Secude

HaloCAD

Technical Reference Manual

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. How does HaloCAD protect your data? 1

1.2. About this Manual 2

1.3. Terminology 2

1.4. Acronyms 3

1.5. Features 4

2. RELATED DOCUMENTATION 5

3. HALOCAD ADD-ON FOR CAD 6

3.1. Architecture 6

3.2. Quick Start 7

3.3. Prerequisites 7

4. HALOCAD FOR PLM 8

4.1. Architecture 8

4.2. Quick Start 10

4.3. Prerequisites 10

5. HALOCAD FOR SOLIDWORKS PDM 11

5.1. Architecture 11

5.2. Quick Start 12

5.3. Prerequisites 13

6. HALOCAD FOR VIEWERS 14

6.1. Architecture 14

6.2. Quick Start 15

6.3. Prerequisites 15

7. HALOCAD FOR TCAI 16

7.1. Architecture 16

7.2. Quick Start 17

7.3. Prerequisites 17

8. PREREQUISITES 18

8.1. Register an Application in Microsoft Entra ID - Public client/native 18

8.1.1. Create an Application 18
8.1.2. Add Required Permissions 21
8.2. Register an Application in Microsoft Entra ID - Web 24
8.2.1. Additional Permission (Only for Decryption) 25
8.2.2. Upload the Certificate 25
8.3. Create and Configure the Sensitivity Labels 27
8.4. Office 365 Subscription Details 27
8.5. Recommended URLs, Addresses, and Ports for MPIP 28
8.6. Secude License Manager for HaloCAD 30
8.7. Enable TLS 1.2 for Microsoft Entra ID Authentication 31
9. LICENSE ADMINISTRATION 32
9.1. Secure Installation (Recommended Method) 33
9.2. UI-based Manual License Activation 37
9.3. License Renewal After Expiration 40
10. APPENDIX 41

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 Provides additional information relevant to the topic. 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

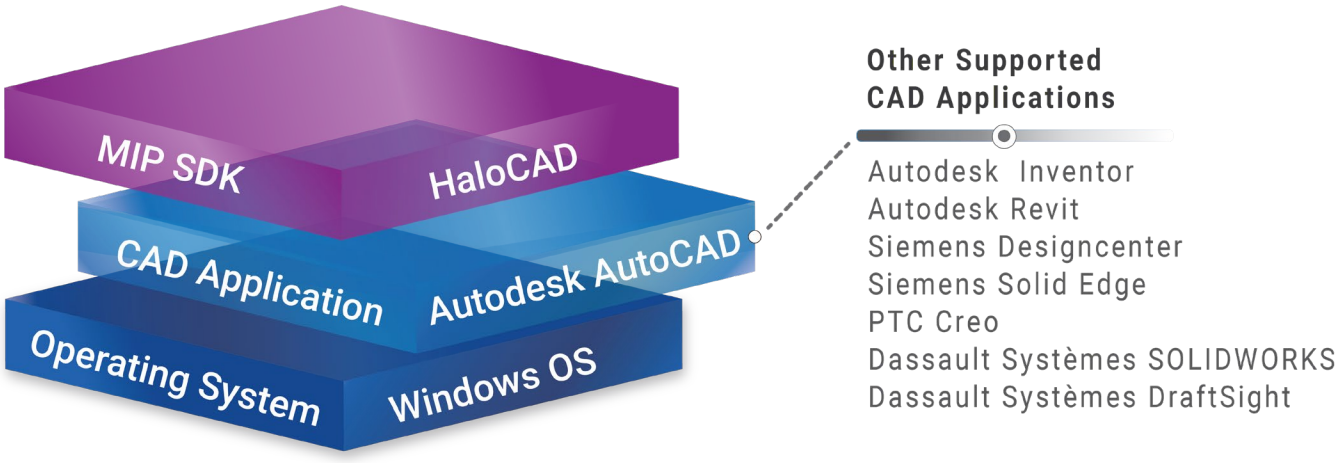
Companies across industries, including automotive, aviation, and high-tech manufacturing, create and manage valuable intellectual property (IP) in the form of CAD drawings. These drawings are often shared with customers, suppliers, and partners to support business operations. Sharing sensitive design data, however, introduces security risks that can lead to unauthorized access, modification, or distribution.

HaloCAD helps organizations protect CAD files by integrating with Microsoft Purview Information Protection (MPIP). It applies sensitivity labels and protection policies to CAD files, helping organizations safeguard their intellectual property throughout its lifecycle.

1.1. How does HaloCAD protect your data?

HaloCAD integrates with Microsoft Purview Information Protection, formerly known as Microsoft Information Protection (MIP), to provide Enterprise Digital Rights Management (EDRM) capabilities for CAD files. HaloCAD applies Microsoft Purview Information Protection sensitivity labels to CAD files and enforces the associated protection policies. Protected files can be accessed only by authorized users according to the permissions defined in the applied sensitivity label.

HaloCAD Add-on for CAD can operate as a standalone solution or integrate with HaloCAD for PLM. When integrated with a supported PLM system, HaloCAD automatically protects downloaded files, decrypts files during upload, and stores them securely in the PLM vault.



HaloCAD Add-on for CAD applications

1.2. About this Manual

This manual provides the common information shared across all HaloCAD products, including product architecture, prerequisites, licensing, and shared configuration requirements. For product-specific installation, configuration, administration, and operating procedures, refer to the appropriate **Installation Manual** and **Operations Manual**.

This manual covers the following products:

- HaloCAD Add-on for CAD
- HaloCAD for Viewers
- HaloCAD for TCAI
- HaloCAD for PLM
- HaloCAD for SOLIDWORKS PDM

1.3. Terminology

Throughout this manual, the following terms are used to refer to supported HaloCAD products and integrations.

Term	Description
HaloCAD Add-on for CAD	An add-on that integrates with supported CAD applications to protect CAD files.
HaloCAD for PLM	A solution that integrates with PLM systems and the HaloCAD Add-on for CAD to automatically lock access to files during download and unlock access when the files are returned to the PLM vault. It supports PLM integrations, such as Teamcenter, Windchill, and Autodesk Vault.
HaloCAD for PDM	A solution that integrates with SOLIDWORKS PDM and the HaloCAD Add-on for SOLIDWORKS to protect files when they are copied or moved outside the PDM vault and decrypt protected files when they are copied into the PDM vault.
HaloENGINE GenNXT	It evaluates file metadata against configured classification rules and determines the applicable action and sensitivity label.
HaloENGINE GenNXT Tomcat Service	A Windows service used by HaloENGINE GenNXT and HaloCAD components.

Terminology

1.4. Acronyms

The following acronyms are used throughout this manual.

Acronym	Description
CAD	Computer-Aided Design
PLM	Product Lifecycle Management
PDM	Product Data Management
MPIP	Microsoft Purview Information Protection
EDRM	Enterprise Digital Rights Management
TCAI	Teamcenter Integration for Autodesk Inventor
SCCM	Microsoft System Center Configuration Manager
TLS	Transport Layer Security

Acronyms

1.5. Features

HaloCAD provides the following capabilities:

1. **Integration with Existing Infrastructure**
   Integrates with your existing CAD and PLM environments without requiring significant infrastructure changes.
2. **CAD File Protection**
   Extends Microsoft Purview Information Protection to supported CAD applications by applying sensitivity labels and protection policies to CAD files.
3. **Rights Management**
   Protects CAD files by applying Microsoft Purview sensitivity labels together with user-defined permissions.
4. **Persistent Data Protection**
   Protects sensitive files wherever they are stored or shared, including cloud and mobile environments.
5. **Policy-Based Access Control**
   a. Controls who can access protected files.
   b. Controls the actions users can perform, such as viewing, editing, copying, printing, exporting, relabeling, or modifying permissions.
   c. Supports watermarking for sensitive documents.
6. **PLM Integration**
   Automatically protects files during download and removes protection from files during upload before storing the unprotected files in the PLM vault.

2. Related Documentation

The following documents provide additional information about HaloCAD products.

Document	Purpose
Installation Manual	Describes product installation, configuration, deployment methods, and uninstallation. Supports installation using the user interface (UI), silent mode, Microsoft System Center Configuration Manager (SCCM), or an encrypted configuration file (`hc.conf.json`).
Operations Manual	Describes product administration, features, and troubleshooting.
Release Notes	Describes new features, resolved issues, known issues, and supported platforms.
Technical Reference Manual	1. Provides architecture, prerequisites, licensing, secure installation, license renewal, and third-party library information for HaloCAD Add-on for CAD. 2. Provides architecture, prerequisites, and secure installation information for HaloCAD for PLM and HaloCAD for PDM.

HaloCAD-related documentation

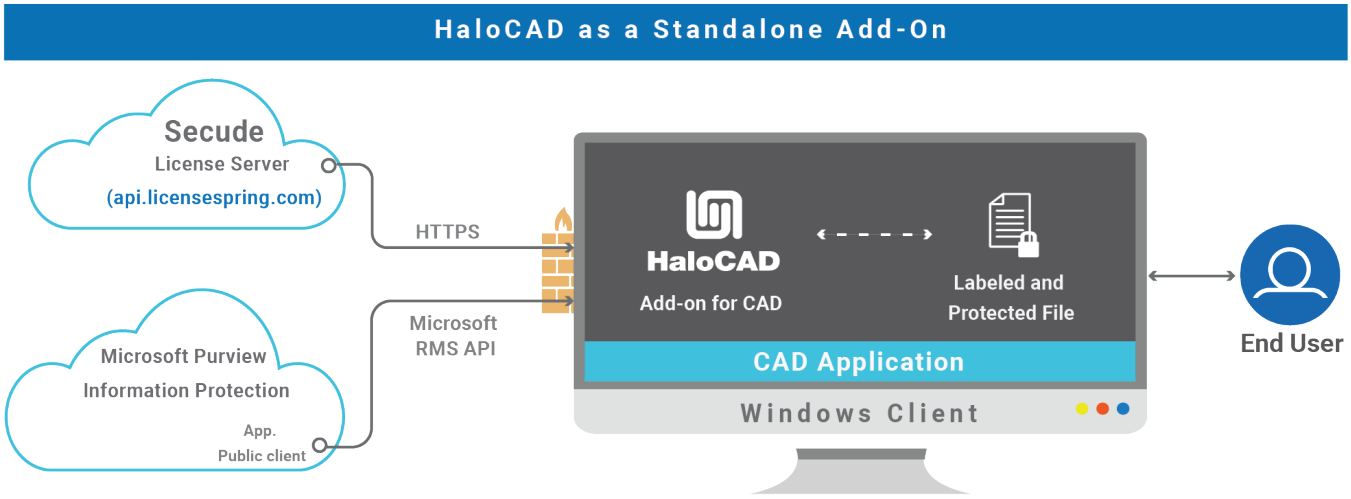
3. HaloCAD Add-on for CAD

HaloCAD Add-on for CAD is a standalone solution that provides the HaloCAD PROTECT feature. It enables users to access protected CAD files, enforces the permissions defined in the applied sensitivity labels, and allows authorized users to apply or modify MPIP sensitivity labels.

3.1. Architecture

HaloCAD Add-on for CAD integrates with Microsoft Purview Information Protection to provide persistent protection for CAD files. When creating a CAD file, users authenticate with MPIP. After successful authentication, HaloCAD downloads the available sensitivity labels. Users then select an appropriate sensitivity label and apply it to the file. In standalone mode, users apply sensitivity labels manually.

Only authorized users can open or modify protected files. The applied protection remains with the file regardless of where it is stored or shared. User permissions are determined by the applied sensitivity label and its associated protection policy. The following figure illustrates the HaloCAD Add-on for CAD operating as a standalone solution.

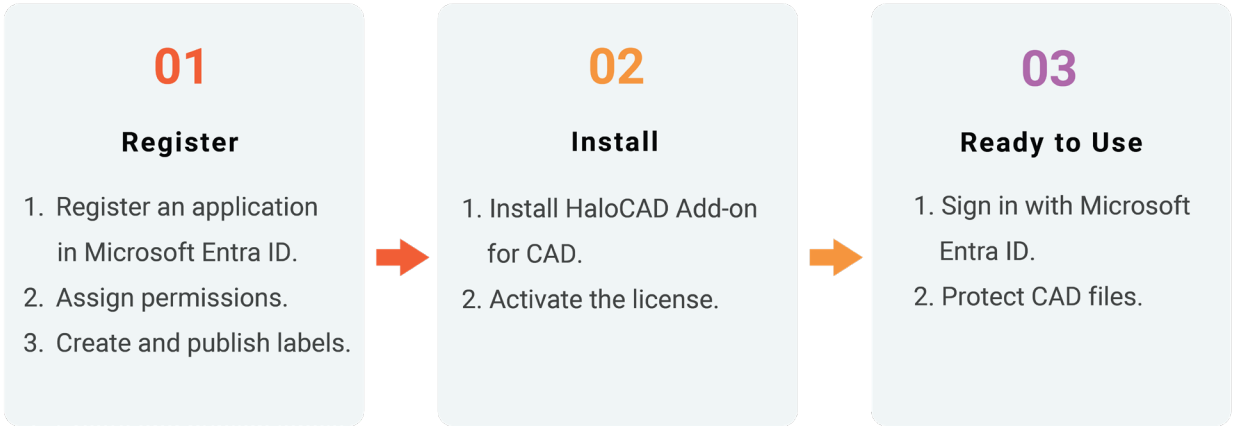


HaloCAD as a standalone add-on

Note: When HaloCAD Add-on for CAD is integrated with HaloCAD for PLM, files are automatically protected according to the configured action rules before they are made available to users.

3.2. Quick Start

The following figure illustrates the high-level process for setting up the HaloCAD Add-on for CAD.



Quick start installation steps for HaloCAD Add-on for CAD

3.3. Prerequisites

Refer to the section “Prerequisites”.

4. HaloCAD for PLM

HaloCAD extends data protection to supported Product Lifecycle Management systems. The supported integrations include:

- HaloCAD for Teamcenter
- HaloCAD for Windchill
- HaloCAD for Autodesk Vault

HaloCAD for PLM integrates with supported PLM systems and combines the capabilities of HaloCAD PROTECT and HaloCAD MONITOR while utilizing Microsoft Purview Information Protection (MPIP) to provide Enterprise Digital Rights Management (EDRM) for CAD files. It automatically protects files during download and removes protection from protected files during upload.

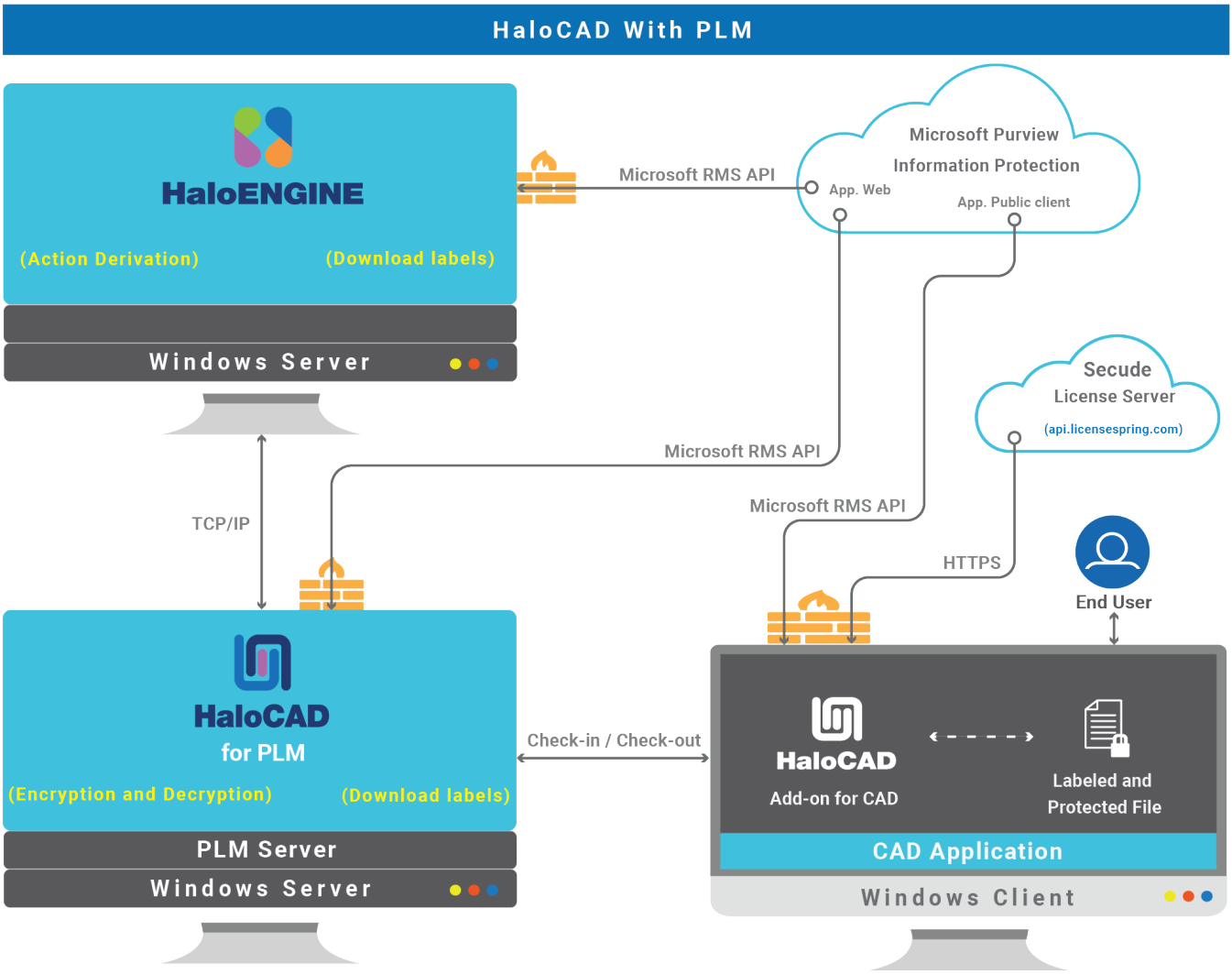
4.1. Architecture

HaloCAD for PLM continuously monitors file upload and download operations within the PLM environment. It integrates with Microsoft Purview Information Protection to download sensitivity labels and perform file encryption and decryption.

- During file upload, HaloCAD for PLM checks whether the file is protected. If the file is encrypted, HaloCAD for PLM decrypts it before storing it in the PLM Vault.
- During file download, HaloCAD for PLM applies protection based on the configured action rules before delivering the file to the user.

For file uploads, HaloCAD for PLM performs file processing independently. For file downloads, HaloCAD for PLM relies on HaloENGINE GenNXT to evaluate the configured classification and action rules.

The following figure illustrates the high-level architecture of HaloCAD for PLM.



HaloCAD for PLM

Separate Installation Requirement

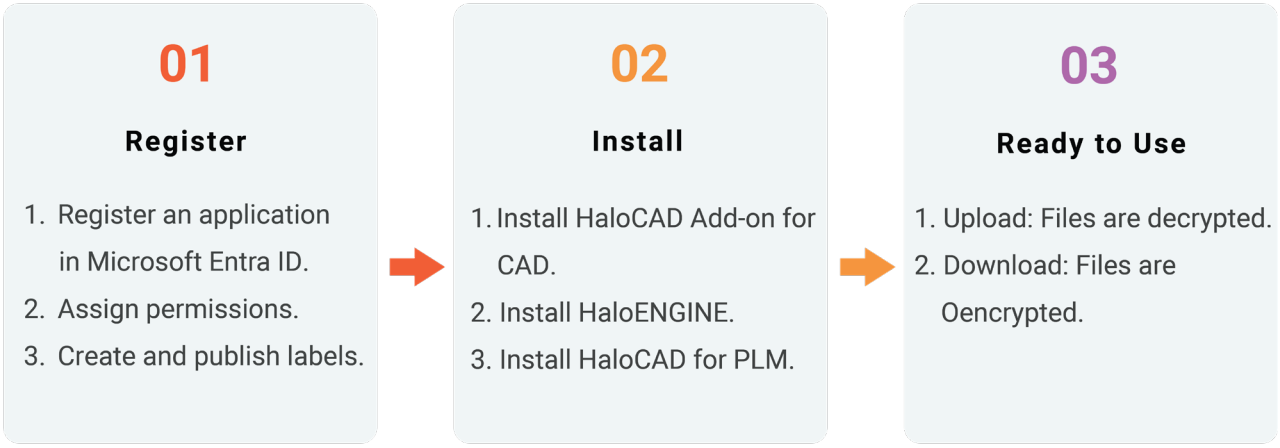
Ensure that HaloENGINE GenNXT and HaloCAD for PLM are installed and configured separately on Windows servers.

HaloENGINE GenNXT integrates with Microsoft Purview Information Protection to download sensitivity labels and make them available for configuration. It evaluates metadata based on the configured classification and action rules to determine the appropriate protection action. All file downloads must comply with these rules.

During a file download, HaloCAD for PLM sends the relevant file metadata to HaloENGINE GenNXT. HaloENGINE GenNXT evaluates the metadata, determines the required protection action and sensitivity label, and returns the result to HaloCAD for PLM. HaloCAD for PLM then applies the appropriate protection before delivering the file to the user.

4.2. Quick Start

The following figure illustrates the high-level process for setting up HaloCAD Add-on for CAD with HaloCAD for PLM.



Quick start installation steps for HaloCAD for PLM

4.3. Prerequisites

Refer to the section “Prerequisites”.

5. HaloCAD for SOLIDWORKS PDM

HaloCAD for SOLIDWORKS PDM integrates with SOLIDWORKS PDM and combines the capabilities of HaloCAD PROTECT and HaloCAD MONITOR while utilizing Microsoft Purview Information Protection (MPIP) to provide Enterprise Digital Rights Management (EDRM) for CAD files.

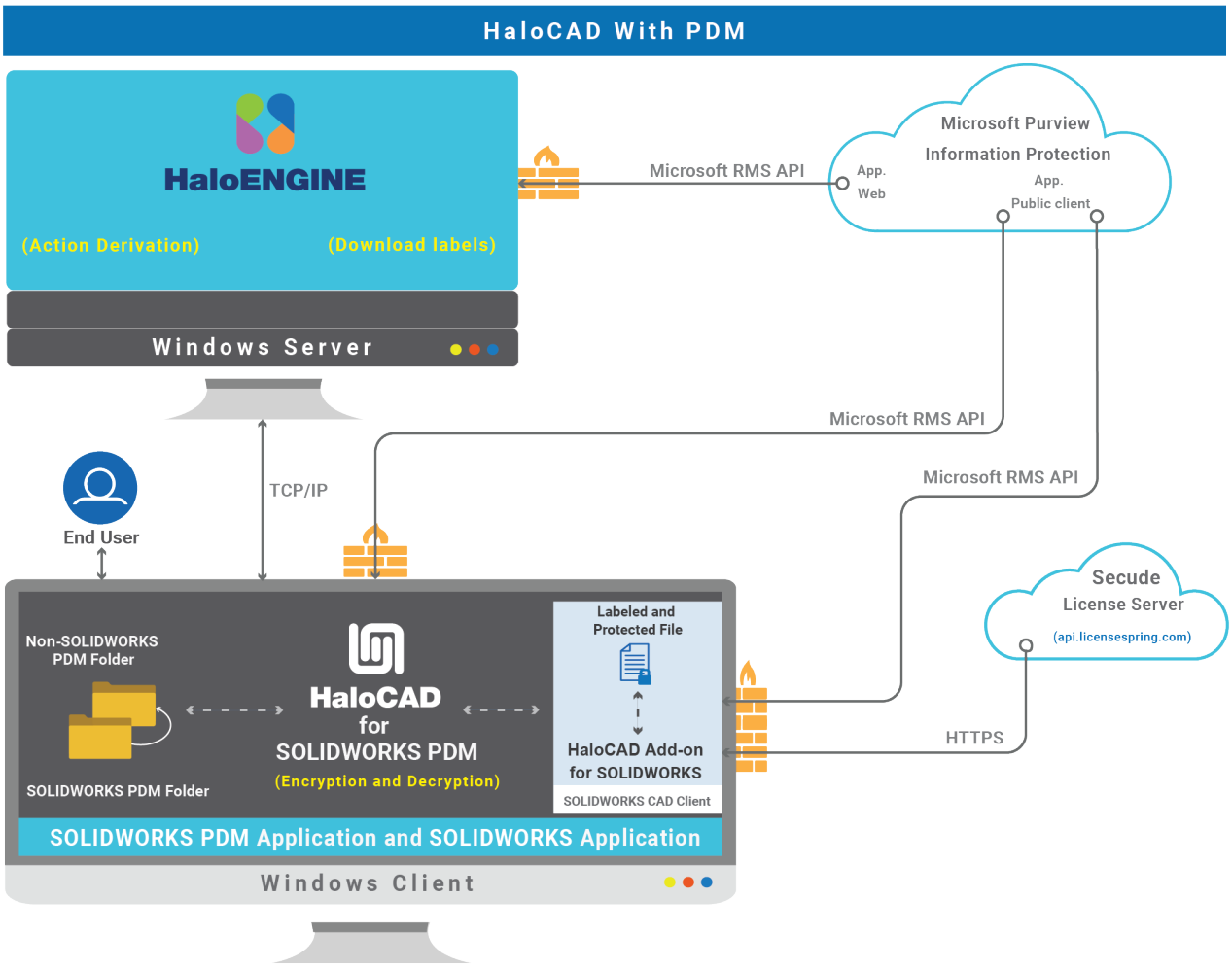
5.1. Architecture

HaloCAD for SOLIDWORKS PDM continuously monitors SOLIDWORKS PDM folders to protect CAD files during file operations.

- When users copy or move files from a SOLIDWORKS PDM folder to a non-SOLIDWORKS PDM location, HaloCAD for SOLIDWORKS PDM automatically protects the files before they reach the destination.
- When protected SOLIDWORKS CAD files or PDF files are copied or moved into a SOLIDWORKS PDM folder, HaloCAD for SOLIDWORKS PDM detects the protected files, decrypts them, and stores the decrypted files in the SOLIDWORKS PDM vault.

HaloENGINE GenNXT evaluates the configured classification and action rules to determine the protection to apply during copy and move operations. Its role is the same as described in HaloCAD for PLM.

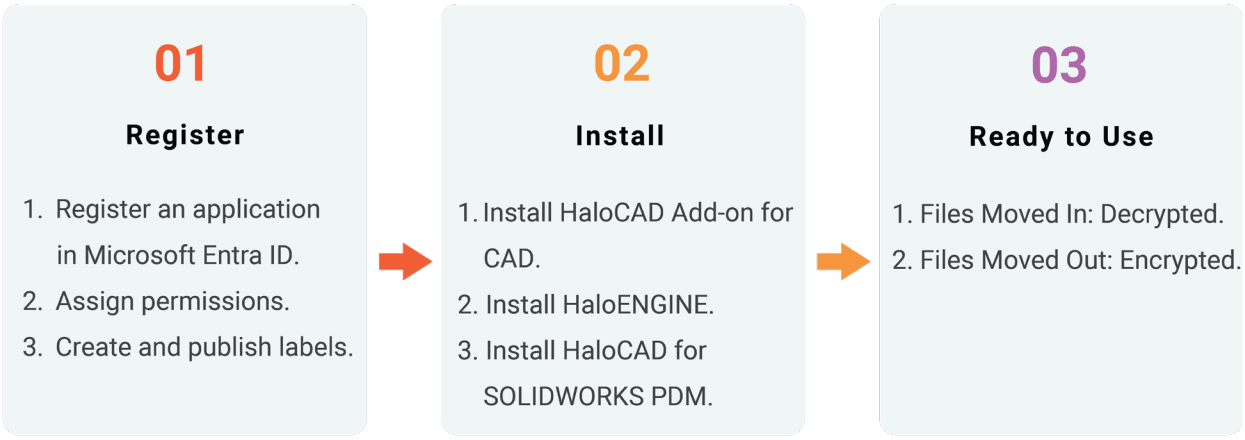
The following figure illustrates the high-level architecture of HaloCAD for SOLIDWORKS PDM.



HaloCAD for SOLIDWORKS PDM

5.2. Quick Start

The following figure illustrates the high-level process for setting up the HaloCAD Add-on for CAD with HaloCAD for SOLIDWORKS PDM.



Quick start installation steps for HaloCAD for SOLIDWORKS PDM

5.3. Prerequisites

Refer to the section “Prerequisites”.

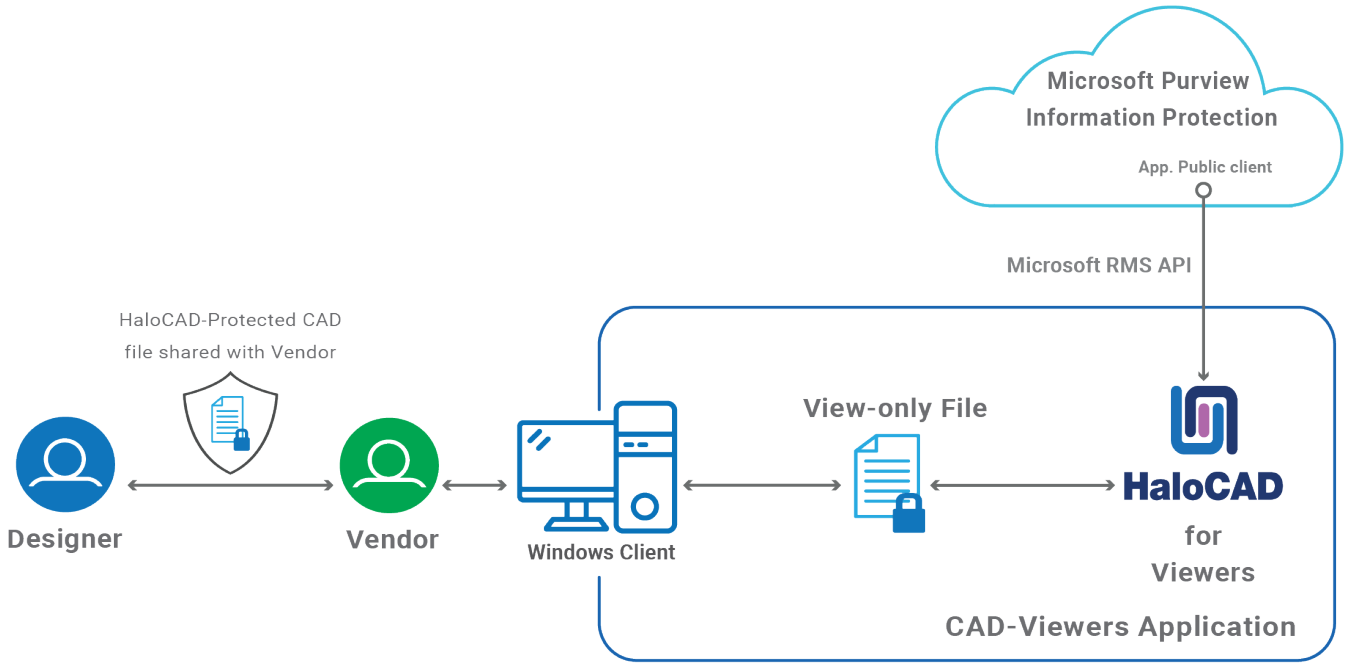
6. HaloCAD for Viewers

HaloCAD for Viewers enables users to access HaloCAD-protected CAD files in supported CAD viewer applications. It integrates with Microsoft Purview Information Protection to enforce the permissions defined in the applied sensitivity labels.

6.1. Architecture

HaloCAD for Viewers provides view-only access to HaloCAD-protected CAD files. It prevents users from modifying, copying, or taking screenshots of protected content.

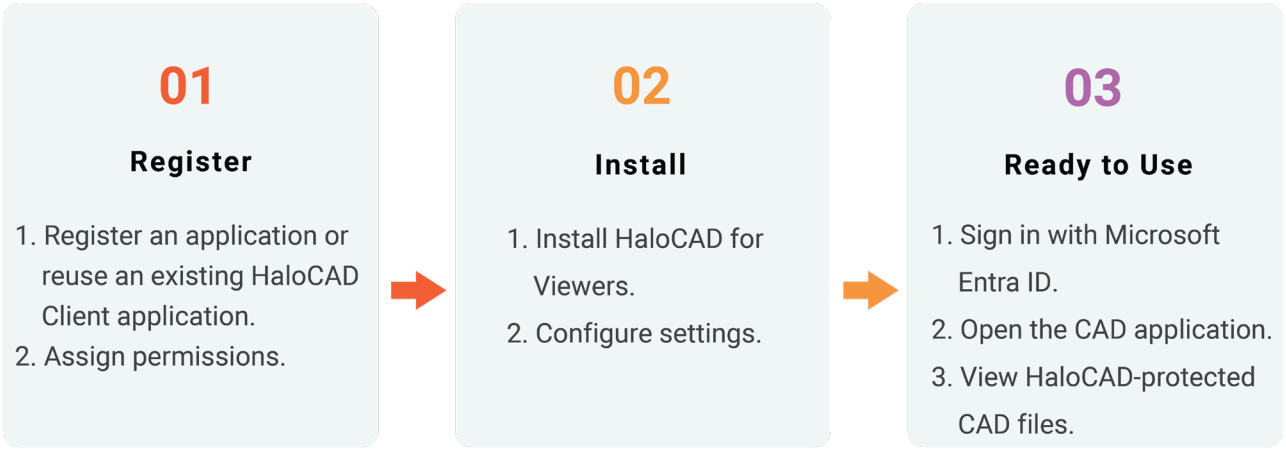
The application is intended for external users, such as suppliers and partners, who need to access protected CAD models or drawings without installing the HaloCAD Add-on for CAD. The following figure illustrates the high-level architecture of HaloCAD for Viewers.



HaloCAD for Viewers

6.2. Quick Start

The following figure illustrates the high-level process for setting up HaloCAD for Viewers.



Quick start installation steps for HaloCAD for Viewers

6.3. Prerequisites

Refer to the section “Prerequisites”.

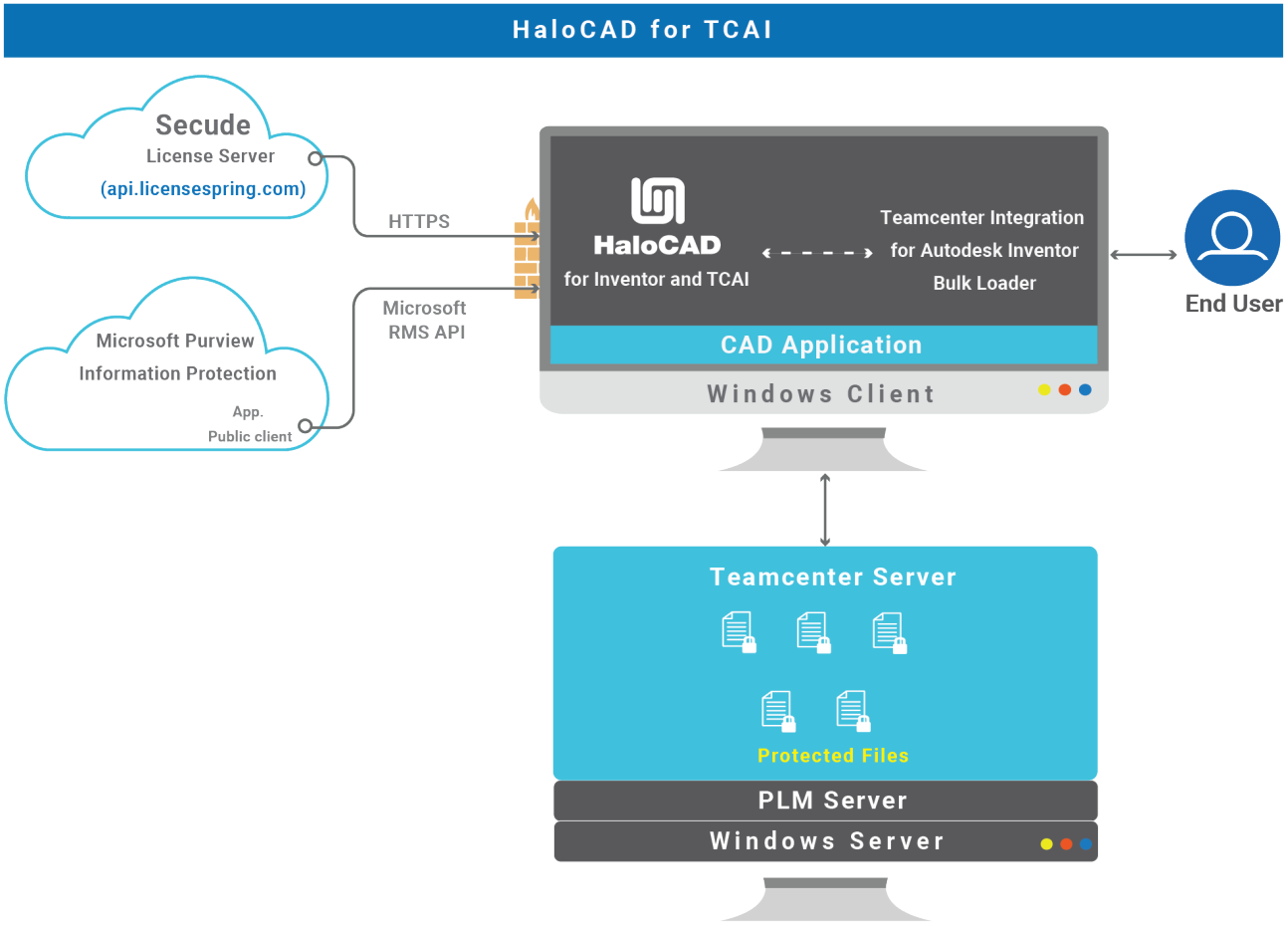
7. HaloCAD for TCAI

HaloCAD for TCAI uses Microsoft Purview Information Protection to decrypt HaloCAD-protected CAD files during bulk loading operations in Teamcenter Integration for Autodesk Inventor (TCAI). This enables the TCAI Bulk Loader to scan and process protected Inventor files before importing them into Teamcenter.

7.1. Architecture

The Teamcenter Integration for Autodesk Inventor Bulk Loader imports Inventor files into Teamcenter. However, the Bulk Loader cannot recognize or process protected (encrypted) Inventor files directly. HaloCAD for TCAI decrypts protected Inventor files before they are processed by the Bulk Loader. This enables the Bulk Loader to scan and import the files into Teamcenter.

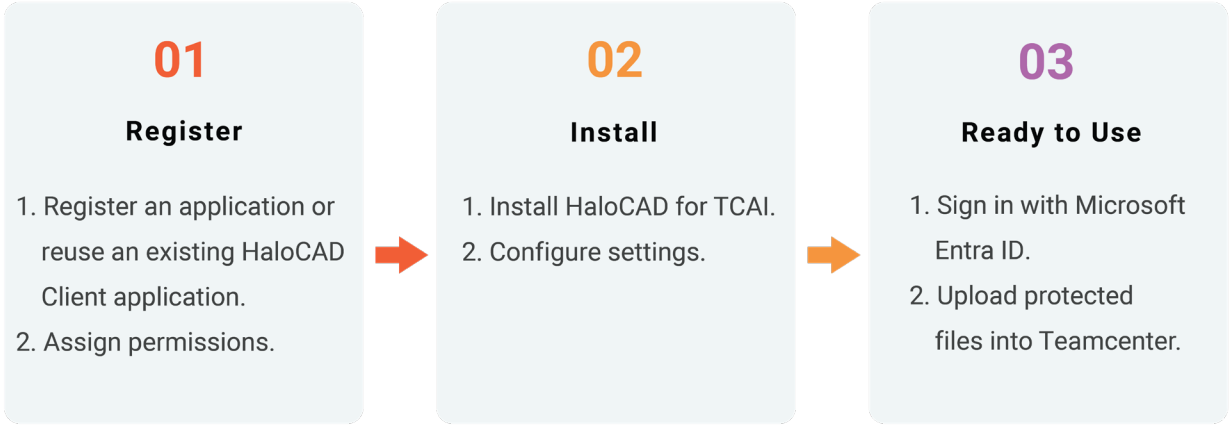
HaloCAD for TCAI uses the same decryption mechanism as HaloCAD for Viewers and is designed specifically to support bulk loading operations in the TCAI environment. The following figure illustrates the high-level architecture of HaloCAD for TCAI.



HaloCAD for TCAI

7.2. Quick Start

The following figure illustrates the high-level process for setting up HaloCAD for TCAI.



Quick start installation steps for HaloCAD for TCAI

7.3. Prerequisites

Refer to the section “Prerequisites”.

8. Prerequisites

This chapter describes the prerequisites for installing and configuring HaloCAD components.

Product	Application Type		License Required
	Public Client	Web	
HaloCAD Add-on for CAD	✓	✗	✓
HaloCAD for Viewers	✓	✗	✗
HaloCAD for TCAI	✓	✗	✗
HaloCAD for Teamcenter	✗	✓	✗
HaloCAD for Windchill	✗	✓	✗
HaloCAD for Autodesk Vault	✗	✓	✗
HaloCAD for SOLIDWORKS PDM	✓	✗	✗
HaloENGINE GenNXT	✗	✓	✓

Prerequisites by Product

8.1. Register an Application in Microsoft Entra ID - Public client/native

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

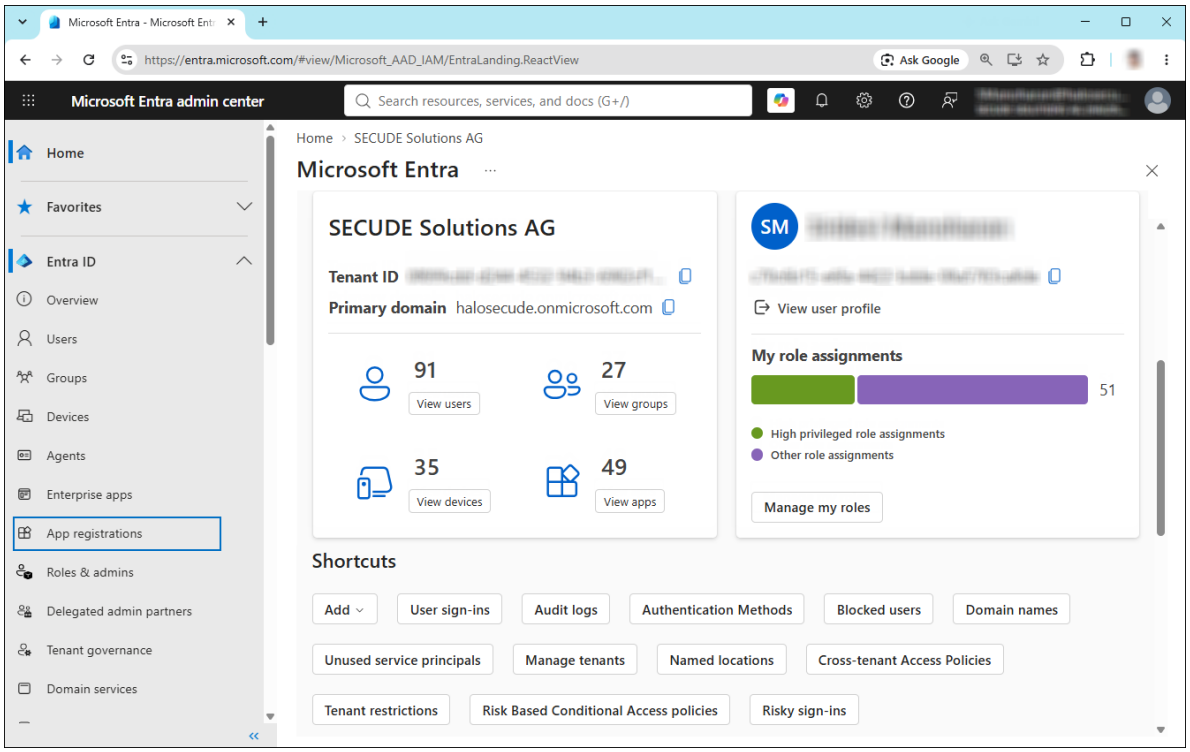
Registering an application in Microsoft Entra ID establishes a trust connection between your application and the identity provider, the Microsoft identity platform. Microsoft documentation takes precedence over this section. Refer to the latest Microsoft documentation for updates.

8.1.1. Create an Application

Follow the instructions below to register an application:

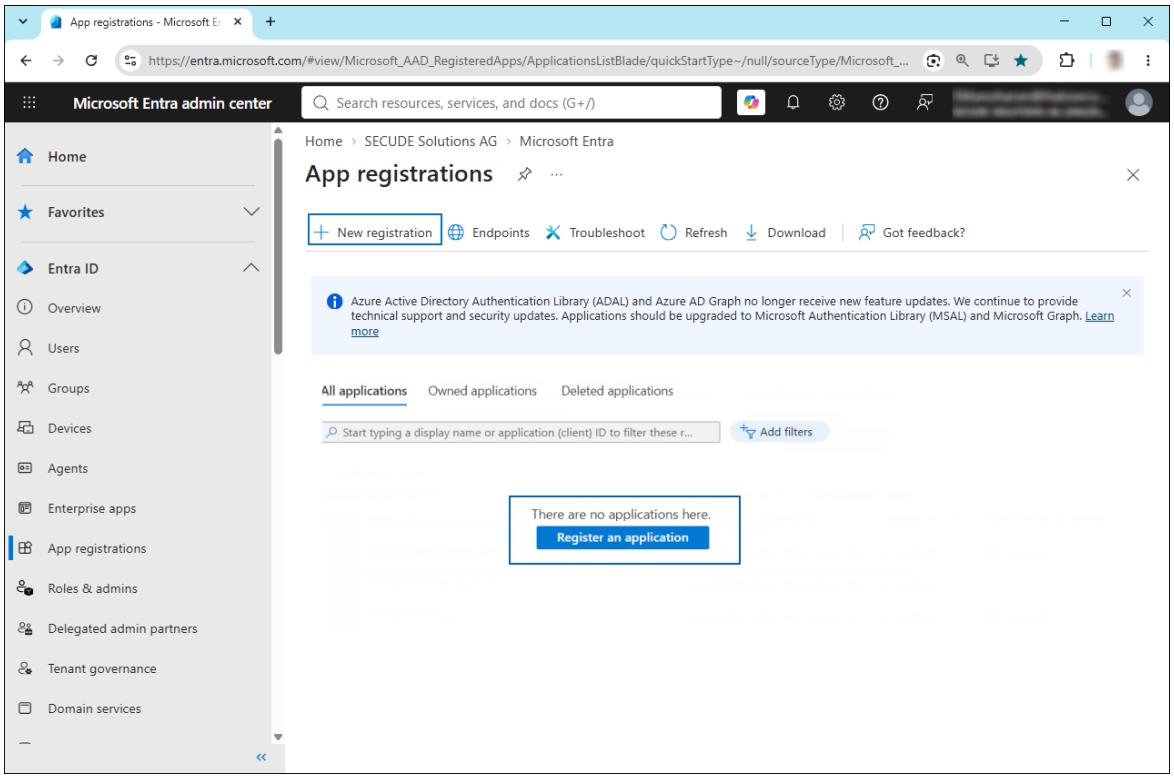
1. Log in to the Microsoft Entra admin center using an account that has administrator privileges.
2. If you have access to multiple tenants, click the **Settings** icon in the top menu. From **Directories + subscriptions**, select the tenant in which you want to register the application.

3. The application homepage opens.



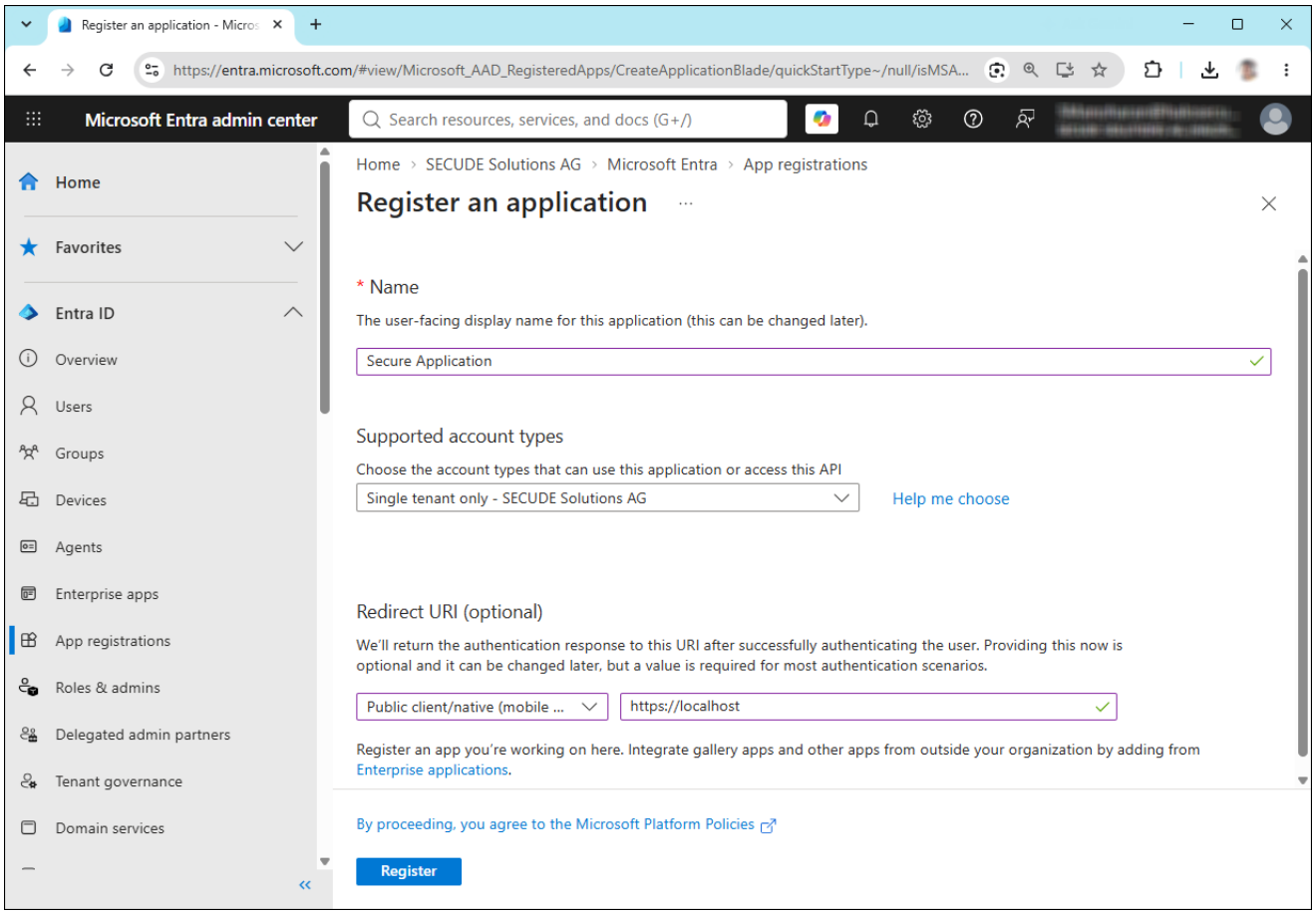
Selecting Microsoft Entra ID

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.



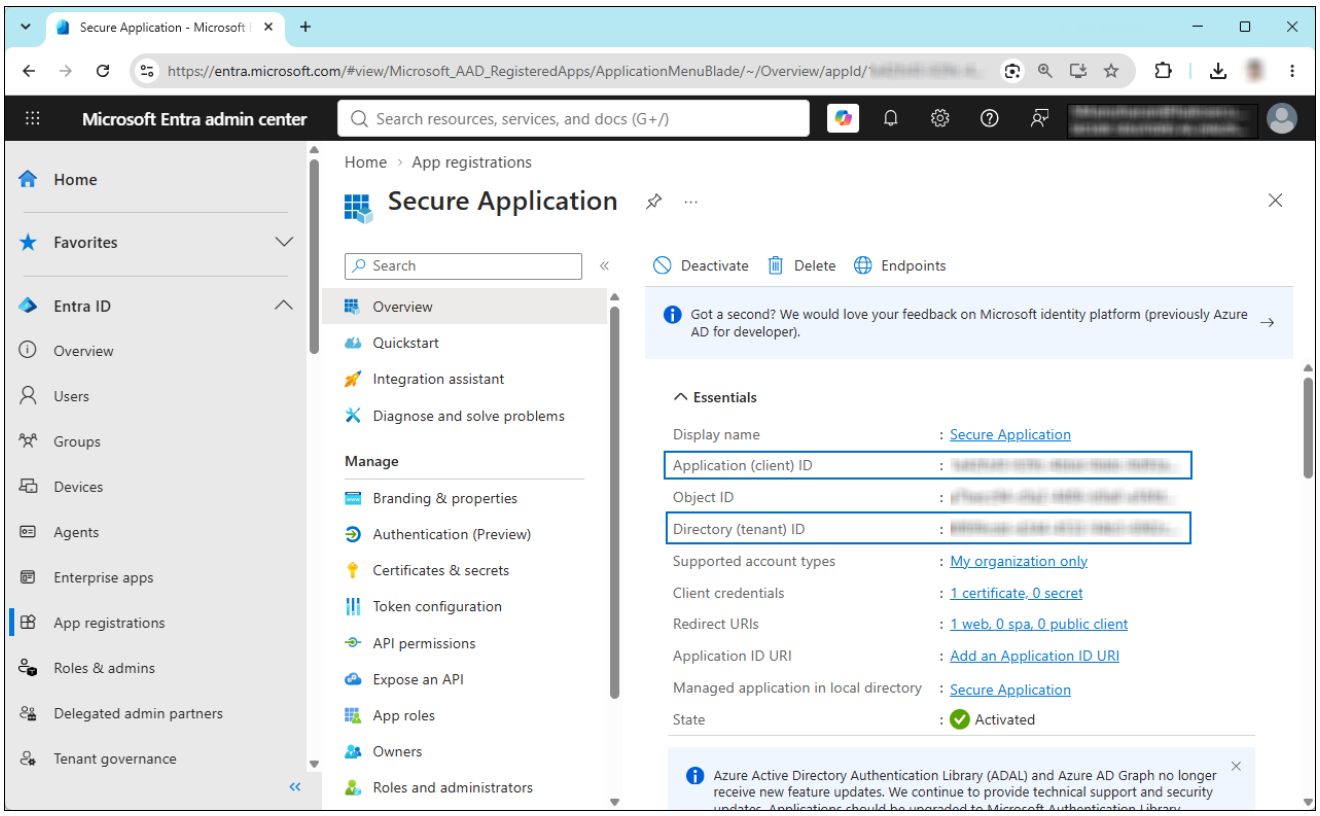
New application registration

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



Application details

7. **Name:** Enter an appropriate name for the application.
8. **Supported account types:** Select which account you would like your application to support. For detailed information on these types, please see Microsoft documentation.
   a. **Single tenant only – <your tenant>**: For users or guests in your tenant.
   b. **Multiple Entra ID tenants**: For users from any Microsoft Entra tenant.
   c. **Any Entra ID Tenant + Personal Microsoft accounts**: For users from any Entra tenant and personal Microsoft accounts.
   d. **Personal accounts only**: For personal Microsoft accounts only.
   e. **Redirect URI:** Select **Public client/native (mobile & desktop)**, and enter a valid redirect URI. For example, `https://localhost`.
9. Click **Register**.
10. The Overview page of the newly registered application opens.



Application ID and Tenant ID

11. 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** – also known as **Client ID**.
    b. **Directory ID** – also known as **Tenant ID**.

Save the authentication parameters

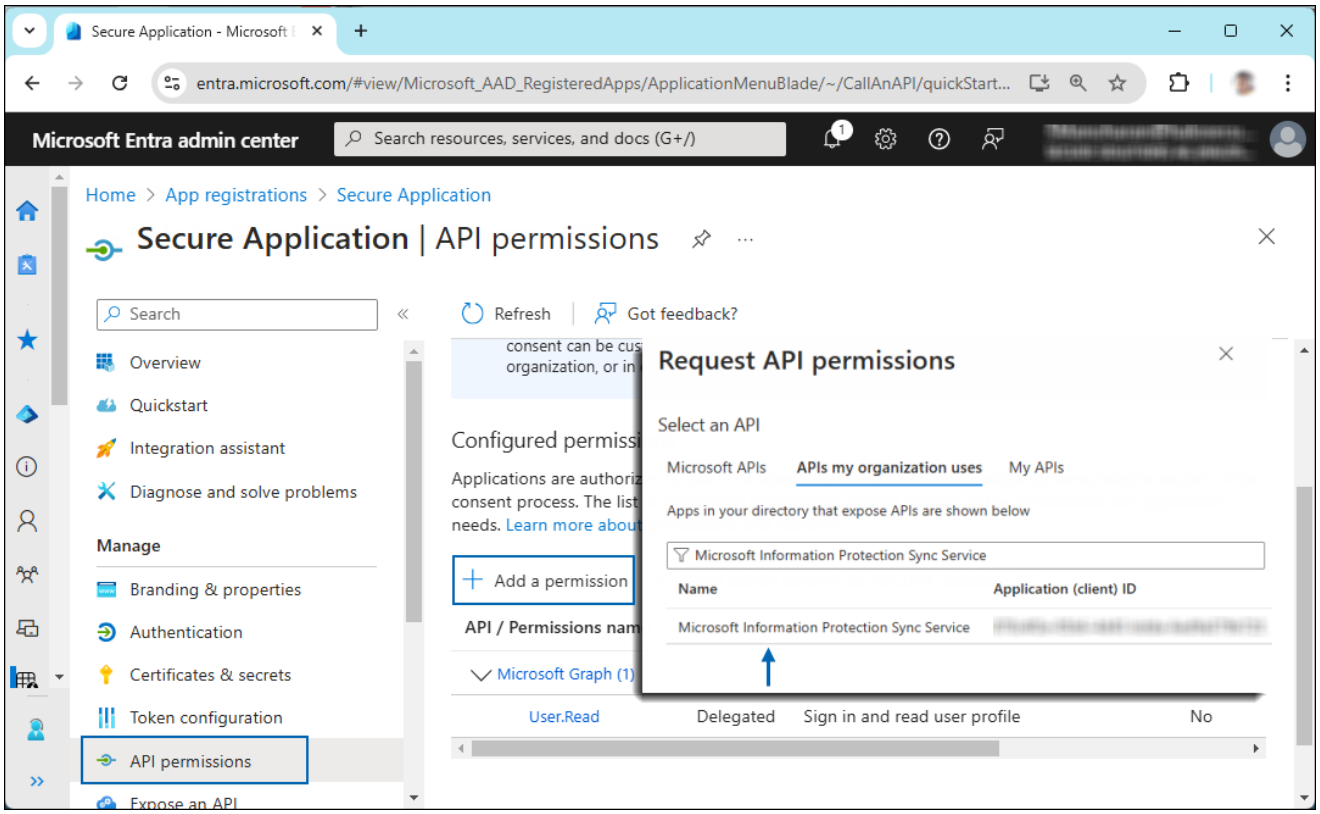
Open a text editor (such as Notepad) and copy the values for the Application (client) ID, Directory (tenant) ID, and Redirect URI. Save these details for initializing the HaloCAD Add-on. Note that the Directory (tenant) ID is required only for single-tenant applications.

8.1.2. Add Required Permissions

To protect content using the MIP SDK, you need to provide the following API permission(s) for the created application ID.

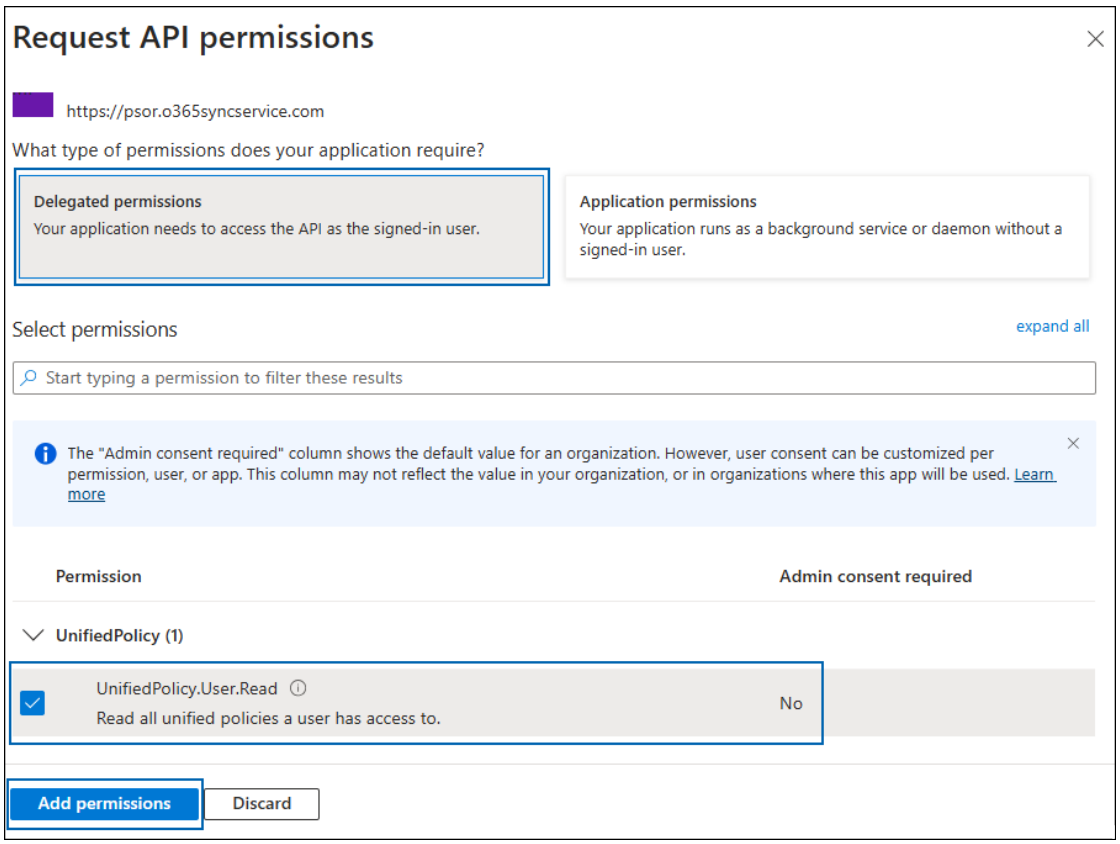
1. In the left navigation pane of the application, select **API permissions**.
2. Click **Add a permission**. The **Request API permissions** page appears.
3. Under the **Select an API** setting, select APIs my organization uses. A list appears, containing the applications in your directory that expose APIs.

4. Type in the search box or scroll to find the required API that is mentioned in the table below, “Required Permissions”.
5. For example, type **Microsoft Information Protection Sync Service**. You can see the API listed as shown in the figure below:



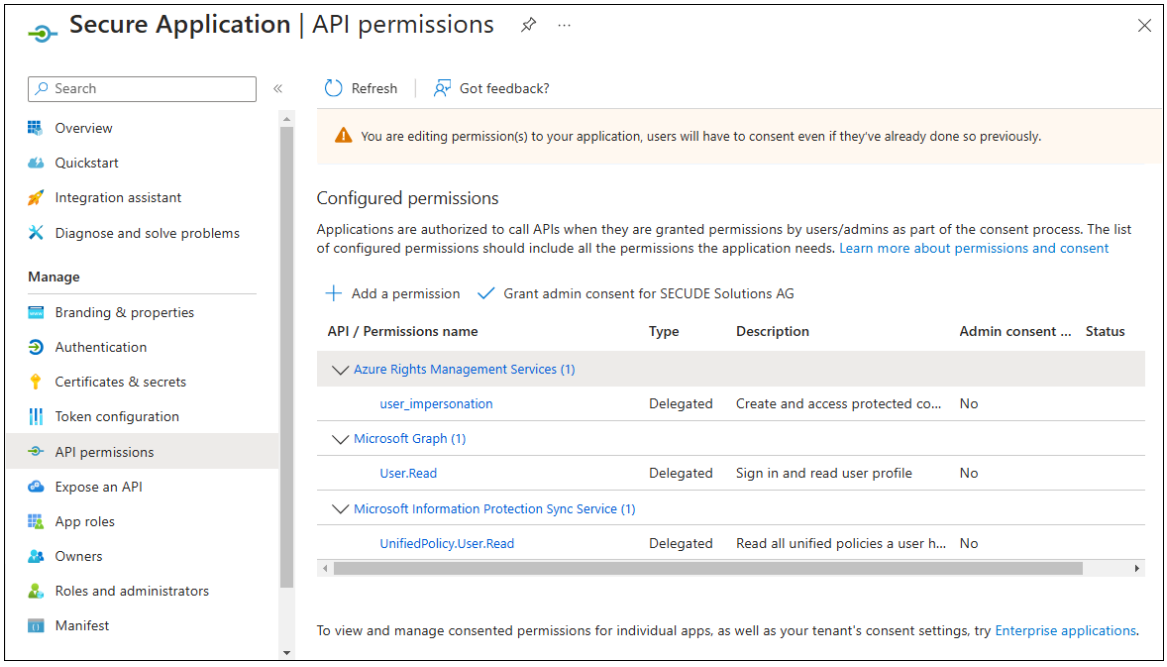
Searching for permissions

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



Adding permission

8. Click **Add permissions**. Repeat the steps outlined above to add the other required permissions listed in the table below.
9. The **API permissions page** opens, and the added permissions appear in the table. Administrator consent is not required for **Delegated Permissions**.



API Required permissions

10. The following table lists the required permissions.

API / Permission name	Display Name	Type	Description
Azure Rights Management Services (Microsoft Rights Management Services)	`User_impersonation`	Delegated	Create and access protected content for users
Microsoft Graph	`User.Read`	Delegated	Sign in and read user profile (added by default)
Microsoft Information Protection Sync Service	`UnifiedPolicy.User.Read`	Delegated	Read all unified policies a user has access to.

Required permissions

8.2. Register an Application in Microsoft Entra ID - Web

Creating an application in Microsoft Entra ID is similar to the steps in the previous section. However, for HaloCAD for PLM, some variations apply.

1. Under **Redirect URI**, select **Web**.
2. Add the permissions listed in the following table.
3. Click **Grant admin consent for your** *<company>*.
4. When the confirmation dialog appears, select **Yes** to approve.
5. After the consent is granted, the **Status** column changes to **Granted**.

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

API / Permission Name	Display Name	Type	Description
Microsoft Information Protection Sync Service	`UnifiedPolicy.Tenant.Read`	Application	Read all unified policies of the tenant

Required permissions #1

8.2.1. 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 in this tenant.

Required permissions #2

8.2.2. 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.

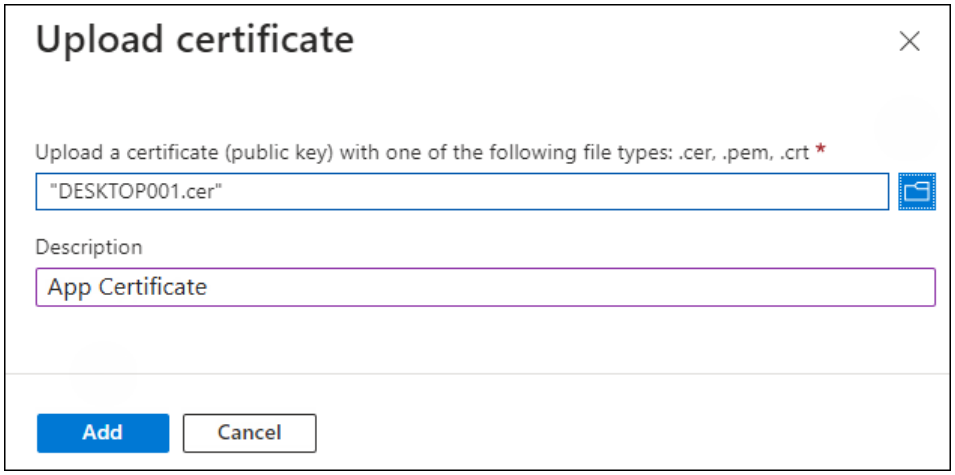
Prerequisites:

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.

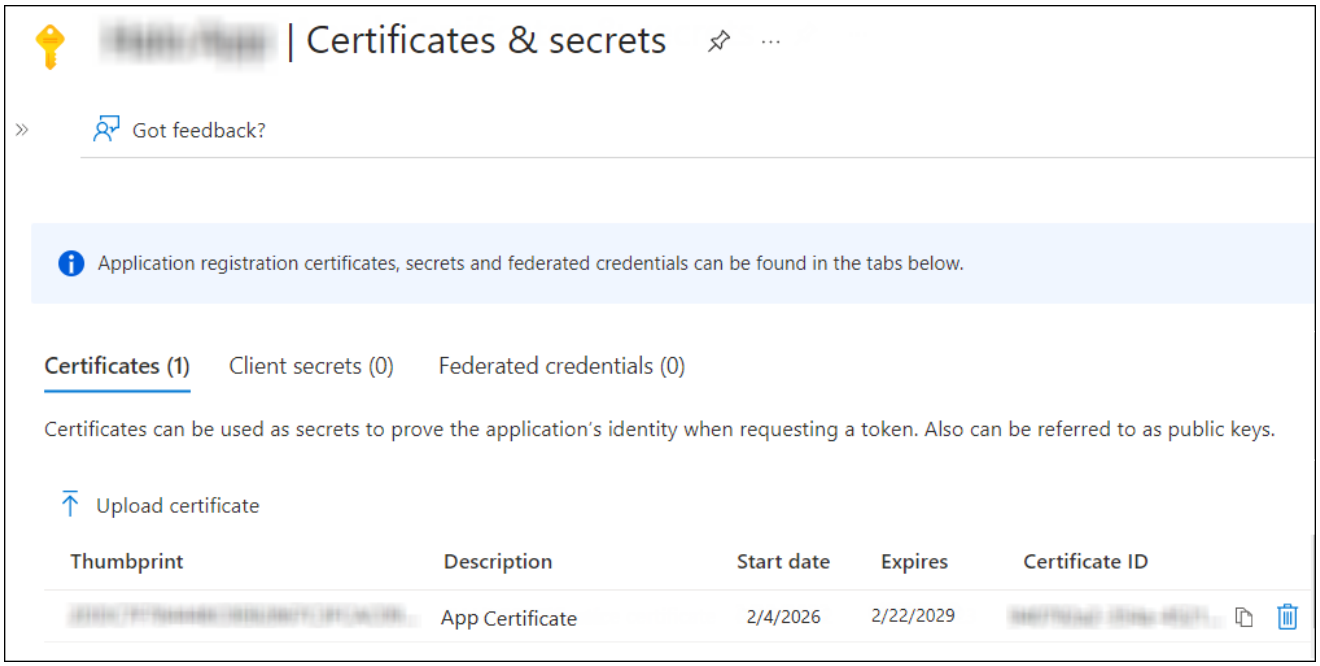
To upload the certificate, follow these steps:

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

The following table lists the Microsoft Entra ID application types that must be registered when using HaloCAD Add-on for CAD, HaloCAD for Viewers, HaloENGINE GenNXT, or HaloCAD for PLM.

Configuration Guidelines

- When HaloCAD for SOLIDWORKS PDM is integrated with HaloENGINE GenNXT, use the same Directory (Tenant) ID.
- When HaloCAD for PLM is integrated with HaloENGINE GenNXT, both components can use the same Web application details.
- HaloCAD for Viewers can use a new or existing HaloCAD application. Ensure that the client type is configured as Public Client (Mobile & Desktop).
- HaloCAD for TCAI can use a new or existing HaloCAD application. Ensure that the client type is configured as Public Client (Mobile & Desktop).

8.3. Create and Configure the Sensitivity Labels

Applicable to	1. HaloCAD Add-on for CAD 2. HaloCAD for PLM/PDM (Teamcenter, Windchill, Vault, and SOLIDWORKS PDM)

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, see the Microsoft documentation.

8.4. Office 365 Subscription Details

Applicable to	1. HaloCAD Add-on for CAD 2. HaloCAD for Viewers 3. HaloCAD for TCAI 4. HaloCAD for PLM/PDM (Teamcenter, Windchill, Vault, and SOLIDWORKS PDM)

1. Fully configured Microsoft Purview Information Protection.
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. Please refer to the section “Enable Support for TLS 1.2 at the Client Workstation for Microsoft Entra ID”.

5. To use the **Revoke Access** feature, the user must be assigned an **Azure Information Protection Premium P1 or P2** license. This license is not required for the **Viewer Add-on**.
6. Monitor logging: Your subscription must include Log Analytics on the same tenant as Microsoft Entra ID.

8.5. Recommended URLs, Addresses, and Ports for MPIP

Applicable to	1. HaloCAD Add-on for CAD 2. HaloCAD for Viewers 3. HaloCAD for TCAI 4. HaloCAD for PLM/PDM (Teamcenter, Windchill, Vault, and SOLIDWORKS PDM)

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

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

Addresses	Ports
Microsoft Entra ID (global service) For details on Microsoft Entra ID endpoints, please 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.

8.6. Secude License Manager for HaloCAD

Applicable to	HaloCAD Add-on for CAD

To communicate with Secude License Manager for HaloCAD, the following URL and port must be whitelisted in the customer's proxy:

Address	**Port**
License API - api.licensespring.com	TCP 443

Recommended license manager endpoint

8.7. Enable TLS 1.2 for Microsoft Entra ID Authentication

Applicable to	1. HaloCAD Add-on for CAD 2. HaloCAD for Viewers 3. HaloCAD for TCAI 4. HaloCAD for PLM/PDM (Teamcenter, Windchill, Vault, and SOLIDWORKS PDM)

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

9. License Administration

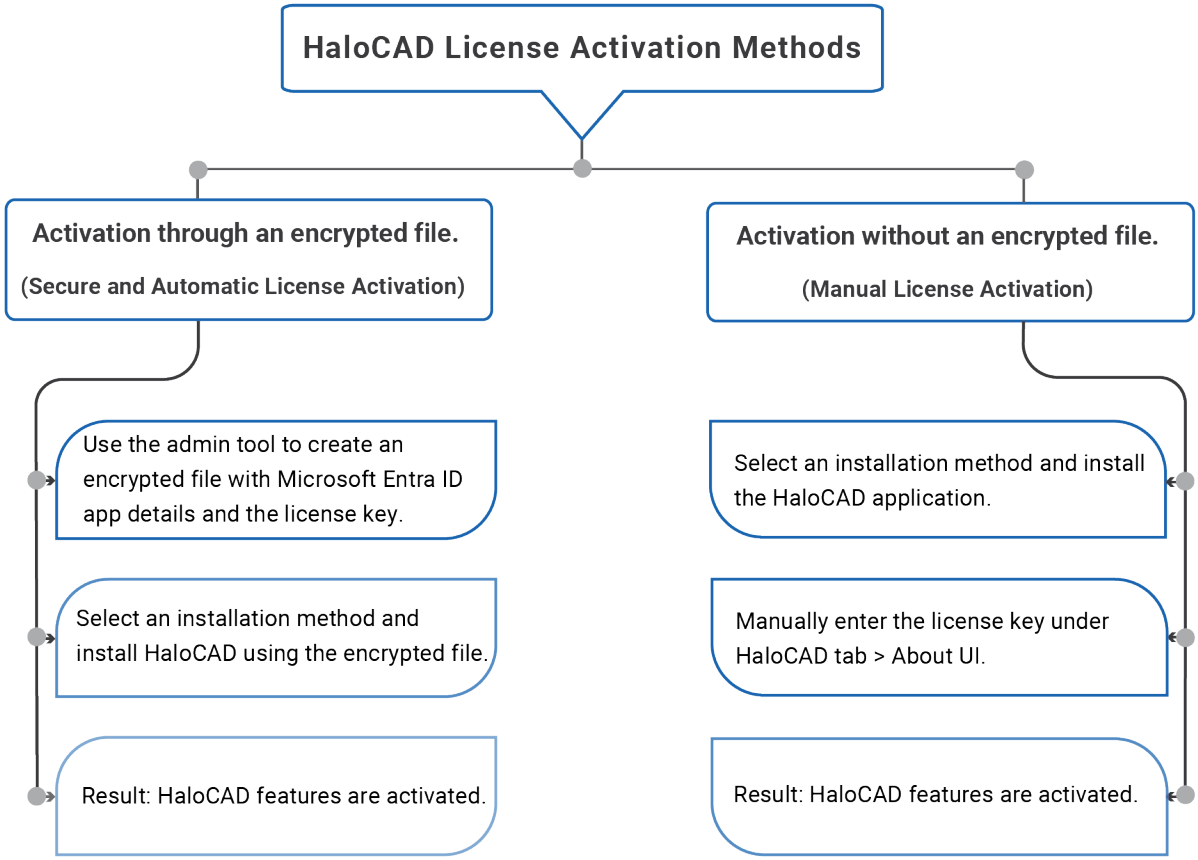
Applicable to	HaloCAD Add-on for CAD

HaloCAD uses license keys to enable product features. Obtain a valid license key from **Secude Support** before installing HaloCAD. For information about purchasing or renewing licenses, contact your Secude representative.

HaloCAD supports the following license activation methods:

1. **Secure Installation (Recommended)**: Uses an encrypted configuration file (`hc.conf.enc`) that contains the license key and Microsoft Entra ID application details. During installation, HaloCAD automatically initializes the application and activates the license. For more information, refer to the "Secure Installation" section.
2. **UI-based manual license activation**: Allows administrators to activate the license manually after installation by entering the license key through the HaloCAD user interface. For more information, refer to the "UI-based Manual License Activation" section.
3. **License Activation in Silent Mode:** Uses an encrypted configuration file to automatically initialize the application and activate the license during a silent installation. For more information, see the Installation Manual.
4. **License activation via Microsoft System Center Configuration Manager**: Uses an encrypted configuration file together with the installer to deploy and activate HaloCAD across multiple workstations. For more information, refer to the Installation Manual.

The following figure illustrates the license activation process.



License activation

9.1. Secure Installation (Recommended Method)

Applicable to	1. HaloCAD Add-on for CAD 2. HaloCAD for Viewers 3. HaloCAD for TCAI 4. HaloCAD for SOLIDWORKS PDM

To protect sensitive configuration information, HaloCAD supports secure installation by using an encrypted configuration file.

The HaloCAD Admin Utility encrypts the Microsoft Entra ID application details, cloud configuration, and license key into an encrypted configuration file (`hc.conf.enc`). During installation, HaloCAD automatically reads the configuration from the encrypted file, initializes the application, and activates the license without requiring users to enter the Microsoft Entra ID application details manually.

Administrators can securely distribute the encrypted configuration file without exposing tenant information or license details.

HaloCAD Admin Utility Tool

The HaloCAD installation package includes the `hc.admintool.exe` utility.

Prerequisites

Before running the utility, collect the following information:

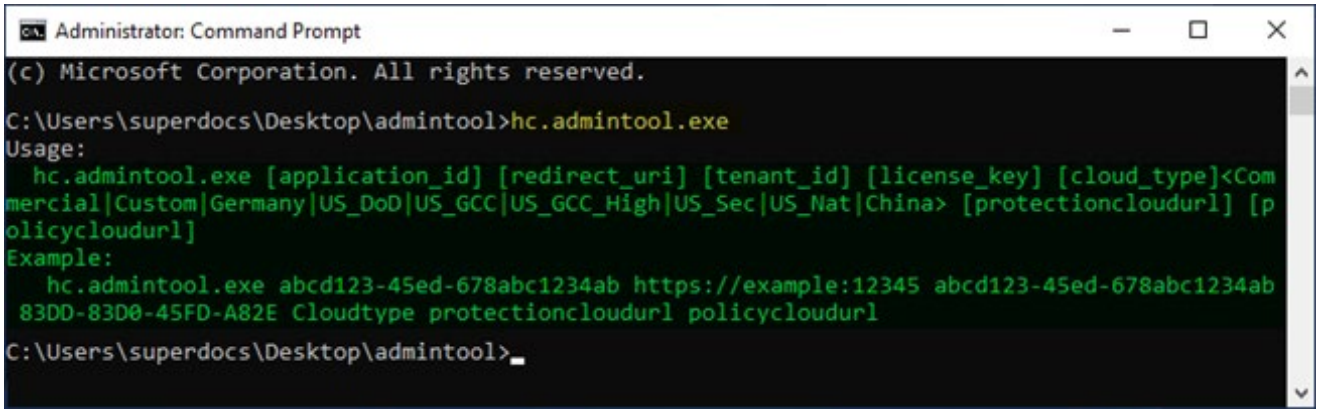
- Microsoft Entra ID application details
- Cloud type
- License key

Note

A license key is not required for HaloCAD for Viewers or HaloCAD for TCAI.

How to Encrypt the Configuration File

1. Copy the **admintool** folder from the installation package to a local directory. For example, `C:\Users\superdocs\Desktop\admintool`.
2. Open **Command Prompt** as an administrator (Run as Administrator).
3. Navigate to the directory of the **admintool** folder and type `hc.admintool.exe` and press **Enter**.



Admin tool with help command

4. Enter the required details. For example,

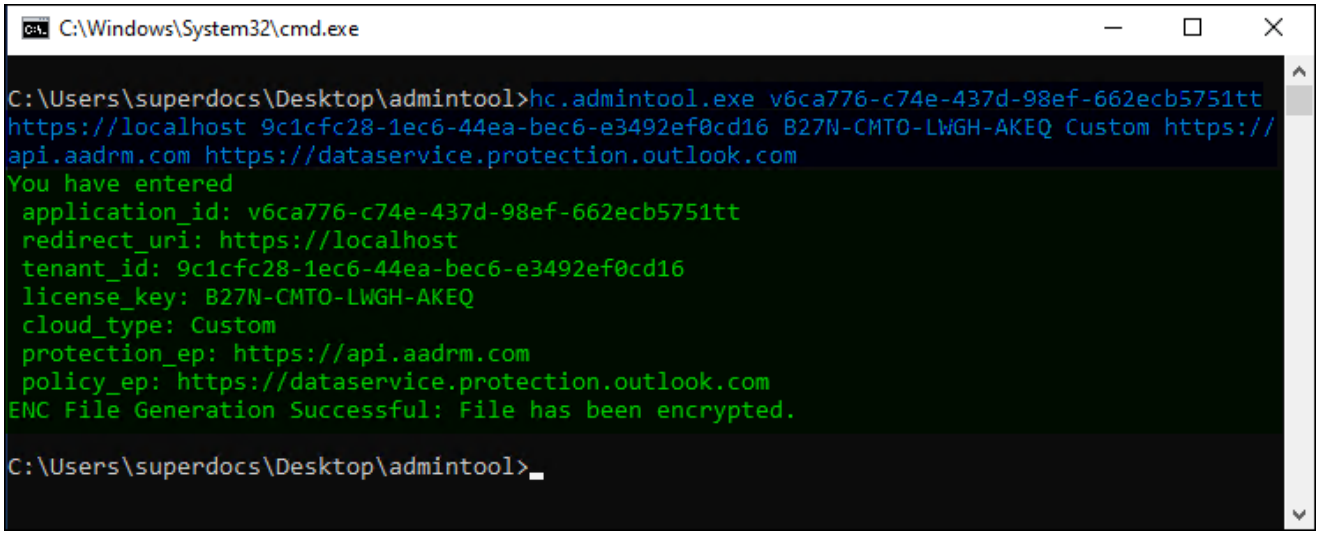
   Cloud type: Commercial - `hc.admintool.exe v6ca776-c74e-437d-98ef-662ecb5751tt https://localhost 9c1cfc28-1ec6-44ea-bec6-e3492ef0cd16 B27N-CMTO-LWGH-AKEQ Commercial`

   Cloud type: US_DoD - `hc.admintool.exe v6ca776-c74e-437d-98ef-662ecb5751tt https://localhost 9c1cfc28-1ec6-44ea-bec6-e3492ef0cd16 B27N-CMTO-LWGH-AKEQ US_DoD`

   Cloud type: Custom - `hc.admintool.exe v6ca776-c74e-437d-98ef-662ecb5751tt`

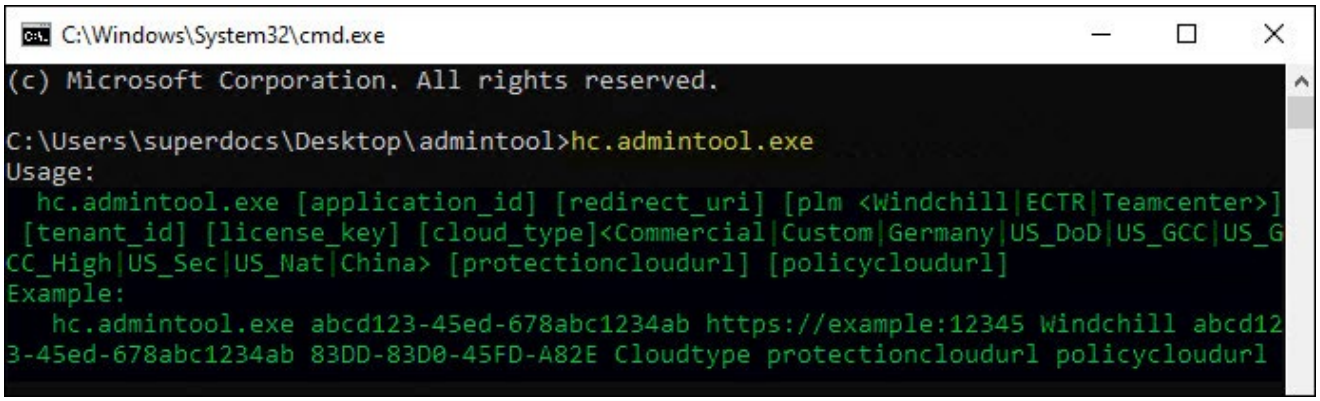
```
https://localhost 9c1cfc28-1ec6-44ea-bec6-e3492ef0cd16 B27N-CMTO-LWGH-AKEQ Custom
https://api.aadrm.com https://dataservice.protection.outlook.com
```

5. The output window appears as follows:

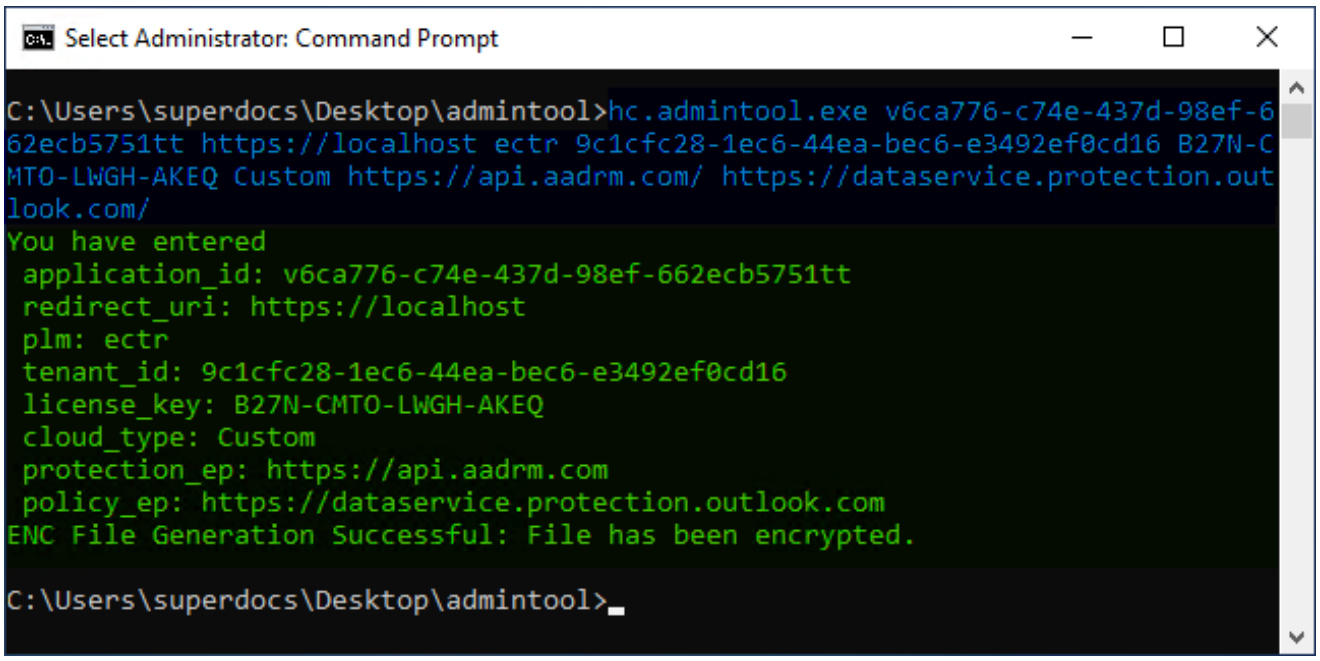


Admin tool displaying the output

6. **HaloCAD add-on for Creo**: The following help commands are specific to the HaloCAD add-on for Creo.

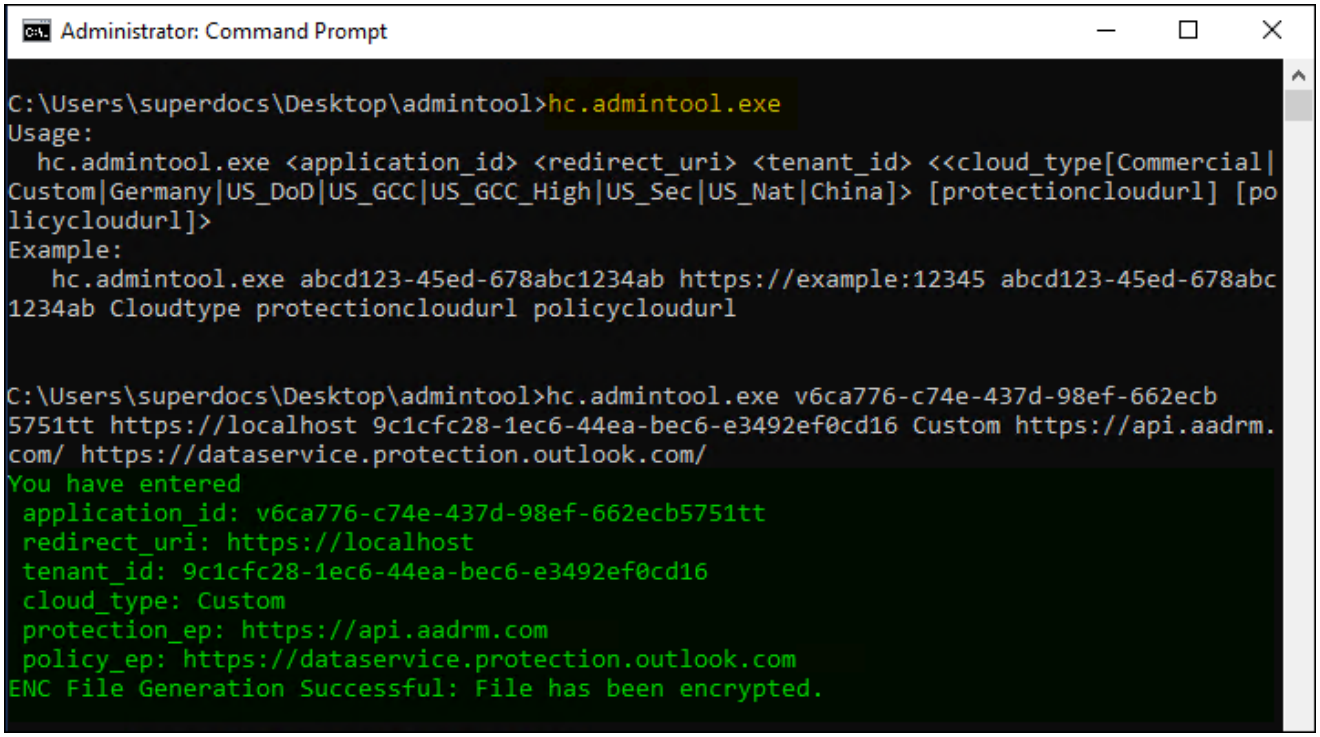


Admin tool with help command for Creo add-on



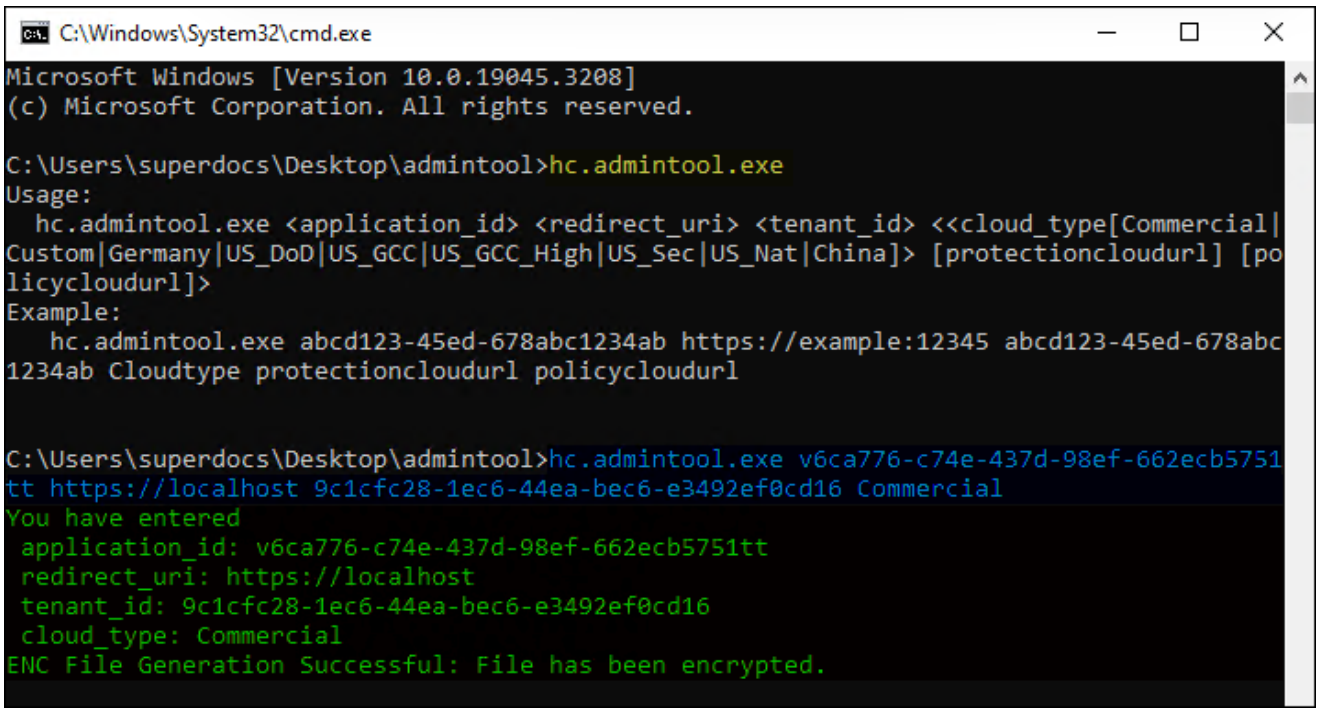
Admin tool displaying the output with ECTR integration (only for Creo add-on)

7. **HaloCAD for SOLIDWORKS PDM**: The following help commands are specific to HaloCAD for SOLIDWORKS PDM.



Admin tool displaying the output for SOLIDWORKS PDM

8. **HaloCAD for Viewers and TCAI**: The following help commands are specific to HaloCAD for Viewers and TCAI.



Admin tool displaying the output for Viewers and TCAI

Result:

- The utility replaces `hc.conf.json` with the encrypted `hc.conf.enc` file.
- Distribute `hc.conf.enc` with the HaloCAD installation package.
- Always use the version of `hc.admintool.exe` included with the current installation package. Configuration files created with earlier releases are not supported.

Next steps

1. Copy `hc.conf.enc` to the same directory as the HaloCAD installer.
2. Run the installer.
3. Complete the installation by following the **Installation Manual**.

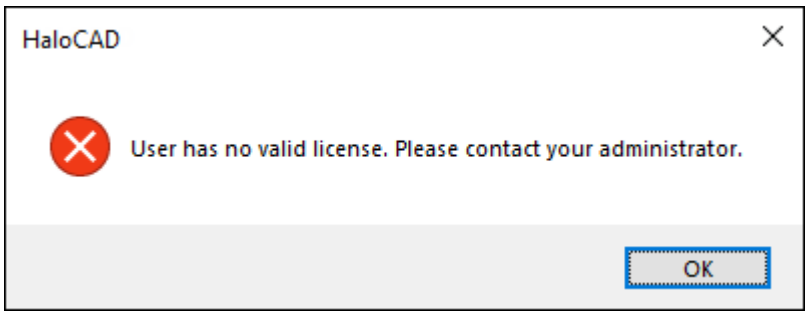
9.2. UI-based Manual License Activation

Applicable to	HaloCAD Add-on for CAD

This section explains how to activate a HaloCAD license using the user interface. If you experience problems activating the license, refer to the Troubleshooting chapter in the Operations Manual.

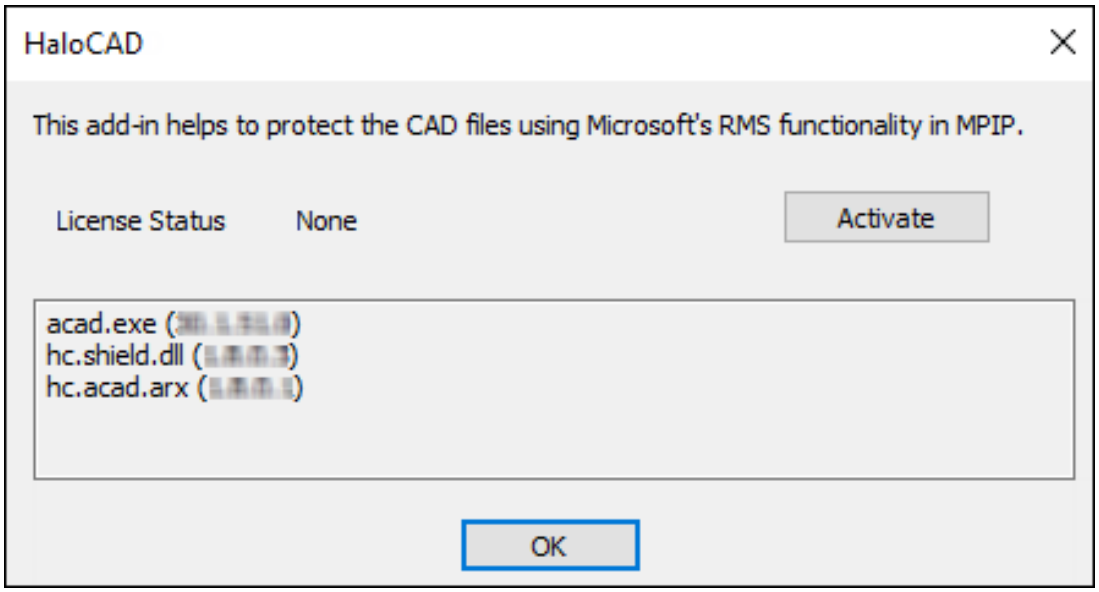
Prerequisite: Ensure that HaloCAD is installed.

1. Open the CAD application for which the add-on was purchased.
2. When the license warning message appears, click **OK**.



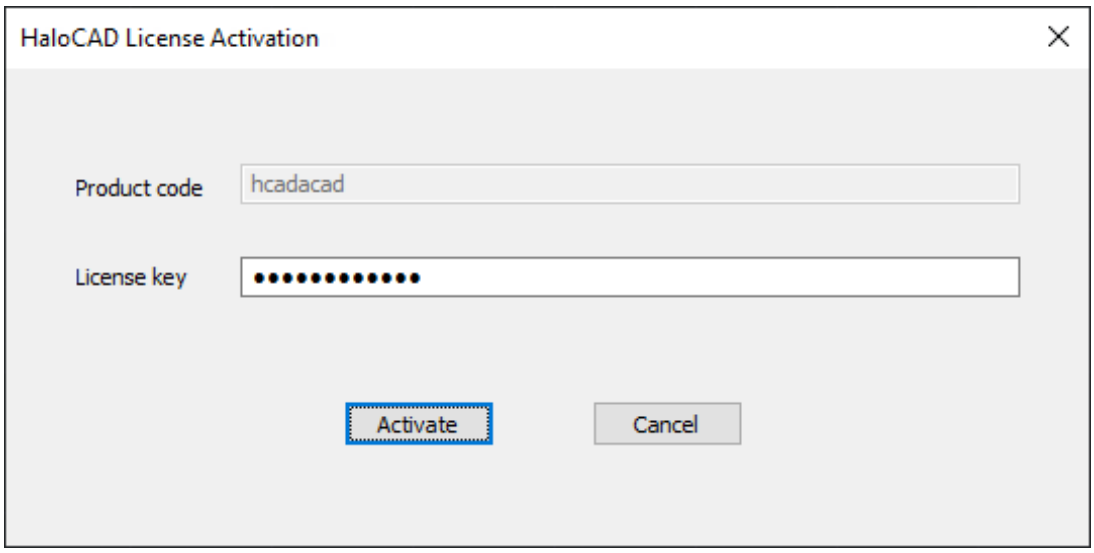
HaloCAD license warning message

3. On the **HaloCAD** tab, click **About**.
4. Verify that the license status is **None**.



License Status: None

5. Click **Activate**.
6. The *HaloCAD License Activation* screen appears:

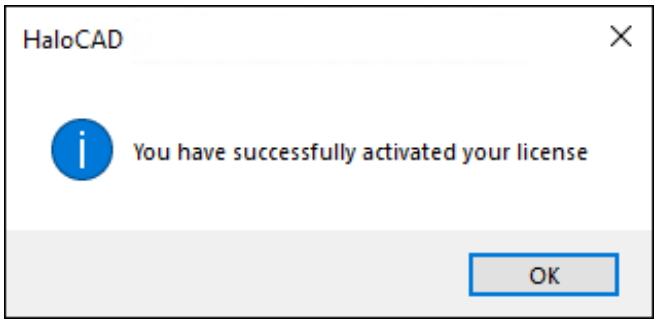


HaloCAD activation screen

7. Enter the license key provided by Secude.
8. Click **Activate**.

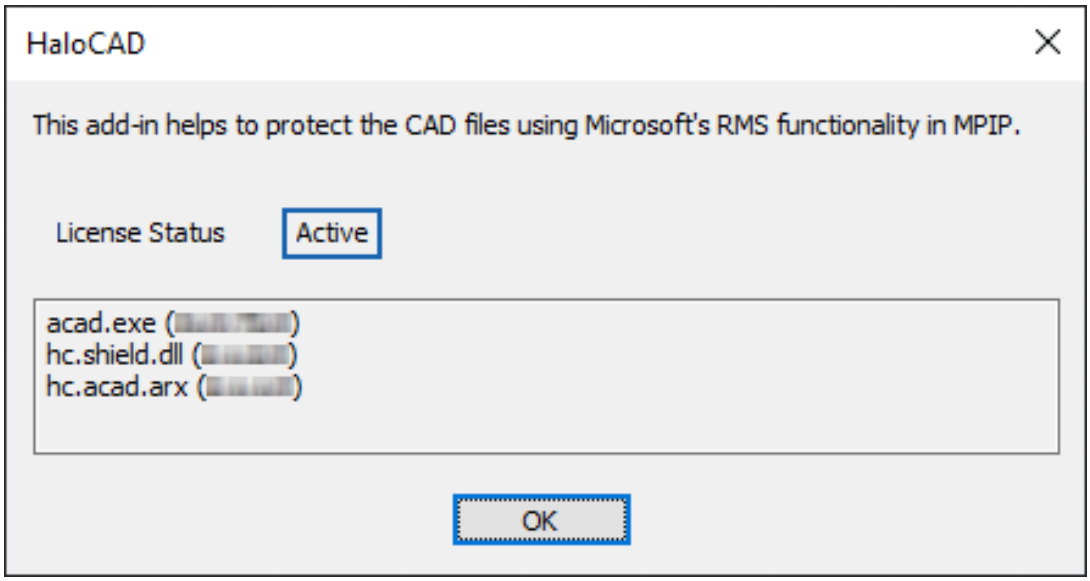
Result:

- The following confirmation message appears:



Activation success message

- Click **OK**.
- The license status changes to **Active**.



License Status: Active

Related tasks:

- If you click the pencil icon (**Click to change label**) to label the file, the Rights Management Service prompts you to sign in. Click **OK**, and then enter your credentials.
- After successful authentication, the labels can be retrieved from Microsoft Purview Information Protection, and the HaloCAD Ribbon is activated. For more details, please refer to the Operations Manual.

9.3. License Renewal After Expiration

Applicable to	HaloCAD Add-on for CAD

HaloCAD licenses are valid until the specified expiration date. After a license expires, HaloCAD displays a warning message when the CAD application starts. To continue using HaloCAD, obtain and activate a new license key.

Prerequisite: Before reactivating the license, obtain a new license key from Secude.

Option 1: Automatic Activation Using the Admin Tool

1. Run the admin tool with the new license key, as explained in the section "How to Encrypt the Configuration File".
2. Navigate to the configuration directory containing the old `hc.conf.enc` file and replace it with the one created in the previous step.
3. Restart the application.

Result:

- The HaloCAD license key is now automatically activated.
- You can start protecting CAD files.

Option 2: Manual Activation Using the About Dialog

1. Open the CAD application.
2. Go to the **HaloCAD** tab and click **About**.
3. Click **Activate**.
4. Enter the new key that Secude has provided.

Result:

- The HaloCAD license key is now manually activated.
- You can start protecting CAD files.

10. Appendix

Third-Party Libraries

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

Applicable to	HaloCAD Add-on for CAD

The third-party libraries and dependencies used by the HaloCAD Add-on for CAD are shown in the table below.

Library	**Version**	**Source Code**	**License Link**
Mhook	2.5.1	https://github.com/apriorit/mhook	https://github.com/apriorit/mhook#license
Protobuf Library	3.15.6	https://github.com/protocolbuffers/protobuf	https://github.com/protocolbuffers/protobuf/blob/master/LICENSE
OpenSSL	3.2	https://github.com/openssl	https://github.com/openssl/openssl/blob/master/LICENSE.txt
Rapidxml	1.13	https://sourceforge.net/projects/rapidxml/files/latest/download	http://rapidxml.sourceforge.net/license.txt
JSON Parser	3.11.3	https://github.com/nlohmann/json	https://github.com/nlohmann/json/blob/develop/LICENSE.MIT
MSAL	4.90.0	https://github.com/AzureAD/microsoft-authentication-library-for-dotnet	https://github.com/AzureAD/microsoft-authentication-library-for-dotnet/blob/master/LICENSE
ConfuserEx	1.0.0.0	https://github.com/yck1509/ConfuserEx	https://github.com/yck1509/ConfuserEx/blob/master/LICENSE
WTL	9.0.4140	https://www.nuget.org/packages/wtl/9.0.4140	https://opensource.org/licenses/cpl1.0.txt

Library	Version	Source Code	License Link
MIP SDK	1.18.124 Creo and Designcenter: 1.16.126	https://learn.microsoft.com/en-us/information-protection/develop/version-release-history	https://docs.microsoft.com/en-us/information-protection/develop/
Licensespring	8.9.0	-	-

Third-party libraries

The third-party libraries used by HaloCAD for Viewers, HaloCAD for TCAI, HaloENGINE GenNXT, HaloCAD for Teamcenter, HaloCAD for Windchill, HaloCAD for Autodesk Vault, and HaloCAD for SOLIDWORKS PDM are documented in their respective Installation Manuals.

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.