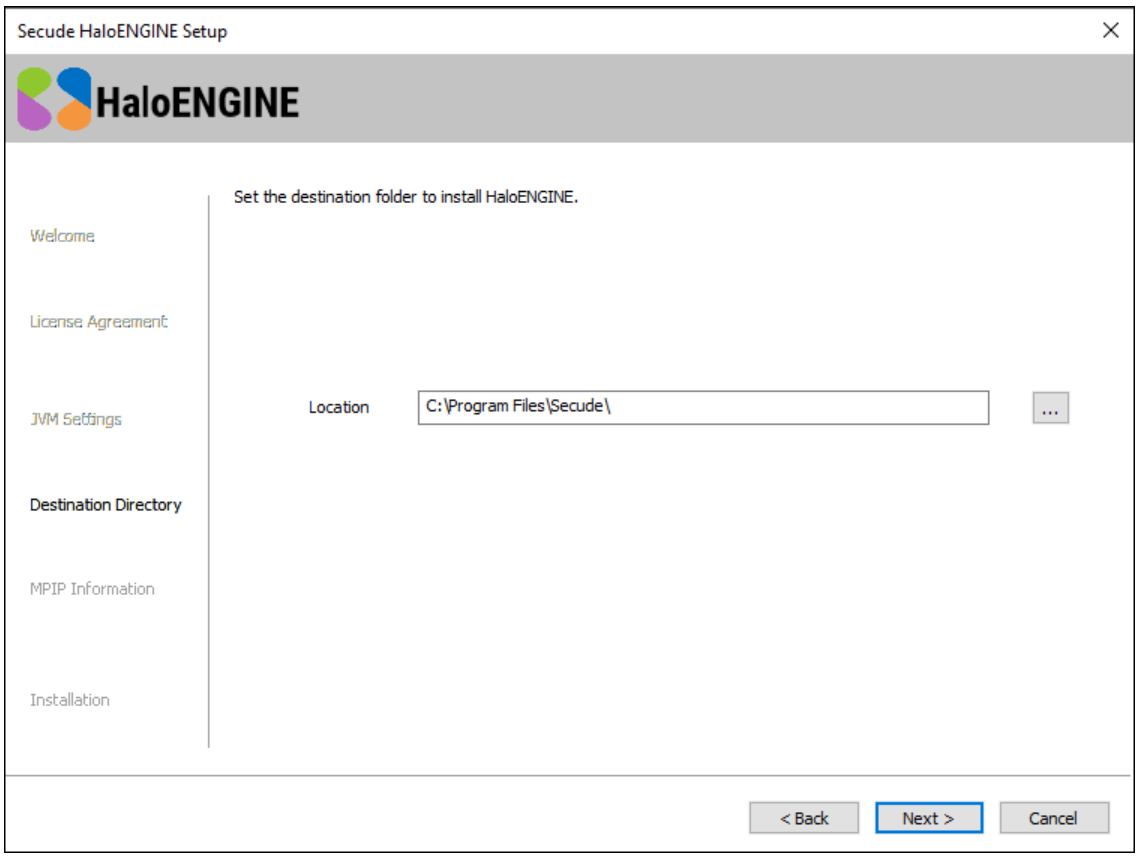
End-User License Agreement dialog

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



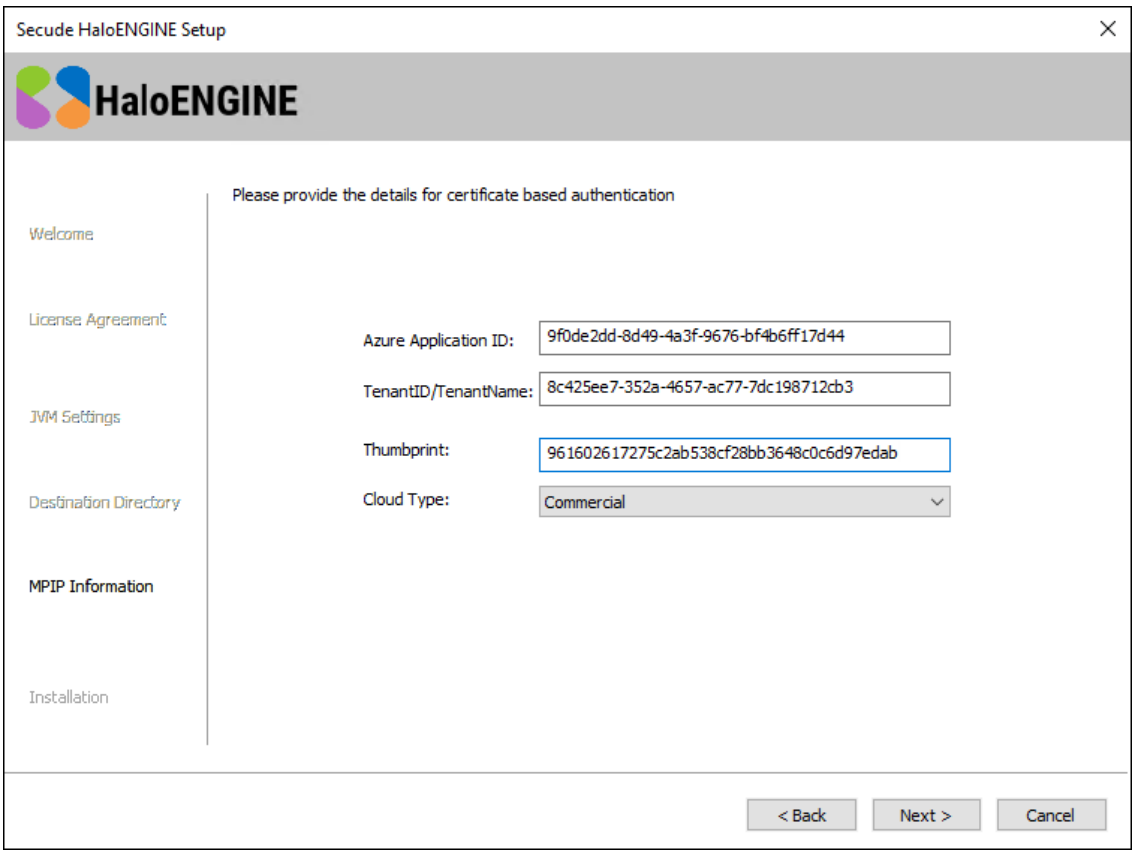
Tomcat pool size configuration dialog

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 appears:



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 certificate-based authentication dialog appears. To avoid errors, please ensure that you enter the correct Azure application registration details in the installation wizard.



Certificate-based authentication dialog

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

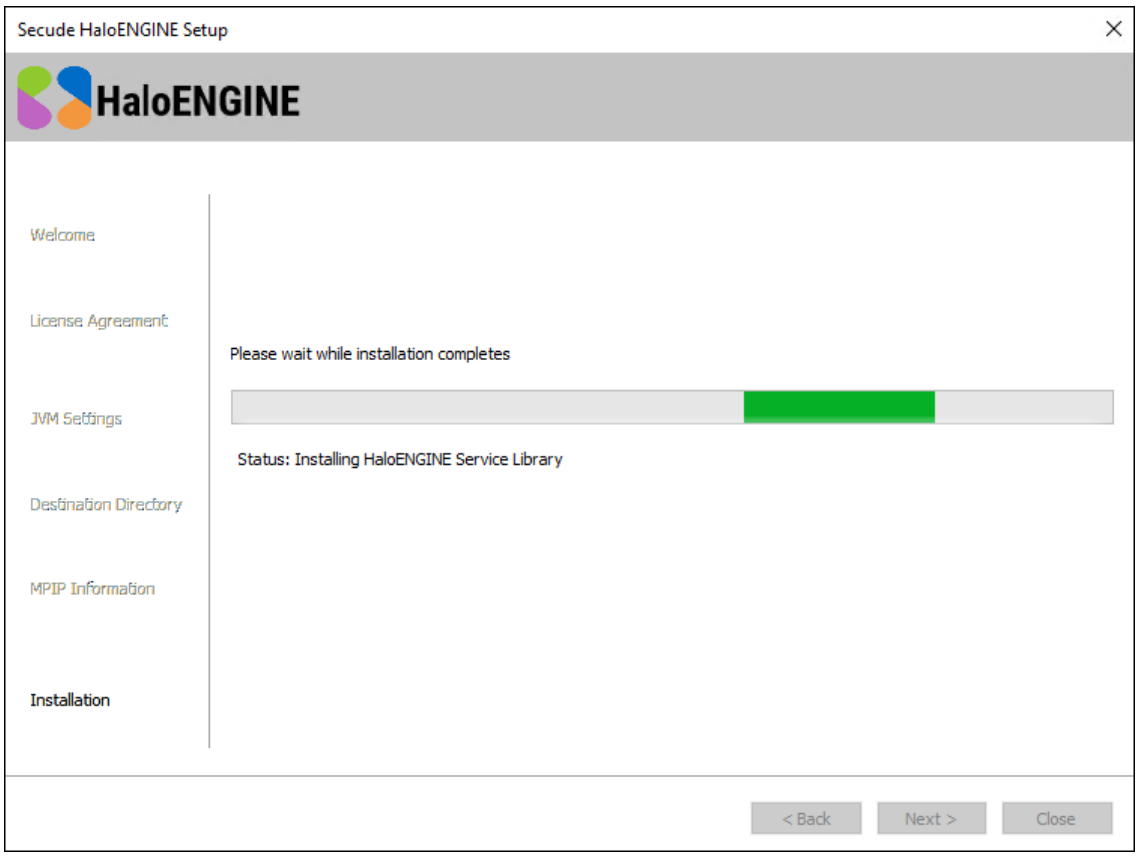
b. **Tenant ID/Tenant Name**: Enter your Microsoft Entra tenant name (for example, `contoso.onmicrosoft.com`) or its tenant ID (for example, `8c425ee7-352a-4657-ac77-7dc198712cb3`).

c. **Thumbprint**: Enter the thumbprint of the MPIP authentication certificate installed in the **Local Computer** certificate store.

d. **Cloud Type**: **Commercial** is selected by default. Based on your Azure subscription and configuration, select the required cloud type from the list: Commercial, Custom, Germany, US_DoD, US_GCC, US_GCC_High, US_Sec, US_Nat, or China_01. If you select **Custom**, enter the appropriate URLs in the **Protection Cloud URL** (for example, `https://api.aadrm.com`) and **Policy Cloud URL** (for example, `https://dataservice.protection.outlook.com`) fields.

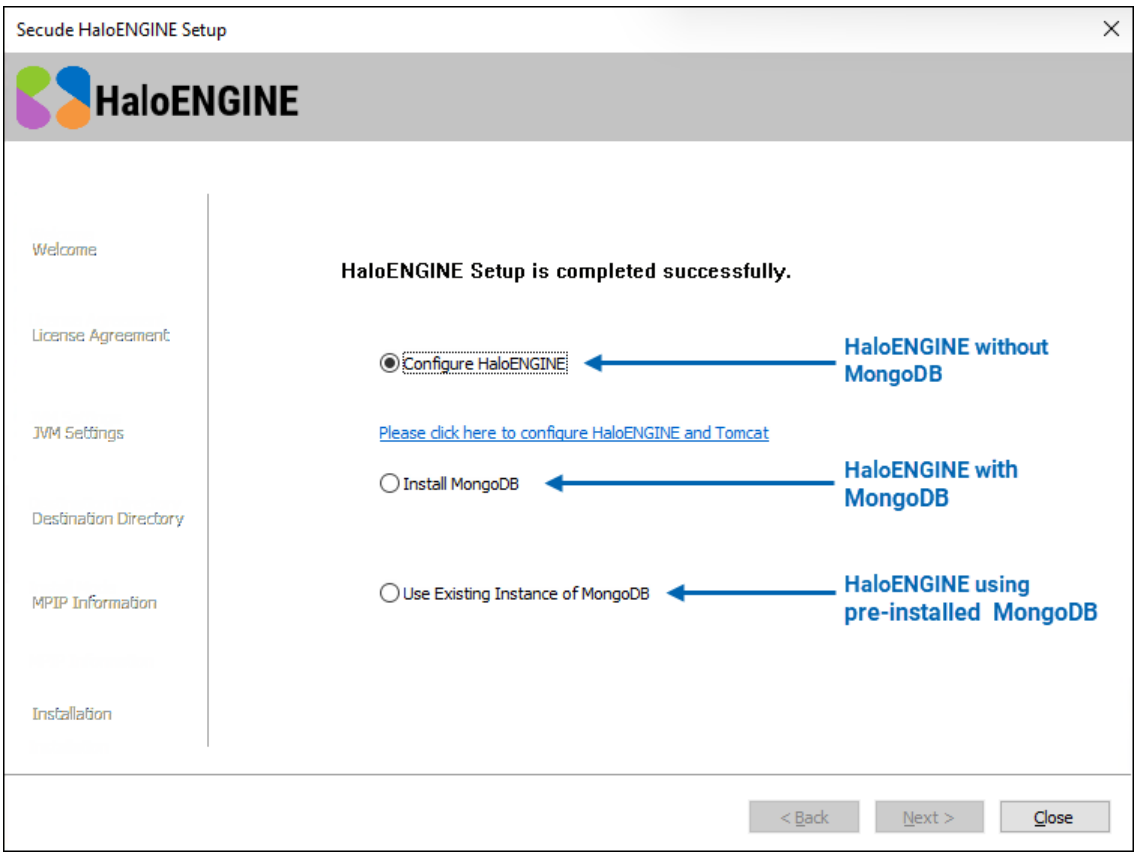
e. Click **Next**.

9. The installation begins, and the progress is displayed in the dialog.



Installation progress dialog

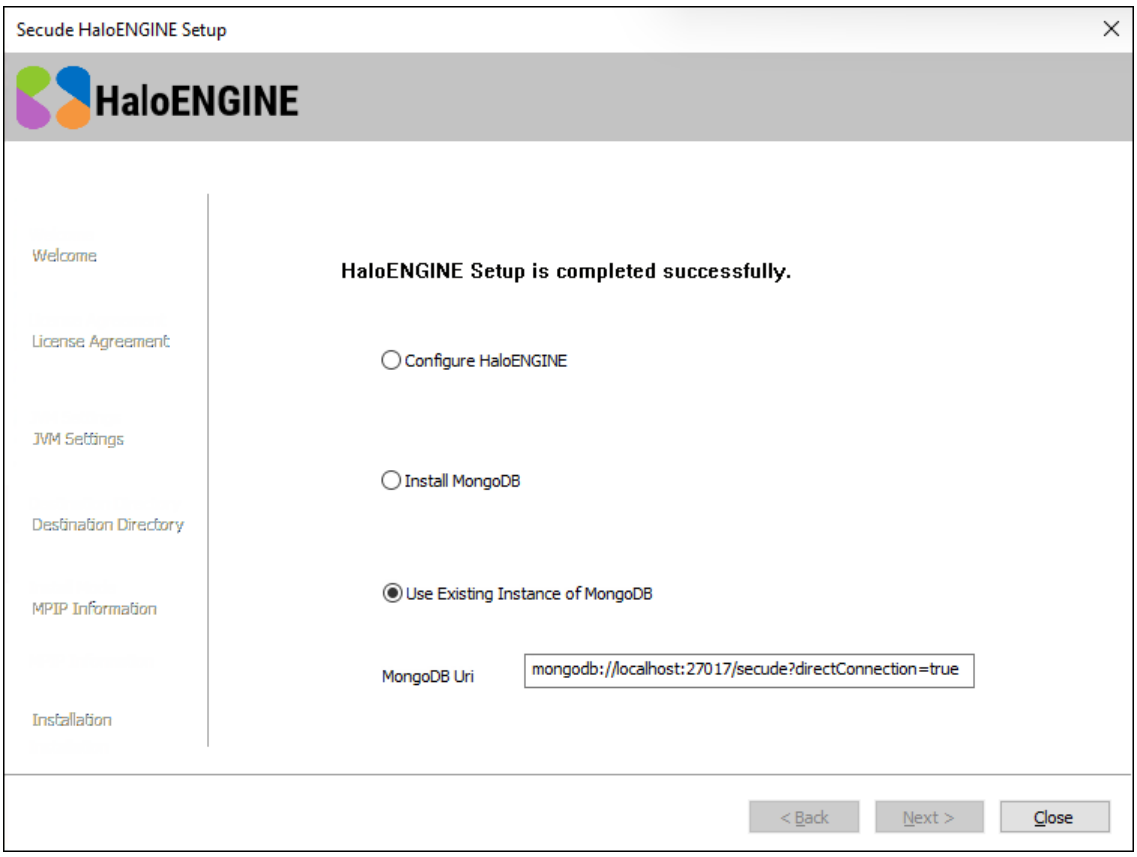
10. When the installation is complete, a message appears confirming that the HaloENGINE has been successfully installed. Select one of the following options to configure the HaloENGINE.



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.



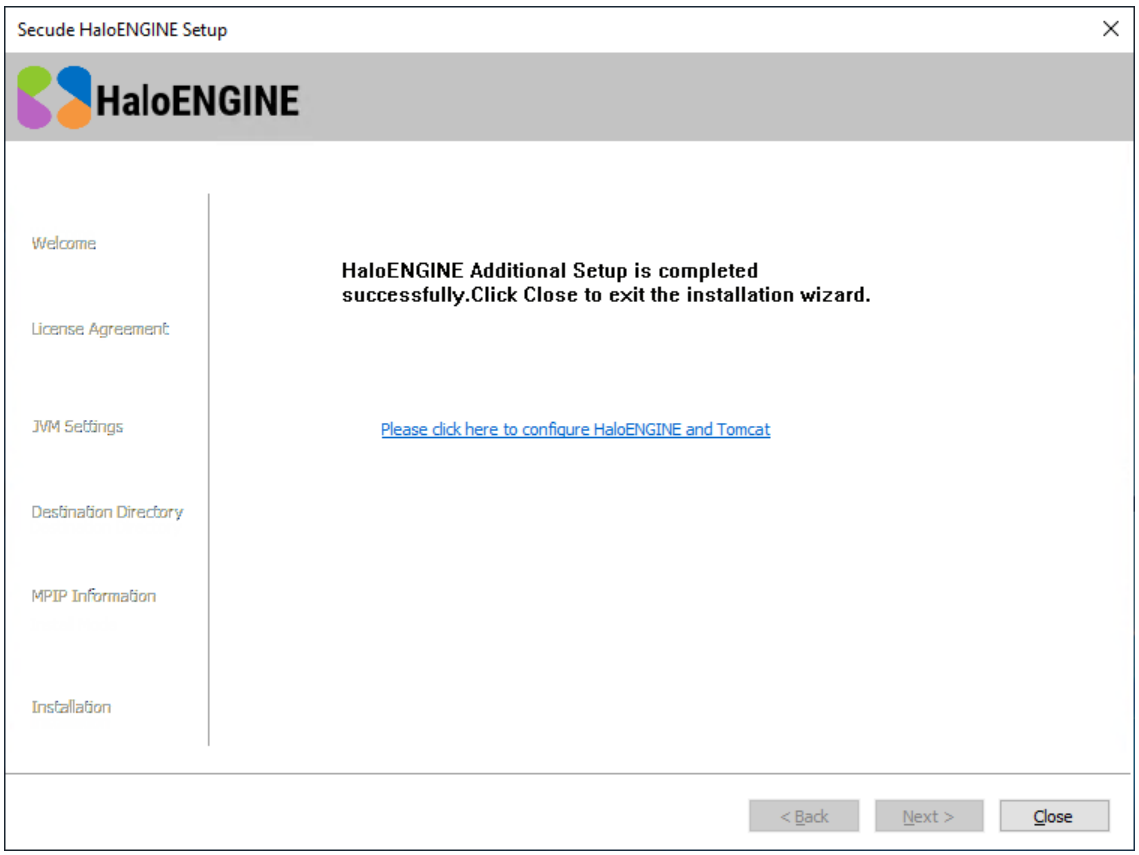
MongoDBHaloENGINE setup with pre-installed

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** to proceed.

11. The configuration screen displays a link. Click the link to access the HaloENGINE Admin Portal.



HaloENGINE with additional setup completed successfully

12. Once you click the link, the admin portal opens in your default browser, and a shortcut icon is created on your desktop.

HaloENGINE Tomcat service start-up delay after reboot

Since the HaloENGINE Tomcat service is set to Automatic (Delayed Start), it will start with a delay of approximately three minutes after a reboot or shutdown. The exact delay depends on the machine, as services marked Automatic (Delayed Start) are initiated only after all other Automatic services have started.

What to do next

1. Verify that the **Maximum memory pool size** in HaloENGINE Tomcat (…`bin/HaloENGINE_Tomcat10.exe`) does not exceed the system RAM. After setting up the HaloENGINE certificate, verify that the **maxSavePostSize** (bytes) in the Connector (SSLEnabled in `server.xml`) is smaller than the "Maximum memory pool size".
2. If you want to send large files (2GB) forward and backward, ensure that the "Maximum memory pool size" is greater 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.

6.3. 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> -applicationid
   <application_id> -tenantid <tenant_id> -thumbprint <thumb_print> -cloudtype
   <(Commercial|Custom|Germany|US_DoD|US_GCC|US_GCC_HIGH|US_Sec|US_Nat|China_01) (if
   cloudtype is Custom) <protectioncloudurl> <policycloudurl>
   HaloENGINE_Setup.exe -uninstall -keepconfig <true|false>
   ```
3. The following command shows how to install and initialize HaloENGINE.

   ```
   HaloENGINE_Setup.exe -install -initmempool 1024 -totalmempool 2048 -dir "C:\Program
   Files\Secude" -applicationid 9f0de2dd-8d49-4a3f-9676-bf4b6ff17d44 -tenantid 8c425ee7-
   352a-4657-ac77-7dc198712cb3 -thumbprint 961602617275c2ab538cf28bb3648c0c6d97edab -
   cloudtype Custom https://api.aadrm.com https://dataservice.protection.outlook.com
   ```
4. Press **Enter**.
5. Please wait until the success message appears. When it is displayed, the installation process is complete, and you can proceed to access the HaloENGINE Admin Portal.

6.4. Configuring the Tomcat Service

The HaloENGINE Tomcat Service communicates directly with the **Microsoft Purview Information Protection** service to fetch the MPIP labels. These labels are then available under the **Protect** option on the **Action Rule** page.

Any changes to labels in the Microsoft Purview portal require restarting the HaloENGINE Tomcat service.

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

6.4.1. Configuration Tool

During installation, Azure details are provided to initialize the HaloENGINE Tomcat Service. After successful authentication, the labels are fetched automatically. To update MPIP-related details (such as the Application ID), use `heslibconfig.exe`.

Default locations of log files

Name	Default Path
HaloENGINE log	`C:\Program Files\Secude\HaloENGINE\logs\customer_tenants\halo_customer\HaloENGINE_Monitor.log`
Configuration tool	`C:\Program Files\Secude\HaloENGINE\HaloENGINEService\lib\heslibconfig.exe`
MIP logs	`C:\Program Files\Secude\HaloENGINE\HaloENGINEService\logs\mip_cache_storage\mip\logs`

Default locations

To update your Azure details, follow the procedure below.

1. Open the Command Prompt with elevated rights (Run as Administrator).
2. Navigate to the directory where `heslibconfig.exe` is located.
3. To view the list of available options in silent mode, enter the following command:

   Type `heslibconfig.exe -help`

   Press `Enter`

   Output

   ```
   Usage:
   heslibconfig.exe -testmip
   heslibconfig.exe -update -applicationid <application_id> -tenantid <tenant_id> -
   ```

```
thumbprint <thumb_print> -cloudtype
<(Commercial|Custom|Germany|US_DoD|US_GCC|US_GCC_HIGH|US_Sec|US_Nat|China_01) (if
cloudtype is Custom) <protectioncloudurl> <policycloudurl>
```

4. The following command illustrates how to update json file.

```
heslibconfig.exe -update -applicationid 9f0de2dd-8d49-4a3f-9676-bf4b6ff17d44 -
tenantid 8c425ee7-352a-4657-ac77-7dc198712cb3 -thumbprint
961602617275c2ab538cf28bb3648c0c6d97edab -cloudtype Custom https://api.aadrm.com
https://dataservice.protection.outlook.com
```

5. A confirmation message appears stating that the configuration JSON file location has been successfully updated, `...\config\HaloENGINESVC.json`

Configuration change in JSON File

After installation, navigate to the configuration folder`...\HaloENGINEService\config`, and you will find a JSON file that contains the HaloENGINE Tomcat Service configuration properties. Note: From the list of default parameters, only the parameters listed below should be modified, and only when necessary. All other parameters must remain at their default values to ensure proper system functionality and stability.

Name	Description
block_pii	Enable or disable the visibility of Personally Identifiable Information (PII) in the MIP SDK logs. • 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	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.

Name	Description
cacheuserlicense	• 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
databoundary	Audit and telemetry events are sent to the nearest collector, where these events are stored and processed. Other options: 1. Asia 2. Europe_MiddleEast_Africa 3. European_Union 4. North_America For example, if your AIP administrator sets North_America, the HaloENGINE Tomcat Service forces all telemetry and audit data to go directly to North America.
enabledke	Double Key Encryption • 0 (default value)—Disables the DKE functionality in the HaloENGINE Tomcat Service. • 1 (On)—Enables the DKE functionality in the HaloENGINE Tomcat Service. Please be aware that DKE labels are only visible when DKE functionality is enabled.
enablefiletracking	To 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	To transmit diagnostic information to Microsoft. • 0 (default value)—all diagnostic events are transmitted. • 1—Minimum diagnostic events are transmitted.

Name	Description
log_level	The available log levels are ERROR, WARNING, INFO, and DEBUG.
log_purge	It indicates removing files older than a defined time frame. By default, the log files older than 7 days will be deleted.
streambuffersize	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.
templatefile_purge	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 Tomcat Service creates a template file in the tmp\GUID folder (which can be located in the HaloENGINE Tomcat Service user's profile folder). In the background, it examines and deletes files that have reached the configured time, i.e., after 16:25 hours. Note: This is only applicable in the event of CAD assembly file labeling.

HaloENGINE Tomcat service configuration

6.4.2. WinHTTP Proxy Settings

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 190.160.166.191:8080`

In this case, the proxy server has been set up with `190.160.166.191:8080`. Once this command is executed successfully, the registry is updated with the proxy server URL, and the HaloENGINE Tomcat Service ensures that the configured proxy settings are applied.

6.5. Initial Configuration of HaloENGINE Admin Portal

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

6.5.1. 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 portal offers 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.

6.5.2. 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 creating or updating any settings in HaloENGINE features, service configuration, profile configuration, basic system configuration, or CAD file types, you must click the Reload Configuration button for the changes to take effect.

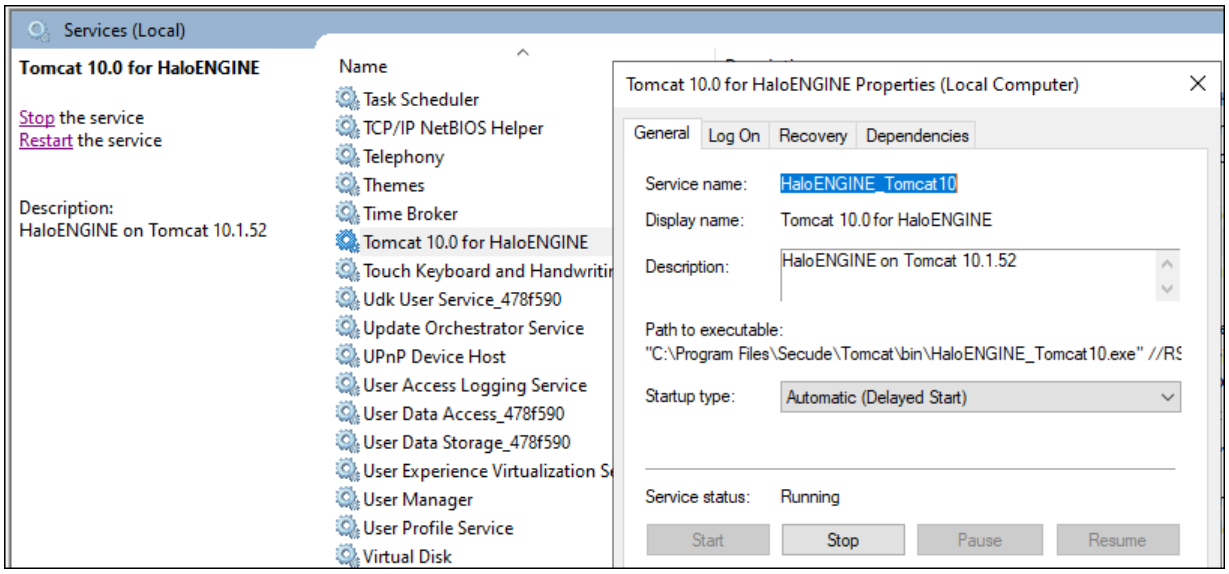
What is meant by restart?

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, import configuration, 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 10.0 for HaloENGINE**.

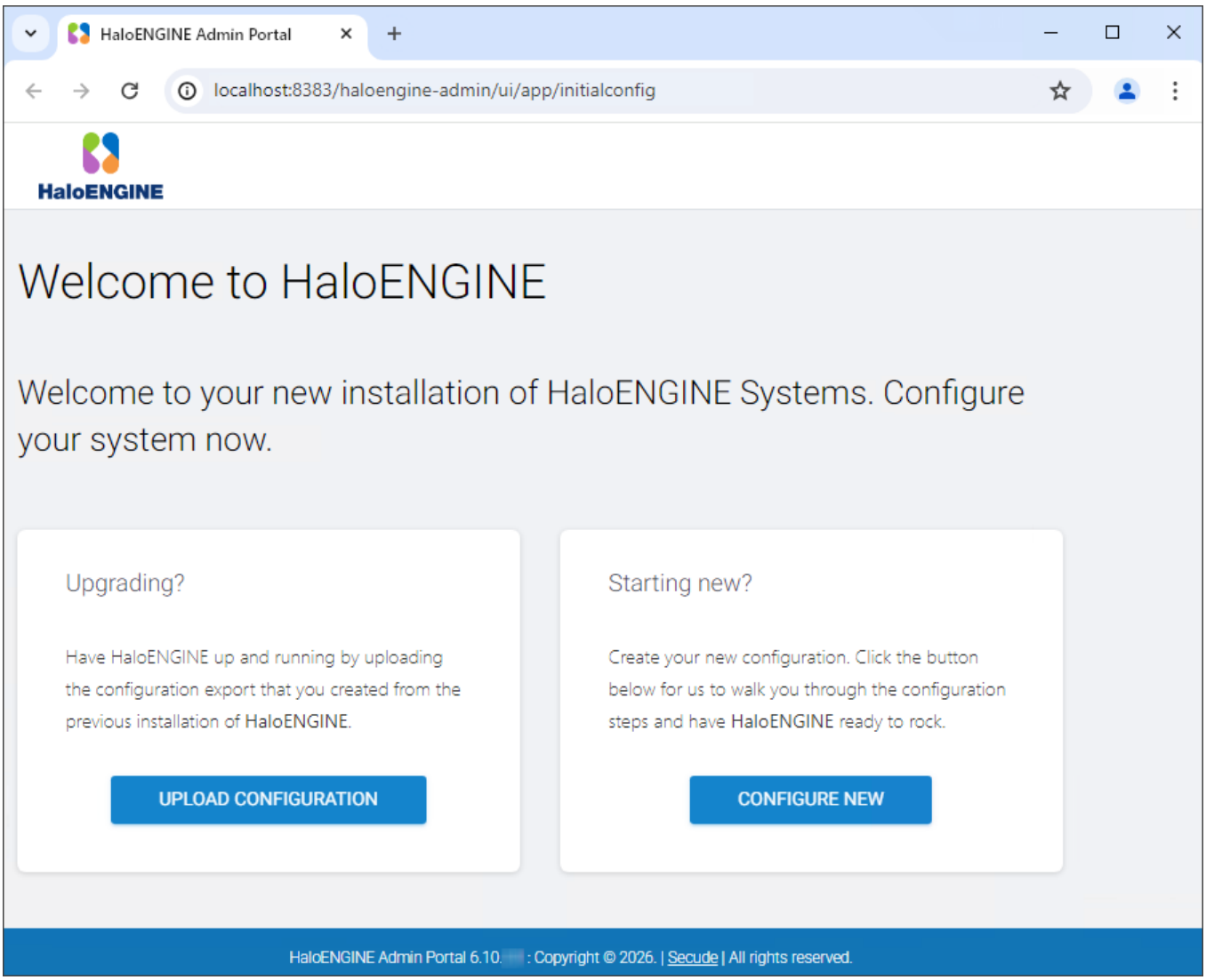


Restarting Tomcat Service

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

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

6.5.4. Upgrade HaloENGINE (Uploading Existing Configuration File)

Use this page to upgrade the HaloENGINE from the current version to the latest version. Note: Upgrading via the HaloENGINE installer is not supported.

Prerequisites:

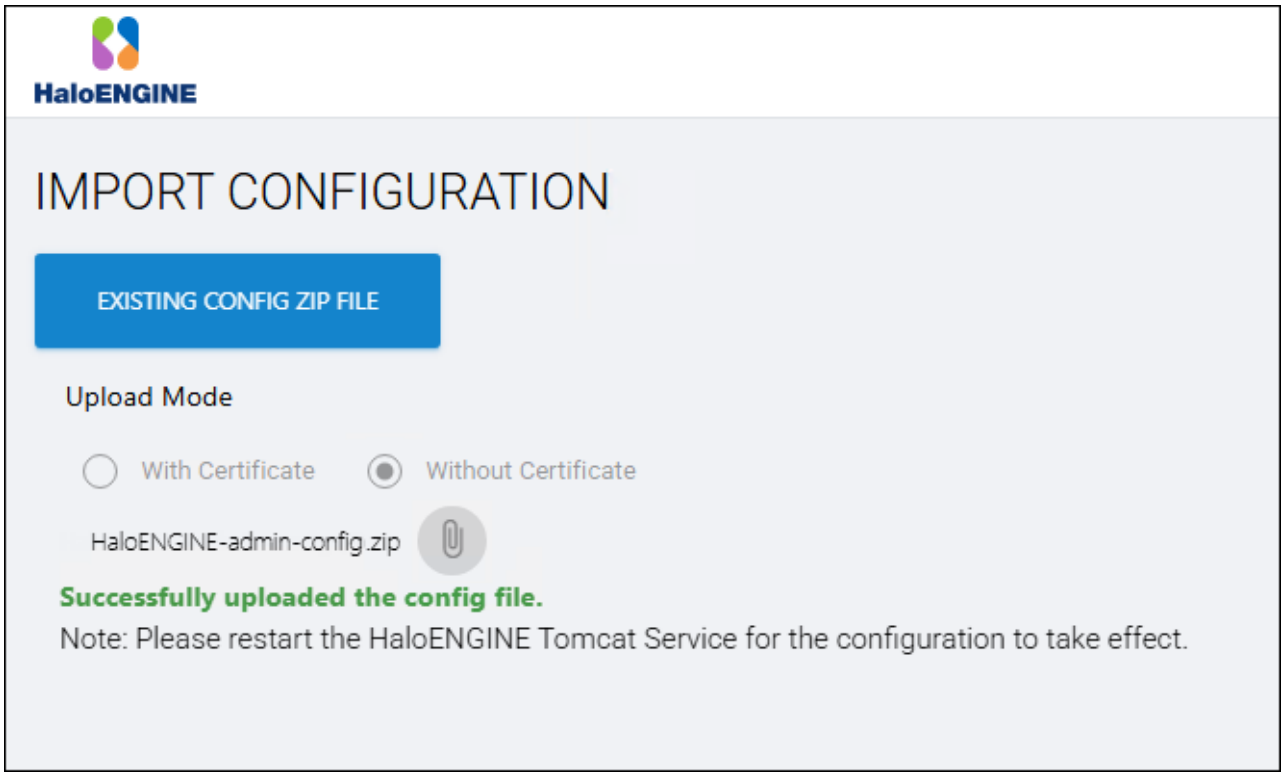
- **For versions earlier than 6.9 (for example, 6.8)**
    - Back up all certificates.

- Export HaloENGINE-admin-config.zip from the Admin Portal.
- Uninstall any existing versions of HaloENGINE and HaloENGINE Service.

- **From version 6.9 and later**
  - Export HaloENGINE-admin-config.zip from the Admin Portal.
  - Uninstall any existing version of HaloENGINE.
  - Ensure HaloENGINE version 6.10.x.x is installed on the system.

Follow the instructions below to upgrade:

1. Click **Upload Configuration** and then click **Existing Config Zip File**.
2. **Upgrading from version 6.8 to 6.10:** Select **Without Certificate**, click the attach button to select HaloENGINE-admin-config.zip, restart the HaloENGINE Tomcat Service, and import the certificates into the HaloENGINE Admin Portal.
3. **Upgrading from version 6.9 to 6.10:** Select **With Certificate**, click the attach button to select HaloENGINE-admin-config.zip, and restart the HaloENGINE Tomcat Service.



Uploading the existing configuration file

What to do next: Set up the Classification Engine. Please refer to the section "Setting Up Classification Engine".

Reset Password

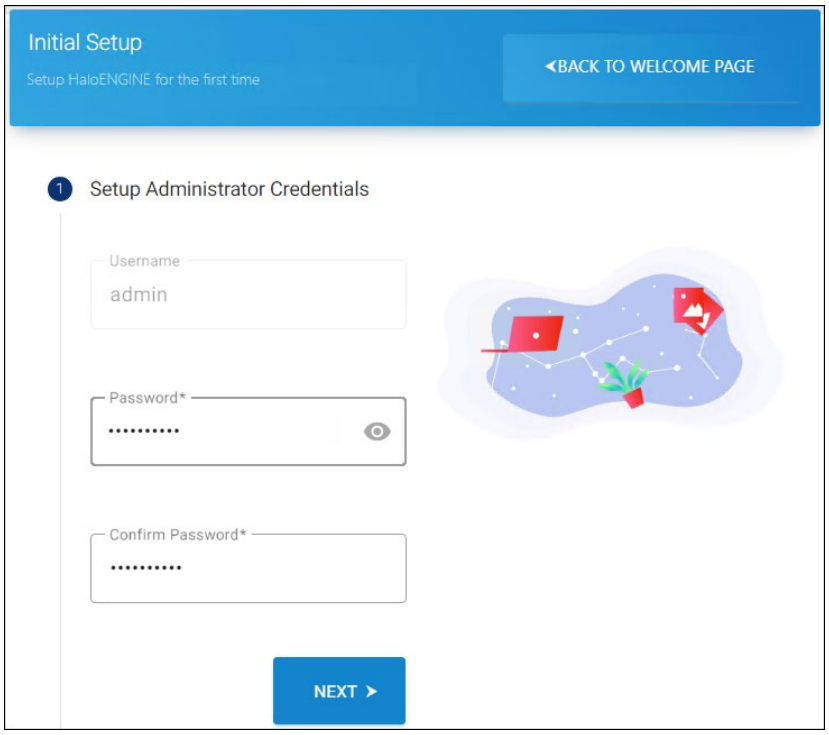
If your administrator password in the previous version is less than 12 characters, you must reset it according to the current password policy. To know how to reset the password, refer to the section "Reset Administrator Password".

6.5.5. Starting a New HaloENGINE

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

6.5.5.1. 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

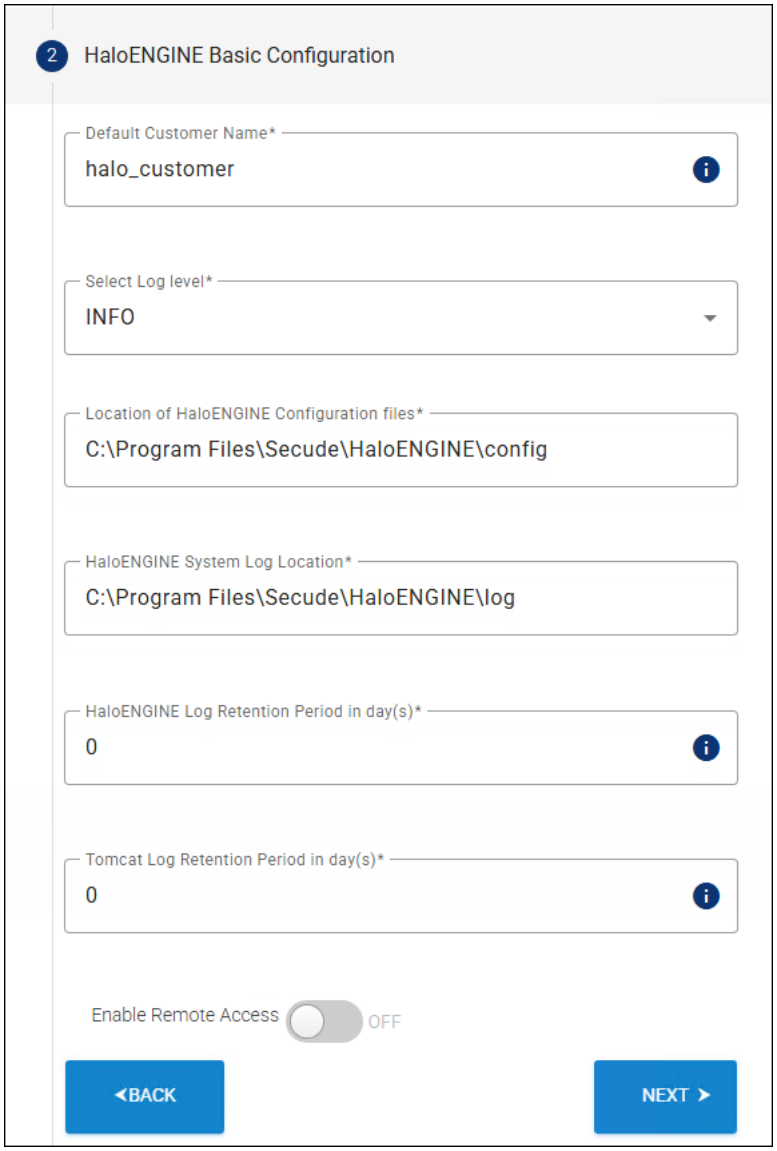
Be sure to use a strong yet memorable password. If you forget it, HaloENGINE provides an option to reset your password. To know how to reset the password, refer to the section "Reset Administrator Password". Password must be 12–30 characters and include:

1. At least one uppercase letter [A-Z]
2. At least one lowercase letter [a-z]
3. At least one number [0-9]
4. At least one symbol (@$!%*?&-)

For example, `HaloENg!nE@-`

6.5.5.2. Step 2. HaloENGINE Basic Configuration

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

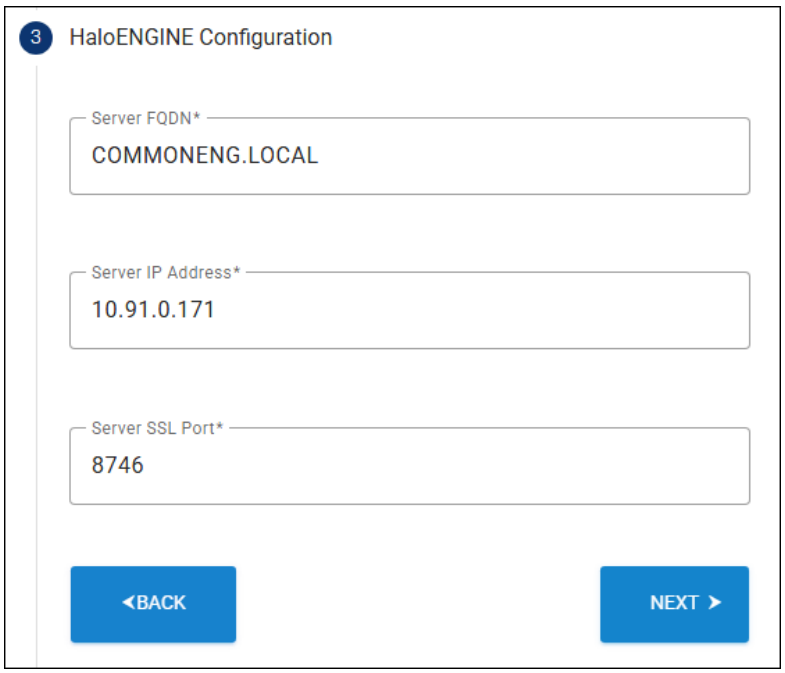


Basic Configuration Page

2. **Default Customer Name**—The initial default customer name is **halo_customer**. You can modify this name after the portal initialization is complete.
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**.

6.5.5.3. 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.

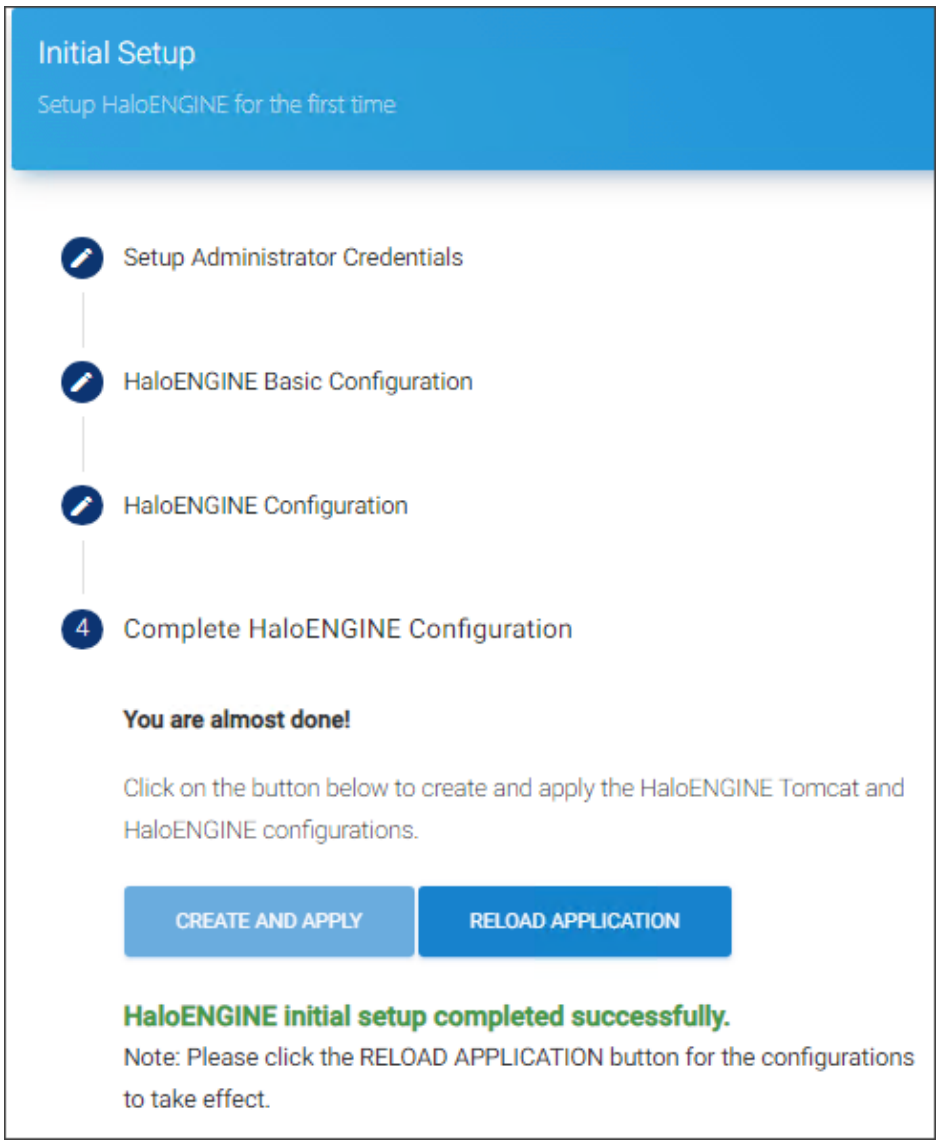


Configuration page

2. Click **Next**.

6.5.5.4. Step 4. Completion Page

1. This is the final page of the configuration.



Final configuration page

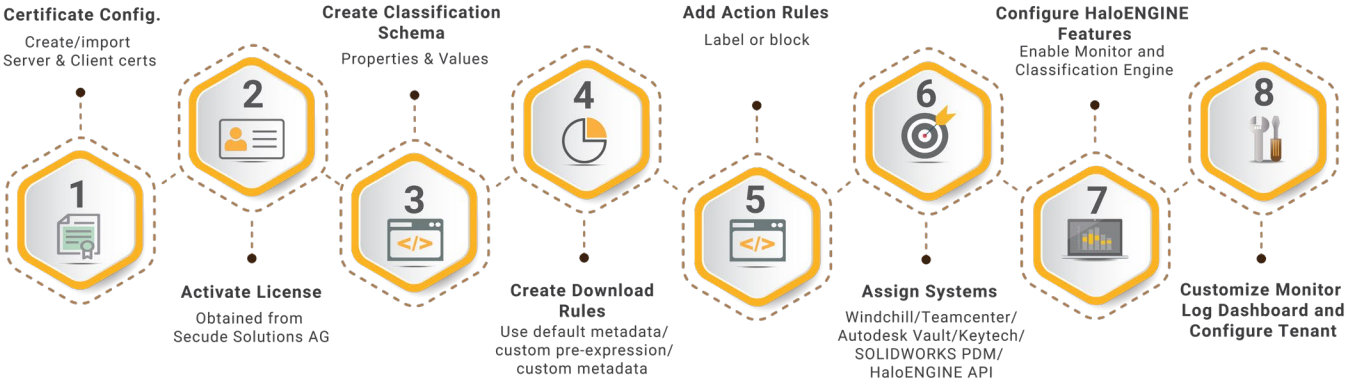
2. Click **Create and Apply** to create `config.properties` file and update the `hc-servlet.xml` file.
3. Click **Reload Application** to apply the changes. After reloading, the page will redirect to the login page.
4. These settings can always be changed through the portal as detailed in the section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

6.6. Setting Up Classification Engine

This chapter describes how to set up HaloENGINE.

6.6.1. Quick Start Set Up

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



Setting up the Classification Engine

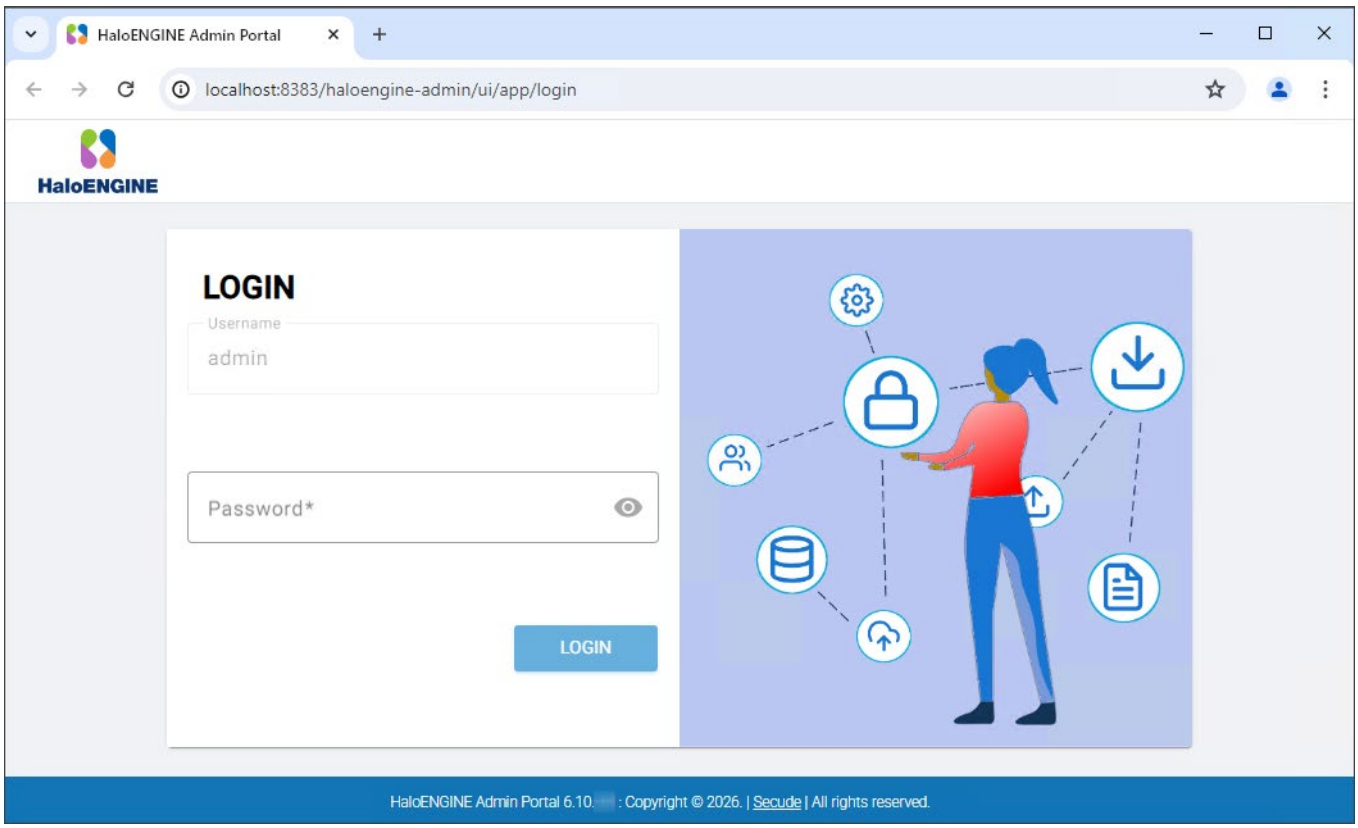
The license file obtained from Secude specifies the available features and supported system types. Accordingly, you can access only the system types listed in your license.

This chapter describes the Monitor, Block, and Protect features that apply across various system types, including Windchill, Teamcenter, Keytech, Autodesk Vault, SOLIDWORKS PDM, and HaloENGINE_API. For illustration purposes, Windchill is used as the visual example throughout this chapter. Refer to the HaloCAD for PLM/PDM Operations Manual if you would like to view the metadata, log, and user interface for a particular system type.

6.6.2. 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: Copying and pasting are not allowed in this field.

   Results:

   a. The HaloENGINE Admin Home page is the first page displayed after you log in to the portal.

   b. Please refer to the following section.

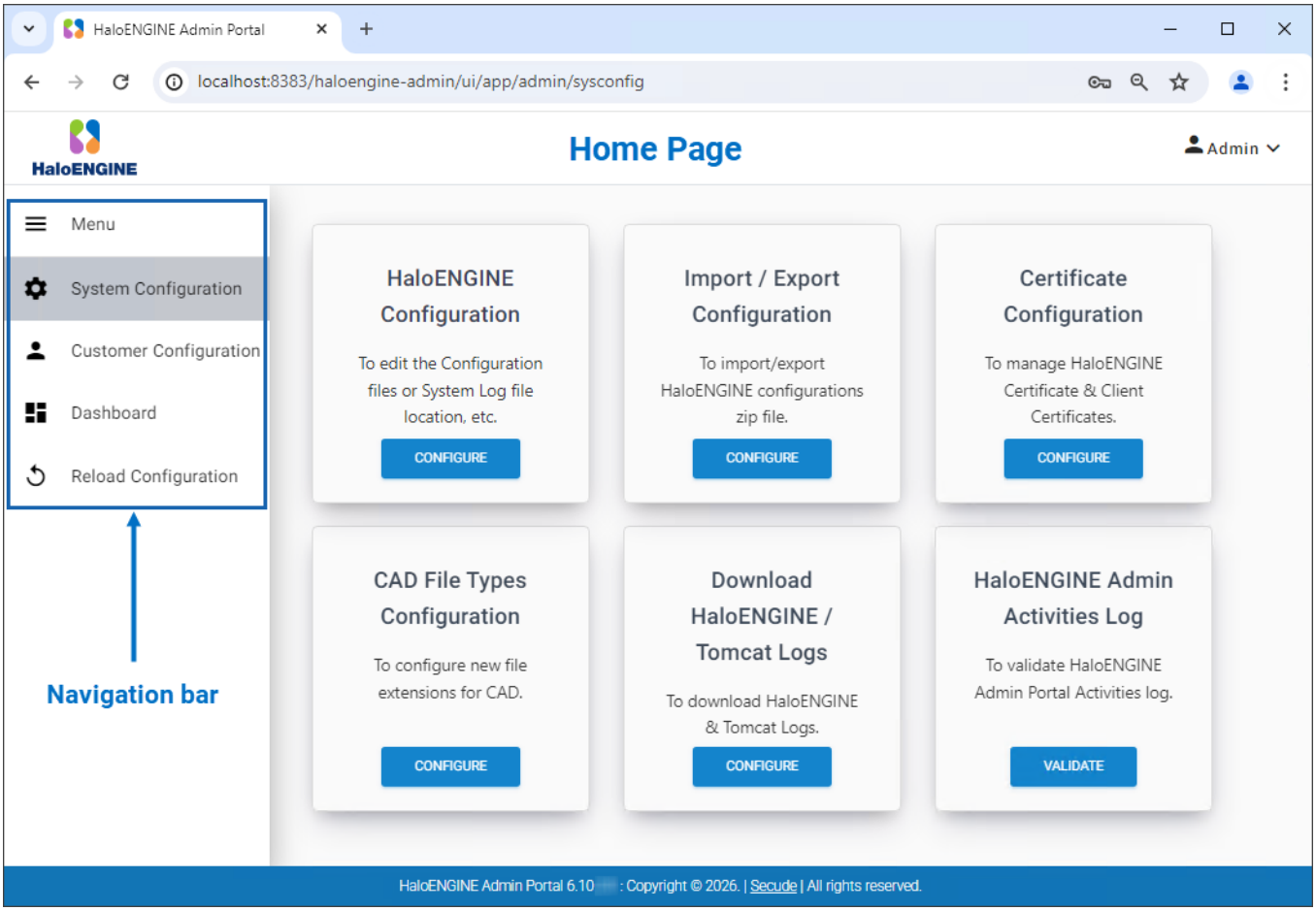
Invalid credentials or the number of sessions exceeded

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.

6.6.3. HaloENGINE Admin Portal Home Page

When an administrator logs in to the Admin Portal, the **Home** page is displayed as the default landing page. This page provides several options that assist you in managing and configuring the portal. Before proceeding with other administrative tasks, it is recommended to familiarize yourself with the main elements of the Home page and understand how to interact with them. The Home page appears as shown in the following figure. The key sections of the Home page are highlighted below.



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 the `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".

6.6.4. 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.
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 their location within the application.

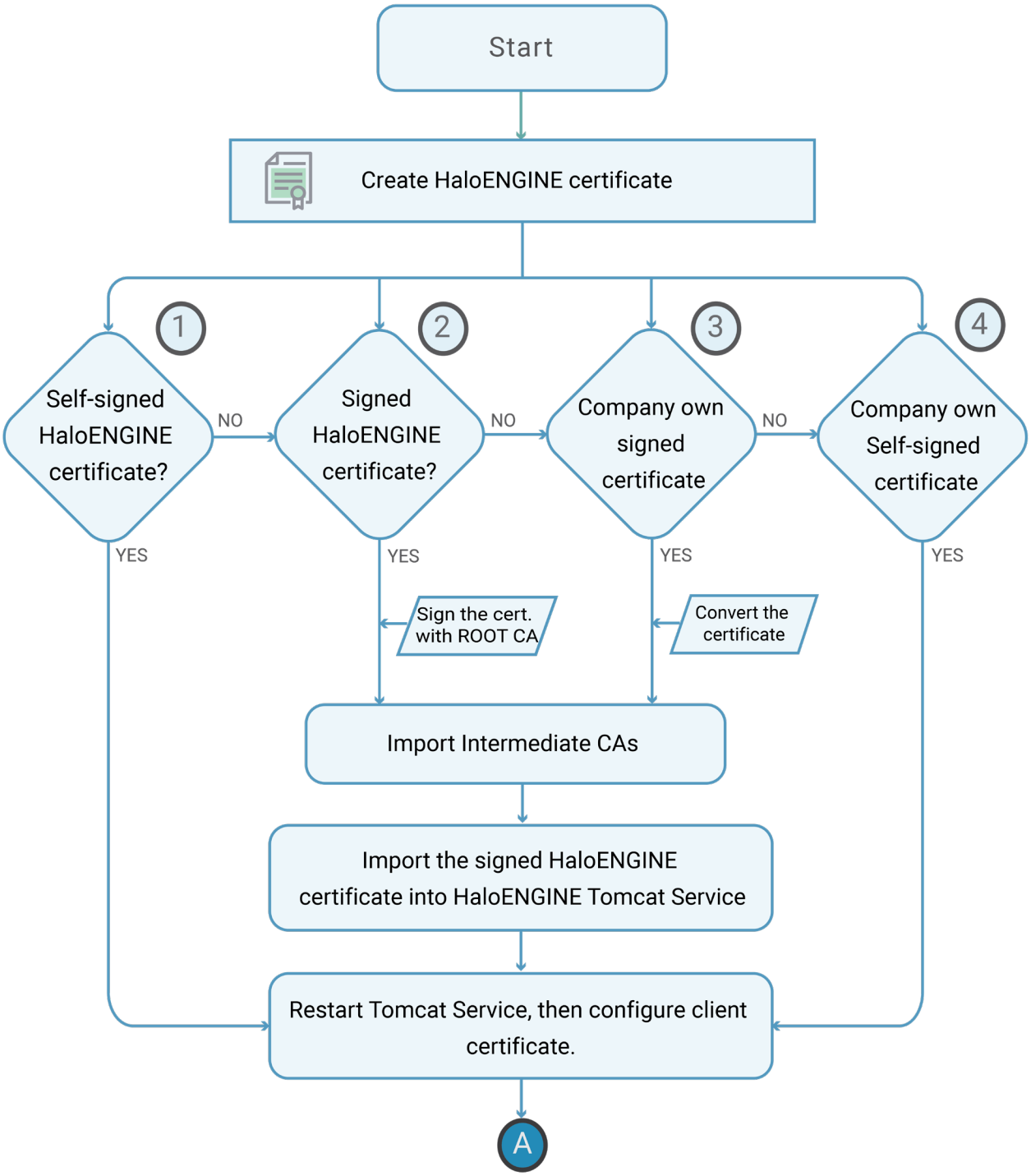
Elements Description

6.6.5. 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.

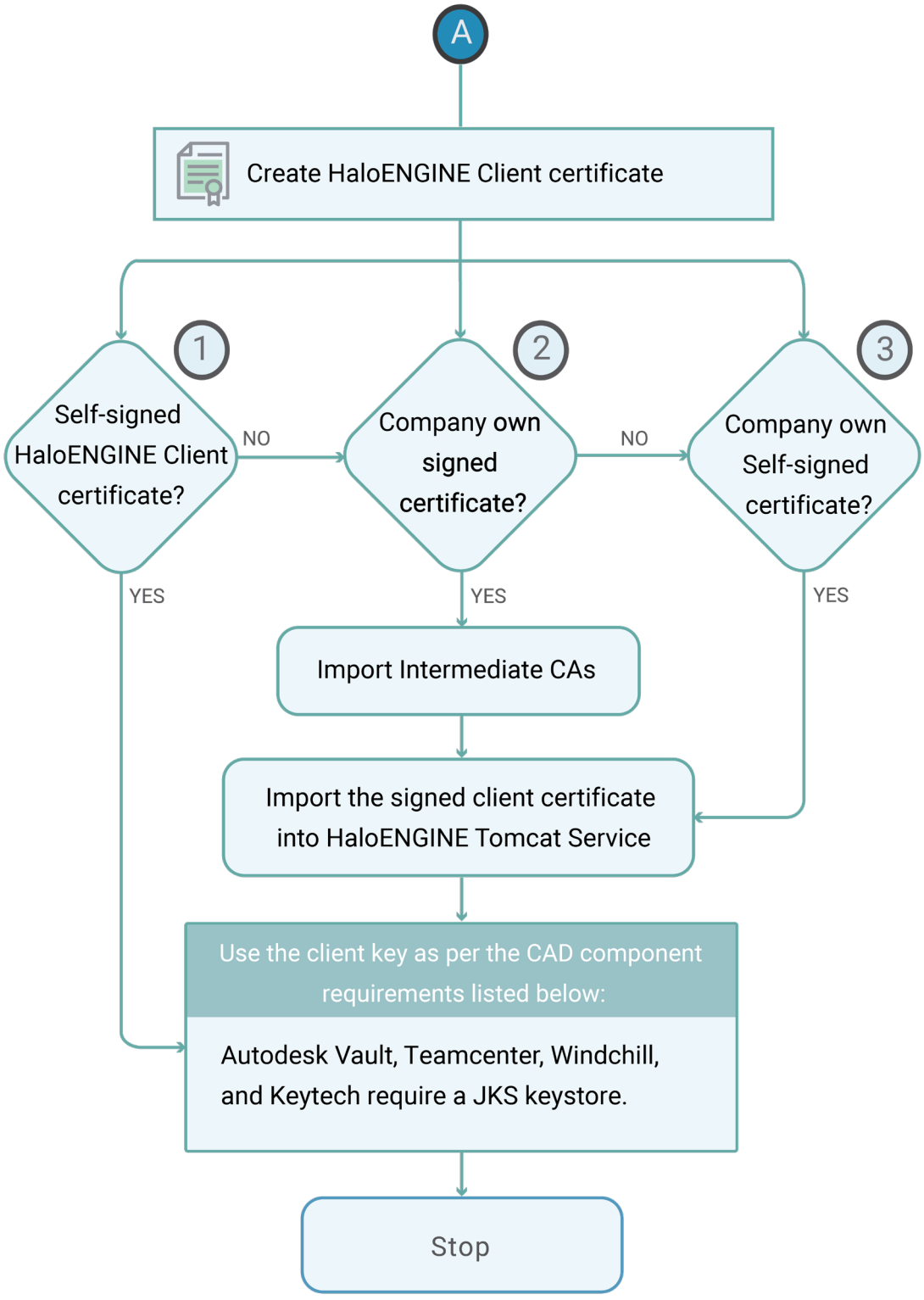
The figure below depicts the high-level steps involved in administering the server certificate.



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 for authentication.

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

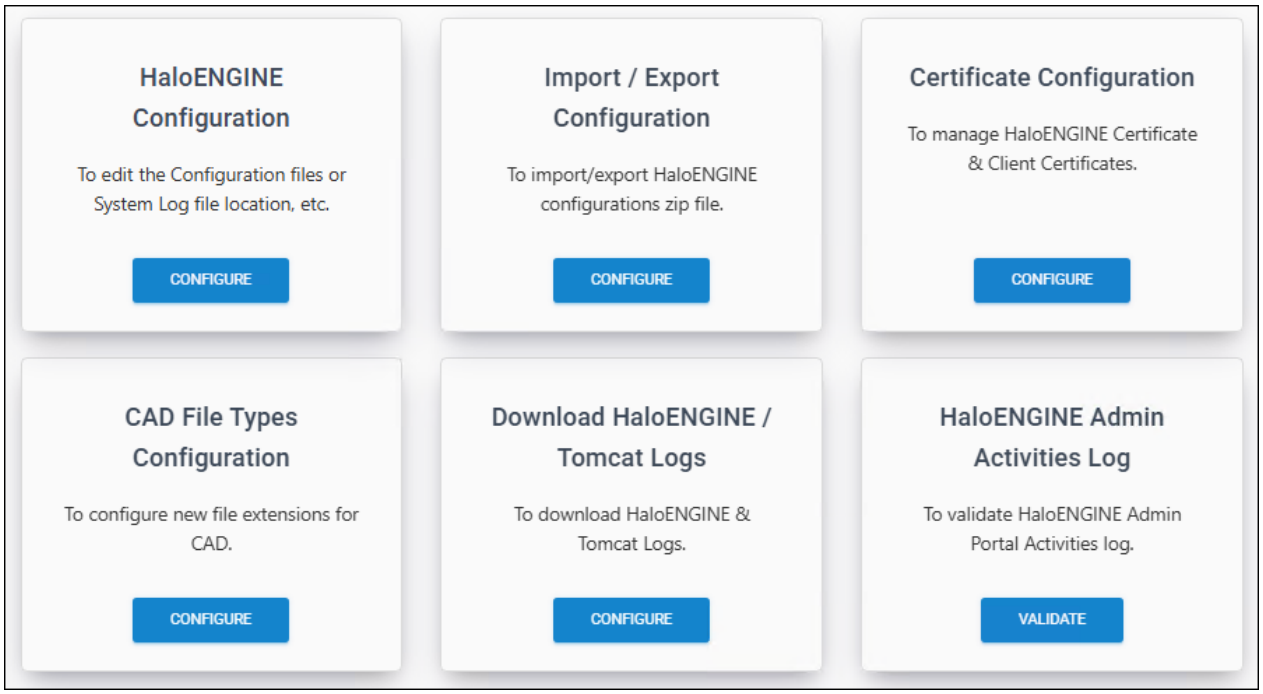


HaloENGINE Client Certificate

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

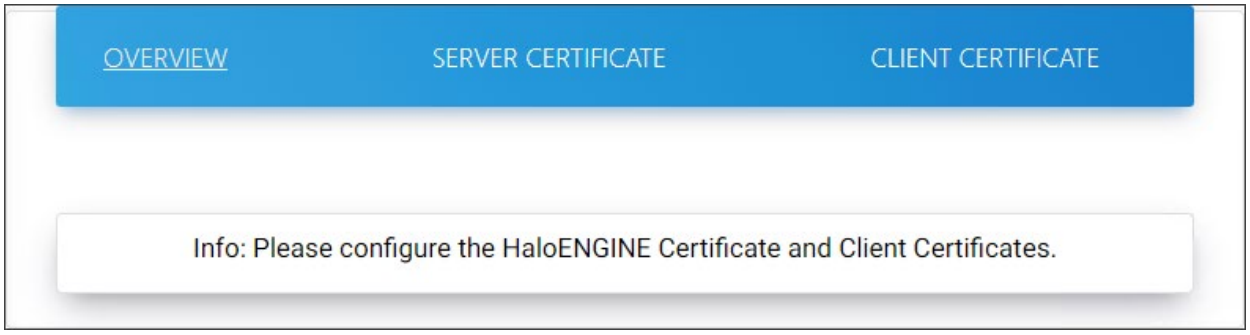
Step 1a. Create a Self-Signed HaloENGINE (Server) Certificate

1. On the left navigation bar, click **System Configuration**, go to the **Certificate Configuration** tab, and click **Configure**.



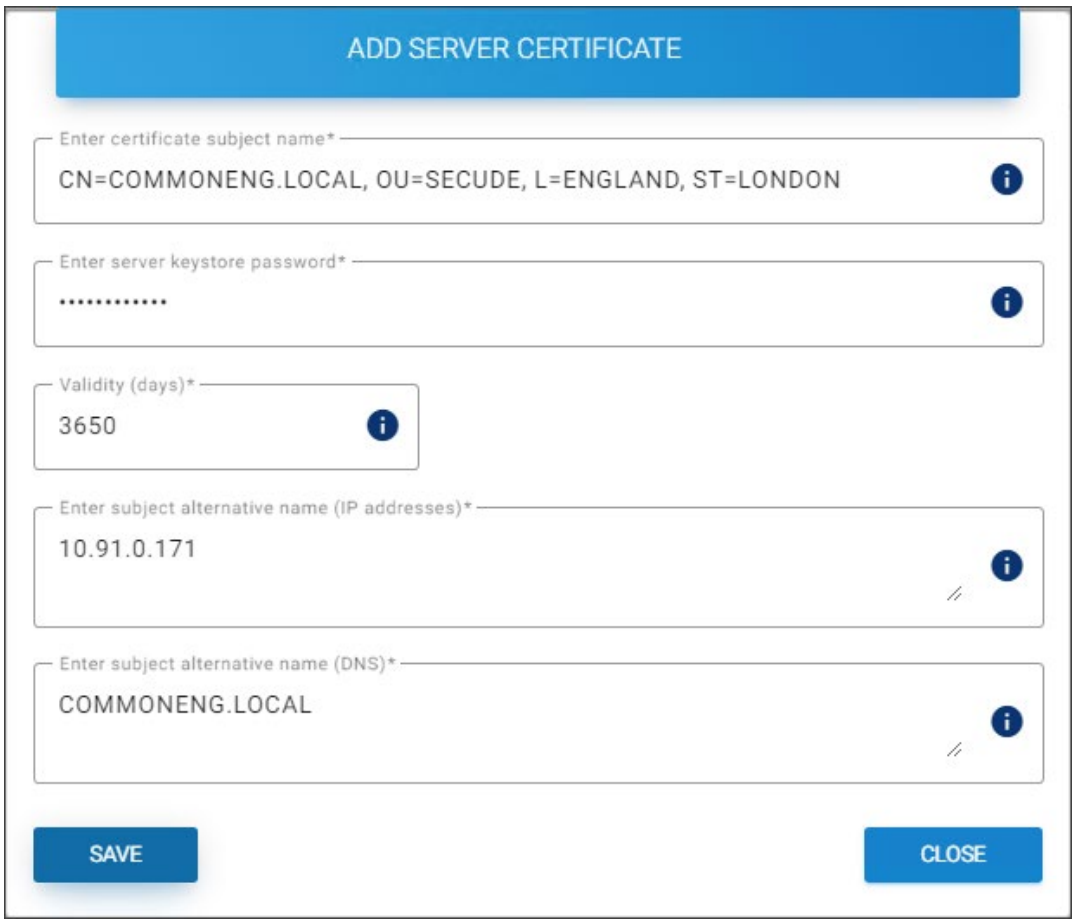
System Configuration page

2. The *Overview* page appears as shown in the figure below:



Overview page

3. Click **Server Certificate**, and then click the **Create Certificate** button.
4. The *Add Server Certificate* page appears 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. A confirmation message appears after the certificate is successfully updated.

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

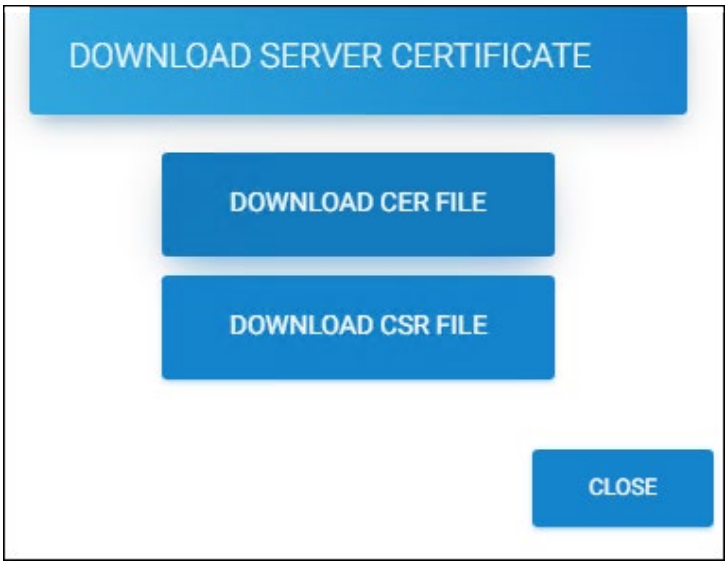
    c. The page displays the server certificate information.

What to do next

a. For client systems such as Windchill, Teamcenter, Keytech, or Autodesk Vault, proceed to Step 4 to generate the client keystore.

b. In case of the SOLIDWORKS PDM client/HaloENGINE_API, download the self-signed certificate (`HaloENGINEServer.cer`) and install it into the Trusted Root Certification Authorities on the client machine.

c. Click the download icon, and in the **Download Server Certificate** dialog, click **Download CER File** to download a copy of the self-signed server certificate `HaloENGINEServer.cer`.



Download Server Certificate

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

Keystore Password Policy

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

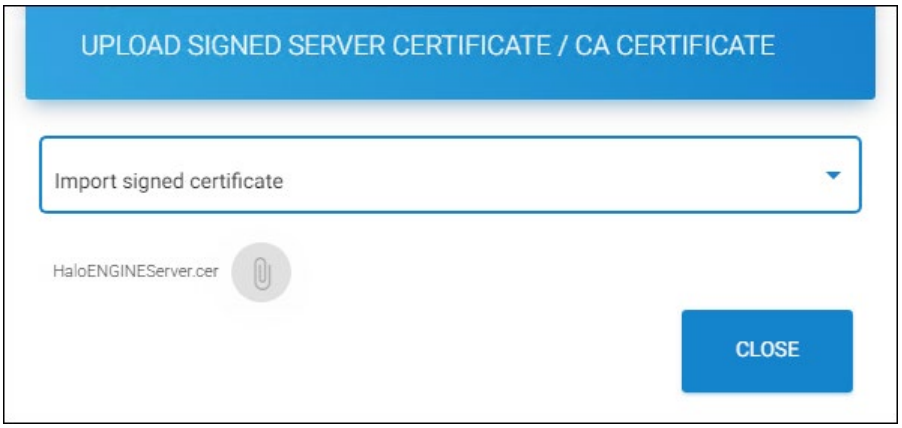
- Passwords must be between **6** to **30 characters** long
- The password should not contain a space
- The first letter should be an alphabetic character [**upper** or **lower** case letter]
- It must contain at least **1 numerical** character [0-9]
- It must contain at least **1 symbol** [$ _ #]

  For example: **HaloENGINE_1**

Step 1b. For a CA-Signed HaloENGINE Certificate

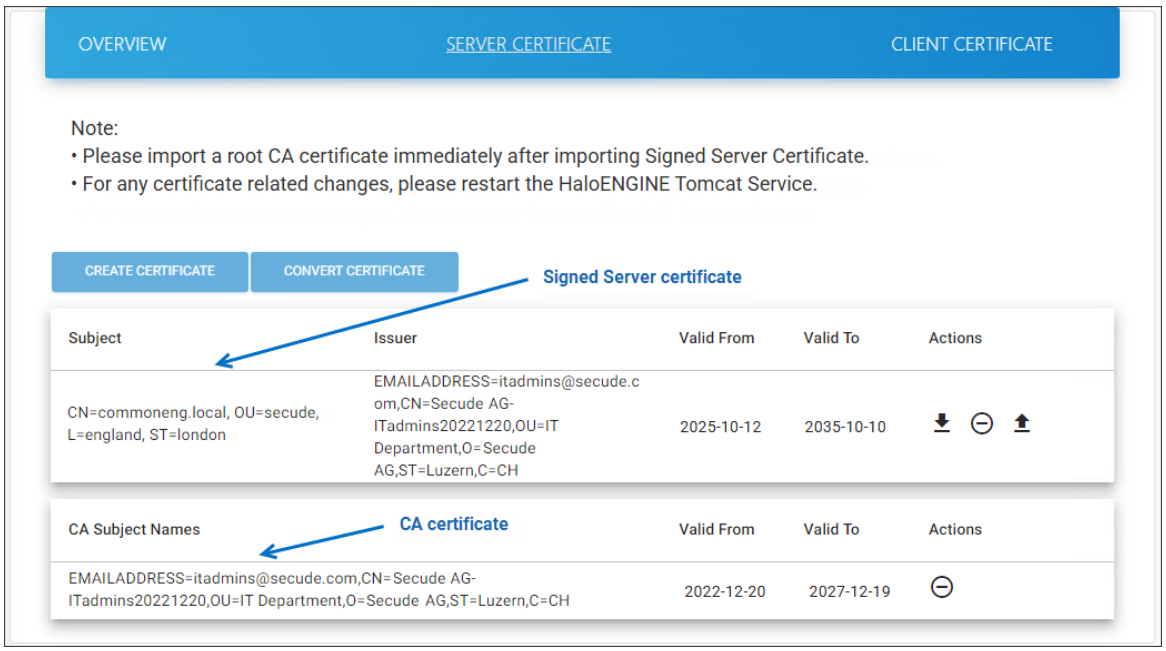
You can convert the self-signed certificate created in Step 1a into a CA-Signed certificate by signing it with your Certificate Authority (CA).

1. Click the download icon, and in the **Download Server Certificate** dialog, click **Download CSR File** to download the Certificate Signing Request (CSR) `HaloENGINEServer.csr`.
2. Submit the `HaloENGINEServer.csr` file to your Certificate Authority to obtain the signed certificate in `HaloENGINEServer.cer` format.
3. Import the CA - refer to Step 3. Note that a signed certificate cannot be imported until its corresponding CA certificate has been uploaded.
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** dialog box.



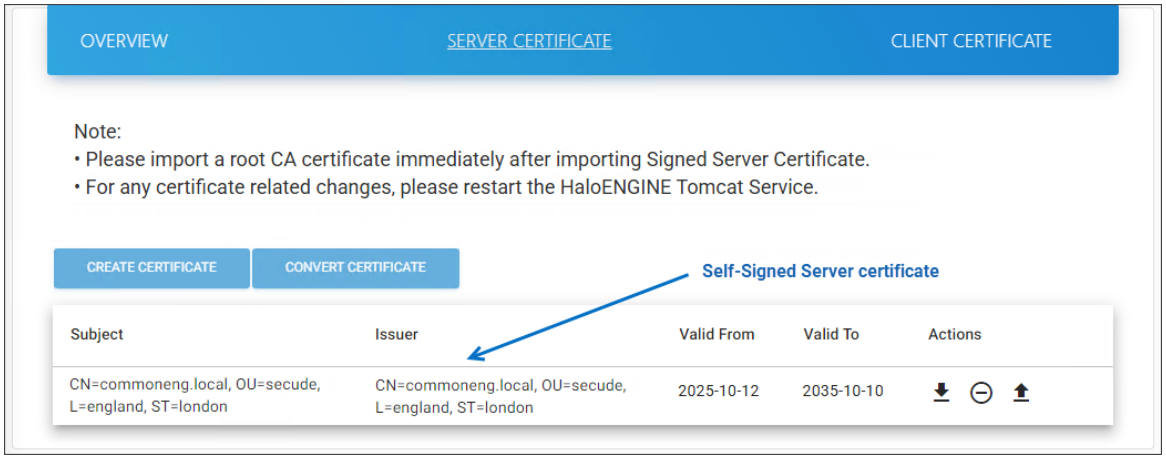
Importing the signed HaloENGINEServer.cer certificate

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

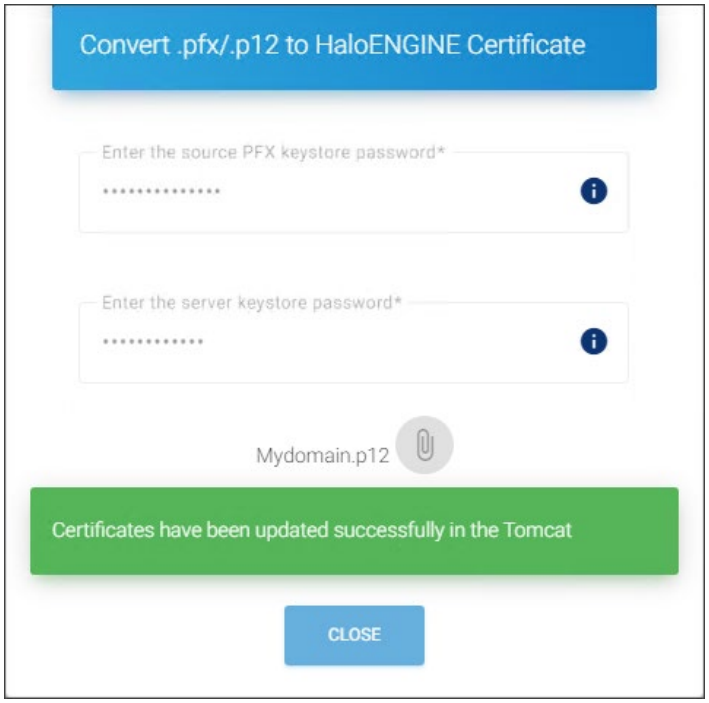
What to do next: Continue from Step 4.

6.6.5.2. Step 2. Use Company Own Certificate as the 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 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**, go to the **Certificate Configuration** tab, and click **Configure**.
2. Click **Server Certificate**, and then click **Convert Certificate**.
3. The **Convert .pfx/.p12 to HaloENGINE Certificate** dialog appears.
4. Enter the source password for the PFX/P12 file you want to convert. Note: Copying and pasting are not allowed in this field.
5. Enter the server keystore password. Please refer to the section "Keystore password policy".
6. Click the **attachment** button and select the PFX/P12 file from the **Open** dialog box.



Convert the existing certificate

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

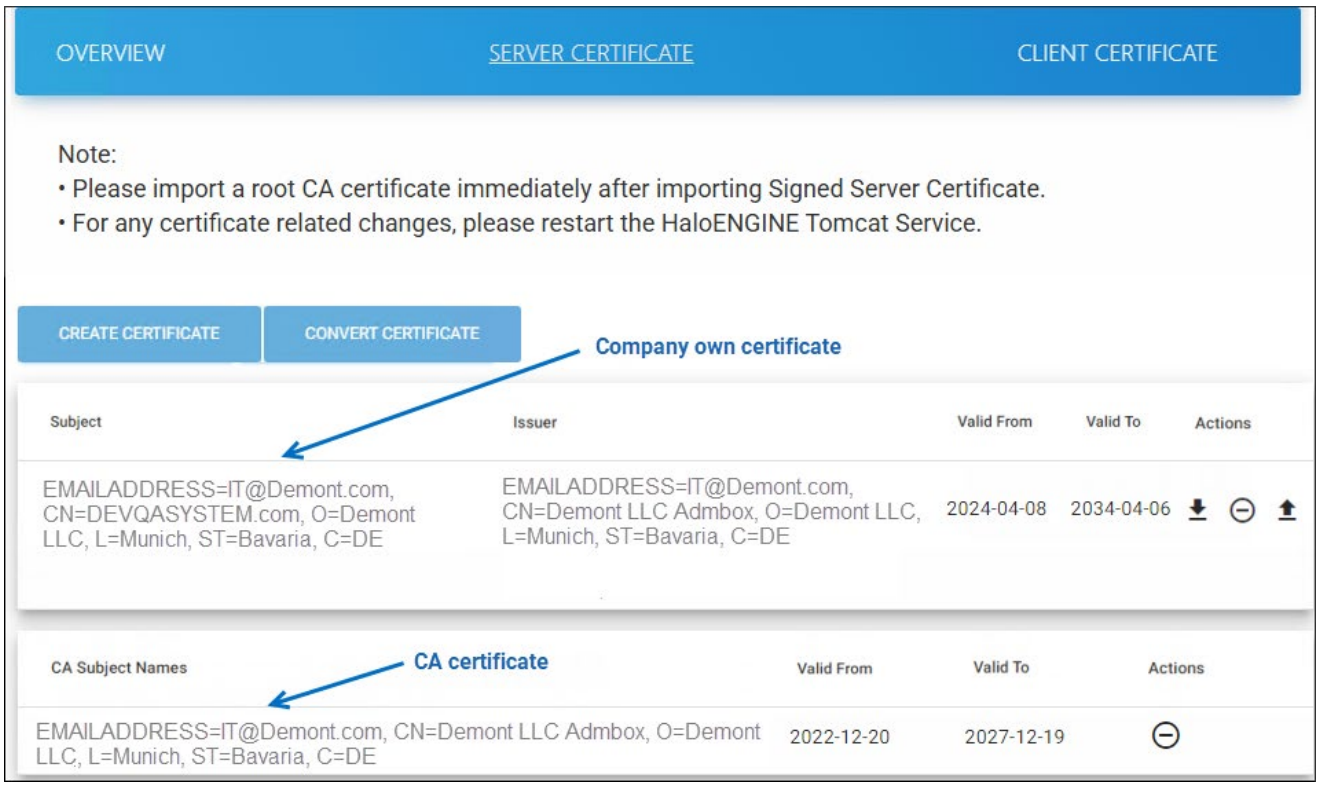
Results:

a. A confirmation message appears once the certificate is uploaded successfully.

b. Click **Close** to exit the dialog box.

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.

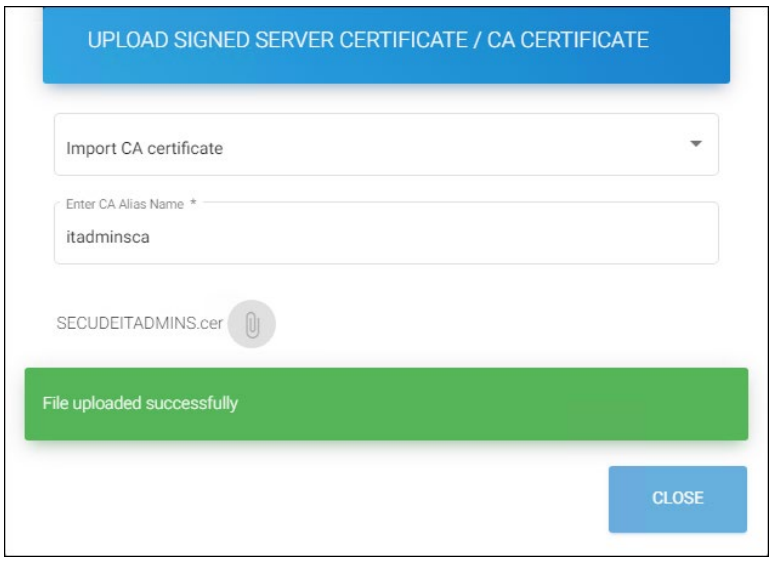
6.6.5.3. Step 3. Import Intermediate CAs

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.

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** appears.
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** dialog box.



Importing the CA certificate

4. The certificate name appears on the page.

   Results:

   a. A confirmation message appears after uploading the certificate

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

6.6.5.4. Step 4. Use Client Certificate from Admin Portal (Option 1)

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 - refer to the below Step 4a.
2. Another option is to use the company's own certificate; refer to Step 5 for SOLIDWORKS PDM and HaloENGINE API clients.

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

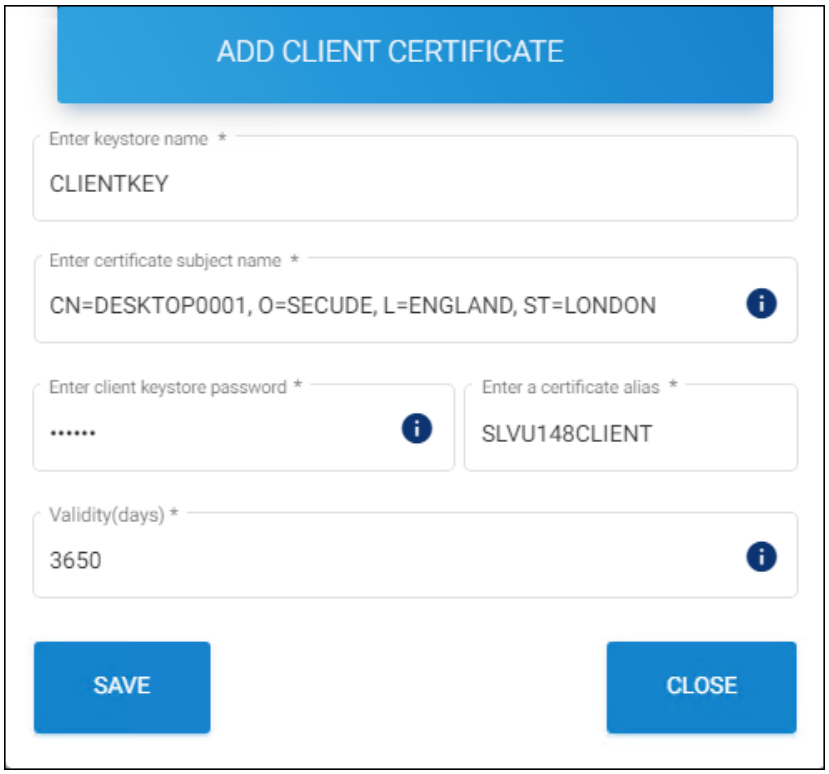
This instruction applies to the clients listed below. Note: Self-signed client certificates can be generated using the HaloENGINE admin portal, and they are added to the client Keystore at the time of creation.

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

Client Keystore

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

1. On the left navigation bar, click **System Configuration**, go to the **Certificate Configuration** tab, and click **Configure**.
2. Click **Client Certificate** and then click **Create Certificate** button.
3. The *Add Client Certificate* page appears 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: Copying and pasting 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. A confirmation message appears after the client's certificates are successfully added.

   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 filename.

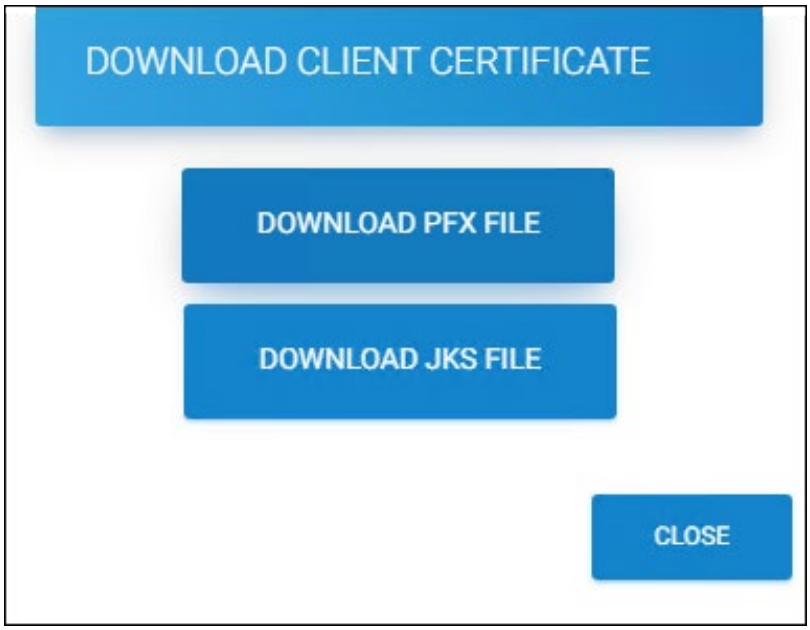
c. Click **Close** to exit the page.

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 it to the client machine.

1. Click the download icon, and the **Download Client Certificate** dialog appears.
2. Click **Download JKS File** to download a copy of the JKS file. In the example shown above, a file named `CLIENTKEY.jks` is downloaded. Note: HaloENGINE client systems, such as Windchill, Teamcenter, Autodesk_Vault, and Keytech, require a JKS Keystore to operate.



Downloading the client certificate

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

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

If you want to use your company's certificate, you must add it to the HaloENGINE Tomcat Service. This option applies to SOLIDWORKS PDM and HaloENGINE API clients.

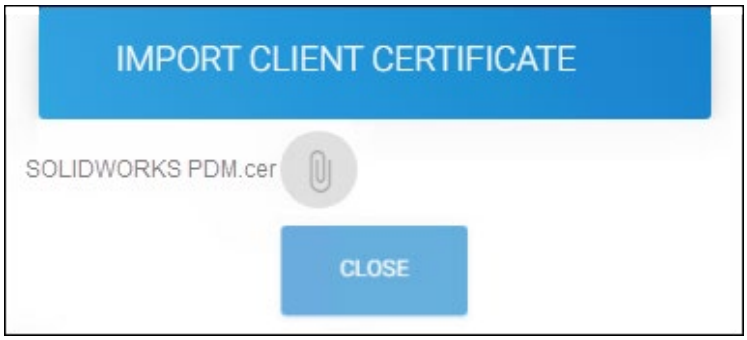
Prerequisites:

1. In the case of other clients, have client certificates ready in advance.
2. 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**.

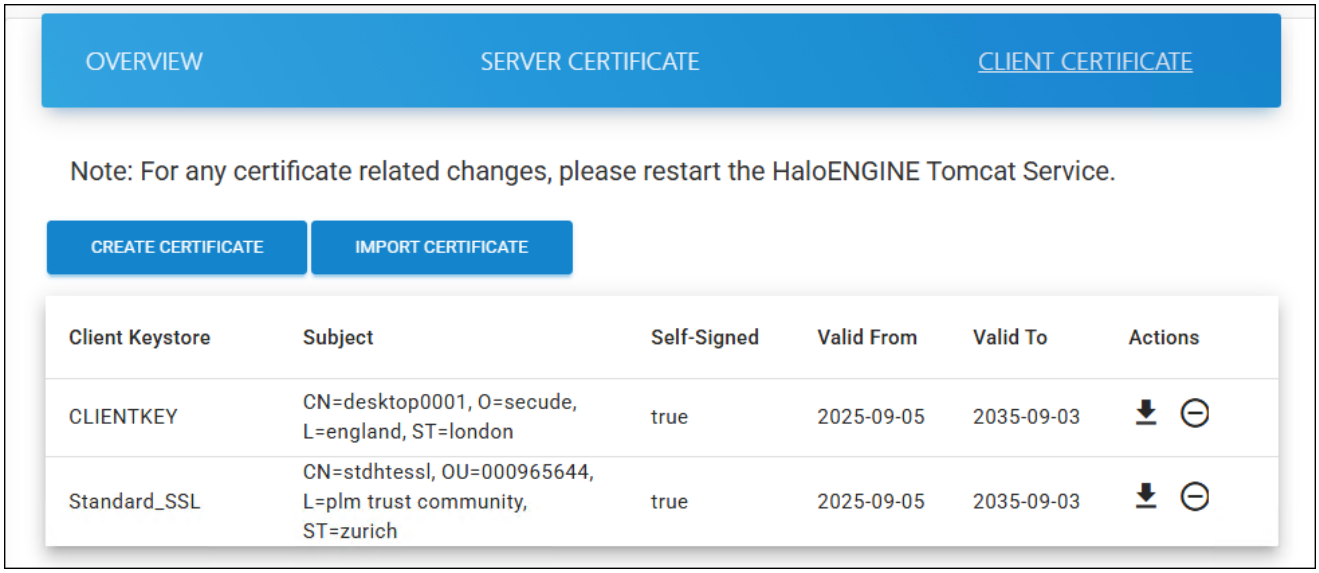
2. The **Import Client Certificate** dialog appears.
3. Click on the attachment button and select the client certificate from the **Open** dialog box.
4. Perform the same steps to upload other client certificates as well.



Uploading existing client certificates

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

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



Uploaded client certificates

6.6.5.6. 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**, go to the **Certificate Configuration** tab, and click **Configure**. Then, click **Client Certificate** in the top-right corner.
2. Select the client certificate and click the delete icon under the **Actions** column.
3. In the prompt *"Are you sure to delete?"*, click **OK**. By clicking **OK**, you confirm the permanent deletion of the client certificate.

   Result: A confirmation message appears after the certificates are successfully deleted.

6.6.5.7. How to Delete the HaloENGINE Certificate?

Deleting the server certificate removes all certificates.

Removing the server certificate will permanently delete all other certificates, including client and CA certificates. After deletion, the admin portal will not load. To access the portal again, manually change the protocol to **HTTP** and the port number to **8383**, and clear your browsing data.

CA Certificate(s)

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

1. On the left navigation bar, click **System Configuration**, go to the **Certificate Configuration** tab, and click **Configure**.
2. Click **Server Certificate** in the center.
3. Select the CA certificate and click the delete icon under the **Actions** column.
4. In the prompt *"Are you sure to delete server CA certificate?"*, click **Yes**. By clicking **Yes**, you confirm the deletion of the CA certificate from the Keystore.
   Result: A confirmation message appears after the certificates are successfully deleted.

Server Certificate

To remove the server certificate, follow these instructions:

1. On the left navigation bar, click **System Configuration**, go to the **Certificate Configuration** tab, and click **Configure**.
2. Click **Server Certificate** in the center.
3. Select the server certificate and click the delete icon under the **Actions** column.
4. In the prompt *"Are you sure to delete the HaloENGINE Certificate?"*, click **OK**. By clicking **OK**, you confirm permanent deletion of the Server and Client certificates from the Keystore.
   Result: A confirmation message appears after the certificates are successfully deleted.

Restart the HaloENGINE Tomcat service

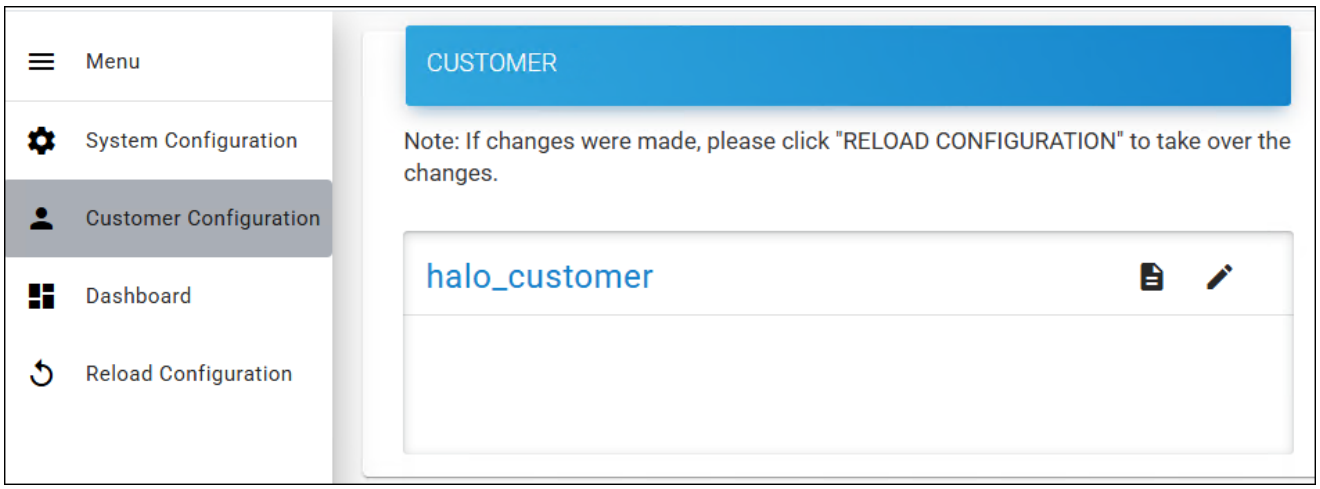
Restart the HaloENGINE Tomcat service after completing all necessary certificate-related changes.

6.6.6. Phase 2. Activate License (First time)

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

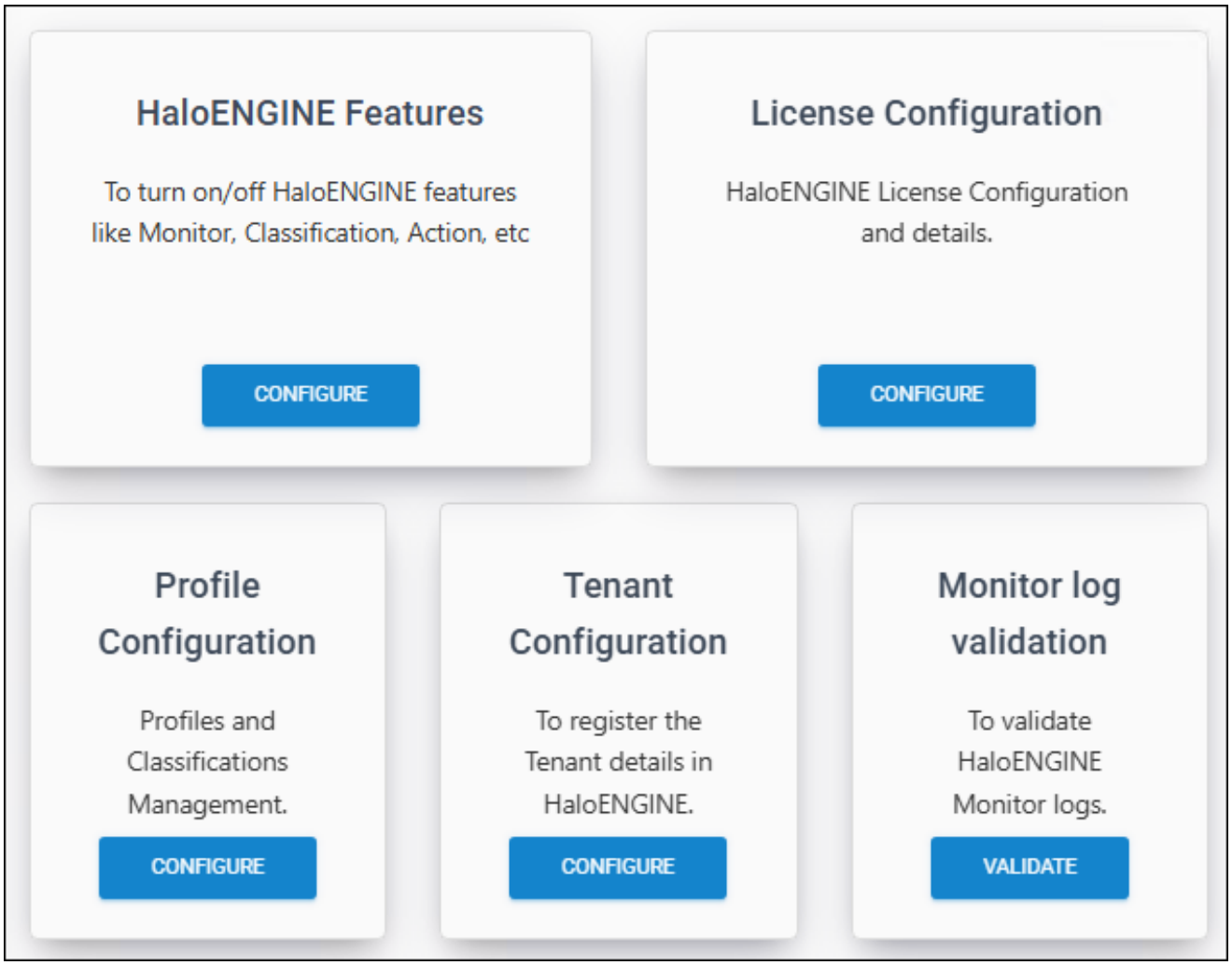
To activate the license, follow the steps outlined below:

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



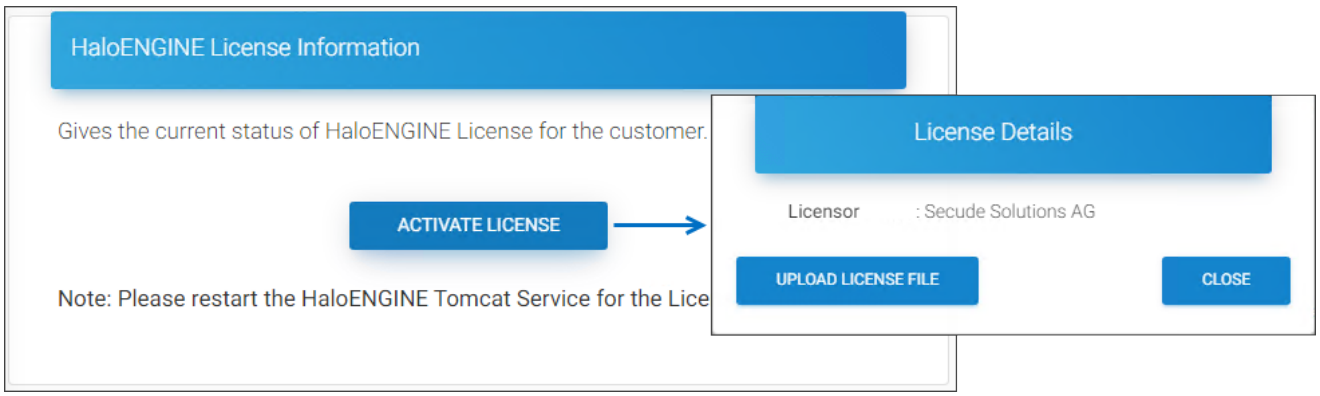
Customer ID page

2. The default customer name is halo_customer, but you can modify it if required.



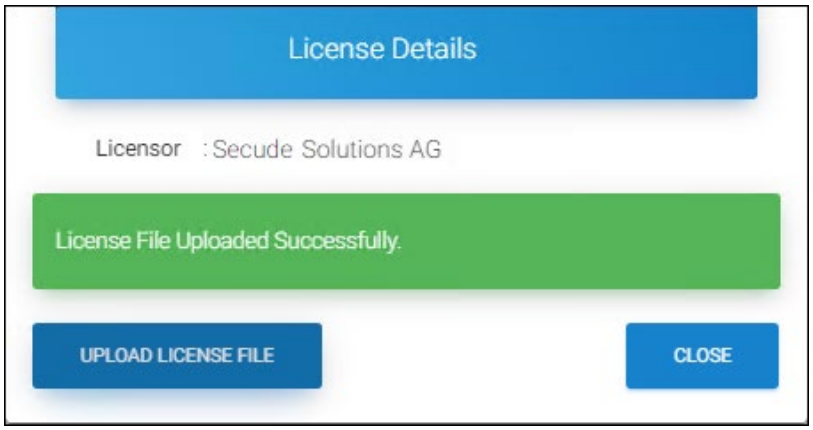
Customer configuration page

3. On the **License Configuration** tab, click **Configure**.
4. The *HaloENGINE License Information* page appears as shown in the figure below:



License activation page #1

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



License activation page #2

6. Select the `license.lic` file from the **Open** dialog box.

   Results:

   a. A confirmation message appears after the file is uploaded successfully.

   b. Click **Close** to exit the dialog box.

   What to do next:

   a. Restart the HaloENGINE Tomcat Service for the license file changes to take effect.

   b. Log in to the Admin Portal and follow the steps below to view or renew the license details.

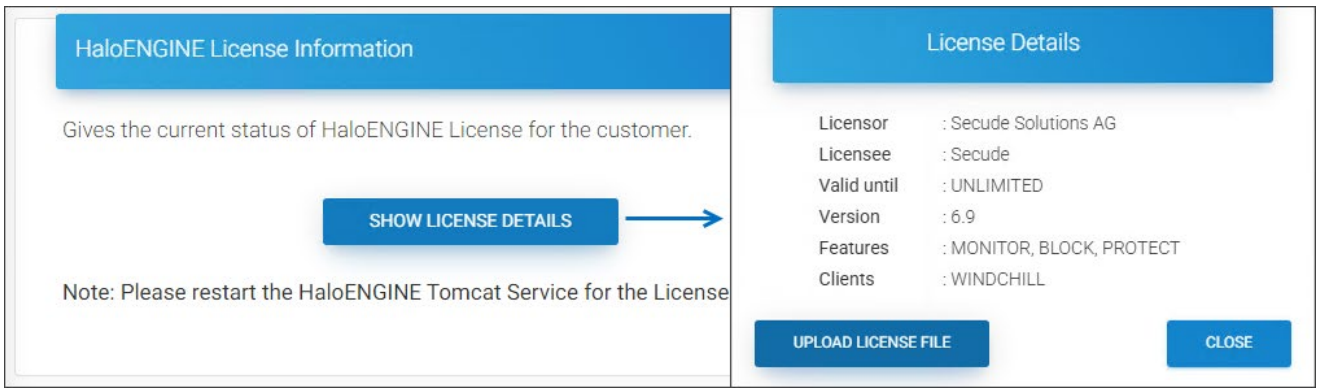
Check License Details / Renew License

This page is also useful for the following purposes:

1. To verify license information, such as validity and activated features.
2. If the current license has expired, renew it through Secude and update it.

To check the license details:

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



Renew/check license dialog

Results: The license details will be displayed.

2. Click **Close** to exit the dialog box.
3. Restart the HaloENGINE Tomcat Service for the configuration changes to take effect.

To renew the license:

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

Results:

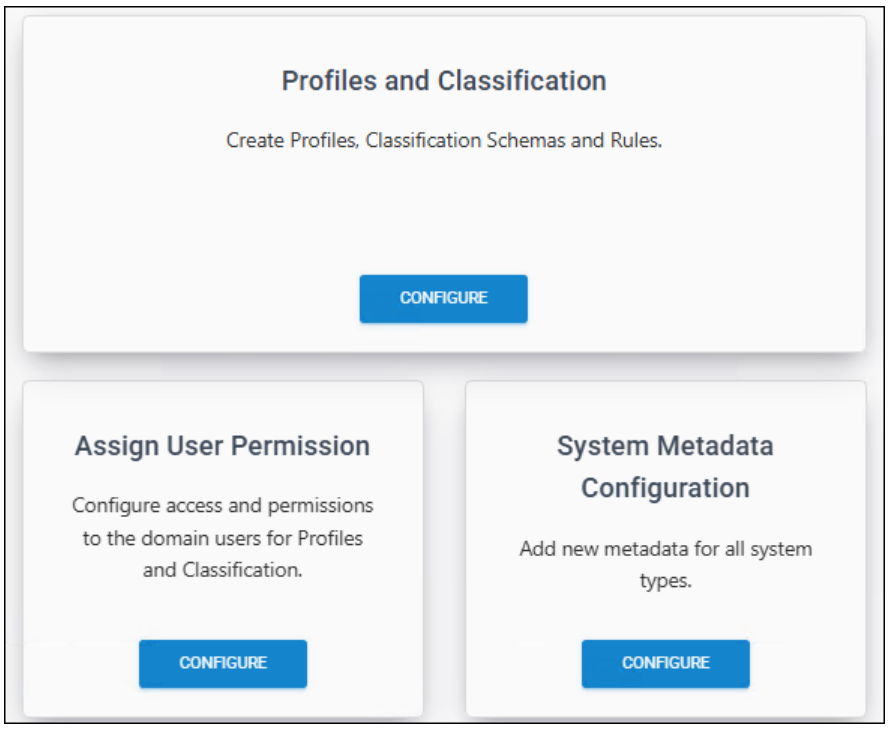
1. A confirmation message appears after the file is uploaded successfully.
2. Click **Close** to exit the dialog box.

6.6.7. Phase 3. Configure Profiles and Classification

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

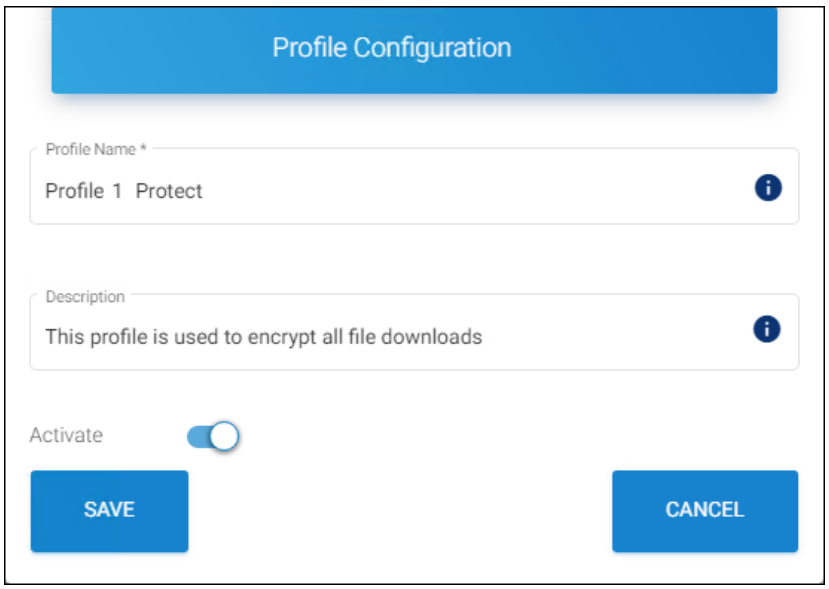
Follow the procedure below to configure the Profile:

1. On the left navigation bar, click **Customer Configuration**, and then select the customer ID (halo_customer) from the list.
2. On the **Profile Configuration** tab, click **Configure**. The following page appears, as shown in the figure below:



Profile Configuration page #1

3. On the **Profiles and Classification** tab, click **Configure**.
4. Upon opening, the Classification Profiles page appears empty, with no profiles added.
5. Click the plus icon, and then enter the following details:



Profile Configuration page #2

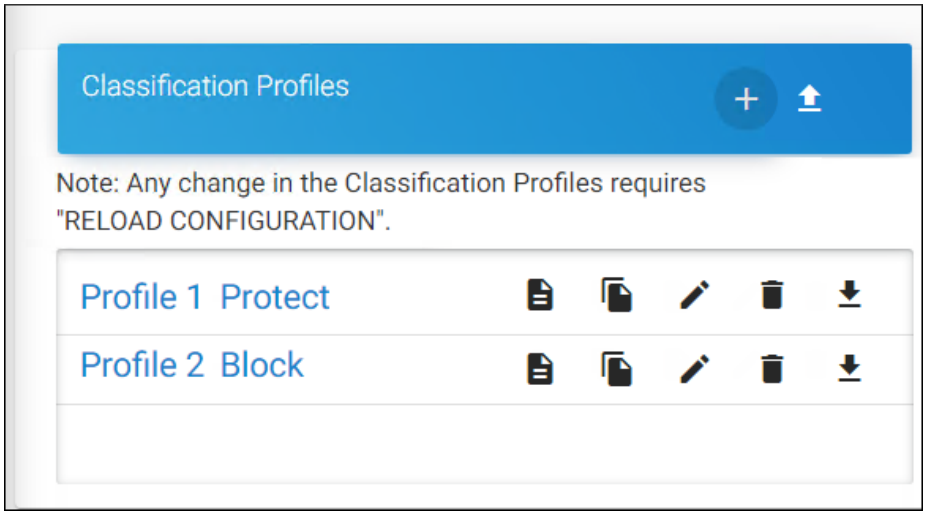
6. **Profile Name** – Enter a name for the new profile. Note: A profile name cannot contain any of the following characters "< >: " / \ |? * ` ~" and can contain “- _"
7. **Description** – Enter a description for the new profile (optional).
8. **Activate** – The current profile is automatically enabled by default. However, you can deactivate it by clicking the **Activate** slider button.

9. Click **Save**.
10. Repeat the above steps to create multiple profiles.

    Results:

    a. A confirmation message appears after the profile is saved successfully.

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



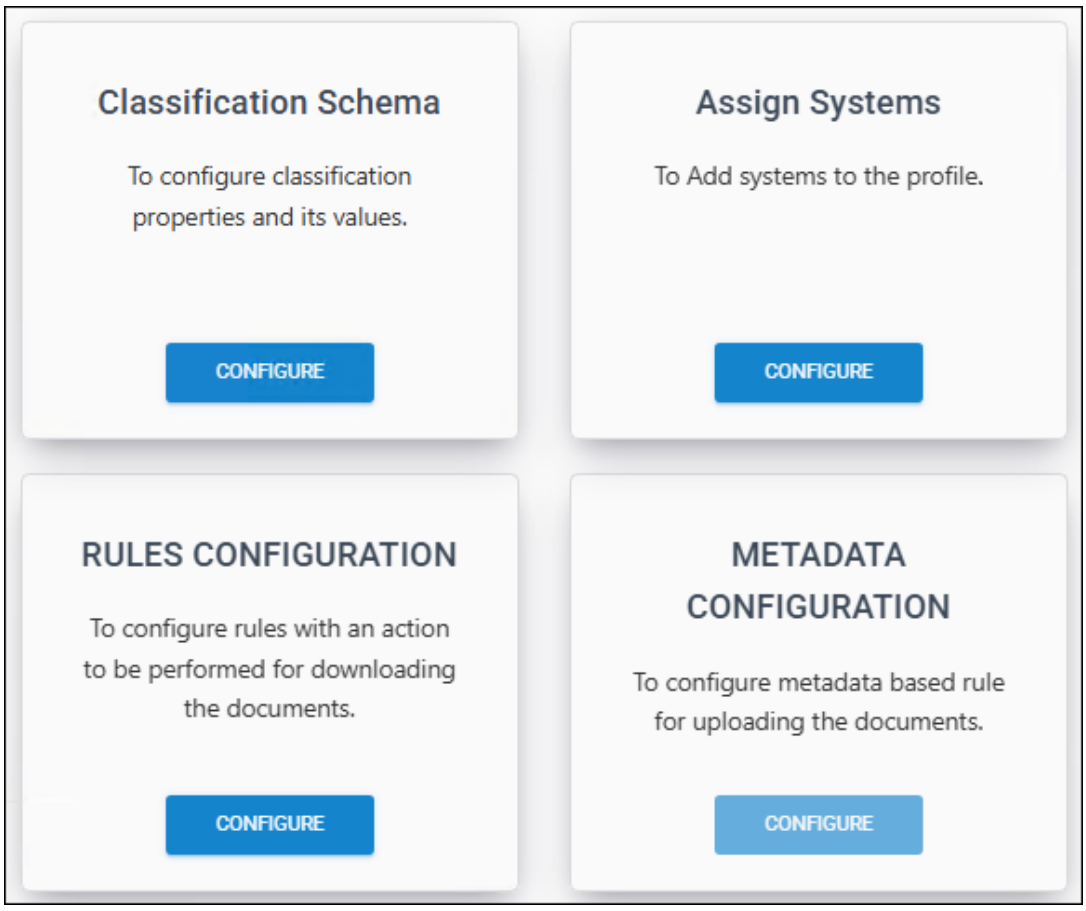
Profile list

Related tasks

1. You can manage Classification Profiles using the Copy, Edit, Delete, Download, and Import icons.
2. To view the details of a profile, click the Profile Details icon.
3. To export a profile configuration, click the **Download** icon. To reuse the profile in another HaloENGINE environment, click the **Import Profile** icon in the upper-right corner and attach the downloaded `Profile.zip` file.

What to do next:

1. Click **Reload Configuration** to apply the changes.
2. Select a classification profile from the displayed list. The **Classification Configuration** page appears, as shown in the figure below:



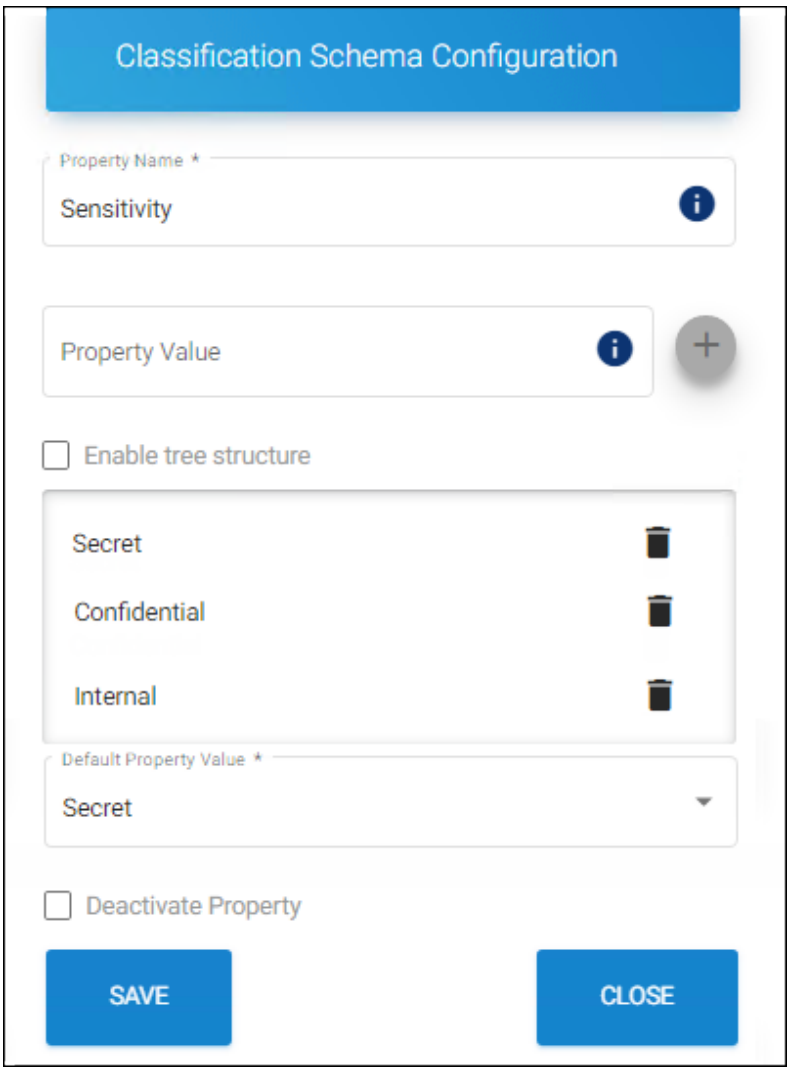
Classification Configuration

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

6.6.7.1. Create Classification Schema

The classification schema contains properties and their values.

1. On the **Classification Schema** tab, click **Configure**. Upon opening, the **Classification Schema** page appears empty, with no schemas added.
2. Click 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. A confirmation message appears after the **Classification Schema** is saved successfully.

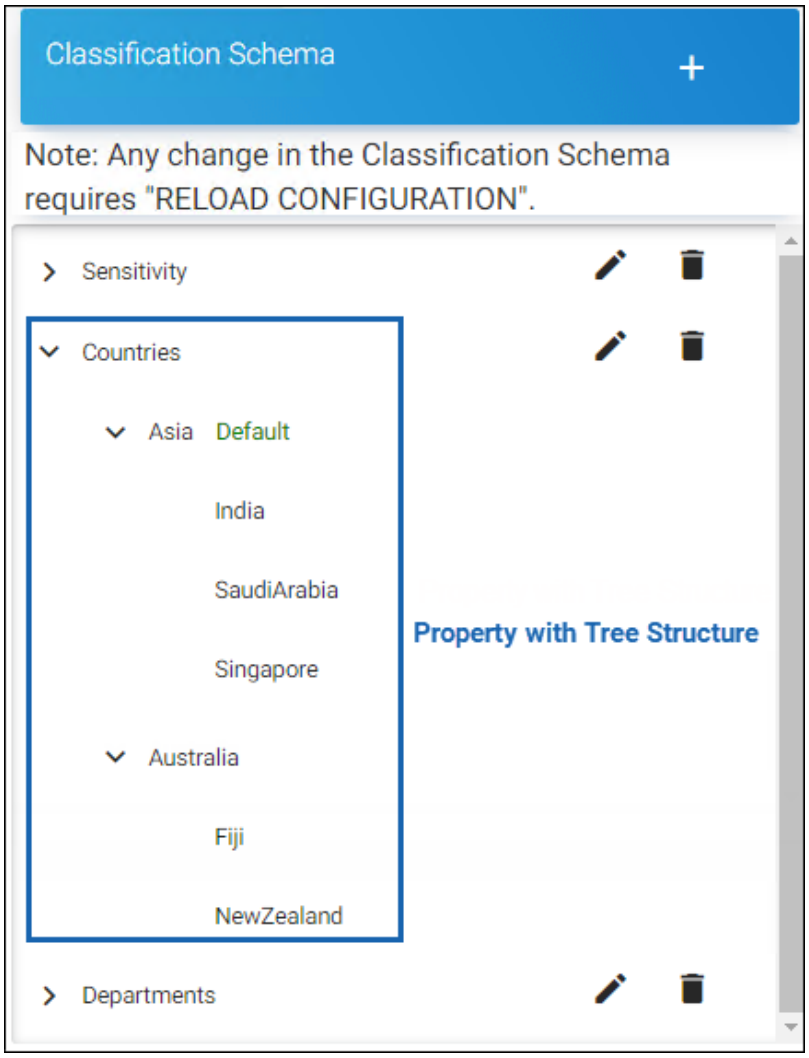
   b. The property name and its values are added as a node.

   c. Similarly, you can add schemas by clicking the plus icon.

6. **Enable tree structure**: To have a tree structure view of information, where each item can have multiple children, select the Property Value (e.g., Asia) and enter a value in the property value field

(e.g., India), and then select the **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 exit the page.



Classification Schema list

8. Click Reload Configuration to apply the changes.

Related tasks

1. By default, the current property is activated. You can deactivate it by selecting the **Deactivate Property** check box.
2. You can manage classification profiles using the Edit and Delete icons.

6.6.7.2. Create Download Classification Rules

Download rules define classification rules based on metadata types and Pre-Expression, while Action rules determine whether a file is blocked, protected, or excluded during download.

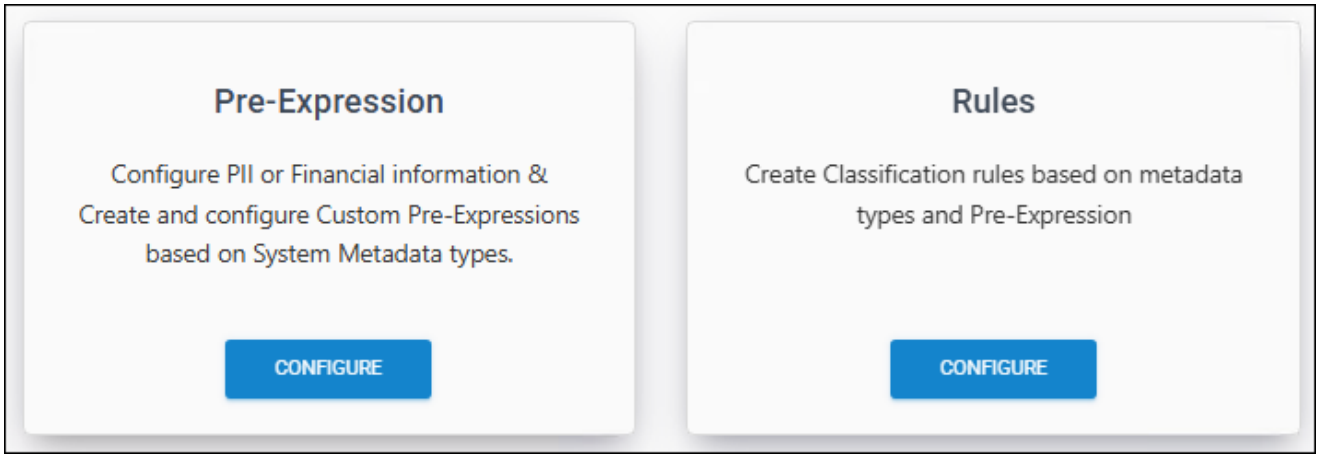
6.6.7.2.1. Custom Pre-Expression

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 such as Windchill, Teamcenter, Keytech, Autodesk_Vault, SOLIDWORKS_PDM, and HaloENGINE_API.

1. Navigate to the **Profile Configuration** tab and click **Configure** > go to the **Profiles and Classification** tab and click **Configure** > select a classification profile > on the **Rules Configuration** tab, click **Configure**. The following page appears, as shown in the figure below:

Download rules configuration page

2. On the **Classification Rules** tab, click **Configure**, and the following page appears, as shown in the figure below:

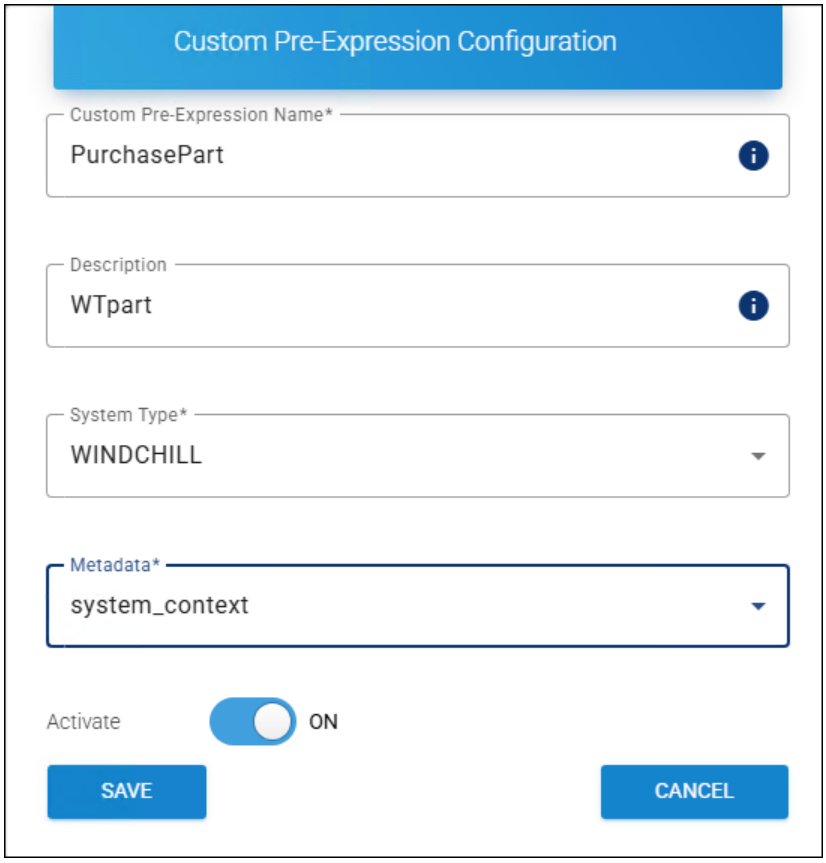


Classification rules page

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

Pre-Expression Configuration

4. On the **Pre-Expression Configuration** page, click **Custom Pre-Expression**. Upon opening, the Custom Pre-Expression page appears empty, with no pre-expressions added.
5. Click the plus icon and enter the following details:



Custom Pre-Expression #1

6. **Custom Pre-Expression Name** – Enter a name for the new custom pre-expression entry. Note: only '**alphabet**', '**numbers**', '_', and '**-**' characters are supported.
7. **Description** – Enter a description of the new custom pre-expression (optional).
8. **System Type** – Based on your license, your system type will be displayed by default.

9. **Metadata** – Select a metadata from the list.
10. **Activate** – The current Custom Pre-Expression is automatically enabled by default. However, you can deactivate it by clicking the **Activate** slider button.
11. Click **Save**.

    Results:

    a. A confirmation message appears after the **Custom Pre-Expression** is added.

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

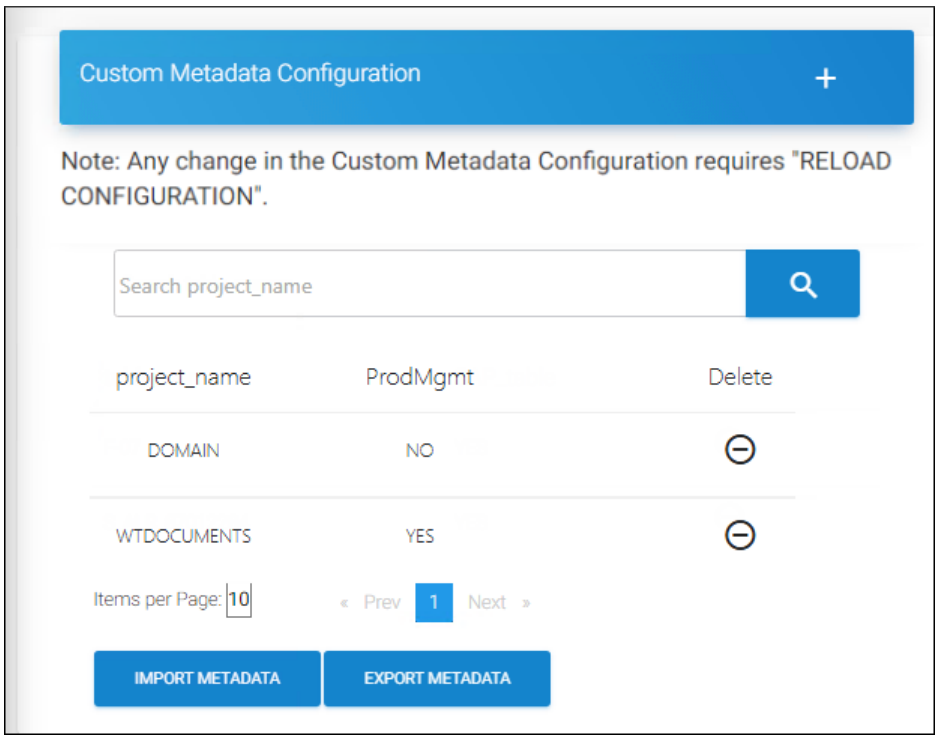
    c. Click **Reload Configuration** to apply the changes.

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

1. Autodesk Vault – HaloCAD for Autodesk Vault Installation Manual
2. Teamcenter – HaloCAD for Teamcenter Installation Manual
3. Windchill – HaloCAD for Windchill Installation Manual
4. SOLIDWORKS PDM – HaloCAD for SOLIDWORKS PDM Installation Manual
5. Keytech – HaloCAD for Keytech Installation Manual
6. HaloENGINE API – Since there is no built-in metadata for the REST SDK, 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 appears, as shown in the figure below. For illustration, a new custom pre-expression "DOMAIN" is added to the list.



Custom Pre-Expression #2

2. Click the plus icon. The **Add Custom Metadata Values** dialog appears.
3. 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**.

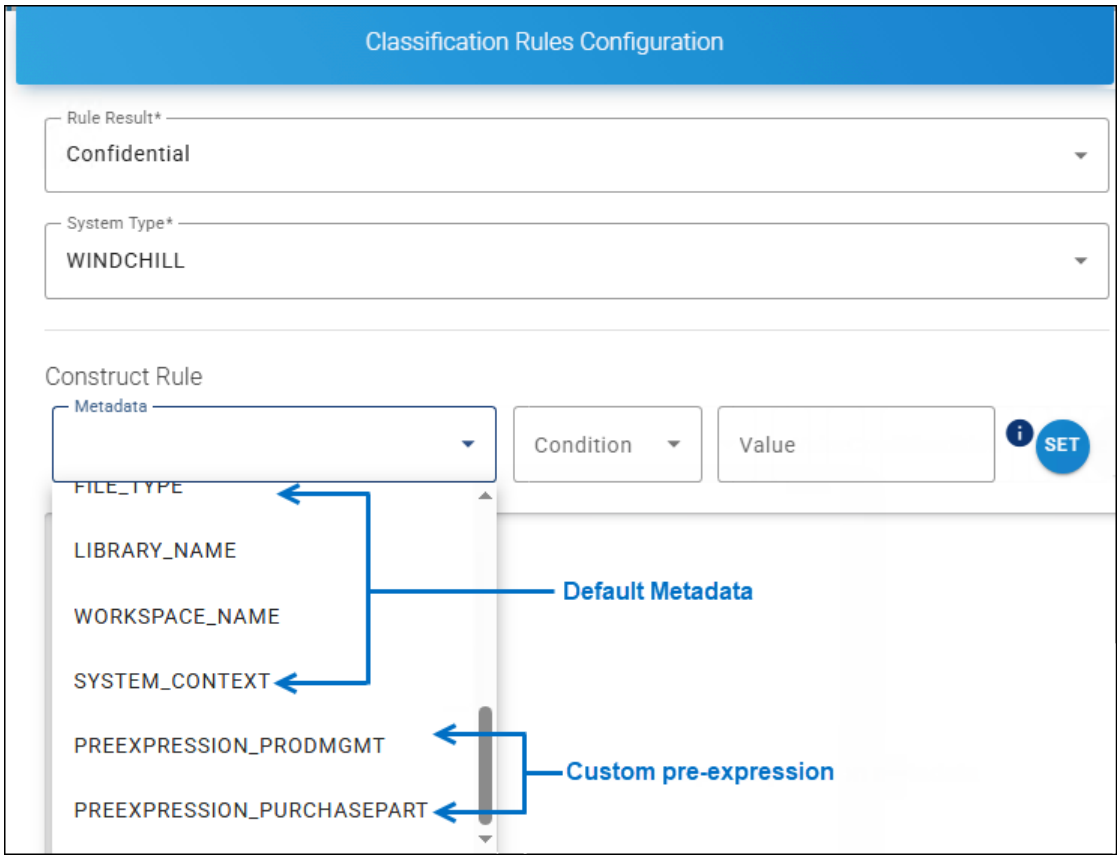
Results:

a. A confirmation message appears after the **Custom Metadata** is saved.
b. The new metadata value is added to the list.
c. Click Reload Configuration to apply the changes.

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 example below:



Example for Custom Pre-Expression #3

5. You can manage Custom Pre-Expressions using the Edit or Delete icons.

6.6.7.2.2. Custom Metadata

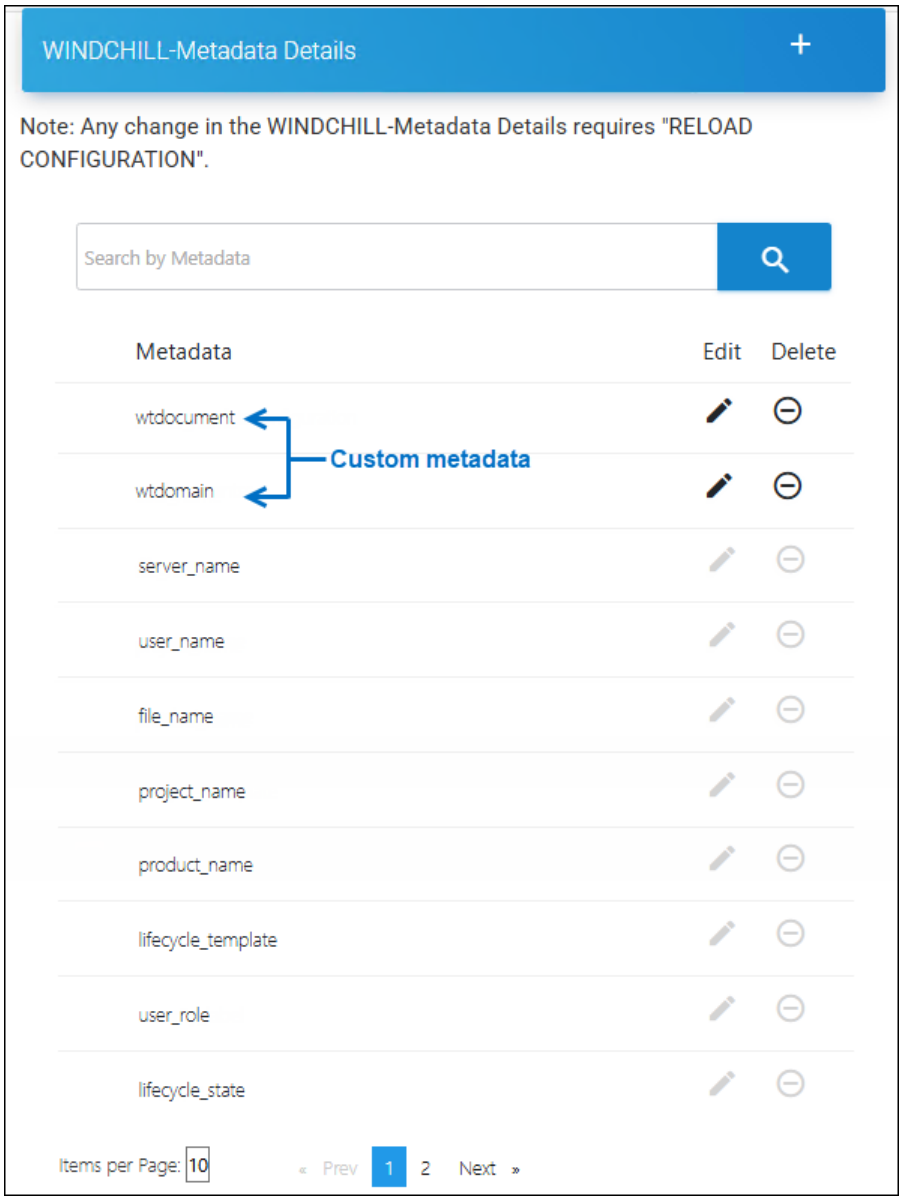
For data classification and secure file downloads, the HaloENGINE Admin Portal uses the default metadata. However, depending on organizational requirements, the portal allows administrators to add custom metadata.

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 procedure below to create custom metadata for System types:

1. On the left navigation bar, click **Customer Configuration**, and then select the customer ID (halo_customer) from the list.
2. Navigate to the **Profile Configuration** tab and click **Configure** > go to the **System Metadata Configuration** tab and click **Configure**.

3. Click the System Type to which you want to add the custom metadata. In this example, the WINDCHILL System Type is selected.
4. Click the plus icon. The **Add Custom Metadata** dialog appears.
5. Enter a name and click **Save**.



Metadata details page

Results:

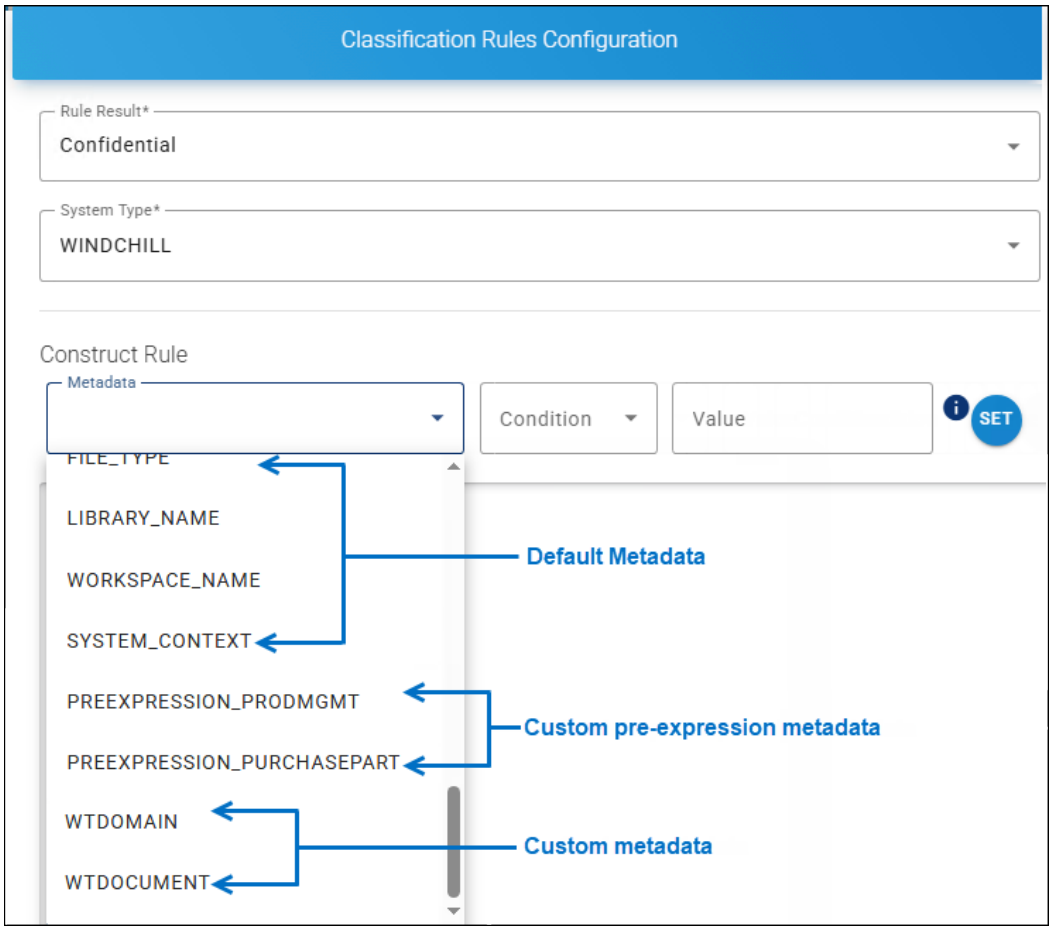
a. A confirmation message appears after the **Custom Metadata** is saved.

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

c. Click **Reload Configuration** to apply the changes.

Related tasks

1. If you want to edit/remove 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 example below:



Example for Custom Metadata

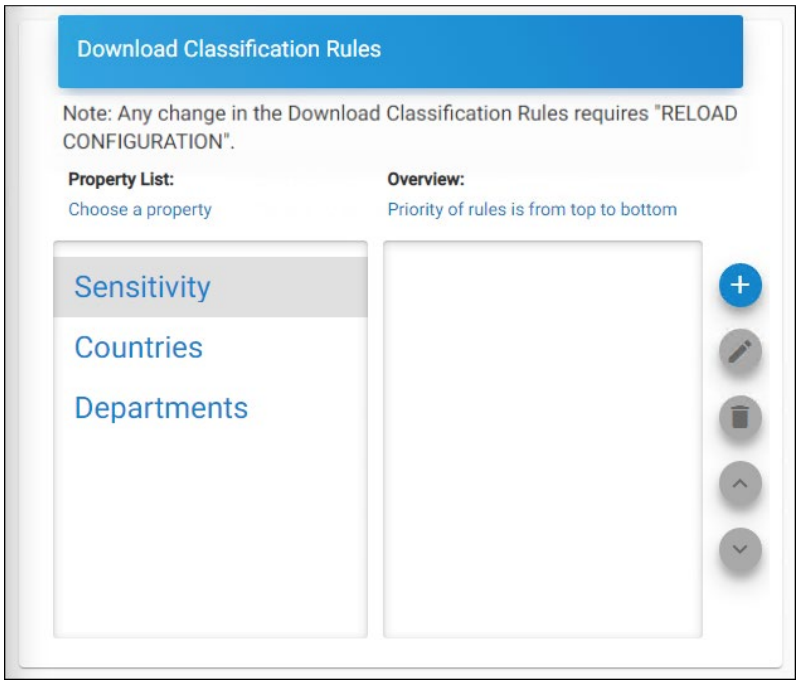
6.6.7.2.3. Create Download Rules

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.

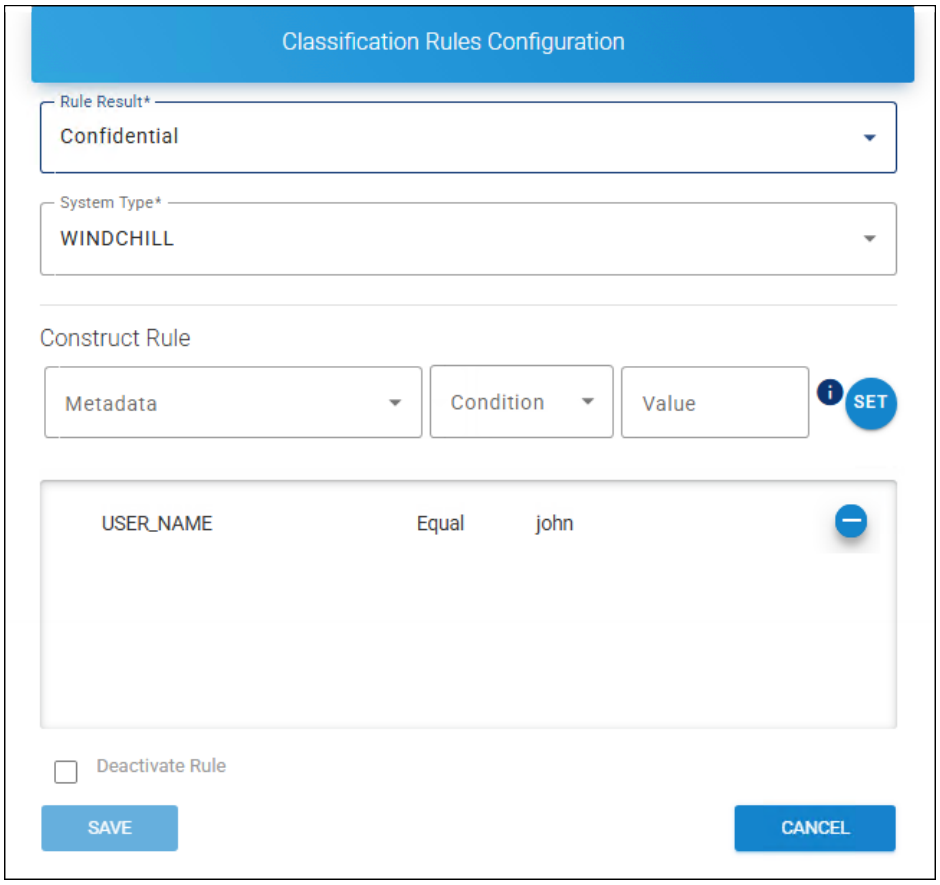
1. Navigate to the **Profile Configuration** tab and click **Configure** > go to the **Profiles and Classification** tab and click **Configure** > select a classification profile > on the **Rules Configuration** tab, click **Configure** > on the **Classification Rules** tab, click **Configure** > finally, click the **Rules** tab and then **Configure**.

2. Upon opening, the *Download Classification Rules* page appears empty, with no rules added.



Download classification rules page

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

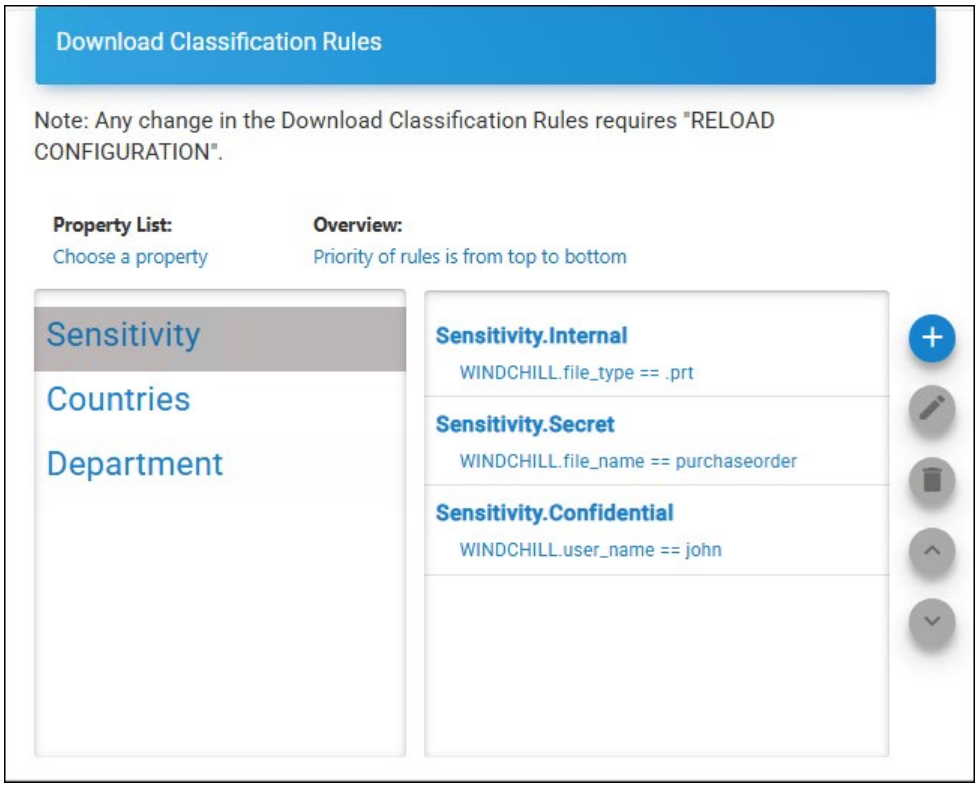


Classification rules configuration

5. Enter the values for the following:
   a. **Rule Result** – Select a value from the list.
   b. **System Type** – 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 are added to the list.
8. Click **Save**.

Results:

1. A confirmation message appears 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

3. Click **Reload Configuration** to apply the changes.

Related tasks

1. By default, the current rule is activated. However, you can disable it by selecting the **Deactivate Rule** checkbox.
2. To adjust a rule's priority, select the rule and click the corresponding **Up Arrow** or **Down Arrow** icon.

3. To undo the priority changes, click the **Restore Priority Changes** icon.
4. To save the updated priority order, click the **Save Priority Changes** icon.

Reference Manuals:

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

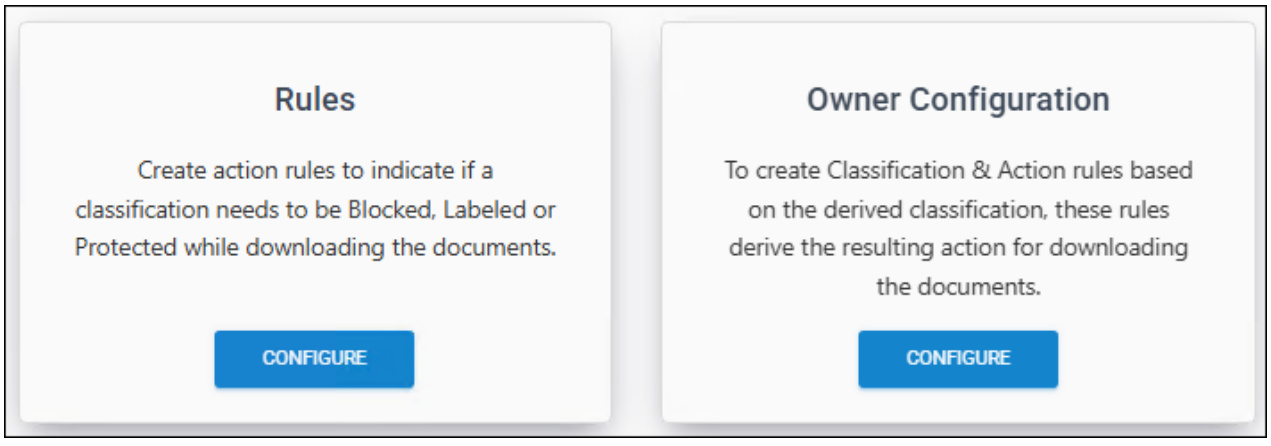
1. Autodesk Vault – HaloCAD for Autodesk Vault Installation Manual
2. Teamcenter – HaloCAD for Teamcenter Installation Manual
3. Windchill – HaloCAD for Windchill Installation Manual
4. SOLIDWORKS PDM – HaloCAD for SOLIDWORKS PDM Installation Manual
5. Keytech – HaloCAD for Keytech Installation Manual
6. HaloENGINE API – Since there is no built-in metadata for the REST SDK, custom metadata can be used to generate new metadata for the HaloENGINE API system type. Please refer to the section "Custom Metadata".

6.6.7.2.4. Add Action Rules

Action rules define the conditions under which a file download is blocked, protected, or excluded.

Follow the procedure below to add Action Rules:

1. Navigate to the **Profile Configuration** tab and click **Configure** > go to the **Profiles and Classification** tab and click **Configure** > select a classification profile > on the **Rules Configuration** tab, click **Configure** > under **Action Rules**, click **Configure**. The following page appears as shown below:

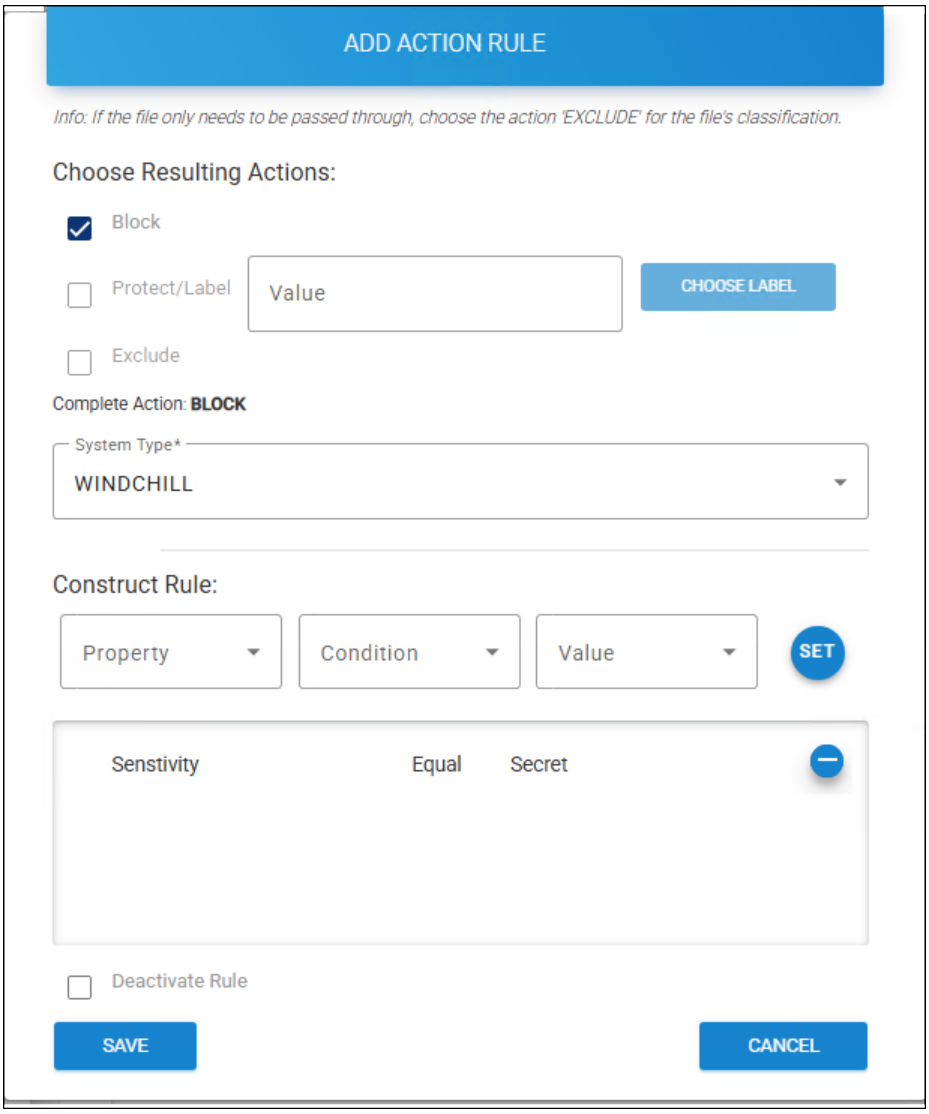


Action Rules

2. On the **Rules** tab, click **Configure**. When opened, the **Action Rules for Download** page appears empty, with no action rules added.
3. Click the plus icon. The *Add Action Rule* page appears.

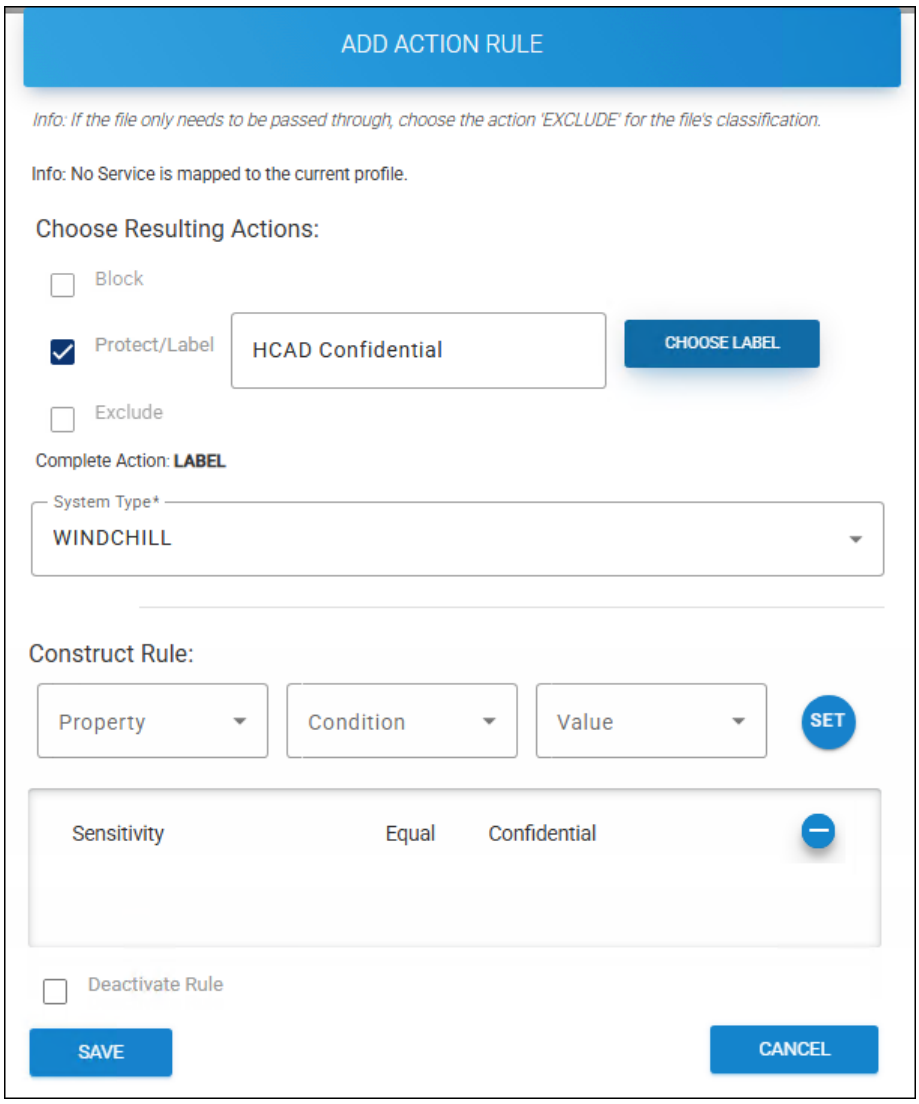
4. Under **Choose Resulting Actions**, select any one of the actions. Please note that you can select only one action at a time: Block, Label, or Exclude.

   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. Proceed to point 6.



Action rule for protection

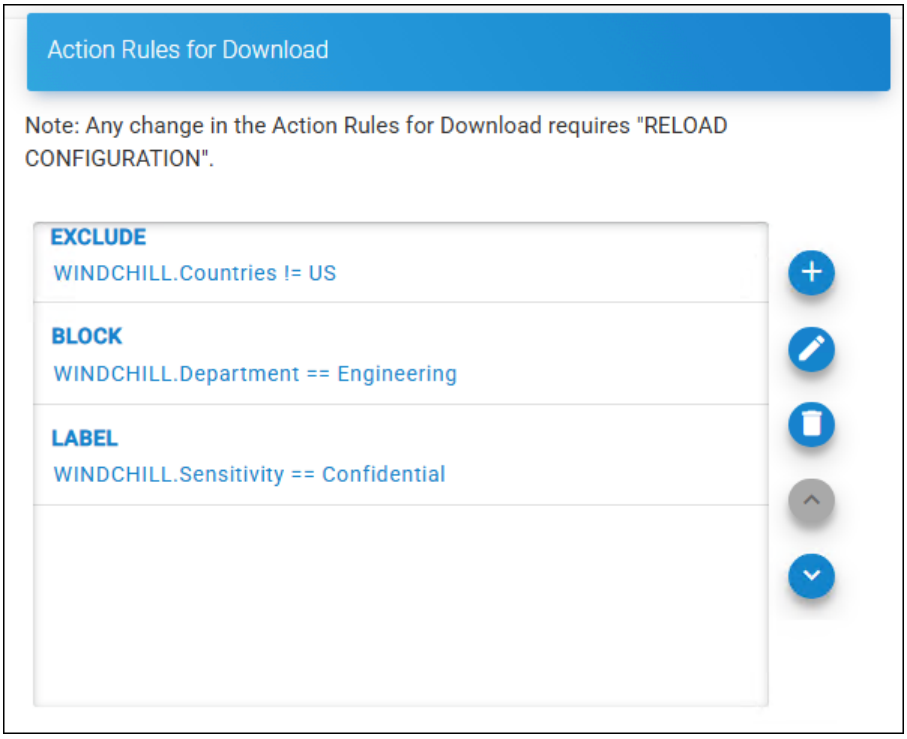
c. **Exclude** – Allows suppressing actions such as monitor, block, label, or protect during a file download by selecting the **Exclude** action based on the configured metadata or Pre-expression. If selected, other options will be disabled. Proceed to point 6.

5. **System Type**– Based on your license, your system type will be displayed by default.
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** – If you want to deactivate a rule, select **Deactivate Rule** check box.
7. Click **Set** to configure the rule. The selected property and its condition are added to the list.
8. Click **Save**.

Results:

a. A confirmation message appears after adding or updating the action rule.

b. The rule is added to the list.



List of action rules

c. Click **Reload Configuration** to apply the changes.

Related tasks

1. You can manage the **Action Rule** using the **Edit** and **Delete** icons.
2. To increase or decrease the priority of a rule, select the rule and click the corresponding **Up Arrow** or **Down Arrow** icon.
3. To reverse any priority changes, click the **Restore Priority Changes** icon.
4. To save your priority changes, click the **Save Priority Changes** icon.

Action Rule priorities

When multiple classification rules exist, the HaloENGINE prioritizes them from top to bottom. For example, consider **Rule 1**, **Rule 2**, **Rule 3**, and **Rule 4** in the Classification Engine.

1. The Classification Engine evaluates 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 performs further verification.
3. This process continues until a correct classification expression is found or no rules apply.

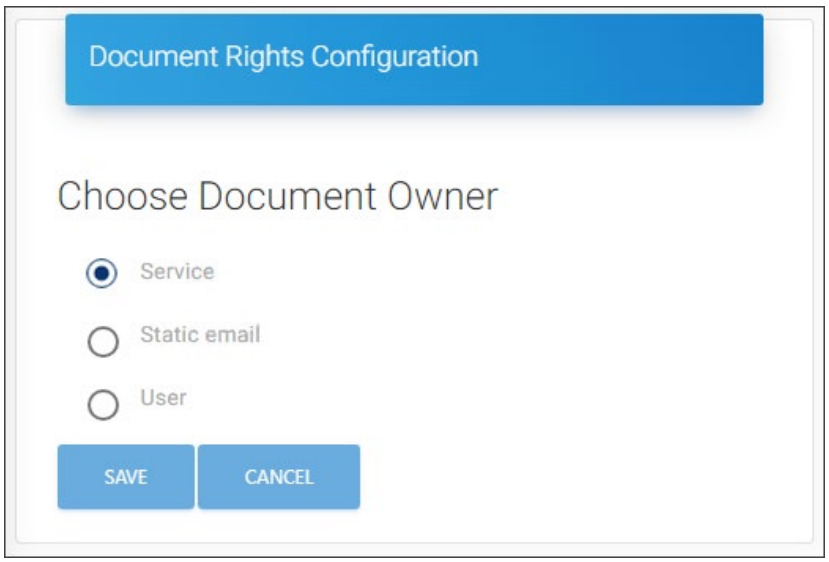
Owner Configuration (Optional)

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

Supported client systems: Teamcenter, Windchill, Autodesk_Vault, and Keytech systems.
Owner configuration does not apply to the SOLIDWORKS PDM client, as protection is managed by HaloCAD for SOLIDWORKS PDM.

Follow the steps below to configure owner rights:

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



Owner rights

3. Select one of the following three options:
   a. **Service** (default) – The Application ID used to initialize the HaloENGINE Tomcat Service becomes the owner of the document.
   b. **Static email** – The email address entered in the text box is considered the owner of the document.
   c. **User** – The mail address is derived from the client system, such as Windchill, Teamcenter, Keytech, Autodesk_Vault, or HaloENGINE_API.
4. Click **Save** to save the rule.
   Results: A confirmation message appears after updating the assigned rights.

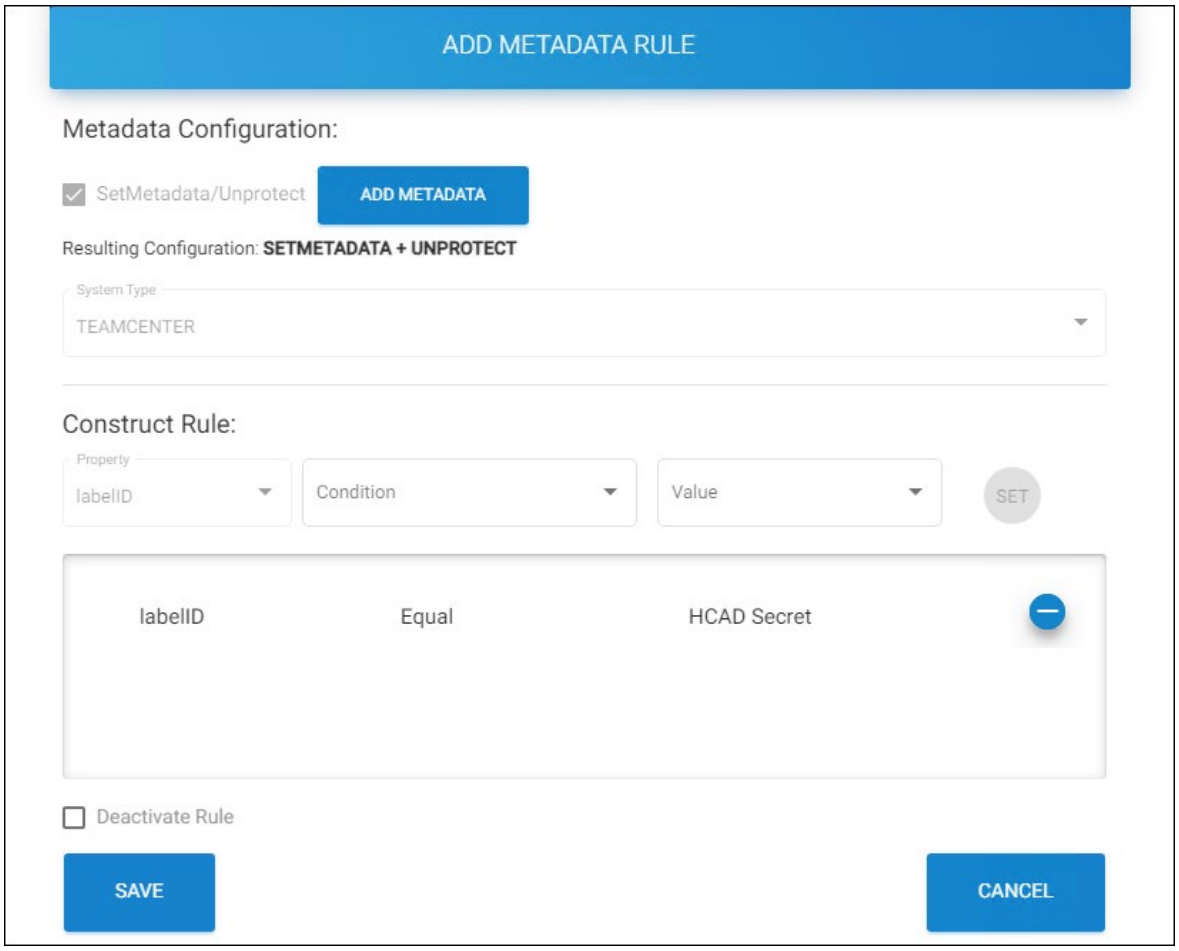
6.6.7.3. Metadata Configuration

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.

Prerequisite: Ensure that the Classification Schema is available.

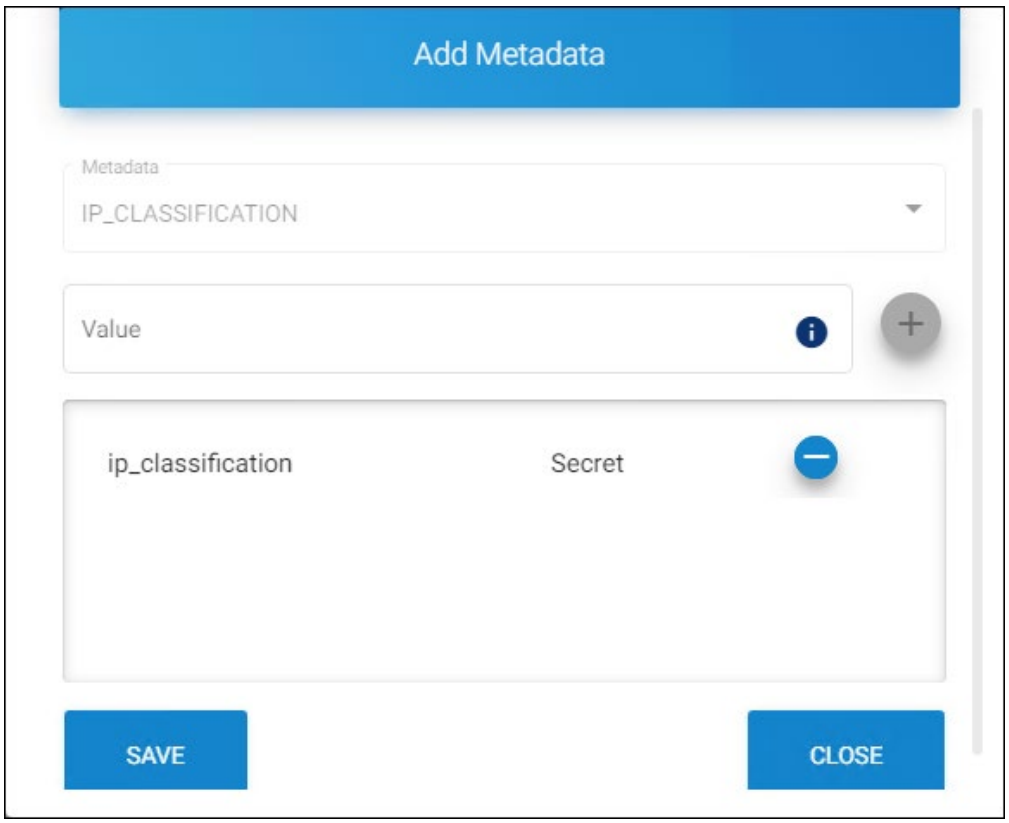
Follow the steps below to configure metadata:

1. Navigate to the **Profile Configuration** tab and click **Configure** > go to the **Profiles and Classification** tab and click **Configure** > select a classification profile > go to the **Metadata Configuration** tab and click **Configure**.
2. Upon opening, the *Add Metadata Rule* page appears empty, with no metadata rules added.



Add metadata rule

3. By default, the **SetMetadata/Unprotect** option is selected.
4. Click **ADD METADATA**.
5. The *Add Metadata* page appears, 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 the 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:

   a. A confirmation message appears after adding or updating the rule.

   b. Click **Reload Configuration** to apply the changes.

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

Profile Configuration							
System Types	**Download Rules (default)**	**PII and Fin. Info.**	**Cust. Pre-Exp.**	**Owner Config.**	**Metadata Config.**	**Sys. Metadata Config.**	**Auth./Comm. Endpoint**
Teamcenter	Yes	N/A	Opt.	Opt.	Opt.	Opt.	Mutual
Autodesk_Vault	Yes	N/A	Opt.	Opt.	N/A	Opt.	Mutual
Windchill	Yes	N/A	Opt.	Opt.	N/A	Opt.	Mutual
Keytech	Yes	N/A	Opt.	Opt.	N/A	Opt.	Mutual
SOLIDWORKS PDM	Yes	N/A	Opt.	N/A	N/A	Opt.	Supports mutual and server-side
HaloENGINE_API	Yes	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. Yes - applicable by default
2. N/A - Not Applicable
3. Opt. - Optional
4. Fin. Info. - Finance Information
5. Cust. Pre-Exp. - Custom Pre-Expression
6. Owner Config. - Owner Configuration
7. Metadata Config. - Metadata Configuration (Profile Configuration > Profile Classification > Classification Configuration > METADATA CONFIGURATION)
8. Sys. Metadata Config. - System Metadata Configuration (Profile Configuration > System Metadata Configuration)

9. Auth. - Authentication
10. Comm. - Communication

6.6.7.4. 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,

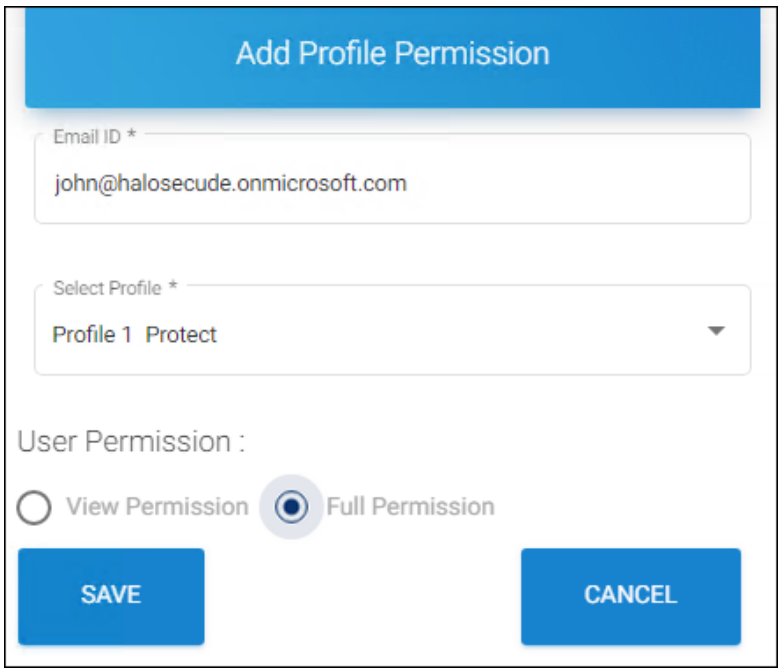
1. User 1 - assigned with full rights as an admin user. So he could access the entire portal without any limitations.
2. User 2 - assigned with read-only access. This user can view the configuration of a particular profile, but is restricted to changing the settings.
3. User 3 - assigned with write access.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

1. Navigate to the **Profile Configuration** tab and click **Configure** > go to the **Assign User Permission** tab and click **Configure**.
2. Upon opening, the *User-Profile Permission* page appears empty, with no profiles added.
3. Click the plus icon and enter the following details:



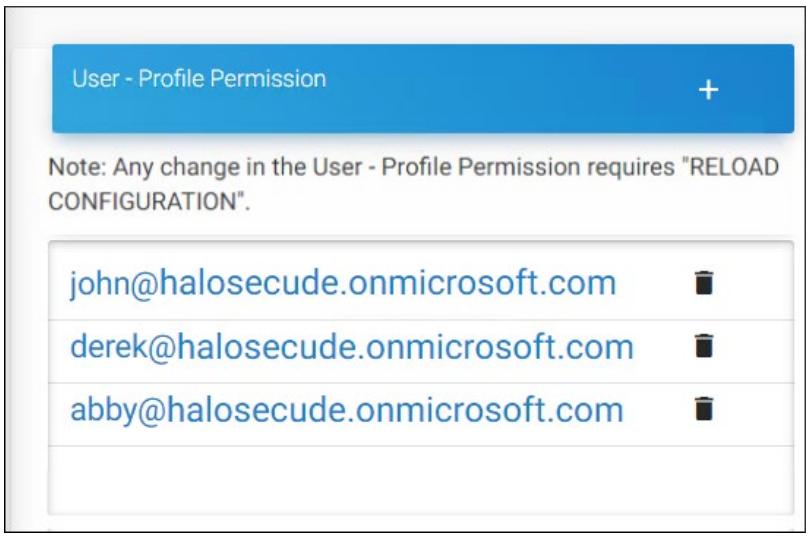
Adding a user page

4. **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".
5. **Select Profile** - Select a profile from the list.
6. **User Permission** - Select either View Permission or Full Permission for the user.
7. Click **Save**.

   Results:

   a. A confirmation message appears after adding the user permission.

   b. The email ID is added to the list, as shown in the figure below:



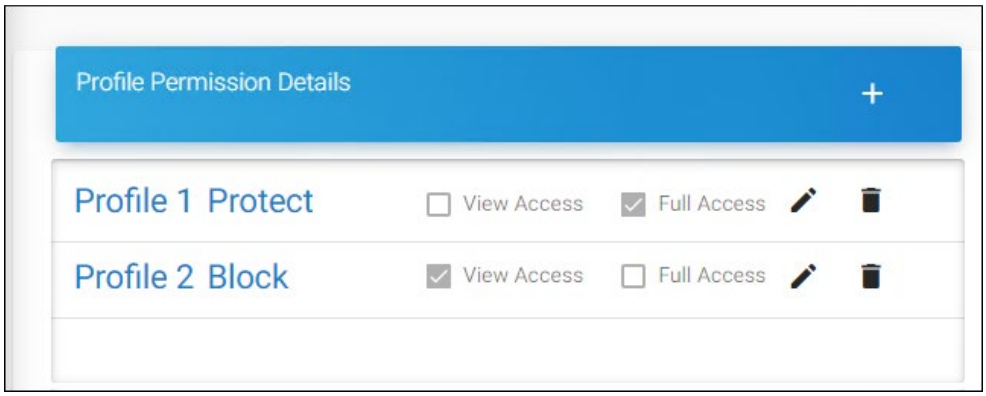
User profile permission #1

c. Click **Reload Configuration** to apply the changes.

Related tasks

To know the details of a user.

1. Click on the user's email ID. The *Profile Permission Details* page appears as shown in the figure below:



User profile permission #2

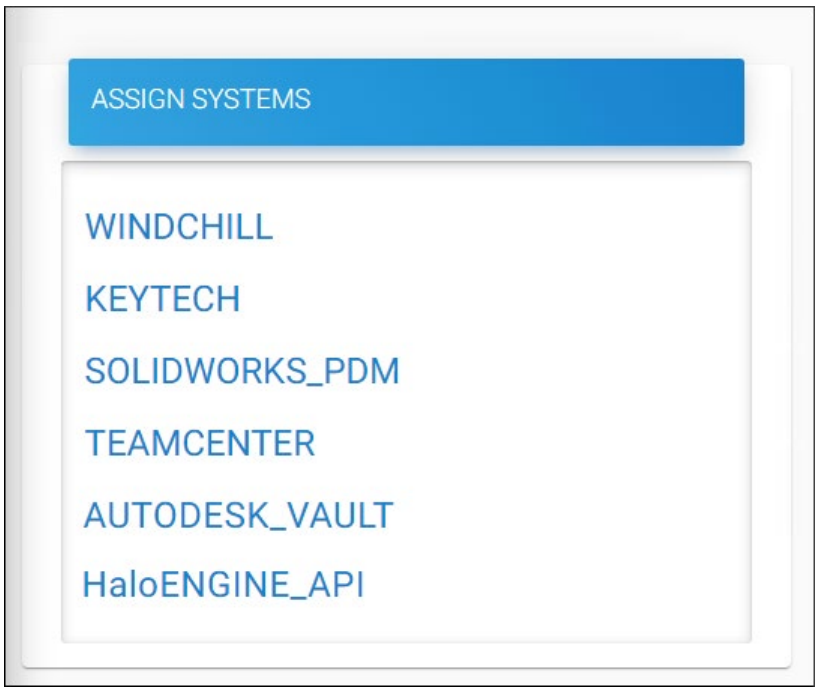
2. You can manage the permission using the **Edit** and **Delete** icons.

6.6.8. Phase 4. 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.

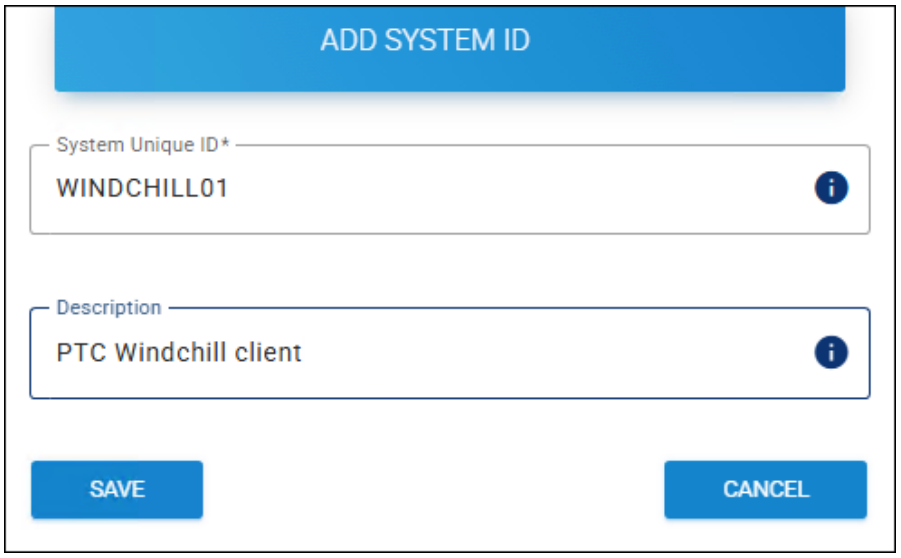
Follow the procedure below to add a system type:

1. On the left navigation bar, click **Customer Configuration**, and then select the customer ID (halo_customer) from the list.
2. Navigate to the **Profile Configuration** tab and click **Configure** > go to the **Profiles and Classification** tab and click **Configure** > select a classification profile > go to the **Assign Systems** tab and click **Configure**.
3. Upon opening, the **Assign Systems** page appears with the licensed system types.
4. 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

5. Select a system type and click the plus icon to add the corresponding system type details.
6. Enter the following details on the *Add System ID* page. For illustration, the Windchill system is selected.



Assign systems page #2

7. **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".
8. **Description** – Enter a description (optional).
9. Click **Save**. Repeat the same steps for other systems.

   Results:

a. A confirmation message appears after adding or updating the system ID.

b. Click **Reload Configuration** to apply the changes.

Related tasks

1. You can manage the systems using the **Edit** and **Delete** icons.
2. You can view system details by clicking the **Assign System Details** icon.
3. After making changes to the classification engine, click **Reload Configuration** to apply the changes. The page will redirect to the login page once the reload completes.
4. Note: 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.

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

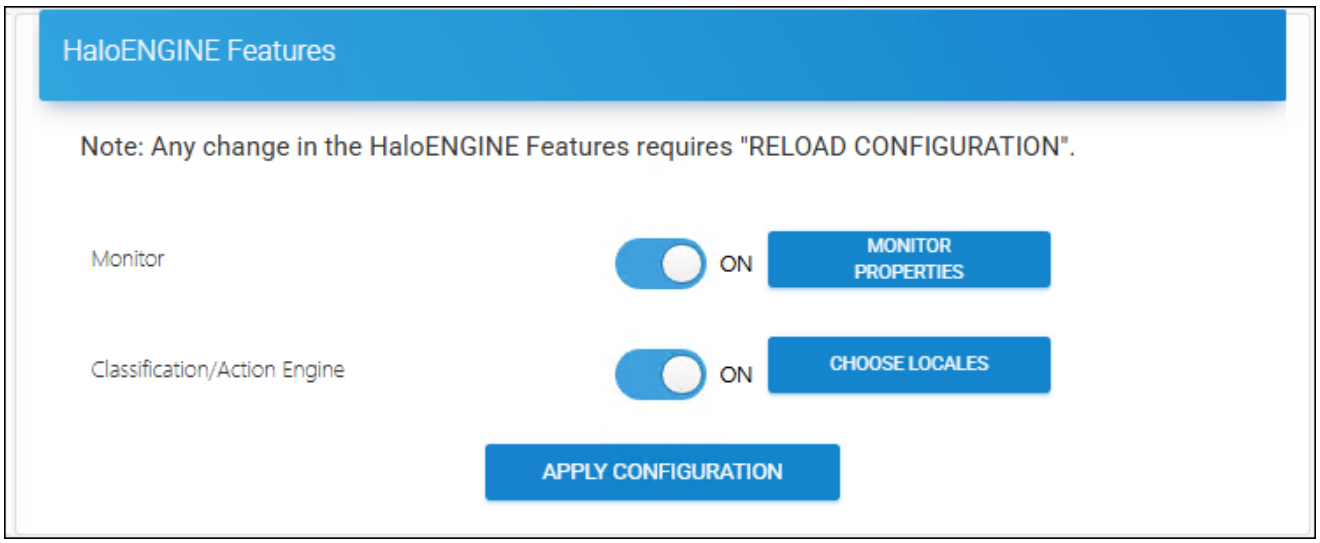
For example, if you set the System Unique ID to **RESTclient** (System ID=RESTclient), the same ID must be used when calling the APIs.

6.6.9. Phase 5. 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 2. Activate License (First time)".

1. On the left navigation bar, click **Customer Configuration**, and then select the customer ID (halo_customer) from the list.
2. On the **HaloENGINE Features** tab, click **Configure**. The *HaloENGINE Features* page appears 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. A confirmation message appears after changing the default configuration.

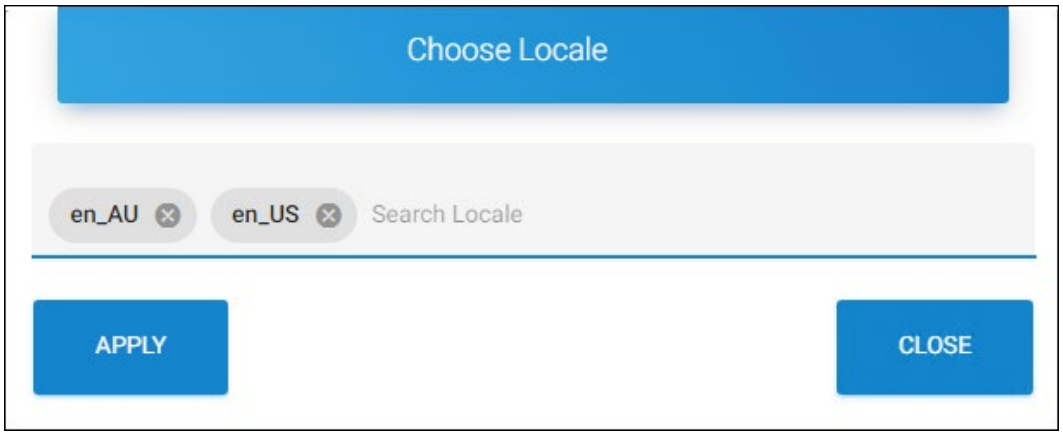
   b. Click **Reload Configuration** to make the changes take effect.

6.6.9.1. Enable Classification/Action Engine

Follow the steps below to enable the classification engine:

1. Click the slider button to enable or disable the **Classification/Action Engine**.
2. The **Choose Locales** button is enabled automatically.

3. Click **Choose Locales**. The **Choose Locale** page appears, 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. Selected texts for translation are added to the list.

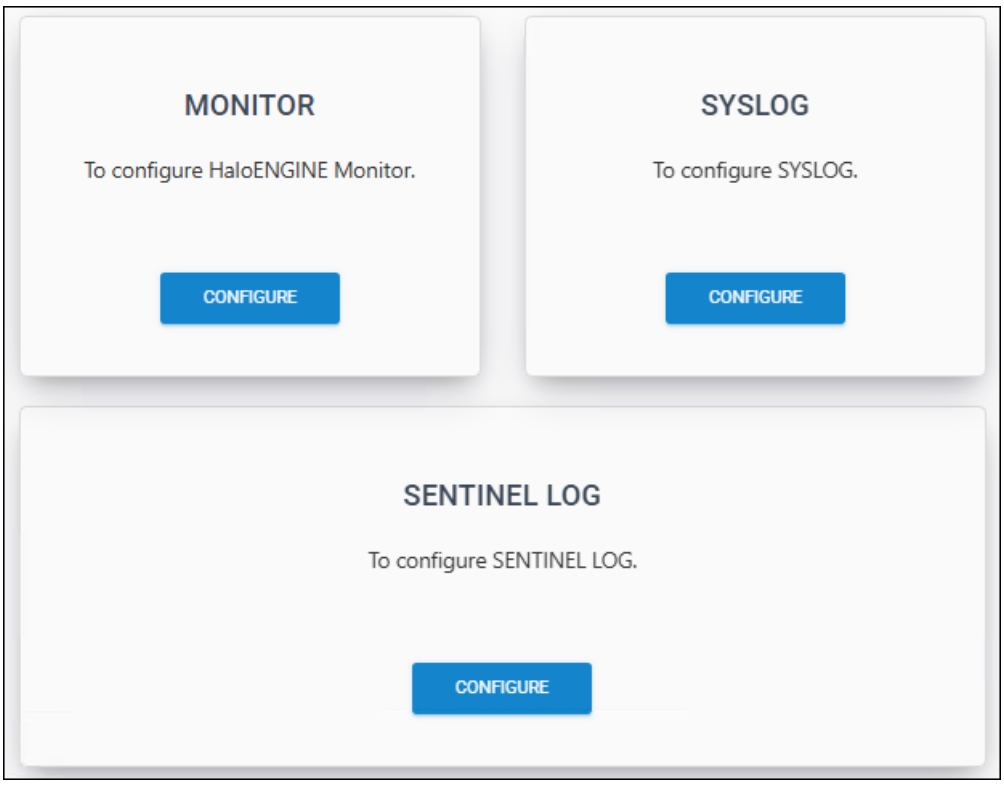
   b. You can either press **Apply Configuration** now and then reload configuration to let the changes take effect, or you can configure further settings and then press **Apply Configuration**.

6.6.9.2. Monitor Configuration

Prerequisite: Ensure that Monitor is enabled, as mentioned above.

Follow the steps below to configure the Monitor:

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



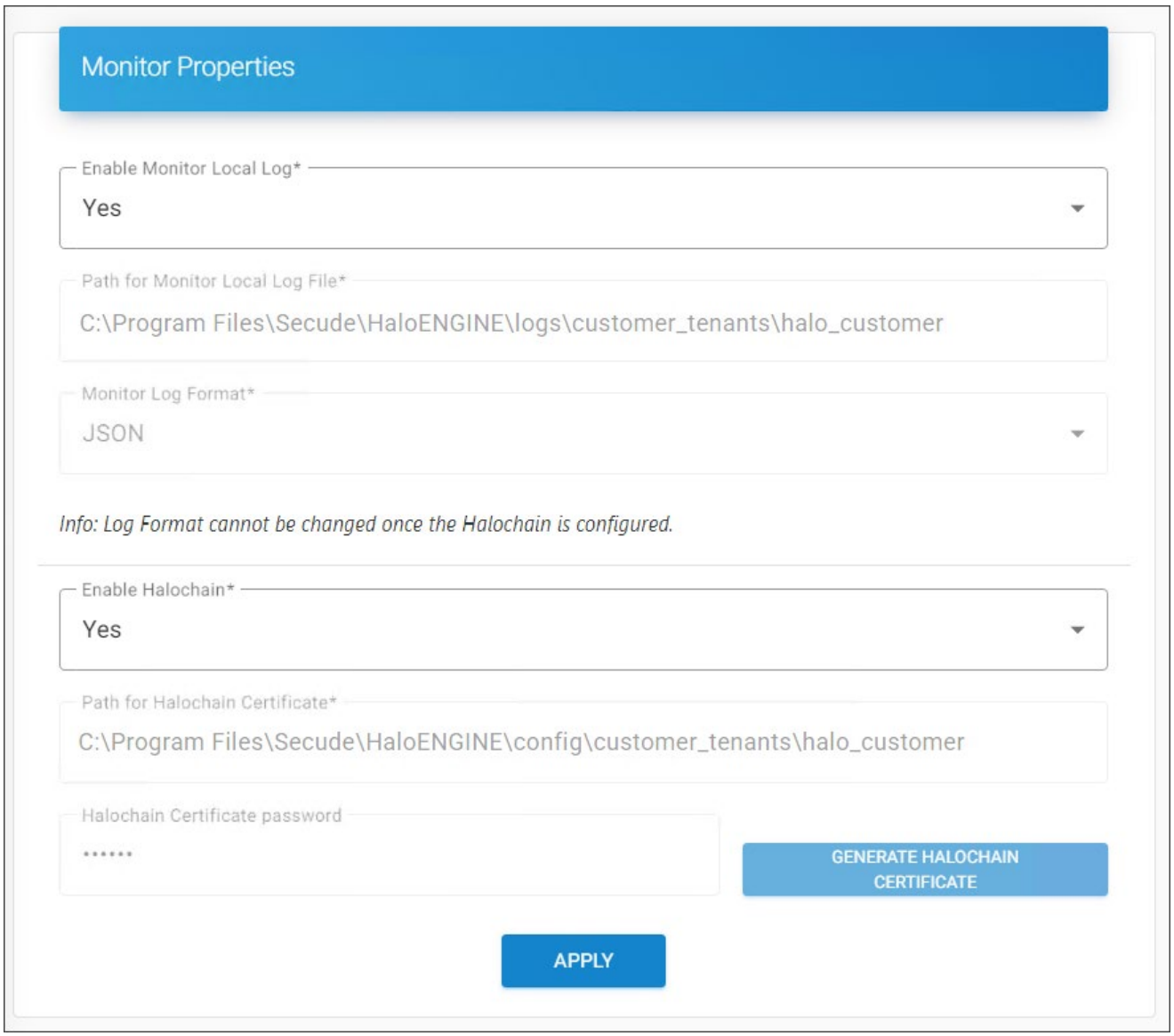
Monitor Configuration

3. Configure Monitor, Syslog, and Sentinel Log individually, as described in the following sections.

6.6.9.2.1. Monitor Properties

Follow the steps below 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** – Select Yes or No to enable or disable the local monitor log. If enabled, the default path is `C:\Program Files\Secude\HaloENGINE\logs\customer_tenants\halo_customer`.
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 Halochain is configured, and the field will be disabled once you enable Halochain.
4. **Enable Halochain** – Select Yes or No to enable or disable the **Halochain** feature. If enabled, the default Halochain certificate path is `C:\Program Files\Secude\HaloENGINE\config\customer_tenants\halo_customer.`
5. **Halochain Certificate Password** – Enter a password for Halochain and click **Generate Halochain Certificate**. You will receive a confirmation message upon creating a certificate.

6. Click **Apply**.

   Results: A confirmation message will appear after the properties are successfully updated.

6.6.9.2.2. Syslog Properties

Prerequisite: Ensure that Monitor Local Log is enabled.

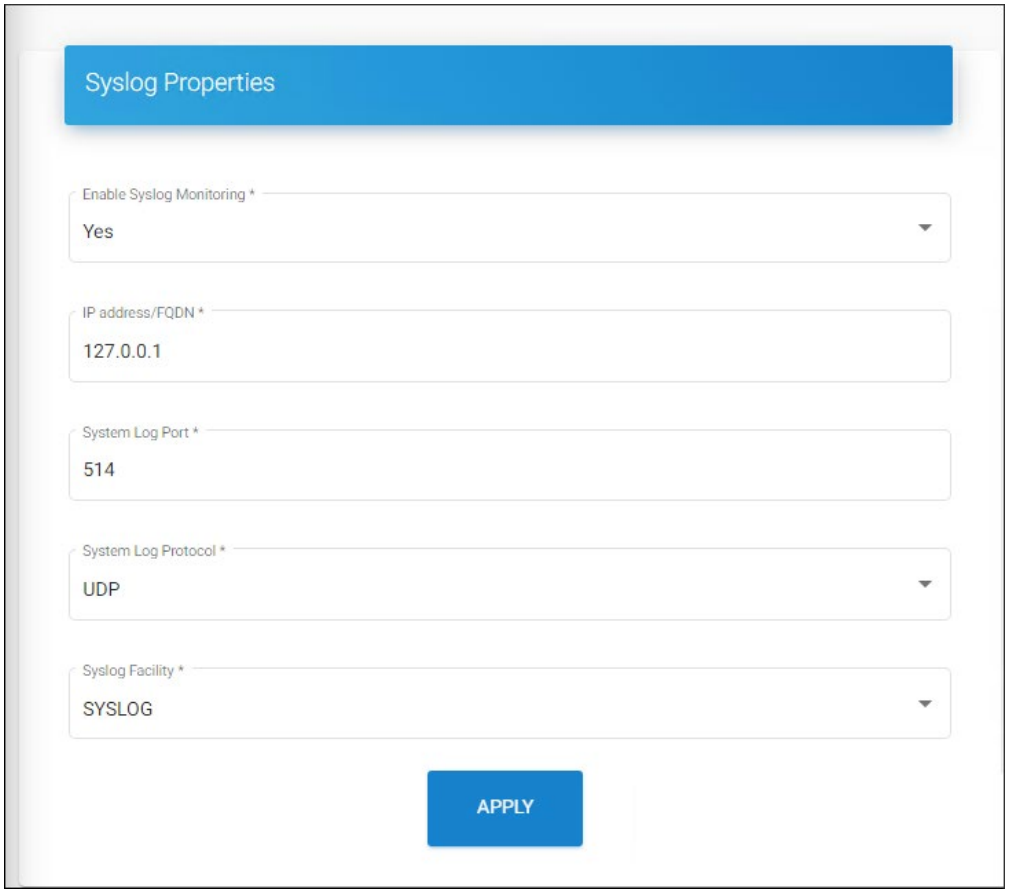
Requirements

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 steps below 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** – Select Yes or No to enable or disable the 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**.

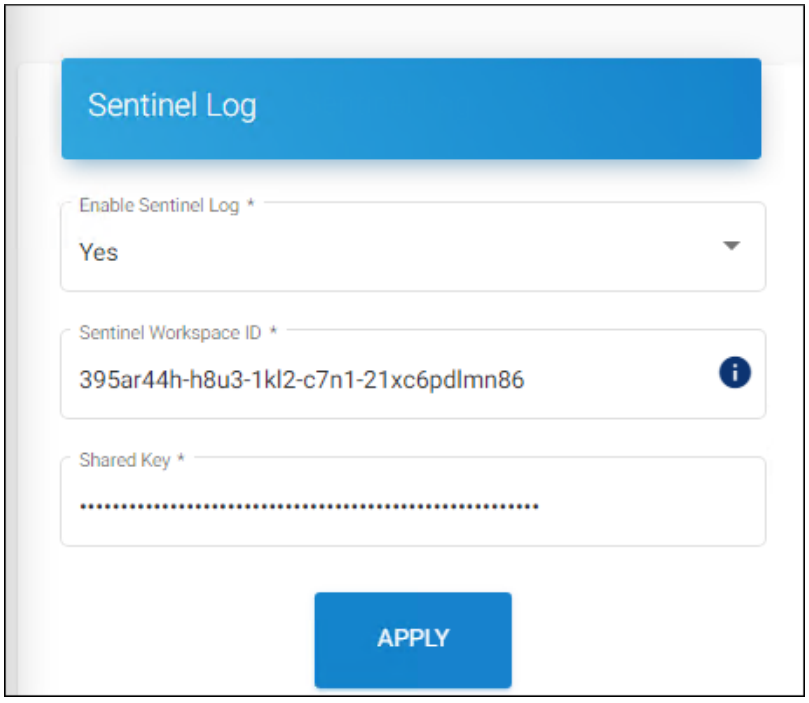
Results: A confirmation message will appear after the properties are successfully updated.

6.6.9.2.3. Sentinel Log

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

Follow the steps below to configure the Sentinel log properties:

1. On the **Sentinel Log** tab, click **Configure** and then enter the following details as shown in the figure below:



Sentinel Log

2. **Enable Sentinel Log** – Select Yes or No to enable or disable the 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: A confirmation message will appear after the properties are successfully updated.

What to do next

1. After configuring **Monitor**, **Syslog**, and **Sentinel Log**, click **Reload Configuration** to apply the changes.
2. Test the log after configuration.

How to obtain logs in Microsoft Sentinel?

Prerequisites:

1. Ensure the HaloENGINE Admin Portal is restarted after configuring Sentinel properties.
2. Perform actions like uploading and downloading only after the admin portal is configured to generate and forward sufficient logs.

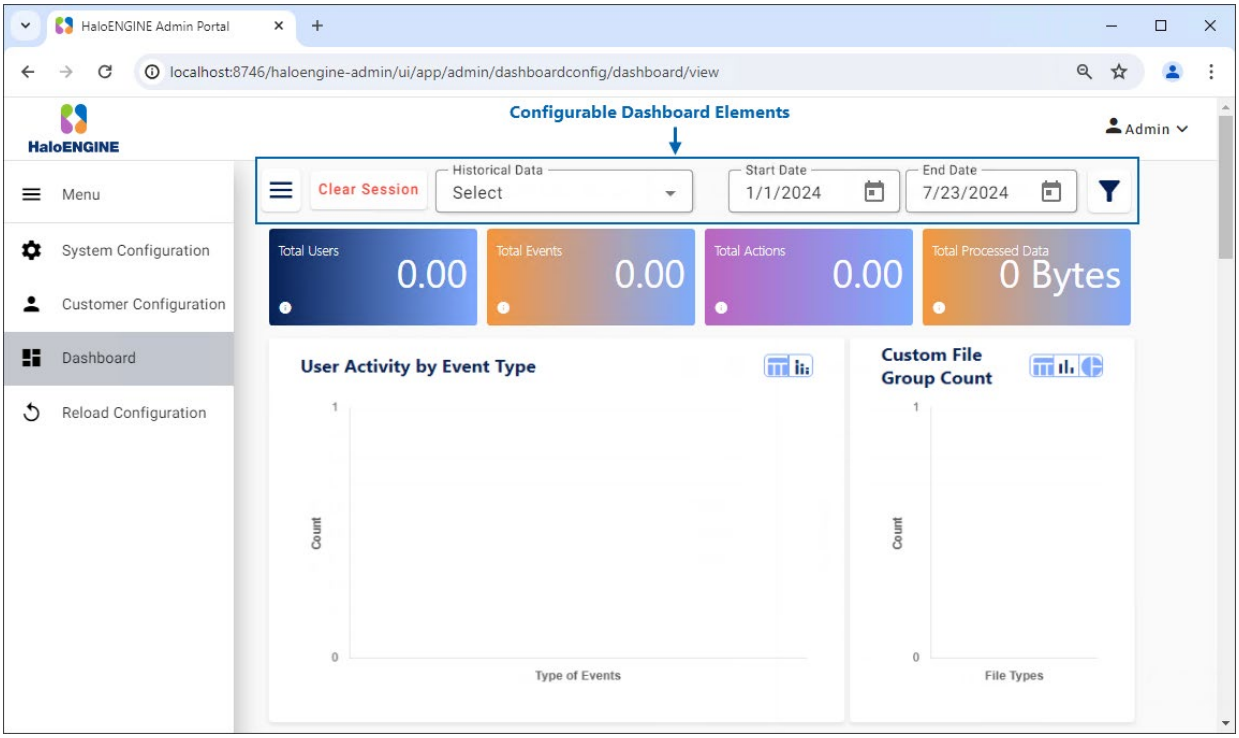
Follow the steps to obtain logs in Microsoft Sentinel.

1. Log in to the Microsoft Azure portal.
2. In 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 appears. Here, you need to click **Create** at 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.

6.6.10. Phase 6. 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.

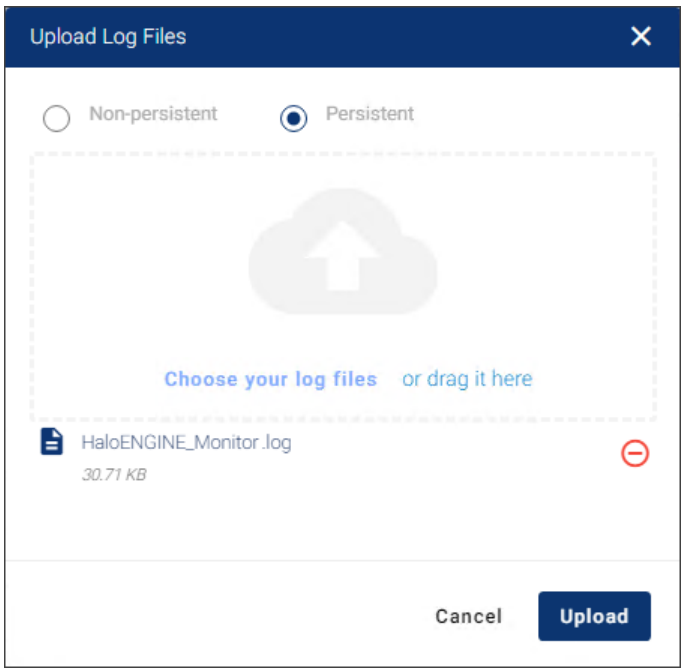
Persistent log: This is real-time log data obtained directly from the HaloENGINE log files. If you want to review a log file permanently, you can upload it using the **Upload Logs** option. These logs are then displayed in the Historical Data section.

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.

6.6.10.1. 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 appears 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 appears 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.

6.6.10.2. 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.

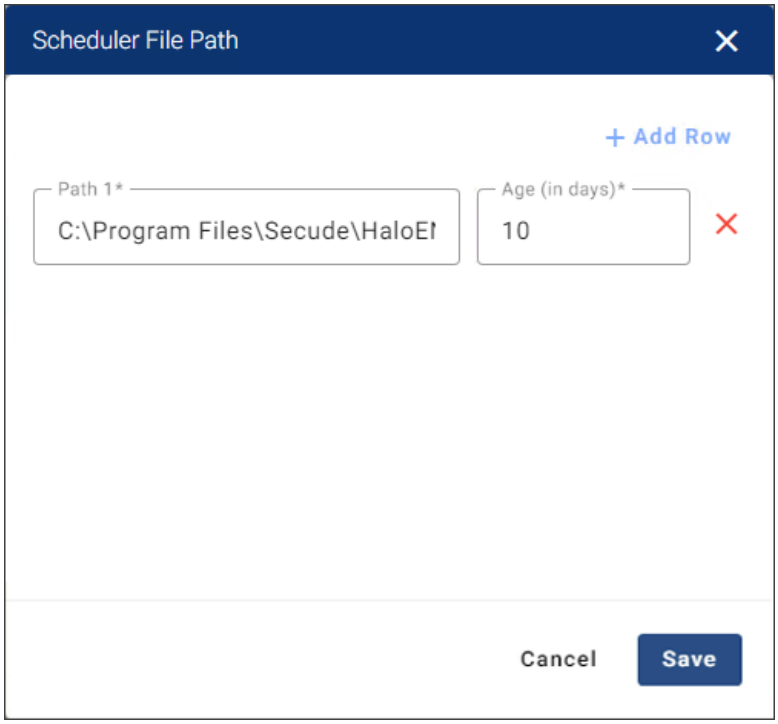
1. The uploaded log IDs appear in the list of **Historical Data**. By selecting one ID, the dashboard will automatically visualize the specified log entry. If you want to remove the uploaded data, click the **Delete** icon.
2. By selecting the **Start Date** and **End Date** in the calendar, the logged 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.

6.6.10.3. 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 appears 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\halo_customer`
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.

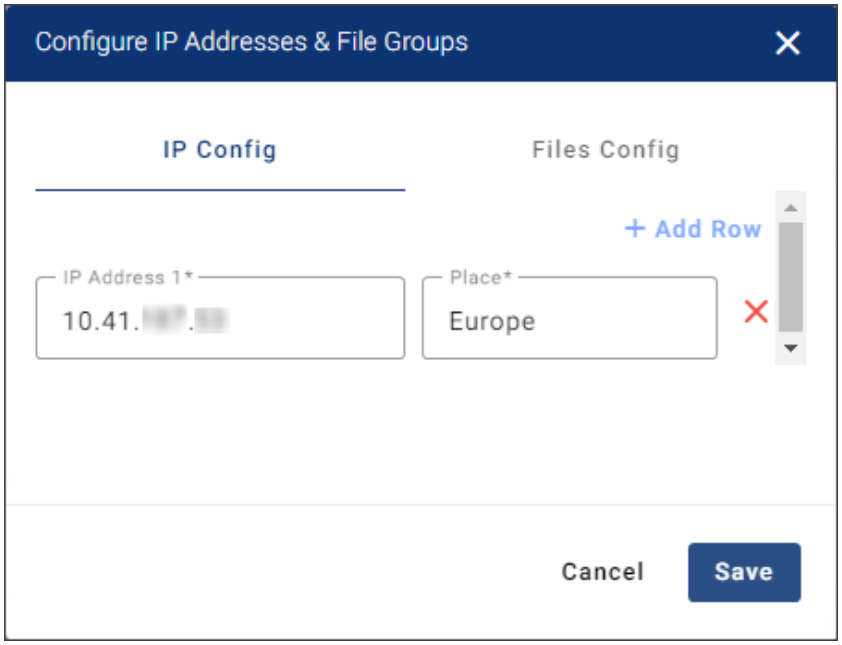
   d. To remove a path, click the remove “X” icon.

6.6.10.4. 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* appears as shown in the figure below:



IP Config

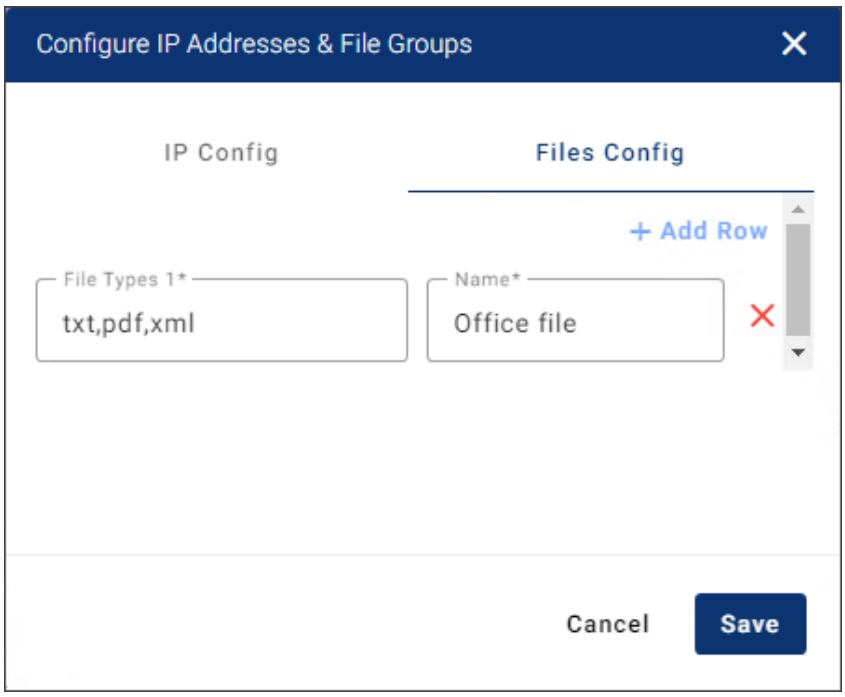
2. Click **+Add Row**, the fields will be visible on the page.
3. Click the **IP Config** tab and enter the IP address and place. For Example:
   a. **IP Address**: `10.41.*.*`
   b. **Place**: `Europe`
4. Click **Save**.

   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

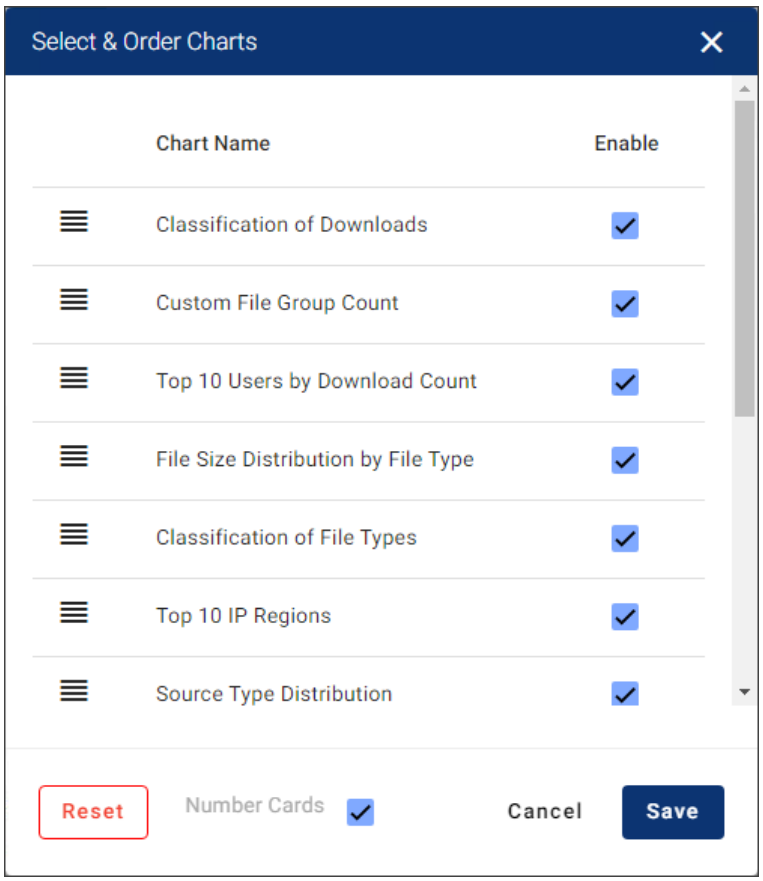
2. Click **+Add Row**, the fields will be visible on the page.
3. Enter the file types and name of the file types. For Example:
   a. **File Types**: `txt`, `pdf`, `xml`
   b. **Name**: Office file
4. Click **Save**.

   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.

6.6.10.5. Select Charts

This option lets you enable or disable dashboard charts and rearrange them by dragging into your preferred order.

1. Click on the **Select Charts**, and the *Select & Order Charts* page appears 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:

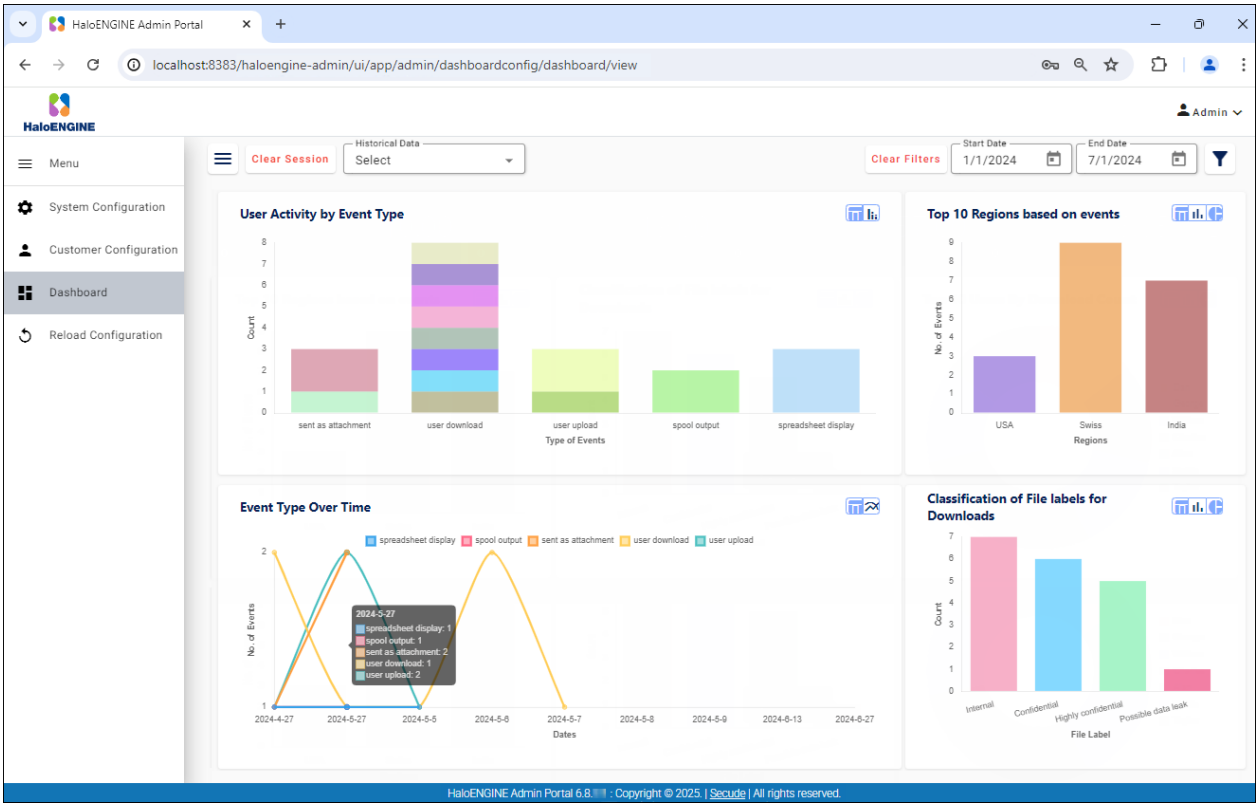
   a. You will receive a confirmation message after successfully configuring the chart order.

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

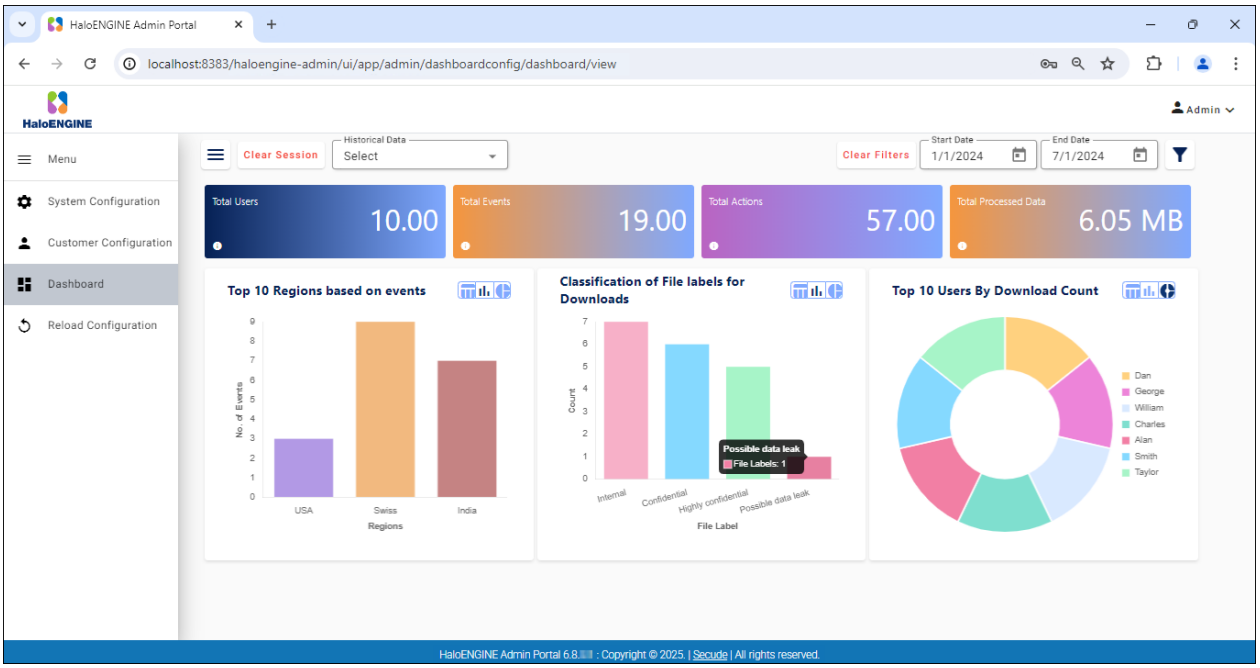
   c. To restore the charts to the default view, click **Reset**. You will receive a confirmation message saying "*Are you sure you want to reset to default*" click **Yes** to confirm.

   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.

6.6.10.6. Sample Screens



Sample 1



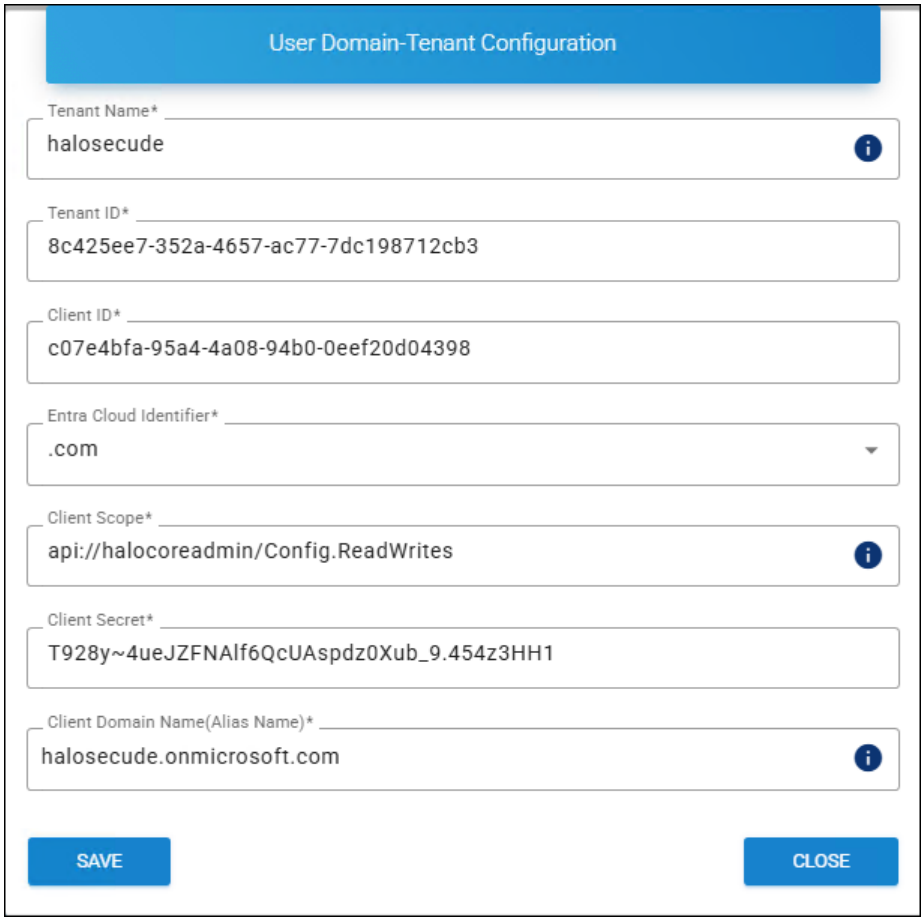
Sample 2

6.6.11. Phase 7. 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 select the customer ID (halo_customer) from the list.
2. On the **Tenant Configuration** tab, click **Configure**.
3. Click the plus icon to open the *User Domain-Tenant Configuration* page, as shown below.



Registering a domain page

Note: Values shown in the example screen have been modified for security reasons.

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, if your tenant domain is "`Contoso.onmicrosoft.com`," enter only "Contoso." Ensure that the name specified in the **Redirect URL** exactly matches the Tenant Name configured in the Admin Portal. This field is case-sensitive.

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 Secret** – Enter the secret assigned to the application. For example, `T928y~4ueJZFNAlf6QcUAspdz0Xub_9.454z3HH1`. Please refer to the section "Step 3: Certificates & Secrets".
10. **Client Domain Name (Alias Name)** – Enter an alias name for your domain. For example, `halosecude.onmicrosoft.com`.
11. Click **Save** and repeat the above steps to register other tenants.
    Results: A confirmation message appears after the user domain is registered.

Related tasks:

1. Use the icons to edit or delete a tenant.
2. Click the **Tenant Details** icon to view tenant information.
3. Registered tenants are listed on the *User Domain-Tenant Configuration* page.

What to do next:

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

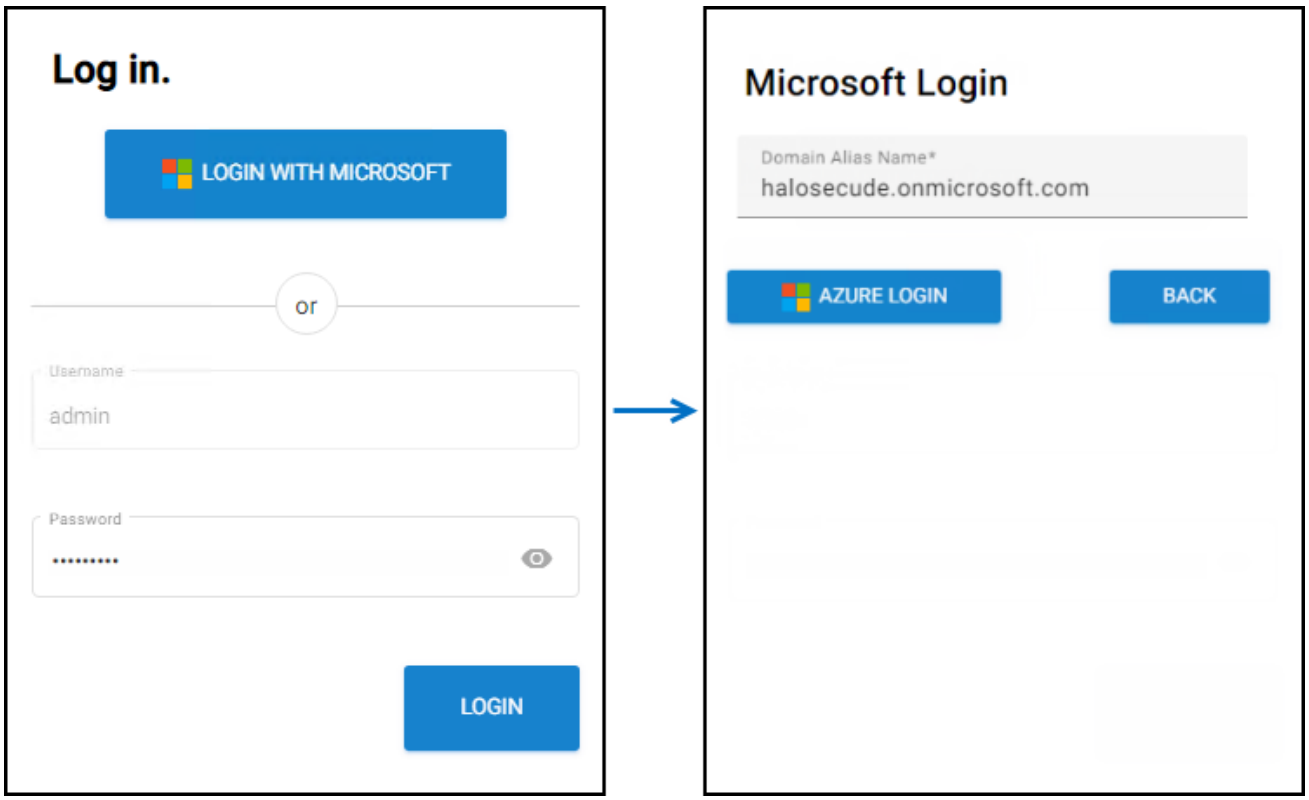
6.6.11.1. User Login (Super Admin/Azure Users)

After completing tenant configuration and reloading, you will be redirected to the login page. Choose one of the following options to log in to the portal.

Option 1 – Default Super Admin Account

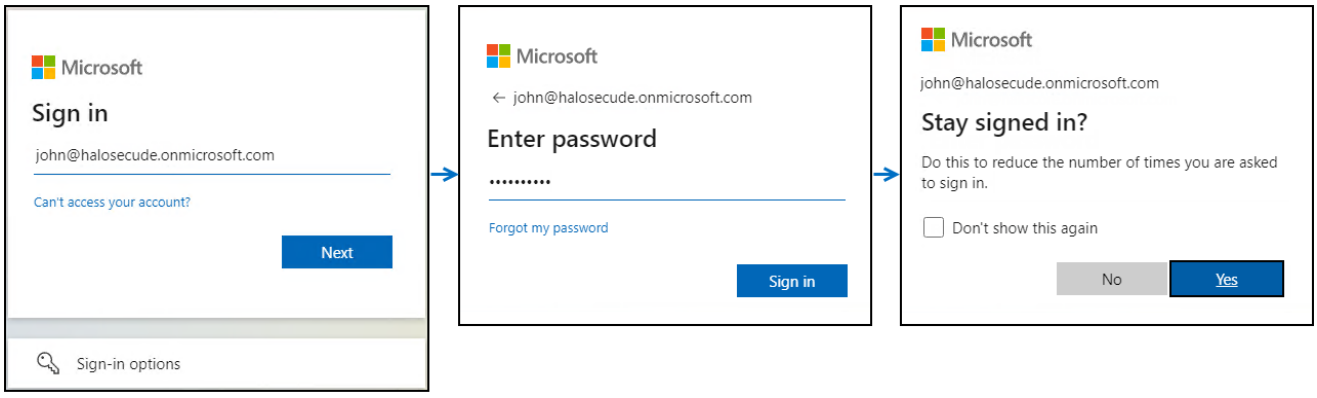
Option 2 – Microsoft account (log in using user account - Customer_Admin or Customer_User)

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



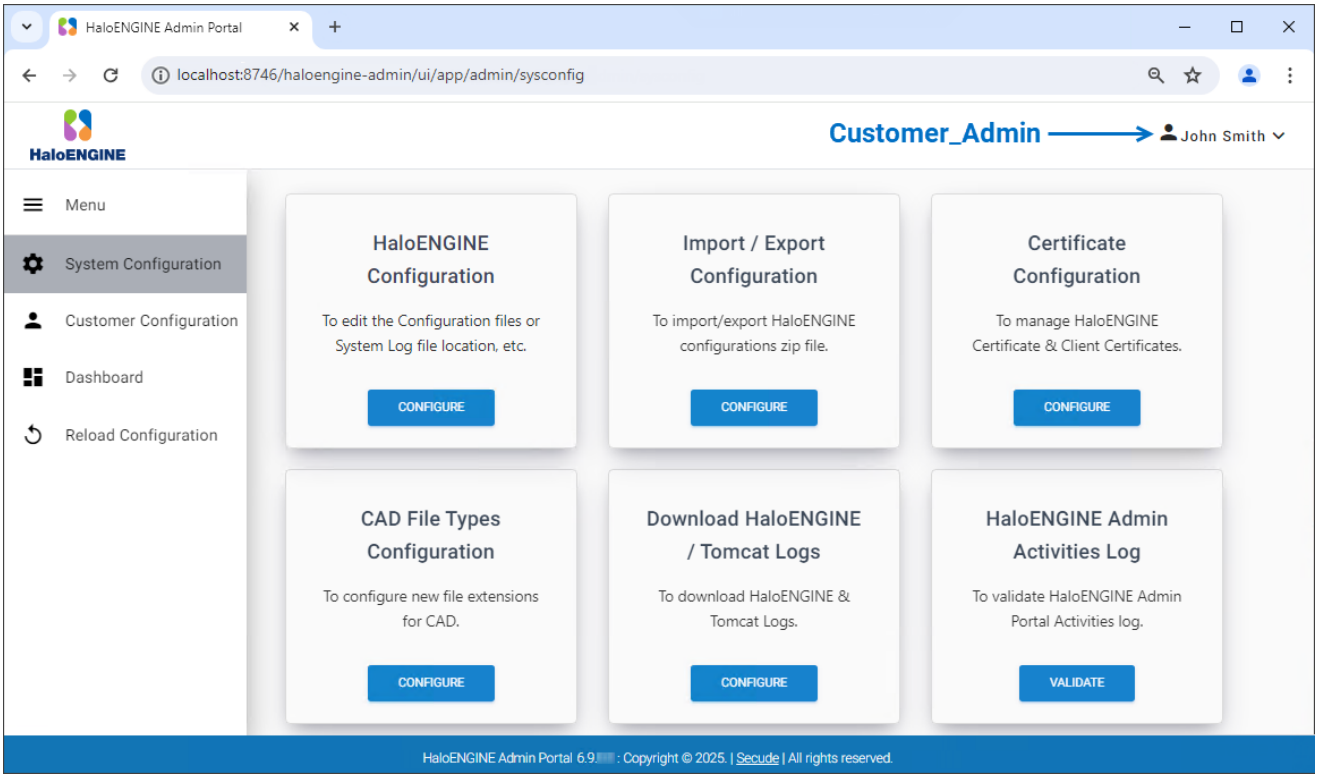
Microsoft Azure Login #1

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

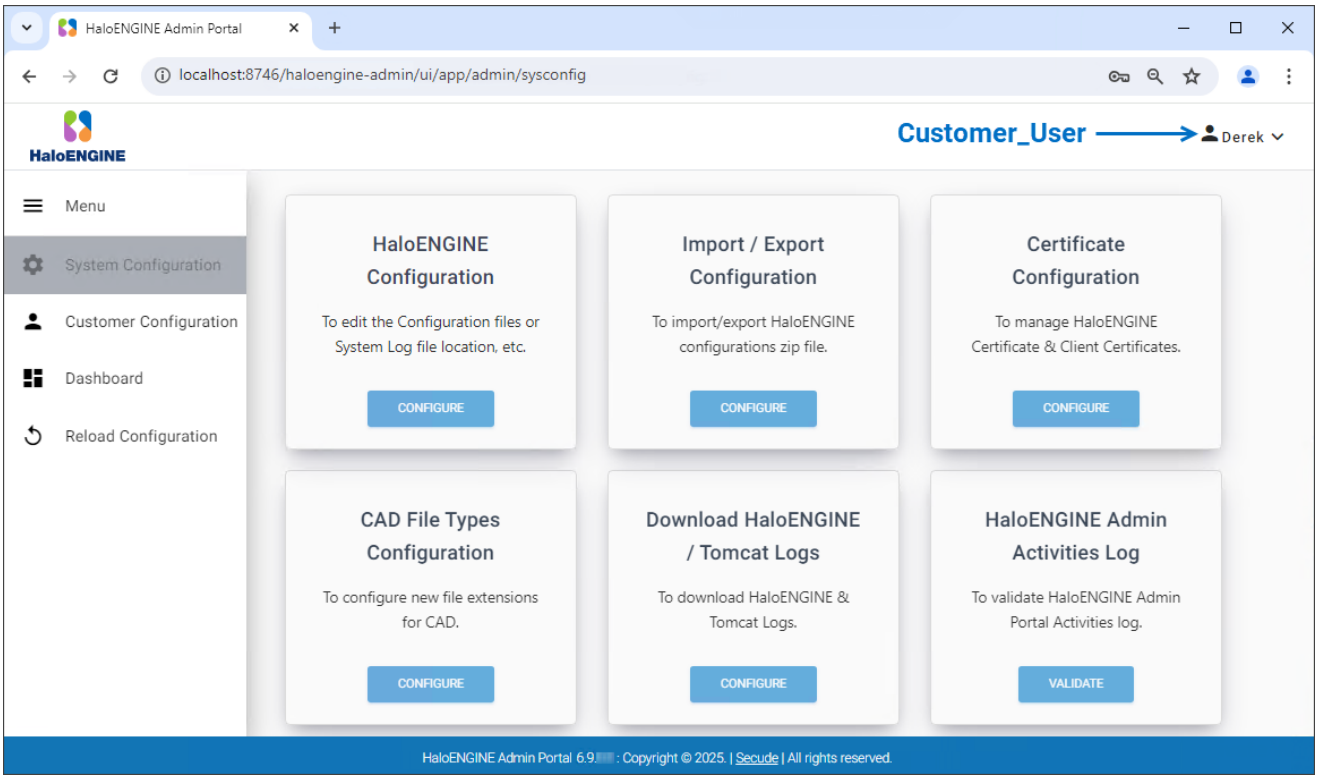


Microsoft Azure Login #2

5. For the prompt "*Stay signed in?*", click **No** or **Yes** based on your preference.
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 of the Azure portal.
7. For illustration purposes, user accounts are shown in the images below:



Admin account



User account

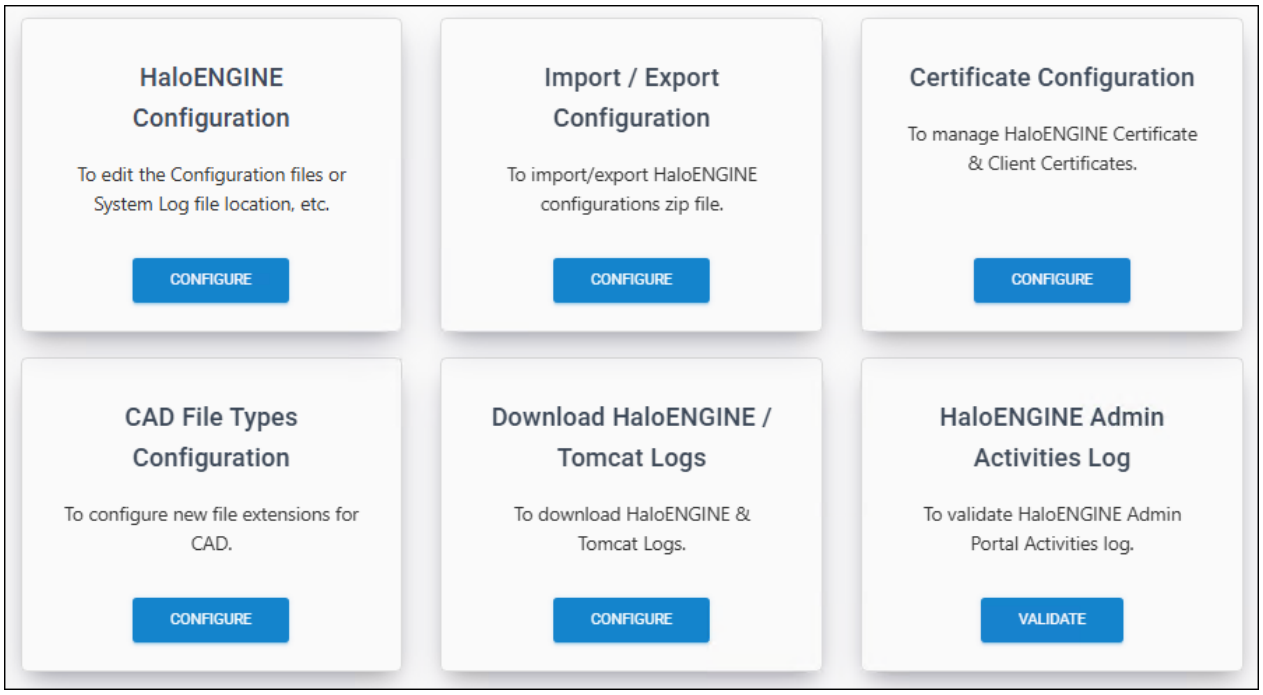
Methods to log in admin portal

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-in 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`

6.7. 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.



System Configuration page

6.7.1. HaloENGINE Configuration

Basic Configuration

Follow the steps below 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

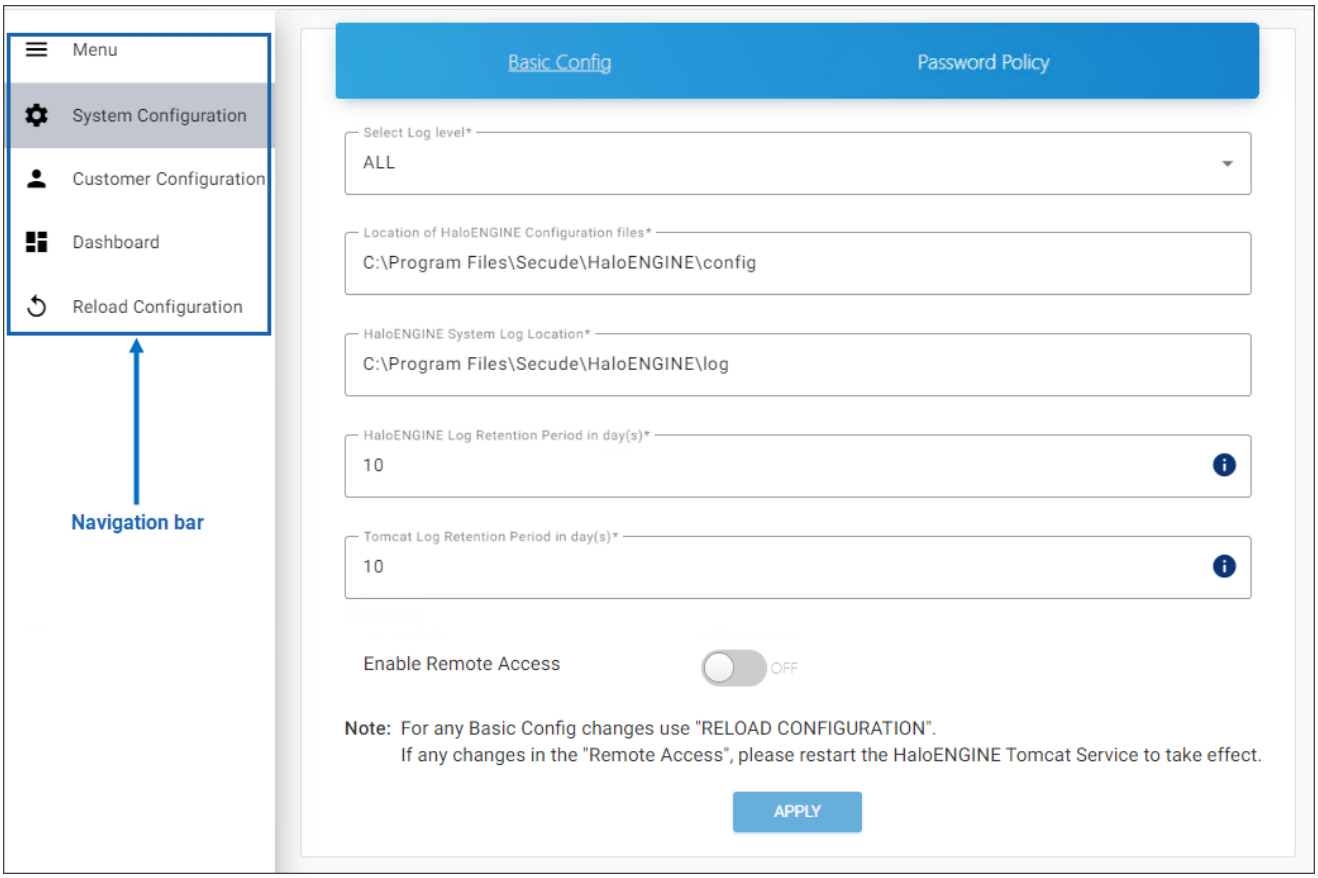
c. Path for HaloENGINE system log

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:

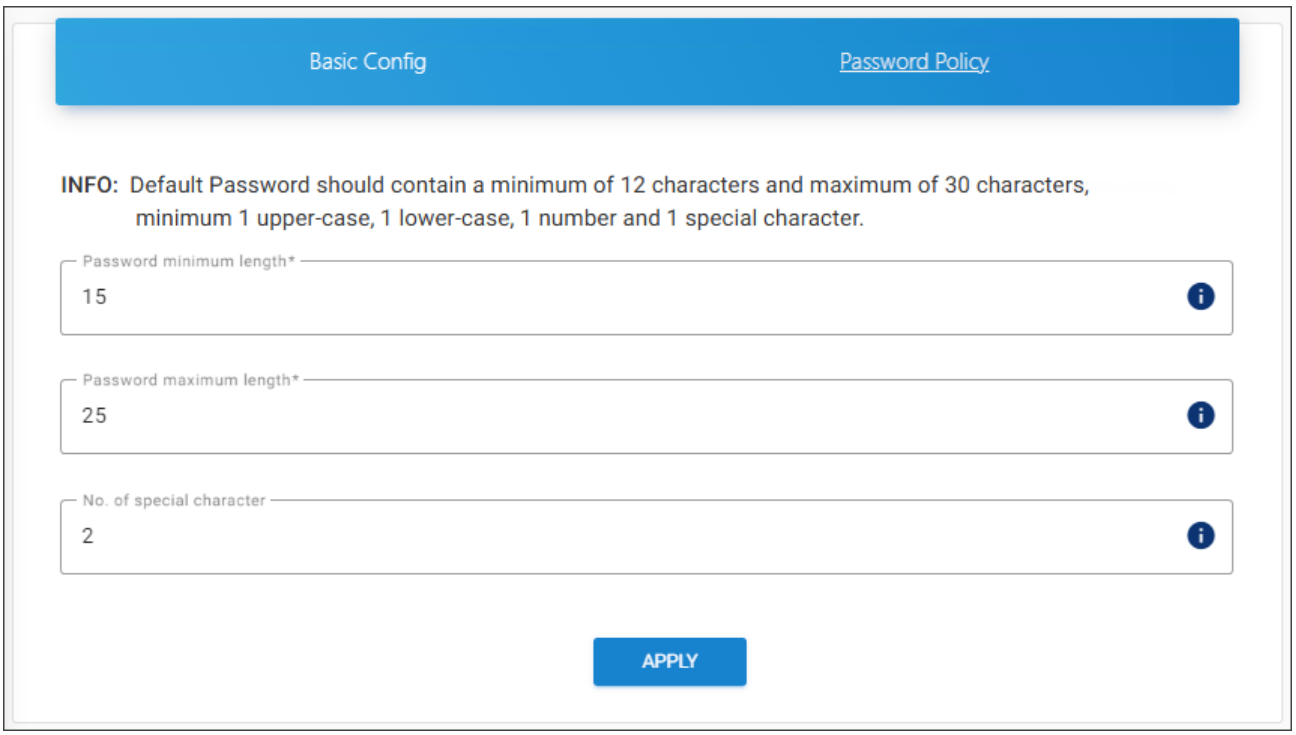
a. The page will be directed to the login page once the reload is done.

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, "*Please change your Password*."

   b. On the warning message screen, click **Change Password**. The **Change Admin Password** screen appears. 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".

   c. The admin portal will restart automatically, and you must enter a new password to access it. The current password cannot be reused."

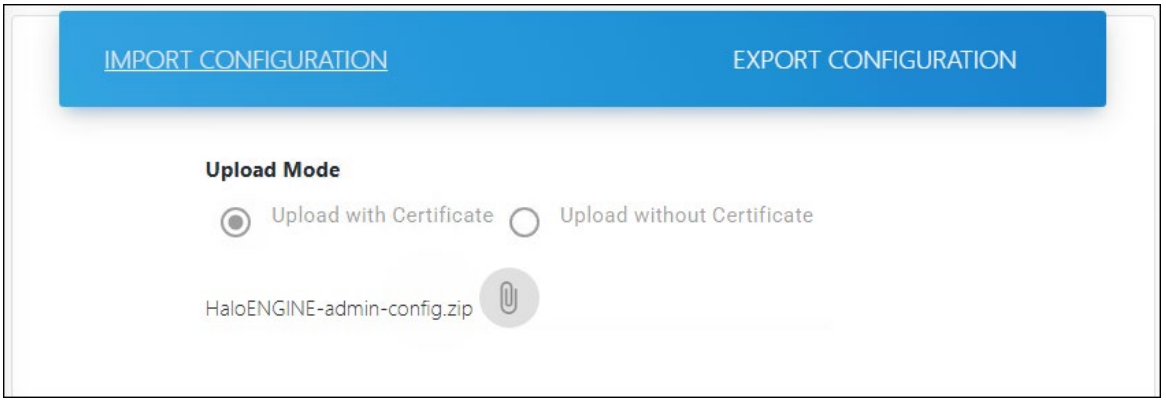
6.7.2. Import/Export Configuration

Exporting the configuration is important because the exported configuration file can be imported during a new installation, allowing retention of existing settings, reducing the time and effort needed for reconfiguration, ensuring consistency across environments, and minimizing the risk of misconfigurations or errors.

Follow the steps below 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 either **Upload with Certificate** to import the configuration file along with the existing certificate, or **Upload without Certificate** to import the configuration file without the certificate.
   b. Click on the button and select the `HaloENGINE-admin-config.zip` file from the **Open** dialog box.

   Results: You can see the name of the zip file displayed on the page.



Import Configuration

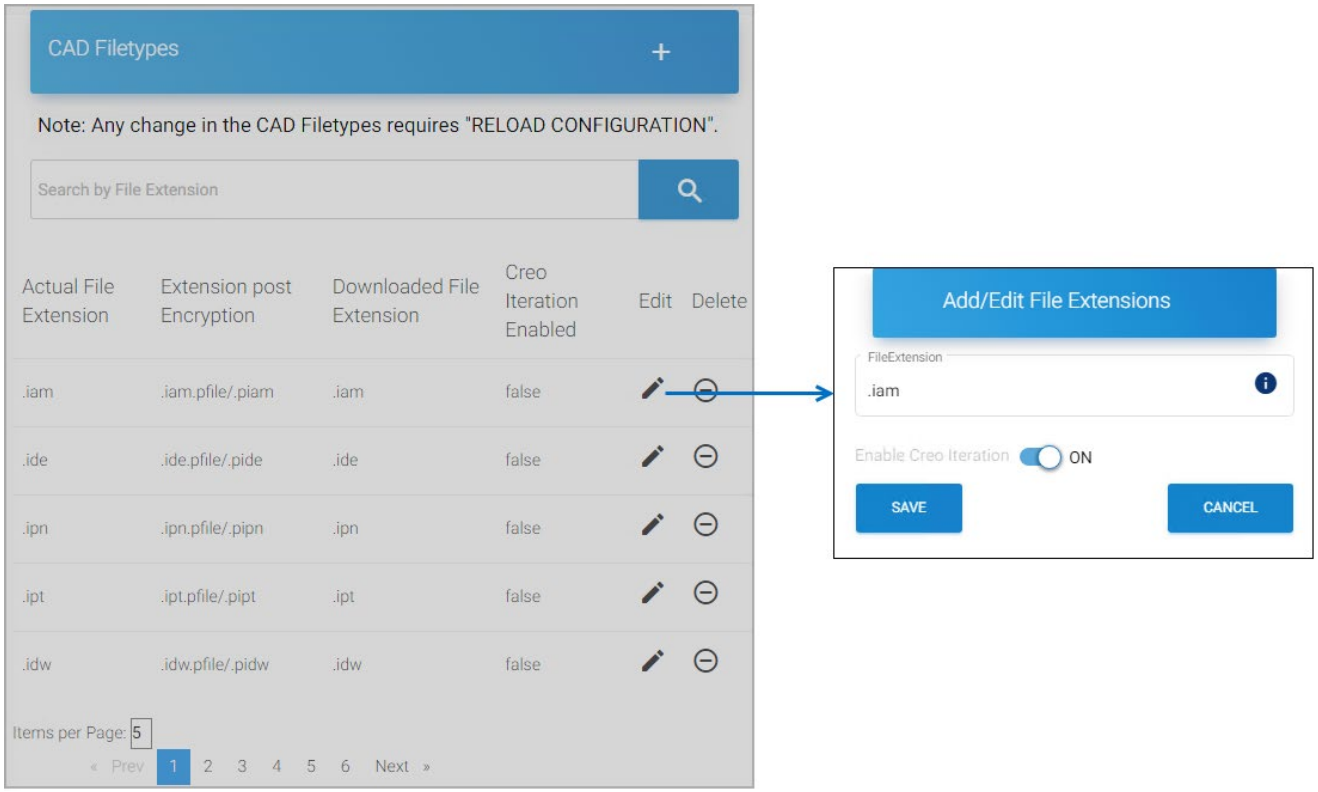
3. **What to do next:** Restart the HaloENGINE Tomcat service for the configuration update to take effect.
4. **To export**:
   a. Click **Export Configuration** and then click **Export Config** button.
   b. Please wait while the file `HaloENGINE-admin-config.zip` is downloaded.

6.7.3. 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:

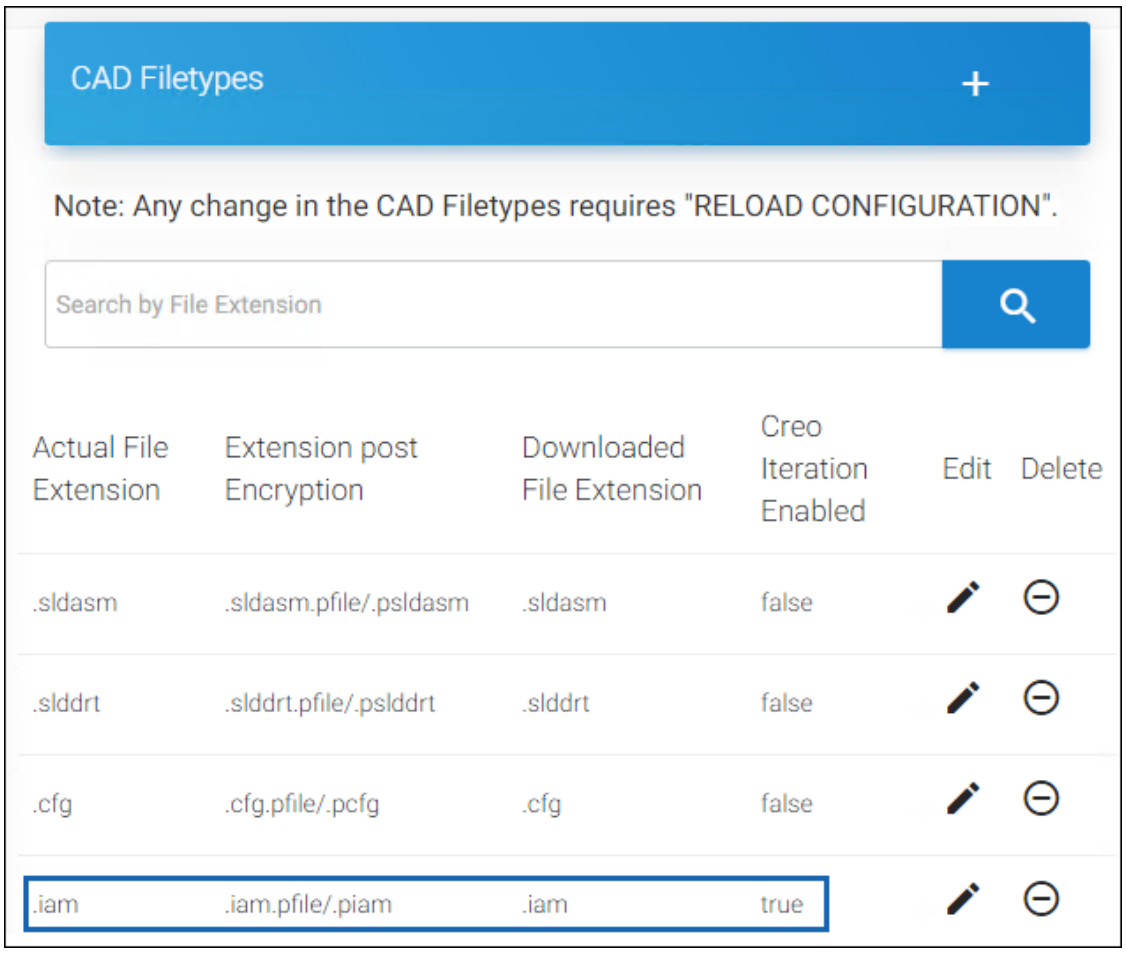
1. On the left navigation bar, click **System Configuration**, and then on the **CAD File Types Configuration** tab, click **Configure**.
2. The *CAD Filetypes* page appears as shown in the figure below:



CAD File Types Configuration

3. **Option 1**:
   a. To change the Creo Iteration of a file type from the existing list.
   b. Turn ON the **Enable Creo Iteration** slider for the file type. 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 example below, the `.iam` row gets appended to the end of the list with **Creo Iteration Enabled = true**.



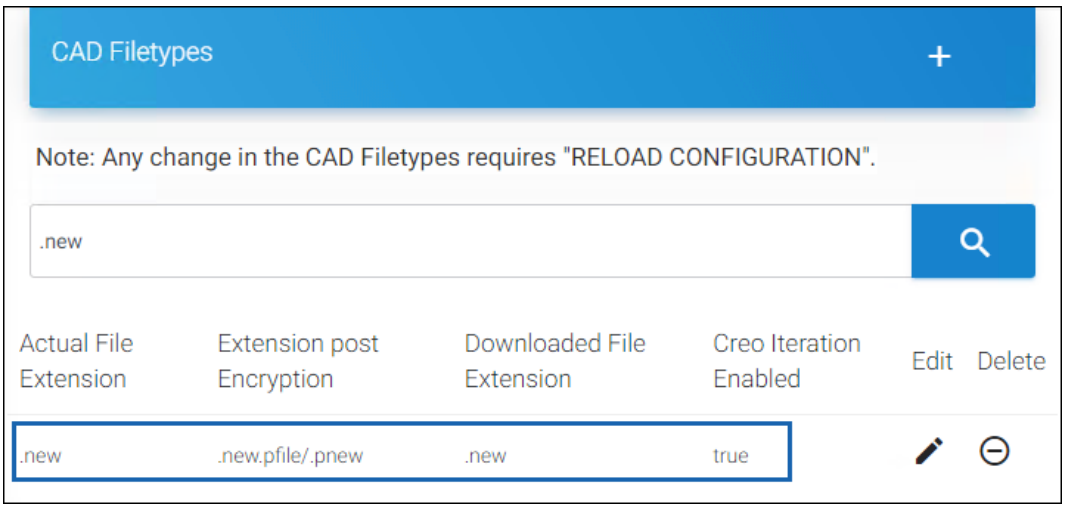
Creo Iteration Enabled

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

      Results: After saving the file type, a confirmation message appears, and the new entry is added to the list. Click **Reload Configuration** to apply the changes.

6. **To find a file extension:**
   a. Click **Search File Extension**. The **Search File Extension** page appears.
   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 using the **Edit** or **Delete** icon.

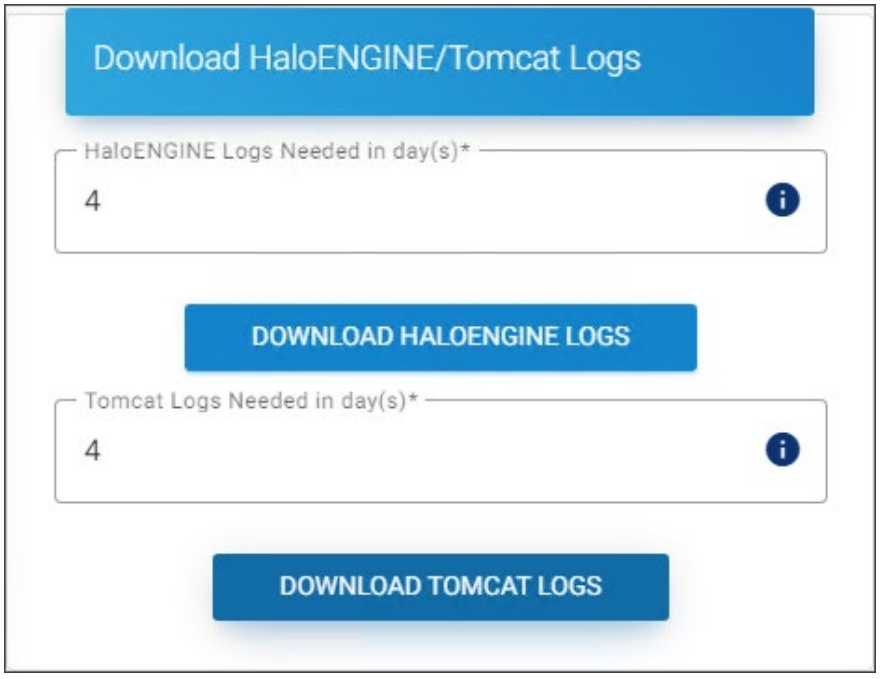


Search File Extension

6.7.4. 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 appears 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**.

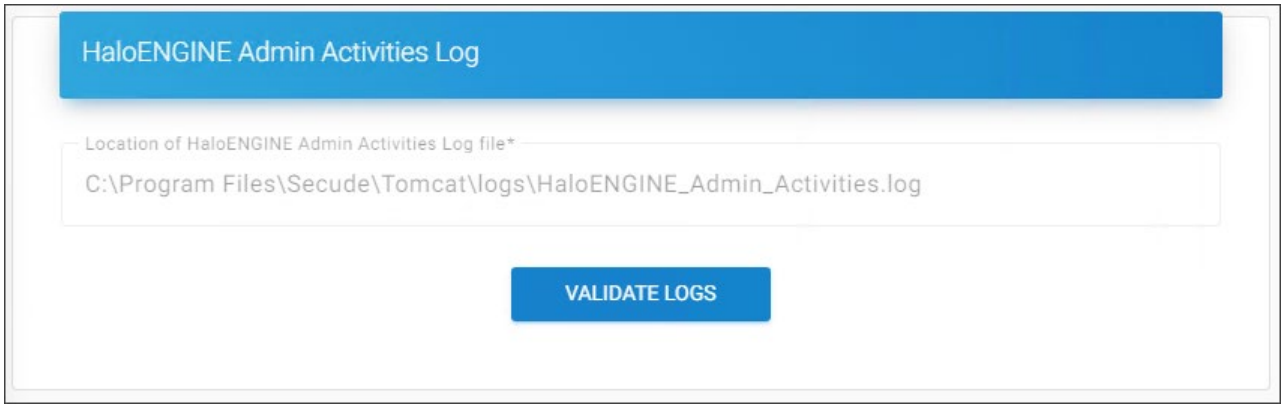
b. **Results**: A zip file (`HaloENGINE-Log`) will be downloaded to the default download location.

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.

6.7.5. HaloENGINE Admin Activities Log

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

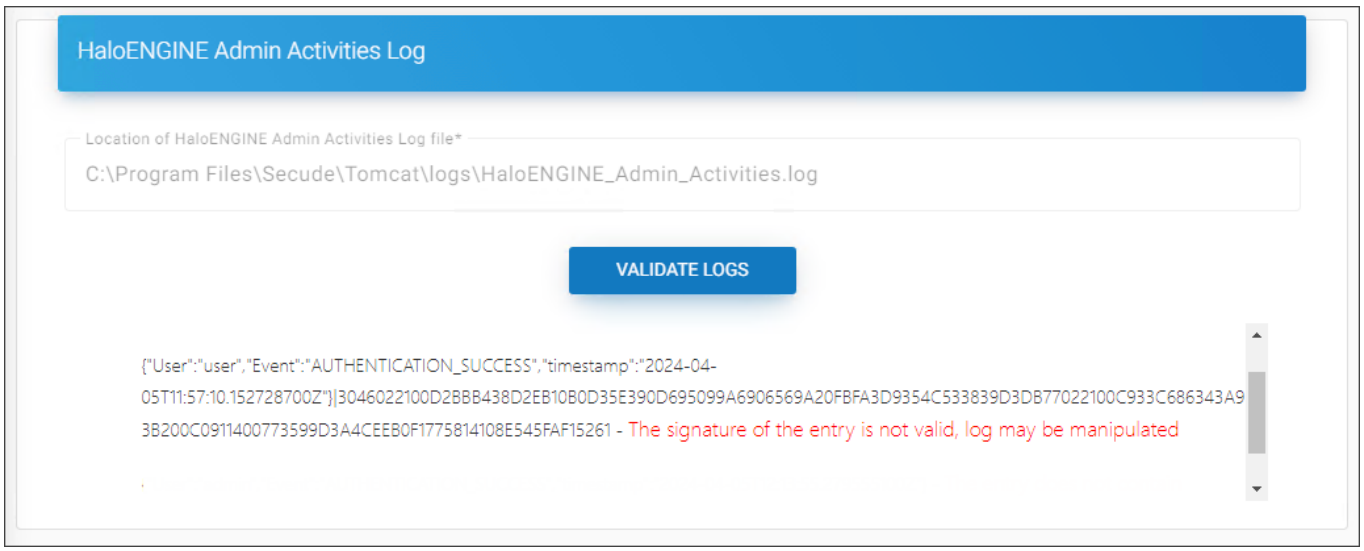
1. On the left navigation bar, click **System Configuration**, and then on the **HaloENGINE Admin Activities Log** tab, click **Validate**.
2. The *HaloENGINE Admin Activities Log* page appears as shown in the figure below:



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

6.7.6. Monitor Log Validation

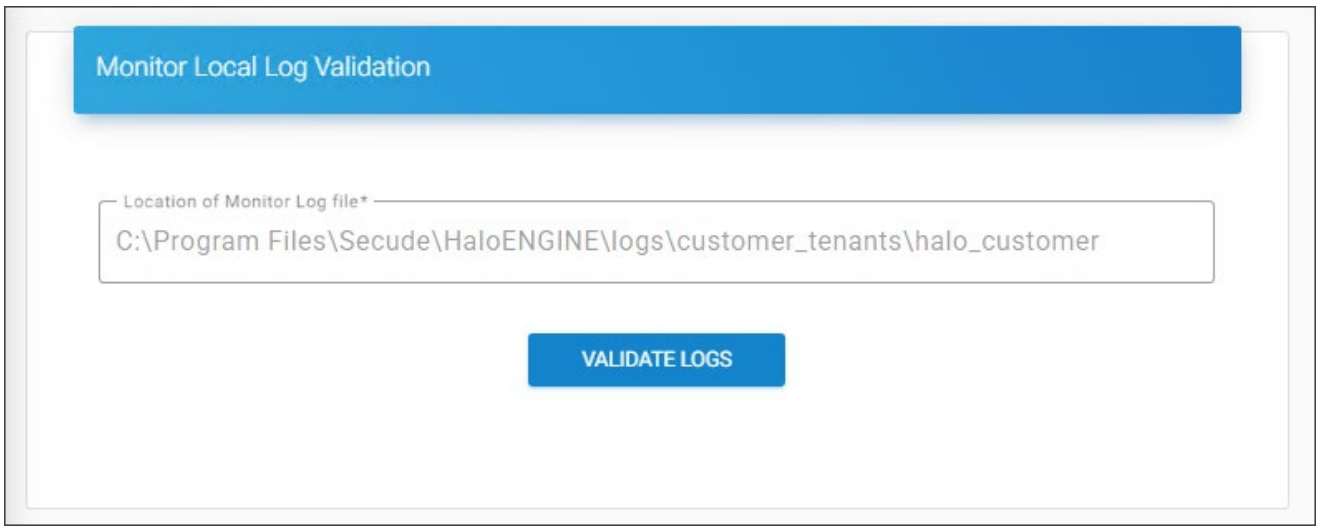
Halochain is a powerful feature that scrutinizes audit log files such as `HaloENGINE_Monitor.log` and `HaloENGINE_Admin_Activities.log` for any manipulation.

Prerequisites:

1. Make sure that you have enabled Halochain in Monitor Properties. Please refer to the section "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 procedure below to validate the audit log file:

1. On the left navigation bar, click **Customer Configuration**, and then select the customer ID (halo_customer) from the list.
2. On the **Monitor Log Validation** tab, click **Configure**.
3. The *Monitor Local Log Validation* page appears as shown below:



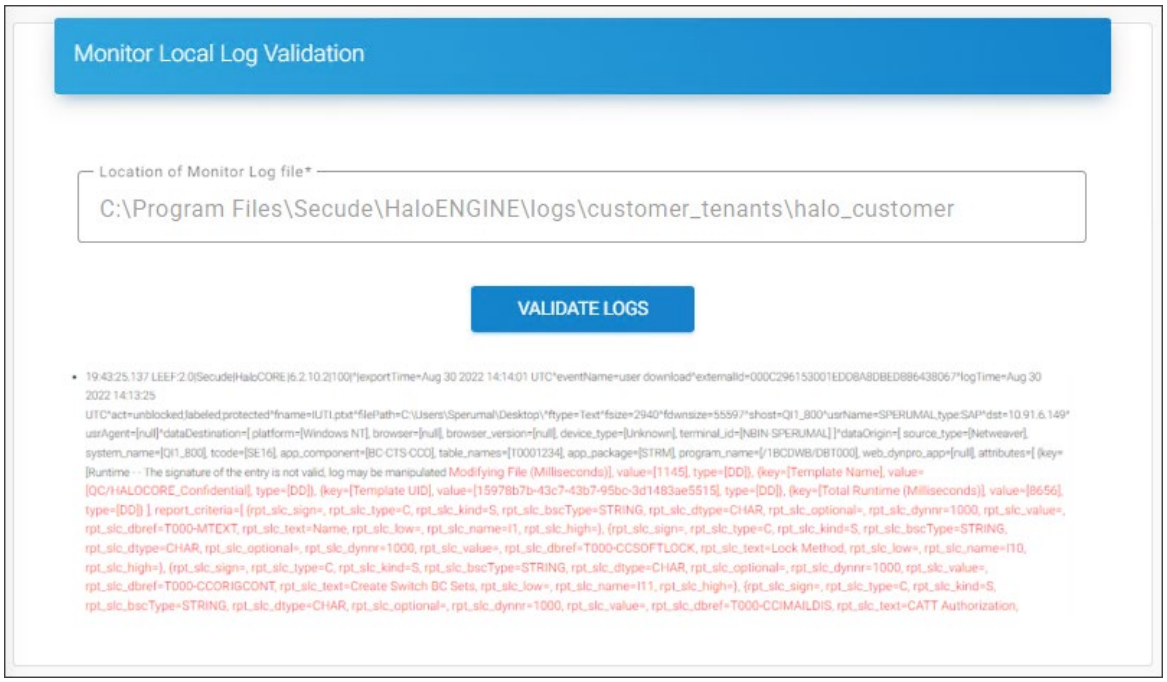
Monitor log validation

4. Click **Validate Logs**.

   Results:

   a. If no manipulation is detected, you will see the message: *The log file has been validated and no manipulated entries found*.

   b. The following output appears if manipulation is detected.



Halochain output

6.7.7. Log Out

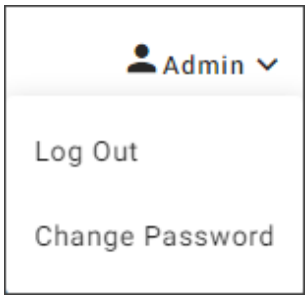
Logging out means terminating the current user's access to the portal. When the **Log Out** button is pressed, the portal is notified that the current user intends to terminate the login session.

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.

6.7.8. Change Password

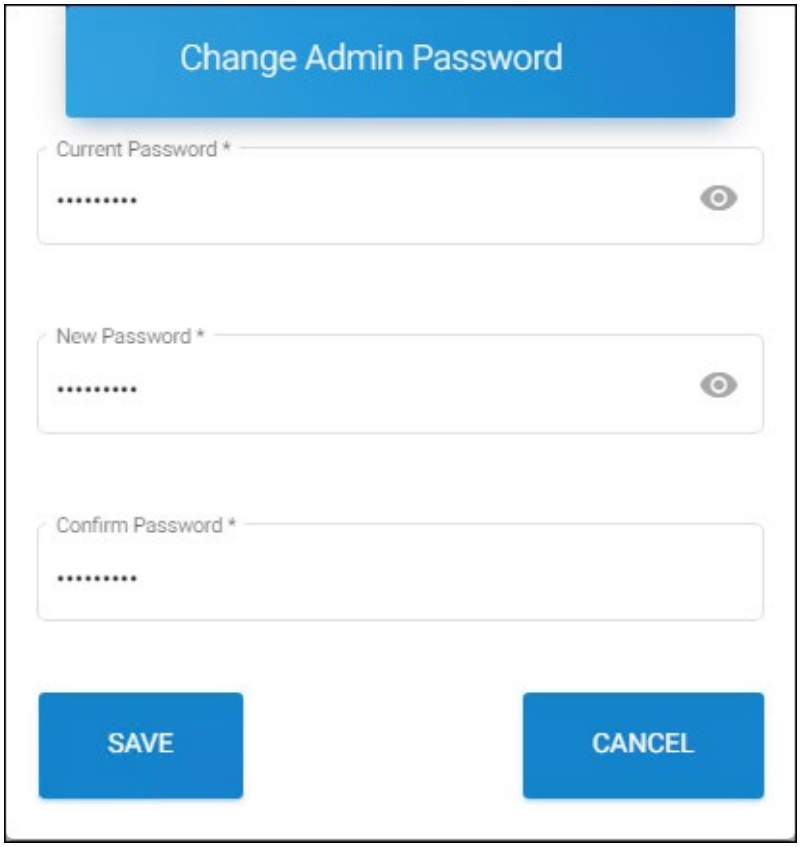
You can change your password for security concerns by following the steps below:

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



Change login password #1

2. The *Change Admin Password* dialog appears 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**.

6.7.9. Reset Administrator Password

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

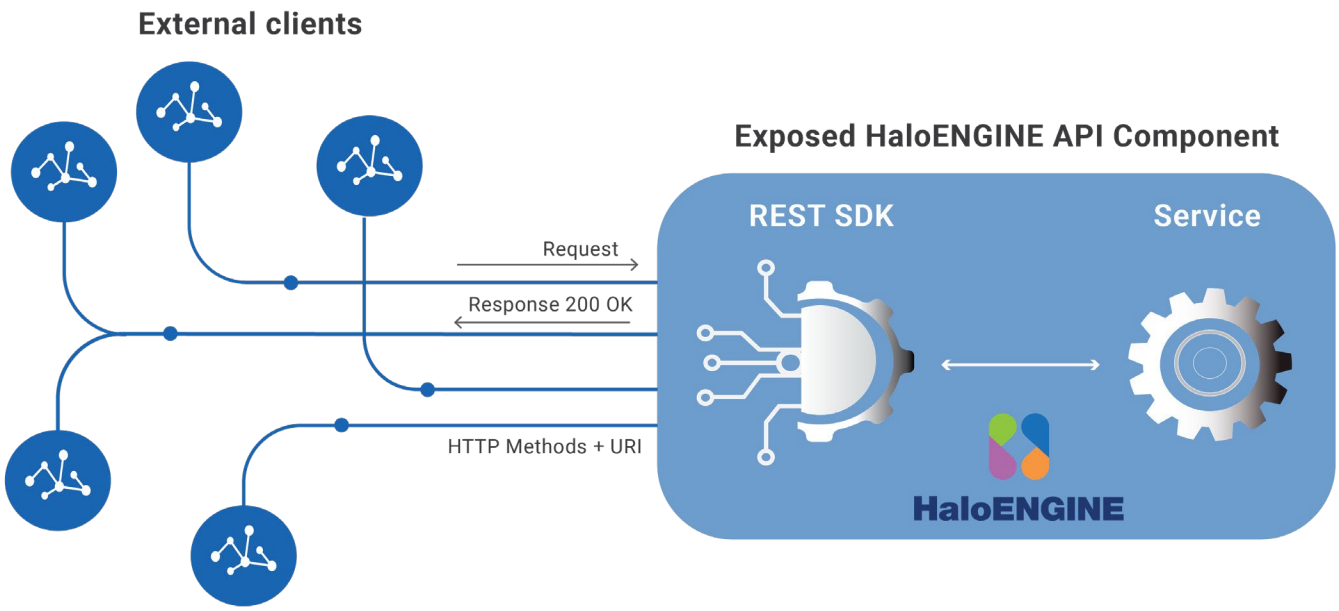
1. Copy `haloengine-password-config-<version>.zip` file to the desktop and extract it.
2. Open Command Prompt with administrator rights and change directory to `haloengine-password-config-<version>\bin`.
3. Type `haloengine-password-config.bat -h` to display the help information.
   For example:
   ```
   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.

7. 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 use of this information and the implementation of any APIs described herein are the sole responsibility of the customer. Successful integration depends on the customer's ability to evaluate, configure, and incorporate the APIs within their business environment.

7.1. About this Chapter

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 note that the examples in this document are intended solely as guidance and should not be applied in a production environment.

7.2. 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 as described in the following chapter, "Installing the HaloENGINE".
2. **Step 2**: Import the license in the admin portal with the HaloENGINE API enabled.
3. **Step 3:** Server Certificate Authentication. Select one of the following authentication approaches.
   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 the 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".
5. Postman or another REST client.

7.3. API Reference

This section provides API examples that can be executed using **Postman**.

7.3.1. 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.
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	`/Version`
POST	`/GetMetaDataTypes`
POST	`/GetActionFormRest`
POST	`/EncryptFile`
POST	`/DecryptFile`
POST	`/SendPLMMonitorLogData`

Endpoints

7.3.2. Version

Description: Returns the HaloENGINE server version.

Request method: GET

7.3.2.1. Request Example

The following example shows a request sent using Postman.

7.3.2.1.1. Request URL

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

7.3.2.1.2. Response

A successful request returns the following information:

- **Status Code:** 200
- **Response Body:** Plain text containing the HaloENGINE version number.

```
6.10.1.0
```

This response confirms that the HaloENGINE service is running and returns the current version.

7.3.3. Get Required Metadata Types

Description: Returns supported metadata types used by the HaloENGINE server.

Request method: POST

7.3.3.1. Request Example

The following example shows a request sent using Postman.

7.3.3.1.1. Request URL

```
POST https://10.41.14.69:8746/haloengine-server/halosdk/GetMetaDataTypes
```

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 "Custom metadata" section.

7.3.3.1.2. Request

The request is sent in the Body-JSON format with the following parameters.

1. **customerId** – Customer ID used by HaloENGINE. Note: `halo_customer` is the default Customer ID in the HaloENGINE Admin Portal and must be used as a mandatory parameter in API requests without modification. Any mismatch in the Customer ID results in an error.
2. **systemId** – Unique system ID of the client system.
3. **systemType** – Type of the client system.

Example

```
{
    "customerId": "halo_customer",
    "systemId": "API_customer",
    "systemType": "HaloENGINE_API"
}
```

7.3.3.1.3. Response

A successful request returns the following information:

- **Status Code:** 200
- **Response Body:** Plain text containing the configured metadata [`user_group, work_in_progress, folder, review, release, file_name, user_name, file_type, project`].

7.3.4. Get Action

Description: Determines the action (monitor, encrypt, or decrypt) based on the provided inputs.

Request method: POST

There are three options in "Owner Configuration": Service (default), Static email, and User. You can set it up on the HaloENGINE admin portal. Note: For 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".

7.3.4.1. Request Example

The following example shows a request sent using Postman.

7.3.4.1.1. Request URL

```
POST https://10.41.14.69:8746/haloengine-server/halosdk/GetActionFormRest
```

7.3.4.1.2. Request

The request is sent in the Body-JSON format with the following parameters.

1. **customerId** – Customer ID used by HaloENGINE.
2. **systemId** – Unique ID of the client system.
3. **systemType** – Type of the client system.
4. Example values `user_name`, `file_type`, and `file_name`.

Example

```
{
  "customerIdentification": {
    "customerId": "halo_customer",
    "systemId": "API_customer",
    "systemType": "HaloENGINE_API"
  },
  "metadata": {
  "simpleValue": {
    "user_name": ["john"],
    "file_type": ["docx"],
    "file_name": ["BOM.docx"]
  }
}
}
```

7.3.4.1.3. Response

A successful request returns the following information:

- **Status Code:** 200
- **Response Body:** A successful request returns a JSON response with the following structure:


```
{
    "simMode": false,
    "labelVendor": "NONE",
    "action": {
        "value": [
            "LABEL",
            "AUDIT"
        ]
    },
    "authorMode": {
        "userEmailNeeded": false,
        "staticEmail": ""
    },
    "classification": "
<?xml version=\"1.0\" encoding=\"UTF-8\" standalone=\"yes\"?>\n
<classification version=\"1.0\">\n
    <class name=\"Default\">\n
        <displayNames>\n
            <displayName locale=\"en_US\" name=\"Default\"/>\n
        </displayNames>\n
        <properties>\n
            <property name=\"Sensitivity\" dataType=\"listValue\">\n
                <displayNames>\n
                    <displayName locale=\"en_US\" name=\"Sensitivity\"/>\n
                </displayNames>\n
                <values>\n
                    <listValue name=\"Secret\">\n
                        <displayNames>\n
                            <displayName locale=\"en_US\" name=\"Secret\"/>\n
                        </displayNames>\n
                    </listValue>\n
                </values>\n
            </property>\n
        </properties>\n
    </class>\n
</classification>\n",
    "template": {
        "guid": "99f1473d-74f4-47ca-9843-e735f94fa797",
```

```
        "templateName": "HCAD Secret"
    }
}
```

The response varies based on the **Owner Configuration** setting:

- **Service** → `"userEmailNeeded": false`, `"staticEmail": ""`
- **Static email** → `"userEmailNeeded": false`, `"staticEmail": "john@halosecude.onmicrosoft.com"`
- **User** → `"userEmailNeeded": true`, `"staticEmail": ""`

7.3.5. Encrypt File

Description: Executes the encrypt action.

Request method: POST

7.3.5.1. Request Example

The following example shows a request sent using Postman.

7.3.5.1.1. Request URL

```
POST https://10.41.14.69:8746/haloengine-server/halosdk/encryptFile
```

7.3.5.1.2. Request

The request is sent in the Body-JSON format with the following parameters.

Key: `file` (File as Type). Browse and select the required file.

Description: File to be encrypted.

Example

```
BOM.txt
```

Key (Optional): `authorEmailId` (Text as Type)

Description: Email address of the document owner. Note: When an email address is provided, the user is assigned owner permissions. If no email address is provided, the service principal ID is assigned as the owner.

Example

```
john@halosecude.onmicrosoft.com
```

Key: `labelId` (Text as Type)

Description: GUID of the template.

Example

```
99f1473d-74f4-47ca-9843-e735f94fa797
```

Key: `type` (Text as Type).

Description: Labeling type. Supported values:

- LABELING
- COMPOUNDFILELABELING

Example

```
LABELING
```

Key: `additionalParam` (Text as Type).

Description: Required when the **COMPOUNDFILELABELING** type is used. Provide the compound file details in JSON format.

Example

```
{"compoundid":"compound123"}
```

7.3.5.1.3. Response

A successful request returns the following information:

- **Status Code:** 200
- **Response Body:** A successful request returns a JSON response with the following structure:

```
{
    "success": true,
    "message": "File encrypted successfully",
    "fileName": "BOM.ptxt",
    "fileType": "ptxt",
    "content": "The encrypted content is displayed."
}
```

7.3.6. Decrypt File

Description: Decrypts an encrypted file.

Request method: POST

7.3.6.1. Request Example

The following example shows a request sent using Postman.

7.3.6.1.1. Request URL

```
POST https://10.41.14.69:8746/haloengine-server/halosdk/decryptFile
```

7.3.6.1.2. Request

The request is sent in the Body-JSON format with the following parameters.

Key: `file` (File as Type). Browse and select the required file.

Description: Encrypted file to be decrypted.

Example

```
BOM.rtf.pfile
```

7.3.6.1.3. Response

A successful request returns the following information:

- **Status Code:** 200
- **Response Body:** A successful request returns a JSON response with the following structure:

```
{
    "success": true,
    "message": "File decrypted successfully",
    "fileName": "BOM.rtf",
    "fileType": "rtf",
    "content": "The decrypted content is displayed."
    "templateID": "99f1473d-74f4-47ca-9843-e735f94fa797"

}
```

7.3.7. Send PLM Monitor Log Data

Description: Accepts monitoring logs for auditing.

Request method: POST

7.3.7.1. Request Example

The following example shows a request sent using Postman.

7.3.7.1.1. Request URL

```
POST https://10.41.14.69:8746/haloengine-server/halosdk/SendPLMMonitorLogData
```

7.3.7.1.2. Request

The request is sent in the Body-JSON format with the following parameters.

- **customerId** – Customer ID used by HaloENGINE.
- **systemId** – Unique ID of the client system.
- **systemType** – Type of the client system.

The request body may also include additional fields, such as:

- **logInfo** – Details about the log event.
- **userInfo** – Information about the user who triggered the event.
- **fileInfo** – Metadata about the file involved in the action.
- **resultedDecision** – Final decision returned by HaloENGINE.

Example


```
{
  "customerIdentification": {
    "customerId": "halo_customer",
    "systemId": "API_customer",
    "systemType": "HaloENGINE_API"
  },
  "logInfo": {
    "utcTimeStamp": "2021-02-23T23:01:00+05:00",
    "timeZone": "+5",
    "logID": "sjkfsdfsd"
  },
  "userInfo": {
    "userName": "john",
    "userType": "DEV",
    "userEmail": "john@techuyt.com"
  },
  "fileInfo": {
    "fileName": "partrocket.asm",
    "filePath": "C:\\",
    "fileType": "asm",
    "fileProtectedBefore": false,
    "sizeOriginal": 4355675,
    "sizeDownload": 67848
  },
  "resultedDecision": {
    "fileBlocked": false,
    "fileLabeled": false,
    "fileProtected": false,
```

```
    "unprotected": true,
    "unlabeled": true,
    "fileBlockedByRule": false,
    "policyName": "HCAD Secret",
    "policyId": "1234",
    "classification": {
      "byUser": "<?xml version=\"1.0\" encoding=\"UTF-8\"?><classification
version=\"1.0\">...</classification>",
      "bySystem": "<?xml version=\"1.0\" encoding=\"UTF-8\"?><classification
version=\"1.0\">...</classification>"
    },
    "abortedBySystem": false,
    "abortedByUser": false,
    "error": false,
    "simMode": false,
    "extendedTags": [
      {
        "key": "Key1",
        "value": "Value1"
      }
    ]
  },
  "plmContextInfo": {
    "eventType": "user download",
    "browserClient": "true",
    "preProcessInfo": [
      {
        "type": "Testing",
        "key": "ABC",
        "value": "12345"
      }
    ],
    "attributes": [
      {
        "type": "Attr1",
        "key": "user_name",
        "value": "sjohn"
      }
    ],
    "documentId": "1222",
    "documentNumber": "222",
    "documentType": "1",
    "documentPart": "j",
    "documentVersion": "00",
```

```
      "viewOnly": false,
      "dmsProcess": false
    },
    "plmDestInfo": {
      "destinationAttributes": [
        {
          "type": "Dest",
          "key": "XYZ",
          "value": "123"
        }
      ],
      "browser": "IE",
      "hostname": "ABC",
      "ipaddress": "10.91.0.1",
      "operatingSystem": "WIN10"
    }
  }
```

7.3.7.1.3. Response

A successful request returns the following information:

- **Status Code:** 200
- **Response Body:** The response body returns the boolean value **true**, represented as plain text.

7.4. 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	Sample error messages: 1. The monitor feature is not enabled. 2. Action rules were not initialized correctly. Check configurations. 3. Invalid or Inactive profile or invalid system ID. 4. System ID does not exist.	1. The Monitor feature is not enabled in the portal. 2. Action rules are not initialized correctly. 3. Invalid or inactive profile, or invalid system ID entered. 4. System ID is invalid.

Status Code	Sample Message	Description
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

8. Troubleshooting

This page will help you through the most common problems that may arise during the installation and configuration of the HaloENGINE, which are described below.

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.

8.1. 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.

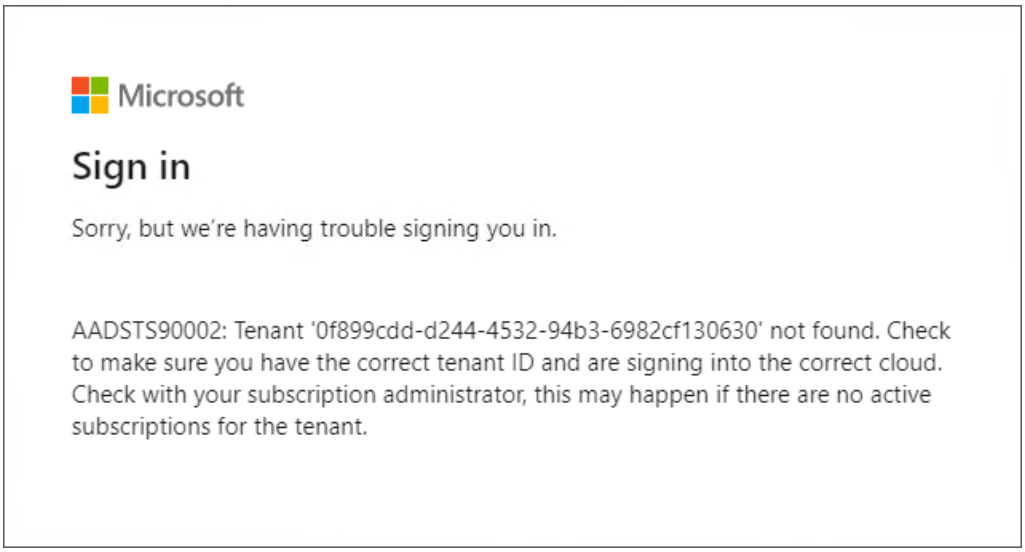
Recommended Action

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.

8.2. 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

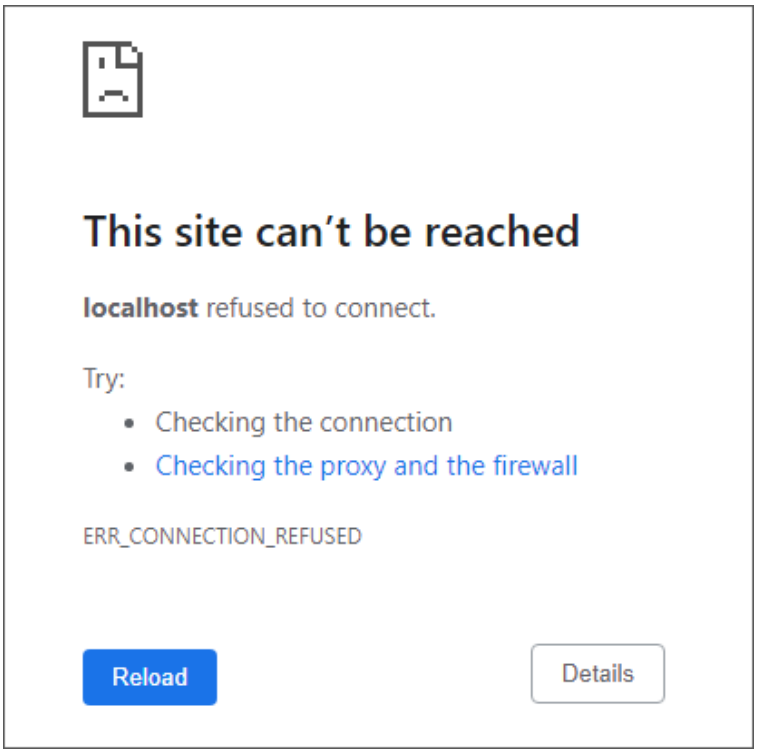
The Tenant ID/Client ID you entered on the *User Domain-Tenant Configuration* page is either incomplete or incorrect.

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.

8.3. Unable to Load the Admin Portal

Symptoms



Error message

The above error message appears in the browser when attempting to open the HaloENGINE Admin Portal using 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.

8.4. Unable to load the Admin Portal or PDM Client could not connect to HaloENGINE

Symptoms

1. Error message occurs in the browser when opening the HaloENGINE Admin Portal.
2. HaloCAD for SOLIDWORKS PDM client cannot connect to HaloENGINE.

Background

The error mentioned above occurs when the admin portal is attempted to open via `https://[server_IP]:8746/haloengine-admin/` but does not open. When a client tries 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"
```

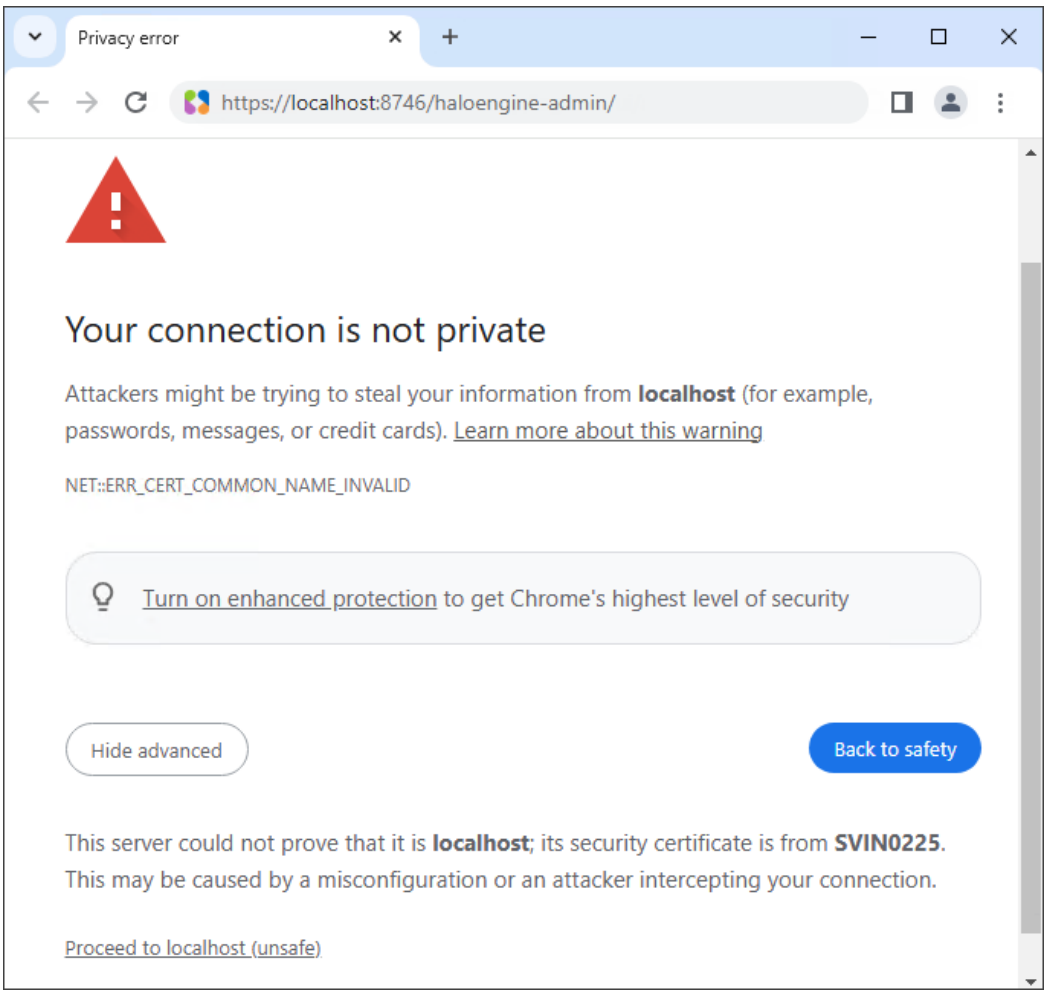
```
            wsdlLocation="WEB-INF/haloengine-server-monitor.wsdl" address="/monitor"
            publishedEndpointUrl = "https://19.41.14.188:8746/haloengine-
    server/monitor" />

        <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.

8.5. 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/`.

8.6. 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>`".

8.7. 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 no Action/Classification rules are configured under Download Rules.
3. **Case 3:** If the HaloENGINE Tomcat Service stops unexpectedly.
4. **Case 4**: If the certificate used by the HaloENGINE has expired.
5. **Case 5:** If the System Unique ID on the Admin Portal does not match the System ID on the client system.

Recommended Action

1. **Case 1**: Check that the **Classification Engine** is turned on.
2. **Case 2**: Make sure to include an appropriate classification rule, followed by a suitable action rule.
3. **Case 3**: Check that the HaloENGINE is running; if not, restart it manually.
4. **Case 4**: Make sure to upload the same valid certificate that is already installed on the Windows Server machine where the HaloENGINE is installed.
5. **Case 5:** 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.
6. Re-try downloading now.

8.8. Dashboard Fails to Load

Symptoms

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.

9. Technical Support

Before contacting Technical Support, ensure that you have the following information available.
Providing this information helps the support team investigate and resolve your issue more efficiently.

- Full contact details
- Product build version
- Date, time, and description of the error (include screenshots, if possible)
- Details of any third-party software used with the product
- Any additional information required to reproduce the issue

Contact Technical Support

Secude provides technical support through email support@secude.com. When contacting Technical Support by email, include your company details, a detailed description of the issue, and the relevant log files (if available). A support representative will respond to your inquiry.

Additional Resources

Visit the Secude website https://secude.com to learn about upcoming events, press releases, and to download white papers.

Documentation Feedback

Secude values your feedback and continuously strives to improve product documentation. To provide feedback, send an email to: documentation@secude.com
Include the following details in your feedback:

- Product name and version
- Documentation topic
- Description of the suggestion or error

The technical documentation team reviews all feedback and incorporates relevant updates in future documentation releases.

10. Appendix

This section contains supplementary information.

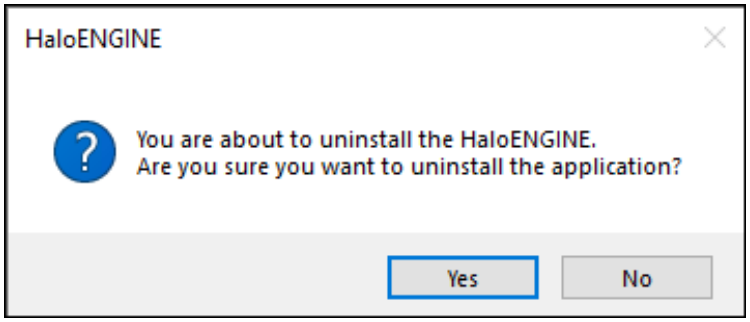
10.1. Uninstalling the HaloENGINE

Before uninstalling, ensure that you export the current configuration. The exported configuration file can be imported during reinstallation to retain existing settings, reduce configuration effort, and minimize the risk of misconfigurations or errors.

Method #1

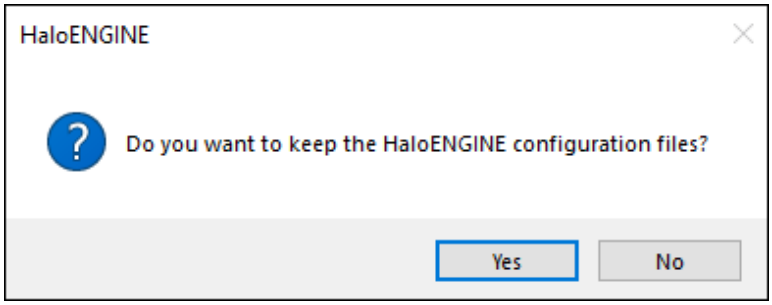
When you no longer use the service, you may uninstall the application. Uninstalling removes all files and registry settings that were added to your computer during the initial installation.

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 appears:



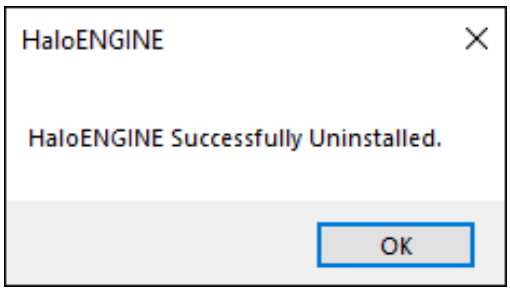
Uninstall message #1

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
   ```

10.2. Metadata Definition

The following section provides a table of built-in metadata for PLM and PDM clients.

10.2.1. Windchill

The table below lists the Windchill metadata available in the HaloENGINE.

Windchill metadata	Use
server_name	Derivation from server name (FQDN of the Windchill server). (For example, `svin0007.secude.local`)
user_name	Derivation from Windchill logged-in users. (For example, John and Derek)
file_name	Derivation from the file name.

Windchill metadata	Use
project_name	Derivation from the project name. (For example, Windchill)
product_name	Derivation from product name (For example, Windchill).
lifecycle_template	Derivation from the lifecycle of a file. Lifecycle provides an overview of how business items develop and serves as a model for the commercialization process. The lifecycle templates may be of the following types: Approval, Basic, Default, and so on. (For example, `Pipeline.prt` - Default)
user_role	Derivation from the user role. (For example, Designer and Engineer)
lifecycle_state	Derivation from the lifecycle of a file. Each phase of a lifecycle template is associated with a lifecycle state. There are different kinds of lifecycle states. 1. Approval (template): In work, under review, approved (states) 2. Basic (template): Basic: In work, released, canceled (states) 3. Default (template): Default: In work, under review, released (states) (For example, `Pipeline.prt`- Default-released)
security_label	Derivation from Windchill access control policy. For more details, please refer to the online PTC Windchill documentation. (For example, Export Control, Corporate Proprietary, and Third Party Proprietary)
file_type	Derivation from file type (Creo file types and MS Office native file types). (For example, sec, prt, asm, xlsx)

Windchill metadata	Use
library_name	Derivation from the library name. (For example, Density, Wheel, and Pipeline)
workspace_name	Derivation from workspace. (For example, Generic_computer and Drive System)
system_context	Derivation from the origin of the data. (For example, Generic_computer, and Drive System)
preexpression_custom_pre-expression	Derivation from custom pre-expression. 1. Yes 2. No

Windchill metadata

10.2.2. Teamcenter

The table below lists the Teamcenter metadata available in the HaloENGINE.

Teamcenter metadata	Use
user_role	Derivation from the user role. Multiple roles may be assigned to a single user. (For example, Designer and Engineer)
user_def_group	Derivation from a group of users who log in. (For example, a user from the Engineering group)
gov_clearance	Derivation from a specific object based on value or licensing value. (For example, secret - single value field)
ip_clearance	Derivation from intellectual property (IP) classification values and clearance levels assigned to data objects and users for IP access evaluation. (For example, super-secret - single value field)
user_name	Derivation from Teamcenter logged-in users.

Teamcenter metadata	Use
	(For example, John and Derek)
file_type	Derivation from file type and Teamcenter object data. (NX file types and MS Office native file types) (For example, prt, asm, and XLSX)
gov_classification	Derivation from a Teamcenter object based on its value or license value. (For example, secret - single value field)
obj_project_names	Derivation from Teamcenter object data. The object could be used in several projects. (For example, project1; project2- multi-value- field)
ip_classification	Derivation from Teamcenter's intellectual property (IP). (For example, secret, internal, and confidential - single value field)
preexpression_custom_pre-expression	Derivation from custom pre-expression. Yes No

Teamcenter metadata

10.2.3. Autodesk Vault

The table below lists the Autodesk Vault metadata available in the HaloENGINE.

Autodesk Vault Metadata	Use
lifecycle_state	Derivation from the lifecycle of Autodesk Vault data. (For example, work-in-progress, review, and released)
file_type	Derivation from file type. File types of AutoCAD, Inventor, and MS Office native file types. (For example, `dwg`, `ipt`, and `iam`)

Autodesk Vault Metadata	Use
folder_name	Derivation from the folder name in the Autodesk Vault server. (For example, `$/DESIGNS/INVENTOR FILES/Jet Engine Model/Workspace/Design Accelerator`)
preexpression_custom_pre-expression	Derivation from custom pre-expression. 1. Yes 2. No

Autodesk Vault metadata

10.2.4. SOLIDWORKS PDM

The table below lists the SOLIDWORKS PDM metadata available in the HaloENGINE.

SOLIDWORKS PDM Metadata	Use
author_name	Derivation from the Web2 client interface Items author.
domain_name	Derivation from the network domain name associated with the current user. (For example, `SZVLU100.com`)
file_type	Derivation from file type. File types of SOLIDWORKS.
user_name	Derivation from machine logged-on user. (For example, John and Derek)
client_hostname	Derivation from the computer where SOLIDWORKS PDM is installed. (For example, `SZVLU100.com`)
current_state	Derivation from the file's status as set in SOLIDWORKS PDM. (For example, Approved and Waiting for approval)
project_name	The name of the project from which the saved file is derived. (For example, CMS Turbo Engine)
ad_group	Derivation from the domain groups. (For example, Domain Users and Superusers)

SOLIDWORKS PDM Metadata	Use
folder_path	Derivation from folder name in SOLIDWORKS PDM server. (For example, `C:/<Folder>`). Please note that files cannot be encrypted if the folder name (`folder_path`) is specified with a backslash "****", such as `C:\folder1\folder2`. Therefore, it is advised to configure with a forward slash "**/**", such as `C:/folder1/folder2`.
preexpression_custom_pre-expression	Derivation from custom pre-expression 1. Yes 2. No

SOLIDWORKS PDM metadata

10.3. Third-Party Libraries

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
jakarta.xml.bind:jakarta.xml.bind-api	3.0.1	https://mvnrepository.com/artifact/jakarta.xml.bind/jakarta.xml.bind-api/3.0.1	CDDL-1.0	https://javaee.github.io/glassfish/LICENSE
jakarta.xml.ws:jakarta.xml.ws-api	3.0.1	https://mvnrepository.com/artifact/jakarta.xml.ws/jakarta.xml.ws-api/3.0.1	CDDL-1.0	https://javaee.github.io/glassfish/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

Library	Version	Source Code	License Name	License Link
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	2.0.+	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
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

Library	Version	Source Code	License Name	License Link
ch.qos.logback:logback-classic	1.5.18	https://github.com/qos-ch/logback	LGPL 2.1	https://github.com/qos-ch/logback/blob/master/LICENSE.txt
ch.qos.logback:logback-core	1.5.18	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
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

Library	Version	Source Code	License Name	License Link
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

Library	Version	Source Code	License Name	License Link
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
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
org.apache.cxf:cxf-rt-frontend-jaxws	4.0.8	https://github.com/apache/cxf	Apache 2.0	https://github.com/apache/cxf/blob/master/LICENSE

Library	Version	Source Code	License Name	License Link
org.apache.cxf:cxf-rt-rs-security-cors	4.0.8	https://github.com/apache/cxf	Apache 2.0	https://github.com/apache/cxf/blob/master/LICENSE
org.apache.cxf:cxf-rt-ws-rm	4.0.8	https://github.com/apache/cxf	Apache 2.0	https://github.com/apache/cxf/blob/master/LICENSE
org.springframework:spring-context	6.2.7	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
org.springframework:spring-web	6.2.7	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

Library	Version	Source Code	License Name	License Link
org.springframework.boot:spring-boot-starter-web	3.3.12	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	3.3.12	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	1.0.10 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

Library	Version	Source Code	License Name	License Link
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
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	3.3.12	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	3.3.12	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

Library	Version	Source Code	License Name	License Link
org.springframework.hateoas:spring-hateoas	2.5.0	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
org.springframework.boot:spring-boot-starter-oauth2-resource-server	6.2.7	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

Library	Version	Source Code	License Name	License Link
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	6.4.6	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.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	10.1.52	https://github.com/apache/tomcat	Apache 2.0	https://github.com/apache/tomcat/blob/main/LICENSE

Library	Version	Source Code	License Name	License Link
Java	21	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		
MIP SDK	1.18.103	https://learn.microsoft.com/en-us/information-protection/develop/version-release-history The MIP SDK is publicly available for integration, but is not open source. It is provided by Microsoft under proprietary licensing terms.	https://docs.microsoft.com/en-us/information-protection/develop/	MIP SDK
MSAL	4.73.1	https://github.com/AzureAD/microsoft-authentication-library-for-dotnet	https://github.com/AzureAD/microsoft-authentication-library-for-dotnet/blob/master/LICENSE	MSAL
Spdlog	1.17.0		https://github.com/gabime/spdlog	Spdlog

Third-party libraries

Index

R

S

T

W

Secude

www.secude.com

About Secude

Secude, a trusted Microsoft and Siemens Digital Industries Software partner, is a global leader in Zero Trust data protection and data governance.

Our solutions extend Microsoft Purview Information Protection (MPIP) to secure sensitive files—including CAD and PLM assets—from the moment of creation. By embedding persistent protection and access controls directly into design and engineering data, we help enterprises prevent Intellectual Property (IP) theft, data leakage, reputational damage, and compliance risks. With operations in Europe, North America, and Asia, Secude supports global manufacturers, defense contractors, and AEC firms in implementing robust IT security strategies across the product lifecycle and digital supply chain.