Secude

HaloENGINE

Installation and Configuration Manual

Version 1.0

Copyright

© 2025-2026 Secude Solutions AG. All Rights Reserved.

This Secude-branded software and its corresponding documentation are the exclusive property of Secude Solutions AG of Luzern, Switzerland and are protected under the various copyright laws around the world and by various other intellectual property laws. The use of this software and/or its documentation and any copying thereof by end users is subject to the terms of a license agreement with Secude Solutions AG. The wrongful use or copying of this software and/or documentation subjects infringers to both criminal and civil liabilities.

ANY USE, COPYING, REPRODUCTION, ALTERATION, TRANSMISSION, OR TRANSLATION OF THESE MATERIALS, IN WHOLE OR IN PART, IN ANY FORM OR BY ANY MEANS, IS STRICTLY PROHIBITED WITHOUT THE PRIOR WRITTEN PERMISSION OF SECUDE SOLUTIONS AG. IF THIS MATERIAL IS PROVIDED WITH SOFTWARE LICENSED BY SECUDE, THE INFORMATION HEREIN IS PROVIDED SUBJECT TO THE TERMS OF THE WARRANTY PROVIDED WITH THE PRODUCT LICENSE. IF THIS MATERIAL IS NOT PROVIDED WITH LICENSED SOFTWARE, THE INFORMATION HEREIN IS PROVIDED “AS IS” WITHOUT WARRANTY OF ANY KIND. IN EITHER CASE, THERE ARE NO OTHER WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT, OR QUALITY. IN NO EVENT SHALL SECUDE SOLUTIONS AG OR ANY OF ITS AFFILIATES BE LIABLE FOR ANY DIRECT OR INDIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL, PUNITIVE, OR EXEMPLARY DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE MATERIALS AND/OR INFORMATION CONTAINED HEREIN. Some jurisdictions do not allow the exclusion of implied warranties, so the above exclusion may not apply to you.

Secude Solutions AG takes reasonable measures to ensure the quality of the data and other information produced herein. However, these materials may contain technical inaccuracies or typographical errors, and are not guaranteed to be error-free. Information may be changed or updated without notice. Secude Solutions AG has no obligation to update these materials based on changes to its products or services or those of third parties. Secude Solutions AG may also make improvements or changes to the products or services described in this information at any time without notice. Secude Solutions AG frequently releases new versions and updates to its software, and therefore images shown in this document may be slightly different from what you see on screen.

As with any security product, Secude Solutions AG highly recommends the back up of data as well as passwords on a regular basis. Secude Solutions AG is not responsible for the loss of passwords or data that cannot be retrieved based upon a user’s failure to adhere to stringent backup and safe-keeping conventions.

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

1. INTRODUCTION 1

1.1. About this Manual 2

1.2. Terminology 2

2. QUICK START INSTALLATION 5

3. SYSTEM REQUIREMENTS 8

4. PREREQUISITES 9

4.1. Register an Application in Microsoft Entra ID 9

4.1.1. Create an Application 10

4.1.2. Add Required Permissions 12

4.1.3. Upload the Certificate 17

4.2. Office 365 Subscription Details 18

4.2.1. Create and Configure Sensitivity Labels 18

4.2.2. Recommended URLs, Addresses, and Ports for MPIP 19

4.2.3. Enable TLS 1.2 for Microsoft Entra ID Authentication 20

4.3. Configure Microsoft Entra ID for User Management 21

4.3.1. Step 1: Create a New Web Application 21

4.3.2. Step 2: Authentication Settings 22

4.3.3. Step 3: Certificates & Secrets 23

4.3.4. Step 4: Token Settings 24

4.3.5. Step 5: Expose API 25

4.3.6. Step 6: Create Roles 26

4.3.7. Step 7: Apply Role to Users 28

4.4. Conditions for Running the HaloENGINE GenNXT Tomcat Service 31

4.4.1. Deny log on as a service policy 31

4.4.2. Prerequisites 31

4.5. Obtain the HaloENGINE GenNXT License 33

4.6. MPIP Authentication 33

4.7. Tomcat HTTPS Configuration 34

5. INSTALLING THE HALOENGINE GENNXT 37

5.1. Configuring the Tomcat Service 46

5.1.1. Configuration Tool 46

5.1.2. WinHTTP Proxy Settings 50
5.2. Initial Configuration of the HaloENGINE GenNXT Admin Portal 51
5.2.1. Welcome Page 51
5.2.2. Create an Administrator Account 52
5.2.3. Log in to the Admin Portal 53
5.2.4. Activate the License 54
5.2.5. Initial Dashboard View 55
5.2.6. Understand the Admin Portal UI Elements 56
5.3. Configuring HaloENGINE GenNXT 58
5.3.1. Configuration 58
5.3.2. Rules Configuration 67
5.3.3. Log Management 84
5.3.4. Security Settings 91
5.3.5. Dashboard 95
6. HALOENGINE GENNXT REST API 97
6.1. API Reference 99
6.1.1. Host/Base URL 99
6.1.2. Version 99
6.1.3. Get Metadata List 100
6.1.4. Get Action 102
6.1.5. Encrypt File 104
6.1.6. Decrypt File 105
6.1.7. Send PLM Monitor Log Data 106
6.2. Error Handling 108
7. TROUBLESHOOTING 109
7.1. Forgot your Admin Portal Password 109
7.2. Cannot Log in to Microsoft after Configuring the Tenant 110
7.3. Protection fails with ServiceDisabledError 111
7.4. Microsoft Login Fails 112
7.5. Error Shown on the Dashboard 113
8. TECHNICAL SUPPORT 114
9. APPENDIX 115
9.1. Classification Rule Use Cases 115
9.2. Sample Logs 116

9.3. Reset Administrator Password 119
9.4. Metadata Definition 120
9.4.1. Windchill 120
9.4.2. Teamcenter 121
9.4.3. Autodesk Vault 122
9.4.4. SOLIDWORKS PDM 124
9.5. Third-Party Libraries 125
9.6. Uninstalling the HaloENGINE GenNXT 136

Typographic Conventions

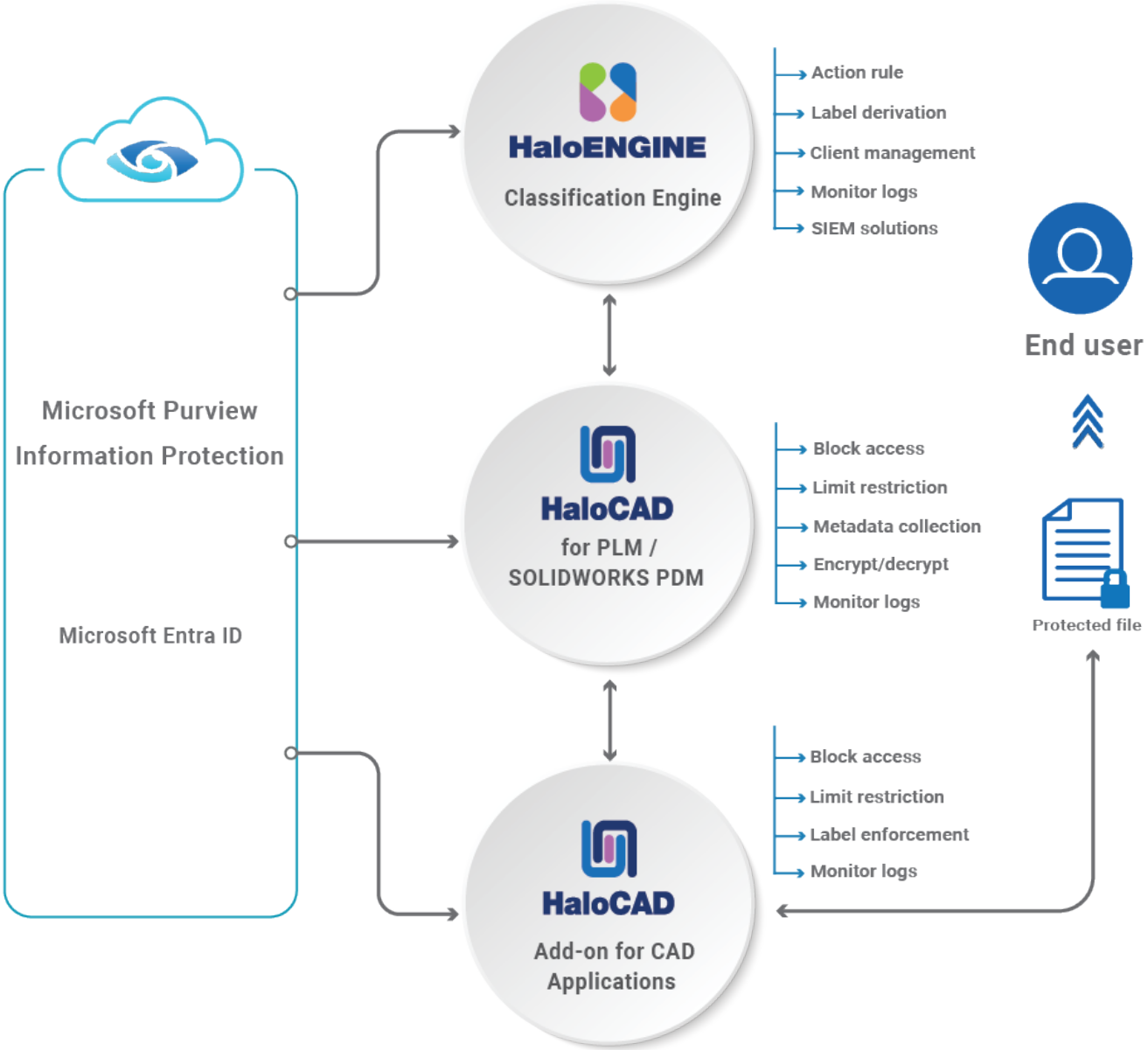
This guide uses the following typographic conventions to distinguish types of in-text information and icons to alert you to important information.

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 GenNXT is a Java-based classification engine that integrates with Microsoft Purview Information Protection (MPIP) to retrieve sensitivity labels for configuration in the Admin Portal. It evaluates file metadata against the configured classification rules and determines the applicable action and sensitivity label.

HaloENGINE GenNXT integrates with client applications to evaluate file metadata against the configured classification rules during the download process and determine the applicable action and sensitivity label. The client application uses the information returned by HaloENGINE GenNXT to perform the required file-processing action.



HaloENGINE GenNXT integrated with HaloCAD for PLM/PDM solution

HaloENGINE GenNXT Features

- **Business rule processing** – Evaluates configured rules and determines the appropriate action for each file.
- **Monitor logging** – Records all file upload and download activities, regardless of whether the files are protected.
- **SIEM integration** – Forwards audit events to a Security Information and Event Management (SIEM) platform.
- **Dashboard** – Provides a centralized view of file activity, including data movement through upload and download operations.

1.1. About this Manual

This manual describes the installation and configuration of the following components:

1. HaloENGINE GenNXT
2. HaloENGINE GenNXT API

1.2. Terminology

This section defines the key terms used throughout this manual. Familiarity with these terms will help you understand the concepts, procedures, and components described in the subsequent sections.

Term	Recommended Description
HaloENGINE GenNXT	Evaluates file metadata against configured classification rules and determines the applicable action and classification property.
HaloENGINE GenNXT Tomcat Service	A Windows service used by HaloENGINE GenNXT and HaloCAD components.
HaloENGINE GenNXT Admin Portal	The web-based administration interface used to configure classification schemas, profiles, rules, labels, monitoring, and system settings.
MPIP	Microsoft Purview Information Protection, Microsoft's information protection platform used to classify and protect files with sensitivity labels.

Term	Recommended Description
Sensitivity Label	A Microsoft Purview label that classifies content and applies protection settings, such as encryption and usage rights.
Classification Schema	Defines the classification properties and their values used to categorize an organization's data.
Property Name	Specifies the name of a classification property used to categorize an organization's data. This manual uses **Public**, **Internal**, **Confidential**, and **Secret** as example property names. You can define property names according to your organization's classification requirements.
Default Property	Defines the classification property applied when no classification rule matches.
Profile Name	Specifies the name of a profile that stores classification settings, schemas, and rules for a specific client.
Client Type	Identifies the type of client integrated with HaloENGINE GenNXT, such as Windchill, Teamcenter, Autodesk Vault, SOLIDWORKS PDM, or **HaloENGINE_API**.
Metadata	Information or properties associated with a file that can be used to evaluate a classification rule.
Pre-Expression	Defines a group of related metadata values used to evaluate a classification rule.
Classification Rule	A configurable rule that evaluates file metadata and determines the action to perform, such as **Block** or **Label**.
Condition	Specifies how the selected metadata is compared with the specified value.
Action	Specifies how HaloENGINE GenNXT processes the file when the rule conditions are met. The available actions are **Block** and **Label**.

Term	Recommended Description
Monitor	Records file upload and download activities without modifying the file.
Block	Prevents file upload or download based on the configured classification rule.
Label	Applies the selected MPIP sensitivity label to classify and protect the file according to the configured rule.
Fail-Safe Mode	Defines how file downloads are handled when an error occurs during file processing.
SIEM	A Security Information and Event Management solution used to collect, analyze, and monitor security events.

2. Quick Start Installation

Reference Manuals

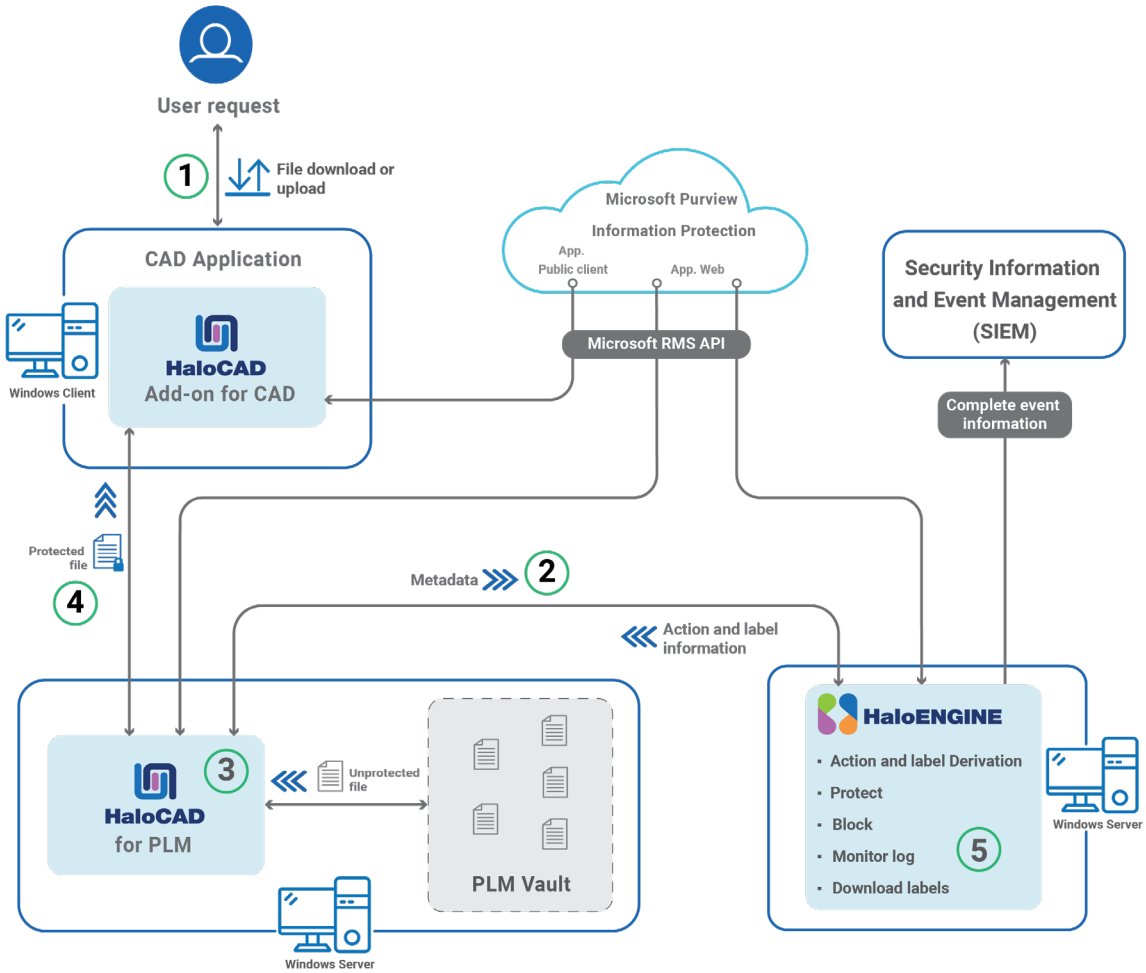
The table below describes where to find information for each step.

Component	Refer to
Step 1 – Install and configure HaloENGINE GenNXT	Refer to this manual.
Step 2 – Install HaloCAD for PLM/PDM	Refer to the corresponding HaloCAD for PLM/PDM Installation Manual.
Steps 3 and 4 – Protection and decryption workflow	Refer to the corresponding HaloCAD for PLM/PDM Operations Manual.

Reference Manuals

How it Works

HaloENGINE GenNXT supports multiple client types, including Windchill, Teamcenter, Autodesk Vault, and SOLIDWORKS PDM. The following steps illustrate the workflow between HaloCAD for PLM and HaloENGINE GenNXT.



Integration Workflow: HaloENGINE GenNXT and Client Applications

1. The user performs a check-out (download) or check-in (upload) operation. For SOLIDWORKS PDM, the user performs a copy or move operation.
2. HaloCAD for PLM retrieves the selected file and its associated metadata.
   a. HaloCAD for PLM sends the metadata to HaloENGINE GenNXT.
   b. HaloENGINE GenNXT identifies the client type and profile name and evaluates the configured classification and action rules.
   c. HaloENGINE GenNXT returns the appropriate action and sensitivity label to HaloCAD for PLM.
3. HaloCAD for PLM processes the file based on the returned action and configured policies.

- If no applicable action rule is configured, the file is downloaded without protection in **Fail-Safe (Tolerant)** mode.
- During check-out, HaloCAD for PLM applies the appropriate MPIP sensitivity label and protection to the file.
- During check-in, HaloCAD for PLM removes the applied protection before storing the file in the PLM repository.
- If a Block action is configured, HaloCAD for PLM prevents the file from being downloaded.

4. HaloCAD for PLM returns the processed file to the user.
5. HaloCAD for PLM records the operation details and forwards them to the HaloENGINE GenNXT Monitor log for auditing.

Note: For the HaloCAD for PDM workflow, refer to the corresponding HaloCAD for PDM Operations Manual. The PDM workflow differs from the PLM workflow.

3. 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	Microsoft Windows Server 2022 or later, with the latest operating system updates installed.
Database	Supports the latest version • MySQL - 8.0 and later • SQLite - Included with the installer • Microsoft SQL Server - 2019 and later, including SQL Server Express
Other Applications	• The HaloENGINE GenNXT Admin Portal supports the latest versions of Microsoft Edge, Google Chrome, and Mozilla Firefox. • Latest Windows Server versions may include a .NET Framework version by default. If .NET Framework 4.7.2 or later is not installed, install it before proceeding with the HaloENGINE GenNXT installation.

Requirements

4. Prerequisites

This chapter describes the prerequisites that must be completed before installing and configuring HaloENGINE GenNXT. Completing these tasks ensures that HaloENGINE GenNXT integrates correctly with your organization's Microsoft Purview Information Protection environment and security infrastructure. The following setup tasks are required:

1. Register an application in Microsoft Entra ID
2. Configure Microsoft Purview Information Protection prerequisites
   a. Create and configure sensitivity labels
   b. Configure the required MPIP endpoints and network ports
   c. Enable TLS 1.2 support on the client workstation for Microsoft Entra ID
3. Configure User Management Settings in Microsoft Entra ID
4. Verify the HaloENGINE GenNXT Tomcat Service runtime requirements
5. Obtain the HaloENGINE GenNXT license
6. Configure MPIP authentication
7. Tomcat HTTPS Configuration

Complete these prerequisites before starting the installation to ensure a smooth deployment and reliable HaloENGINE GenNXT operation.

4.1. Register an Application in Microsoft Entra ID

This section describes how to register an application in Microsoft Entra ID, obtain the **Application (client) ID** and **Directory (tenant) ID**, assign the required API permissions, and upload the certificate required for MPIP authentication.

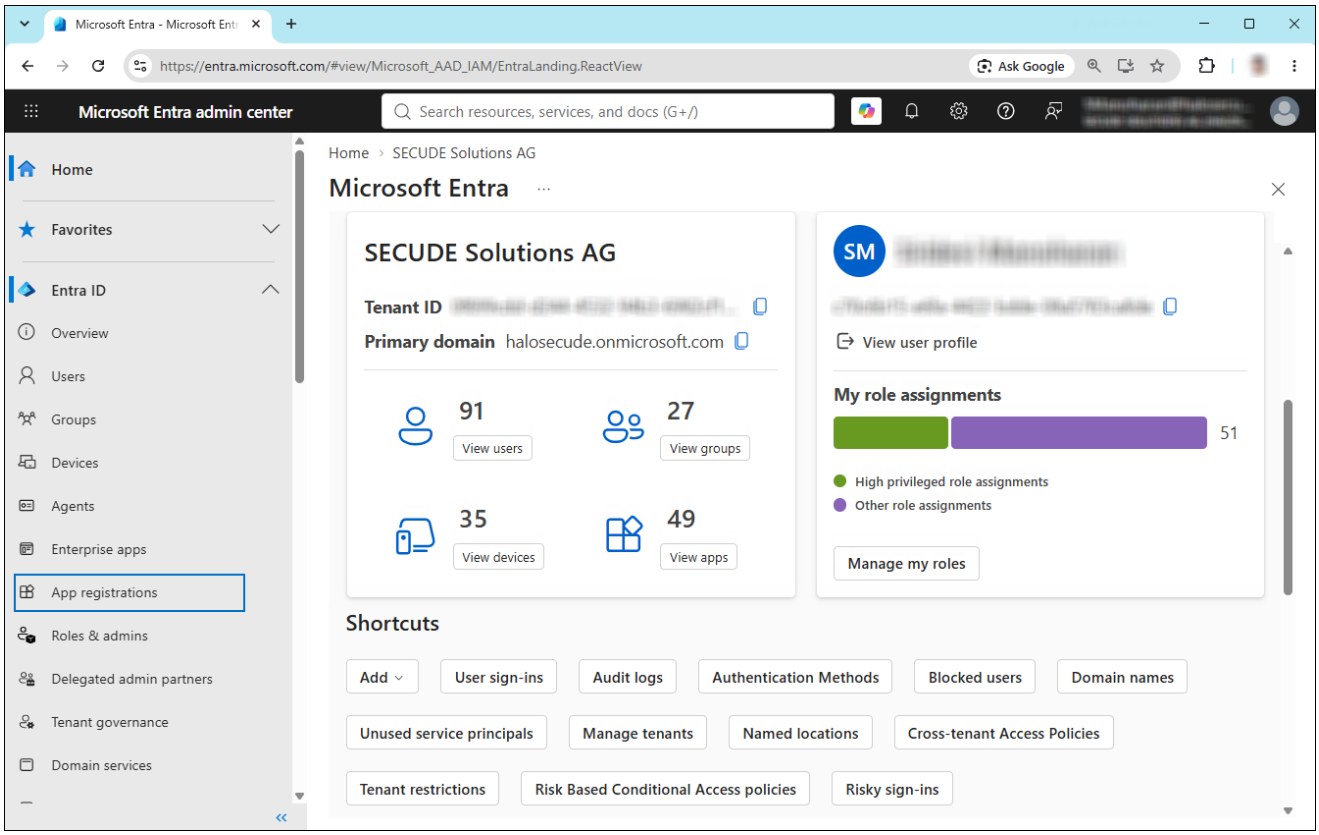
Microsoft documentation
Registering an application in Microsoft Entra ID establishes a trust connection between your application and the identity provider, the Microsoft identity platform. Microsoft documentation takes precedence over this section. Refer to the latest Microsoft documentation for updates.

Prerequisite: You must have sufficient administrative privileges to register an application in your Microsoft Entra ID tenant.

4.1.1. Create an Application

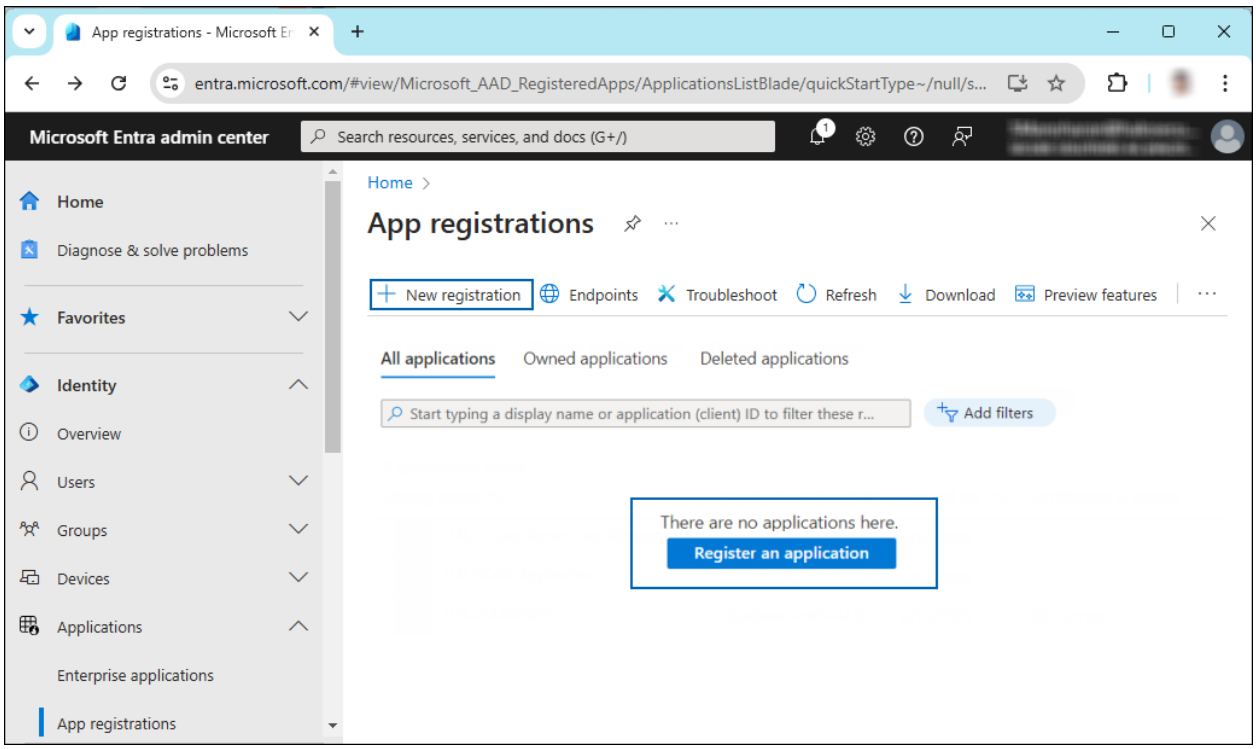
Follow these steps to register the application:

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. From **Directories + subscriptions**, select the tenant in which you want to register the application.
3. The application homepage opens.



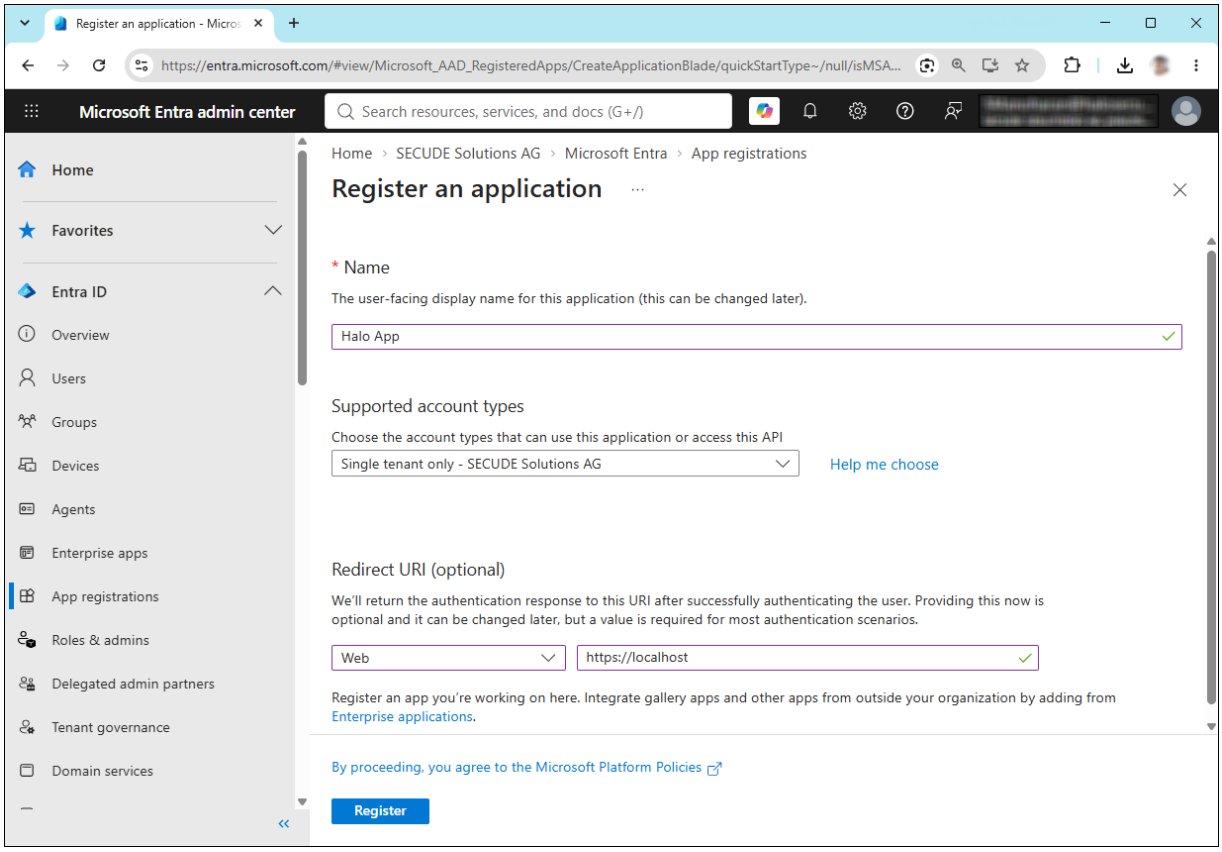
Selecting Microsoft Entra ID

4. In the left navigation pane, select **Entra ID** > **App registrations**.
5. On the **App registrations** page, click **New registration** or **Register an Application.** The **Register an Application** button appears only if no applications have already been created.



New application registration

6. On the **Register an application** page, configure the following:



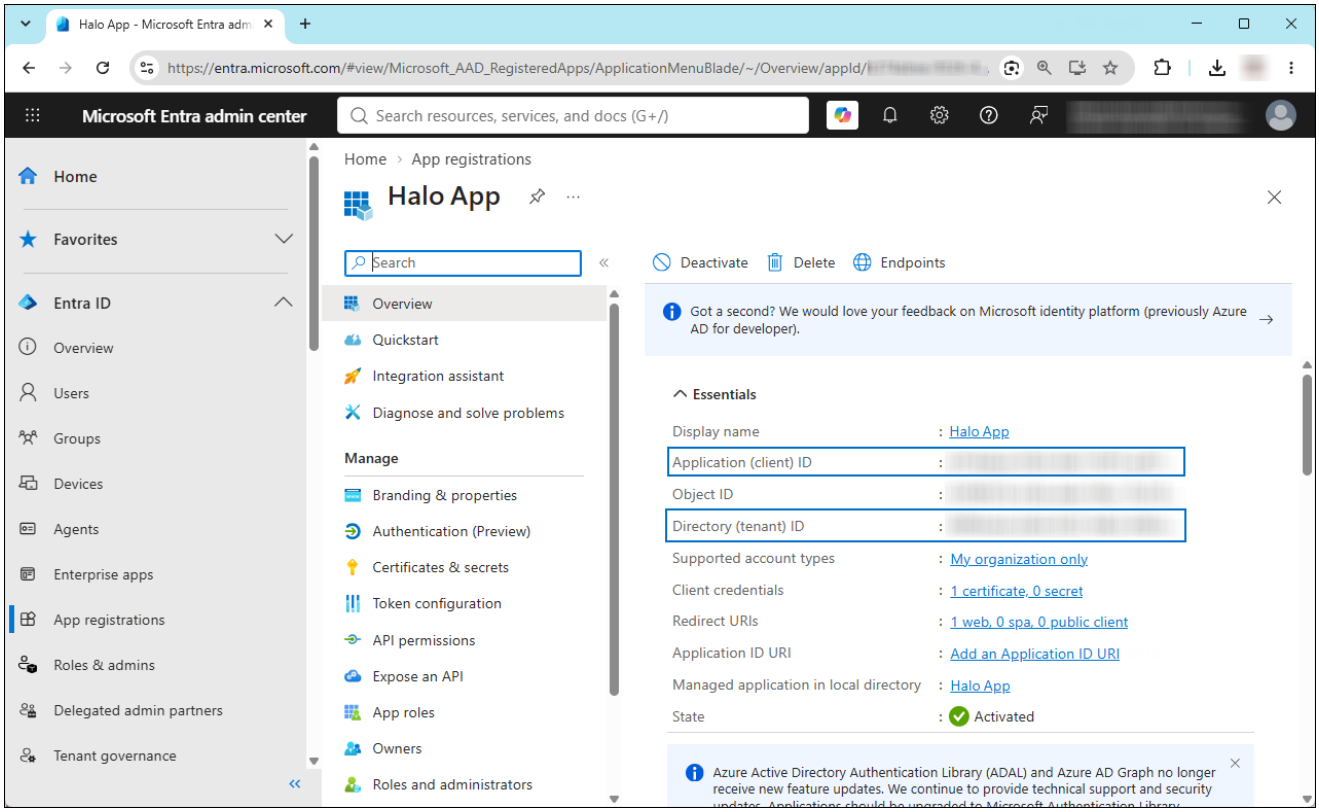
Application details

a. **Name:** Enter an appropriate name for the application.

b. **Supported account types:** Select **Single tenant only** from the list. HaloENGINE GenNXT currently supports only single-tenant applications.

c. **Redirect URI:** Select **Web** and enter a valid redirect URI. For example, `https://localhost`.

7. Click **Register**.
8. The Overview page of the newly registered application opens.



Application ID and Tenant ID

9. Once registration is complete, the portal displays the following values. 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

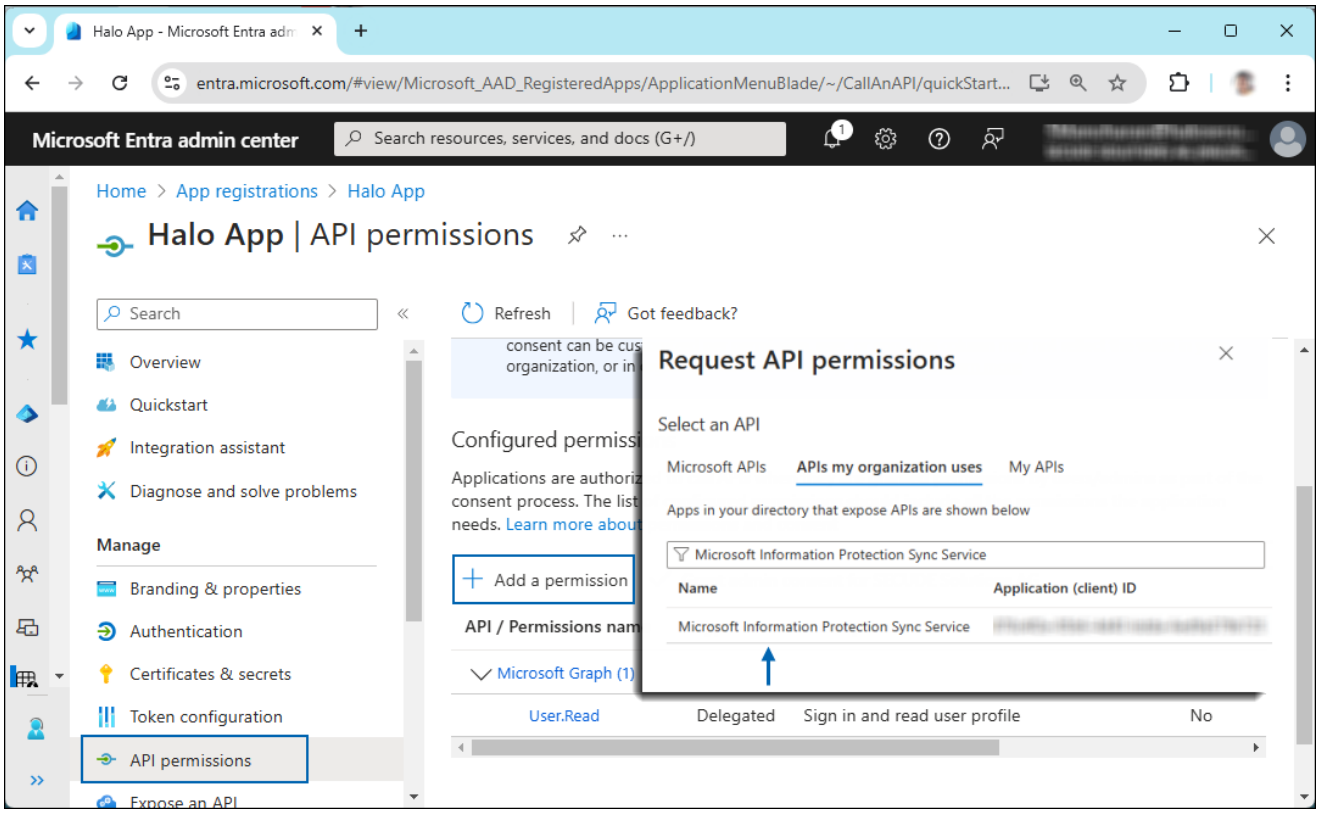
In a text editor (such as Notepad), copy the value of **Application (client) ID** and **Directory (tenant) ID**, and save them for configuring the HaloENGINE GenNXT Tomcat Service.

4.1.2. Add Required Permissions

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

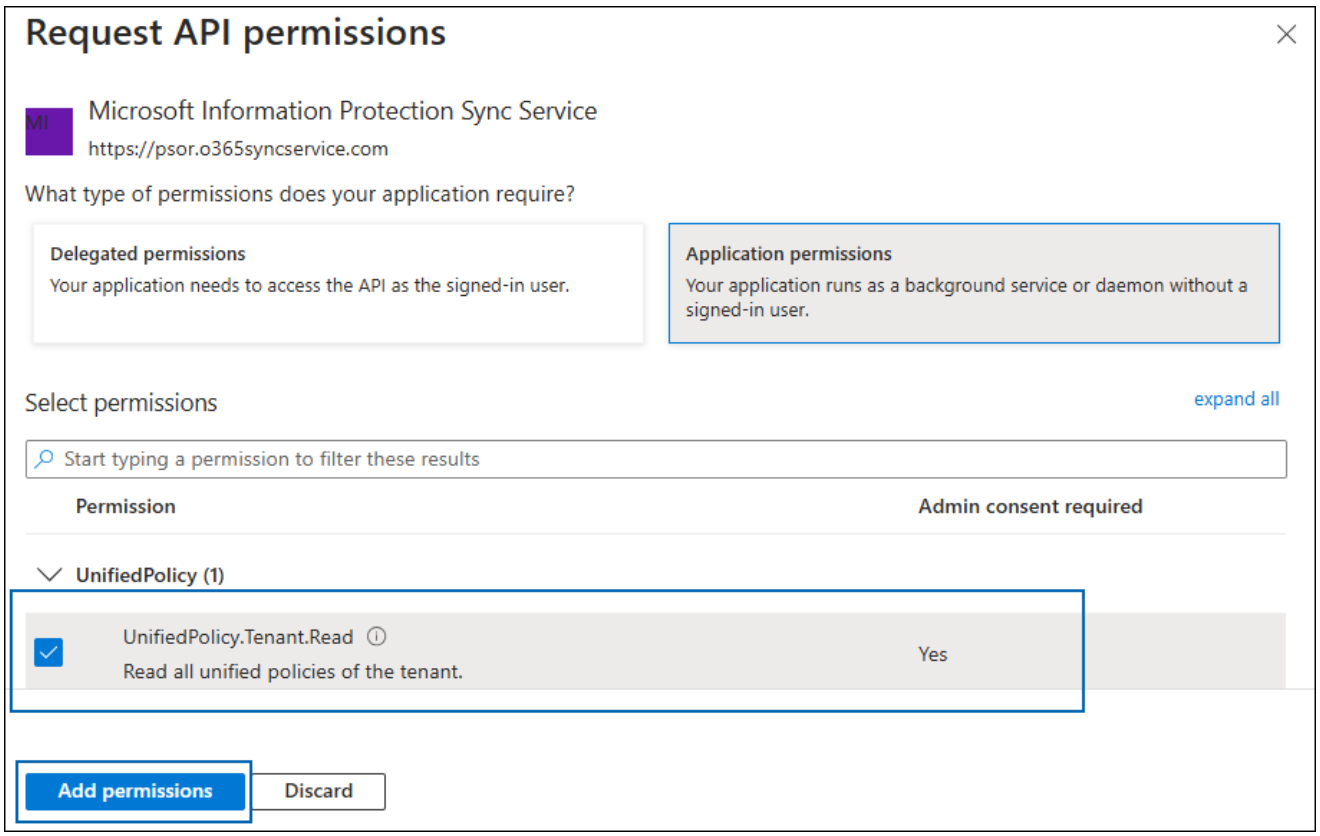
1. In the left navigation pane of the application, select **API permissions**.

2. Click **Add a permission**. 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, enter the name of the API listed in the Required API Permissions table. 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:



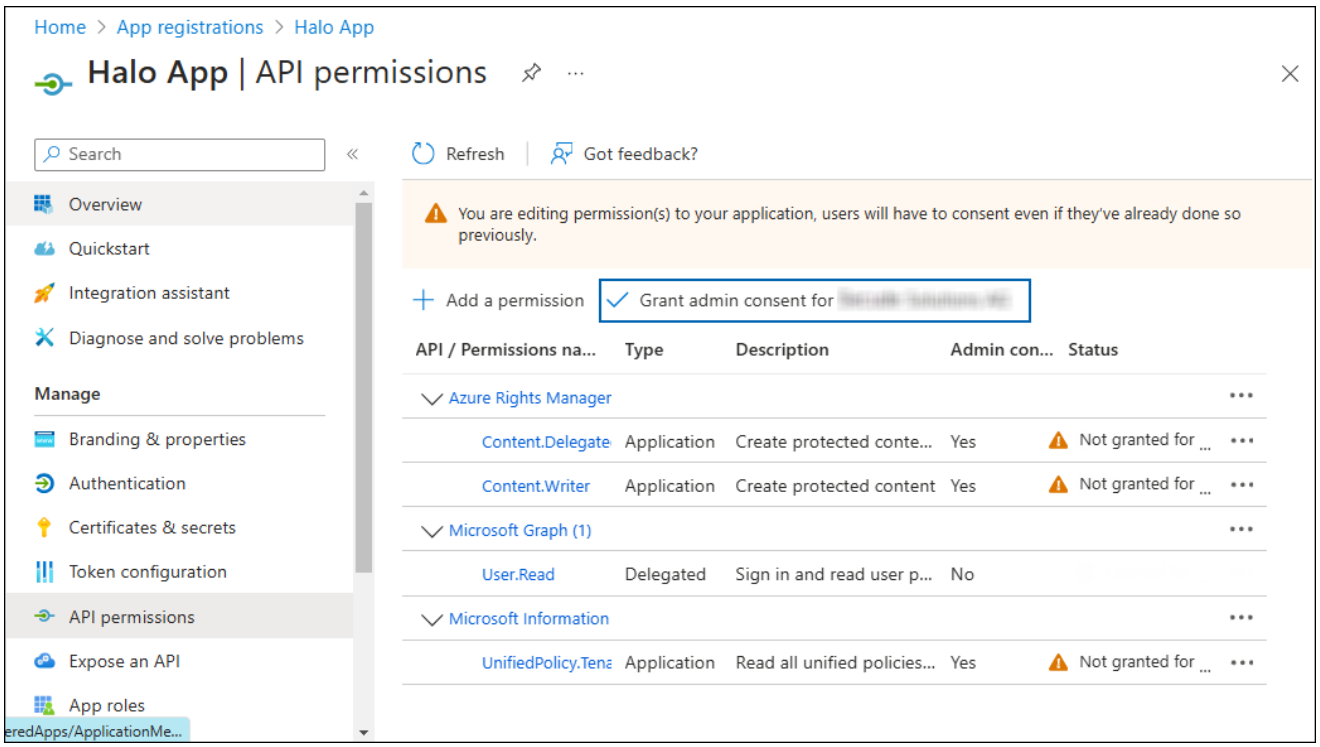
API selection

6. Select the displayed API. The page displays two permission types: **Delegated permissions** and **Application permissions**.
7. Click **Application permissions** and then, under the **Permission** section, select the checkbox near "**Read all unified policies of the tenant**."



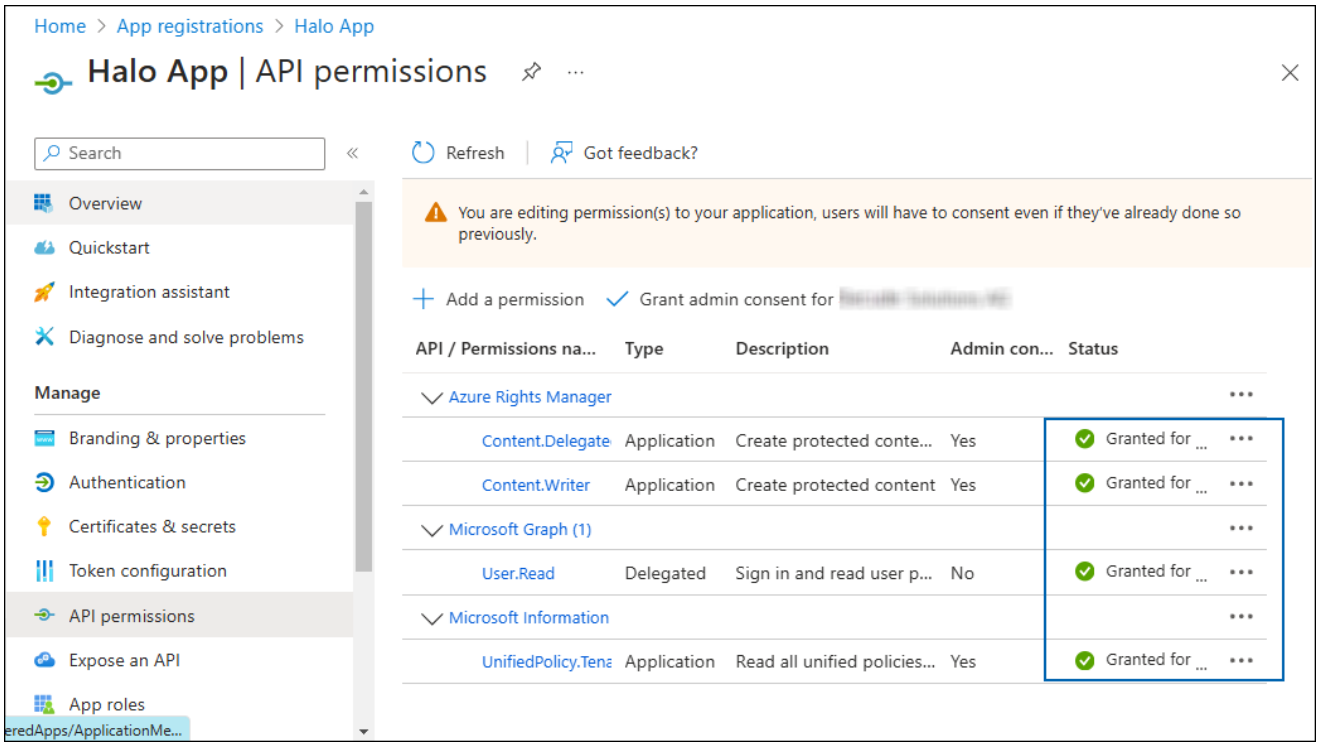
Adding permission

8. Click **Add permissions**.
9. Repeat the steps outlined above to add the other required permissions listed in the “Required permissions” table below.
10. The **API permissions** page opens, and the added permissions appear in the table with the status **Not granted**.



Required API Permissions

11. Click **Grant admin consent for your company**. When prompted, click **Yes** to confirm the consent request.
12. After the admin consent is accepted, the status changes 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 GenNXT 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 GenNXT 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.

Required permissions #2

4.1.3. Upload the Certificate

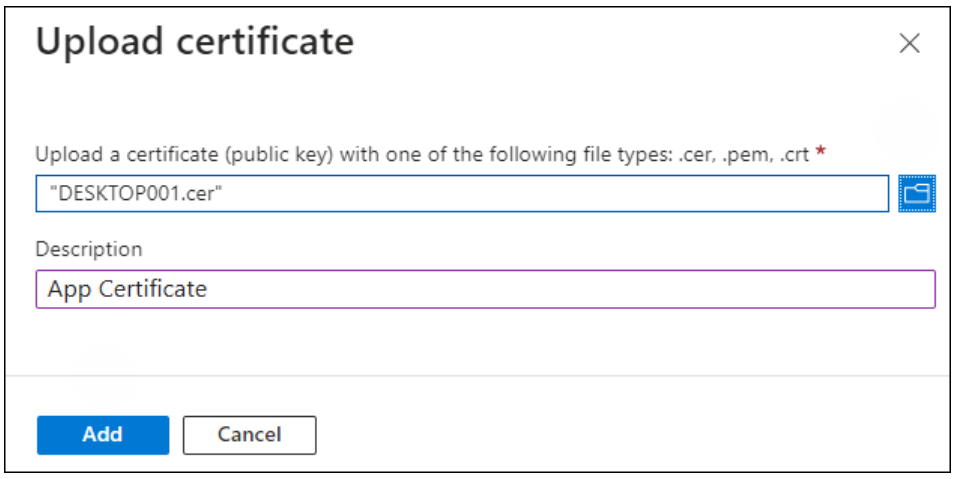
The HaloENGINE GenNXT Tomcat Service uses certificate-based authentication to access MPIP services. Therefore, you must upload the certificate to the registered application before proceeding with the configuration.

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. As a best practice, use a self-signed certificate only in a test environment.
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.

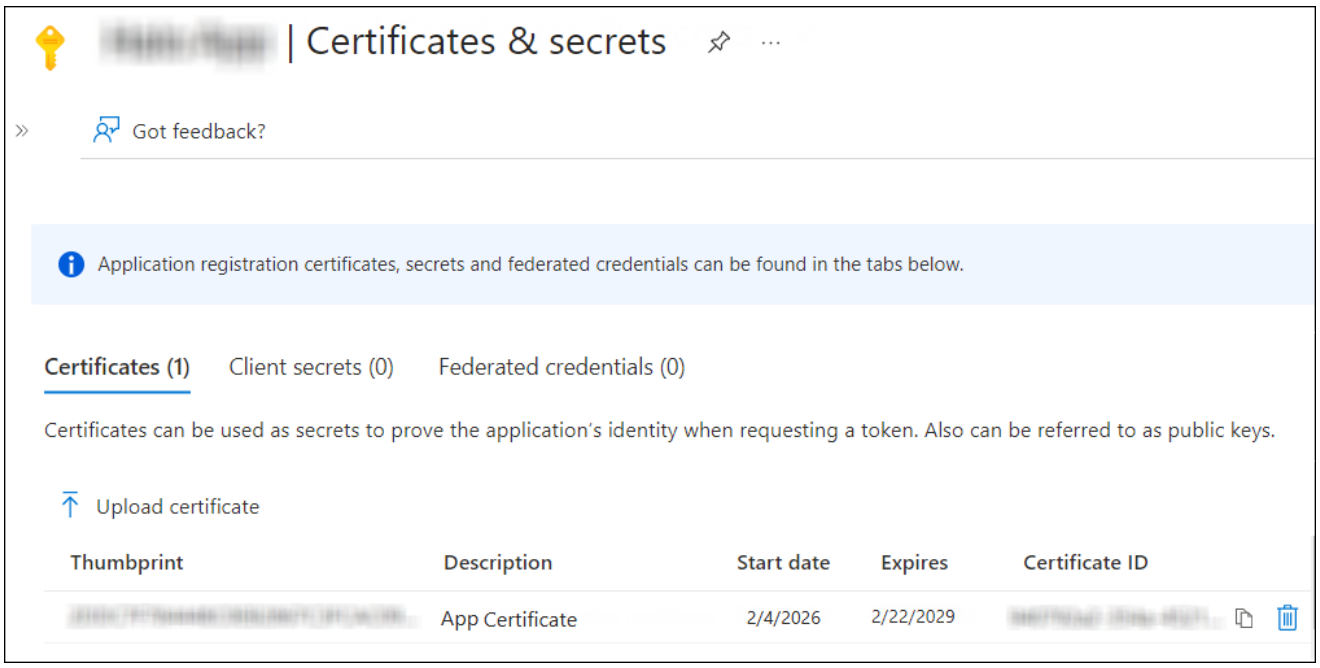
To upload the certificate, follow these steps:

1. In the sidebar of the application page, select **Certificate & secrets**.
2. Under **Certificates**, click **Upload certificate**. The Upload certificate dialog box opens.



Upload certificate #1

3. Click the folder icon, select the certificate, and click Open. For example, the file `DESKTOP001.cer` is used.
4. Click **Add**. The certificate is uploaded, and its thumbprint appears on the page.



Upload certificate #2

4.2. Office 365 Subscription Details

1. Microsoft Purview Information Protection must be fully configured.
2. An Office 365 subscription is required to use Azure RMS and 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. For more information, refer to the section "Enable Support for TLS 1.2 at the Client Workstation for Microsoft Entra ID".
5. Monitor logging: Your subscription must include Log Analytics on the same tenant as Microsoft Entra ID.

4.2.1. 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 information, refer to the Microsoft online documentation.

4.2.2. Recommended URLs, Addresses, and Ports for MPIP

MIP SDK does not support the use of authenticated proxies. Therefore, ensure that you set the Microsoft 365 endpoints to bypass the proxy. For a list of endpoints, refer to the Microsoft documentation "Microsoft Online Documentation". The following endpoints are recommended:

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, refer to "Microsoft Online Documentation".	`https://login.microsoftonline.com`

Recommended endpoints

Sovereign cloud: For Microsoft 365 U.S. Government GCC High and DoD environments, configure the required Microsoft service endpoints. For endpoint details, see Microsoft 365 U.S. Government GCC High endpoints.

4.2.3. Enable TLS 1.2 for Microsoft Entra ID Authentication

To improve tenant security and comply 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)

To authenticate with Microsoft Entra ID, TLS 1.2 must be enabled on the client workstation. For instructions, refer to the Microsoft documentation on enabling TLS 1.2 in the following link: Microsoft article to enable TLS 1.2.

Microsoft documentation

The Microsoft documentation takes precedence over the information in this section. Because Microsoft may update its guidance, always refer to the latest Microsoft documentation before making configuration changes.

Complete the following steps:

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

4.3. Configure Microsoft Entra ID for User Management

During the first sign-in to the HaloENGINE GenNXT Admin Portal, a default administrator account with Super Admin privileges is created. The Super Admin account has full administrative privileges and unrestricted access to the HaloENGINE GenNXT Admin Portal.

You can configure additional user accounts by creating application roles and assigning them to users based on their business responsibilities in **Microsoft Entra ID**. The following user roles are available:

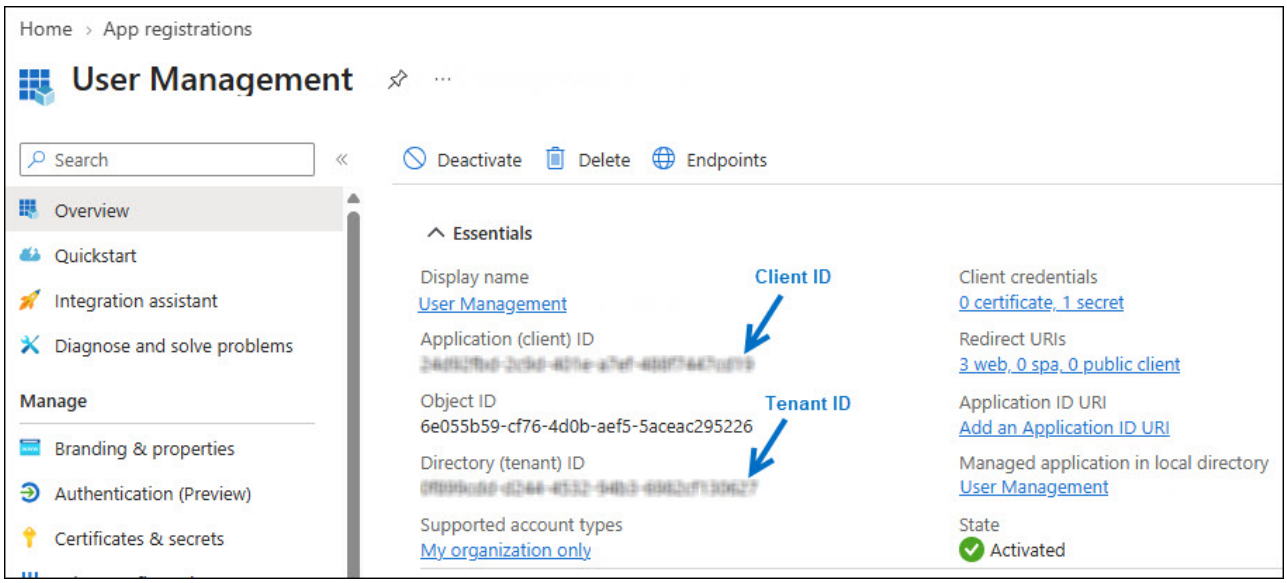
- **Customer_Admin**
  - **Role:** ROLE_CUSTOMER_ADMIN
  - **User validation:** Microsoft Entra authentication
- **Customer_User**
  - **Role:** ROLE_CUSTOMER_USER
  - **User validation:** Microsoft Entra authentication

Complete the following steps in the Microsoft Entra admin center to configure user authentication and authorization for the HaloENGINE GenNXT Admin Portal.

Any application that uses Microsoft Entra ID for authentication must be registered in the Microsoft Entra tenant. Because Microsoft may update its procedures, the Microsoft documentation takes precedence over the information provided in this section.

4.3.1. Step 1: Create a New Web Application

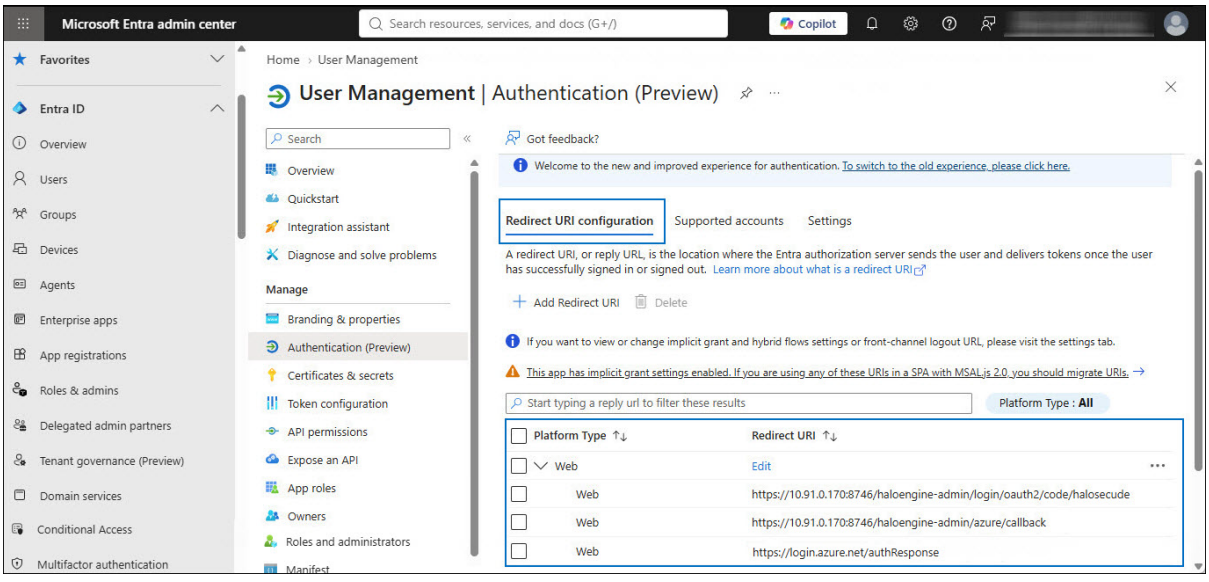
1. You can use the web application created in the previous section or create a new application in the Microsoft Entra admin center. For this example, a new web application named **User Management** is created.
2. When registration is complete, the **Overview** page displays the **Application ID** (**Client ID**) and **Directory ID** (**Tenant ID)**. Copy these values and save them in a text editor, such as Notepad, for later use.



Client ID and Tenant ID

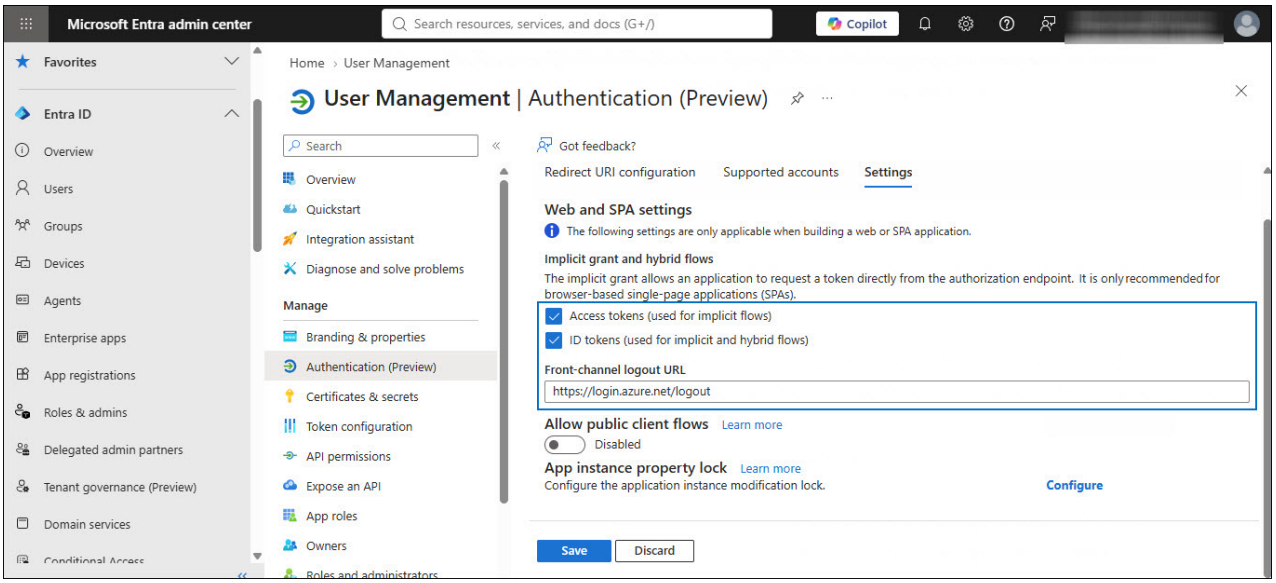
4.3.2. Step 2: Authentication Settings

1. In the left navigation pane, select **Authentication**.
2. Under **Redirect URI Configuration** tab, click **Add Redirect URI**.
3. On the **Select a platform to add redirect URI** page, under **Web applications**, select **Web**. Enter the following redirect URIs:
   - `https://<ip>:<port>/haloengine-admin/login/oauth2/code/<tenant name>`
   - `https://<ip>:<port>/haloengine-admin/azure/callback`
   - `https://login.azure.net/authResponse`
   - Click **Configure**.



Redirect URI

4. Go to the **Settings** tab.
   - Under **Front-channel logout URL**, enter the following URL: `https://login.azure.net/logout`
   - Under **Implicit grant and hybrid flows**, select the following check boxes: **Access tokens (used for implicit flows)** and **ID tokens (used for implicit and hybrid flows)**.

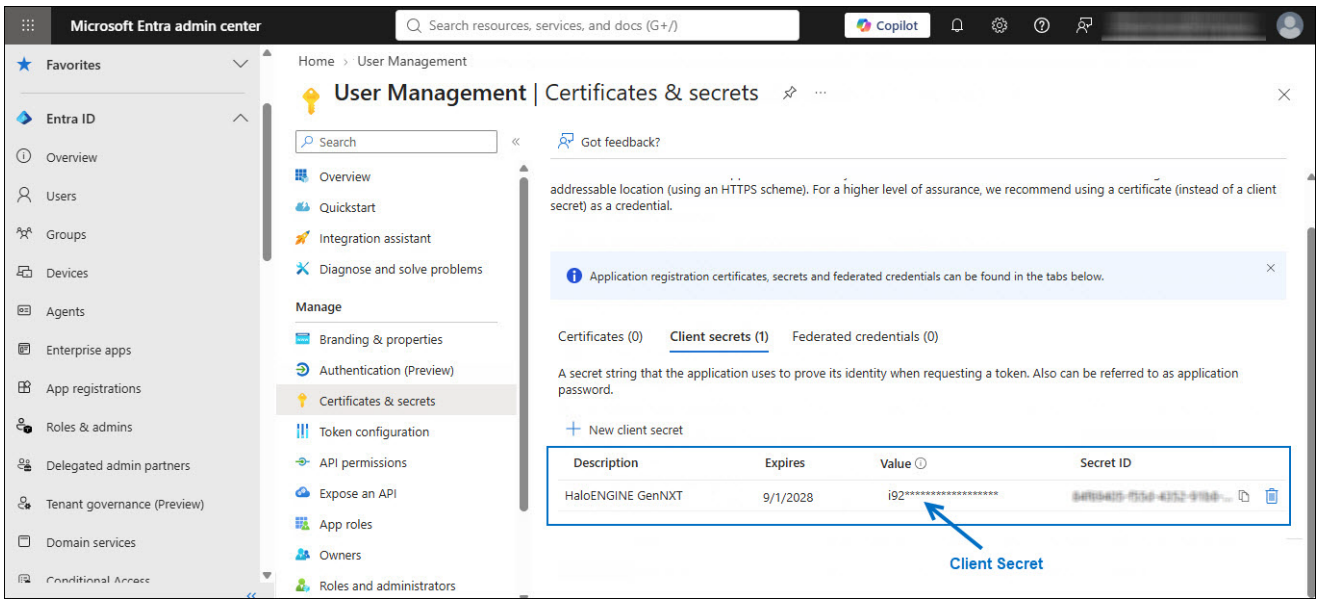


Front-channel logout URL

5. Click **Save**.

4.3.3. Step 3: Certificates & Secrets

1. In the left navigation pane, select **Certificates & secrets**.
2. Under **Client secrets**, click **+ New client secret**.
3. On the **Add a client secret** page, enter a description, select an expiration period under **Expires**, and then click **Add**.
4. After you click **Add**, the new client secret appears under **Client secrets**.

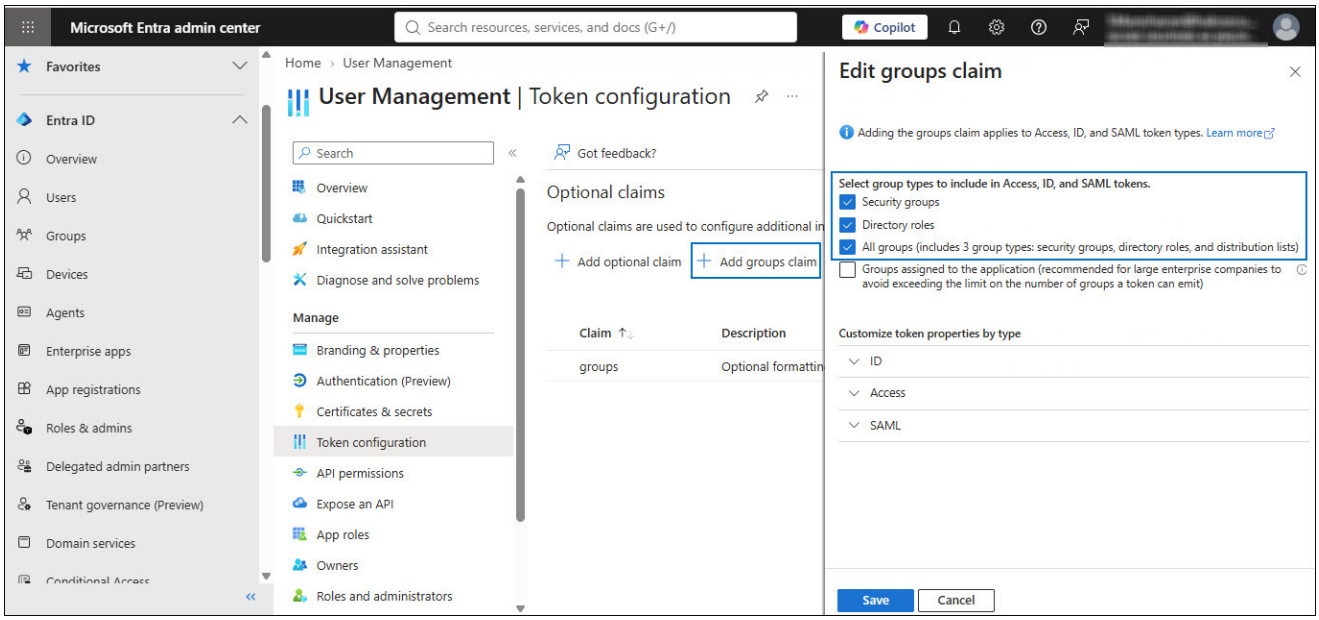


Client secret

5. Copy the **Value** immediately. It is displayed only once.
6. Store the client secret securely. You will need it when configuring the tenant in the Admin Portal.

4.3.4. Step 4: Token Settings

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



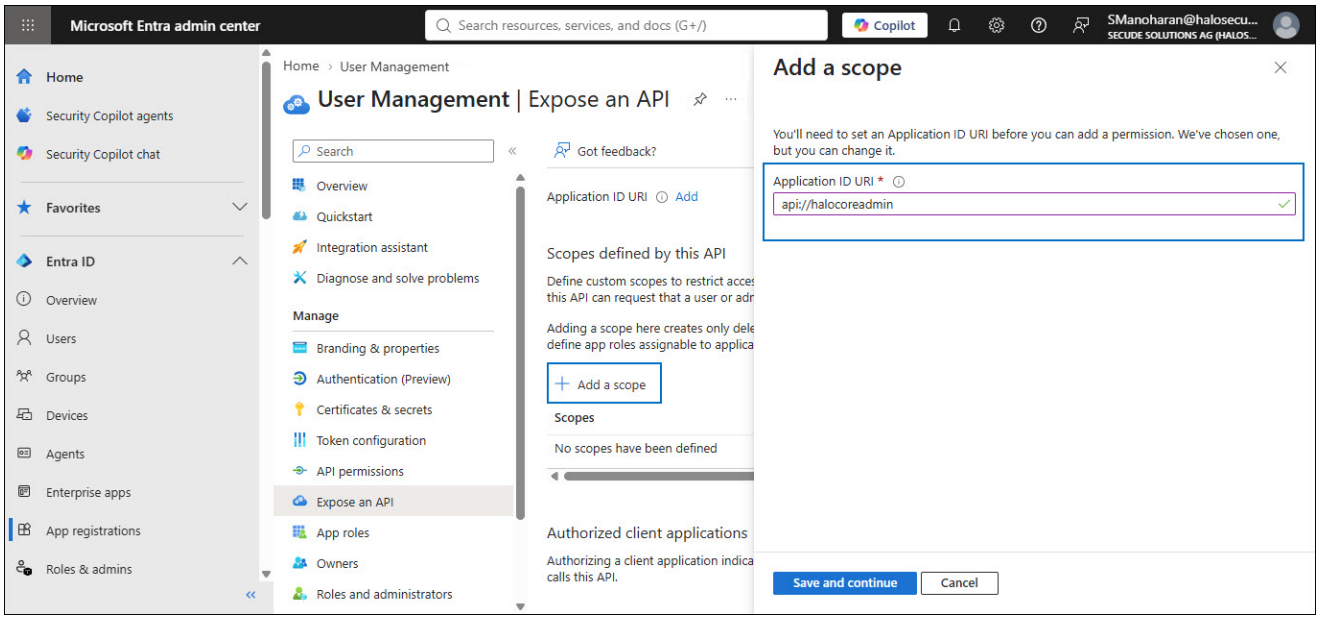
Token configuration

2. Select the following group types:
   a. **Security groups**
   b. **Directory roles**
   c. **All groups**

3. Click **Save**.

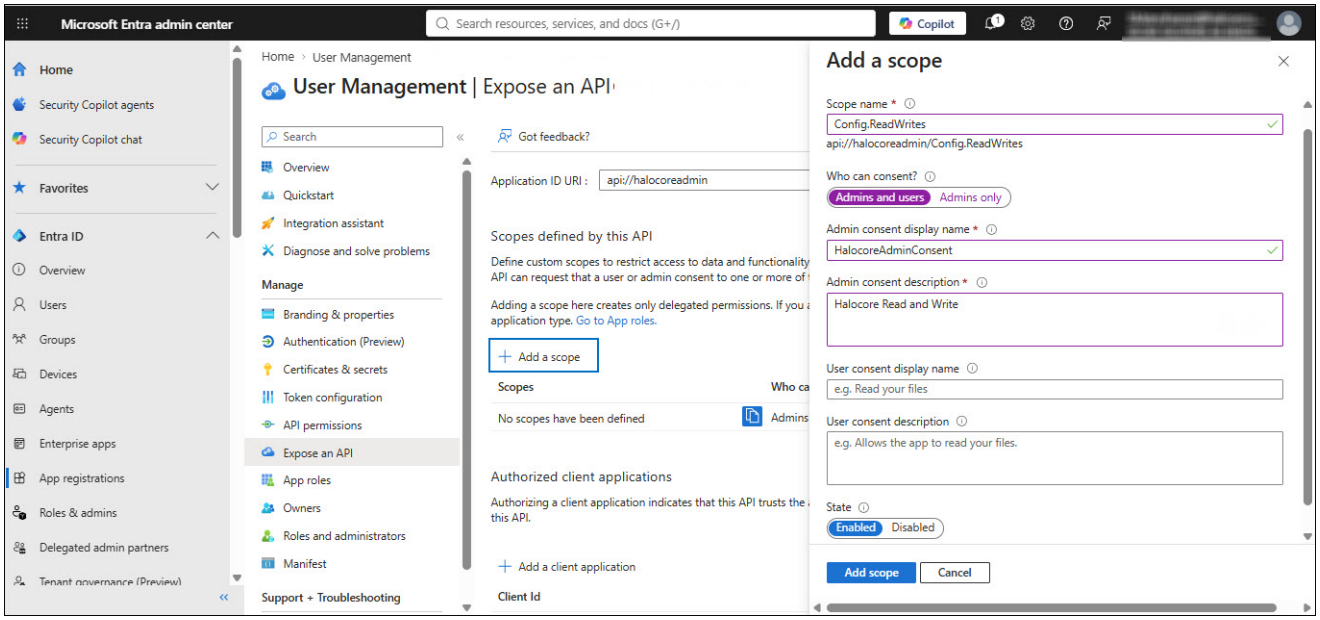
4.3.5. Step 5: Expose API

1. In the left navigation pane, select **Expose an API**.
2. Click **Add a scope**.
3. In the Application ID URI field, enter the application ID URI. In this example, `api://halocoreadmin` is used.



Application ID URI

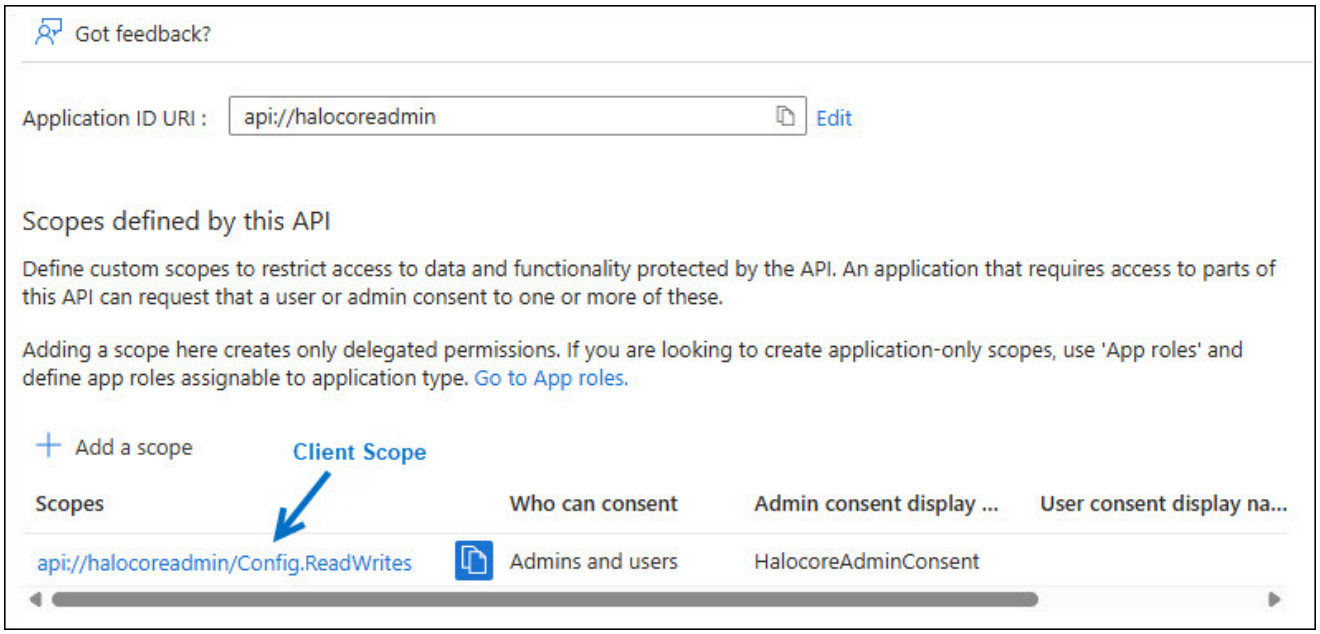
4. Click **Save and continue**.
5. Click **Add a scope** again, and then enter the following values:



Add a scope

- **Scope name:** `Config.ReadWrites`
- **Who can consent?:** Admins and users
- **Admin consent display name:** `HalocoreAdminConsent`
- **Admin consent description:** `Halocore Read and Write`
- **State:** Enabled

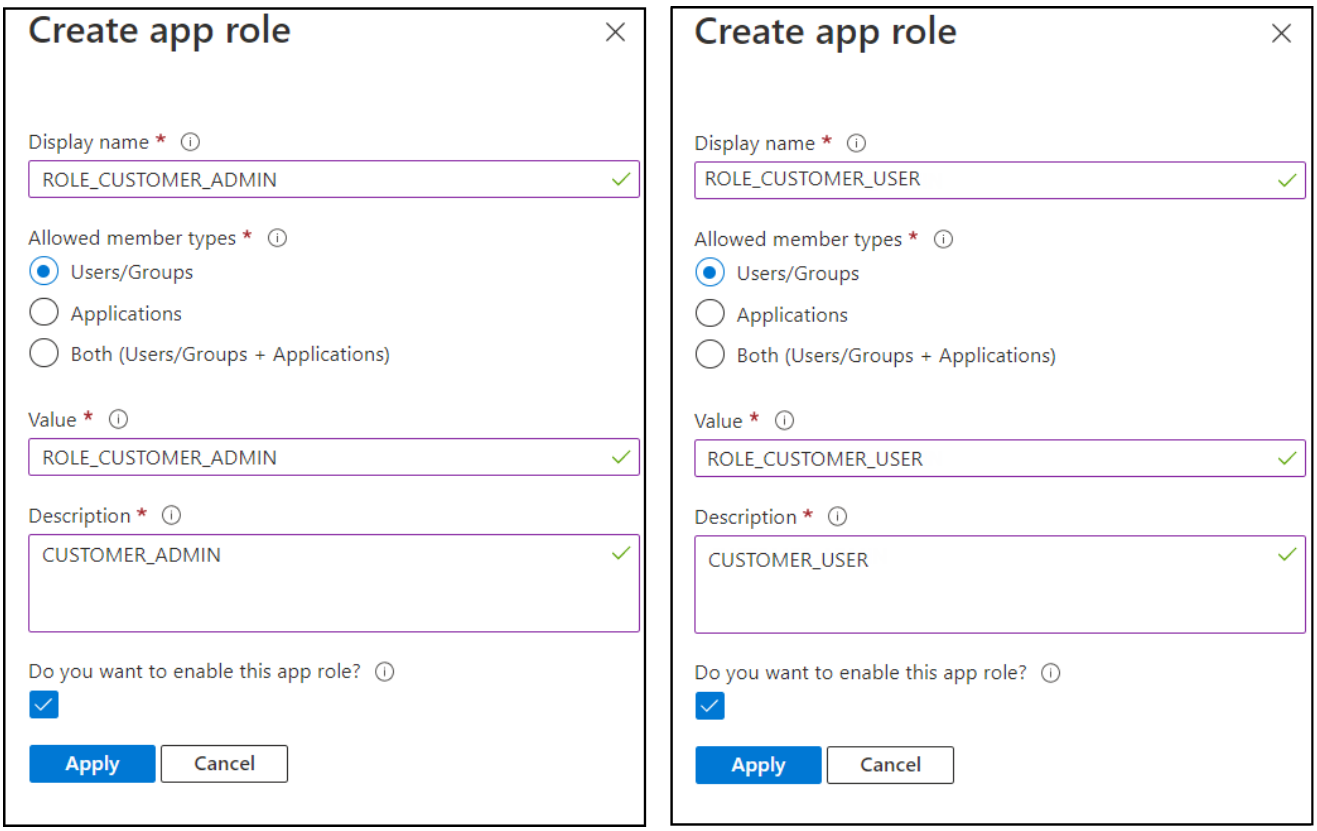
6. Click **Add scope**. The new scope appears in the list.
7. Copy the generated scope `api://halocoreadmin/Config.ReadWrites` and save it in a text editor, such as Notepad, for later use.



Client Scope (API scope)

4.3.6. Step 6: Create Roles

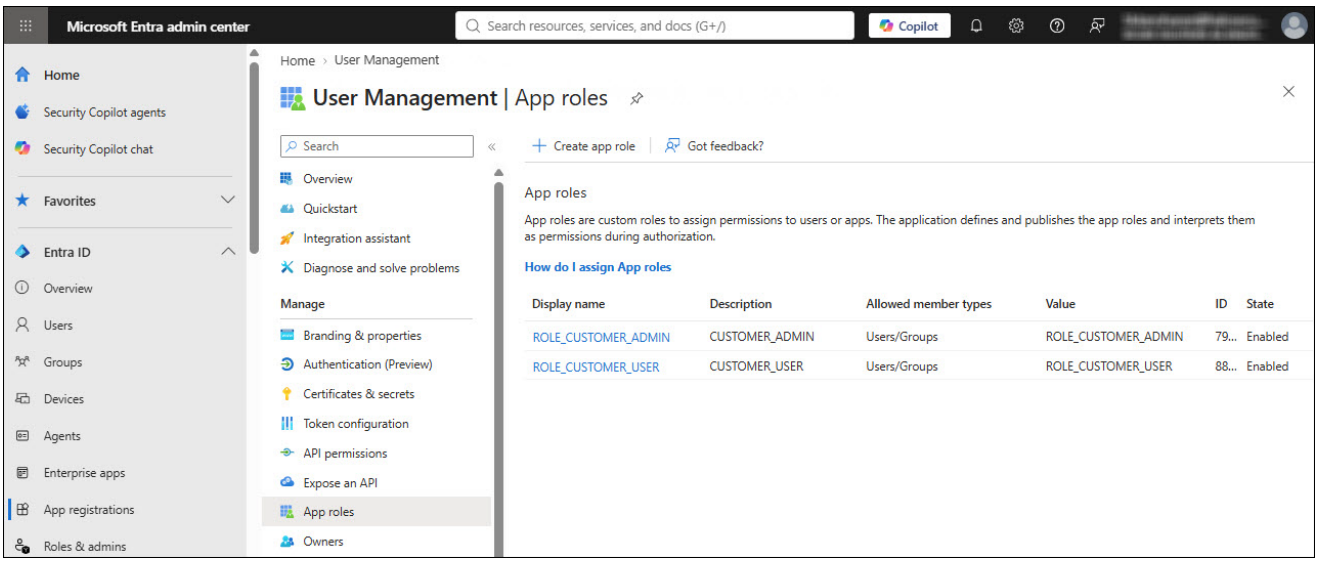
1. In the left navigation pane, select **App roles**.
2. Click **Create app role**, and then enter the following values:



App roles

- **Display name:** `ROLE_CUSTOMER_ADMIN`
- **Allowed member types:** `Users/Groups`
- **Value:** `ROLE_CUSTOMER_ADMIN`
- **Description:** `CUSTOMER_ADMIN`
- **Enable this app role:** Selected

3. Repeat these steps to create the **ROLE_CUSTOMER_USER** role.
4. Click **Apply**.

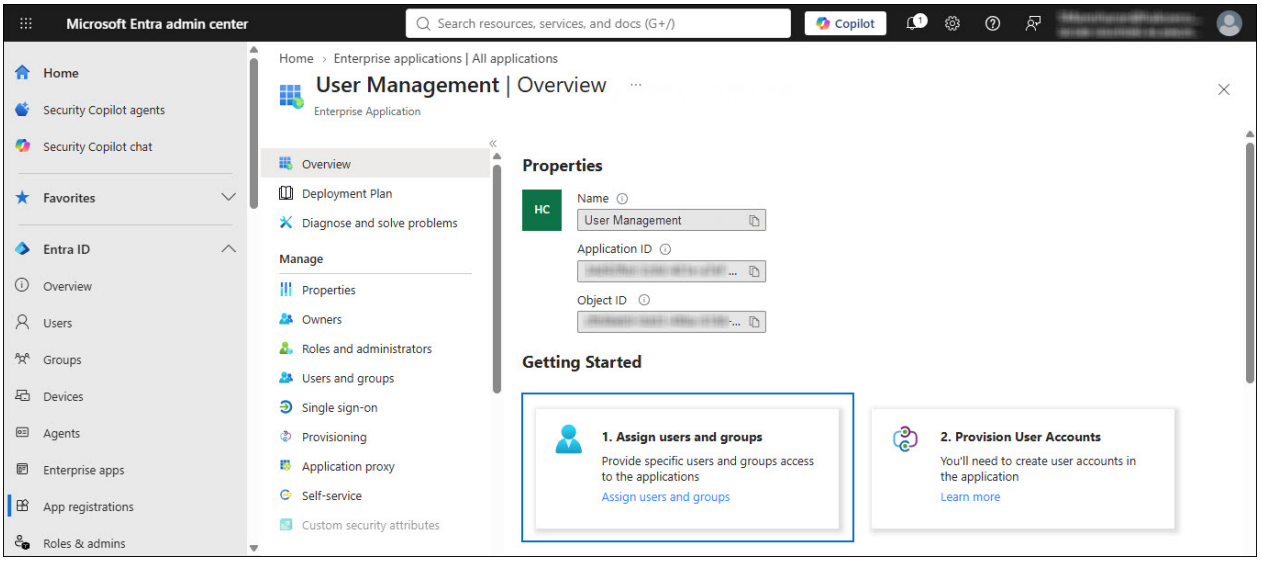


Role List

5. The new roles appear in the list.

4.3.7. Step 7: Apply Role to Users

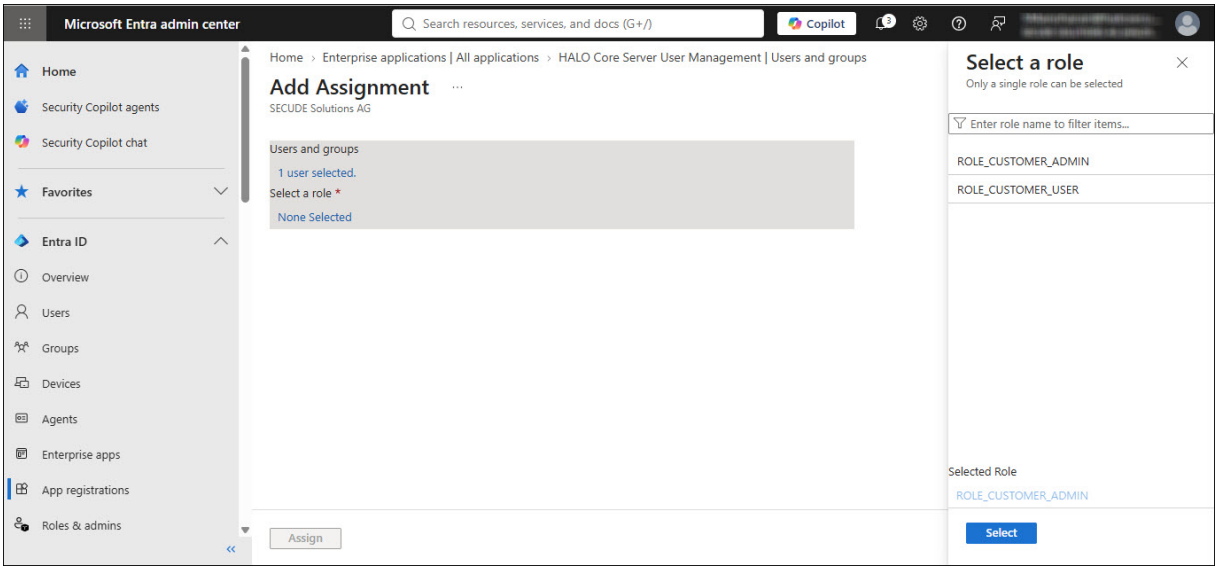
1. In the Microsoft Entra admin center navigation pane, select **Enterprise applications**.
   a. The **Enterprise applications** page displays the service principals available in your tenant.
   b. In the search box, enter the application name. For example, enter **User Management**.
   c. Select the application from the search results. The **Overview** page opens.



Overview page

   d. Select **Assign users and groups**. The **Users and** groups page opens.
   e. On the **Users and groups** page, click **Add user/group**. The **Add Assignment** page opens.
   f. Under **Users and groups**:

- Click **None Selected**.
- Search for and select a user (for example, **John**).



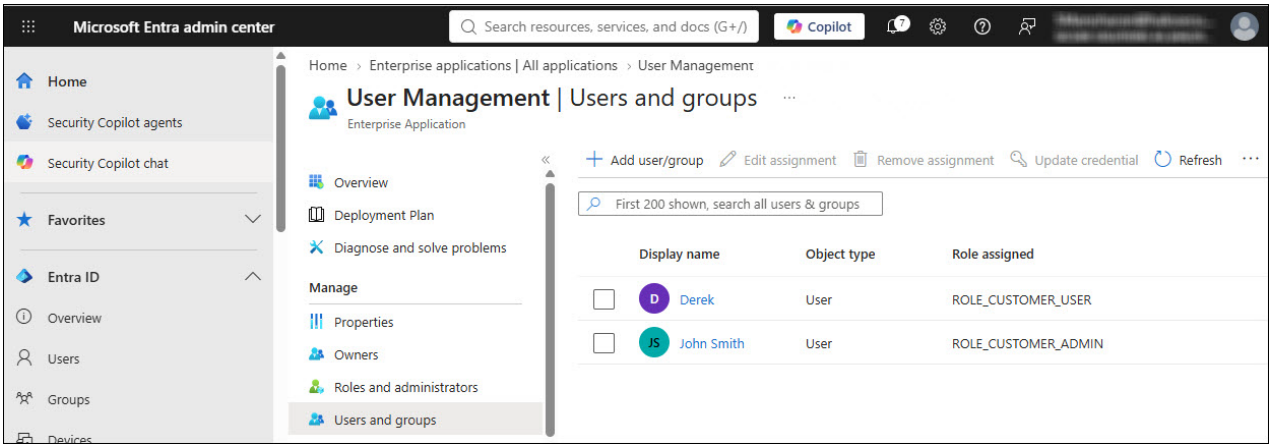
Select a user

- Click **Select**, and then click **Assign**.

g. Under **Select a role**:

- Click **None Selected**.
- Select **ROLE_CUSTOMER_ADMIN**.
- Click **Select**, and then click **Assign**.

h. Repeat these steps to assign the **ROLE_CUSTOMER_USER** role to additional users. In this example, **Derek** is assigned the **ROLE_CUSTOMER_USER** role.



Assigned Roles

During **Microsoft Entra Tenant Configuration** in the HaloENGINE GenNXT Admin Portal, you will need the following values. Save them in a secure location before proceeding.

- From **Step 1: Create a New Web Application**, copy the **Client ID** and **Tenant ID**.
- From **Step 3: Certificates & Secrets**, copy the **Client Secret**.
- From **Step 5: Expose an API**, copy the **Client Scope**.
- From the **Microsoft Entra admin center** home page, copy the **Tenant Name** and **Client Domain Name**.

4.4. Conditions for Running the HaloENGINE GenNXT Tomcat Service

Before running the HaloENGINE GenNXT Tomcat Service, ensure that the following prerequisites are met.

4.4.1. Deny log on as a service policy

If the service runs under a specific user account or 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 is restricted by this policy, the following error message appears when starting the HaloENGINE GenNXT Tomcat Service: *"Error 1069: The service did not start due to a logon failure."*

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

During installation, HaloENGINE GenNXT retrieves the required Microsoft Entra ID application details and certificate thumbprint. When the HaloENGINE GenNXT Tomcat Service starts, it connects to the MPIP services by using the details provided 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 during installation must match the thumbprint of the certificate installed in the **Local Computer** certificate store.

If the service runs under a non-administrative user account, the user might not have sufficient permissions to access the certificate's private key when the certificate is installed in the **Local Computer** certificate 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 procedure below. Any errors encountered during this process are recorded in the log file. If the verification succeeds, the service continues with initialization.

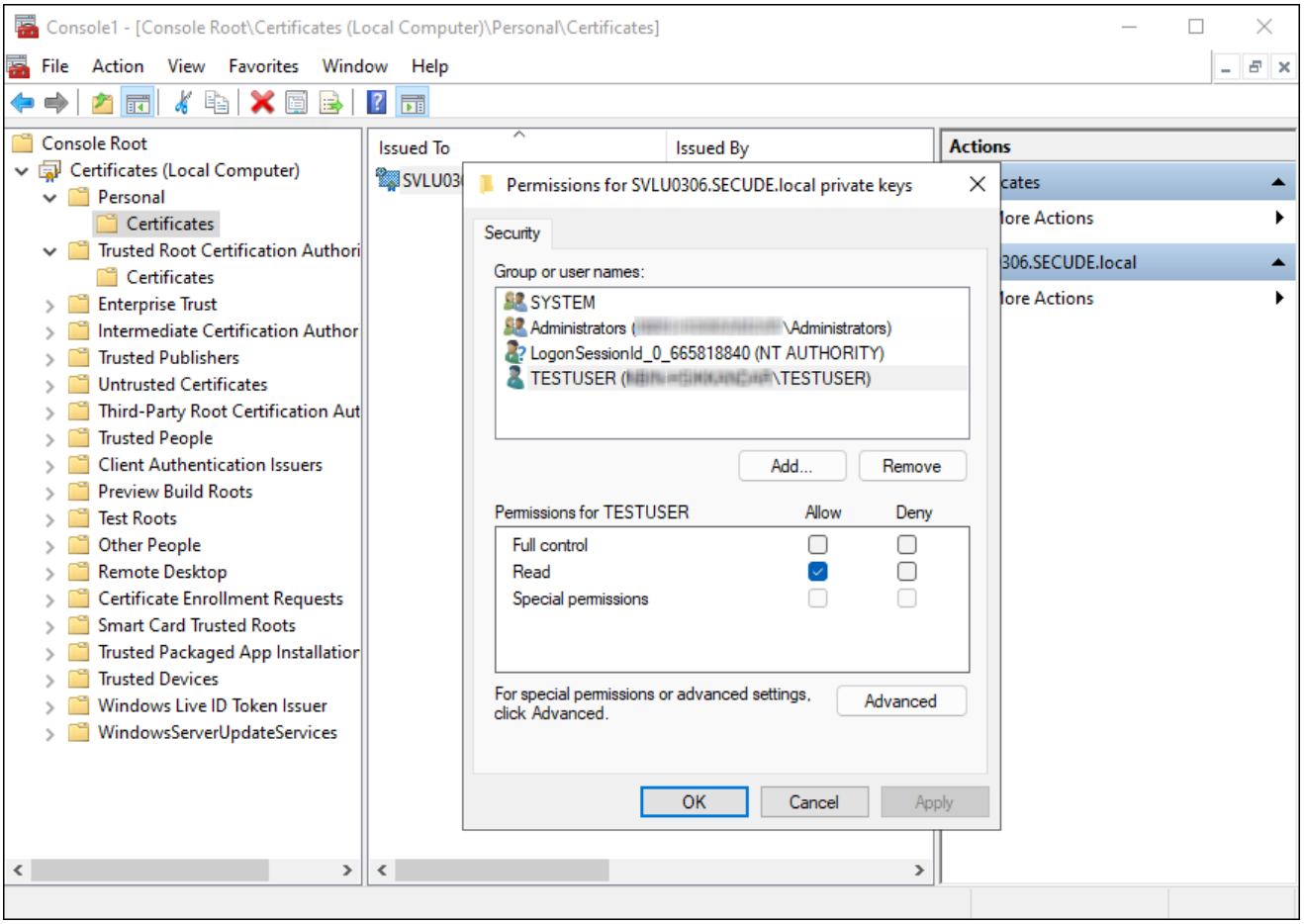
4.4.2. Prerequisites

- The required certificates (certificate used by MPIP service, root CA, and intermediate CA) are installed.
- The private key is stored in the Windows Certificate Store under **Local Computer**.
- You have administrator privileges to perform the configuration.

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. Select **Computer account**, click **Next**, select **Finish**, and then click **OK**.
6. In the left navigation pane, 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-administrator 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

Result

The specified non-administrative user can access the certificate's private key, allowing the HaloENGINE GenNXT Tomcat Service to authenticate successfully with MPIP services.

4.5. Obtain the HaloENGINE GenNXT License

Before installing HaloENGINE GenNXT, obtain the license file (`license.lic`) from Secude Support. The license file enables HaloENGINE GenNXT functionality and defines the licensed features and supported client systems. Only the client systems included in the license are available through their corresponding endpoints.

Do not rename the license file.
Use the license file exactly as provided by Secude. Renaming the file prevents the license from being activated.

Use the following table to determine the appropriate license feature set based on your requirements:

Customer Requirement	License Feature Set	Description
Monitor	Monitor	For environments that require monitoring only.
Block	Monitor + Block	For environments that require blocking. Monitoring is included by default.
Block and Label	Monitor + Block + Label	For environments that require both blocking and protection. This option requires a full license that includes the **Block** and **Label** features. Monitoring is included by default.

Obtaining license

4.6. MPIP Authentication

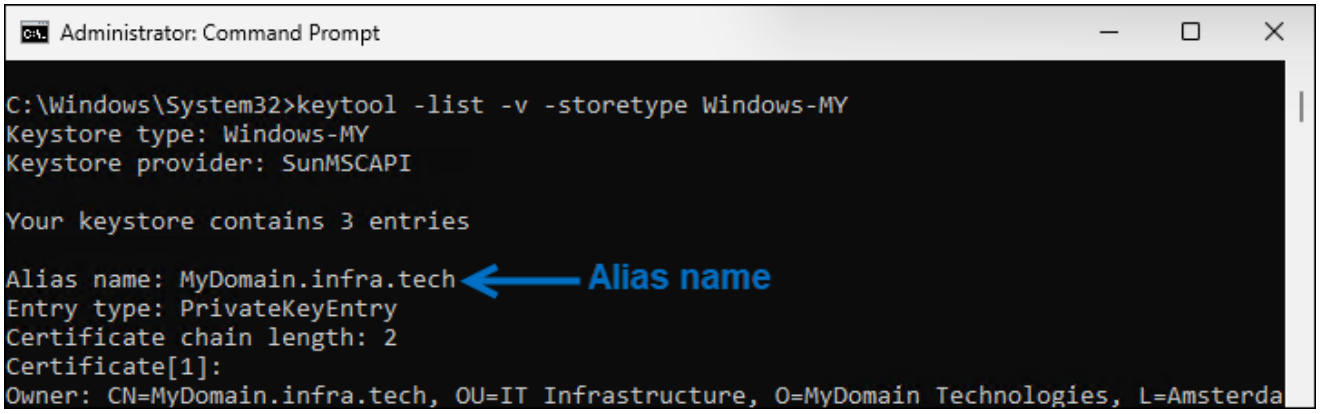
The **HaloENGINE Service (MPIP module)** requires a certificate for MPIP authentication. Install the certificate in the **Local Computer** certificate store along with the required Root CA and Intermediate CA certificates.

- If the certificate is **CA-signed**, install the certificate and all related certificates in their respective **Root**, **Intermediate**, and **Personal** stores.
- If the certificate is **self-signed**, install it in both the **Trusted Root Certification Authorities** and **Personal** stores under **Local Computer**.

4.7. Tomcat HTTPS Configuration

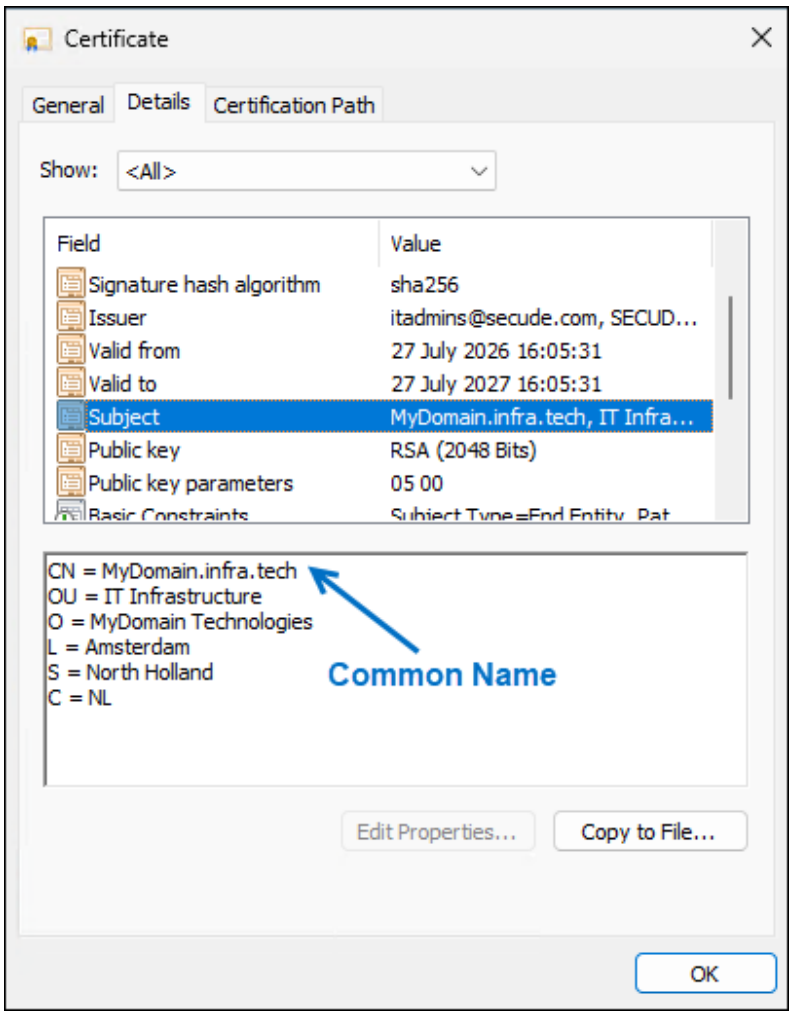
Before installing HaloENGINE GenNXT, ensure that the certificate to be used for HTTPS is installed in the Windows Certificate Store on the server where HaloENGINE GenNXT will be installed.

1. Import the self-signed or CA-signed certificate into one of the following certificate stores:
   - **Local Computer → Personal → Certificates**
   - **Current User → Personal → Certificates**
2. Identify the **alias name** of the imported certificate.
3. Open Command Prompt and run the following command: `keytool -list -v -storetype Windows-MY`



Alias name

4. If an alias is not available, use the **Common Name (CN)** of the certificate. You can find the Common Name on the certificate **Details** tab.



Common Name of the certificate

Note: If HaloENGINE GenNXT is installed in the Current User certificate store, ensure that the following conditions are met for the Admin Portal to launch successfully:

1. The HaloENGINE GenNXT Tomcat service runs under the specified user account, not **LocalSystem**.
2. The certificate is installed in the **Current User** certificate store of the specified user account.
3. If the specified user does not have logon permission and does not have administrator privileges, install the certificate in the **Local Computer** certificate store and grant the user access to the certificate's private key. The specified user must have the required minimum privileges. Additionally, update the following file: `C:\Program Files\Secude\Tomcat\conf\server.xml`.
   Set the certificate keystore type to:

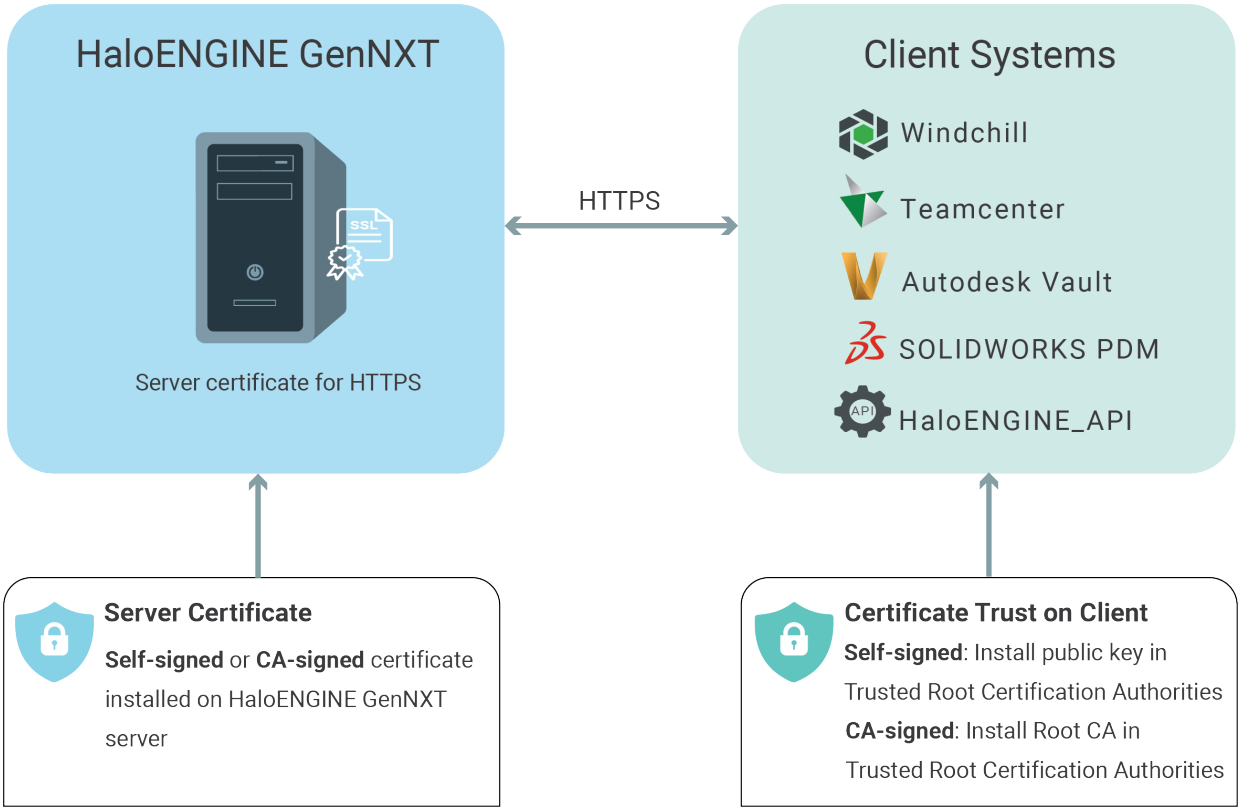
```
certificateKeystoreType="Windows-MY-LOCALMACHINE"
```

```
<Connector port="8746"
maxSavePostSize="2147483640" maxThreads="200"
protocol="org.apache.coyote.http11.Http11NioProtocol"
sslImplementationName="org.apache.tomcat.util.net.jsse.JSSEImplementation"
SSLEnabled="true"
scheme="https"
secure="true">
<SSLHostConfig protocols="TLSv1.2" sslProtocol="TLSv1.2">
<Certificate
certificateKeystoreType="Windows-MY-LOCALMACHINE"
certificateKeystoreFile=""
certificateKeyAlias="MyDomain.infra.tech" />
</SSLHostConfig>
</Connector>
```

Sample Server XML

Client Integration and Communication

HaloENGINE GenNXT communicates with supported client systems over HTTPS. The server certificate configured for HaloENGINE GenNXT secures the connection, and the client system must trust the certificate to establish a secure connection. Note: The URL used by the client must match a Subject Alternative Name (SAN) in the certificate. For example, if the client accesses the server using an IP address, the IP address must be included in the certificate SAN.



Client Integration and Certificate Trust

5. Installing the HaloENGINE GenNXT

This chapter describes how to install HaloENGINE GenNXT using the graphical installation method.

Prerequisites

Before installing HaloENGINE GenNXT, ensure that the following prerequisites are met:

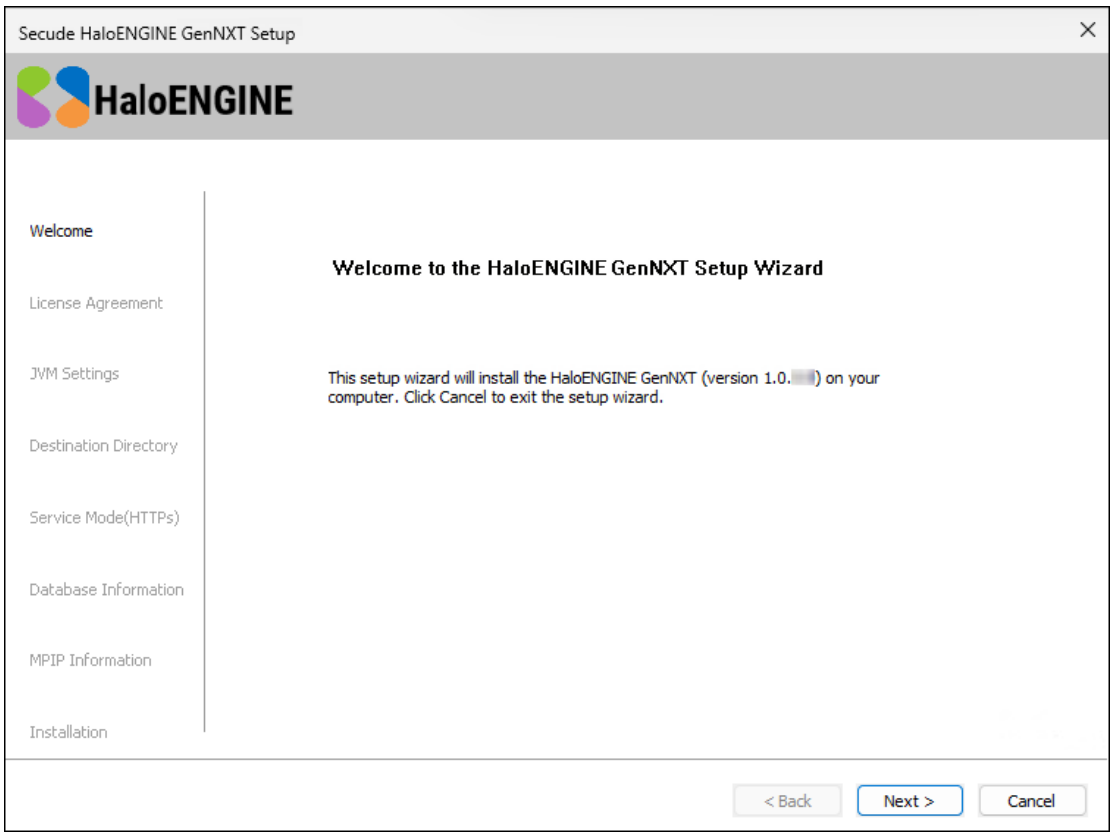
- The user performing the installation has administrator privileges.
- The Application ID and Tenant ID of the Microsoft Entra ID application are available.
- The Windows certificate alias name or Common Name (CN) can be used.
- The thumbprint of the MPIP authentication certificate installed in the Local Computer certificate store is available.
- For Microsoft SQL Server, create the database before installing HaloENGINE GenNXT. For example: `HaloENGINE_DB`. Then, establish a connection to the Microsoft SQL Server instance that hosts the HaloENGINE GenNXT database.
- For MySQL, ensure that the database user has the necessary remote access permissions when connecting from another machine.
- For SQLite, the database is stored in the installer package. No separate database server installation is required.

Procedure

1. To begin the interactive installation, double-click `HaloENGINEGenNXT_Setup.exe`. 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.

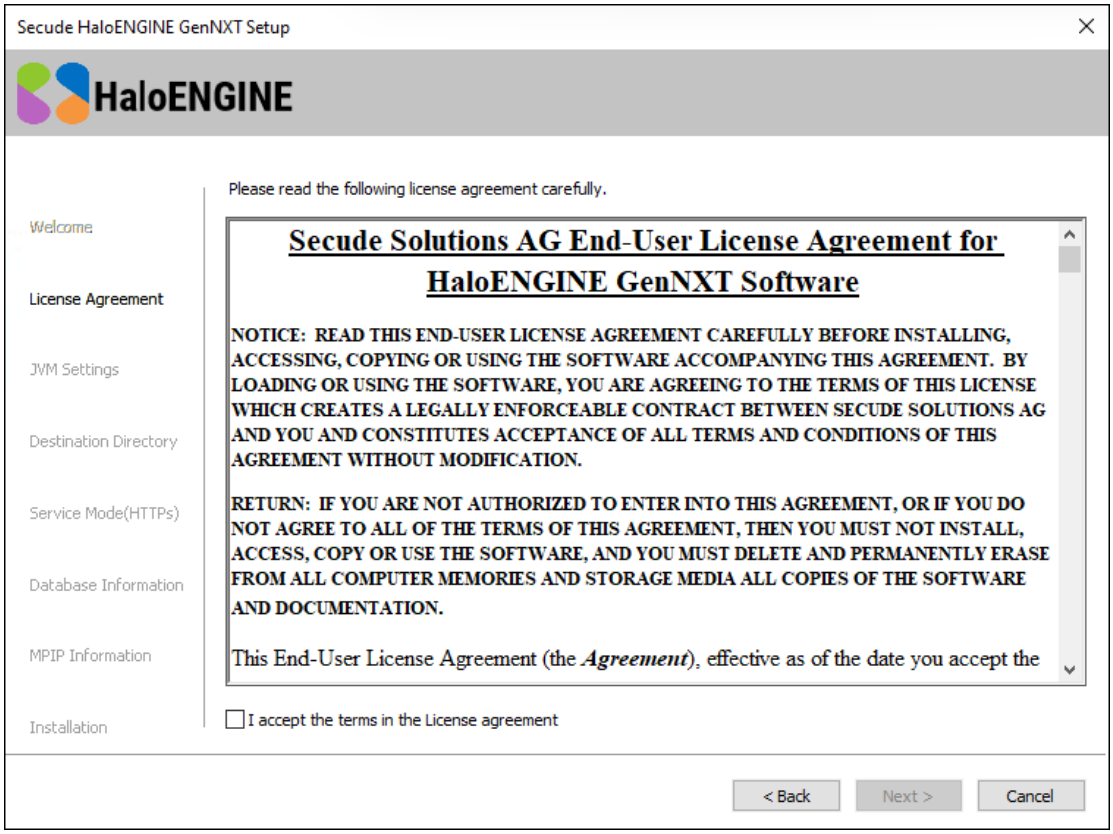


Startup Dialog



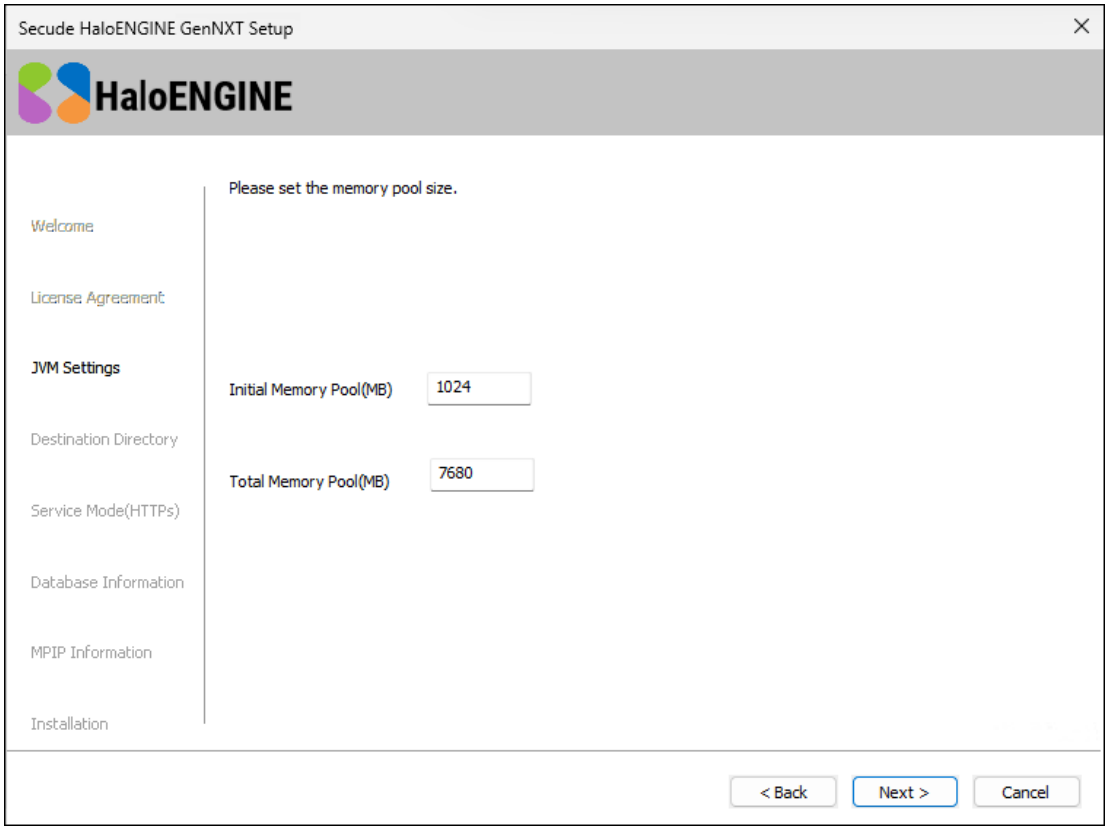
Welcome dialog

3. Click **Next**. The **License Agreement** dialog appears.



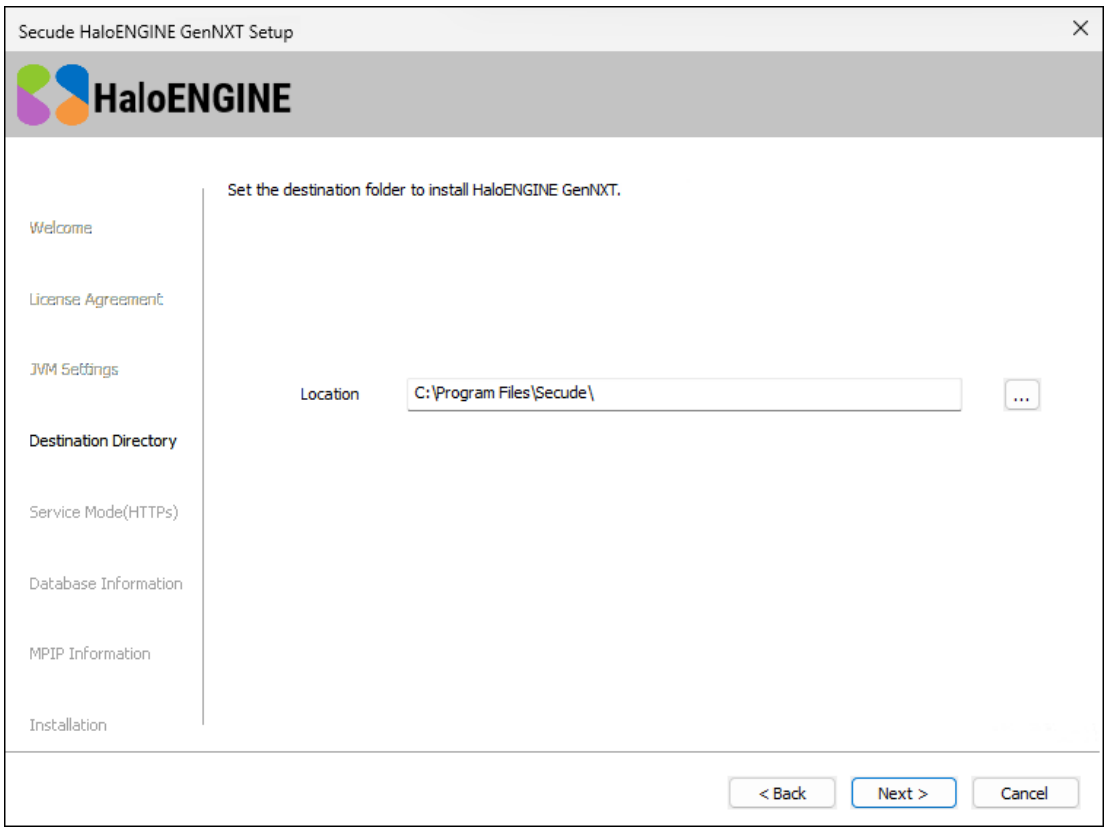
End-User License Agreement dialog

4. Read the **End-User License Agreement (EULA)**. If you accept the terms, select **I accept the terms in the License Agreement**, and then click **Next**.
5. The **JVM Settings** dialog appears.



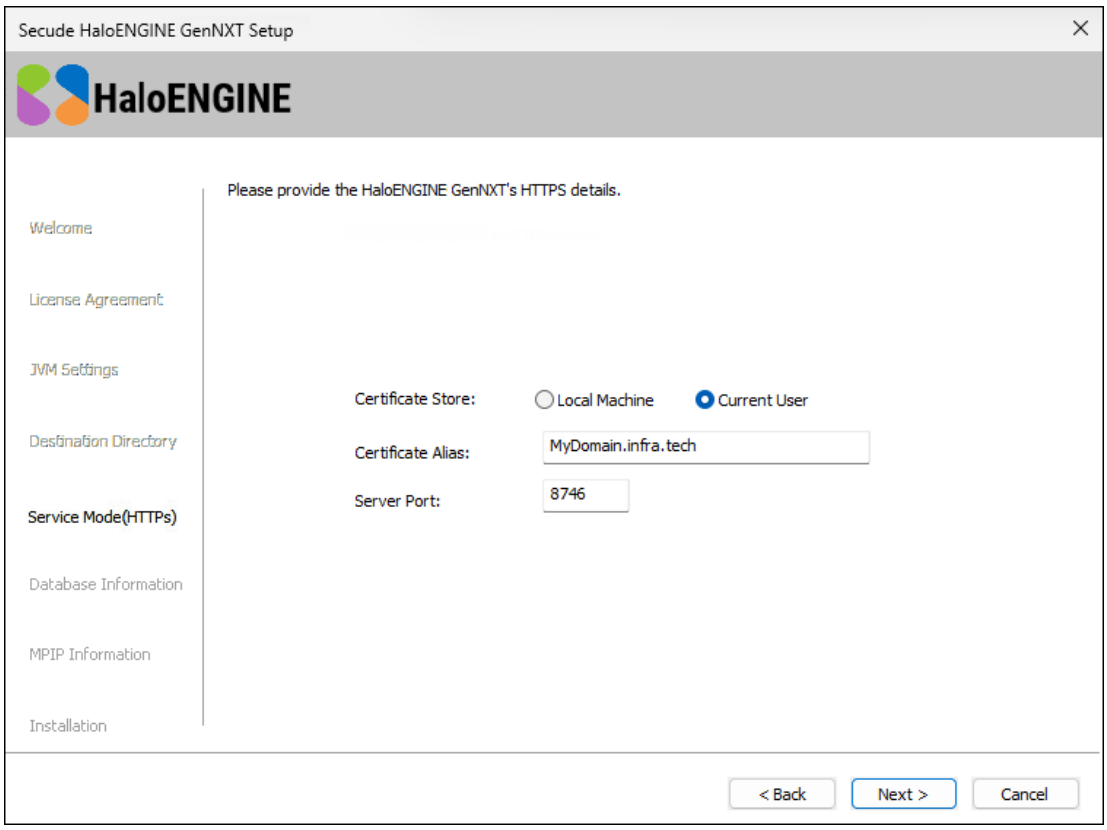
Tomcat memory pool size configuration dialog

6. If required, modify the **Initial Memory Pool and Total Memory Pool** values. Note: Ensure that the **Total Memory Pool** does not exceed 75% of the available system RAM.
7. Click **Next**.
8. The **Destination Directory** selection dialog appears.



Destination folder selection dialog

9. By default, HaloENGINE GenNXT is installed in `C:\Program Files\Secude\`. To install HaloENGINE GenNXT in a different location, click **Browse**, select the destination folder.
10. Click **Next**.
11. The **Service Mode (HTTPS)** dialog appears.



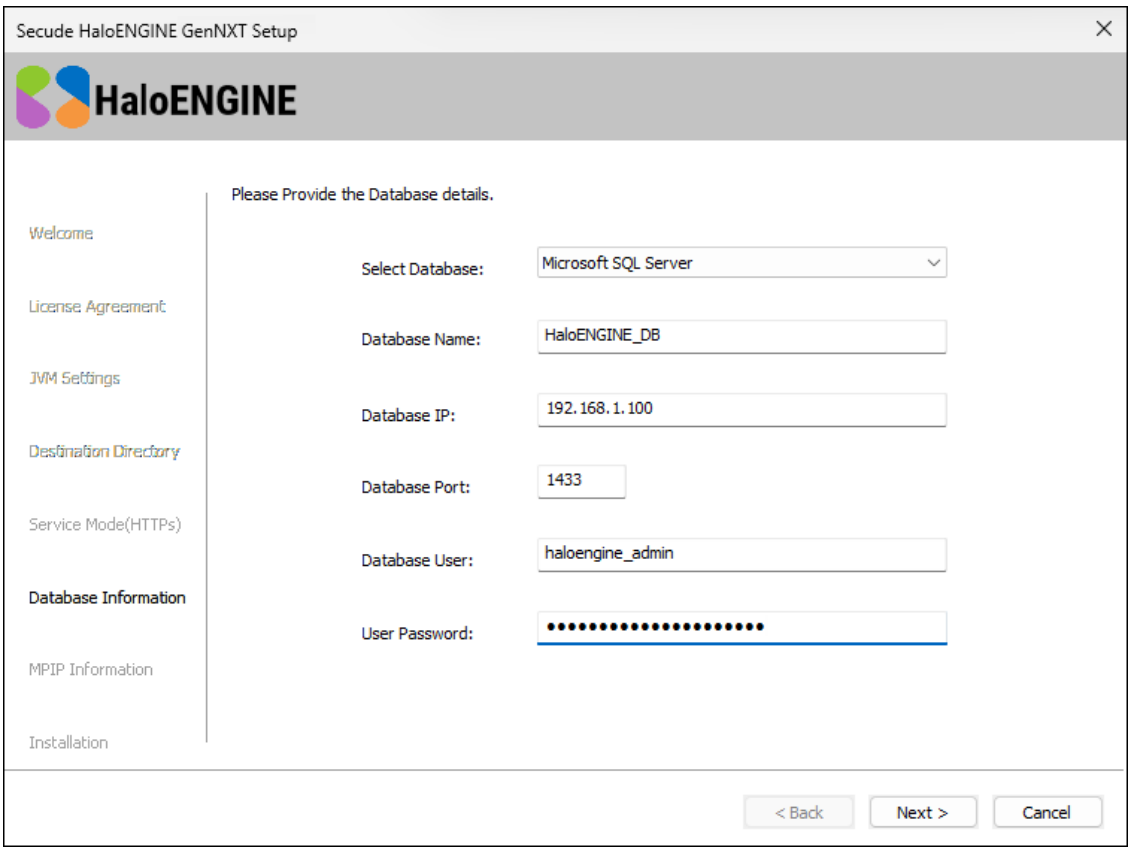
Service mode selection dialog

a. **Certificate Store**: Select **Local Machine** or **Current User**.

b. **Certificate Alias**: Enter the alias name of the certificate. If an alias is not available, enter the Common Name (CN) of the certificate.

c. **Service Port**: Enter the port on which you want to launch the Admin Portal.

12. Click **Next**.
13. The **Database Information** dialog appears.



Database Information dialog

a. **Database:** Select the database type: **Microsoft SQL Server**, **MySQL**, or **SQLite**. If you select **SQLite**, go to Step 14.

b. **Database Name:** Enter the database name. For **Microsoft SQL Server**, enter the name of the database created earlier. For **MySQL**, enter a database name. The database is created during installation. For example: `HaloENGINE_DB`.

c. **Database IP:** Enter the IP address of the database server. For example: `192.168.1.100`.

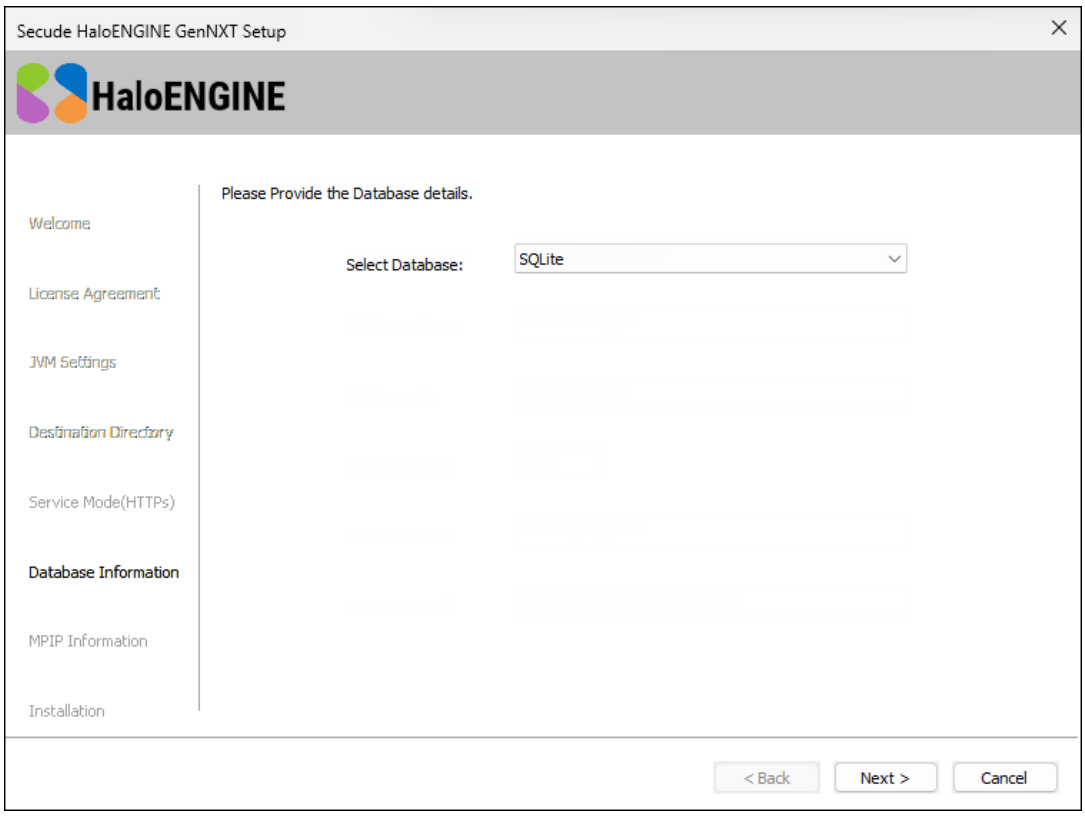
d. **Database Port:** Enter the database port number. For example:

- **Microsoft SQL Server:** `1433`
- **MySQL:** `3306`

e. **Database User:** Enter the database user name. For example: `haloengine_admin`.

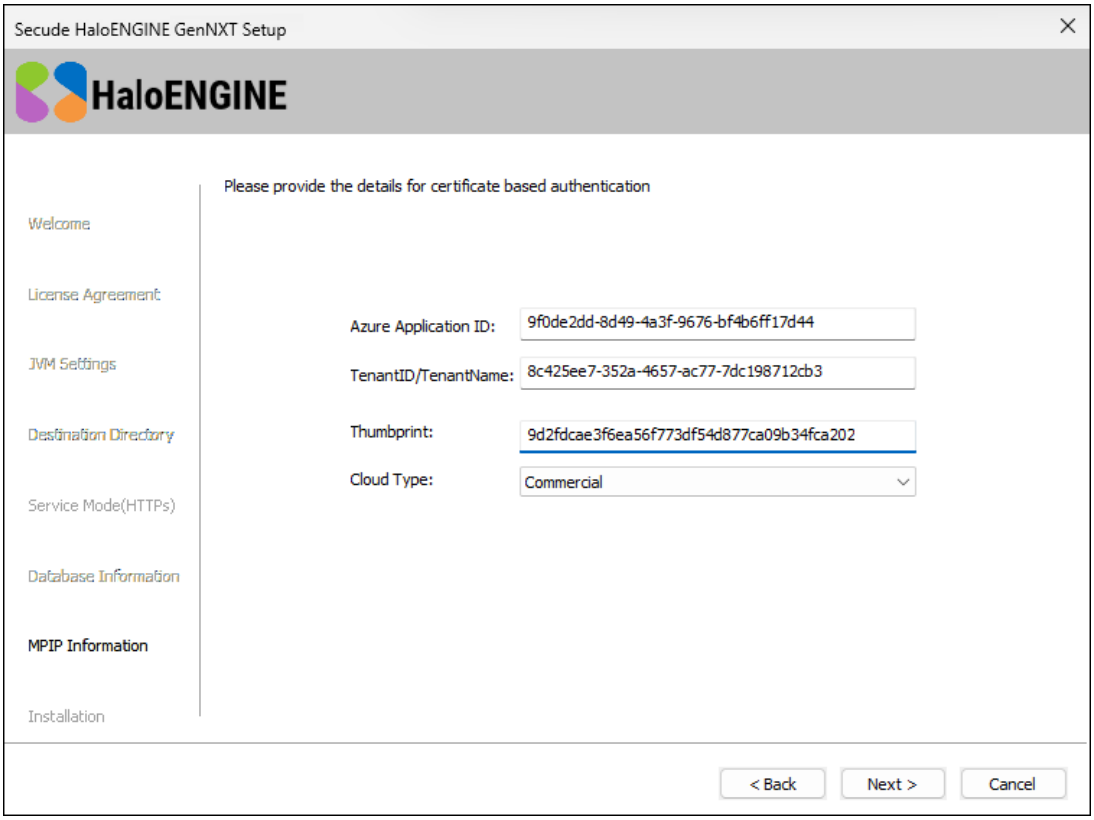
f. **User Password:** Enter the password for the database user. Then, go to Step 15.

14. **SQLite Database:** For SQLite, no further database configuration is required because the SQLite database is included in the installer package.



SQLite Database

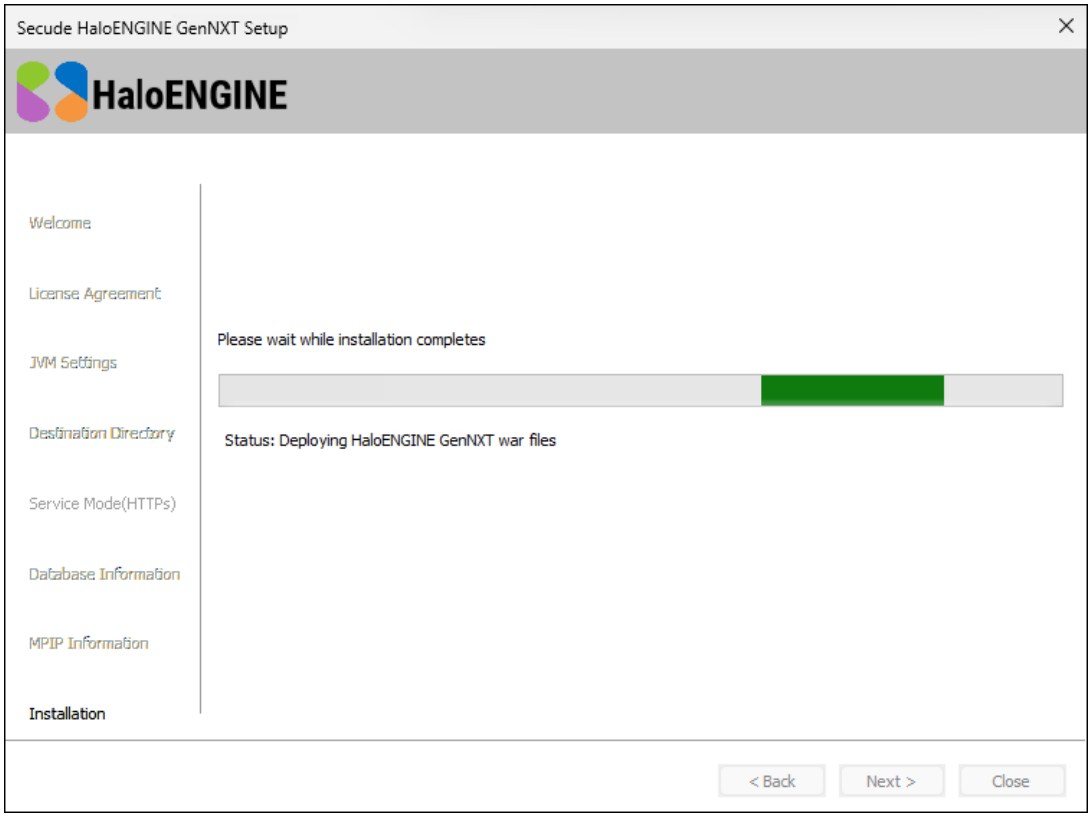
15. Click **Next**.
16. The **MPIP Information** dialog appears.



MPIP Information dialog

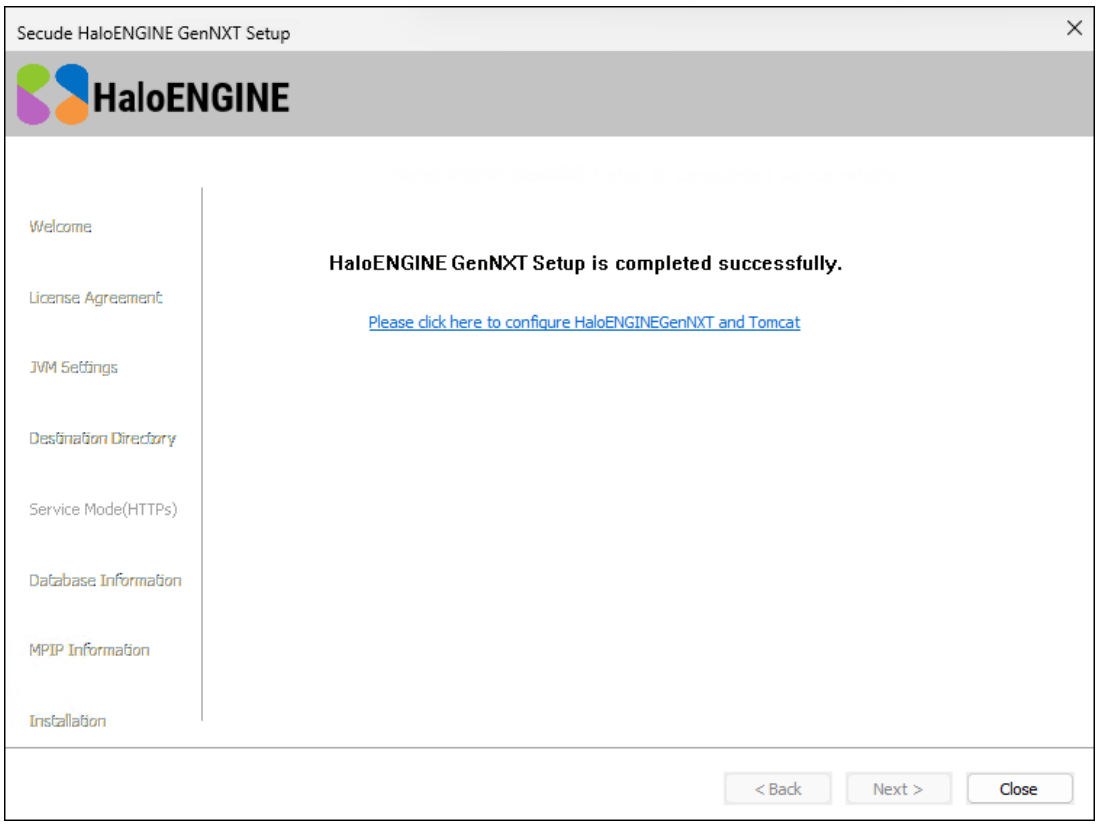
- **Application ID:** Enter the unique identifier of the registered Microsoft Entra ID application. For example, `9f0de2dd-8d49-4a3f-9676-bf4b6ff17d44`.
- **Tenant ID/Tenant Name:** Enter the Microsoft Entra tenant name (for example, `contoso.onmicrosoft.com`) or the tenant ID (for example, `8c425ee7-352a-4657-ac77-7dc198712cb3`).
- **Thumbprint:** Enter the thumbprint of the MPIP authentication certificate installed in the **Local Computer** certificate store. For example, `9d2fdcae3f6ea56f773df54d877ca09b34fca202`.
- **Cloud Type: Commercial** is selected by default. Depending on your Microsoft Entra ID cloud environment, select one of the following cloud types: **Commercial**, **Custom**, **US_DoD**, **US_GCC**, **US_GCC_High**, **US_Sec**, **US_Nat**, or **China_01**. If you select **Custom**, specify the following:
  - **Protection Cloud URL:** For example, `https://api.aadrm.com`
  - **Policy Cloud URL:** For example, `https://dataservice.protection.outlook.com`
- Click **Next**.

17. The **Installation** dialog appears, displaying the installation progress.



Installation progress dialog

18. When the installation is complete, a confirmation message appears. Click the link in the installer to open the HaloENGINE GenNXT Admin Portal. Alternatively, close the installation wizard and click the desktop shortcut .



Installation completed dialog

19. The HaloENGINE GenNXT Admin Portal opens in your default web browser at `https://<localhost>:<port>/haloengine-admin/`.

HaloENGINE GenNXT Tomcat service start-up delay after reboot

The HaloENGINE GenNXT Tomcat service is configured to use Automatic (Delayed Start). After the computer restarts, the service starts after approximately three minutes. The actual startup time depends on the system because Windows starts delayed services only after all Automatic services have started.

What to do next

1. Verify that the **Maximum memory pool size** in HaloENGINE GenNXT Tomcat (…`bin/HaloENGINE_Tomcat10.exe`) does not exceed the system RAM. After setting up the HaloENGINE GenNXT 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. For more information on initial configuration, refer to the section "Initial Configuration of HaloENGINE GenNXT Admin Portal".

5.1. Configuring the Tomcat Service

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

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

5.1.1. Configuration Tool

During installation, the Microsoft Entra ID application details are used to initialize the **HaloENGINE GenNXT Tomcat service**. After successful authentication, the sensitivity labels are retrieved automatically. Use `heslibconfig.exe` to update MPIP-related settings, such as the Application ID.

Default locations of log files

Name	Default Path
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 Microsoft Entra ID application 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 Silent Mode options, enter the following command:

   Type `heslibconfig.exe -help`

   Press `Enter`

   Output

   ```
   Usage:
   heslibconfig.exe -testmip
   ```

```
heslibconfig.exe -view
heslibconfig.exe -update -applicationid <application_id> -tenantid <tenant_id> -
thumbprint <thumb_print> -certstore <LocalComputer|CurrentUser>
heslibconfig.exe -testprotection <label_id>
```

Example Commands and Output

To display the labels, enter the following command:

```
heslibconfig.exe -testmip
MIP test started with config path C:\Program
Files\Secude\HaloENGINE\HaloENGINEService\config
Using policy from file: C:\Program
Files\Secude\HaloENGINE\HaloENGINEService\logs\mippolicy.xml
Using policy from file: C:\Program
Files\Secude\HaloENGINE\HaloENGINEService\logs\mippolicy.xml
Protection engine ID: b96cd9fb-72de-483a-bf69-a17e3beb4801
MPIP Initialization test passed. getting label details...
{
  "TotalLabels": 69,
  "labels": [
    {
      "id": "erd28959f-6ab8-4193-8580-a310ac1a5529",
      "isActive": true,
      "name": "Confidential"
    },
    {
      "id": ghefa4170-0d19-0005-0000-bc88714345d2",
      "isActive": true,
      "name": "Personal"
    },
```

To display the tenant details, enter the following command:

```
heslibconfig.exe -view
Application Id:9f0de2dd-8d49-4a3f-9676-bf4b6ff17d44
Tenant Id:8c425ee7-352a-4657-ac77-7dc198712cb3
ThumbPrint Id:d0d739fd4b4128f5e16c8d241360220ea8fb11fa
Certificate Store:LocalComputer
```

To update the JSON file, enter the following command:

```
heslibconfig.exe -update -applicationid 9f0de2dd-8d49-4a3f-9676-bf4b6ff17d44 -tenantid
8c425ee7-352a-4657-ac77-7dc198712cb3 -thumbprint d0d739fd4b4128f5e16c8d241360220ea8fb11fa
-certstore LocalComputer
Updating the config json file located in C:\Program
Files\Secude\HaloENGINE\HaloENGINEService\config\HaloENGINESVCMIPInfo.enc
```

```
Configuration file updated successfully.
```

To verify that protection is successful, enter the following command:

```
heslibconfig.exe -testprotection ttf1473d-74f4-47ca-9843-e735f94fa797
MIP protection test started with config path C:\Program
Files\Secude\HaloENGINE\HaloENGINEService\config
Using policy from file: C:\Program
Files\Secude\HaloENGINE\HaloENGINEService\logs\mippolicy.xml
Using policy from file: C:\Program
Files\Secude\HaloENGINE\HaloENGINEService\logs\mippolicy.xml
Protection engine ID: 8d56d1bd-972a-4450-b0b1-dc26573c87g5
MPIP Initialization test passed. Proceeding with protection...
Label Id...99f1473d-74f4-47ca-9843-e735f94fa797
File name ...C:\Program Files\Secude\HaloENGINE\HaloENGINEService\lib\testfile.txt
File protected successfully
Protected file C:\Program Files\Secude\HaloENGINE\HaloENGINEService\lib\testfile.ptxt
```

Configuration Changes in the JSON File

After installation, navigate to the configuration folder `...\HaloENGINEService\config`. The folder contains the JSON file that stores the **HaloENGINE GenNXT Tomcat Service** configuration properties. Note: Modify only the parameters listed below, 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 is visible in clear text in the MIP SDK logs. • true — PII is masked with asterisks in the MIP SDK logs, helping to protect PII confidentiality.
cachetype	Specifies the MPIP cache storage type used by the service. • In Memory (0) — Stores the cache in application memory. • On Disk (1, default) — Stores the SQLite3 database on disk in the directory specified in the settings object. The database is stored in plain text. • On Disk Encrypted (2) — Stores the SQLite3 database on disk in the directory specified in the settings object. The database is encrypted by using operating system-specific APIs.

Name	Description
cacheuserlicense	Controls whether the End User License (EUL) is stored in the MPIP cache. • 0 (false) — The End User License (EUL) is not stored in the MPIP cache. • 1 (true, default) — The End User License (EUL) is stored in the MPIP cache.
databoundary	Specifies the geographic region where audit and telemetry events are stored and processed.
enabledke	Enables or disables Double Key Encryption (DKE). • 0 (default) — Disables DKE in the HaloENGINE GenNXT Tomcat Service. • 1 (On) — Enables DKE in the HaloENGINE GenNXT Tomcat Service. Note: DKE labels are visible only when DKE is enabled.
enablefiletracking	Registers protected files for tracking and access revocation. • 0 (default) — Protected files are not registered for file tracking or access revocation. • 1 — Protected files are registered for file tracking and access revocation.
enableminimaltelemetry	Controls the diagnostic information transmitted to Microsoft. • 0 (default) — All diagnostic events are transmitted. • 1 — Only minimum diagnostic events are transmitted.
log_level	Specifies the logging level. Available values are ERROR, WARNING, INFO, and DEBUG.
log_purge	It indicates the removal of files older than a defined time frame. By default, log files older than 7 days are deleted.
streambuffersize	Specifies the buffer size used for memory-based encryption with the MIP SDK. When the configured buffer size is exceeded, additional memory equal to the configured stream buffer size is allocated. This process continues until the encryption or decryption operation is complete. The default value is 10 MB.

Name	Description
templatefile_purge	Defines the purge time of template files that are generated for each CAD assembly file (compound file) download. The default value is one hour. For example, when a file is downloaded at 15:25, the HaloENGINE GenNXT Tomcat Service creates a template file in the tmp\GUID folder, which is located in the HaloENGINE GenNXT Tomcat Service user's profile folder. In the background, it checks for and deletes files that have reached the configured purge time, for example, after 16:25. Note: This setting applies only to CAD assembly file labeling.

HaloENGINE GenNXT Tomcat service configuration

5.1.2. 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 is as shown above, the proxy server has not been configured in the WinHTTP registry.

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 GenNXT Tomcat Service ensures that the configured proxy settings are applied.

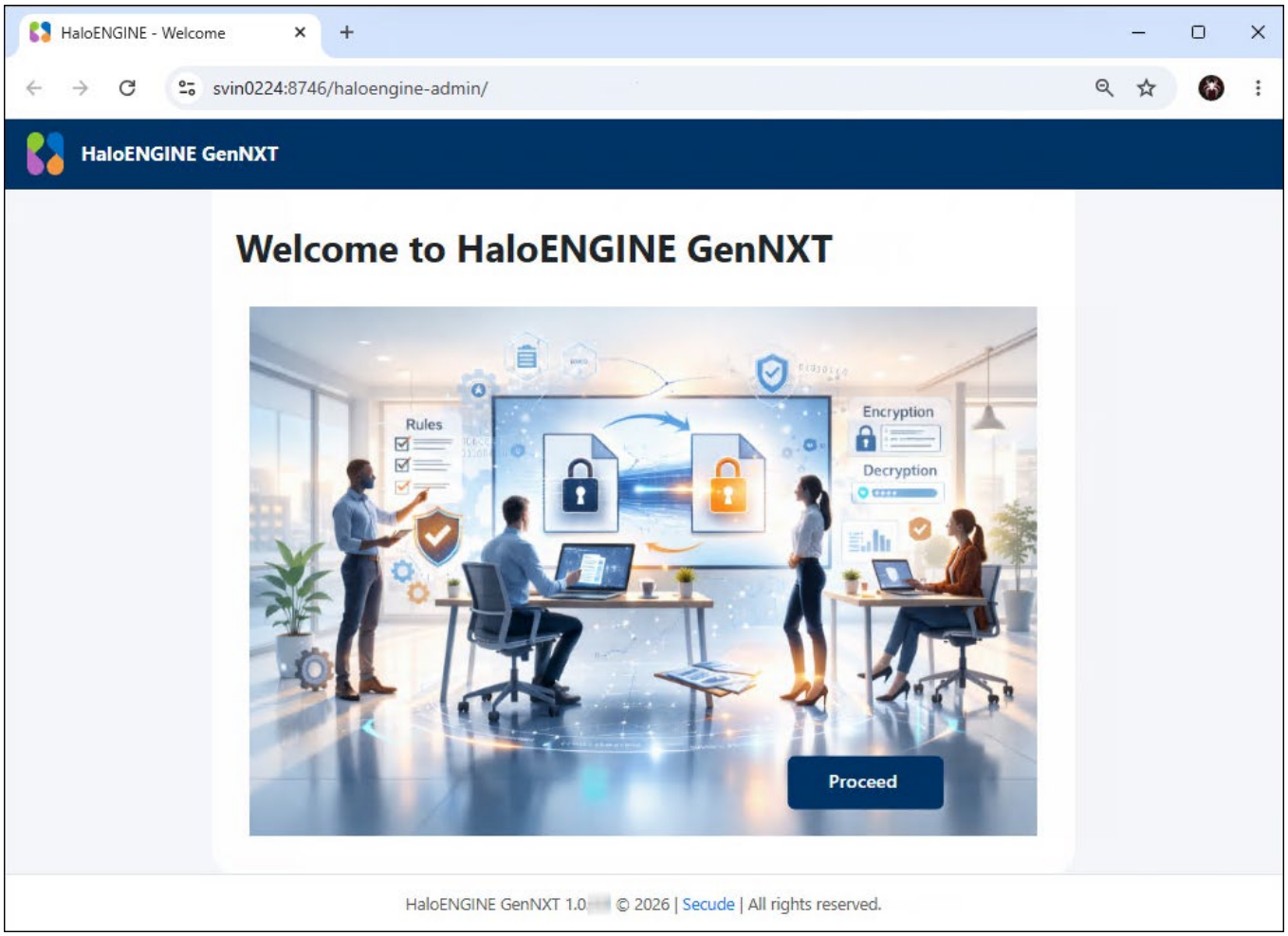
5.2. Initial Configuration of the HaloENGINE GenNXT Admin Portal

This section describes how to get started with the HaloENGINE GenNXT Admin Portal. Complete the following tasks when you access the Admin Portal for the first time:

- **Create an administrator account** – Create the default administrator account.
- **Log in** – Log in using the administrator account.
- **Activate the license** – Upload the license file to access the Admin Portal. The license defines the available features and supported client systems. Only the client systems included in the license are available for configuration.

5.2.1. Welcome Page

The first time you access the HaloENGINE GenNXT Admin Portal, the Welcome page appears. Click **Proceed** to begin the initial configuration.



Welcome page

5.2.2. Create an Administrator Account

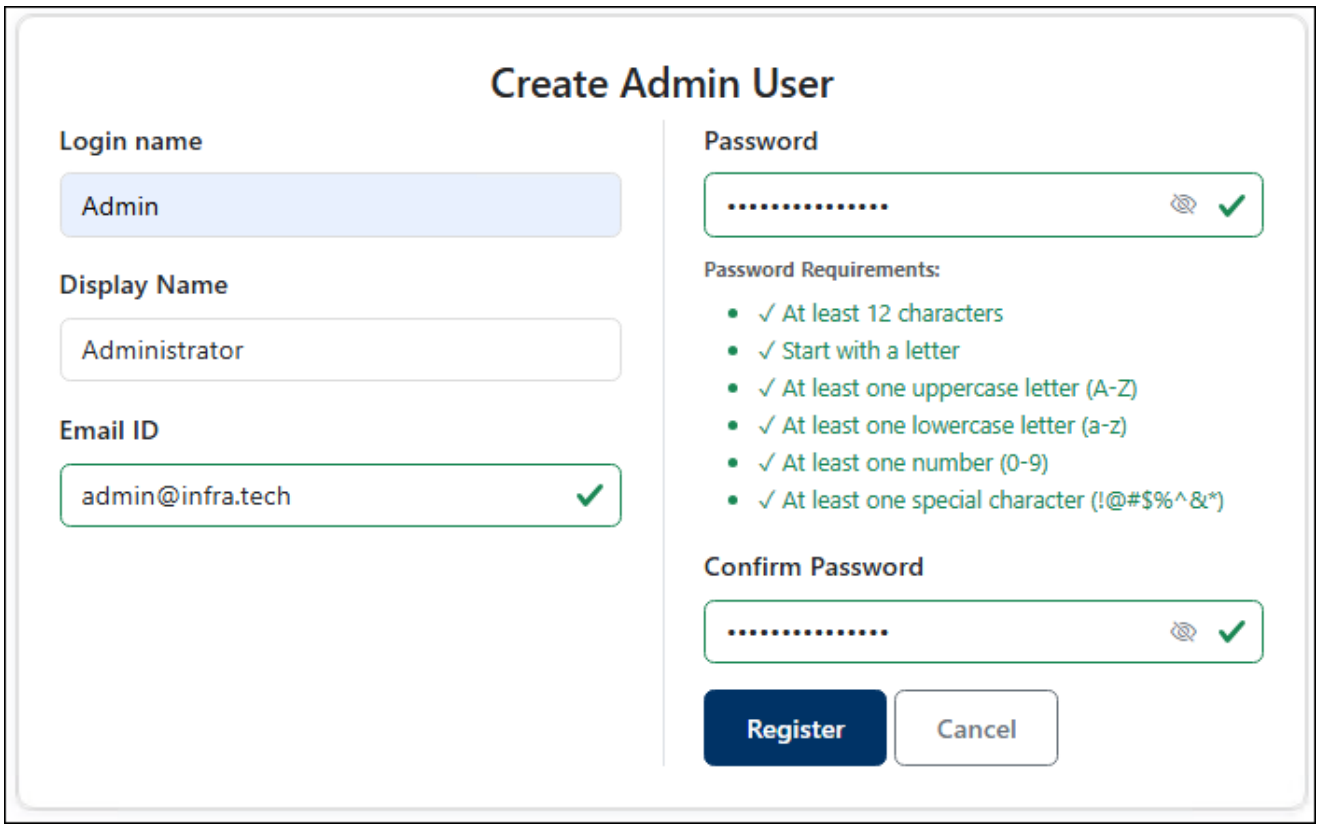
When you open the Admin Portal for the first time, you must create the default super administrator account. This account has **Super Admin** privileges and unrestricted access to all features in the Admin Portal.

To create the administrator account, follow these steps:

1. In **Login Name**, enter a user name. **Example:** `Admin`
2. In **Display Name**, enter the administrator's full name. **Example:** `Administrator`
3. In **Email ID**, enter a valid email address. **Example:** `admin@infra.tech`
4. In **Password**, enter a password that meets the following requirements:
   - At least **12 characters**
   - Starts with a **letter**
   - Includes at least **one uppercase letter (A–Z)**
   - Includes at least **one lowercase letter (a–z)**
   - Includes at least **one number (0–9)**
   - Includes at least **one special character** (`! @ # $ % ^ & *`)

     Example: `Admin@Portal123`

   Note: As you enter the password, each requirement is validated in real time. A **green check mark** indicates that the requirement is met. A **red cross** indicates that the requirement is not met.
5. In **Confirm Password**, re-enter the password.



New user creation

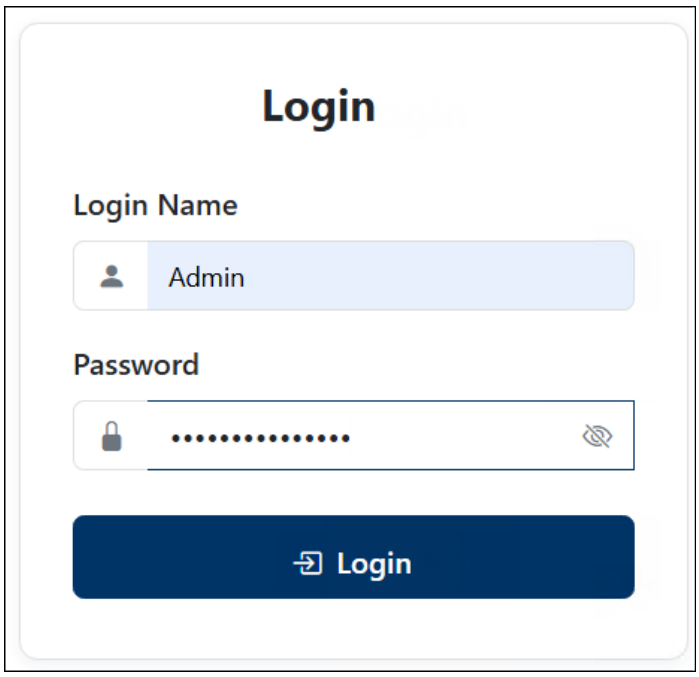
6. To display the credentials, click the **Show/Hide** (eye) icon.
7. Click **Register**.

Result: The Admin Portal creates the administrator account, displays a confirmation message, and redirects you to the **Login** page.

5.2.3. Log in to the Admin Portal

After you create the administrator account, the system redirects you to the **Login** page.

1. In **Login Name**, enter your username.
2. In **Password**, enter your password.



Login page

3. To display the credentials, click the **Show/Hide** (eye) icon.
4. Click **Login**.

Result: On your first login, the **Upload License File** page appears.

Next step: Activate the license provided by Secude, as described in the next section.

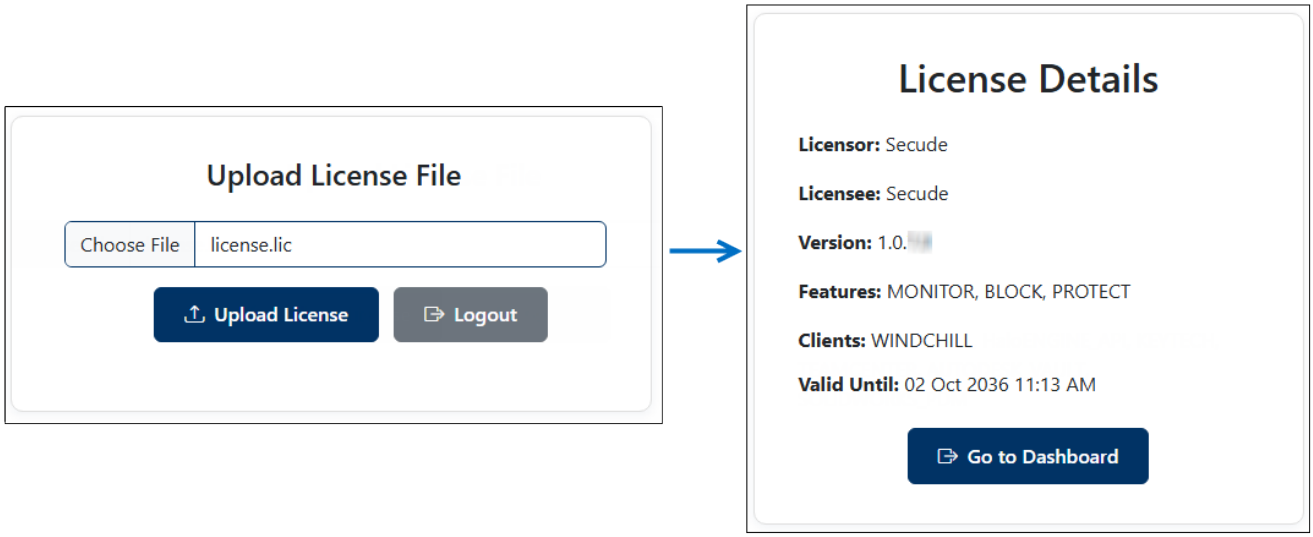
5.2.4. Activate the License

To access all HaloENGINE GenNXT features, upload a valid license file.

Prerequisite: Ensure that you have a valid `license.lic` file obtained from Secude.

To upload the license file, follow these steps:

1. On the **Upload License File** page, click **Choose File**.
2. In the **Open** dialog box, select the `license.lic` file. If you do not have a license file or do not want to upload it at this time, click **Logout**.
3. Click **Upload License**.



License page

4. For illustration purposes, the license shown in this example is associated with Windchill.

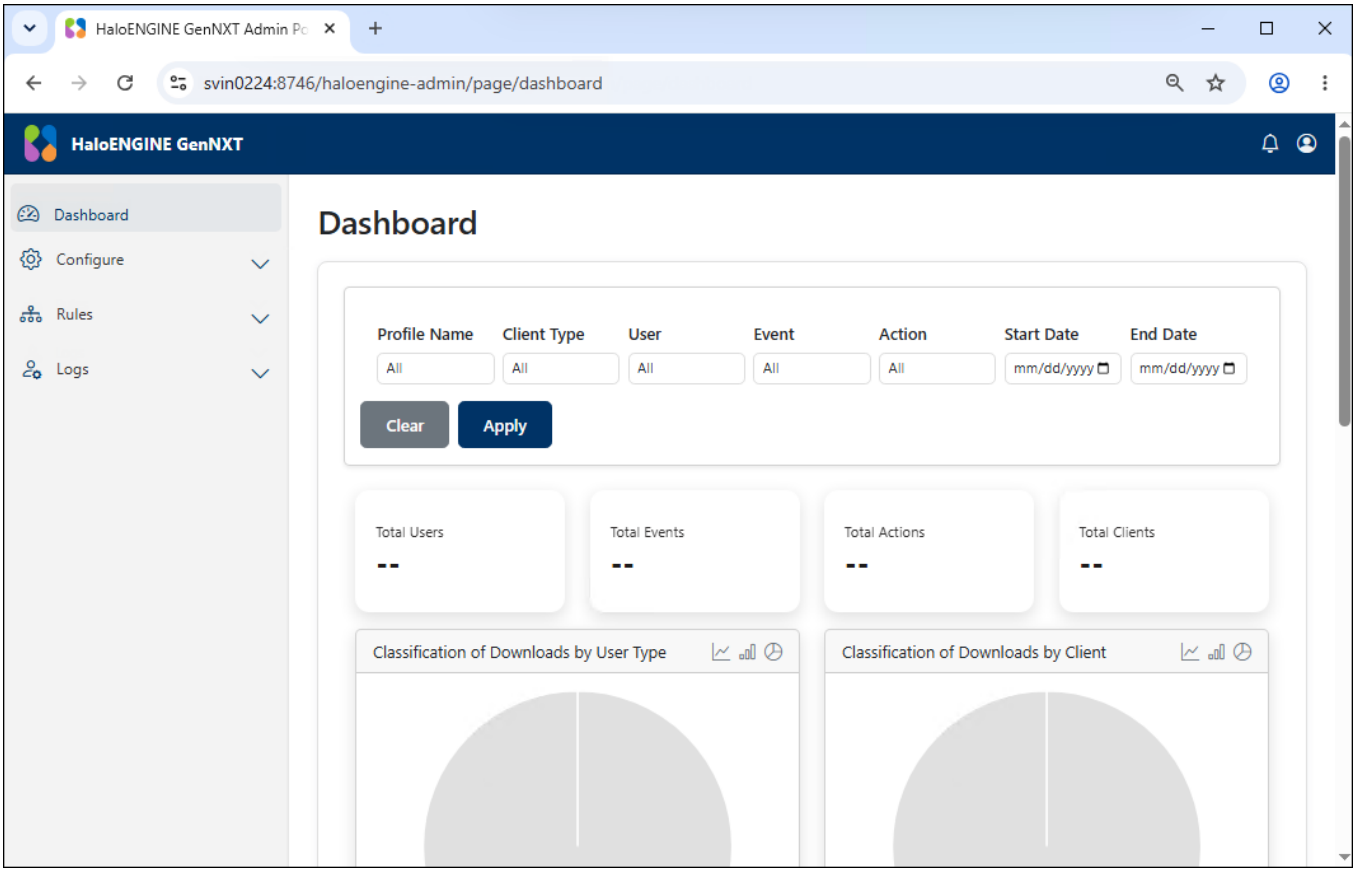
Result: The **License Details** page displays the product version, available features, supported client systems, and the license validity period.

Next step: Click **Go to Dashboard** to open the **Dashboard**. The Dashboard appears automatically on all subsequent logins.

Related task: To renew an expired license, refer to the section "Check License Details or Update the License".

5.2.5. Initial Dashboard View

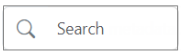
The HaloENGINE GenNXT Dashboard provides an overview of system information, metrics, and file processing activities. During the first login or after a fresh HaloENGINE GenNXT installation, the Dashboard may appear empty because no operational data is available. Once HaloENGINE GenNXT begins processing events, the Dashboard displays the corresponding information.

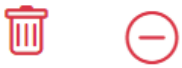
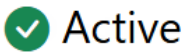
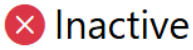


Initial Dashboard View

5.2.6. Understand the Admin Portal UI Elements

This section describes the user interface elements available in the Admin Portal.

S.No	Elements	Description
1		Displays system notifications and alerts.
2		Provides access to account details, password change, and logout options.
3		Filters and displays results based on the specified search criteria.
4		Indicates that the metadata is locked and cannot be deleted.

S.No	Elements	Description
5		Indicates that the selected item can be deleted.
6		Creates a new item.
7		Edits the selected item.
9		Moves the selected item up or down in the list.
10		Allows you to select a date from the calendar.
11		Opens a list of available options for selection.
12		Indicates the default sensitivity level.
13		Indicates a non-default sensitivity level.
14		Indicates that the profile or rule is active.
15		Indicates that the profile or rule is inactive.

Elements Description

5.3. Configuring HaloENGINE GenNXT

This chapter describes how to configure classification schemas, action rules, logs, and licenses in HaloENGINE GenNXT.

1. **Configuration (Optional)**
   This step is optional. You can configure it during initial setup, later, or use the default settings.
2. **Rules Management (Required)**
   Create classification schemas based on your organization's requirements. Create profiles for client types and add rules. Setting metadata for upload decryption is optional.
3. **Log Management (Optional)**
   This step is optional. You can configure it during initial setup, later, or use the default settings.
4. **Security Settings (Optional)**
   This step is optional. You can configure it during initial setup, later, or use the default settings.

Each of these steps is described in detail in the following sections.

> **Client Type**
> For illustration purposes, **Windchill** is used as the example client type throughout this chapter. If you use a different client type, select the appropriate client from the **Client Type** selection list (Teamcenter, Autodesk Vault, and SOLIDWORKS PDM) whenever required.

5.3.1. Configuration

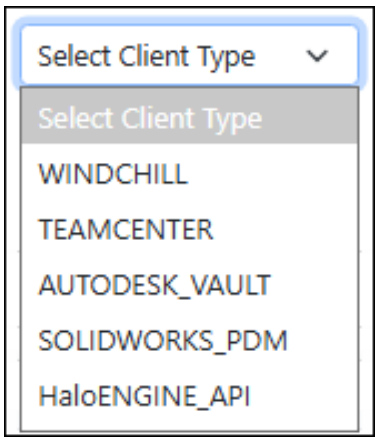
This section describes how to configure HaloENGINE GenNXT, add custom metadata, and view or update the license.

5.3.1.1. Metadata Configuration

The Admin Portal includes **built-in metadata** for each PLM and PDM client. This metadata supports data classification and secure file downloads. The metadata assigned to a label determines label derivation for file encryption in HaloENGINE GenNXT. Administrators can add custom metadata based on organizational requirements. After you create custom metadata, you can use it to define file rules.

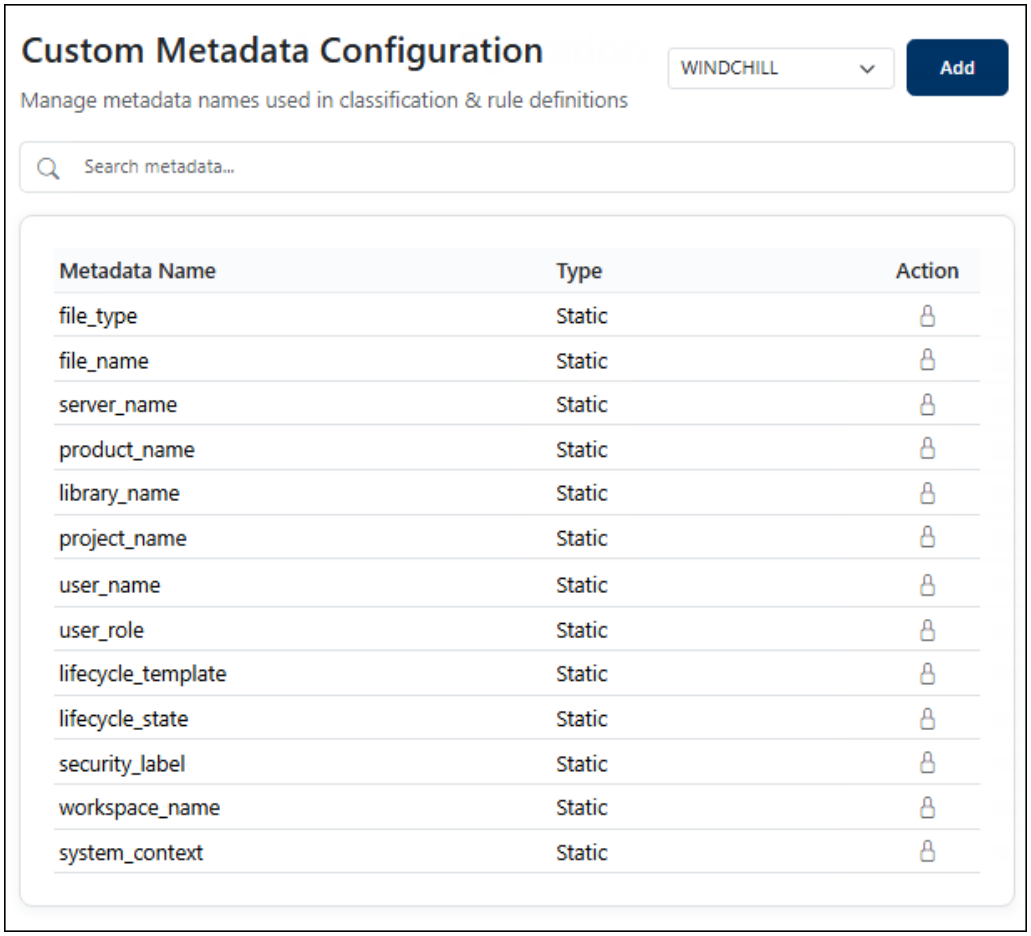
To view and add metadata, follow these steps:

1. In the left navigation bar, click **Configure**, and then click **Metadata**.
2. The **Custom Metadata Configuration** page appears.
3. From the **Client Type** list, select a client type: **Windchill**, **Teamcenter**, **Autodesk Vault**, or **SOLIDWORKS PDM**. If the license file contains only one client type, only that client appears in the list. If the license includes multiple client types, all licensed clients appear in the list.



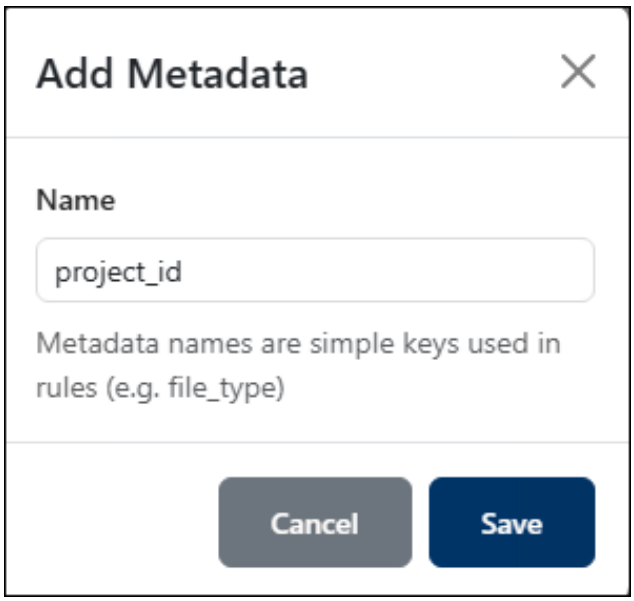
Client types

4. The built-in metadata for the selected client type appears on the page.



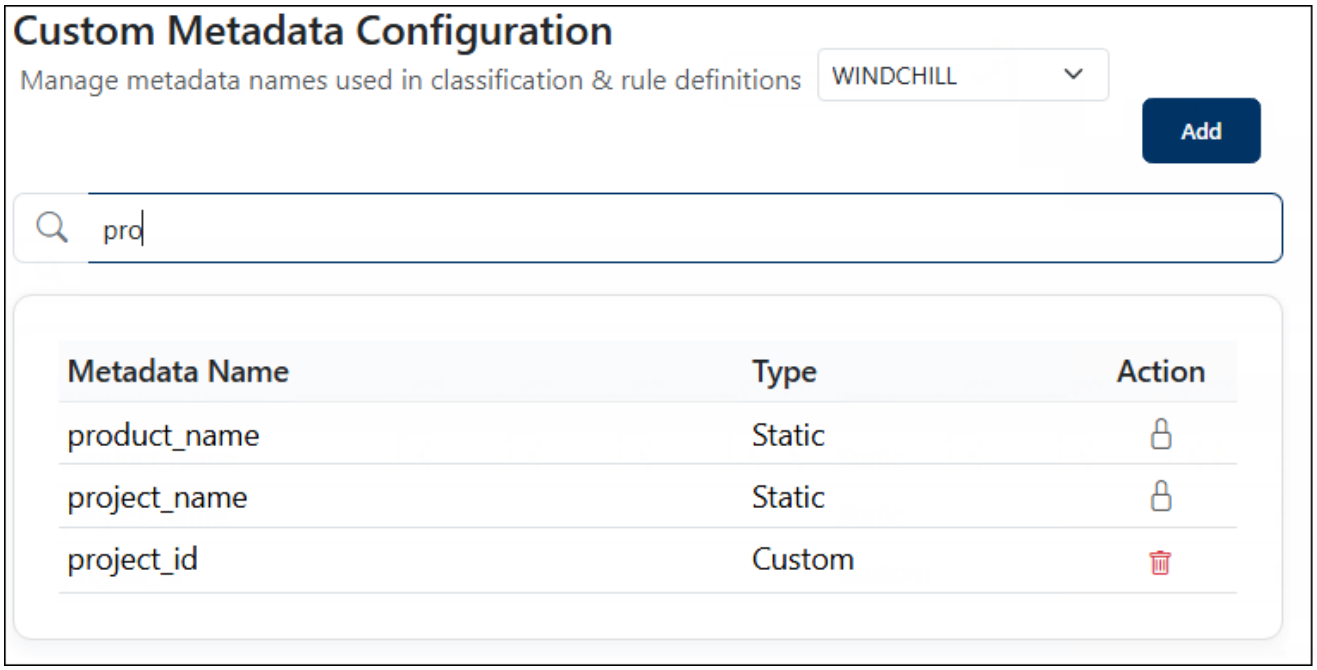
Windchill built-in metadata

5. To add custom metadata, click **Add**.
6. The **Add Metadata** dialog box appears.



Add metadata dialog

7. Enter a name for the metadata (for example, `project_id`).
8. Click **Save**.



Custom metadata added for Windchill client type

Result:

- The built-in metadata is displayed first, followed by the custom metadata. Custom metadata is added to the end of the list on the **Custom Metadata Configuration** page.
- To search for metadata, enter text in the search bar. Matching results appear in the list.

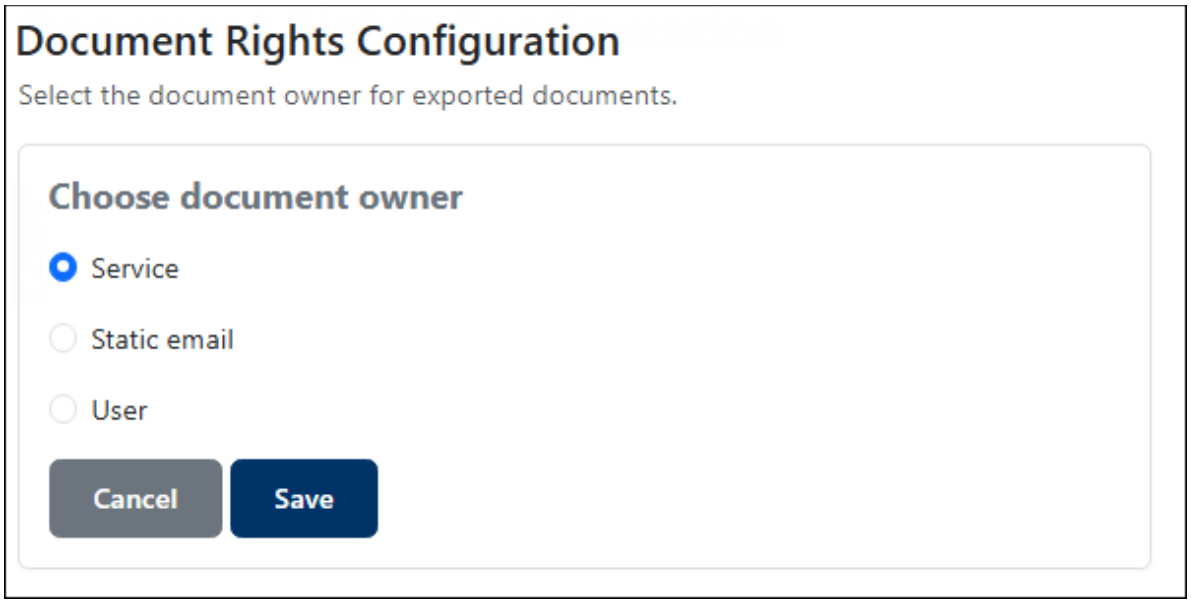
- Built-in metadata is categorized as **Type: Static**, and custom metadata is categorized as **Type: Custom**. For a description of each metadata field, see the corresponding client type section: Windchill, Teamcenter, Autodesk_Vault, or SOLIDWORKS PDM.
- To delete custom metadata, click the **Delete** icon in the **Action** column. Static metadata cannot be deleted.

5.3.1.2. Configure Owner Rights

This feature defines how a user is identified as the owner of exported documents. Supported clients include Teamcenter, Windchill, and Autodesk_Vault. However, this configuration does not apply to the SOLIDWORKS PDM client because document protection is managed directly by HaloCAD for SOLIDWORKS PDM.

To configure owner rights, follow these steps:

1. In the left navigation pane, click **Configure**, and then click **Owner**.
2. The **Document Rights Configuration** page appears.



Owner Rights

3. Select one of the following options:
   - **Service (default)** – Uses the Application ID that initializes the HaloENGINE GenNXT Tomcat Service as the document owner.
   - **Static email** – Uses the email address entered in the text box as the document owner.
   - **User** – Derives the email address from the connected client (Windchill, Teamcenter, and Autodesk_Vault).
4. Click **Save**.

Result: A confirmation message appears, indicating that the owner rights are updated successfully.

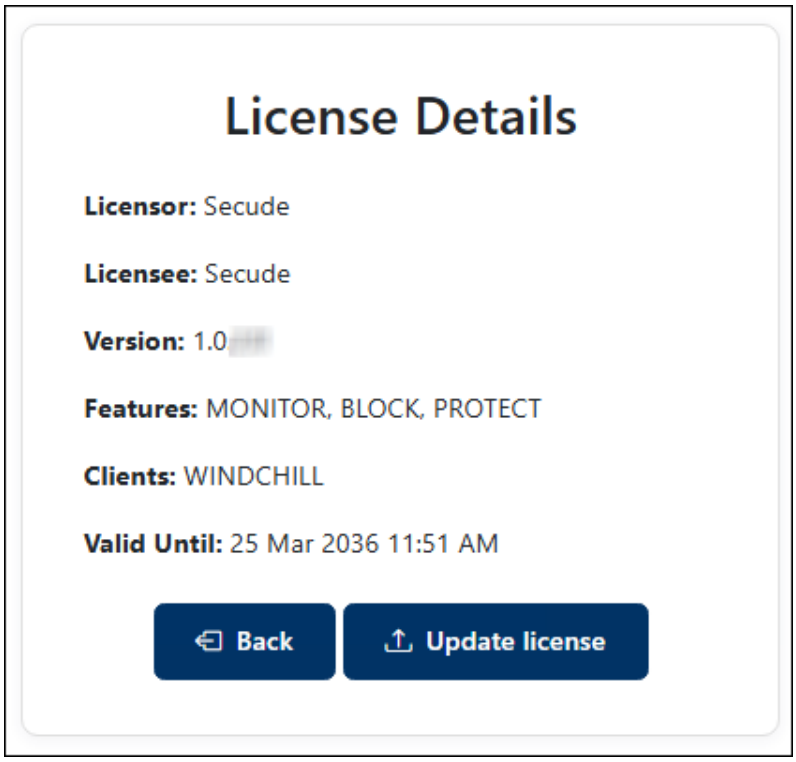
5.3.1.3. Check License Details or Update the License

The **License** page allows the administrator to view the license status and update the license when a renewal is required.

- Verify the license validity period and activated features.
- Upload the renewed license obtained from Secude.

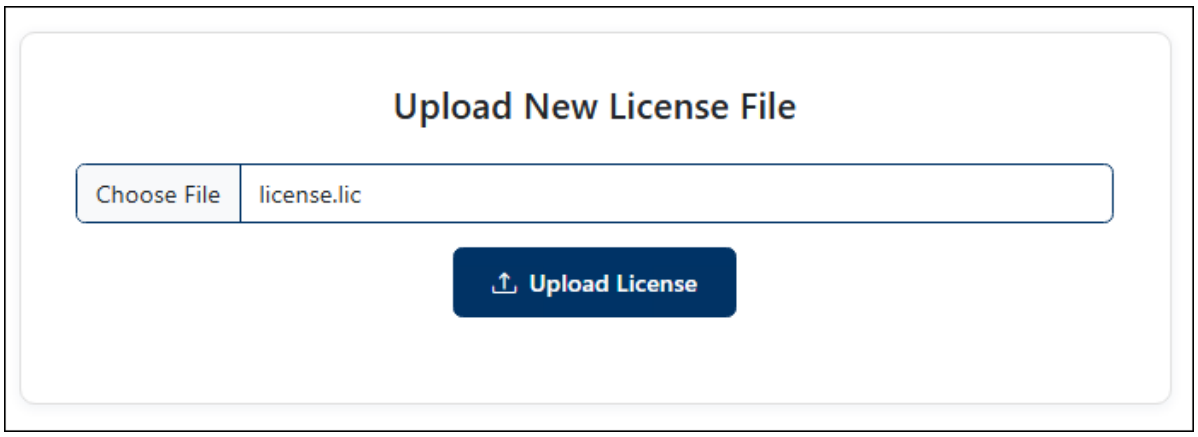
To view and update the license, follow these steps:

1. In the left navigation bar, click **Configure**, and then click **License**.
2. The **License Details** page appears and displays the license information.



Viewing license details

3. To update the license, click **Update License**.
4. On the **Upload New License File** page, click **Choose File**, and then select the `license.lic` file in the **Open** dialog box.



Uploading a new license

5. Click **Upload License**.

Result:

- The new license file is uploaded.
- A confirmation message appears, and the **License Details** page displays the updated license information with the new validity period.
- When the license approaches its expiration date, a notification appears. Refer to the Notification section.

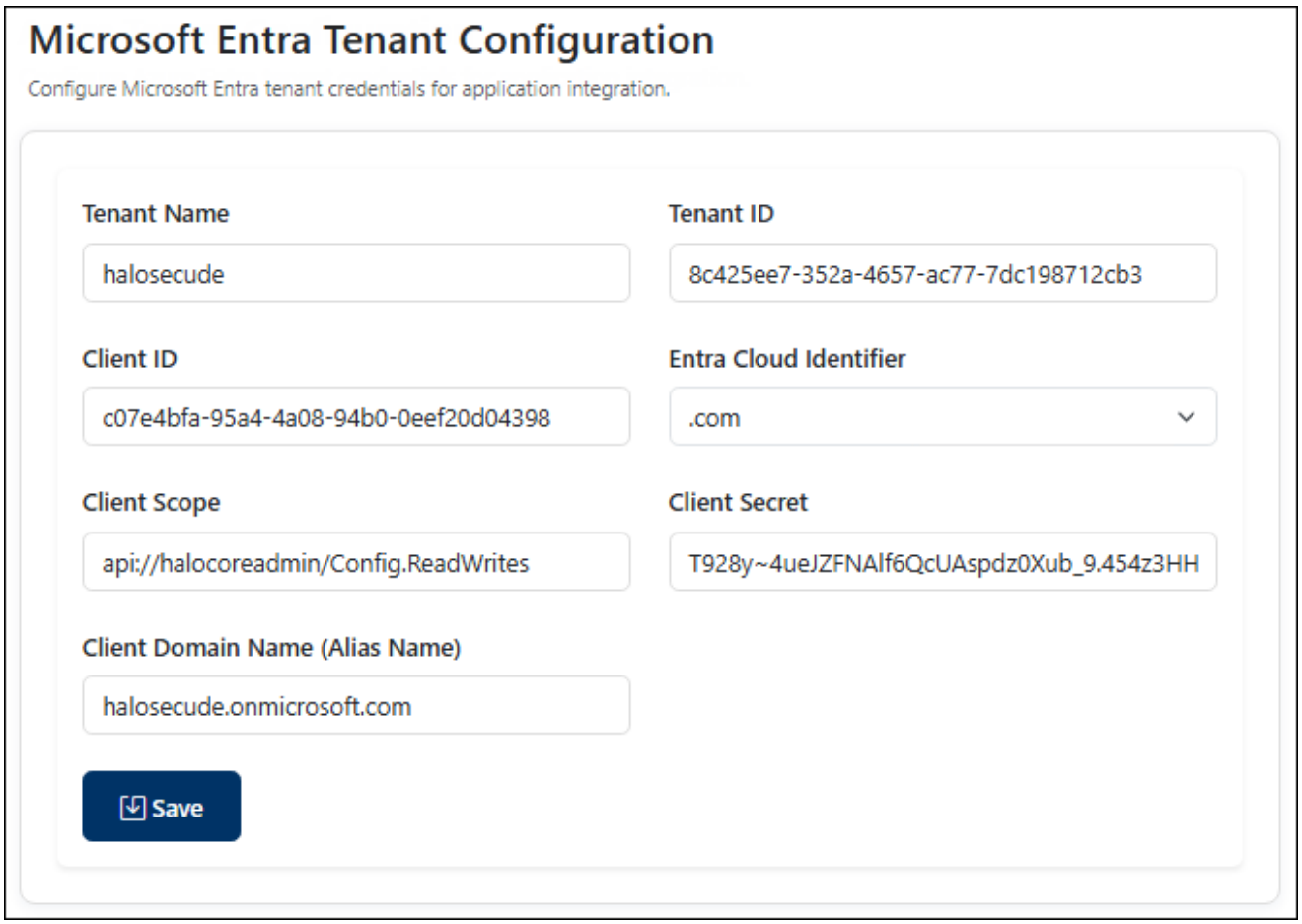
5.3.1.4. Microsoft Entra

The **Micro Entra Tenant Configuration** page enables you to configure the Microsoft Entra tenant and domain details required for user authentication and validation in HaloENGINE GenNXT.

Prerequisite: Ensure that you have configured the required details as described in **Step 3** in the Configure Microsoft Entra ID for User Management section.

To configure the tenant details, follow these steps:

1. In the left navigation bar, click **Configure**, and then click **Microsoft Entra**.
2. The **Microsoft Entra Configuration** page appears.
3. Enter the following details.



Microsoft Entra Tenant Configuration

a. **Tenant Name** – Enter the name of your Microsoft Entra tenant. For example, if your tenant domain is `Contoso.onmicrosoft.com`, enter `Contoso`.

   Note: The tenant name can contain a maximum of 30 characters. Only alphanumeric characters, hyphens, and underscores are allowed. Ensure that the tenant name specified in the **Redirect URL** exactly matches the **Tenant Name** configured in the Admin Portal. This field is case-sensitive.

b. **Tenant ID** – Enter the unique identifier of your Microsoft Entra ID instance. For example, `8c425ee7-352a-4657-ac77-7dc198712cb3`.

c. **Client ID** – Enter the identifier assigned when registering the application. For example, `c07e4bfa-95a4-4a08-94b0-0eef20d04398`.

d. **Azure Cloud Identifier** – Select the appropriate identifier from the list. For example, `.com` or `.us`.

e. **Client Scope** – Enter the scope assigned to the application. For example, `api://halocoreadmin/Config.ReadWrites`.

f. **Client Secret** – Enter the secret assigned to the application. For example, `T928y~4ueJZFNAlf6QcUAspdz0Xub_9.454z3HH1`.

g. **Client Domain Name (Alias Name)** – Enter an alias name for your domain. For example, `halosecude.onmicrosoft.com`.

4. If any configured detail is incorrect, you cannot sign in using your Microsoft account. Verify all details carefully.
5. Click **Save**.

Result:

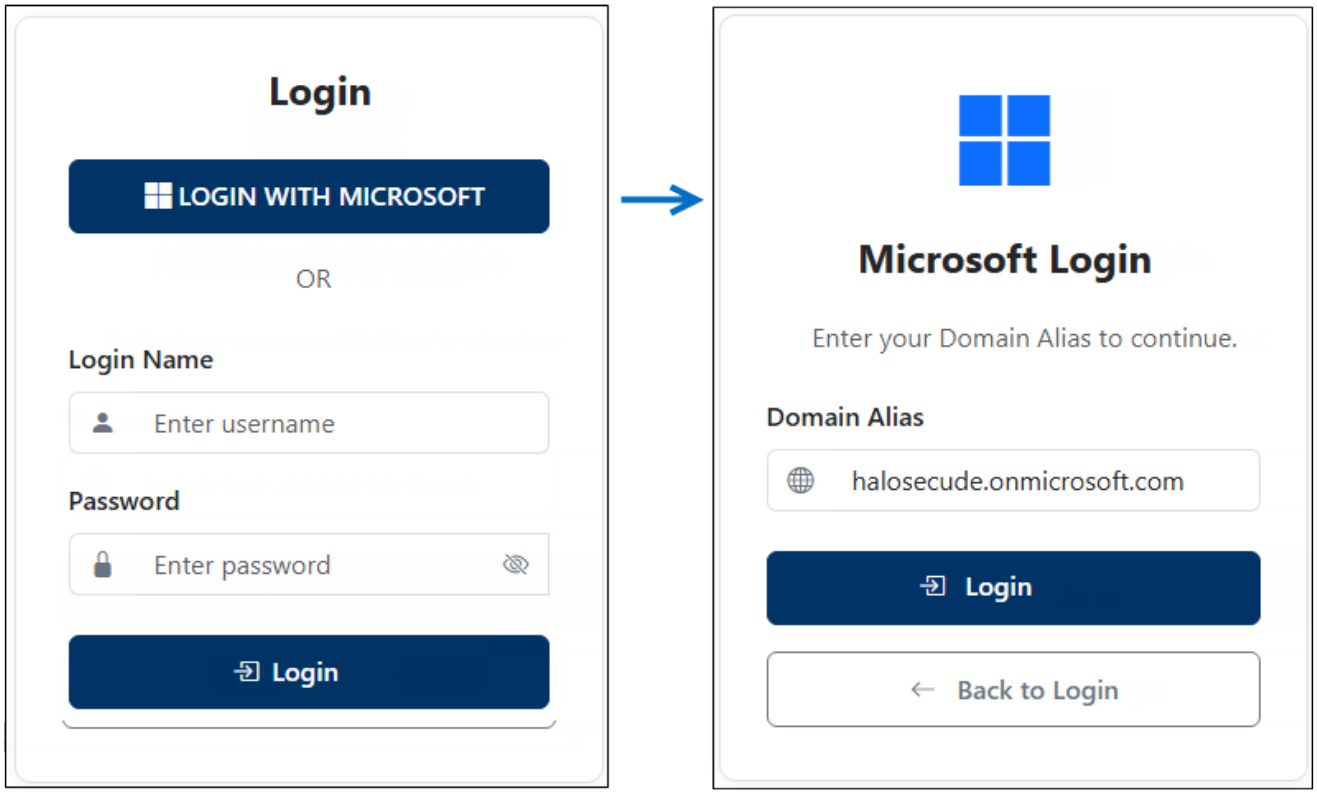
- The Microsoft Entra tenant configuration is saved, and a confirmation message appears.
- To update the configuration, click **Edit**.

What to do next:

Log out of the current Admin Portal session and follow the procedure below to log in using a Microsoft account.

5.3.1.4.1. Sign in using a Microsoft Account

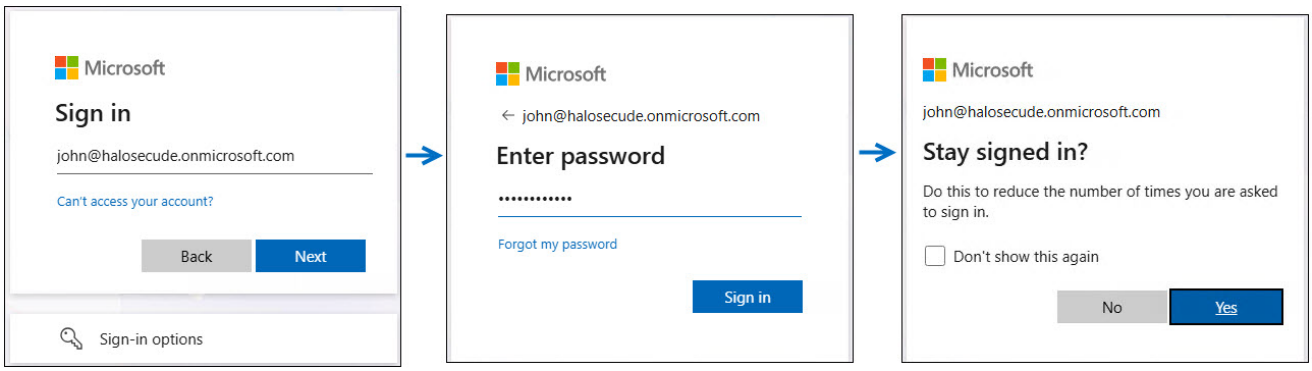
1. The Admin Portal returns to the login page displaying the **Login with Microsoft** option.
2. Click **Login with Microsoft**.



Log in with a Microsoft account

3. The **Microsoft Login** page appears.
4. Enter the **Domain Alias**. For example: `halosecude.onmicrosoft.com`

5. Click **Login**.
6. The **Microsoft sign-in** page appears. Enter the user account credentials and click **Sign in**.



Microsoft sign-in

Note: Ensure that the user is assigned to the appropriate role, as explained in Step 7: Apply Role to Users.

Result

- The **HaloENGINE GenNXT Dashboard** page is displayed.
- The user menu displays the logged-in user's name. For example: `John Smith`.

5.3.1.4.2. Role-Based Access

Users assigned the **ROLE_CUSTOMER_USER** role have read-only access to the Admin Portal. The following access limitations apply:

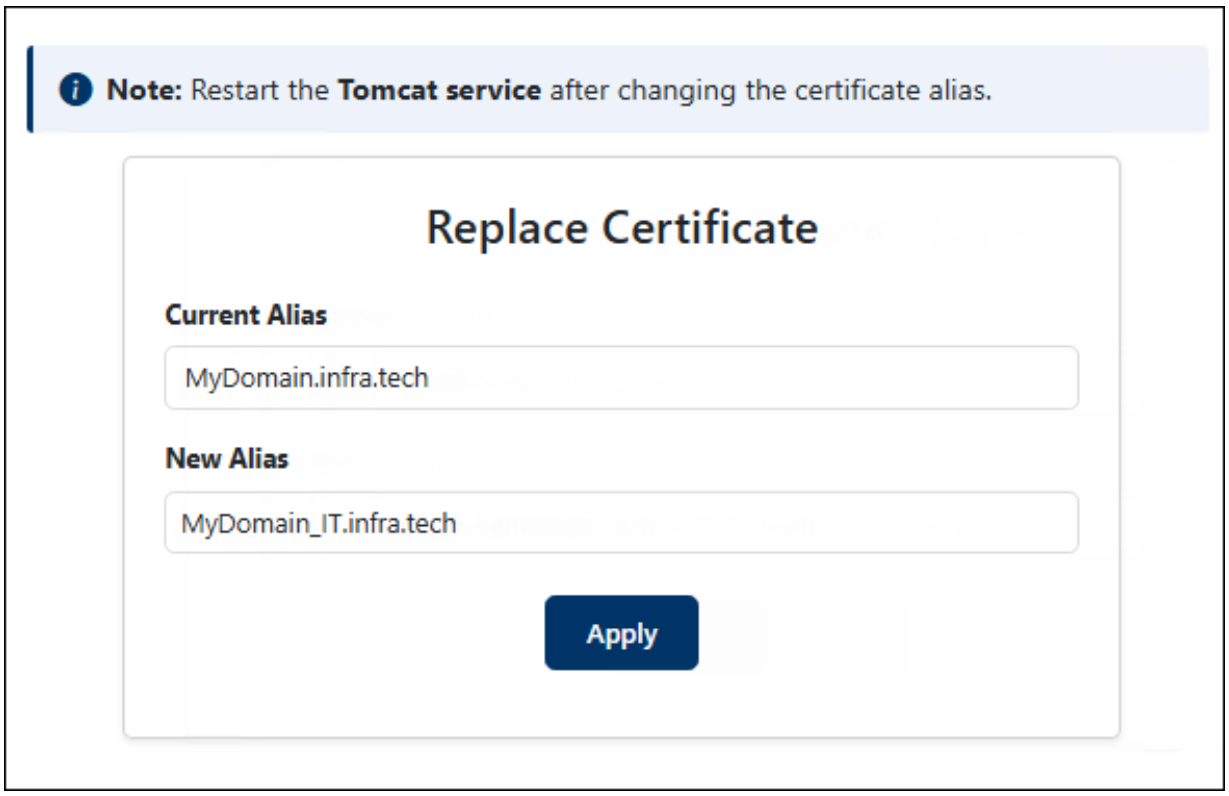
- **Dashboard:** Available
- **Configure:** Disabled
- **Rules:** Available in read-only mode
- **Logs:** Disabled

5.3.1.5. Replace Certificate

The server certificate used for HTTPS may need to be replaced when it expires or is renewed. Use the **Replace Certificate** page to update the certificate alias.

To update the certificate alias, follow these steps:

1. In the left navigation pane, select **Configure**, and then select **Replace Certificate**.
2. The **Current Alias** field displays the current certificate alias. For example: `MyDomain.infra.tech`.



Replace certificate

3. In **New Alias**, enter the alias of the new certificate. If an alias is not available, enter the **Common Name** of the certificate. For example: `MyDomain_IT.infra.tech`.
4. Click **Apply**.
5. A confirmation message appears. Click **Yes** to update the certificate details.
6. Restart the **HaloENGINE GenNXT Tomcat Service** to apply the new certificate alias.

Result:

- The new certificate alias is saved and used by the HaloENGINE GenNXT Tomcat Service.
- Log in to the Admin Portal again to continue configuring HaloENGINE GenNXT.

5.3.2. Rules Configuration

This section describes how to configure classification schemas, rules, and metadata rules for download and upload actions.

5.3.2.1. Classification Schema

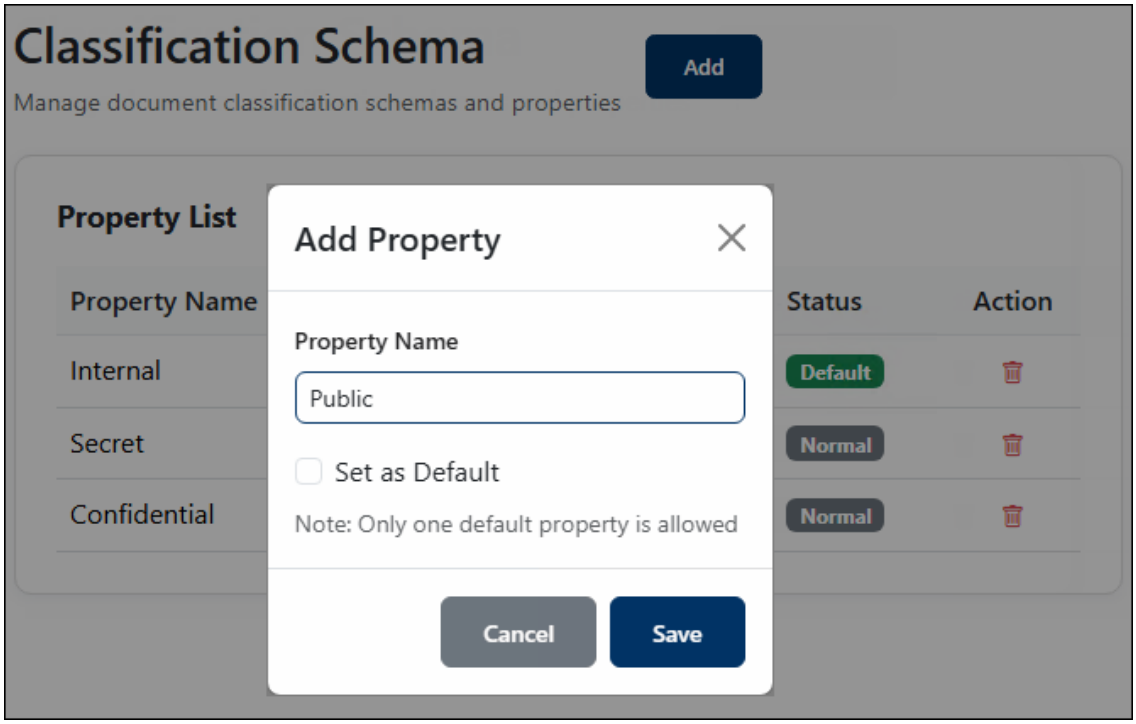
Defines the classification properties and their values used to categorize an organization's data. Once a classification property is created, it becomes available for all client types when creating classification rules. The values, such as Public, Internal, Confidential, and Secret, represent different classification levels. Classification rules use these values with defined conditions to determine how files are classified, labeled, and protected according to the organization's requirements. For more information about rules, refer to the next section, Classification Rules.

Property Name

Specifies the name of a classification property used to categorize an organization's data. This manual uses **Secret**, **Confidential**, **Internal**, and **Public** as examples of classification levels. You can define property names that align with your organization's classification requirements.

Follow these steps to create a classification schema:

1. In the left navigation bar, select **Rules**, and then select **Classification Schema**.
2. The **Classification Schema** page appears.
3. Click **Add**.
4. The **Add Property** dialog appears.

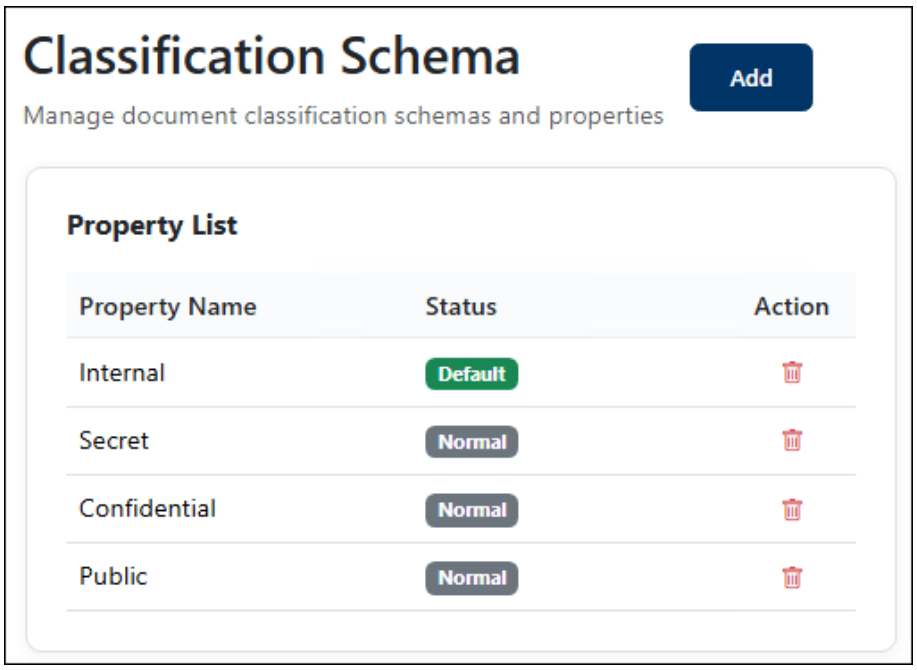


Add property dialog

5. Enter a name for the property you want to define.
6. To set the property as the default, select the **Set as Default** checkbox. The first property is selected as the default automatically.

Note: Only one property can be set as the default at a time.

7. Click **Save**.



Classification Schema list

Result:

- The new property is added to the list and displayed on the page with a **Status** value:
  - **Default** – Indicates that the property is set as the default.
  - **Normal** – Indicates that the property is not set as the default.
- To change a property status from **Default** to **Normal**, or vice versa, click the **Status** value. When prompted, confirm the change by clicking **OK**.
- To delete a property, click the **Delete** icon under the **Action** column. Note: You cannot delete the **Default** property directly when it is associated with one or more rules. To delete the **Default** property, first delete all the associated rules, and then delete the **Default** property.
- In this example, **Secret**, **Confidential**, **Internal**, and **Public** are defined as sample property names, with **Internal** configured as the default property.

Default Property

If no classification rule matches the file, HaloENGINE GenNXT uses the default property configured in the classification schema.

For example, if **Internal** is configured as the default property, HaloENGINE GenNXT applies **Internal** when no classification rule matches the file.

For file downloads, HaloENGINE GenNXT handles the request according to the **Fail-Safe Mode** configured in the PLM client:

- In **Strict** mode, HaloENGINE GenNXT blocks the file download if an error occurs.
- In **Tolerant** mode, HaloENGINE GenNXT allows the file download even if an error occurs.

5.3.2.2. Classification Rules

Classification rules define the conditions used to determine how a file is processed. Each rule consists of a **Pre-Expression**, **metadata**, **condition**, **value**, and **action**.

- **Pre-Expression:** Defines a group of metadata values used to evaluate the rule.
- **Metadata:** Specifies information or properties associated with a file that can be used to evaluate the rule.
- **Condition:** Specifies how HaloENGINE GenNXT compares the selected metadata with the specified value. The available conditions are **equal to** and **not equal to**.
- **Value:** Specifies the information that HaloENGINE GenNXT uses to evaluate the selected metadata against the specified condition.
- **Action:** Specifies how HaloENGINE GenNXT processes the file when the rule conditions are met. You can select **Block** or **Label**. If you select **Label**, you must also select an MPIP label. If you select **Block**, an MPIP label is not required.

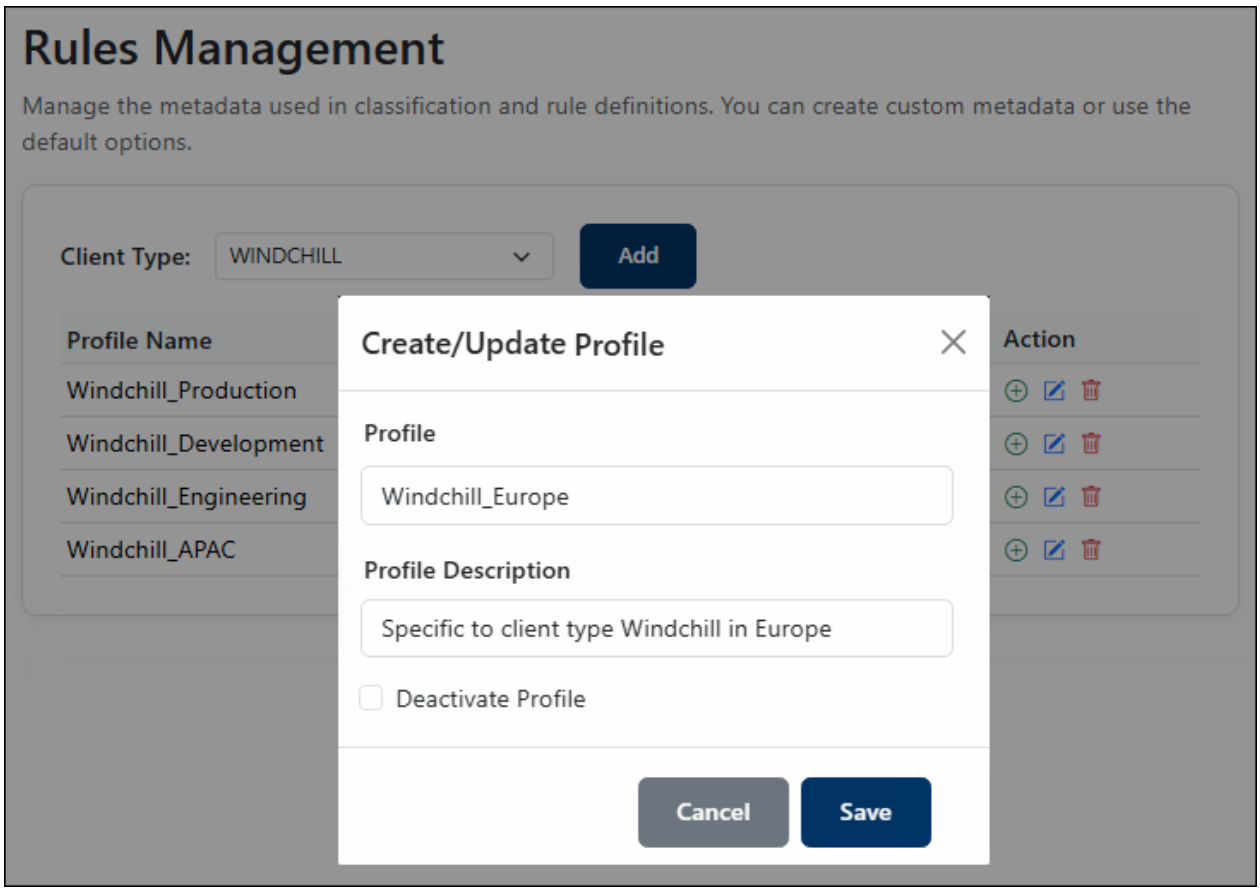
Creating classification rules involves two steps: first, create a profile for the required teams in the organization, and then add rules to the profile.

5.3.2.2.1. Create or Update Profile

A profile stores the classification settings, rules, and metadata for a specific PLM or PDM client. You can create a new profile or update an existing profile to manage its rules and metadata. A client type can have multiple profiles, and each profile can contain multiple classification schemas.

Follow these steps to create a profile:

1. In the left navigation bar, select **Rules**, and then select **Rules**.
2. The **Rules Management** page appears.
3. From the **Client Type** list, select a client type: **Windchill**, **Teamcenter**, **Autodesk Vault**, or **SOLIDWORKS PDM**. If the license file contains only one client type, only that client appears in the list. If the license includes multiple client types, all licensed clients appear in the list.
4. Click **Add**.
5. The **Create/Update Profile** dialog appears.



Create/update Profile dialog

6. In **Profile**, enter a name for the profile.
7. In **Profile Description**, enter a description for the profile.
8. Click **Save**.
9. Repeat the preceding steps to create additional profiles.

Result: The new profiles are added to the list with the following information:

- **Profile Name** – Name of the profile.
- **Rule Count** – Indicates the number of rules associated with the profile. Initially, it displays **0**. After you add rules, it updates to show the actual number of rules.
- **Status** – Indicates whether the profile is active or inactive.
- **Action** – Indicates the actions available for the profile , such as **Add Rule**, **Edit Profile**, and **Delete Profile**.

Next step: The profiles are created. To complete the configuration, add rules to the profiles.

5.3.2.2.2. Add Rules to Profile

The following rule actions are supported when configuring rules for a profile. All file upload and download events are monitored by default.

Rule Action Definitions

- **Block:** Blocks file upload and download operations based on the rule configuration.
- **Label:** Classifies files during upload and download operations. Applies the appropriate MPIP label and embeds the classification label in the file metadata based on the rule configuration.
- **Exclude:** Prevents **Block** and **Label** actions from being applied during file upload and download operations.

Prerequisites:

- Ensure that at least one classification schema is configured.
- If you want to add a rule using a pre-expression, ensure that a pre-expression is configured.

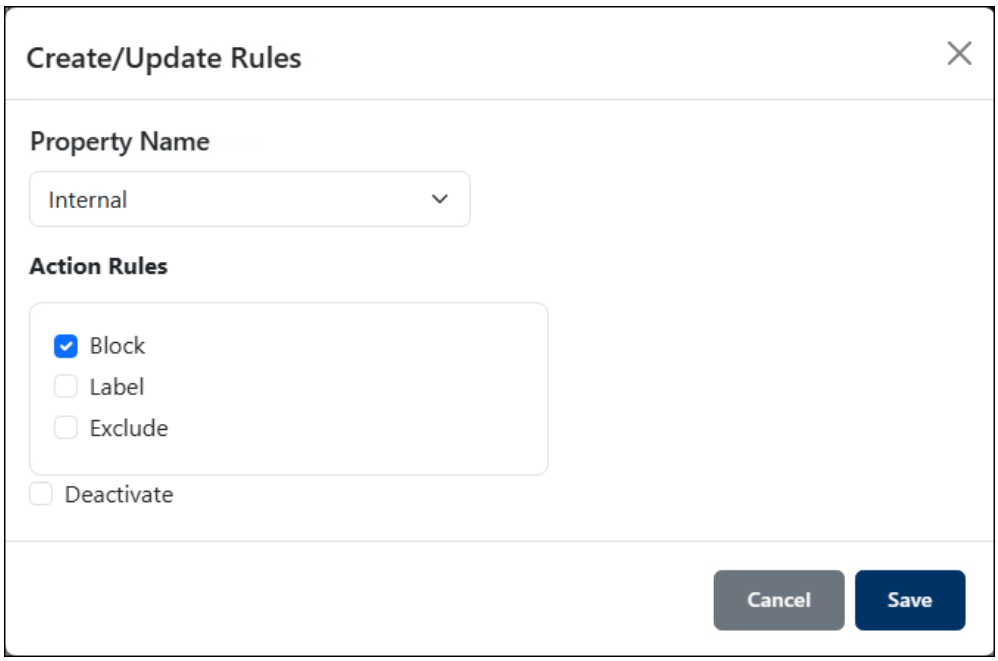
Applying the Default Property

In this manual, **Internal** is configured as the default property. **Secret**, **Confidential**, and **Public** are configured as normal property.

- For the **Label** action with a default property selected, a classification rule is not required and is therefore not displayed.
- For the **Label** action with a non-default property selected, classification rules are displayed.
- For the **Block** action with the default property selected, classification rules are displayed.

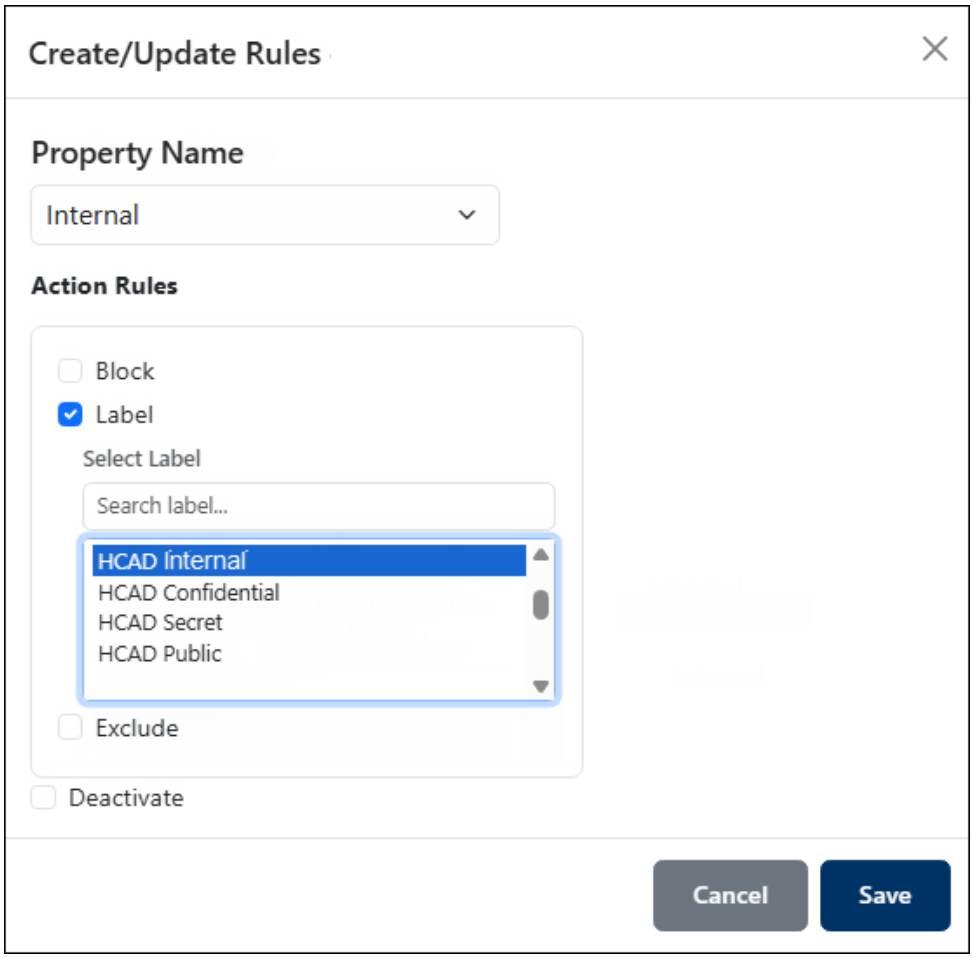
Follow these steps to configure action rules for the default property:

1. Select the profile for which you want to add rules, and click the **Add Rule (+)** icon under the **Action** column.
2. The **Create/Update Rules** dialog appears.
3. From the **Property Name** list, select the default property. For example, select **Internal**.
    a. To block a file download, select **Block**, then continue with step 5.



Default schema with block action

b. To protect the file, select **Label**, and then select an MPIP label. Move to step 5.



Default schema with label action

4. To prevent any classification action from being applied to a file, select the **Exclude** option. When selected, all other action options are disabled, and the file is downloaded without classification, labeling, or protection.
5. Click **Save**.

Block and Label Rules

Use **Block** and **Label** rules to define how HaloENGINE GenNXT processes files when a **non-default property** is selected.

Follow these steps to configure the Block and Label action rules:

1. Select the profile for which you want to add rules, and then click the **Add Rule (+)** icon in the **Action** column.
2. The **Create/Update Rules** dialog box appears.
3. From the **Property Name** list, select a property. For example, select **Secret**.
4. Under **Classification Rules**, define the classification conditions.
   a. If you want to add a pre-expression, select the **Pre-Expression** option, and then select a group from the **Value** list. Note: The **Value** field displays a selection list only when you select the **Pre-Expression** option. Otherwise, enter the required value manually.
   b. In the **Metadata** column, select the metadata. For example: `user_role`. For detailed information about the metadata available for each client type, refer to the Metadata Definition section.
   c. In the **Condition** column, select a condition. For example: `equal to`
   d. In the **Value** field, enter a value. For example: `designer`
   e. To add another condition to the rule, click the **Add (+)** icon in the **Action** column. The additional condition is combined with the existing condition by using the **AND** operator. For example, configure the following condition: **Rule 1**
      - **Metadata:** `system_context`
      - **Condition:** `equal to`
      - **Value:** `Domain*`
5. Click **Add**.
6. The rule is added to the **Rules** list.
7. To add additional rules, repeat steps 4 and 5 with different combinations of metadata, conditions, and values. For example, you can configure the following rules:

Rule 2

a. **Metadata:** `project_id` (custom metadata)

b. **Condition:** `equal to`

c. **Value:** `Plant_701`

Rule 3

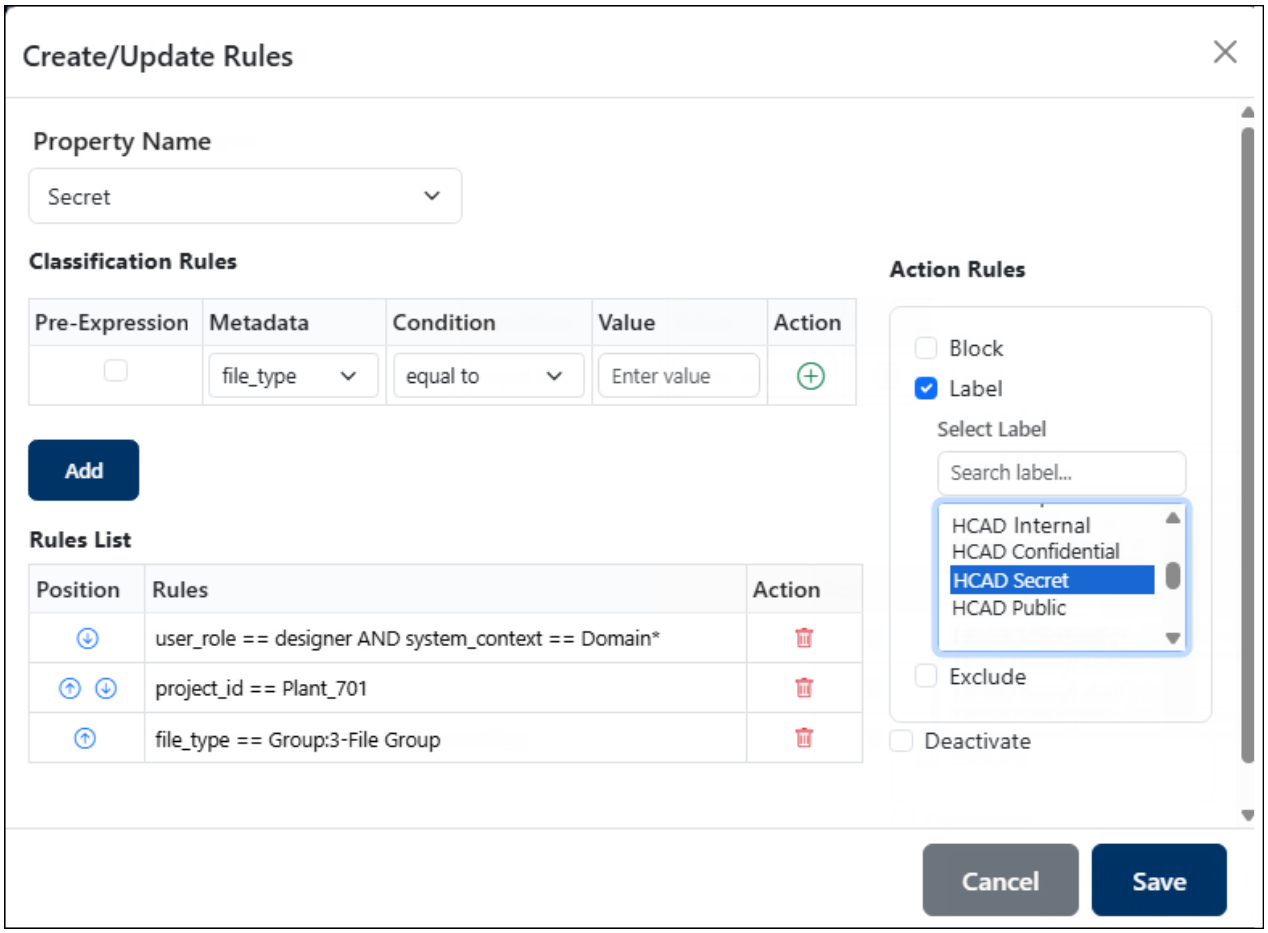
a. **Metadata:** `file_type`

b. **Condition:** `equal to`

c. **Value:** `Group:3-File Group` (a **Pre-Expression** group)

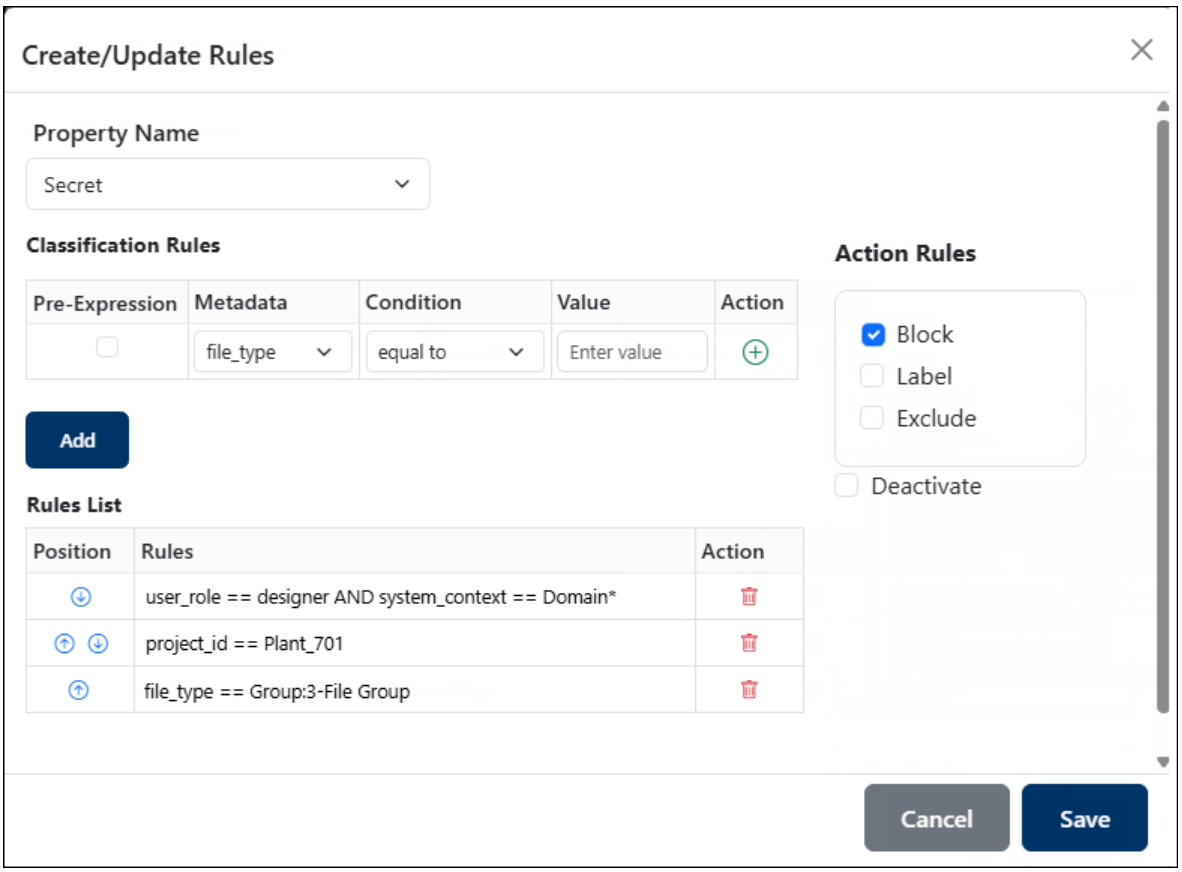
8. Under **Action Rules**, select the action to apply when the classification conditions are met:

   a. To protect the file, select **Label**, and then select an MPIP label from the **Select Label** list.



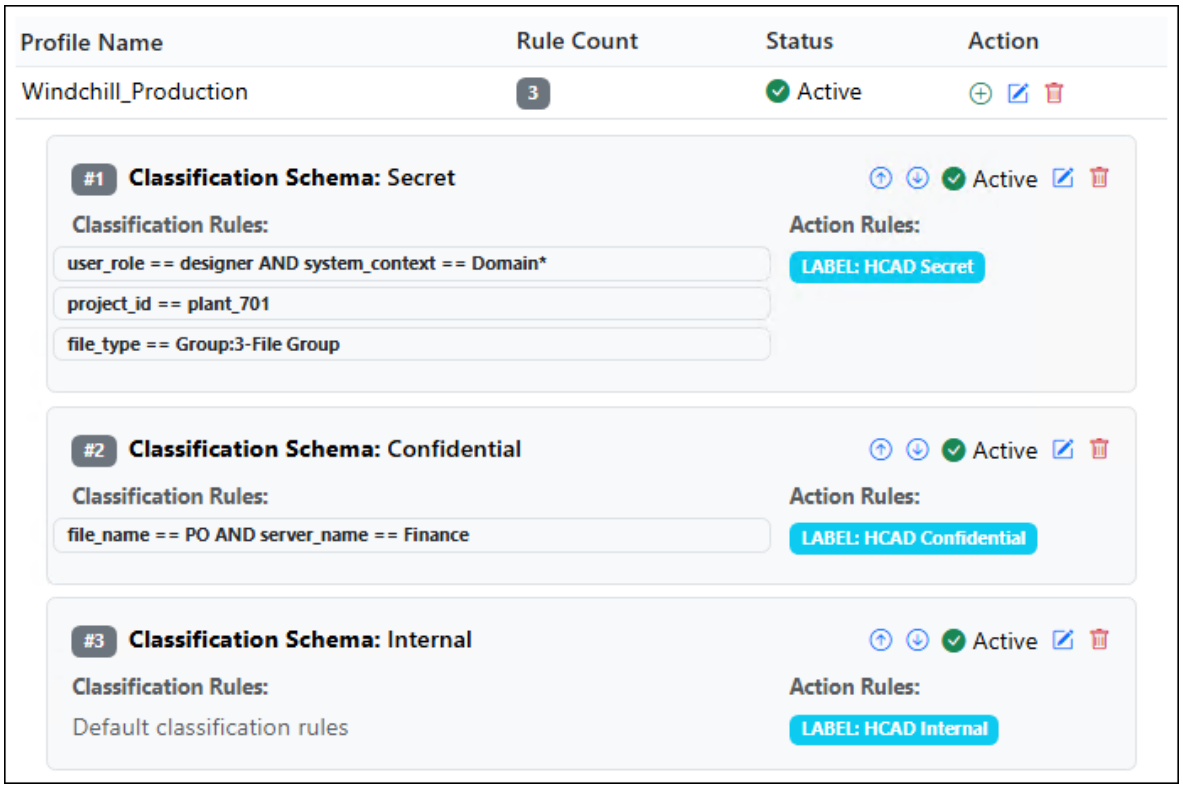
Adding classification rules for Label action

   b. To block the file download, select **Block**. The **Select Label** list is not displayed when you select **Block**.



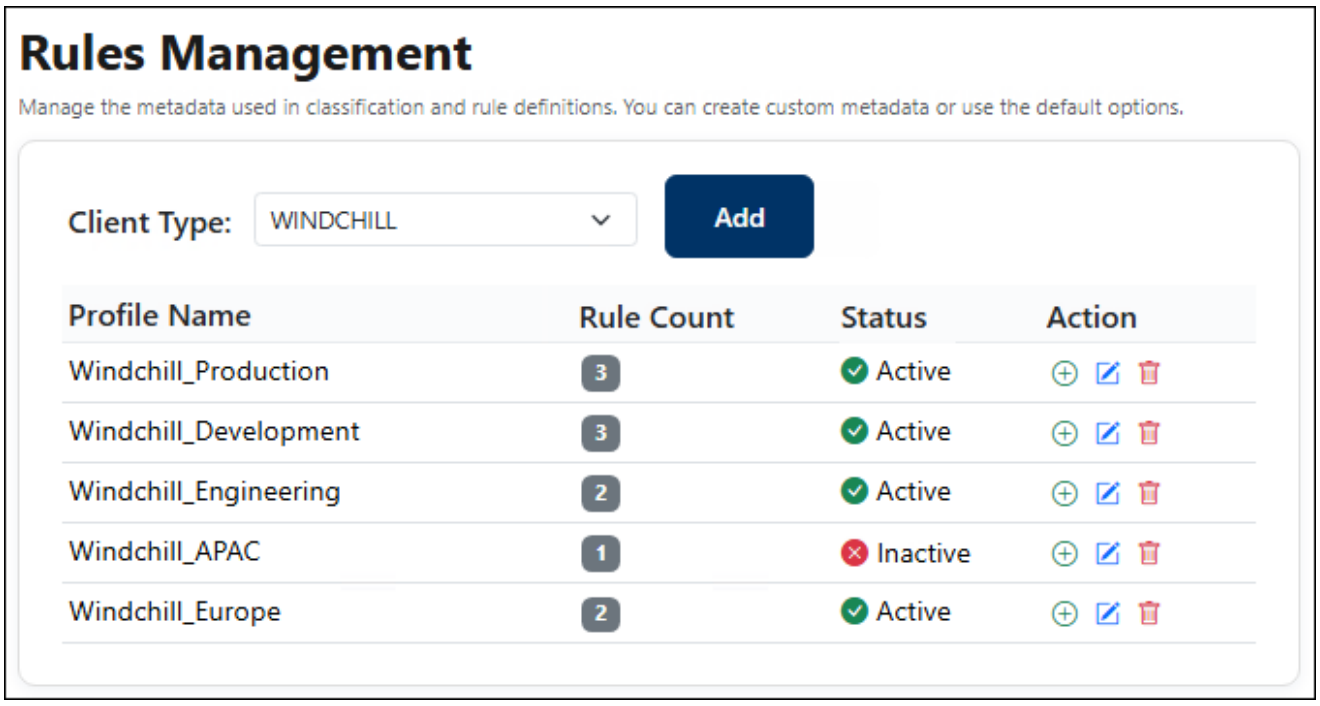
Adding classification rules for Block action

9. Click **Save**.



Action rules

10. Repeat the same steps using different combinations of metadata, conditions, and values to create multiple rules within multiple profiles.



Rule List

Result:

- The rule count updates from **0** to reflect the number of rules added.
- To view a profile, click the profile name. The profile details are displayed.
- To edit a profile, click the **Edit Profile** icon in the **Action** column next to the profile name, and make the required changes, such as updating the description or deactivating the profile.
- To delete a profile, click the **Delete Profile** icon in the **Action** column next to the profile name.
- To deactivate a profile, click the **Profile Name** with the **Active** status. The status changes to **Inactive**. To reactivate the profile, use the same toggle to change the status to **Active**. Alternatively, deactivate the profile from the **Create/Update Profile** dialog box.
- To update a rule, click the profile name, select the classification rule you want to edit, click the **Edit Rule** icon, and make the required changes.
- To delete a rule, click the profile name, select the classification rule you want to delete, and click the **Delete Rule** icon.
- To deactivate a classification rule, select a profile, select the classification schema that contains the rule, and click the **Active** status. The status changes to **Inactive**. To reactivate the rule, use the same toggle to change the status to **Active**. Alternatively, deactivate the rule from the **Create/Update Rules** dialog box.

- To change the priority of a rule or classification property within the profile, click the **Move Up** or **Move Down** arrow icon.

5.3.2.2.3. How HaloENGINE GenNXT Evaluates Rules

For example, consider the `Windchill_Production` property configured with **Rule 1**, **Rule 2**, and **Rule 3**, as shown in the previous section.

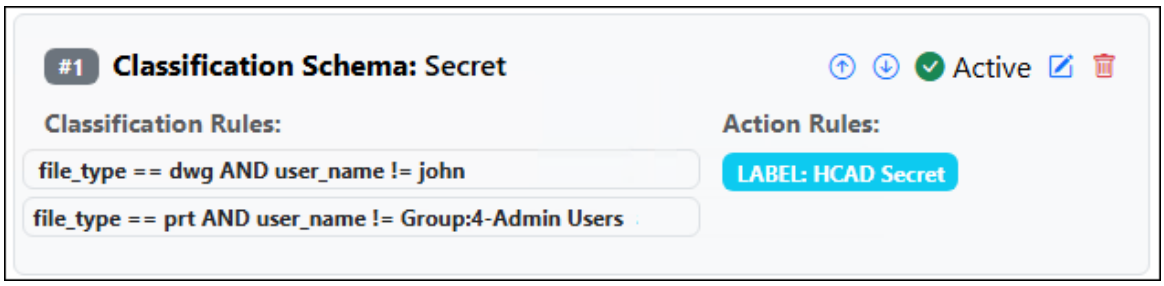
During a file download, HaloENGINE GenNXT evaluates the rules as follows:

1. HaloENGINE GenNXT identifies the applicable **Client Type** and **Property Name**.
2. HaloENGINE GenNXT evaluates the classification rules in the order in which they are listed, from top to bottom.
3. HaloENGINE GenNXT evaluates **Rule 1** first. If all classification conditions are satisfied, HaloENGINE GenNXT applies the configured action.
4. If the conditions in **Rule 1** are not satisfied, HaloENGINE GenNXT evaluates **Rule 2**. This process continues until a matching rule is found.
5. If no classification rule matches, HaloENGINE GenNXT applies the default property, if one is configured.
6. If no default property is configured, no classification action is applied.
7. When the default property is applied, the file is downloaded according to the **Fail-Safe Mode** configured in the PLM client.

5.3.2.2.4. Using Rules for Whitelisting

You can use classification rules to exclude specific users, groups of users, files, or groups of files from file protection or blocking based on your business requirements. To use a group of items in a rule, first create the group as a **Pre-Expression**. You can then use the **Pre-Expression** when creating rules for any client type.

In the following illustration, the first rule excludes a specific user, and the second rule excludes a group of users. You can create additional rules to meet your business requirements.



Using rules for whitelisting

- First rule: All DWG files are protected except files associated with the user `john`.
- Second rule: All PRT files are protected except files associated with the `Group:4-Admin Users` group.

When the conditions are met, HaloENGINE GenNXT applies the configured MPIP label, **HCAD Secret**, to protect the file according to the rule, while excluding the specified users or groups.

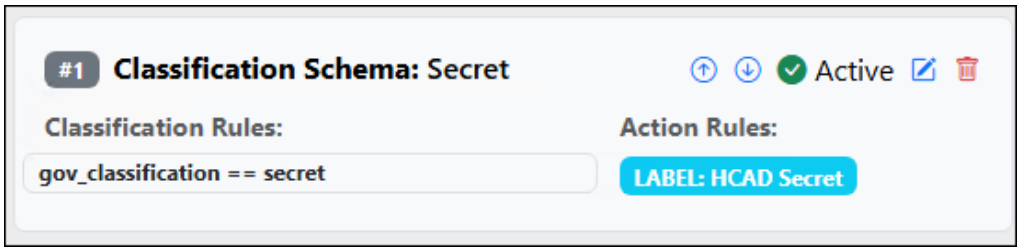
5.3.2.3. Retain Label

The Retain Label feature is available only for Teamcenter PLM. During a file upload event in Teamcenter PLM, HaloENGINE GenNXT uses file-related metadata, such as `ip_classification`, `gov_classification`, and `Custom metadata`, together with the configured label. When a protected file is uploaded, HaloENGINE GenNXT decrypts the file and sets the configured metadata value based on the applicable label.

When the same file is subsequently downloaded, HaloENGINE GenNXT can retain the label applied to the file during the upload. To retain the same label during the download, configure the corresponding metadata and value for the label on the Retain Label page. HaloENGINE GenNXT uses this configuration to apply the same label during the download event.

For example, if the **HCAD Secret** label is configured with the following classification rule:

- **Metadata:** `gov_classification`
- **Condition:** `equal to`
- **Value:** `secret`



Retain label classification rule

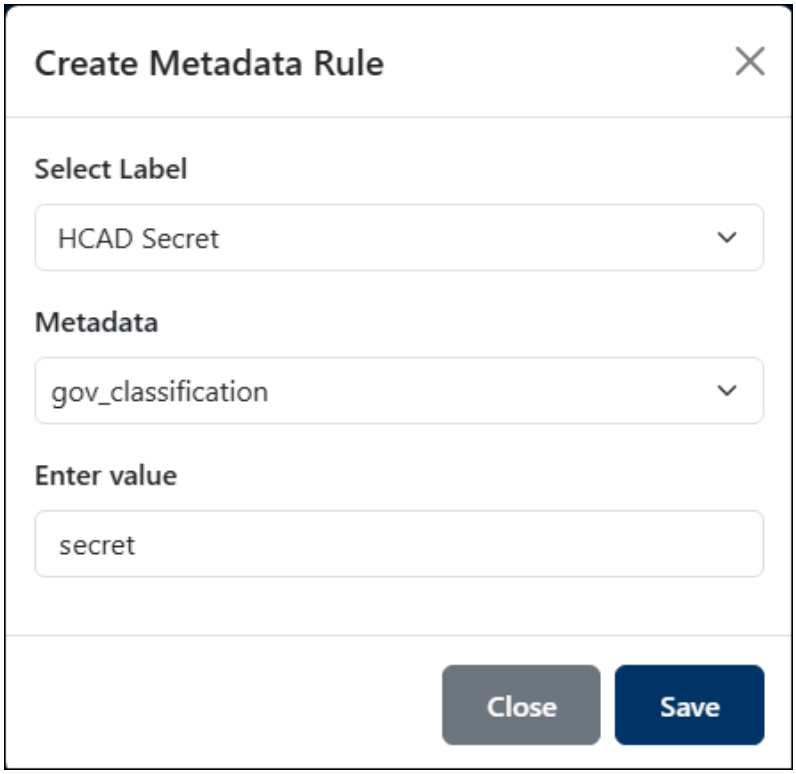
Configure the corresponding entry on the **Retain Label** page as follows:

- **Label Name:** `HCAD Secret`
- **Metadata:** `gov_classification`
- **Value:** `secret`

The **Label Name**, **Metadata**, and **Value** configured on the **Retain Label** page must match the corresponding classification rule.

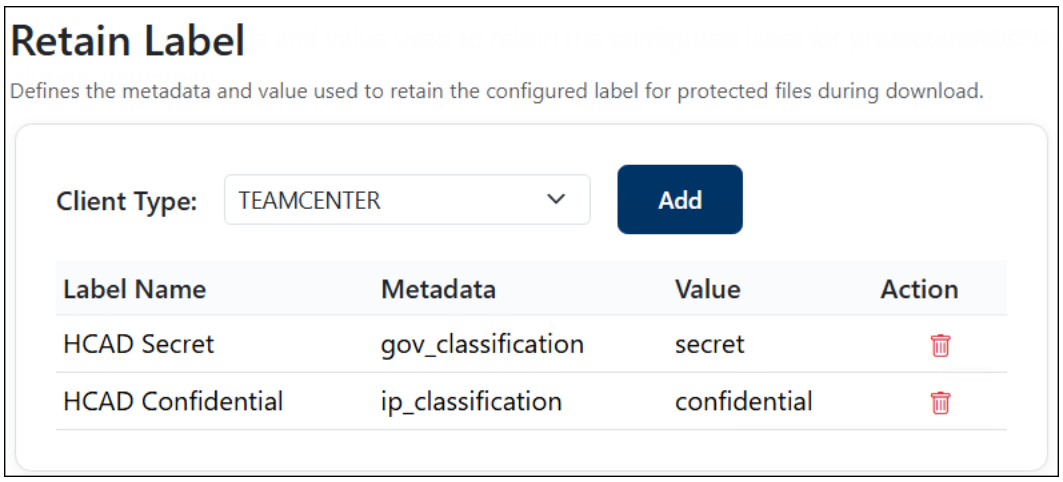
Follow these steps to retain the label:

1. In the left navigation bar, select **Rules**, and then select **Retain Label**.
2. The **Retain Label** page appears.
3. By default, **Client Type** shows Teamcenter.
4. Click **Add**.
5. The **Create Metadata Rule** page appears.



Creating metadata rules

6. In **Select Label**, select an equivalent MPIP label from the list. For example: `HCAD Secret`
7. In **Metadata**, select the required metadata from the list. For example: `gov_classification`
8. In **Enter Value**, enter the value associated with the selected metadata. For example: secret
9. Click **Save**.



Retain label

Result:

- The metadata and value associated with the selected label are saved and listed on the **Retain Label** page.
- To delete an entry, click the **Delete** icon in the **Action** column.

5.3.2.4. Pre-Expression

A Pre-Expression is a group of related values associated with existing metadata that helps evaluate classification rules. You can create Pre-Expressions based on your business requirements and use them across all client types. The grouped values, such as file extensions, servers, users, or files, are based on the available metadata.

For example:

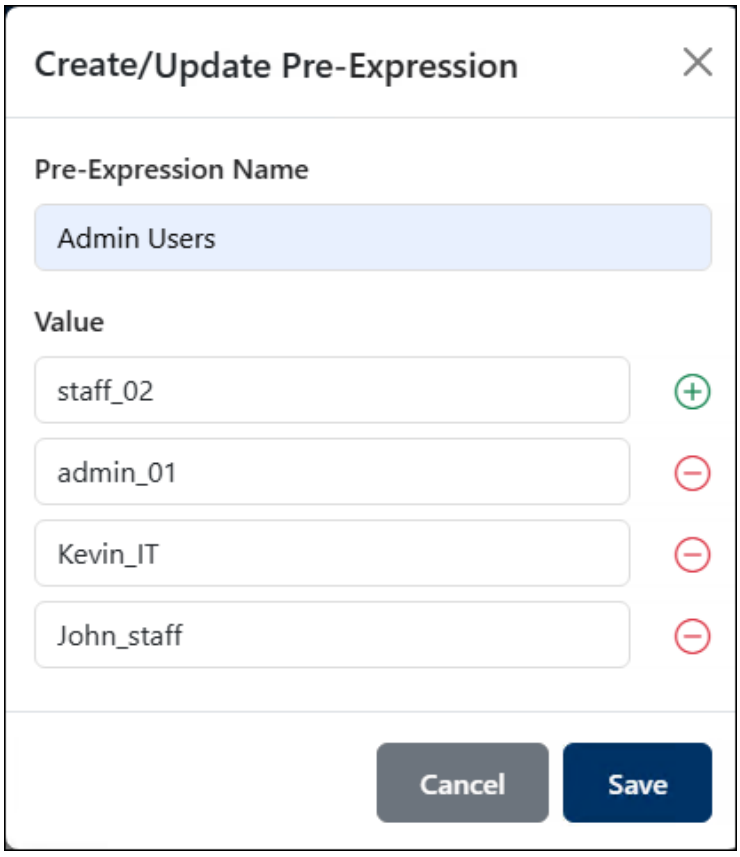
- To group multiple file types, create a Pre-Expression containing the required file types.
- To group multiple users, create a Pre-Expression containing the required users.

You can then select the Pre-Expression when creating a classification rule instead of specifying each value individually.

Follow these steps to add a pre-expression:

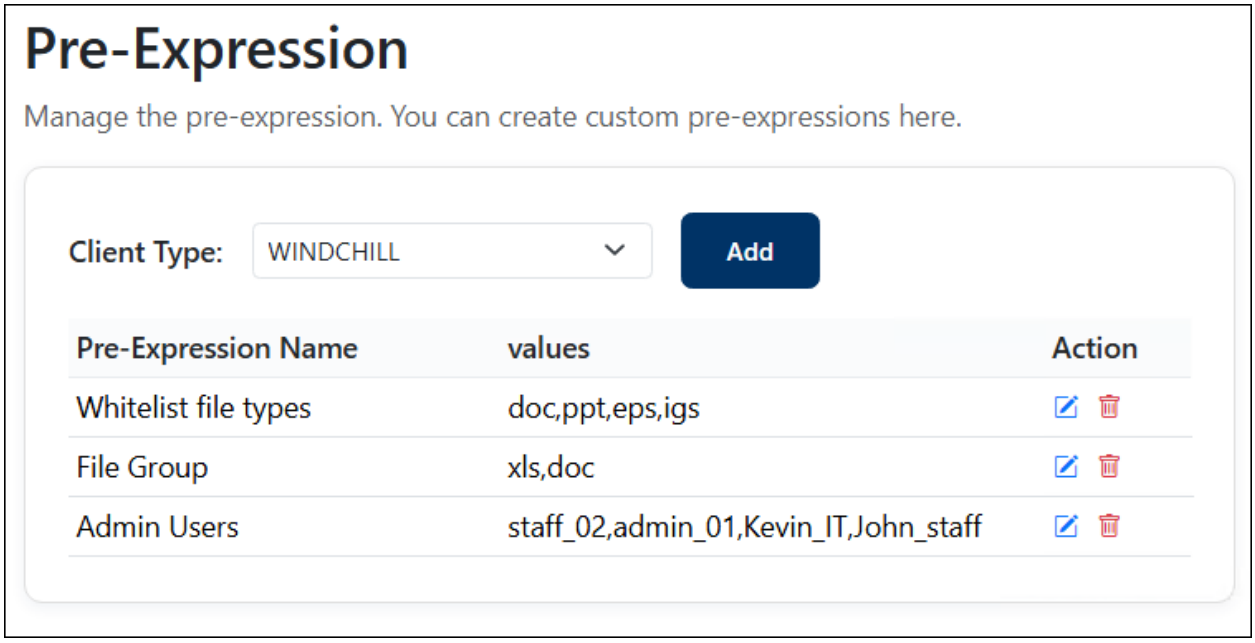
1. In the left navigation bar, select **Rules**, and then select **Pre-Expression**.
2. The **Pre-Expression** page appears.
3. From the **Client Type** list, select the client type: **Windchill**, **Teamcenter**, **Autodesk_Vault**, or **SOLIDWORKS_PDM**.
   a. If the license file contains only one client type, only that client is displayed.
   b. If two or more client types are licensed, all licensed clients are displayed in the list.
4. Click **Add**.

5. The **Create/Update Pre-Expression** dialog appears.



Adding a new pre-expression

6. In **Pre-Expression Name**, enter a name.
7. In **Value**, enter a value and click the **Edit** icon.
8. Repeat the same procedure to add one or more values to the pre-expression group.
9. Click **Save**.



Pre-expression list

Result:

- A confirmation message appears when the values are saved.
- The Pre-Expression groups and their values are available on the **Classification Rules** page.
- To update a Pre-Expression, click the **Edit** icon next to it in the **Action** column, and make the required changes.
- To delete a Pre-Expression, click the **Delete** icon next to it in the **Action** column. Note: You cannot delete a **Pre-Expression** that is associated with one or more rules. To delete the Pre-Expression, first delete all associated rules, and then delete the Pre-Expression.

5.3.2.5. Points to Remember

- **Classification Rules** define how HaloENGINE GenNXT processes files based on configured metadata, conditions, values, and actions.
- All file upload and download events are monitored by default.
- The available classification actions are **Block** and **Label**. When **Label** is selected, you must also select an MPIP label.
- The **Exclude** option prevents **Block** and **Label** actions from being applied to files based on the configured rule.
- **Pre-Expression** allows you to group related metadata values and reuse the group when configuring classification rules.
- When multiple classification rules are configured, HaloENGINE GenNXT evaluates them from top to bottom. Use the **Move Up** and **Move Down** arrows to change the rule priority.
- If no classification rule matches, HaloENGINE GenNXT applies the configured **Default** property, if available.
- For the **Label** action, a classification rule is not required when the **Default** property is selected.
- For the **Label** action with a non-default property selected, classification rules are displayed.
- For the **Block** action with the default property selected, classification rules are displayed.
- A client type can have multiple profiles, and each profile can contain multiple classification schemas.
- A profile can contain multiple properties, and you can configure multiple classification rules for each property.
- A **Default** property used in a classification rule cannot be deleted until all rules associated with that **Default** property are deleted.

- At least one **Default** classification schema must exist. Set another schema as **Default** before deleting the current **Default** schema.
- A **Pre-Expression** used in a classification rule cannot be deleted until all rules associated with that **Pre-Expression** are deleted.
- Use rule conditions carefully when configuring exclusions for users, groups, files, or other metadata values. You can configure an exclusion by using a condition such as **not equal to (**!=**)**.
- Duplicate metadata is not allowed within a single classification rule. For example, if `file_type` is already added to a rule, you cannot add `file_type` again. The Admin Portal does not allow duplicate metadata within the same rule.
- The **Retain Label** feature is available only for **Teamcenter PLM**. It uses the configured metadata and value to retain the applicable label during subsequent file downloads.
- The **Select Label** list may appear empty when the **HaloENGINE GenNXT Tomcat Service** is not responding, or its certificate has expired.
- Any changes to labels in the **Microsoft Entra admin center** require you to restart the **HaloENGINE GenNXT Tomcat Service**.
- The **Notifications** icon displays a message when the license is approaching expiration. Renew the license before it expires to avoid service interruption.
- An inactive **Admin Portal** session is automatically locked after an extended period. Click **Login Again** to authenticate and continue using the Admin Portal.

5.3.3. Log Management

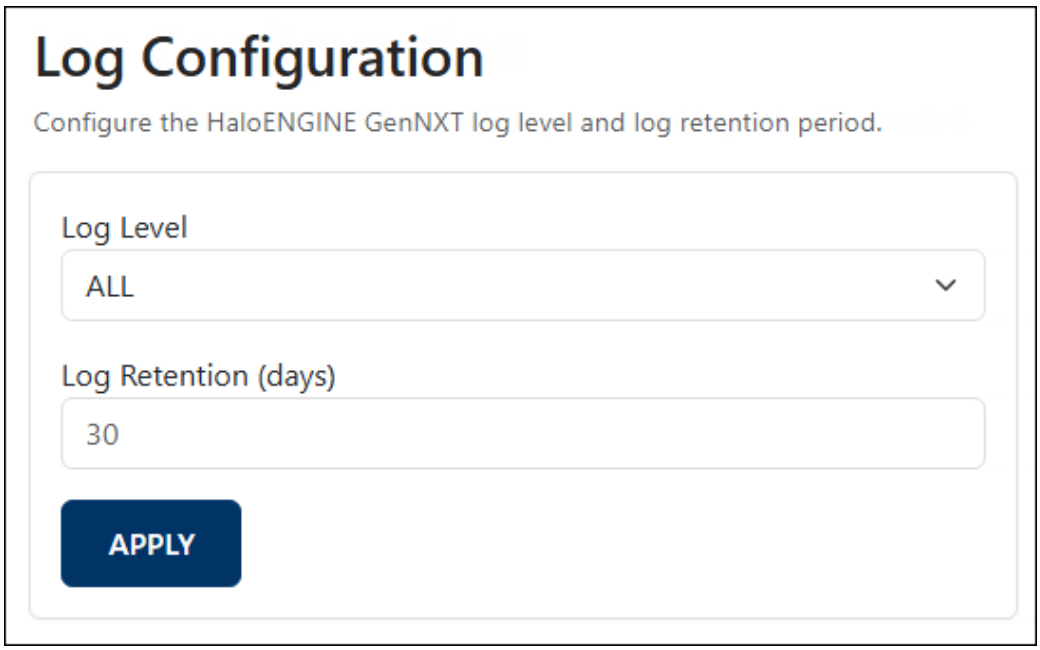
This section describes how to configure, and view logged administrative activities and monitor logs.

5.3.3.1. Log Configuration

The **Log Configuration** page displays options for configuring the general settings of HaloENGINE GenNXT.

To configure the general settings, follow these steps:

1. In the left navigation bar, click **Logs**, and then click **Log Configuration**.
2. The **Log Configuration** page appears.



Log Configuration

3. In the **Log Level** list, select the required log level:
   - **ERROR** – Logs only error messages.
   - **WARN** – Logs warning and error messages.
   - **INFO** – Logs informational, warning, and error messages.
   - **DEBUG** – Logs detailed debugging information along with all other log messages.
   - **ALL** – Logs all messages. This is the default value.
4. In **Log Retention (days)**, specify the number of days to retain log files. Log files older than the specified retention period are automatically deleted. The default value is `30`.
   For example, if the value is set to 10, log files older than 10 days are deleted. The valid range is `0` to `90` days.
5. Click **Apply**.

Result:

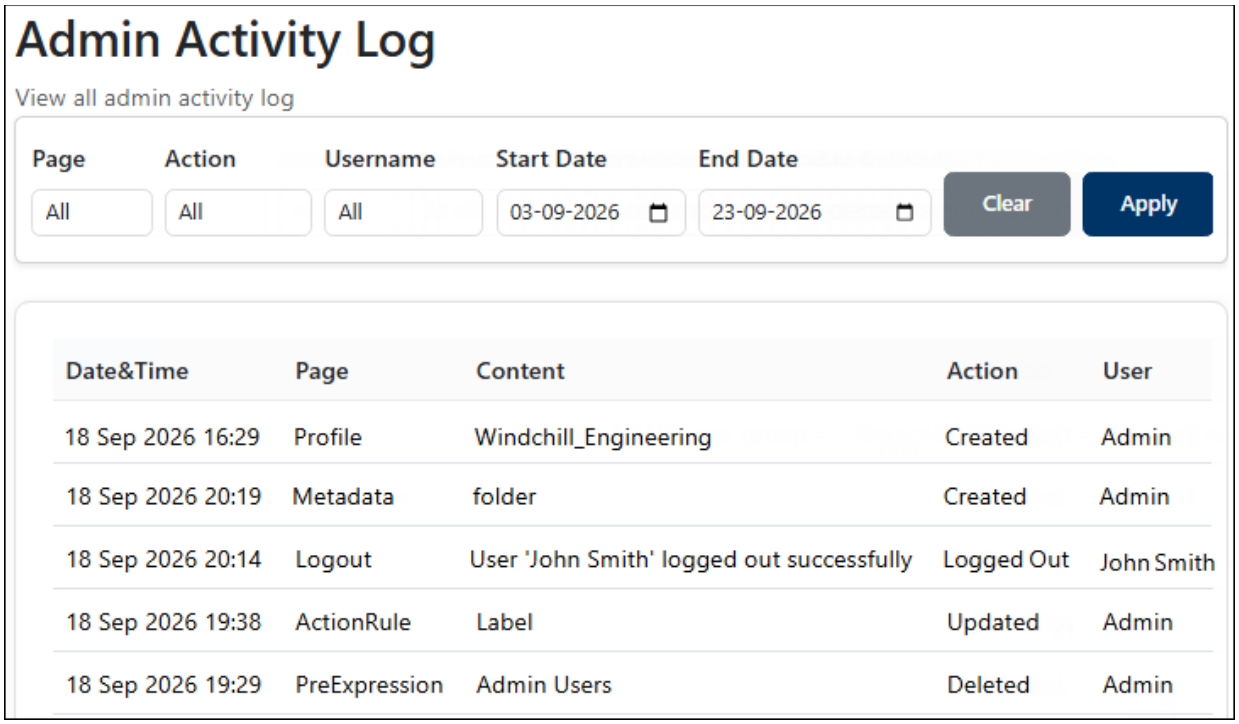
- On successful configuration, a confirmation message appears.
- The configuration file is created with the updated details.

5.3.3.2. Admin Activity Log

The Admin Activities Log page displays all logged administrative activities. It shows the page where the activity occurred, the action performed, the user who performed the action, and the start and end dates, which can be used to filter and refine the displayed activities.

Follow these steps to view the admin activities:

1. In the left navigation bar, select **Logs**, and then select **Admin Activities**.
2. The **Admin Activity Log** page appears.



Admin activities log

3. The page displays real-time data.
   a. **Date & Time** – The date and time when the action was performed.
   b. **Page** – The page on which the action was performed. For example, Profile.
   c. **Content** – Displays the exact content that was modified or acted upon. For example, `Windchill_Engineering` profile was created on the Rules Management page.
   d. **Action** – The action that was performed. For example, Created indicates that a metadata named `folder` was created.
   e. **User** – The person who performed the action. For example, Admin and John Smith.
4. To filter the results, specify the **Page**, **Action**, **Username**, **Start Date**, and **End Date**, and then click **Apply**.

Result

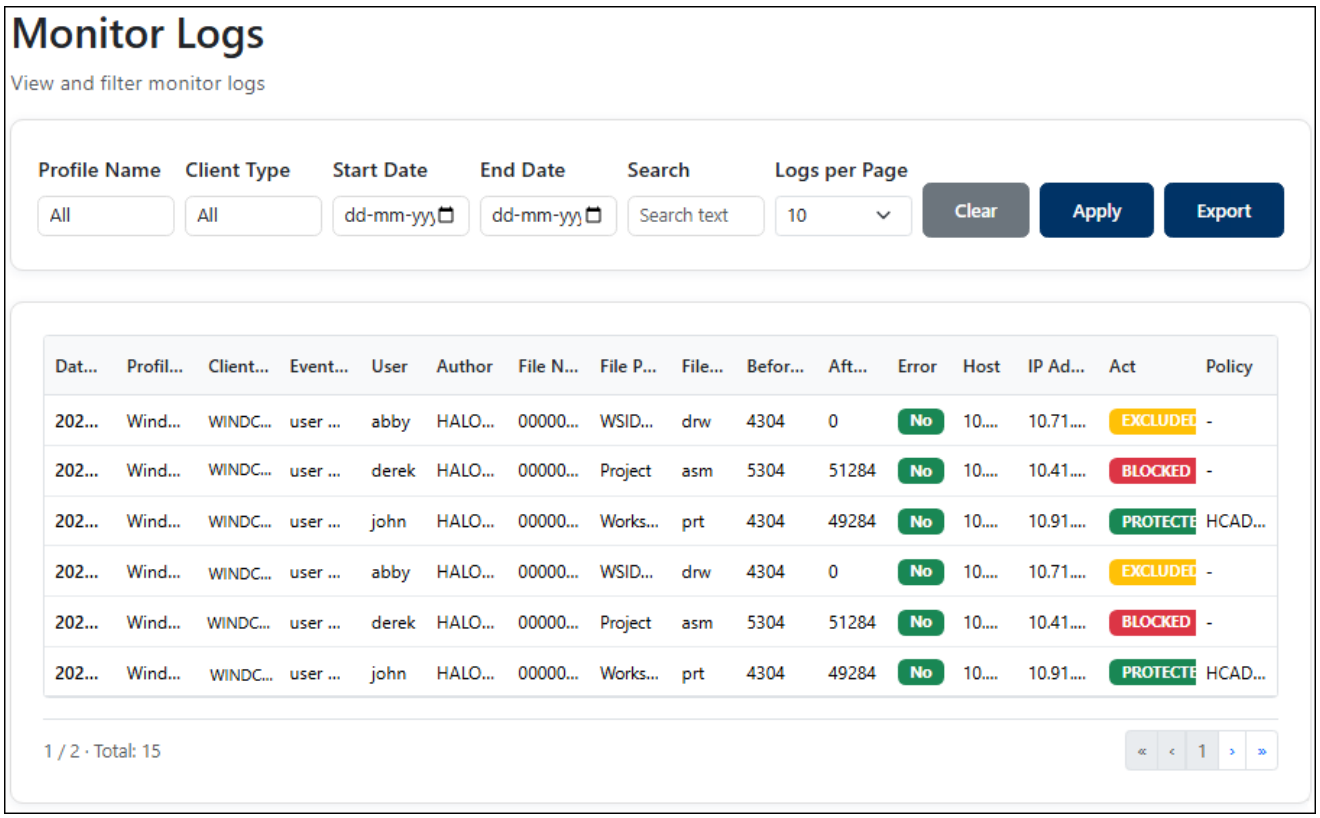
- The filtered results are displayed based on the selected criteria.
- To clear the filters, click **Clear**.

5.3.3.3. Monitor Logs

Monitor is a key feature of HaloENGINE GenNXT that tracks user upload and download activities when integrated with PLM clients. It records the date and time of each activity and displays the activity log in JSON format. During the first login or after a fresh HaloENGINE GenNXT installation, the **Monitor Logs** page is empty because no operational data is available. Once HaloENGINE GenNXT begins processing events, the page displays the corresponding log information.

Follow these steps to view the monitor logs:

1. In the left navigation bar, select **Logs**, and then select **Monitor**.
2. The **Monitor Logs** page appears.



Monitor logs page

3. The page displays the following details:
   a. Date/Time
   b. Profile Name
   c. Client Type
   d. Event Type
   e. User
   f. Author

g. File Name
h. File Path
i. File Type
j. Before Size
k. After Size
l. Error
m. Host
n. IP Address
o. Act - Excluded, Blocked, and Protected

   Note: **Excluded** appears when a rule is not applied, does not match, an upload event occurs, or no decryption takes place.

p. Policy

4. To filter the results, specify values for fields such as **Profile Name**, **Client Type**, **Start Date**, and **End Date**. Additionally, use the search bar to filter the displayed records.
5. To control the number of displayed records, enter a value from `10` to `100` in the **Logs per Page** field
6. Click **Apply**.

Result

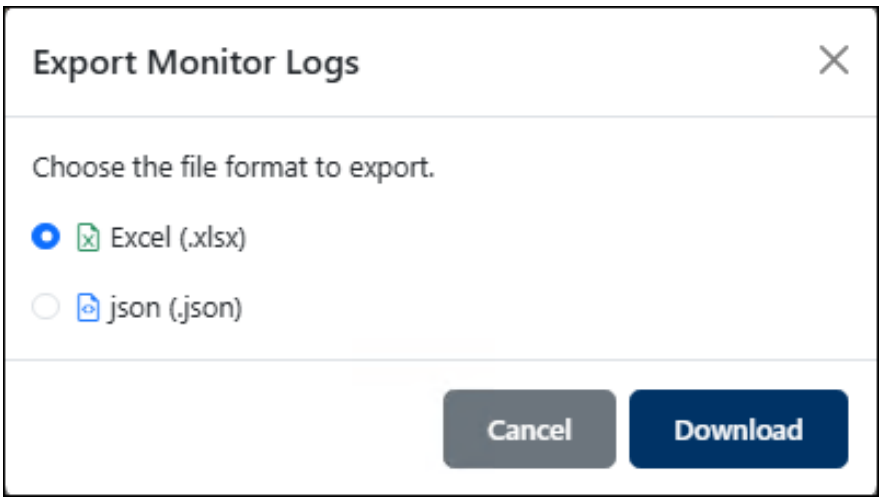
- The filtered results are displayed based on the selected criteria.
- To clear the filters, click **Clear**.

Exporting Monitor Logs

Use the **Export** button to download the Monitor logs.

Follow these steps to export the Monitor logs:

1. Click **Export**.
2. The **Export Monitor Logs** dialog appears.



Export Monitor Logs

3. Select the required file format:
   a. **Excel (.xlsx)**: Exports the log entries displayed on the **Monitor Logs** page.
   b. **JSON (.json)**: Exports detailed log entries.
4. Click **Download**.

Result:

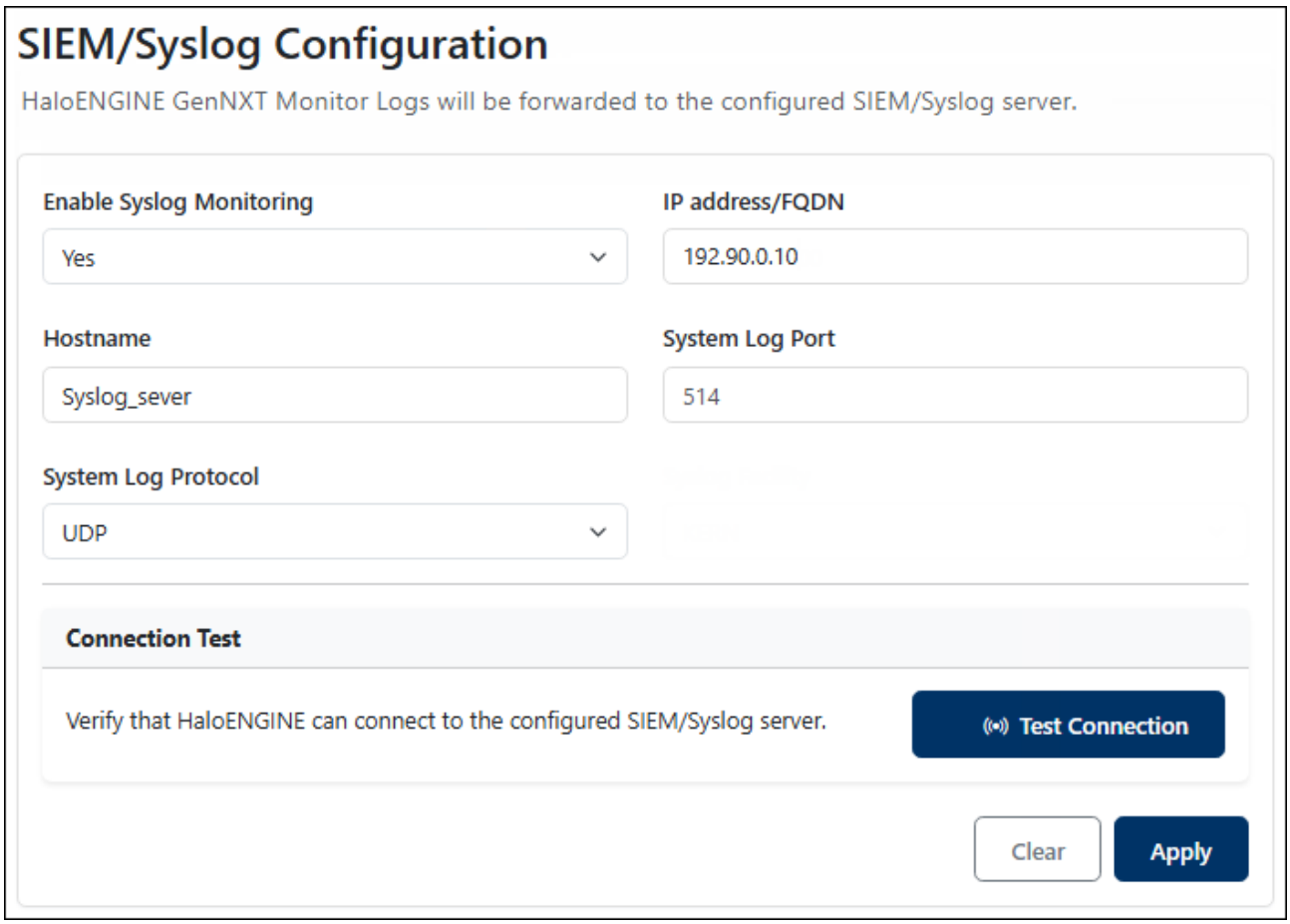
- The Monitor logs are downloaded to your default download location in the selected file format.
- For example, Excel files are downloaded as `monitor_logs_<yyyy>-<MM>-<dd>.xlsx`, and JSON files are downloaded as `monitor_logs_<yyyy>-<MM>-<dd>.json`.

5.3.3.4. SIEM/Syslog Configuration

The SIEM/Syslog Configuration page enables you to configure a SIEM/Syslog server to receive HaloENGINE GenNXT Monitor logs.

To configure SIEM/Syslog:

1. In the left navigation bar, click **Logs**, and then click **SIEM/Syslog**.
2. The **SIEM/Syslog Configuration** page appears.



SIEM/Syslog Configuration

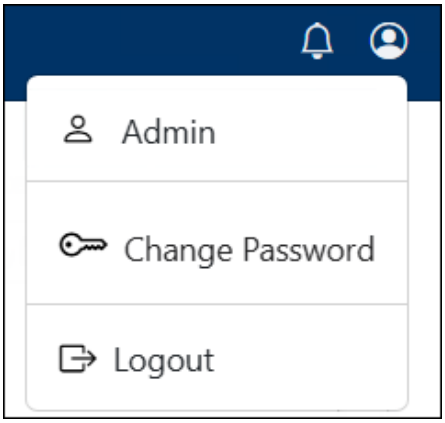
3. Configure the following fields.
    a. **Enable Syslog Monitoring** – Select **Yes** to enable forwarding of HaloENGINE GenNXT Monitor logs to the configured SIEM/Syslog server.
    b. **IP Address/FQDN** – Enter the IP address or fully qualified domain name (FQDN) of the SIEM/Syslog server. For example, `192.90.0.10`.
    c. **Hostname** – Enter the hostname of the Syslog server. For example, `Syslog_server`.
    d. **System Log Port** – Enter the port number used by the SIEM/Syslog server. For example, `514`.
    e. **System Log Protocol** – Select the protocol (**UDP** or **TCP**) used to send the logs.
4. To verify the connection to the configured SIEM/Syslog server, click **Test Connection**. If the connection is successful, a confirmation message appears.
5. Click **Apply**.

Result:

- The SIEM/Syslog configuration is saved, and HaloENGINE GenNXT Monitor logs are forwarded to the configured SIEM/Syslog server.
- To reset the SIEM/Syslog configuration fields, click **Clear**.

5.3.4. Security Settings

The user icon in the top-right corner provides quick access to user account options, such as viewing profile information, changing the account password, and logging out of the application. Click the user icon to open the **User** menu.



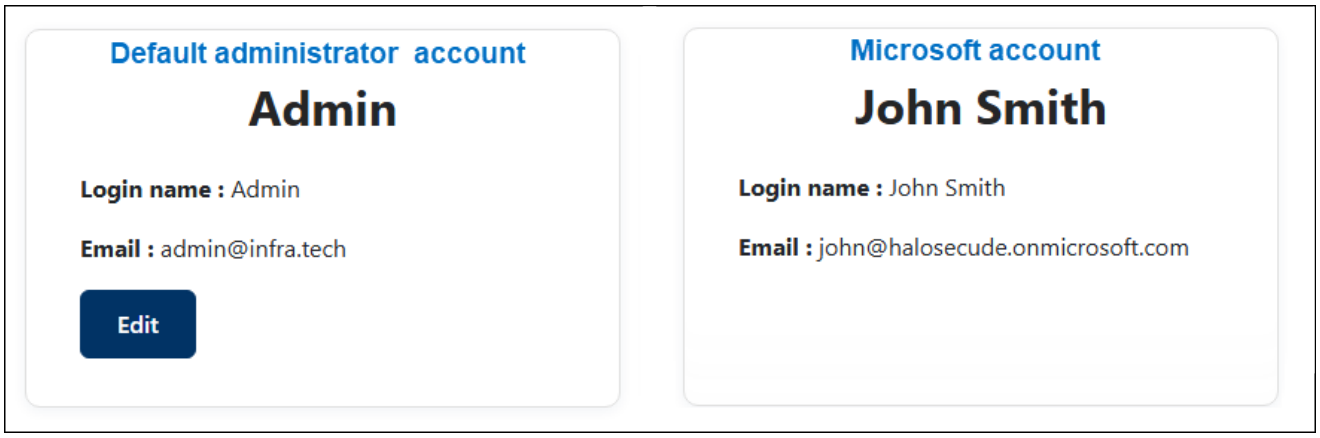
User menu

5.3.4.1. User (Profile)

When you hover over this menu, it displays the name of the currently logged-in user. This menu lets you view and update your account information, such as your login name and email address.

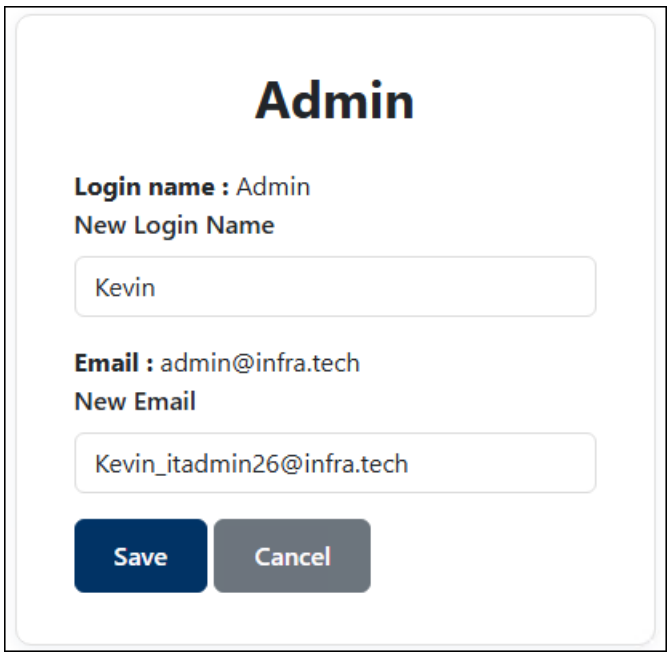
Note: Only the Super Administrator account details can be edited. User accounts authenticated through Microsoft Entra ID cannot be edited.

1. Select the **User** icon in the upper-right corner.
2. Click **User**.
3. The page displays the current profile details.



Profile - Admin User and Microsoft User accounts

4. Click **Edit**.



Admin User Profile

5. In **New Login Name**, enter the new login name. For example: Kevin.
6. In **New Email**, enter the new email address. For example: `Kevin_itadmin26@infra.tech`.
7. Click **Save** to apply the changes, or click **Cancel** to discard them.

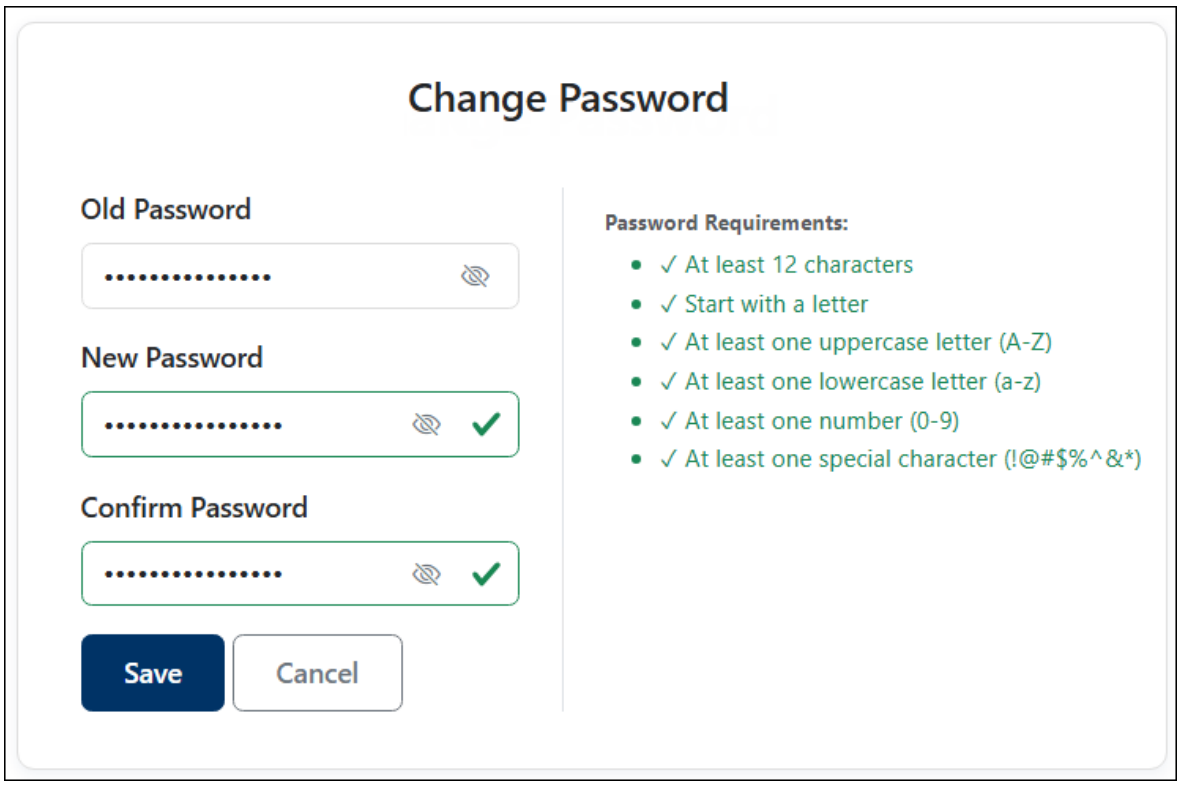
Result

- An error message appears if the new username is the same as the existing username.
- A confirmation message appears after the details are successfully updated.
- The updated details are displayed on the **User** page.

5.3.4.2. Change Your Password

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

1. Select the **User** icon in the upper-right corner.
2. Click **Change Password**.
3. The **Change Password** page appears.



Changing password

4. In **Old Password**, enter your current password.
5. In **New Password**, enter a new password that meets all of the following requirements:
   a. At least **12 characters**
   b. Starts with a **letter**
   c. Includes at least **one uppercase letter** (`A–Z`)
   d. Includes at least **one lowercase letter** (`a–z`)
   e. Includes at least **one number** (`0–9`)
   f. Includes at least **one symbol** (`! @ # $ % ^ & *`)
   g. New password cannot be the same as the **current** password

   For example: `Admin@User0123`

   Note

   As you type the password, each requirement is validated in real time. A green check mark indicates that a requirement is met. A cross indicates that a requirement is not met.
6. In **Confirm Password**, re-enter the password.
7. To display the credentials, click the **Show/Hide** (eye) icon.
8. Select **Save**.

Result

- The Admin Portal updates your password, displays a success message, and redirects you to the **Login** page.
- Log in using the new password.

5.3.4.3. Log Out

Logging out ends your current session in the portal. When you select **Log Out**, the portal closes your active session and removes your access until you sign in again.

1. Select the **User** icon in the upper-right corner.
2. Click **Log Out**.
3. When the portal asks you to confirm, click **OK**.

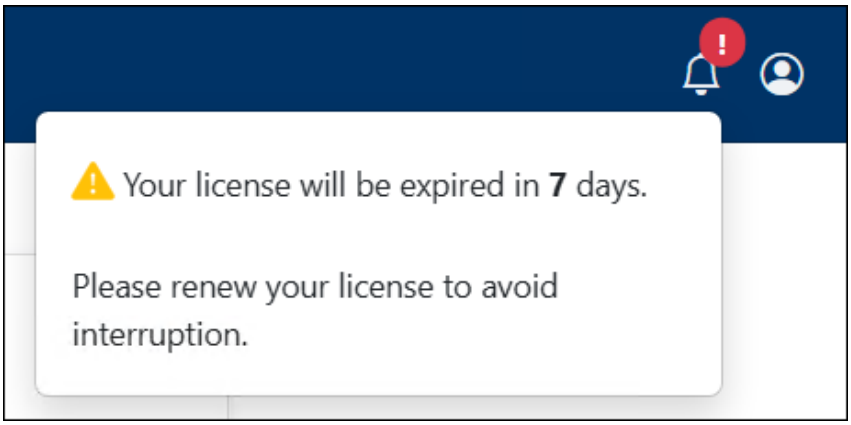
Result

- A success message appears. To return to the portal, click **Back to login**.
- The **Login** page opens.

5.3.4.4. Notification

License Expiration

HaloENGINE GenNXT displays a notification when the license is nearing expiration. The notification appears on the **Notifications** icon and shows the remaining validity period.

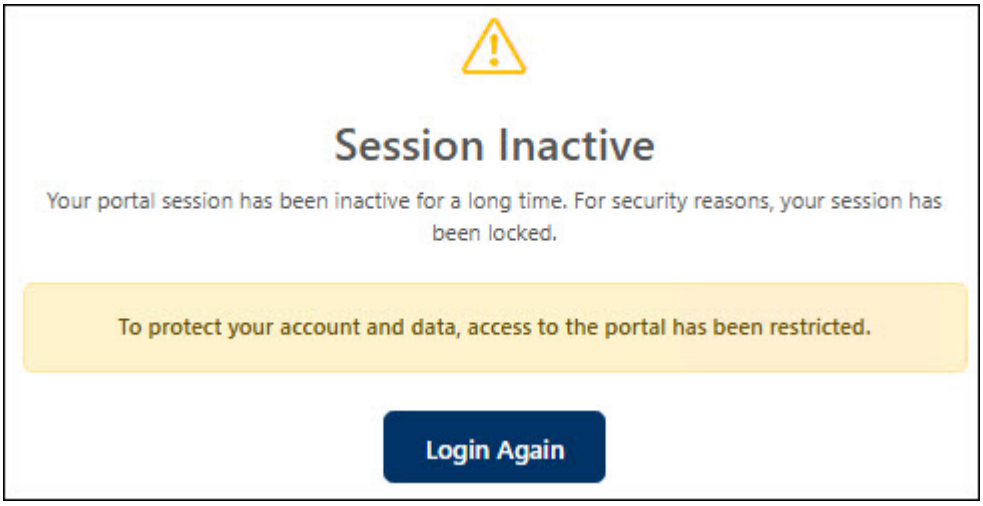


License Notification

If the license expires before you upload a new license, you are directed to the **License** page when you log in. Upload a valid license to continue using HaloENGINE GenNXT.

5.3.4.5. Session Timeout

If the Admin Portal session remains inactive for an extended period, the session is automatically locked to protect your account and data. Click **Login Again** to authenticate and continue using the Admin Portal.



Session inactive dialog

5.3.5. Dashboard

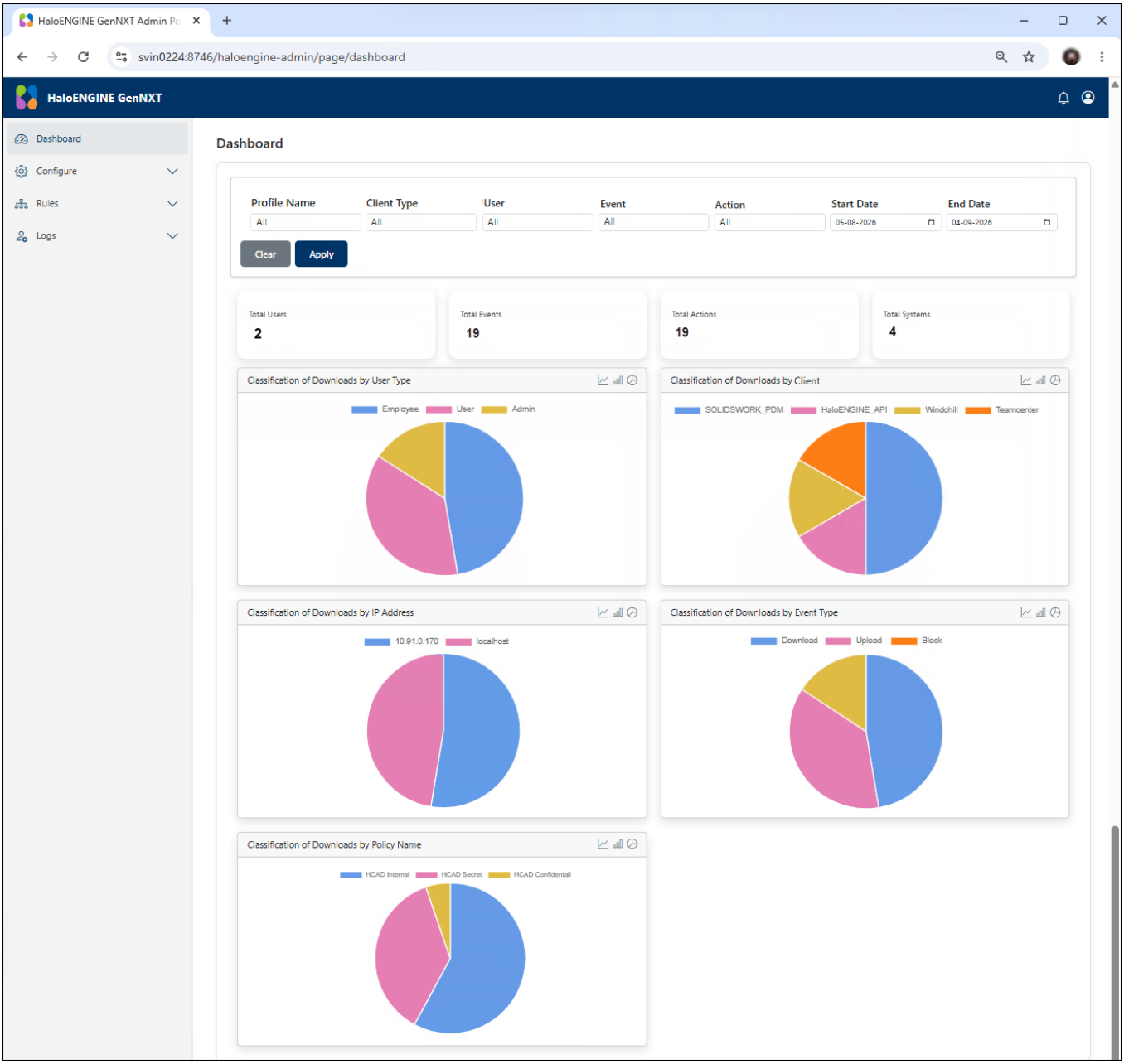
After the HaloENGINE GenNXT setup is complete and the service is operational, the HaloENGINE GenNXT Dashboard provides a centralized information management interface for monitoring and visualizing key performance indicators and metrics. It offers an overview of company data upload and download events and helps users track client activities effectively.

You can filter the Dashboard data by **Profile Name**, **Client Type**, **User**, **Event**, **Action**, **Start Date**, and **End Date**. Click **Apply** to display data based on the selected filters, or click **Clear** to reset the filters.

The Dashboard displays the following summary metrics:

- **Total Users** – Displays the total number of users associated with the recorded activities.
- **Total Events** – Displays the total number of recorded events.
- **Total Actions** – Displays the total number of actions performed.
- **Total Systems** – Displays the total number of systems associated with the recorded activities.

The Dashboard also provides graphical views of download activities, including classification by **User Type**, **Client**, **IP Address**, **Event Type**, and **Policy Name**. These charts provide a visual overview of file processing and classification activities.

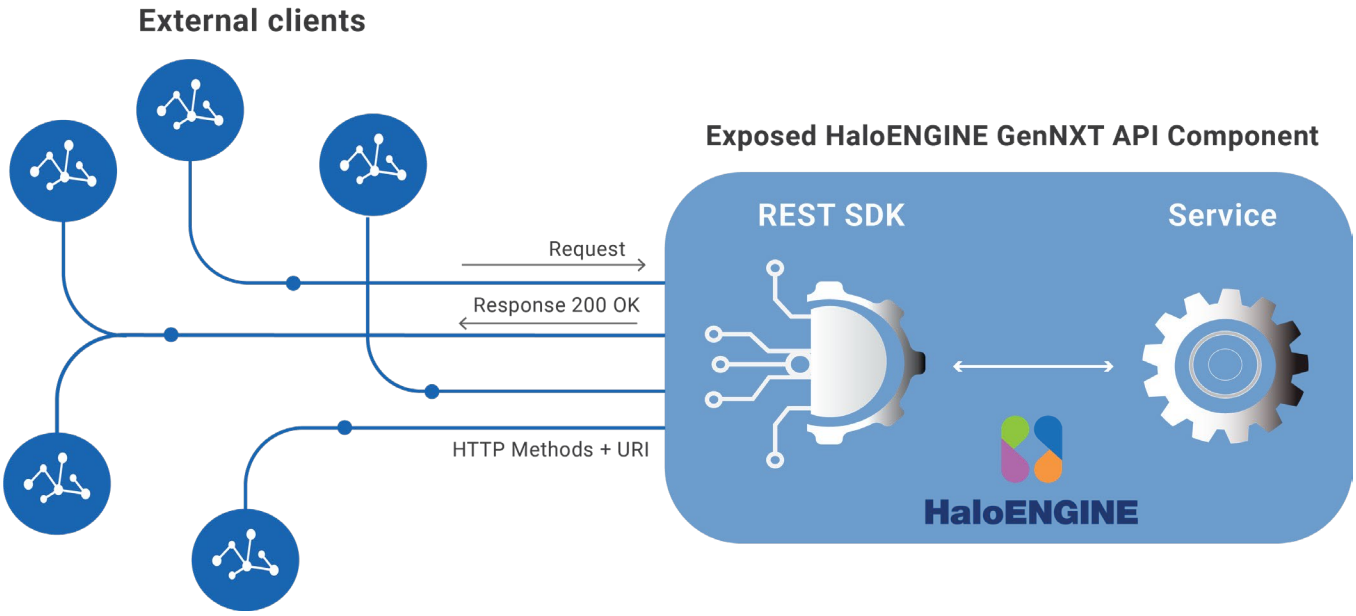


Dashboard with activities

6. HaloENGINE GenNXT REST API

The HaloENGINE GenNXT REST API enables client applications to access HaloENGINE GenNXT services programmatically. You can use these APIs to perform operations such as metadata retrieval, action execution, log monitoring, and version checks.

- View supported APIs and HTTP methods
- Review request and response schemas
- Test endpoints directly from the browser



HaloENGINE GenNXT API

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.

This chapter demonstrates how to successfully call the HaloENGINE GenNXT 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.

Quick Start

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

1. Step 1: Install HaloENGINE GenNXT as described in the following chapter, “Installing the HaloENGINE GenNXT”.
2. Step 2: Import the license with HaloENGINE_API client enabled.
3. Step 3: Configure HaloENGINE GenNXT for the HaloENGINE_API client type. For more information, refer to the chapter “Configuring HaloENGINE GenNXT”.
4. Step 4: Ensure that an authentication approach is selected for HaloENGINE GenNXT and HaloENGINE_API: **Self-Signed Certificate** or **CA-Signed Certificate**.
   a. For a **Self-Signed Certificate**, export the public key of the HaloENGINE GenNXT server's self-signed certificate and install it in **Trusted Root Certification Authorities** on the client system.
   b. For a **CA-signed certificate**, install the **Root CA certificate** in **Trusted Root Certification Authorities** on the client system. If an intermediate CA is used, ensure that the **intermediate CA certificate** is also available on the client system to validate the certificate chain.

6.1. API Reference

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

6.1.1. 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

6.1.2. Version

Description: Retrieves the current HaloENGINE GenNXT package version.

Request method: GET

6.1.2.1. Request Example

6.1.2.1.1. Request URL

```
GET https://10.91.0.170:8746/haloengine-server/halosdk/Version
```

6.1.2.1.2. Response

A successful request returns the following information:

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

```
1.0.7.0
```

6.1.3. Get Metadata List

Description: Retrieves the metadata list configured on the HaloENGINE GenNXT Admin Portal in your environment.

Request method: POST

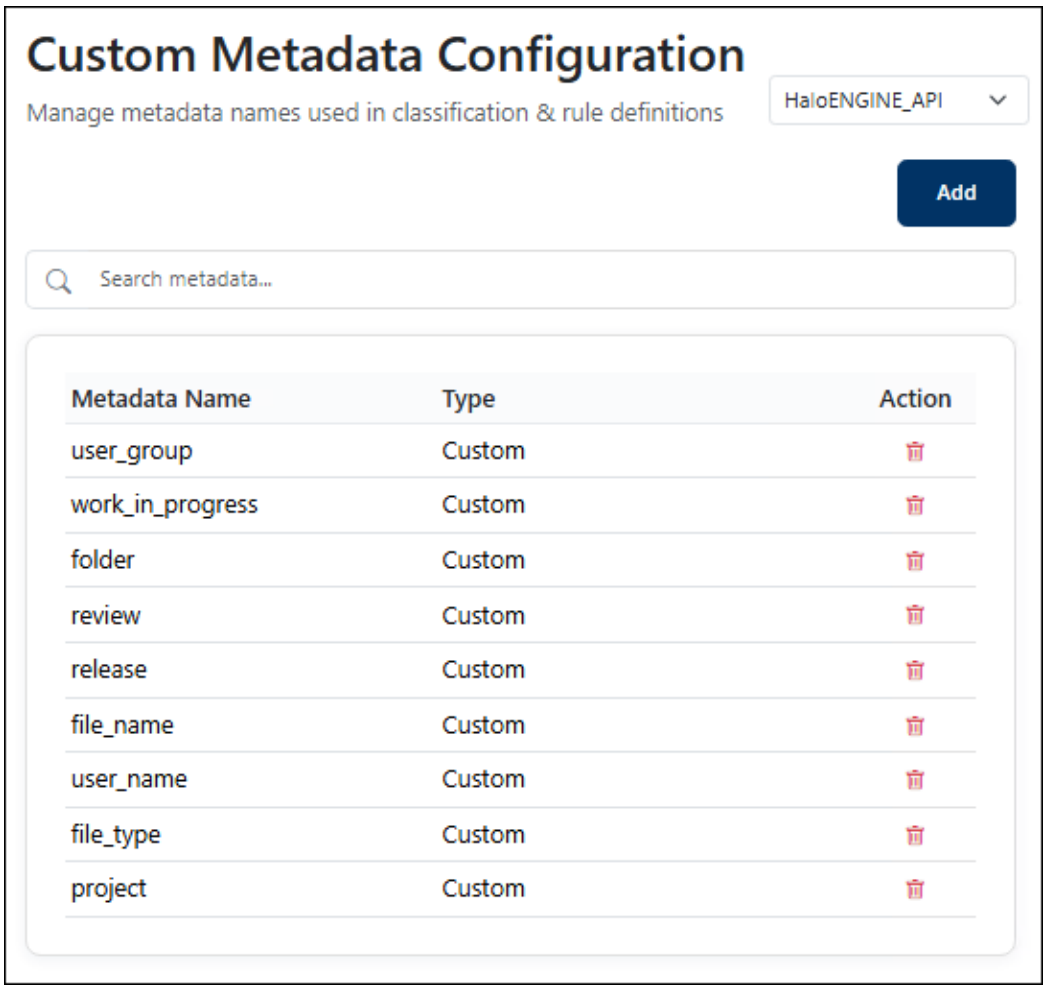
6.1.3.1. Request Example

6.1.3.1.1. Request URL

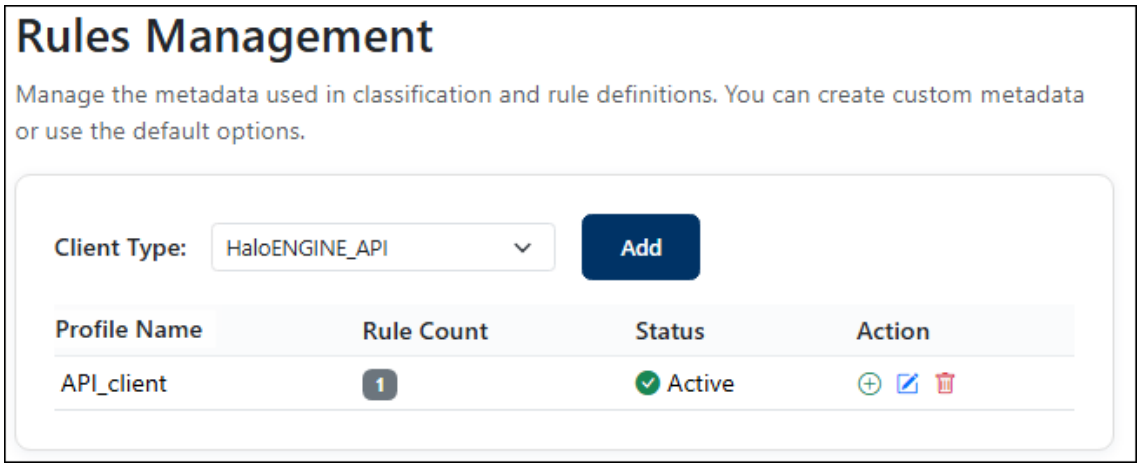
```
POST https://10.91.0.170:8746/haloengine-server/halosdk/getmetadatalist
```

Prerequisites:

- The **HaloENGINE_API** client type does not have any built-in metadata. Create the required metadata using **Metadata Configuration**. For example, `user_group`, `work_in_progress`, `folder`, `review`, `release`, `file_name`, `user_name`, `file_type`, and `project` are sample metadata, as shown in the following image.
- Ensure that classification rules are created for the **HaloENGINE_API** client type.



Custom metadata added for HaloENGINE_API



Rules for API client

6.1.3.1.2. Request

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

- **profileName** – Specifies the profile name used by HaloENGINE GenNXT.

- **clientType** – Specifies the type of client system.

Example

```
{
    "clientType": "HaloENGINE_API"
}
```

6.1.3.1.3. Response

A successful request returns the following information:

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

6.1.4. Get Action

Description: Determines the action to apply to the file.

Request method: POST

6.1.4.1. Request Example

6.1.4.1.1. Request URL

```
POST https://10.91.0.170:8746/haloengine-server/halosdk/getaction
```

6.1.4.1.2. Request

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

Prerequisite: Ensure that classification rules are created for the **HaloENGINE_API** client type.

Note: Owner Configuration provides three options: Service (default), Static Email, and User. For Static Email, enter the user's email address in the Admin Portal. For information about configuring owner settings, see Configure Owner Rights.

- **profileName** – Specifies the profile name used by HaloENGINE GenNXT.
- **clientType** – Specifies the type of client system.
- Example values `file_type`, `user_group`, and `project`.

Example

```
{
  "customerIdentification": {
    "profileName": "API_client",
```

```
    "clientType": "HaloENGINE_API"
  },
  "metadata": {
    "simpleValue": {
      "file_type": [
        "*"
      ],
      "user_group": [
        "finance"
      ],
      "project": [
        "project_steer"
      ]
    }
  }
}
```

6.1.4.1.3. Response

A successful request returns the following information:

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

```
{
    "action": {
        "value": [
            "AUDIT",
            "LABEL"
        ]
    },
    "authorMode": {
        "userEmailNeeded": false,
        "staticEmail": null
    },
    "template": {
        "id": "7afc9a97-cefc-4ae1-9a45-ea9acfed9f8c",
        "name": "HCAD Confidential",
        "active": true,
        "isActive": true
    },
    "returnMessage": {
        "success": true,
        "message": "Action rules found for this profile"
    }
```

```
}
```

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

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

6.1.5. Encrypt File

Description: Executes the encrypt action.

Request method: POST

6.1.5.1. Request Example

6.1.5.1.1. Request URL

```
POST https://10.91.0.170:8746/haloengine-server/halosdk/encryptfile
```

6.1.5.1.2. Request

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

Key: `file` (File as Type).

Description: Browse and select the file to be labeled. For example: `BOM.txt`

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 label 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"}
```

6.1.5.1.3. 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."
}
```

6.1.6. Decrypt File

Description: Decrypts an encrypted file.

Request method: POST

6.1.6.1. Request Example

6.1.6.1.1. Request URL

```
POST https://10.91.0.170:8746/haloengine-server/halosdk/decryptfile
```

6.1.6.1.2. Request

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

Key: `file` (File as Type).

Description: Browse and select the file to be decrypted.

Example

```
BOM.rtf.pfile
```

6.1.6.1.3. 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"

}
```

6.1.7. Send PLM Monitor Log Data

Description: Sends audit log to the Admin Portal.

Request method: POST

6.1.7.1. Request Example

6.1.7.1.1. Request URL

```
POST https://10.91.0.170:8746/haloengine-server/halosdk/sendmonitorlog
```

6.1.7.1.2. Request

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

- **profileName** – Specifies the profile name used by HaloENGINE GenNXT.
- **clientType** – Specifies the type of 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.
- **resultedDecision** – Final decision returned by HaloENGINE GenNXT.

Example


```
{
    "identification": {
    "profileName": "API_client",
    "clientType": "HaloENGINE_API"
     },
    "logInfo":{
        "datetime":"30/01/2026",
        "timeZone":123123,
        "logID":"FinTEAM"
    },
    "userInfo":{
        "userName":"John",
        "userType":"Employee",
        "userEmail":"john.smith@tservice.com"
    },
    "resultedDecision":{
        "fileBlocked":false,
        "fileLabeled":true,
        "fileProtected":true,
        "unprotected":false,
        "unlabeled":false,
        "fileBlockedByRule":"",
        "policyName":"HCAD Secret",
        "policyId":"99f1473d-74f4-47ca-9843-e735f94fa797",
        "classification":{
            "byUser":"user",
            "bySystem":"server00045"
        },
        "abortedBySystem":false,
        "abortedByUser":false,
        "error":false,
        "simMode":false,
        "extendedTags":[]
    },
    "plmContextInfo":{
        "eventType":"Test",
        "preProcessInfo":[],
```

```
        "attributes":[],
        "documentId":"PurchaseOrder.pdf",
        "documentNumber":"0nu74rf",
        "documentType":"pdf",
        "documentPart":"prt",
        "documentVersion":"1.9",
        "viewOnly":"false",
        "dmsProcess":"false",
        "browserClient":"false"
    },
    "plmDestInfo":{
        "destinationAttributes":[],
        "browser":"Chrome",
        "hostname":"localhost",
        "ipaddress":"localhost",
        "operatingSystem":"Windows"
    }
}
```


6.1.7.1.3. 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.

6.2. Error Handling

Although the API returns **200 OK**, the response may contain an application-level error when the request cannot be processed successfully.

Sample Message	Description
`Profile not found`	The specified `profileName` is incorrect or does not exist.
`"returnMessage": null`	The specified `clientType` is incorrect or does not match a supported client type.
`No action rules found for this profile`	No valid action rules are configured for the specified profile.

Error Codes

7. Troubleshooting

This section describes common problems that may occur during installation and configuration.

As the first step in troubleshooting, make sure that your HaloENGINE GenNXT version is up to date. Each release of HaloENGINE GenNXT adds new features and fixes many problems. Installing the latest version may resolve any issues without further troubleshooting.

7.1. Forgot your Admin Portal Password

Symptoms

Login fails with the error message "*Invalid credentials*".

Background

Entered the wrong password to access the HaloENGINE GenNXT Admin Portal.

Probable Cause

You may be unable to access the Admin Portal if you forget your password.

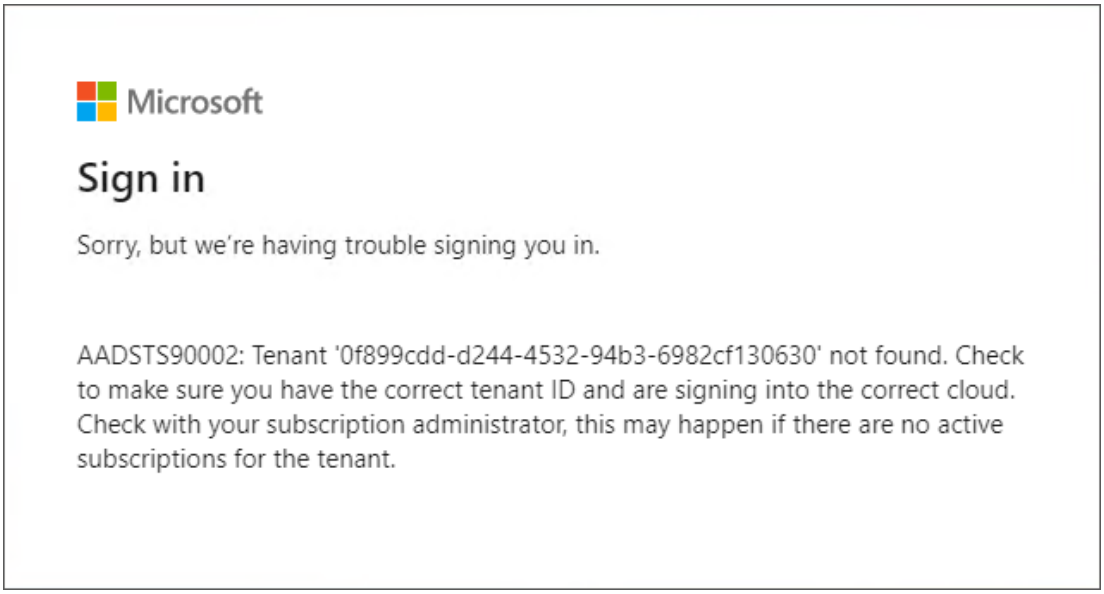
Recommended Action

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.

7.2. 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 GenNXT Admin Portal using Microsoft Sign-In.

Probable Cause

The Tenant ID/Client ID you entered on the **Microsoft Entra Tenant Configuration** page is either incomplete or incorrect.

Recommended Action

1. Check that the Tenant ID/Client ID given on the **Microsoft Entra Tenant Configuration** page is correct.
2. Log in to the Admin Portal.

7.3. Protection fails with ServiceDisabledError

Symptoms

During a protection operation, HaloCAD displays an error similar to one of the following:

HTTP operation failed Failed with: [ServiceDisabledError: 'RMS service is disabled for this tenant., ServiceDisabledError.Extent=Tenant, HttpRequest.Id]"

or

HTTP operation failed Failed with: [ServiceDisabledError: 'RMS service is disabled for this tenant., ServiceDisabledError.Extent=User, HttpRequest.Id]"

Background

This issue affects content creation (protection) only. It does not affect opening or consuming protected documents.

Some organizations deploy Microsoft Purview Information Protection in phases by using an onboarding control policy. During this phase, only designated users or groups (for example, administrators) are permitted to create protected content until the deployment is complete.

This issue can also occur in Microsoft sovereign cloud environments (for example, Microsoft 365 GCC High) if the tenant or application is not configured correctly. Sovereign cloud environments are intended for government agencies and eligible organizations that handle regulated government data. Most commercial Microsoft 365 tenants are not deployed in these environments.

Probable Cause

The error can occur if one of the following conditions is true:

1. RMS is not enabled for the Microsoft 365 tenant.
2. The onboarding control policy restricts the current user or service principal from creating protected content.

Recommended Action

1. Verify that RMS is enabled for the Microsoft 365 tenant.
2. Verify that the user or service principal has permission to create protected content under the organization's onboarding control policy.
3. If the onboarding control policy is enabled, contact your Microsoft 365 administrator to grant the required permissions or complete the onboarding process.

7.4. Microsoft Login Fails

Symptoms

When logging in to the HaloENGINE GenNXT Admin Portal using a Microsoft account, one of the following error messages is displayed:

Authentication processing fault: 401 Unauthorized or Authentication failed. Please verify that the Azure Tenant ID, Client ID, and Client Secret are correct and try again.

Background

The authentication process starts successfully, but the Admin Portal displays an authentication error after the login attempt.

Probable Cause

Incorrect Microsoft Entra ID authentication details are configured for the Domain Alias. For example, the error can occur if an incorrect Client Secret is entered.

Recommended Action

Verify the authentication details on the Microsoft Entra Tenant Configuration page. Ensure that the **Tenant Name**, **Tenant ID**, **Client ID**, **Client Scope**, **Client Secret**, and **Client Domain Name** are correct.

7.5. Error Shown on the Dashboard

An error appears on the **Dashboard** with the following message: "*The HaloENGINE Service is not responding or is not connected. Check the HaloENGINE logs at the following location: /Secude/HaloENGINE*".

Background

When an administrator logs in to the HaloENGINE GenNXT Admin Portal, a warning appears at the top of the Dashboard. In addition, the **Select Label** list on the **Classification Rules** page is empty.

Probable Cause

One of the following conditions may have occurred:

- The HaloENGINE MPIP module is stopped.
- The HaloENGINE MPIP module certificate has expired.

Recommended Action

1. Check the status of the HaloENGINE MPIP module and start the service if it is stopped.
2. Check the HaloENGINE MPIP module certificate. If the certificate has expired, renew it using the `heslibconfig.exe` tool and restart the HaloENGINE Service.
3. Log in to the HaloENGINE GenNXT Admin Portal and verify that the **Select Label** list displays the available labels.

8. Technical Support

Before Contacting 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.

9. Appendix

This section contains supplementary information.

9.1. Classification Rule Use Cases

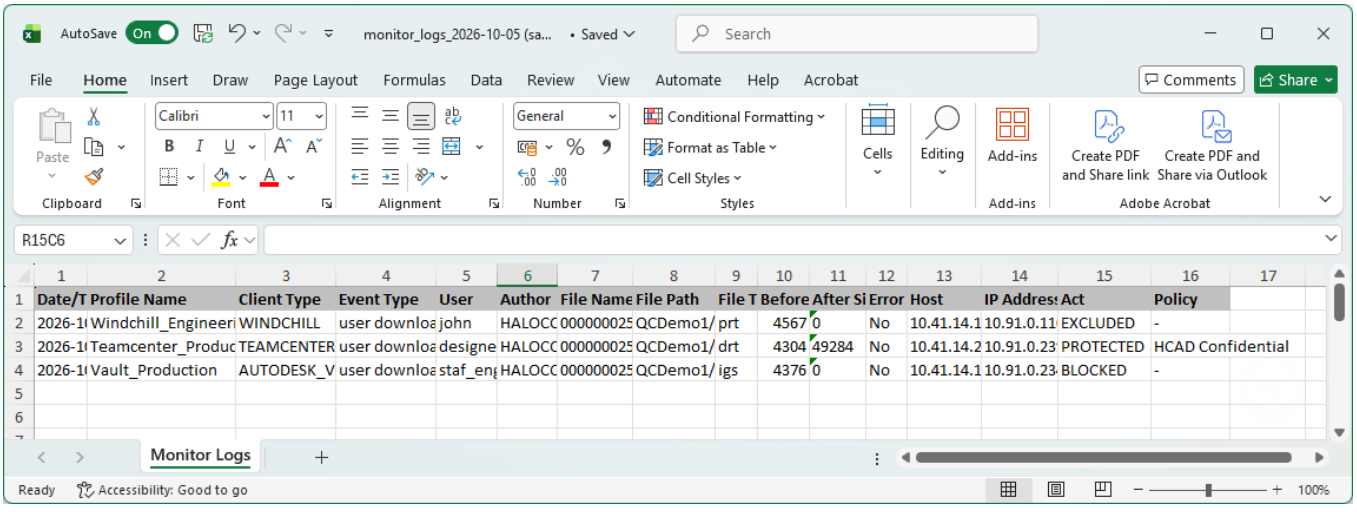
The following use cases illustrate how you can configure classification rules to block or protect files based on file type, server, project, or user. You can also use other metadata in classification rules based on your business requirements. These examples also demonstrate how multiple conditions and **Pre-Expressions** can be combined to meet specific business requirements.

Use Case	Classification Rule	Action	Result
Block PDF files	`file_type == pdf*`	Block	When the file type matches `pdf`, HaloENGINE GenNXT blocks the PDF file download and allows other file types.
Protect files from a specific server	`server_name == Windchill_Engineering`	Label: `Confidential`	When the server name matches `Windchill_Engineering`, HaloENGINE GenNXT applies the **Confidential** MPIP label to all files from that server.
Protect a specific file type except for a specific user	`file_type == prt AND user_name != john`	Label: `Confidential`	When the file type is `prt`, HaloENGINE GenNXT applies the **Confidential** MPIP label to the file for all users except `john`. John's PRT files remain unprotected.

Use Case	Classification Rule	Action	Result
Protect project files except for a group of users	`project_name == robot AND user_name != Group:4-Admin Users` **Note:** `Group:4-Admin Users` is a **Pre-Expression** value that contains a group of users to exclude.	Label: `Confidential`	When the project name is `robot`, HaloENGINE GenNXT applies the **Confidential** MPIP label to the files for all users except members of the `Group:4-Admin Users` group.
Protect final documents except for documents from specific workspaces	`life_cycle == final AND workspace != Engineering_Workspaces` **Note:** `Engineering_Workspaces` is a **Pre-Expression** value that contains a group of workspaces to exclude.	**Label:** `Confidential`	When the lifecycle state is `final`, HaloENGINE GenNXT applies the **Confidential** MPIP label to documents except those from the specified group of workspaces.

9.2. Sample Logs

The following sample logs illustrate the information recorded for **Block**, **Label**, and **Exclude** events.



Date/T	Profile Name	Client Type	Event Type	User	Author	File Name	File Path	File T	Before	After Si	Error	Host	IP Address	Act	Policy
2026-1	Windchill_Engineeri	WINDCHILL	user downloa	john	HALOCC	000000025	QCDemo1/	prt	4567	0	No	10.41.14.1	10.91.0.11	EXCLUDED	-
2026-1	Teamcenter_Produc	TEAMCENTER	user downloa	designe	HALOCC	000000025	QCDemo1/	drt	4304	49284	No	10.41.14.2	10.91.0.23	PROTECTED	HCAD Confidential
2026-1	Vault_Production	AUTODESK_V	user downloa	staf_en	HALOCC	000000025	QCDemo1/	igs	4376	0	No	10.41.14.1	10.91.0.23	BLOCKED	-

Sample monitor log in Excel

```
. {
.   "identification" : {
.     "profileName" : "Windchill_Engineering",
```

```
    "clientType" : "WINDCHILL"
  },
  "logInfo" : {
    "utcTimeStamp" : 1793101510008,
    "datetime" : null,
    "timeZone" : 0.0,
    "logID" : null
  },
  "userInfo" : {
    "userName" : "plm1user",
    "userType" : "Product Manager",
    "userEmail" : "HaloENGINE Service"
  },
  "fileInfo" : {
    "fileName" : "dasfger.asm",
    "filePath" : "Sample/Workspace on Sample",
    "fileType" : "asm",
    "fileProtectedBefore" : false,
    "sizeOriginal" : 298067,
    "sizeDownload" : 298067
  },
  "resultedDecision" : {
    "fileBlocked" : false,
    "fileLabeled" : false,
    "fileExcluded" : true,
    "fileDecrypted" : false,
    "fileProtected" : false,
    "unprotected" : false,
    "unlabeled" : false,
    "fileBlockedByRule" : false,
    "policyName" : null,
    "policyId" : null,
    "classification" : null,
    "abortedBySystem" : false,
    "abortedByUser" : false,
    "error" : false,
    "simMode" : false,
    "extendedTags" : [ ]
  },
  "plmContextInfo" : {
    "eventType" : "user download",
    "preProcessInfo" : [ ],
    "attributes" : [ {
      "type" : null,
```

```
        "key" : "product_name",
        "value" : "Sample"
      }, {
        "type" : null,
        "key" : "system_context",
        "value" : "Sample"
      }, {
        "type" : null,
        "key" : "organization_name",
        "value" : "Secude"
      }, {
        "type" : null,
        "key" : "lifecycle_template",
        "value" : "Basic"
      }, {
        "type" : null,
        "key" : "lifecycle_state",
        "value" : "In Work"
      }, {
        "type" : null,
        "key" : "workspace_name",
        "value" : "Workspace on Sample"
      } ],
      "documentId" : null,
      "documentNumber" : null,
      "documentType" : null,
      "documentPart" : null,
      "documentVersion" : null,
      "viewOnly" : null,
      "dmsProcess" : false,
      "browserClient" : false
    },
    "plmDestInfo" : {
      "destinationAttributes" : [ {
        "type" : null,
        "key" : "client_ip",
        "value" : "10.41.0.103"
      }, {
        "type" : null,
        "key" : "client_host",
        "value" : "10.41.0.103"
      } ],
```

```
.      "browser" : "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
  like Gecko) Chrome/146.0.7680.179; Creo Browser; Wildfire NoTrail; ProE-
  Datecode:4402026092 Safari/537.36",
.      "hostname" : "10.41.0.124",
.      "ipaddress" : "10.41.0.103",
.      "operatingSystem" : "WINDOWS"
.    }
. }
```

Sample monitor log in JSON

9.3. Reset Administrator Password

HaloENGINE GenNXT lets you change or reset 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.

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`

9.4. Metadata Definition

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

9.4.1. Windchill

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

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

Windchill metadata	Use
security_label	Derivation from the 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 the file type (Creo file types and MS Office native file types). (For example, sec, prt, asm, xlsx)
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

9.4.2. Teamcenter

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

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.

Teamcenter metadata	Use
	(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. (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. 1. Yes 2. No

Teamcenter metadata

9.4.3. Autodesk Vault

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

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`)
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

9.4.4. SOLIDWORKS PDM

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

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)
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

9.5. Third-Party Libraries

Third-party software/code is included or bundled with Secude's products according to its appropriate license. Secude tests third-party products to ensure they are compatible with, and perform as intended in, Secude applications.

The third-party libraries and dependencies used by HaloENGINE GenNXT are shown in the table below.

Library names	Version	Source Code URLs	License Links	Library names
org.eclipse.angus:angus-activation	2.0.2	https://github.com/eclipse-ee4j/angus-activation	EDL 1.0	http://www.eclipse.org/org/documents/edl-v10.php
org.antlr:antlr4-runtime	4.13.0	https://github.com/antlr/antlr4	BSD-3-Clause	https://www.antlr.org/license.html
org.aspectj:aspectjweaver	1.9.22.1	https://github.com/eclipse-aspectj/aspectj	Eclipse Public License - v 2.0	https://www.eclipse.org/org/documents/epl-2.0/EPL-2.0.txt
org.attoparser:attoparser	2.0.7.RELEASE	https://github.com/attoparser/attoparser	The Apache Software License, Version 2.0	https://www.apache.org/licenses/LICENSE-2.0.txt
net.bytebuddy:byte-buddy	1.14.19	https://github.com/raphw/byte-buddy	Apache License, Version 2.0	https://www.apache.org/licenses/LICENSE-2.0.txt
com.fasterxml:classmate	1.7.0	https://github.com/FasterXML/java-classmate	Apache License, Version 2.0	https://www.apache.org/licenses/LICENSE-2.0.txt
commons-codec:commons-codec	1.16.1	https://github.com/apache/commons-codec	Apache-2.0	https://www.apache.org/licenses/LICENSE-2.0.txt
org.apache.commons:commons-collections4	4.4	https://github.com/apache	Apache License, Version 2.0	https://www.apache.org/licenses/LICENSE-2.0.txt

Library names	Version	Source Code URLs	License Links	Library names
org.apache.commons:commons-compress	1.25.0	https://github.com/apache	Apache-2.0	https://www.apache.org/licenses/LICENSE-2.0.txt
commons-io:commons-io	2.21.0	https://mvnrepository.com/artifact/commons-io/commons-io/2.21.0	Apache-2.0	https://www.apache.org/licenses/LICENSE-2.0.txt
org.apache.commons:commons-math3	3.6.1	https://github.com/apache	Apache 2.0	http://www.apache.org/licenses/LICENSE-2.0.txt
com.github.virtuald:curvesapi	1.08	https://github.com/virtuald/curvesapi	BSD License	http://opensource.org/licenses/BSD-3-Clause
org.hdrhistogram:HdrHistogram	2.2.2	https://github.com/HdrHistogram/HdrHistogram	BSD 2-Clause	https://github.com/HdrHistogram/HdrHistogram/blob/master/LICENSE.txt
org.hibernate.common:hibernate-commons-annotations	6.0.6.Final	https://github.com/hibernate/hibernate-commons-annotations	GNU Library General Public License v2.1 or later	http://www.opensource.org/licenses/LGPL-2.1
org.hibernate:hibernate-community-dialects	6.6.4.Final	https://github.com/hibernate/hibernate-orm	GNU Library General Public License v2.1 or later	https://www.opensource.org/licenses/LGPL-2.1
org.hibernate.orm:hibernate-core	6.5.3.Final	https://github.com/hibernate/hibernate-orm	GNU Library General Public License v2.1 or later	https://www.opensource.org/licenses/LGPL-2.1
org.hibernate:hibernate-validator	8.0.1.Final	https://github.com/hibernate/hibernate-validator	Apache License 2.0	http://www.apache.org/licenses/LICENSE-2.0.txt

Library names	Version	Source Code URLs	License Links	Library names
com.zaxxer:HikariCP	5.1.0	https://github.com/brettwooldridge/HikariCP	Apache 2.0	https://www.apache.org/licenses/LICENSE-2.0.txt
com.sun.istack:istack-commons-runtime	4.1.2	https://github.com/eclipse-ee4j/jaxb-istack-commons	Eclipse v 1.0	http://www.eclipse.org/org/documents/edl-v10.php
com.fasterxml.jackson.core:jackson-annotations	2.17.3	https://github.com/FasterXML/jackson-annotations	Apache 2.0	https://www.apache.org/licenses/LICENSE-2.0.txt
com.fasterxml.jackson.core:jackson-core	2.17.3	https://github.com/FasterXML/jackson-core	Apache 2.0	https://www.apache.org/licenses/LICENSE-2.0.txt
com.fasterxml.jackson.core:jackson-databind	2.17.3	https://github.com/FasterXML/jackson-databind	Apache 2.0	https://www.apache.org/licenses/LICENSE-2.0.txt
com.fasterxml.jackson.datatype:jackson-datatype-jdk8	2.17.3	https://github.com/FasterXML/jackson-modules-java8	Apache 2.0	http://www.apache.org/licenses/LICENSE-2.0.txt
com.fasterxml.jackson.module:jackson-module-parameter-names	2.17.3	https://github.com/FasterXML/jackson-modules-java8	Apache 2.0	http://www.apache.org/licenses/LICENSE-2.0.txt
jakarta.activation:jakarta.activation-api	2.1.3	https://github.com/jakartaee/jaf-api	EDL 1.0	http://www.eclipse.org/org/documents/edl-v10.php
jakarta.inject:jakarta.inject-api	2.0.1	https://github.com/eclipse-ee4j/injection-api	Apache 2.0	http://www.apache.org/licenses/LICENSE-2.0.txt

Library names	Version	Source Code URLs	License Links	Library names
jakarta.persistence:jakarta.persistence-api	3.1.0	https://github.com/jakartaee/persistence	EPL 2.0 / BSD 3 (EDL 1.0)	https://www.eclipse.org/legal/epl-2.0/
jakarta.transaction:jakarta.transaction-api	2.0.1	https://github.com/eclipse-ee4j/jta-api	EPL 2.0 / GPL 2.0	https://www.eclipse.org/legal/epl-2.0/
jakarta.validation:jakarta.validation-api	3.0.2	https://github.com/jakartaee/validation	Apache 2.0	http://www.apache.org/licenses/LICENSE-2.0.txt
jakarta.xml.bind:jakarta.xml.bind-api	4.0.2	https://github.com/jakartaee/jaxb-api	Eclipse v 1.0	http://www.eclipse.org/org/documents/edl-v10.php
org.jboss:jandex	3.1.2	https://github.com/jboss/jboss-parent-pom	Public Domain	http://repository.jboss.org/licenses/cc0-1.0.txt
com.sun.xml.bind:jaxb-core	4.0.5	https://github.com/eclipse-ee4j/jaxb-ri	Eclipse v 1.0	http://www.eclipse.org/org/documents/edl-v10.php
org.glassfish.jaxb:jaxb-runtime	4.0.5	https://github.com/eclipse-ee4j/jaxb-ri	Eclipse v 1.0	http://www.eclipse.org/org/documents/edl-v10.php
org.jboss.logging:jboss-logging	3.5.3.Final	https://github.com/jboss-logging/jboss-logging	Apache License 2.0	https://repository.jboss.org/licenses/apache-2.0.txt
io.jsonwebtoken:jjwt-api	0.12.6	https://github.com/jwtk/jjwt	Apache 2.0	https://www.apache.org/licenses/LICENSE-2.0
io.jsonwebtoken:jjwt-impl	0.12.6	https://github.com/jwtk/jjwt	Apache 2.0	https://www.apache.org/licenses/LICENSE-2.0
io.jsonwebtoken:jjwt-jackson	0.12.6	https://github.com/jwtk/jjwt	Apache 2.0	https://www.apache.org/licenses/LICENSE-2.0

Library names	Version	Source Code URLs	License Links	Library names
net.java.dev.jna:jna	5.13.0	https://github.com/java-native-access/jna	Apache 2.0 / LGPL 2.1	https://github.com/java-native-access/jna/blob/master/LICENSE
org.slf4j:jul-to-slf4j	2.0.16	https://github.com/qos-ch/slf4j	MIT License	http://www.opensource.org/licenses/mit-license.php
org.latencyutils:LatencyUtils	2.0.3	https://github.com/LatencyUtils/LatencyUtils	Public Domain, per Creative Commons CC0	http://creativecommons.org/publicdomain/zero/1.0/
com.javax0.license3j:license3j	3.3.0	https://github.com/verhas/License3j	Apache 2.0	http://www.apache.org/licenses/LICENSE-2.0.txt
org.apache.logging.log4j:log4j-api	2.24.2	https://github.com/apache/logging-log4j2	Apache-2.0	https://www.apache.org/licenses/LICENSE-2.0.txt
org.apache.logging.log4j:log4j-core	2.25.3	https://github.com/apache/logging-log4j2	Apache-2.0	https://www.apache.org/licenses/LICENSE-2.0.txt
org.apache.logging.log4j:log4j-to-slf4j	2.23.1	https://github.com/apache/logging-log4j2	Apache-2.0	https://www.apache.org/licenses/LICENSE-2.0.txt
ch.qos.logback:logback-classic	1.5.12	https://github.com/qos-ch/logback	EPL 1.0 / LGPL 2.1	https://github.com/qos-ch/logback/blob/master/LICENSE.txt
ch.qos.logback:logback-core	1.5.12	https://github.com/qos-ch/logback	EPL 1.0 / LGPL 2.1	logback/LICENSE.txt at master · qos-ch/logback
io.micrometer:micrometer-commons	1.13.8	https://github.com/micrometer-metrics/micrometer	Apache 2.0	http://www.apache.org/licenses/LICENSE-2.0.txt
io.micrometer:micrometer-core	1.13.8	https://github.com/micrometer-metrics/micrometer	Apache 2.0	http://www.apache.org/licenses/LICENSE-2.0.txt

Library names	Version	Source Code URLs	License Links	Library names
io.micrometer:micrometer-jakarta9	1.13.8	https://github.com/micrometer-metrics/micrometer	Apache 2.0	http://www.apache.org/licenses/LICENSE-2.0.txt
io.micrometer:micrometer-observation-test	1.13.8	https://github.com/micrometer-metrics/micrometer	Apache 2.0	http://www.apache.org/licenses/LICENSE-2.0.txt
com.microsoft.sqlserver:mssql-jdbc	12.8.1.jre11	https://github.com/Microsoft/mssql-jdbc	MIT License	http://www.opensource.org/licenses/mit-license.php
com.mysql:mysql-connector-j	9.3.0	https://github.com/mysql/mysql-connector-j	GPL 2.0	https://github.com/mysql/mysql-connector-j/blob/release/9.x/LICENSE
org.apache.poi:poi	5.2.5	https://github.com/AlfrescoArchive/poi	Apache 2.0	http://www.apache.org/licenses/LICENSE-2.0.txt
org.apache.poi:poi-ooxml	5.2.5	https://github.com/AlfrescoArchive/poi	Apache 2.0	http://www.apache.org/licenses/LICENSE-2.0.txt
org.apache.poi:poi-ooxml-lite	5.2.5	https://github.com/apache/poi	Apache 2.0	http://www.apache.org/licenses/LICENSE-2.0.txt
org.slf4j:slf4j-api	2.0.16	https://github.com/qos-ch/slf4j	MIT License	http://www.opensource.org/licenses/mit-license.php
org.yaml:snakeyaml	2.2	https://github.com/yaml	Apache 2.0	http://www.apache.org/licenses/LICENSE-2.0.txt

Library names	Version	Source Code URLs	License Links	Library names
com.zaxxer:SparseBitSet	1.3	https://github.com/brettwooldridge/SparseBitSet	Apache 2.0	http://www.apache.org/licenses/LICENSE-2.0.txt
org.springframework:spring-aop	6.1.15	https://github.com/spring-projects/spring-framework	Apache 2.0	https://www.apache.org/licenses/LICENSE-2.0
org.springframework:spring-core	6.1.15	https://github.com/spring-projects/spring-framework	Apache 2.0	https://www.apache.org/licenses/LICENSE-2.0
org.springframework:spring-beans	6.1.15	https://github.com/spring-projects/spring-framework	Apache 2.0	https://www.apache.org/licenses/LICENSE-2.0
org.springframework.boot:spring-boot	3.3.6	https://github.com/spring-projects/spring-boot	Apache 2.0	https://www.apache.org/licenses/LICENSE-2.0
org.springframework.boot:spring-boot-starter-actuator	3.3.6	https://github.com/spring-projects/spring-boot	Apache 2.0	https://www.apache.org/licenses/LICENSE-2.0
org.springframework.boot:spring-boot-actuator-autoconfigure	3.3.6	https://github.com/spring-projects/spring-boot	Apache 2.0	https://www.apache.org/licenses/LICENSE-2.0
org.springframework.boot:spring-boot-autoconfigure	3.3.6	https://github.com/spring-projects/spring-boot	Apache 2.0	https://www.apache.org/licenses/LICENSE-2.0
org.springframework.boot:spring-boot-devtools	3.3.6	https://github.com/spring-projects/spring-boot	Apache 2.0	https://www.apache.org/licenses/LICENSE-2.0

Library names	Version	Source Code URLs	License Links	Library names
org.springframework.boot:spring-boot-starter	3.3.6	https://github.com/spring-projects/spring-boot	Apache 2.0	https://www.apache.org/licenses/LICENSE-2.0
org.springframework.boot:spring-boot-starter-actuator	3.3.6	https://github.com/spring-projects/spring-boot	Apache 2.0	https://www.apache.org/licenses/LICENSE-2.0
org.springframework.boot:spring-boot-starter-aop	3.3.6	https://github.com/spring-projects/spring-boot	Apache 2.0	https://www.apache.org/licenses/LICENSE-2.0
org.springframework.boot:spring-boot-starter-data-jpa	3.3.6	https://github.com/spring-projects/spring-boot	Apache 2.0	https://www.apache.org/licenses/LICENSE-2.0
org.springframework.boot:spring-boot-starter-jdbc	3.3.6	https://github.com/spring-projects/spring-boot	Apache 2.0	https://www.apache.org/licenses/LICENSE-2.0
org.springframework.boot:spring-boot-starter-json	3.3.6	https://github.com/spring-projects/spring-boot	Apache 2.0	https://www.apache.org/licenses/LICENSE-2.0
org.springframework.boot:spring-boot-starter-logging	3.3.6	https://github.com/spring-projects/spring-boot	Apache 2.0	https://www.apache.org/licenses/LICENSE-2.0
org.springframework.boot:spring-boot-starter-security	3.3.6	https://github.com/spring-projects/spring-boot	Apache 2.0	https://www.apache.org/licenses/LICENSE-2.0
org.springframework.boot:spring-boot-starter-thymeleaf	3.3.6	https://github.com/spring-projects/spring-boot	Apache 2.0	https://www.apache.org/licenses/LICENSE-2.0
org.springframework.boot:spring-boot-starter-validation	3.3.6	https://github.com/spring-projects/spring-boot	Apache 2.0	https://www.apache.org/licenses/LICENSE-2.0

Library names	Version	Source Code URLs	License Links	Library names
org.springframework.boot:spring-boot-starter-web	3.3.6	https://github.com/spring-projects/spring-boot	Apache 2.0	https://www.apache.org/licenses/LICENSE-2.0
org.springframework:spring-context	6.1.15	https://github.com/spring-projects/spring-framework	Apache 2.0	https://www.apache.org/licenses/LICENSE-2.0
org.springframework:spring-core	6.1.15	https://github.com/spring-projects/spring-framework	Apache 2.0	https://www.apache.org/licenses/LICENSE-2.0
org.springframework.data:spring-data-commons	3.3.6	https://github.com/spring-projects/spring-data-jpa	Apache 2.0	https://www.apache.org/licenses/LICENSE-2.0
org.springframework.data:spring-data-jpa	3.3.6	https://github.com/spring-projects/spring-data-jpa	Apache 2.0	https://www.apache.org/licenses/LICENSE-2.0
org.springframework:spring-expression	6.1.15	https://github.com/spring-projects/spring-framework	Apache 2.0	https://www.apache.org/licenses/LICENSE-2.0
org.springframework:spring-jcl	6.1.15	https://github.com/spring-projects/spring-framework	Apache 2.0	https://www.apache.org/licenses/LICENSE-2.0
org.springframework:spring-jdbc	6.1.15	https://github.com/spring-projects/spring-framework	Apache 2.0	https://www.apache.org/licenses/LICENSE-2.0
org.springframework:spring-orm	6.1.15	https://github.com/spring-projects/spring-framework	Apache 2.0	https://www.apache.org/licenses/LICENSE-2.0

Library names	Version	Source Code URLs	License Links	Library names
org.springframework.security:spring-security-config	6.3.5	https://www.apache.org/licenses/LICENSE-2.0	Apache 2.0	https://www.apache.org/licenses/LICENSE-2.0
org.springframework.security:spring-security-core	6.3.5	https://www.apache.org/licenses/LICENSE-2.0	Apache 2.0	https://www.apache.org/licenses/LICENSE-2.0
org.springframework.security:spring-security-crypto	6.3.5	https://www.apache.org/licenses/LICENSE-2.0	Apache 2.0	https://www.apache.org/licenses/LICENSE-2.0
org.springframework.security:spring-security-web	6.3.5	https://www.apache.org/licenses/LICENSE-2.0	Apache 2.0	https://www.apache.org/licenses/LICENSE-2.0
springframework:spring-tx	6.1.15	https://github.com/spring-projects/spring-framework	Apache 2.0	https://www.apache.org/licenses/LICENSE-2.0
org.springframework:spring-web	6.1.15	https://github.com/spring-projects/spring-framework	Apache 2.0	https://www.apache.org/licenses/LICENSE-2.0
org.springframework:spring-webmvc	6.1.15	https://github.com/spring-projects/spring-framework	Apache 2.0	https://www.apache.org/licenses/LICENSE-2.0
org.xerial:sqlite-jdbc	3.47.1.0	https://github.com/xerial/sqlite-jdbc	Apache 2.0	https://github.com/xerial/sqlite-jdbc/blob/master/LICENSE
org.thymeleaf:thymeleaf	3.1.2.RELEASE	https://github.com/thymeleaf/thymeleaf	Apache 2.0	https://www.apache.org/licenses/LICENSE-2.0
org.thymeleaf.extras:thymeleaf-extras-springsecurity6	3.1.2.RELEASE		Apache 2.0	https://www.apache.org/licenses/LICENSE-2.0

Library names	Version	Source Code URLs	License Links	Library names
		https://github.com/thymeleaf/thymeleaf-extras-springsecurity		
org.thymeleaf:thymeleaf-spring6	3.1.2.RELEASE	https://github.com/thymeleaf/thymeleaf	Apache 2.0	https://www.apache.org/licenses/LICENSE-2.0
org.glassfish.jaxb:txw2	4.0.5	https://github.com/eclipse-ee4j/jaxb-ri	Apache 2.0	https://www.eclipse.org/org/documents/edl-v10.php
org.unbescape:unbescape	1.1.6.RELEASE	https://github.com/unbescape/unbescape	Apache 2.0	https://www.apache.org/licenses/LICENSE-2.0
org.apache.xmlbeans:xmlbeans	5.2.0	https://github.com/apache/xmlbeans	Apache 2.0	https://www.apache.org/licenses/LICENSE-2.0

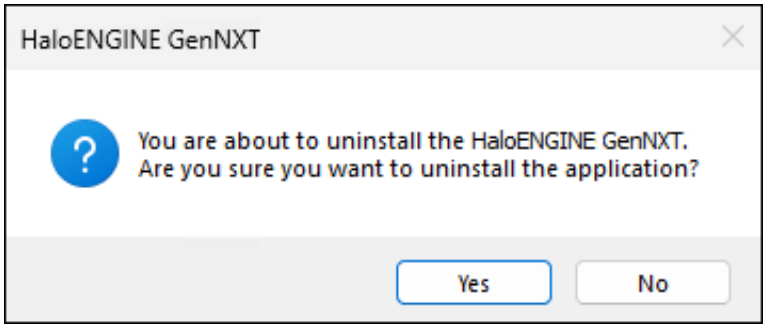
Third-party libraries

9.6. Uninstalling the HaloENGINE GenNXT

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.

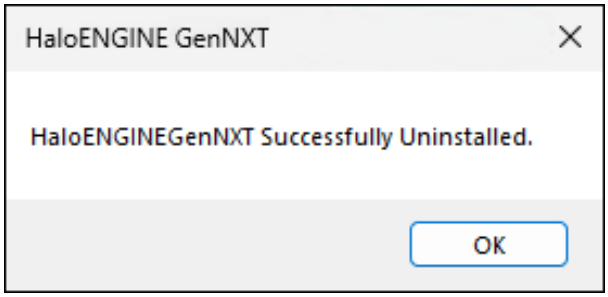
When you no longer use the service, you may uninstall the application. Uninstalling removes all files and registry settings added to your computer during initial installation.

1. Click **Start** menu > go to **Control Panel** > **Programs** > **Programs and Features** > **Uninstall a Program** > select **HaloENGINE GenNXT** application from the list > right-click and select **Uninstall** option, or double-click on the installer `HaloENGINEGenNXT_Setup.exe`.
2. Depending on your Windows security settings, you may see a security warning asking, "*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. The application is uninstalled successfully.



Uninstall message #2

6. Click **OK** to close the dialog.

Remove the Database Files Manually

Uninstallation does not automatically remove the database files from the configuration folder.

- For **MySQL** and **MSSQL**, select the database created for HaloENGINE GenNXT, right-click it, and select **Delete**.
- Manually delete all files from the following folder: `%HaloENGINE_HOME%\HaloENGINE\config`.

Index

A

Alias-name 9, 37, 58
Application-id 9, 37

C

Ca-signed 9
Check-in 5
Check-out 5
Client-id 58
Client-scope 9, 58
Client-secret 9, 58
Common-name 9, 37
Computer-account 9
Current-user 9
Custom 58

D

Directory-id 9
Dke 46

E

Exclude 58, 115

F

Fail-safe-mode 1, 5, 58

M

Mpip 1, 9
Mysql 8

P

Pre-expression 1, 58

R

Redirect-uri 9
Root-ca 9

S

Self-signed 9
Sensitivity-label 1
Siem 1
Sqlite 8
Static 58
Static-email 58
Strict 58
Subject-alternative-name 9

T

Tcp 9
Tenant-id 37, 58
Tenant-name 9, 58
Thumbprint 37
Tls 9
Tolerant 58

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.