



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. Features	2
2. QUICK START INSTALLATION SUMMARY - STANDALONE HALOCAD ADD-ON	3
3. QUICK START INSTALLATION SUMMARY - INTEGRATED WITH PLM/PDM	6
4. QUICK START INSTALLATION SUMMARY - HALOCAD FOR VIEWERS	8
5. HALOCAD ARCHITECTURE	10
5.1. HaloCAD Add-on for CAD	10
5.2. HaloCAD Reader Add-on for CAD	11
5.3. HaloCAD for PLM.....	11
5.4. HaloCAD for Viewers.....	15
5.5. HaloCAD for TCAI	15
6. PREREQUISITES	17
6.1. Register an Application in Microsoft Entra ID - Public client/native.....	17
6.1.1. Create an Application	17
6.1.2. Add Required Permissions	20
6.2. Register an Application in Microsoft Entra ID - Web	24
6.2.1. Additional Permission (Only for Decryption).....	24
6.2.2. Upload the Certificate in the Azure Portal	25
6.3. Create and Configure the Sensitivity Labels	28
6.4. Office 365 Subscription Details	28
6.5. Recommended URLs, Addresses, and Ports for MPIP.....	29
6.6. Enable Support for TLS 1.2 at the Client Workstation for Microsoft Entra ID.....	30
7. LICENSE ADMINISTRATION	32
7.1. Secure Installation (Recommended).....	33
7.2. UI-based Manual License Activation	37
7.3. License Expiration	39
8. 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.

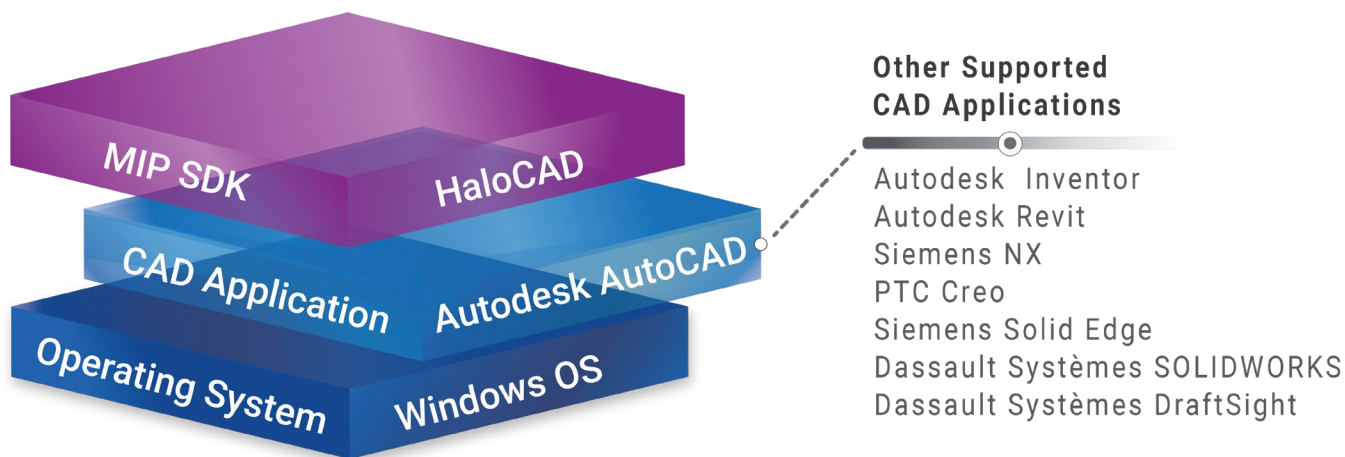
Convention	Description
Boldface type	<ul style="list-style-type: none">• Items you must select, such as menu options, command buttons, or items in a list.• Titles of sections, sub-sections, etc.
<i>Italic type</i>	<ul style="list-style-type: none">• To emphasize a word• Error messages• Table and Figure captions
Consolas Font	<ul style="list-style-type: none">• Package names• Filenames and directory names• XML element names and attribute names• Parameters• File type• Code examples <p>Example:</p> <pre>hesadm.exe start -user <domain\user> -pwd <password></pre>
Hyperlink	Provides quick and easy access to cross-referenced topics. Hyperlinks are highlighted in blue and underlined.
Admonitions	<div data-bbox="416 1171 1394 1279" style="border: 1px solid yellow; padding: 5px;"><p>Note Provides additional information relevant to the topic.</p></div> <div data-bbox="416 1335 1394 1518" style="border: 1px solid red; padding: 5px;"><p>Warning Contains information about circumstances, parameters, and so on that MUST be fulfilled. Failure to comply will have consequences for the current operation.</p></div> <div data-bbox="416 1574 1394 1682" style="border: 1px solid green; padding: 5px;"><p>Tip Contains useful information about the operation of the application.</p></div> <div data-bbox="416 1738 1394 1883" style="border: 1px solid blue; padding: 5px;"><p>Info Contains information, guidelines, or suggestions for performing tasks more effectively.</p></div>

1. Introduction

Companies across industries, such as automotive, aviation, and high tech, create and manage their intellectual property (IP) based on drawings. These drawings are created digitally using computer-aided design (CAD) applications and are shared with users outside the organization owing to business considerations. It's essential to understand the potential risks associated with sharing business information. Comprehensive security measures are essential to reducing risks and safeguarding sensitive data. HaloCAD, a purpose-built data protection solution, is designed to help organizations achieve this objective effectively.

1.1. How does HaloCAD protect your Data?

HaloCAD effortlessly integrates Microsoft Purview Information Protection (MPIP), formerly known as Microsoft Information Protection (MIP), the leading technology for Enterprise Digital Rights Management (EDRM). It acts as a shield for your CAD files by automatically labeling them with MPIP and manages data assets across your environment. HaloCAD modules can be used either in standalone mode or in combination with HaloCAD for PLM, which automatically protects file downloads, decrypts files during upload, and returns them to the PLM vault.



HaloCAD Add-on for CAD applications

1.2. About this Manual

This manual provides administrators with the information required to successfully deploy HaloCAD components. It explains how to set up the HaloCAD environment, describes the overall architecture, lists the prerequisites and system requirements for each component, and offers step-by-step guidance for installation and configuration. The manual covers the HaloCAD Add-on for CAD, the HaloCAD Reader Add-on for CAD, HaloCAD for Viewers, HaloCAD for TCAI, and HaloCAD for PLM and PDM, along with detailed explanations to ensure smooth implementation and usage.

The term **HaloCAD Add-on for CAD** is a generic reference to the supported CAD applications, namely AutoCAD, Inventor, Revit, Creo, Solid Edge, NX, SOLIDWORKS, and DraftSight. Throughout this manual, any reference to this term denotes these supported CAD applications. Additionally, the HaloCAD Add-on for CAD includes a corresponding reader add-on for each of the above-listed applications, which is collectively referred to by the generic term **HaloCAD Reader Add-on for CAD**.

The term **HaloCAD for PLM** is a general reference to the supported PLM applications, namely Teamcenter, Windchill, and Autodesk Vault. Wherever this term appears in the manual, it denotes these supported PLM systems. Similarly, references to **HaloCAD for PDM** correspond to SOLIDWORKS PDM.

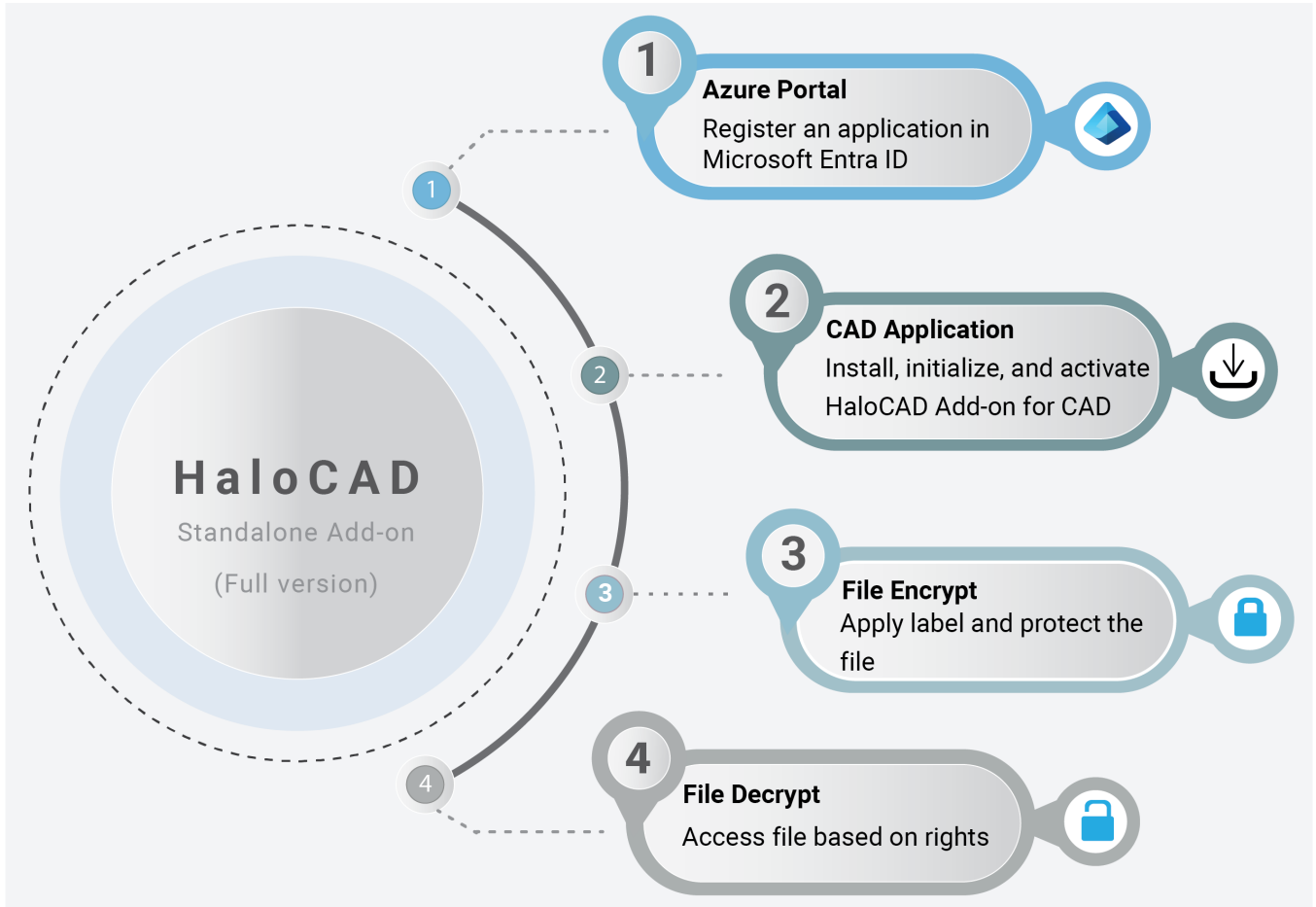
This is the primary document that administrators should read before installing the HaloCAD components. After completing this, proceed with the installation and operations manuals.

1.3. Features

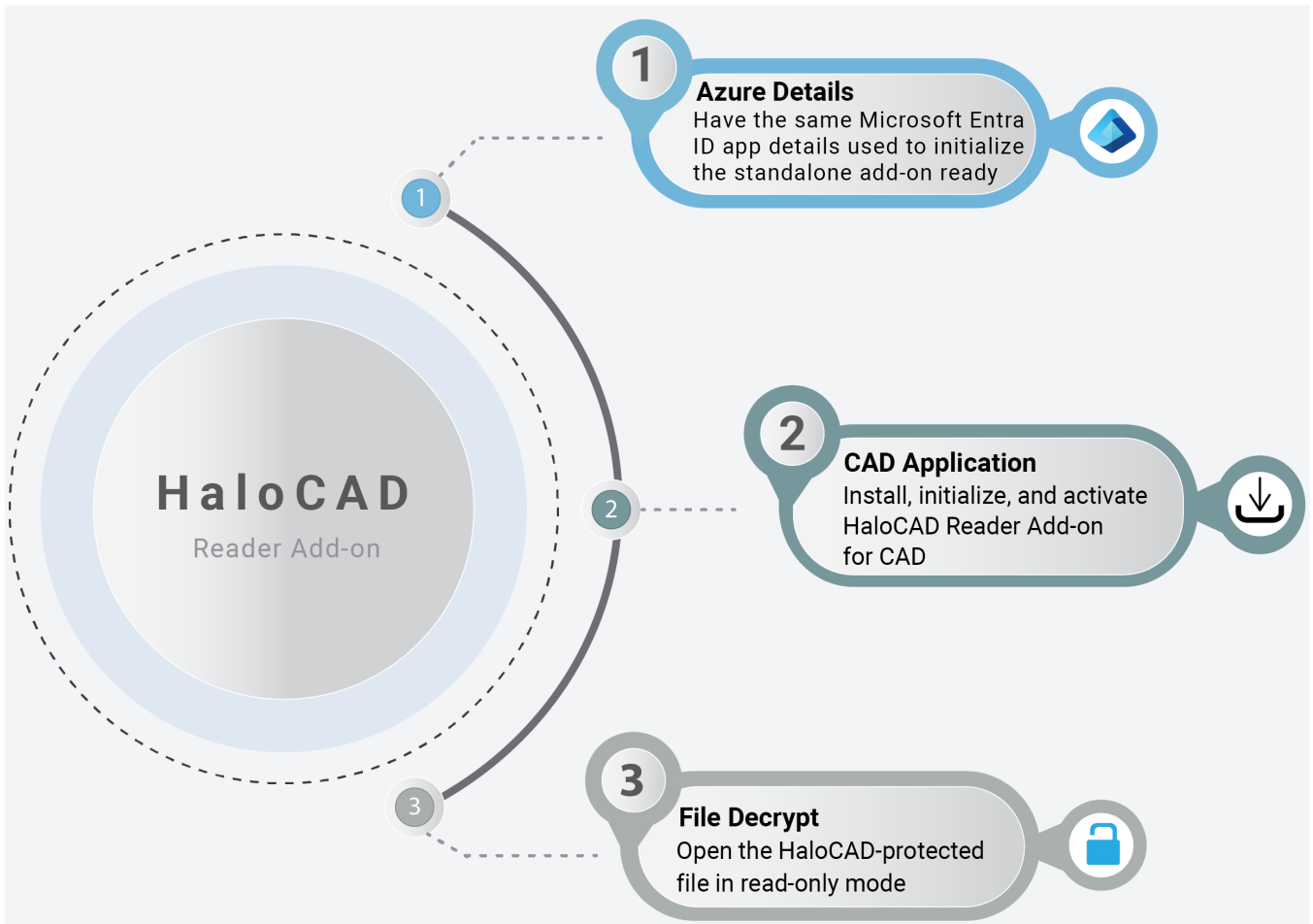
1. **Business infrastructure:** HaloCAD connects effortlessly with existing infrastructure, making it simple to use and manage.
2. **CAD:** HaloCAD add-on seamlessly extends MPIP security to CAD files.
3. **Usage rights:** Applies label-based protection using Microsoft Purview Information Protection (MPIP) and user-defined custom permissions.
4. **Data security:** Sensitive information is protected persistently regardless of where it is moved, including mobile and cloud platforms.
5. **Data Access and Usage:** Policy enforcement for managing sensitive file access and usage.
 - a. Policies specify who has access to sensitive files and what actions they can do with them.
 - b. Furthermore, it specifies how data may be used, such as restrictions on viewing, editing, copying, printing, exporting, relabeling, or modifying the rights. Watermarks can be applied to documents that contain sensitive information.
6. **Seamless integration with PLM:** Automatically protects file downloads, decrypts files during upload, and returns them to the PLM vault.

2. Quick Start Installation Summary - Standalone HaloCAD Add-on

The image below illustrates the high-level process of setting up the HaloCAD Add-on for CAD.



Quick start installation steps for HaloCAD Standalone Add-on



Quick start installation steps for HaloCAD Reader Add-on

Reference Manuals

The table below describes where to obtain information in the HaloCAD documentation set.

For information on	Name of the Reference
1. Prerequisites, architecture, and supported license activation methods 2. Secure installation using an encrypted JSON configuration file 3. Actions to take when a license expires	Please refer to the current manual.
HaloCAD Installation Options – UI, Silent, and SCCM	Refer to the Installation Manual for the add-on you purchased.
HaloCAD features, operations, and troubleshooting, if you face any issues	Refer to the Operations Manual for the add-on you purchased.

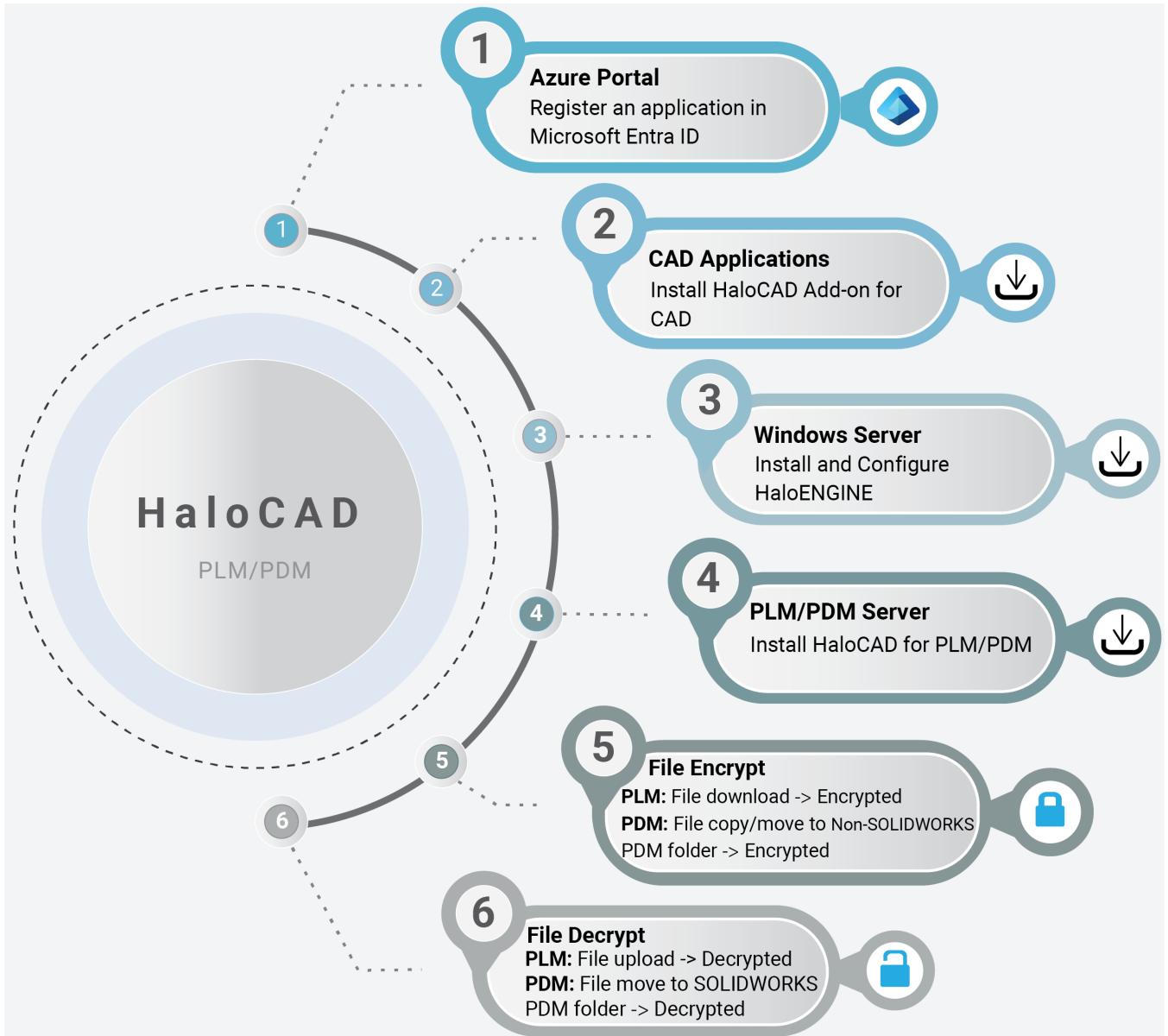
Secude

For information on	Name of the Reference
Overview of new features, resolved issues, known issues, and supported file types	Refer to the Release Notes for the add-on you purchased.

HaloCAD standalone add-on reference documentation

3. Quick Start Installation Summary - Integrated with PLM/PDM

The image below illustrates the high-level process of setting up the **HaloCAD Add-on for CAD** with **HaloCAD for PLM/PDM** environment.



Quick start installation steps for HaloCAD for PLM/PDM

Reference Manuals

The table below describes where to obtain information in the HaloCAD documentation set.

For information on	Name of the Reference
Step 1 – Registering an Application in Entra ID.	Please refer to the current manual.
Step 2 – How to install HaloCAD Add-on for CAD.	Refer to the Installation Manual for the add-on you purchased.
Step 3 – How to install HaloENGINE.	HaloENGINE_Manual_Installation_EN_Online.pdf
Step 4 – How to install HaloCAD for PLM/PDM.	Refer to the Installation Manual for the HaloCAD for PLM/PDM you purchased.
Step 5 and Step 6 – Workflow illustrating protection and decryption.	Refer to the Operations Manual for the HaloCAD for PLM/PDM you purchased.

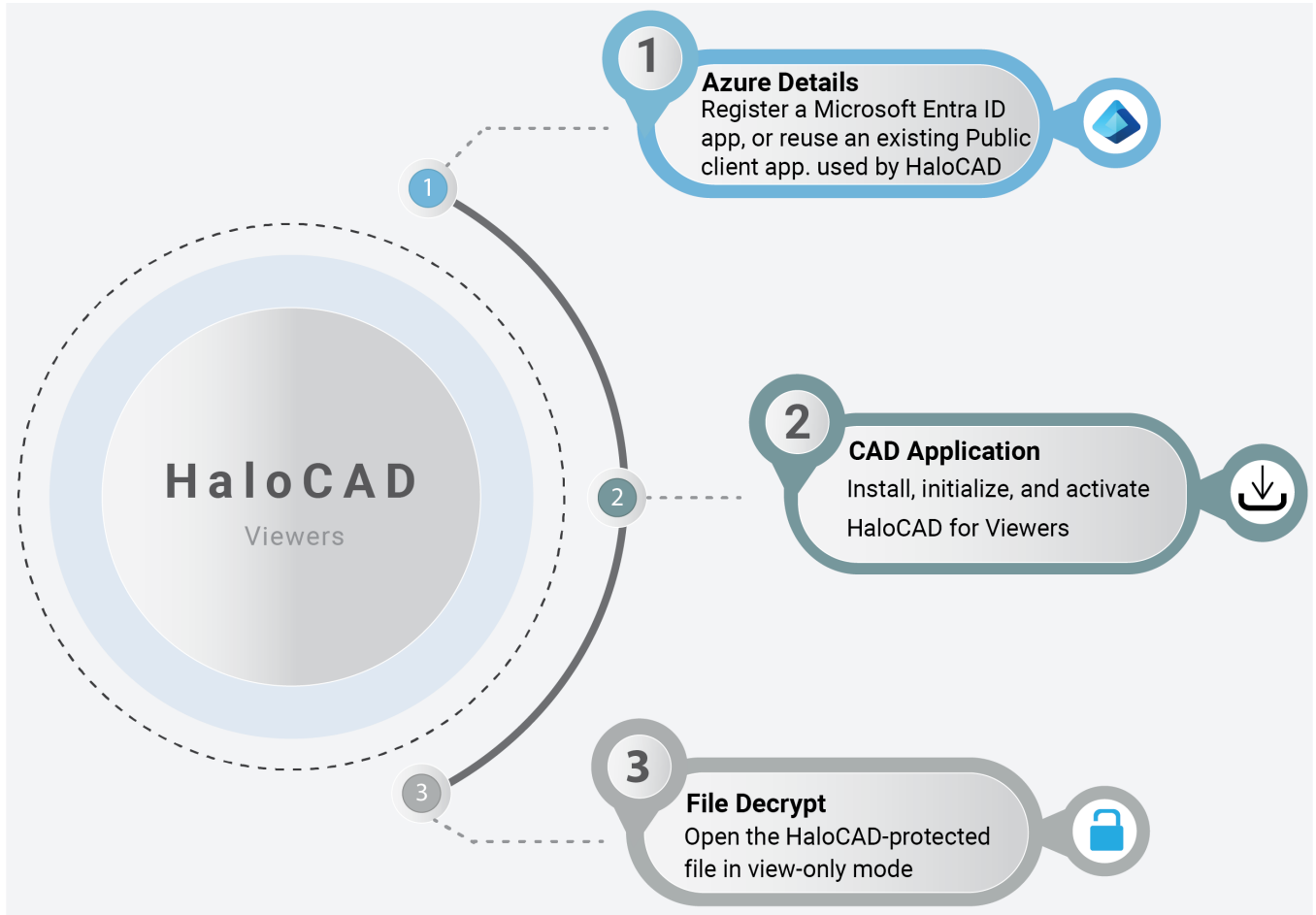
HaloCAD for PLM/PDM reference documentation

About the Term “HaloENGINE Tomcat Service”

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

4. Quick Start Installation Summary - HaloCAD for Viewers

The image below illustrates the high-level process of setting up HaloCAD for Viewers.



Quick start installation steps for HaloCAD for Viewers

For HaloCAD for TCAI, follow the same Quick Start installation steps described for HaloCAD for Viewers. Refer to the HaloCAD for TCAI documentation set for additional information.

Reference Manuals

The table below describes where to obtain information in the HaloCAD documentation set.

For information on	Name of the Reference
1. Prerequisites, architecture, and supported license activation methods	Please refer to the current manual.
2. Secure installation using an encrypted JSON configuration file	
3. Actions to take when a license expires	

Secude

For information on	Name of the Reference
Installation Options – UI, Silent, and SCCM	HaloCAD_Viewers_Manual_InstallationAndUsage_EN_Online.pdf
Overview of new features, resolved issues, known issues, and supported file types	HaloCAD_Viewers_ReleaseNotes_EN_Online.pdf

HaloCAD for Viewers reference documentation

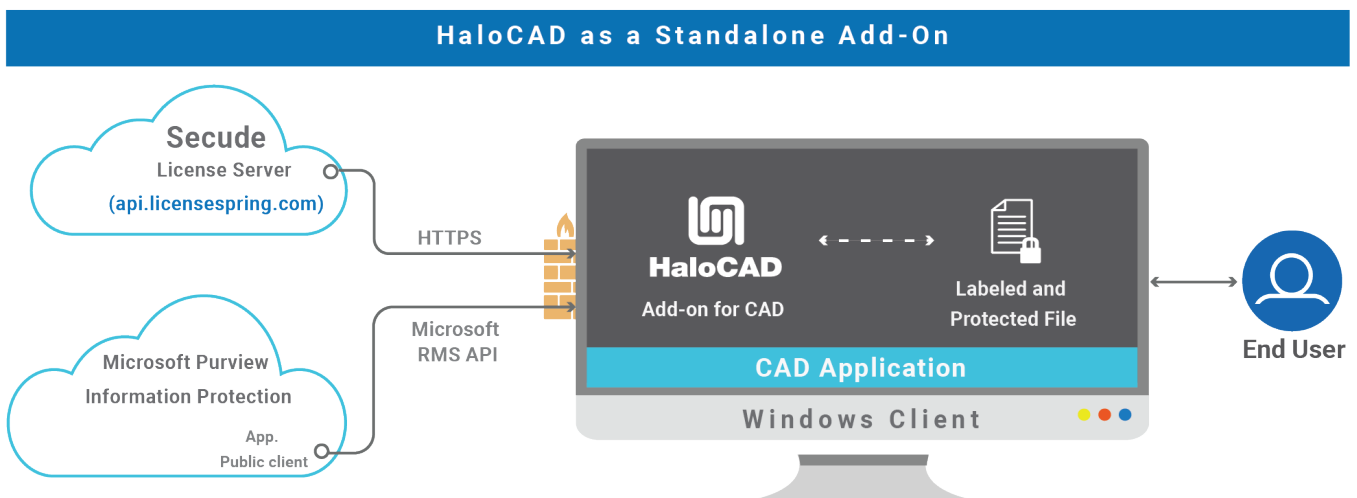
5. HaloCAD Architecture

The architecture is designed to provide secure and efficient management of CAD and PLM data through three core components: HaloCAD Add-on for CAD, HaloCAD for PLM, and the HaloENGINE.

5.1. HaloCAD Add-on for CAD

A standalone solution that contains the HaloCAD PROTECT feature. It enables access to protected files, enforces associated privileges, and allows controlled modification of MPIP labels via direct interaction with the user.

HaloCAD Add-on for CAD leverages the Microsoft Purview Information Protection solution to provide persistent document security. During the process of creating a new CAD file, the user downloads MPIP labels using valid credentials, selects a suitable label, and applies it to the file. In the standalone add-on, no automation is available, as setting labels is done manually. Protected files can only be opened and modified by authorized users, and thus, protection remains even when multiple users access the file. The user's rights are governed by pre-established policies. The following figure shows the HaloCAD Add-on for CAD as a standalone add-on.

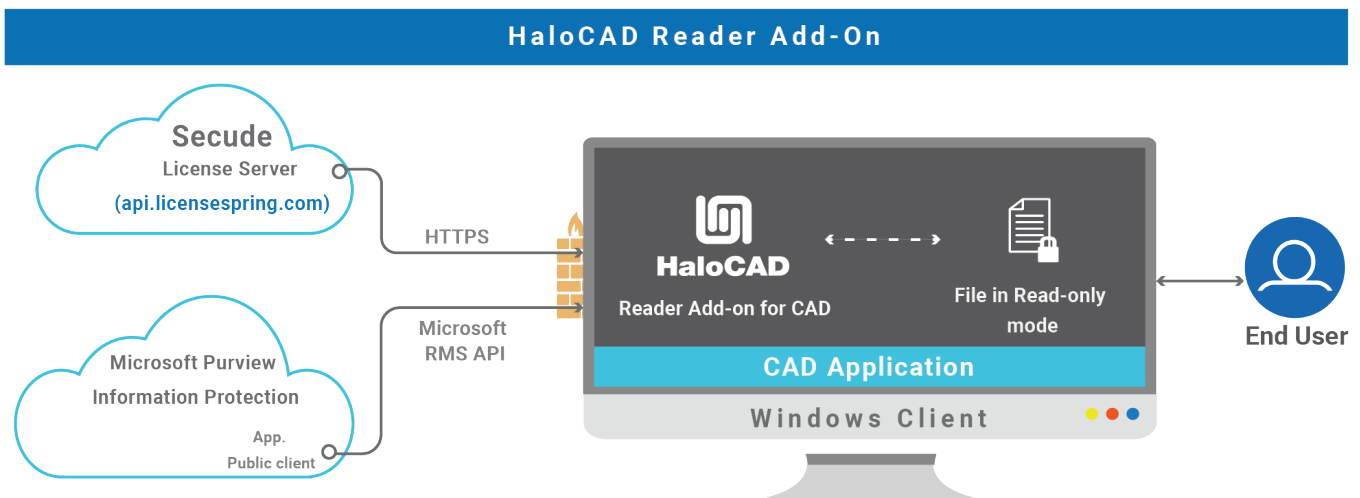


HaloCAD as a standalone add-on

Note: When HaloCAD (standalone add-on) is integrated with HaloCAD for PLM, files are automatically protected based on predefined rules before the end user can access them.

5.2. HaloCAD Reader Add-on for CAD

Secude offers a standalone reader add-on for CAD applications that lets you view MPIP-protected files containing sensitive data. It enforces 'read-only' privileges to all users and thus even authorized users cannot sneak sensitive information out by copying it or taking a screenshot. Additionally, it does not support the setting or modification of labels. Note: When a HaloCAD MPIP-protected file is shared with partners/suppliers, they don't need to install the HaloCAD Add-on for CAD on their machines; instead, just this simple reader add-on is sufficient. The following figure shows the HaloCAD Reader Add-on for CAD.



HaloCAD Reader Add-on for CAD

5.3. HaloCAD for PLM

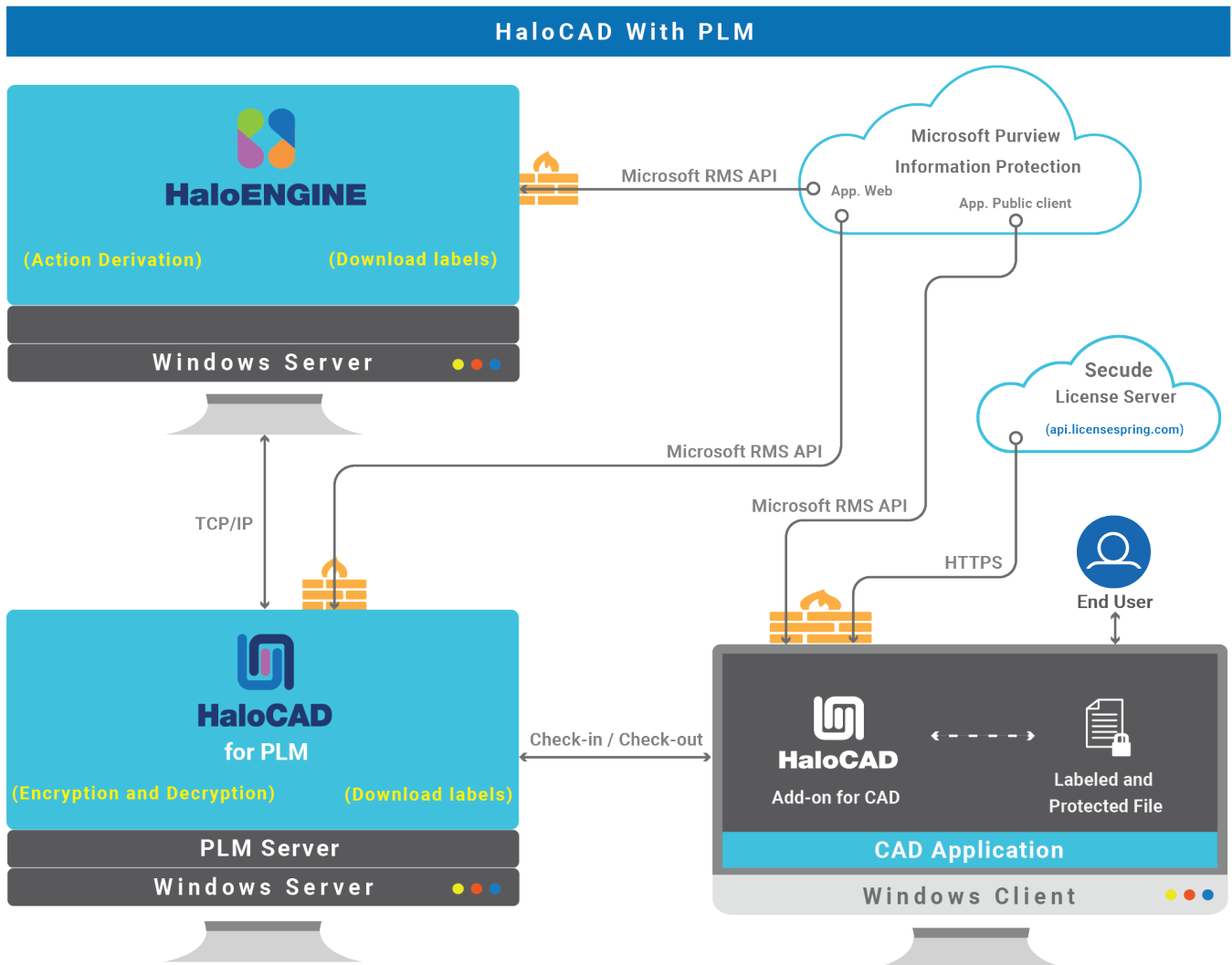
HaloCAD for PLM (HaloCAD for Teamcenter, HaloCAD for Windchill, and HaloCAD for Autodesk Vault)

This solution integrates seamlessly with the PLM application, including the features of HaloCAD PROTECT and HaloCAD MONITOR, while utilizing Microsoft Purview Information Protection (MPIP), formerly Microsoft Information Protection (MIP), to provide Enterprise Digital Rights Management (EDRM) capabilities.

HaloCAD for PLM operates continuously in the background, monitoring file uploads and downloads. It connects to Microsoft Purview Information Protection to download sensitivity labels and handle file encryption and decryption.

Secude

During a file upload, it checks whether the file is already encrypted and, if so, automatically decrypts it before allowing it to be checked into the PLM Vault. Similarly, whenever a file is downloaded, HaloCAD for PLM automatically enforces protection in accordance with defined action rules, ensuring that all file operations adhere to security rules and keep data safe. It operates independently during the file check-in or upload process. However, during file check-out or download, it depends on the rules defined in the Classification Engine (HaloENGINE).



HaloCAD for PLM

Separate Installation Requirement

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

HaloENGINE—A Java-based classification engine that implements the business logic of the architecture. It integrates with Microsoft Purview Information Protection to download sensitivity labels and make them available for configuration. HaloENGINE uses metadata to classify and organize data, and it also enforces classification schemas and action rules. All file downloads must comply with the rules defined in this engine, making it the central component of the architecture.

During file download, HaloENGINE receives relevant metadata from HaloCAD for PLM, determines the appropriate action based on the configured rules, and forwards the label and action information to HaloCAD for PLM for file processing (encryption).

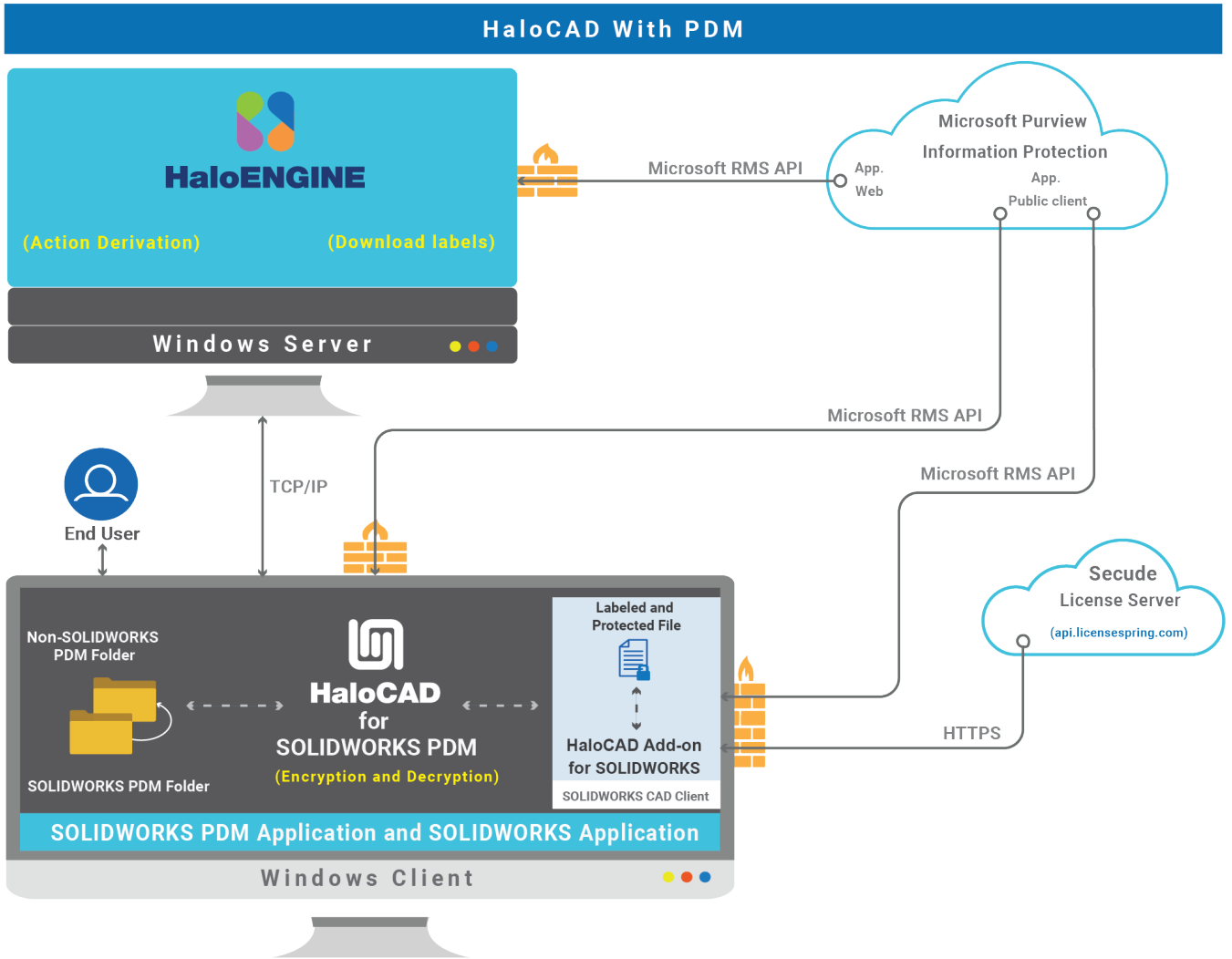
HaloCAD for PDM (HaloCAD for SOLIDWORKS PDM)

This solution integrates HaloCAD PROTECT and MONITOR capabilities with the respective PDM application. It connects to Microsoft Purview Information Protection to download sensitivity labels and handle file encryption and decryption.

SOLIDWORKS PDM folders are actively monitored to ensure file security and compliance. When files are cut or copied from a SOLIDWORKS PDM folder to a non-SOLIDWORKS PDM folder, they are automatically intercepted and protected before reaching the destination. Conversely, when previously encrypted SOLIDWORKS application files or PDF files are copied or moved into a SOLIDWORKS PDM folder, they are seamlessly decrypted and saved for use within the environment.

HaloENGINE—A Java-based classification engine that implements the business logic of the architecture. As described in HaloCAD for PLM, it provides similar functionality when integrated with PDM.

All file copy/move must comply with the rules defined in this engine, making it the central component of the architecture.



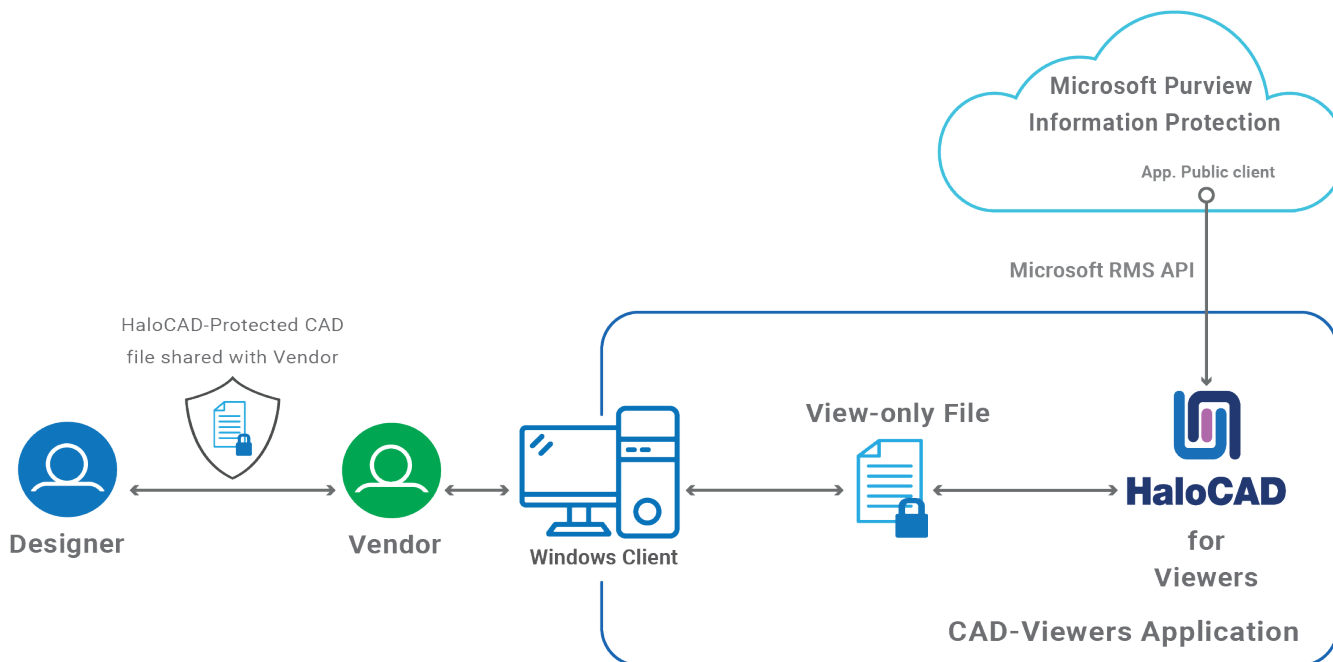
HaloCAD for PDM

For comprehensive details, please refer to the respective manuals as per your PLM environment:

1. If your environment is integrated with Windchill PLM, refer to the HaloCAD for Windchill Installation Manual.
2. If your environment is integrated with Teamcenter PLM, refer to the HaloCAD for Teamcenter Installation Manual.
3. If your environment is integrated with Autodesk Vault PLM, refer to the HaloCAD for Autodesk Vault Installation Manual.
4. If your environment is integrated with SOLIDWORKS PDM, refer to the HaloCAD for SOLIDWORKS PDM Installation Manual.

5.4. HaloCAD for Viewers

HaloCAD for Viewers is a lightweight application designed to view HaloCAD-protected files in other CAD-Viewer applications with “View only” access to all users who have access to it. This application is useful for suppliers or partners who need to access HaloCAD-protected models or drawings in their environment. The high-level architecture of HaloCAD for Viewers is illustrated in the following figure.



HaloCAD for Viewers

5.5. HaloCAD for TCAI

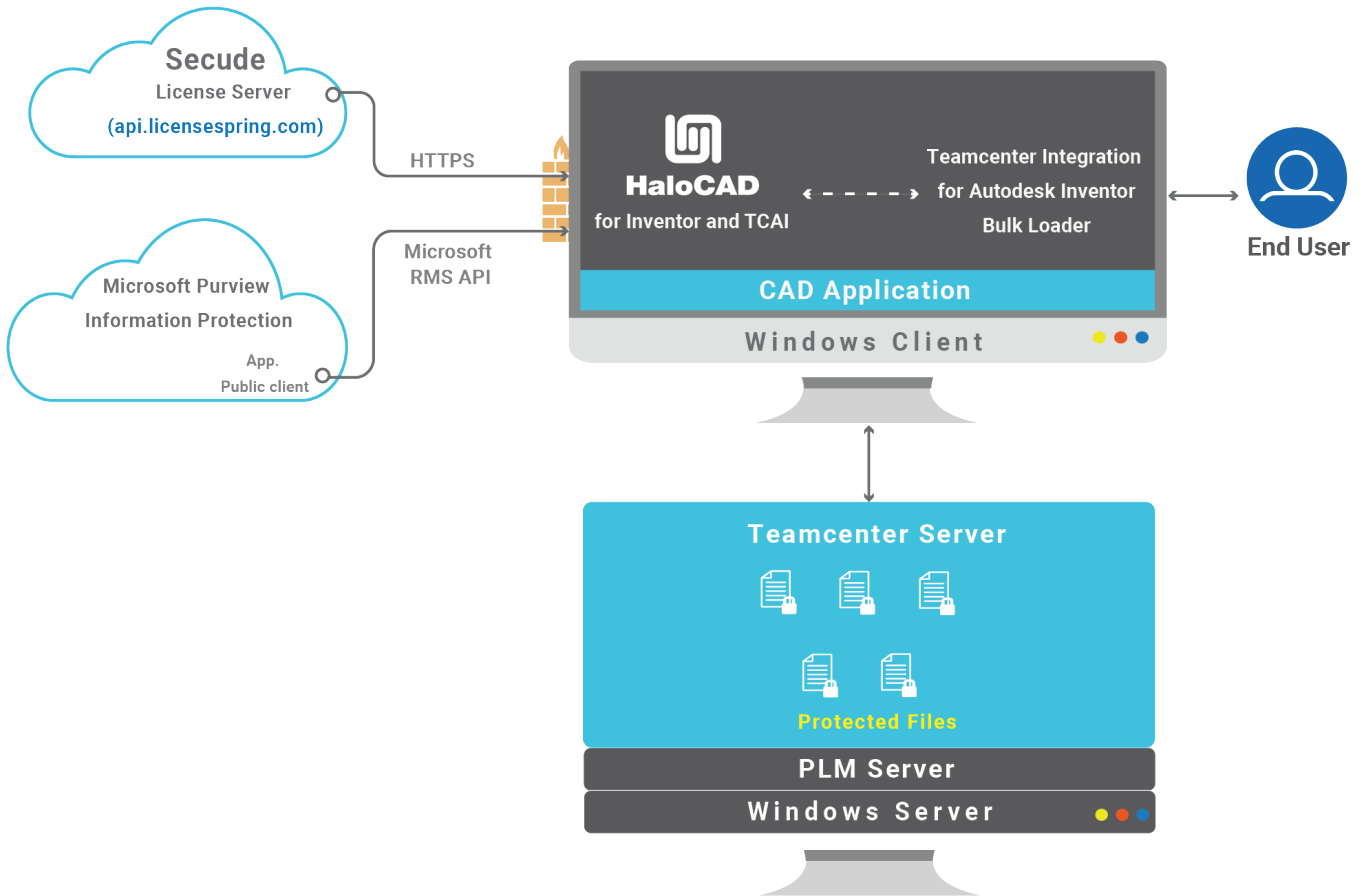
HaloCAD for TCAI is a lightweight application that uses Microsoft Purview Information Protection functionality to decrypt HaloCAD-protected CAD files during bulk loading operations in Teamcenter integration with Autodesk Inventor. This enables protected Inventor files to be scanned and processed by the TCAI Bulk Loader.

The Teamcenter Integration for Autodesk Inventor (TCAI) Bulk Loader utility allows administrators to automatically import large numbers of Inventor files into Teamcenter. However, when Inventor files are protected (encrypted), the Bulk Loader cannot recognize or process them directly.

By decrypting protected files during the loading process, HaloCAD for TCAI enables the Bulk Loader to scan and load these files into Teamcenter.

HaloCAD for TCAI uses the same underlying decryption mechanism as HaloCAD for Viewers, but it is specifically designed to support bulk loading operations in the TCAI environment.

HaloCAD for TCAI



HaloCAD for TCAI

Microsoft Purview Information Protection

HaloCAD seamlessly integrates with Microsoft Purview Information Protection solution to protect your sensitive documents. Microsoft Purview Information Protection is an industry-standard document security solution that enables businesses to ensure only authorized users can open protected content while also regulating what they can do with it, such as print, edit, or save. Even if sensitive data is leaked accidentally or maliciously, unauthorized parties cannot view it in clear text, thus leaving it useless.

Microsoft documentation

This manual assumes that you already have a complete Microsoft Purview Information Protection setup and are familiar with using the Microsoft Purview portal and related concepts. If you are new, you can refer to Microsoft's online documentation for setup and configuration.

6. Prerequisites

The prerequisites and dependencies for installing and configuring the HaloCAD add-ons are summarized in this section.

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

Applicable to	<ol style="list-style-type: none">1. HaloCAD Add-on for CAD2. HaloCAD Reader Add-on for CAD3. HaloCAD for Viewers4. HaloCAD for TCAI5. HaloCAD for SOLIDWORKS PDM
----------------------	---

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

Microsoft documentation

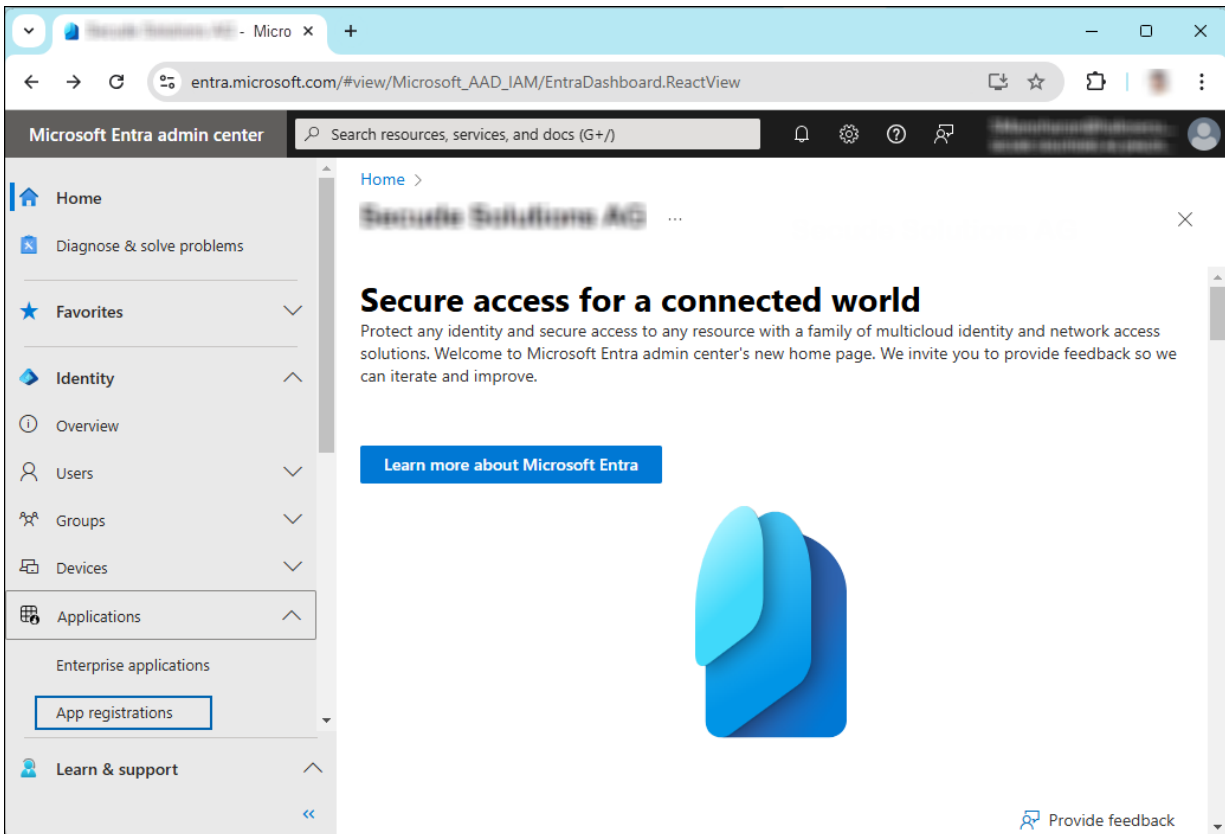
Registering an application in Microsoft Entra ID establishes a trust connection between your application and the identity provider, the Microsoft identity platform.

The information in the Microsoft documentation overrides any information published in this section. For a comprehensive description, refer to Microsoft documentation.

6.1.1. Create an Application

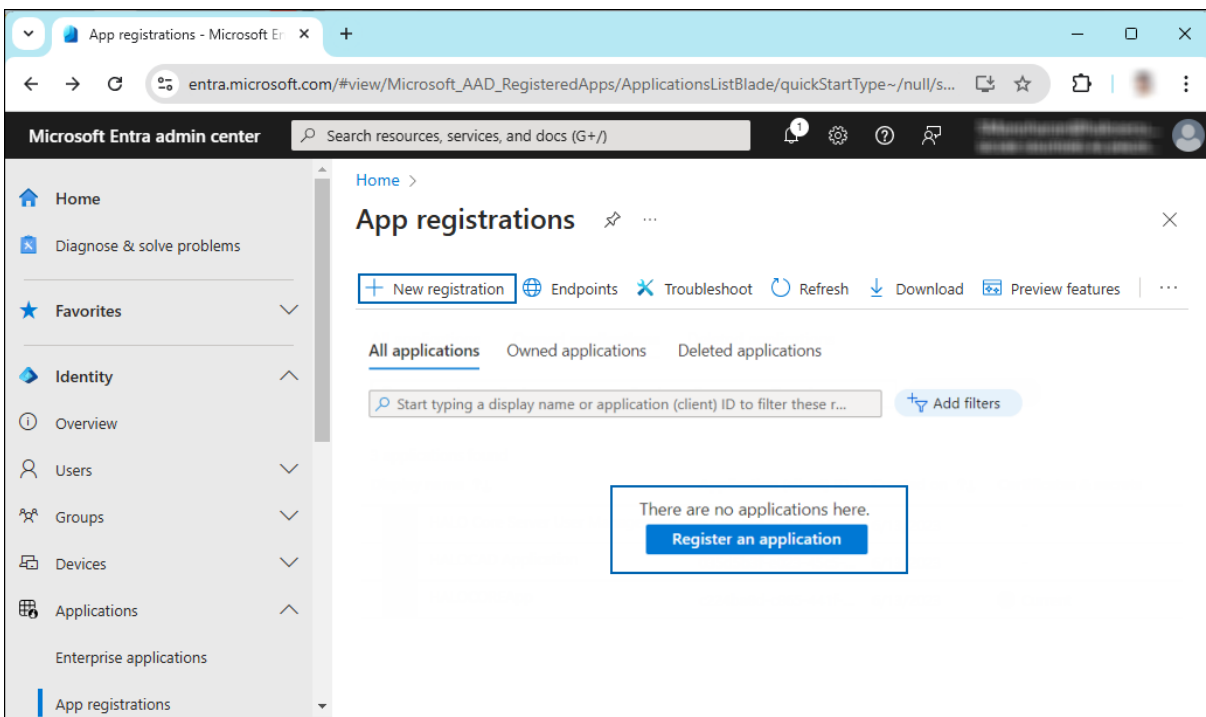
Follow the instructions below to register an application:

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 and select the tenant for which you want to register the application from the **Directories + subscriptions** menu.
3. You will be directed to the homepage.



Selecting Microsoft Entra ID

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



New application registration

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

Register an application

*** Name**
The user-facing display name for this application (this can be changed later).

Supported account types

Who can use this application or access this API?

Accounts in this organizational directory only (Single tenant)

Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)

Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

Personal Microsoft accounts only

[Help me choose...](#)

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Public client/native (mobile ...

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from [Enterprise applications](#).

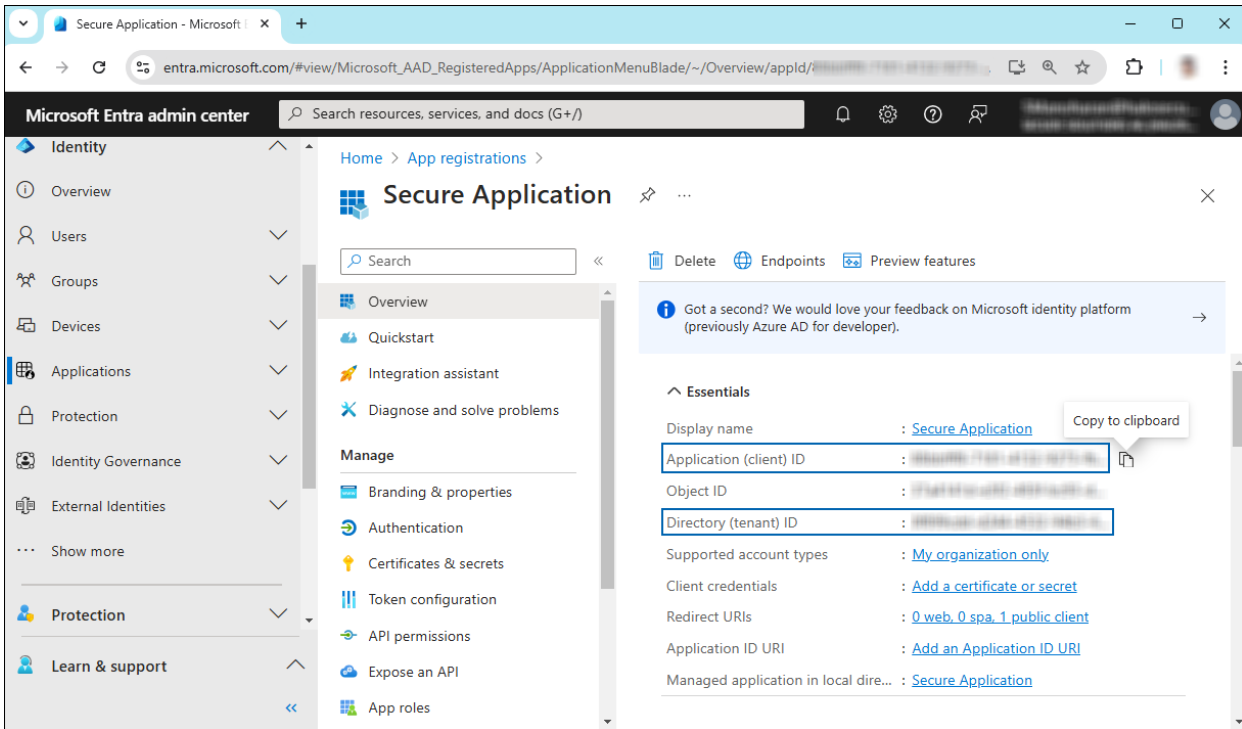
By proceeding, you agree to the [Microsoft Platform Policies](#)

Register

Application details

7. In the **Name** field, enter an appropriate application name.
8. Under **Supported account types**, select which account you would like your application to support. For detailed information on these types, please see Microsoft documentation.
 - a. To target only accounts that are internal to your organization, select **Accounts in this organizational directory only**.
 - b. To target only business or educational customers, select **Accounts in any organizational directory**.
 - c. To target the widest set of Microsoft identities and to enable multitenancy, select **Accounts in any organizational directory and personal Microsoft accounts**.
 - d. To target the widest set of Microsoft identities, select **Personal Microsoft account only**.

- e. Under **Redirect URI**: Select **Public client/native (mobile & desktop)**, and then type a valid redirect URI for your application. For example, `https://localhost`.
 - f. When finished, click **Register**.
9. The home page of the new application is created and displayed.



Application ID and Tenant ID

10. Once registration is complete, the following values are shown on the portal. 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

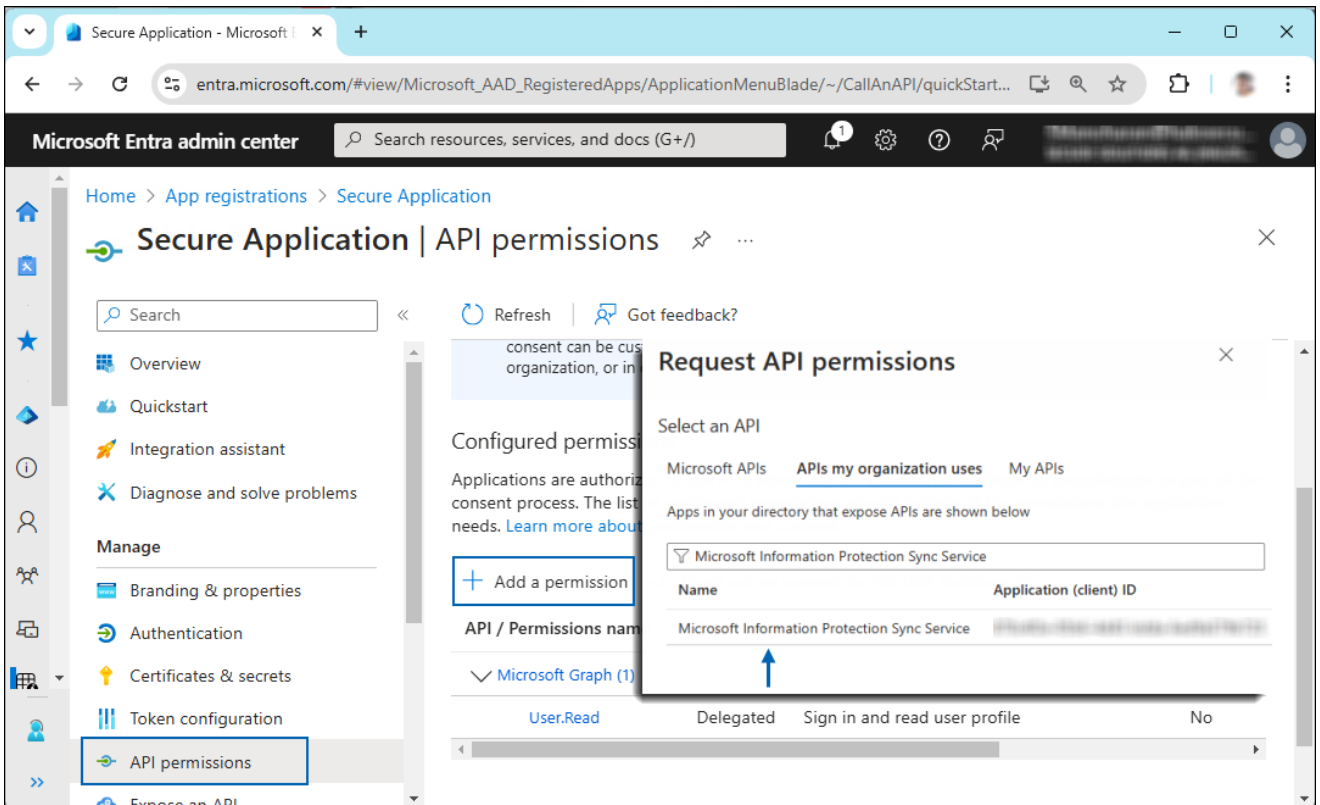
Open a text editor (such as Notepad) and copy the values for the Application (client) ID, Directory (tenant) ID, and Redirect URI. Save these details for initializing the HaloCAD Add-on. Note that the Directory (tenant) ID is required only for single-tenant applications.

6.1.2. 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 sidebar of the new application page, select **API permissions**. The **API permissions** page for the new application registration will appear.

2. Click **Add a permission** button. The **Request API permissions** page will appear.
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".

Request API permissions ✕

<https://psor.o365syncservice.com>

What type of permissions does your application require?

Delegated permissions
Your application needs to access the API as the signed-in user.

Application permissions
Your application runs as a background service or daemon without a signed-in user.

Select permissions [expand all](#)

i The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your organization, or in organizations where this app will be used. [Learn more](#) ✕

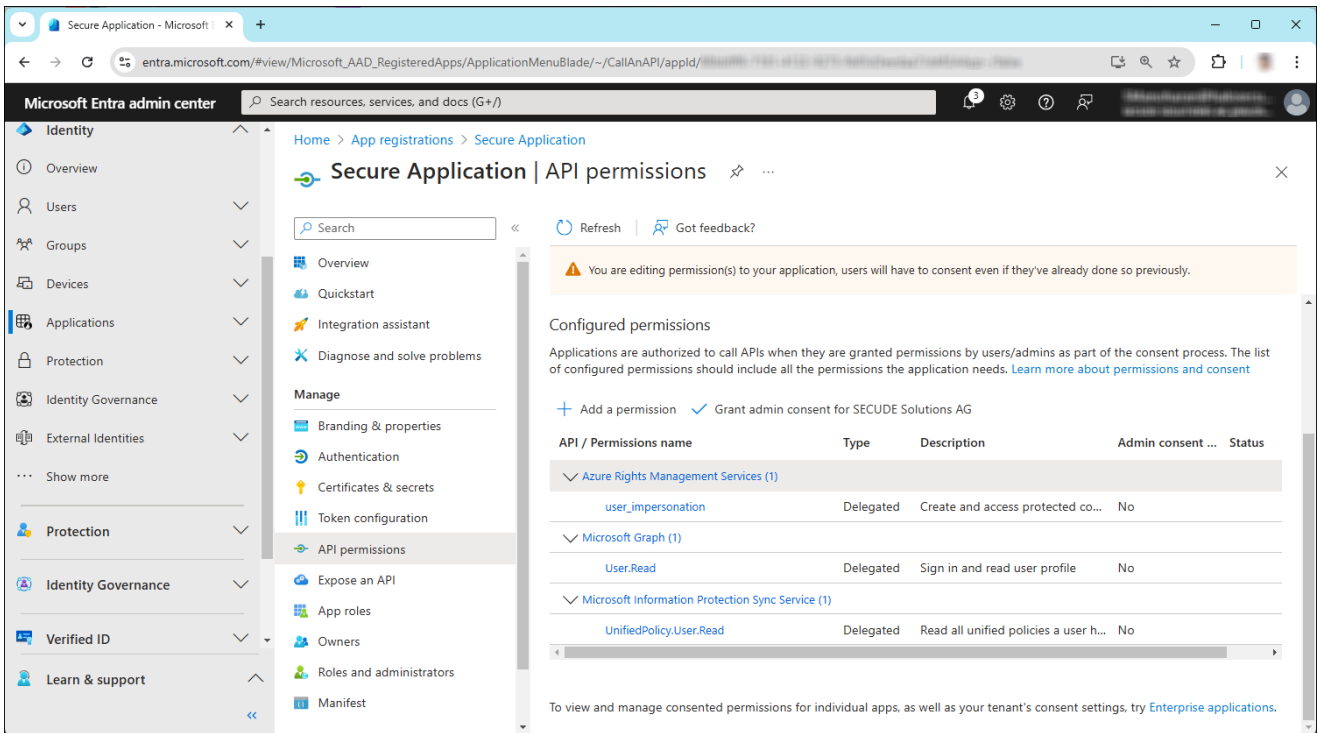
Permission	Admin consent required
▼ UnifiedPolicy (1)	
<input checked="" type="checkbox"/> UnifiedPolicy.User.Read ⓘ Read all unified policies a user has access to.	No

Add permissions

Discard

Adding permission

8. Click **Add permissions**. Repeat the steps outlined above to add the other required permissions listed in the table below.
9. You will return to the API permissions page, where the permissions have been saved and added to the table. Please note that administrator consent is not necessary 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 (will be added by default)
Microsoft Information Protection Sync Service	UnifiedPolicy.User.Read	Delegated	Read all unified policies a user has access to.

Required permissions

6.2. Register an Application in Microsoft Entra ID - Web

Applicable to	<ol style="list-style-type: none"> 1. HaloCAD for Teamcenter 2. HaloCAD for Windchill 3. HaloCAD for Autodesk Vault
----------------------	--

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 Tomcat Service.
Azure Rights Management Services	Content.DelegateWriter	Application	Create protected content on behalf of a user
(Microsoft Rights Management Services)	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

6.2.1. 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 Tomcat Service requires the following superuser privilege for the decryption function when the owner is not as SPN.

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

Required permissions #2

6.2.2. Upload the Certificate in the Azure Portal

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

Prerequisites:

1. Certificate:

- a. Ensure that you have a valid certificate containing the following key properties: -
KeyExportPolicy Exportable and -KeySpec Signature.
- b. The certificate can also be self-signed. Note: As a best practice and for security reasons, use a self-signed certificate only in a test environment. It is not recommended for production environments.

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

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

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

1. In the sidebar of the new application page, select **Certificate & secrets**.
2. Under the **Certificate** section, click **Upload certificate**. The **Upload certificate** dialog appears as shown in the figure below:

Secude

Component and Combination	Application Type	Configuration Guideline
HaloCAD Add-on for CAD and HaloCAD Reader Add-on for CAD	Public client/native (mobile & desktop)	Create a new Microsoft Entra ID application in your tenant for the HaloCAD Add-on for CAD installation and use the same application details for the Reader Add-on. The Reader Add-on cannot open protected files if the tenant details do not match.
HaloCAD for Viewer	Public client/native (mobile & desktop)	Create a new Microsoft Entra ID application in your tenant for HaloCAD for Viewer installation. Alternatively, if you already have an existing HaloCAD application, use the same app details and ensure that the client type is set to Public client/native.
HaloCAD for TCAI		
HaloCAD for SOLIDWORKS PDM	Public client/native (mobile & desktop)	Create a new Microsoft Entra ID application in your tenant for the HaloCAD for SOLIDWORKS PDM installation. When used in combination with HaloENGINE, ensure that the same Directory (Tenant) ID is used. Mismatched IDs will cause configuration errors.
HaloENGINE	Web	Create a new Microsoft Entra ID application in your tenant for the HaloENGINE. For more details, please refer to the HaloENGINE Installation Manual.
HaloCAD for PLM and HaloENGINE	Web	Both use a Web-type application, so the same application details can be used during installation.

HaloCAD and Application Type

6.3. Create and Configure the Sensitivity Labels

Applicable to	<ol style="list-style-type: none"> 1. HaloCAD Add-on for CAD 2. HaloCAD Reader for Add-on 3. 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 details, please refer to Microsoft online documentation.

6.4. Office 365 Subscription Details

Applicable to	<ol style="list-style-type: none"> 1. HaloCAD Add-on for CAD 2. HaloCAD Reader Add-on for CAD 3. HaloCAD for Viewers 4. HaloCAD for TCAI 5. HaloCAD for PLM/PDM (Teamcenter, Windchill, Vault, and SOLIDWORKS PDM)
----------------------	---

1. Fully configured Microsoft Purview Information Protection.
2. An Azure subscription is required to use Azure RMS and the MPIP functionality.
3. A working Microsoft Entra ID service must be available.
4. Transport Layer Security (TLS) 1.2 or higher must be enabled to ensure the use of cryptographically secure protocols at all client workstations. Please refer to the section "[Enable Support for TLS 1.2 at the Client Workstation for Microsoft Entra ID](#)".
5. To avail the revoke access feature, the user should be assigned to the Microsoft Purview Information Protection Premium P1/P2 license. (Not required for the reader and viewer add-on)
6. Audit logging: Your Azure subscription must include Log Analytics on the same tenant as Microsoft Entra ID.

6.5. Recommended URLs, Addresses, and Ports for MPIP

Applicable to	<ol style="list-style-type: none"> 1. HaloCAD Add-on for CAD 2. HaloCAD Reader for Add-on 3. HaloCAD for Viewers 4. HaloCAD for TCAI 5. HaloCAD for PLM/PDM (Teamcenter, Windchill, Vault, and SOLIDWORKS PDM)
----------------------	---

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

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

Recommended endpoints

Secude License Manager for HaloCAD

Applicable to	<ol style="list-style-type: none"> 1. HaloCAD Add-on for CAD 2. HaloCAD Reader 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

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

Applicable to	<ol style="list-style-type: none"> 1. HaloCAD Add-on for CAD 2. HaloCAD Reader Add-on for CAD 3. HaloCAD for Viewers 4. HaloCAD for TCAI 5. HaloCAD for PLM/PDM (Teamcenter, Windchill, Vault, and SOLIDWORKS PDM)
----------------------	---

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

1. TLS 1.1
2. TLS 1.0
3. 3DES cipher suite (TLS_RSA_WITH_3DES_EDE_CBC_SHA)

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

Microsoft documentation

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

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

In summary, the following steps must be performed:

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

S.No	Windows Registry	Values
1	[HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432 Node\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

7. License Administration

Applicable to	<ol style="list-style-type: none">1. HaloCAD Add-on for CAD2. HaloCAD Reader Add-on for CAD
----------------------	--

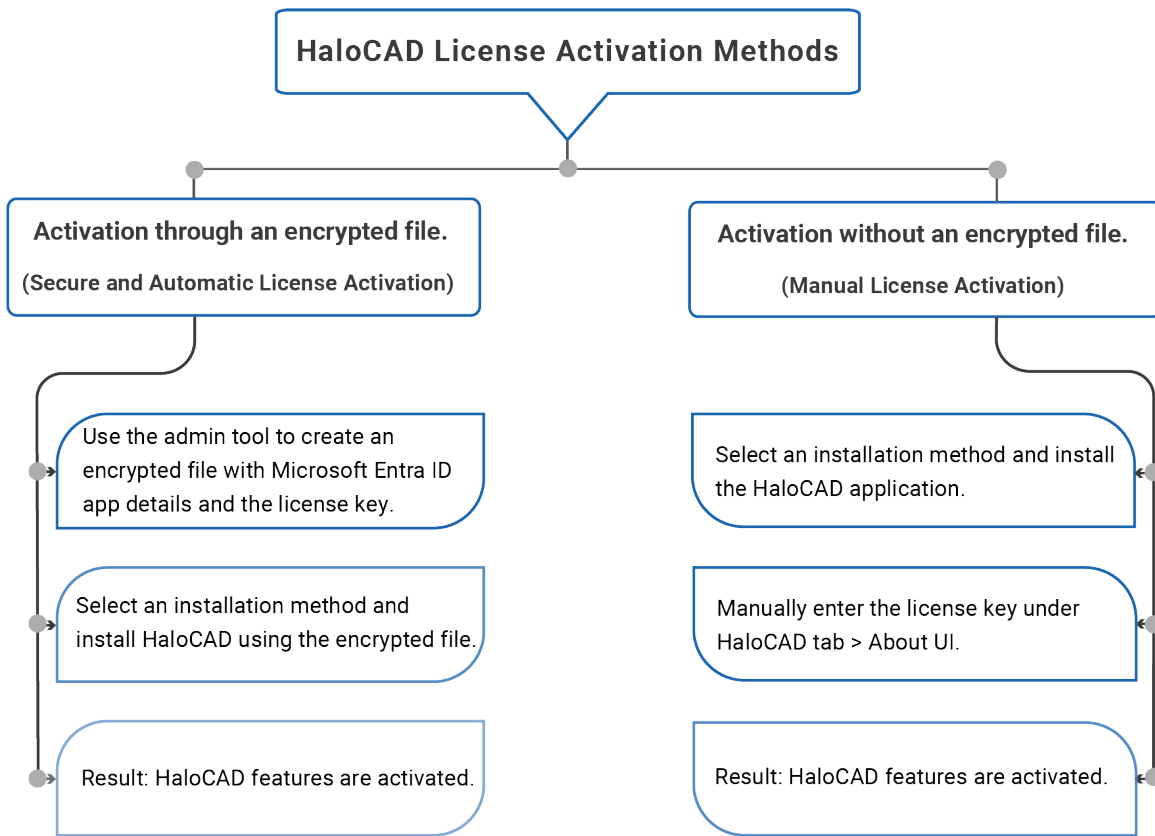
HaloCAD uses a key-based license to control application features. Obtain the license key from Secude Support before installing HaloCAD.

This document does not cover all the specifics of purchasing a license. Please contact Secude's representative for additional details.

The following methods are available to activate the license in HaloCAD.

- 1. Tool-based automatic initialization and license activation:** This method generates an encrypted configuration file that contains the license key and Microsoft Entra ID application details. Using this file, the installer automatically completes the installation, application initialization, and license activation. For more information, refer to the "[Secure Installation](#)" section.
- 2. UI-based manual license activation:** This method provides a straightforward installation process without automatic license activation. After launching the CAD application, the administrator must manually activate the license by entering the license key in the HaloCAD license screen. For more information, refer to the "[UI-based Manual License Activation](#)" section.
- 3. License activation in silent mode:** This method uses an encrypted configuration file to automatically initialize the application and activate the license during installation. For more details, refer to the **Silent Mode** section of the HaloCAD Installation Manual provided with your purchased application.
- 4. License activation via System Center Configuration Manager (SCCM):** For organization-wide deployment and activation of the HaloCAD add-on, an encrypted configuration file containing the license key information and Microsoft Entra ID application details is used together with the installer. For additional information on SCCM, please refer to the HaloCAD Installation Manual.

The following is a high-level diagram that illustrates license activation.



License activation

7.1. Secure Installation (Recommended)

Applicable to	<ol style="list-style-type: none"> 1. HaloCAD Add-on for CAD 2. HaloCAD Reader Add-on for CAD 3. HaloCAD for Viewers 4. HaloCAD for TCAI 5. HaloCAD for SOLIDWORKS PDM
----------------------	---

As a best practice, application secrets should not be shared with end users, third parties, or trusted vendors. However, to avail of HaloCAD features (standard add-on and reader add-on), it is necessary to share such sensitive information for a successful installation.

To overcome this challenge, Secude offers an admin utility tool that can write and encrypt data, including Microsoft Entra ID application details (Application ID, Tenant ID, and Redirect URI), Cloud type details, and a license key in an encrypted configuration file. It uses the RSA algorithm for cryptography, allowing only the HaloCAD installer to access the configuration file with the private key during the initialization process, effectively masking the Initialization screen from the user.

An administrator can create an encrypted JSON file using this admin tool and share it with internal/external parties without disclosing the original tenant details.

HaloCAD Admin Utility Tool

The HaloCAD product package comprises an additional component—`hc.admintool.exe`.

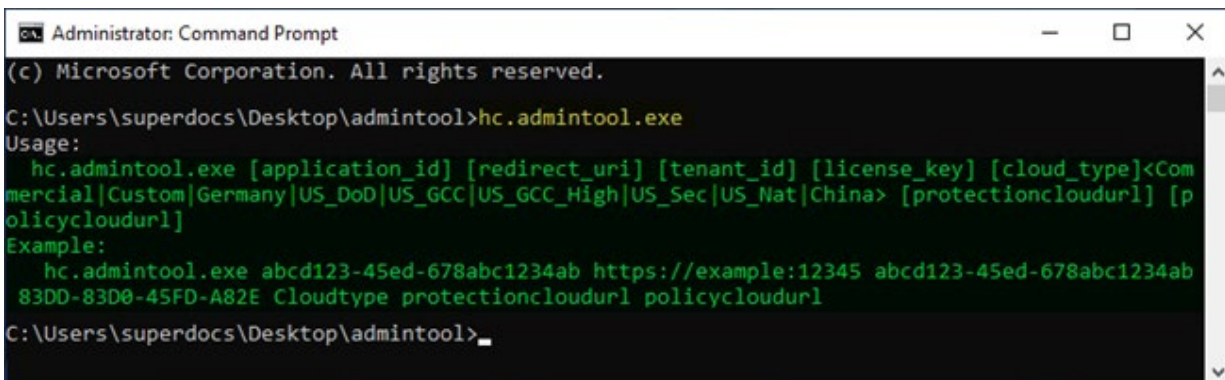
Prerequisites: Before executing the admin tool, make sure you have the necessary information.

1. Microsoft Entra ID application details for initialization
2. Cloud type details
3. A license key

Note: A license key is not required for HaloCAD for Viewers and HaloCAD for TCAL.

How to Encrypt the Configuration File

1. From the product package, move the **admintool** folder to your preferred location. For example, `C:\Users\superdocs\Desktop\admintool`.
2. Open the Command Prompt with elevated rights (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

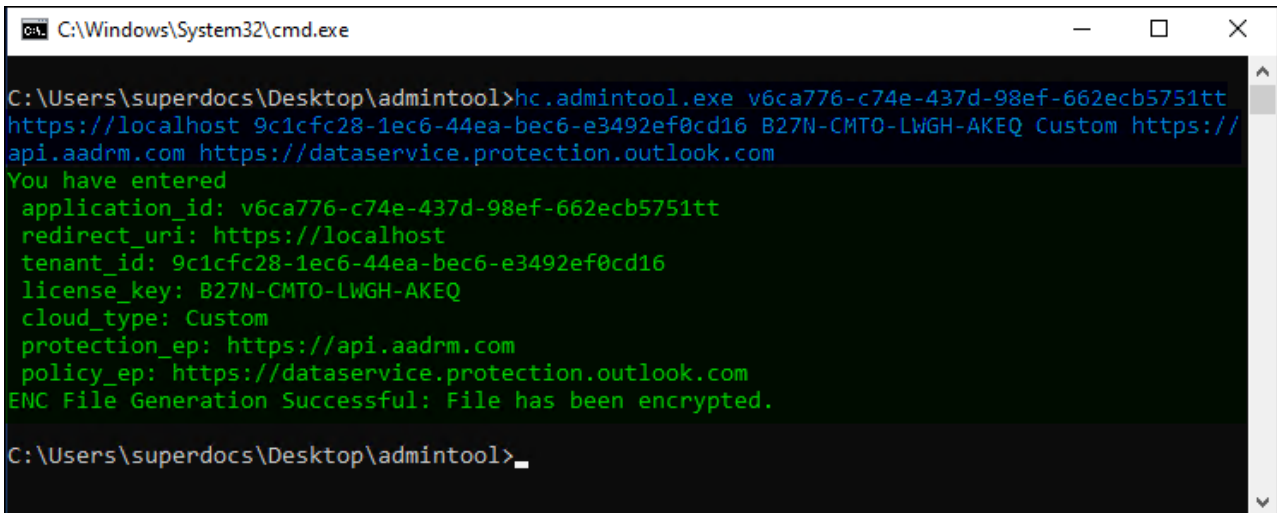
4. Enter the required details. For example,

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 will now appear as follows:



```

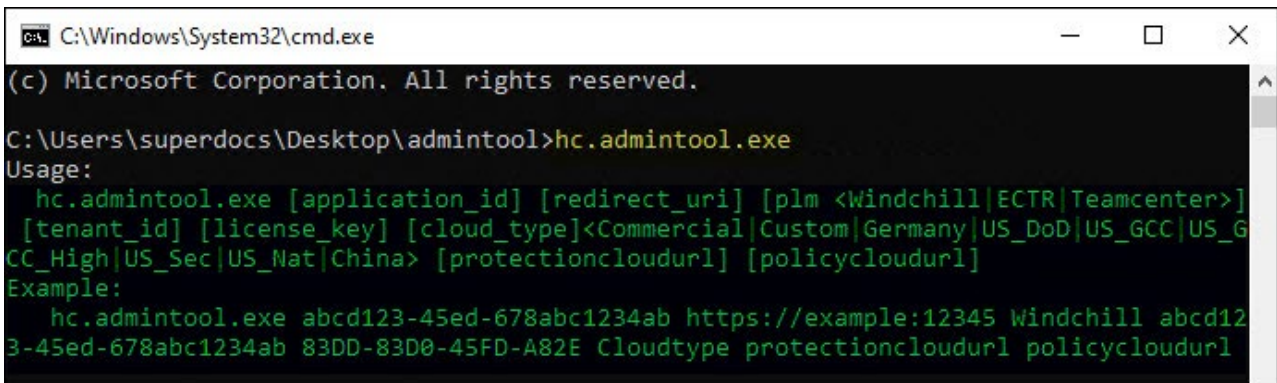
C:\Windows\System32\cmd.exe

C:\Users\superdocs\Desktop\admintool>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
You have entered
  application_id: v6ca776-c74e-437d-98ef-662ecb5751tt
  redirect_uri: https://localhost
  tenant_id: 9c1cfc28-1ec6-44ea-bec6-e3492ef0cd16
  license_key: B27N-CMTO-LWGH-AKEQ
  cloud_type: Custom
  protection_ep: https://api.aadrm.com
  policy_ep: https://dataservice.protection.outlook.com
ENC File Generation Successful: File has been encrypted.

C:\Users\superdocs\Desktop\admintool>_
    
```

Admin tool displaying the output

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



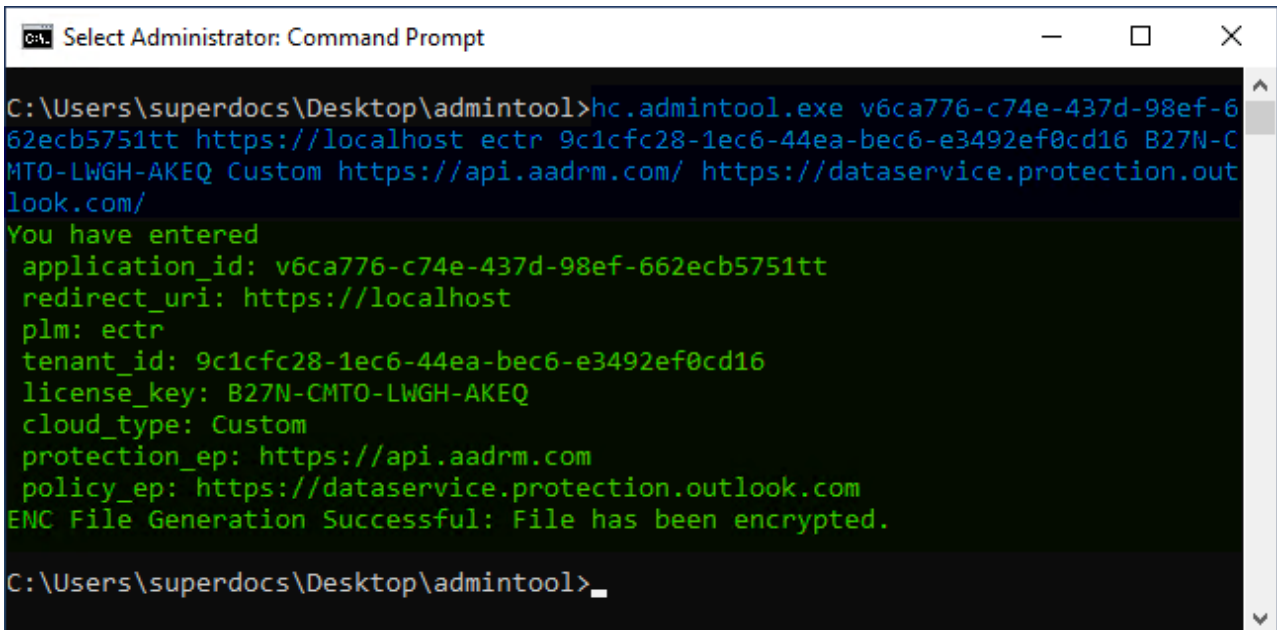
```

C:\Windows\System32\cmd.exe

(c) Microsoft Corporation. All rights reserved.

C:\Users\superdocs\Desktop\admintool>hc.admintool.exe
Usage:
  hc.admintool.exe [application_id] [redirect_uri] [plm <Windchill|ECTR|Teamcenter>]
  [tenant_id] [license_key] [cloud_type]<Commercial|Custom|Germany|US_DoD|US_GCC|US_G
  CC_High|US_Sec|US_Nat|China> [protectioncloudurl] [policycloudurl]
Example:
  hc.admintool.exe abcd123-45ed-678abc1234ab https://example:12345 Windchill abcd12
  3-45ed-678abc1234ab 83DD-83D0-45FD-A82E Cloudtype protectioncloudurl policycloudurl
    
```

Admin tool with help command for Creo add-on



```

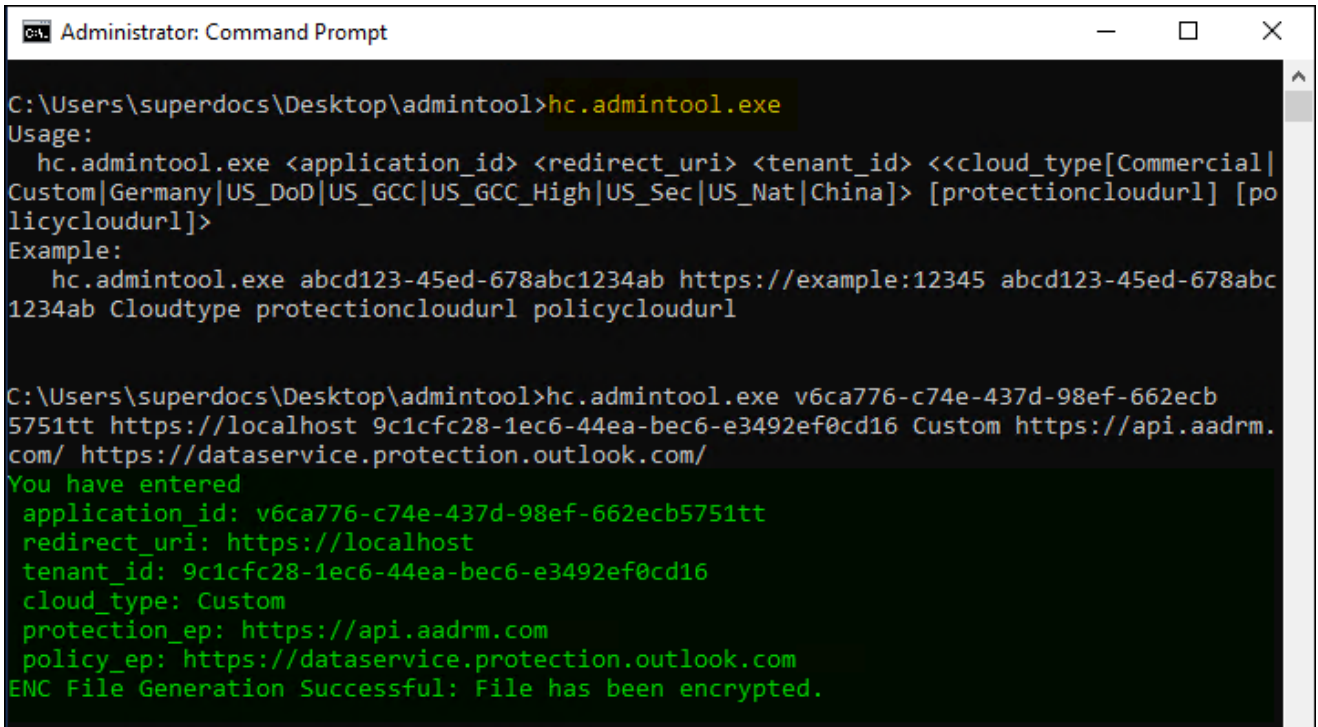
Select Administrator: Command Prompt

C:\Users\superdocs\Desktop\admintool>hc.admintool.exe v6ca776-c74e-437d-98ef-6
62ecb5751tt https://localhost ectr 9c1cfc28-1ec6-44ea-bec6-e3492ef0cd16 B27N-C
MTO-LWGH-AKEQ Custom https://api.aadrm.com/ https://dataservice.protection.out
look.com/
You have entered
  application_id: v6ca776-c74e-437d-98ef-662ecb5751tt
  redirect_uri: https://localhost
  plm: ectr
  tenant_id: 9c1cfc28-1ec6-44ea-bec6-e3492ef0cd16
  license_key: B27N-CMTO-LWGH-AKEQ
  cloud_type: Custom
  protection_ep: https://api.aadrm.com
  policy_ep: https://dataservice.protection.outlook.com
ENC File Generation Successful: File has been encrypted.

C:\Users\superdocs\Desktop\admintool>_
    
```

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.

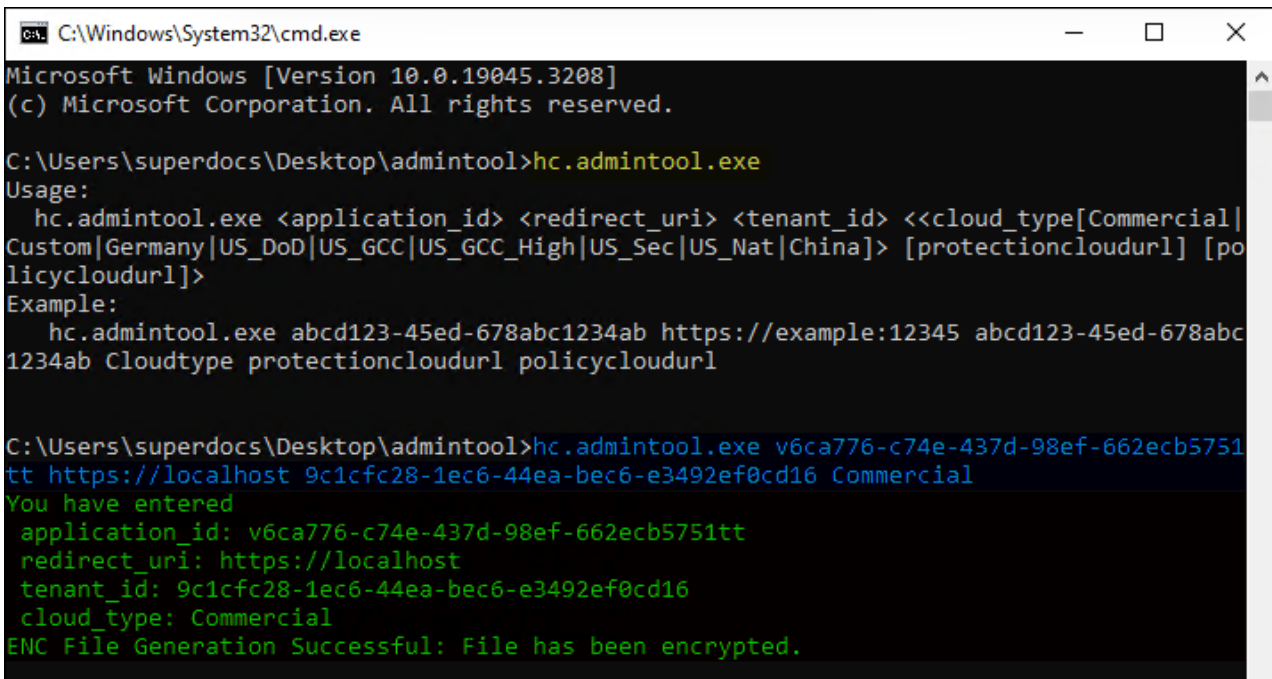


```
C:\Users\superdocs\Desktop\admintool>hc.admintool.exe
Usage:
  hc.admintool.exe <application_id> <redirect_uri> <tenant_id> <<cloud_type[Commercial|
Custom|Germany|US_DoD|US_GCC|US_GCC_High|US_Sec|US_Nat|China]> [protectioncloudurl] [po
licycloudurl]>
Example:
  hc.admintool.exe abcd123-45ed-678abc1234ab https://example:12345 abcd123-45ed-678abc
1234ab Cloudtype protectioncloudurl policycloudurl

C:\Users\superdocs\Desktop\admintool>hc.admintool.exe v6ca776-c74e-437d-98ef-662ecb
5751tt https://localhost 9c1cfc28-1ec6-44ea-bec6-e3492ef0cd16 Custom https://api.aadrm.
com/ https://dataservice.protection.outlook.com/
You have entered
application_id: v6ca776-c74e-437d-98ef-662ecb5751tt
redirect_uri: https://localhost
tenant_id: 9c1cfc28-1ec6-44ea-bec6-e3492ef0cd16
cloud_type: Custom
protection_ep: https://api.aadrm.com
policy_ep: https://dataservice.protection.outlook.com
ENC File Generation Successful: File has been encrypted.
```

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.



```
C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.19045.3208]
(c) Microsoft Corporation. All rights reserved.

C:\Users\superdocs\Desktop\admintool>hc.admintool.exe
Usage:
  hc.admintool.exe <application_id> <redirect_uri> <tenant_id> <<cloud_type[Commercial|
Custom|Germany|US_DoD|US_GCC|US_GCC_High|US_Sec|US_Nat|China]> [protectioncloudurl] [po
licycloudurl]>
Example:
  hc.admintool.exe abcd123-45ed-678abc1234ab https://example:12345 abcd123-45ed-678abc
1234ab Cloudtype protectioncloudurl policycloudurl

C:\Users\superdocs\Desktop\admintool>hc.admintool.exe v6ca776-c74e-437d-98ef-662ecb5751
tt https://localhost 9c1cfc28-1ec6-44ea-bec6-e3492ef0cd16 Commercial
You have entered
application_id: v6ca776-c74e-437d-98ef-662ecb5751tt
redirect_uri: https://localhost
tenant_id: 9c1cfc28-1ec6-44ea-bec6-e3492ef0cd16
cloud_type: Commercial
ENC File Generation Successful: File has been encrypted.
```

Admin tool displaying the output for Viewers and TCAI

Result:

- The `hc.conf.json` file will be replaced by an encrypted file named `hc.conf.enc`.
- You can now share the configuration file with external users. With this file, users can install the HaloCAD add-on on their workstations seamlessly, without requiring any additional configuration details.
- Configuration files created with earlier releases are not supported. Always use the admin tool included in the installation package to generate a new configuration file.

Next step

1. Place the encrypted file `hc.conf.enc` in the same directory as the HaloCAD installer you have purchased.
2. To start the interactive installation, double-click the installer and follow the steps provided in the Installation Manual for your purchased add-on.

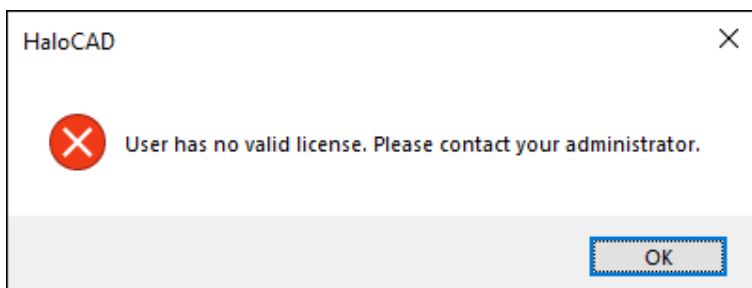
7.2. UI-based Manual License Activation

Applicable to	<ol style="list-style-type: none"> 1. HaloCAD Add-on for CAD 2. HaloCAD Reader for Add-on
----------------------	---

This section describes how to activate a license using the HaloCAD user interface. Note: If you encounter any issues while activating the license, please refer to the “Troubleshooting” chapter in the Operations Manual.

Prerequisite: Ensure that the HaloCAD installation is complete by following the instructions provided in the Installation Manual.

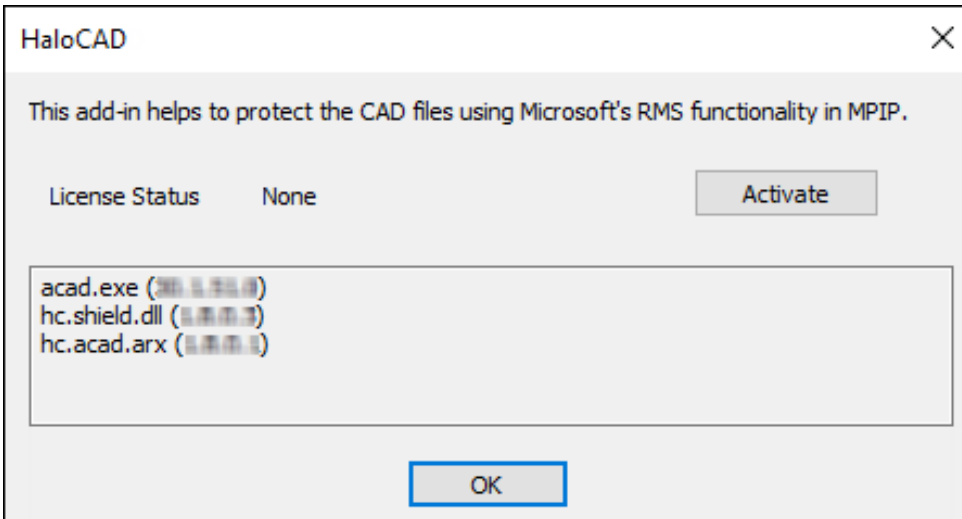
1. Open the CAD application for which the add-on was purchased.
2. HaloCAD programmatically sends a license validation request to Secude's License Manager, and the following warning message appears:



HaloCAD license warning message

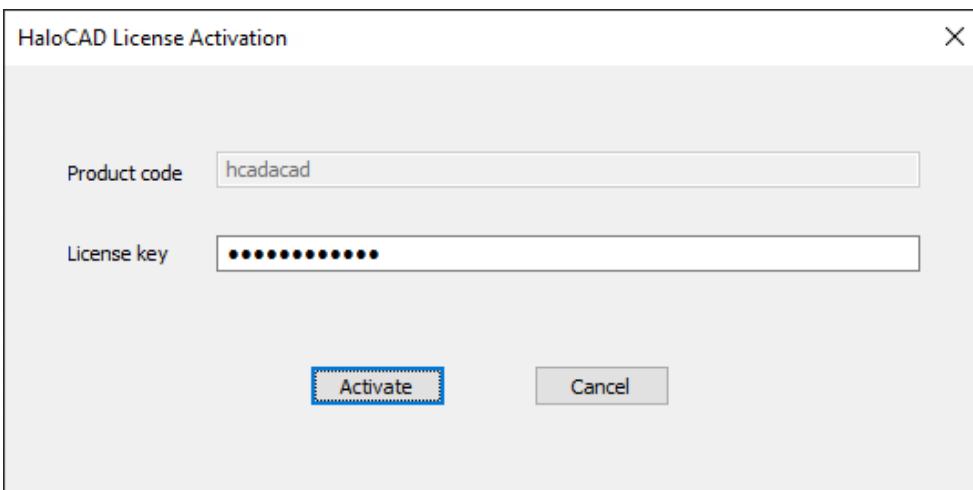
3. Click **OK**.

- Go to the **HaloCAD** tab and click **About** to see the status of your license. You will see **None** on the screen, indicating that the license has not yet been enabled.



License Status: None

- Click **Activate**.
- The *HaloCAD License Activation* screen will appear.

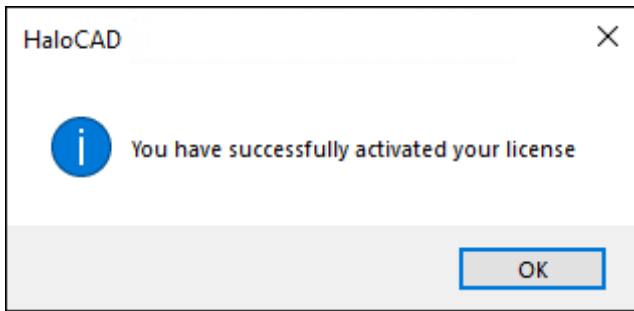


HaloCAD activation screen

- Enter the license key for the standard add-on for protection. Note: Ensure you enter the license key provided specifically for the reader add-on when using it. Interchanging license keys results in activation failure.
- Click **Activate**.

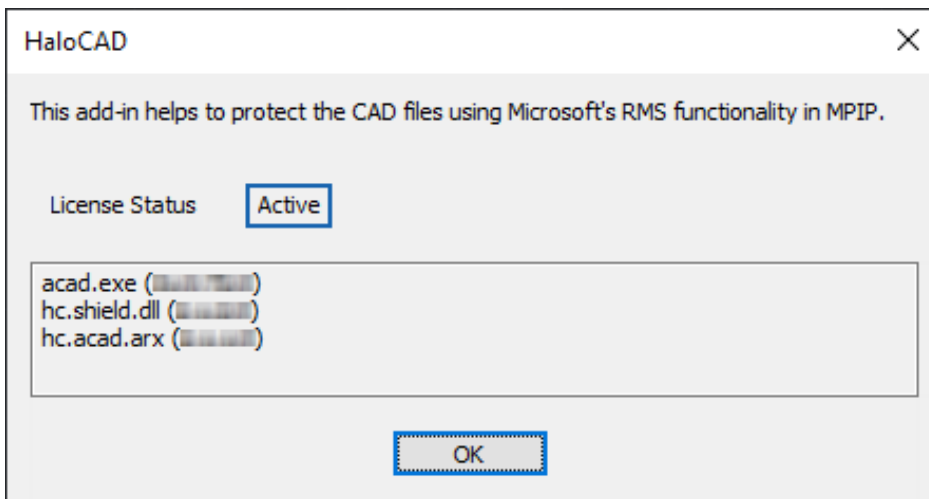
Result:

- You will receive the following confirmation message:



Activation success message

- Click **OK**.
- As a result, you will see **Active** on the screen, indicating that the license has been activated.



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.

7.3. License Expiration

Applicable to	<ol style="list-style-type: none"> 1. HaloCAD Add-on for CAD 2. HaloCAD Reader Add-on for CAD
----------------------	---

HaloCAD licenses are valid only until the specified expiration date. After the license expires, launching the CAD application will display a warning message stating *"The license is invalid."* After clicking **OK**, another message will appear stating *"User has no valid license. Please contact your administrator."* To continue using the application, a new valid license must be obtained and activated.

Prerequisite: Before reactivating it, ensure that you have a new license key from Secude.

Option 1 - Using the Admin Tool (Automatic Activation)

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 - Using the About UI (Manual Activation)

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.

8. 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	<ol style="list-style-type: none"> 1. HaloCAD Add-on for CAD 2. HaloCAD Reader 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	4.72.1.0	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

Secude

Library	Version	Source Code	License Link
MIP SDK	1.18.103 Creo and NX: 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	7.40.0	-	-

Third-party libraries

The third-party libraries and dependencies used by HaloCAD for Viewers, HaloCAD for TCAI, HaloENGINE, HaloCAD for Teamcenter PLM, HaloCAD for Windchill PLM, HaloCAD for Autodesk Vault PLM, and HaloCAD for SOLIDWORKS PDM are listed in its Installation Manual.



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.