Secude

HaloCAD

Technical Reference Manual

Copyright

Contact

Secude Solutions AG

Landenbergstrasse 34

6005 Luzern

Switzerland

Tel: +41 41 510 70 70

Mail: info@secude.com

Support

Web: https://support.secude.com

Mail: support@secude.com

Table of Contents

Typographic Conventions

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

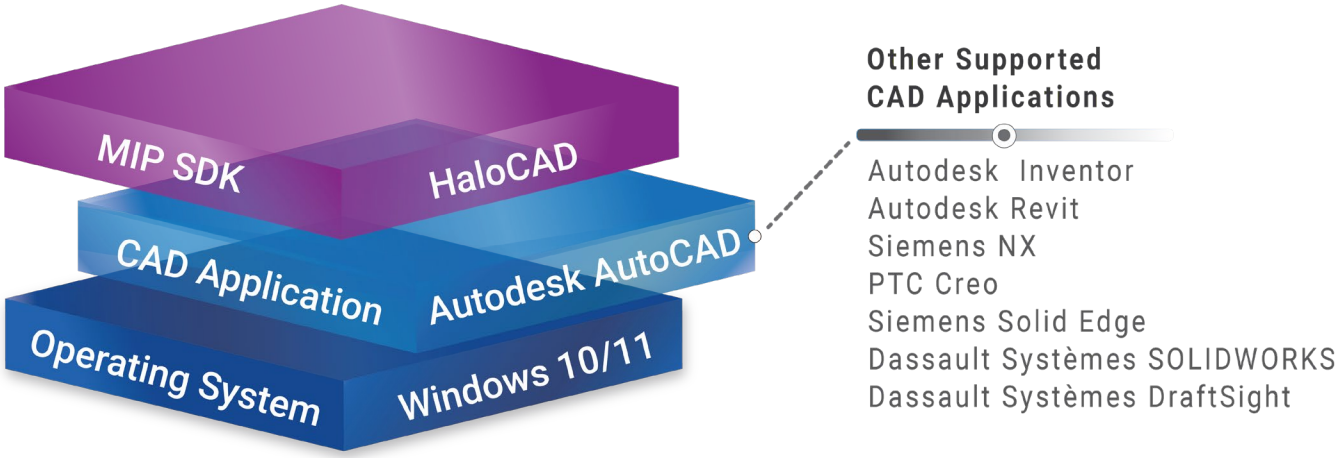
Convention	Description
Boldface type	• Items you must select, such as menu options, command buttons, or items in a list. • Titles of sections, sub-sections, etc.
Italic type	• To emphasize a word • Error messages • Table and Figure captions
`Consolas Font`	• Package names • Filenames and directory names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

1. Introduction

Companies across industries, such as automotive, aviation, high tech, and even fashion, 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. By implementing comprehensive security measures you can significantly reduce the risks and safeguard your data.

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. As a plug-in for CAD applications, HaloCAD offers access to MPIP-protected files, including label handling and privilege enforcement. CAD users will not notice any differences in the handling of CAD files because they take place in the background. By seamlessly attaching MPIP labels to the CAD files while they are being created, it provides end-to-end security for those files.



HaloCAD Add-on for CAD applications

1.2. About this Manual

This guide describes how to set up your environment, the technical requirements for HaloCAD, and in-depth explanations to enable administrators to install and configure the HaloCAD Add-on successfully.

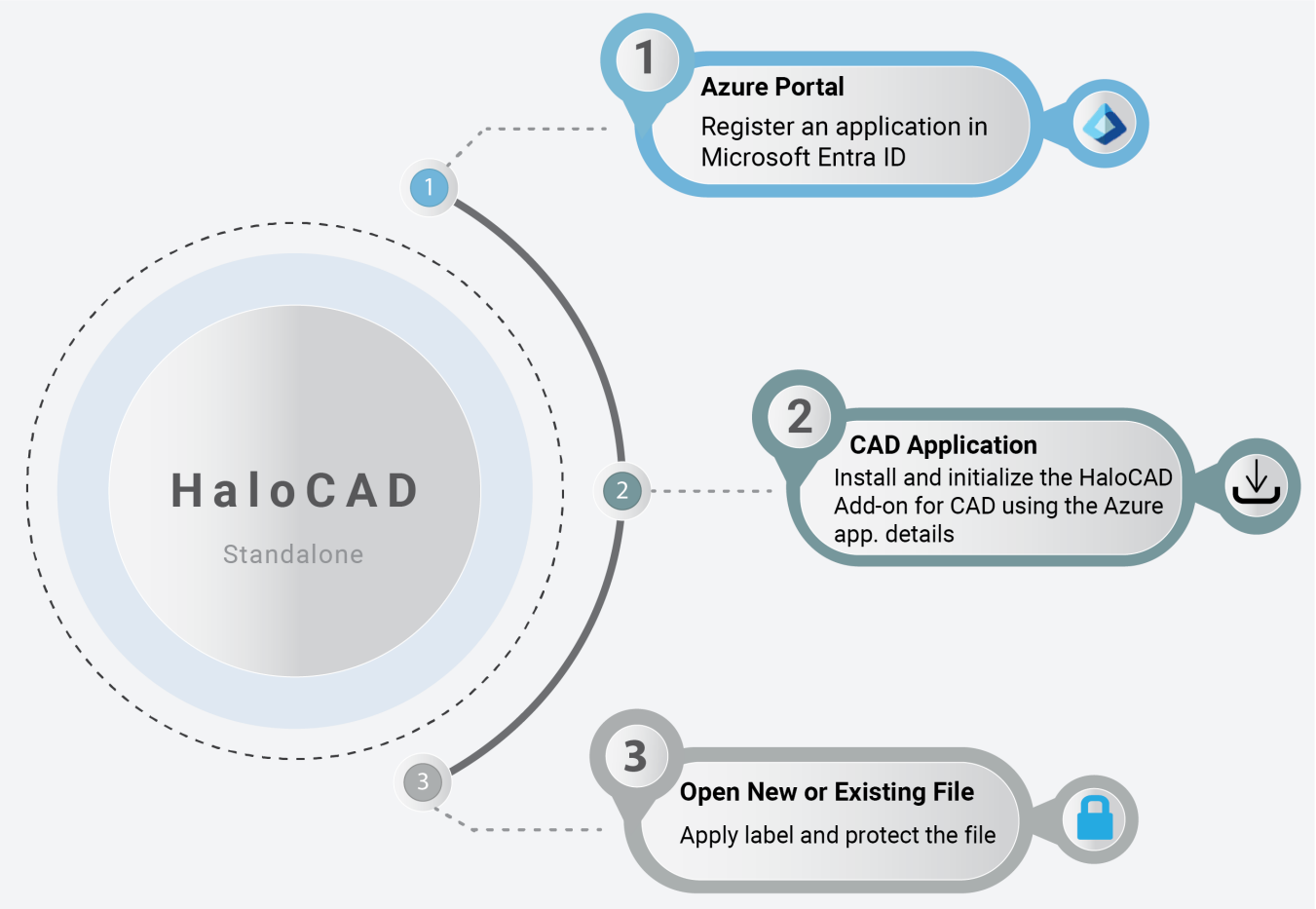
This is the main document that administrators should read before installing the HaloCAD add-on. Following that, read the installation and operations manuals.

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**: Both template-based (or static) labels and user-defined (custom permissions) labels are integrated for seamless protection.
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.

2. Quick Start Installation Summary

The following image shows the high-level idea of setting up HaloCAD.



HaloCAD quick start installation steps

2.1. Reference Manuals

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

For information on	Name of the Reference
1. Prerequisites 2. The architecture of full and reader modes 3. Activate license using various methods 4. Secure installation using the HaloCAD Admin Utility Tool 5. Actions should be taken when a license expires	Please refer to the current manual.
How to install HaloCAD Add-on.	Refer to the Installation Manual for the add-on you purchased.
HaloCAD features and troubleshoot if you face any issues.	Refer to the Operations Manual for the add-on you purchased.
What's new, fixed, and known issues.	Refer to the Release Notes for the add-on you purchased.

HaloCAD documentation

3. HaloCAD Architecture

HaloCAD is available in three variants:

HaloCAD Add-on for CAD—A standalone solution that contains the HaloCAD PROTECT feature. It enables CAD applications to use MPIP directly with user interaction.

HaloCAD for PLM—This solution includes HaloCAD PROTECT and MONITOR capabilities and interacts with the respective PLM application. HaloCAD for PLM actively monitors file access, upload, and download events while running in the background. During a file upload, HaloCAD examines to see if the file is already encrypted, and if so, it decrypts and then allows the file to get check-in to the PLM Vault. In the event of a file access/download, the selected file is automatically protected. HaloCAD operates independently throughout the check-in and check-out process following the rules stated in the Classification Engine.

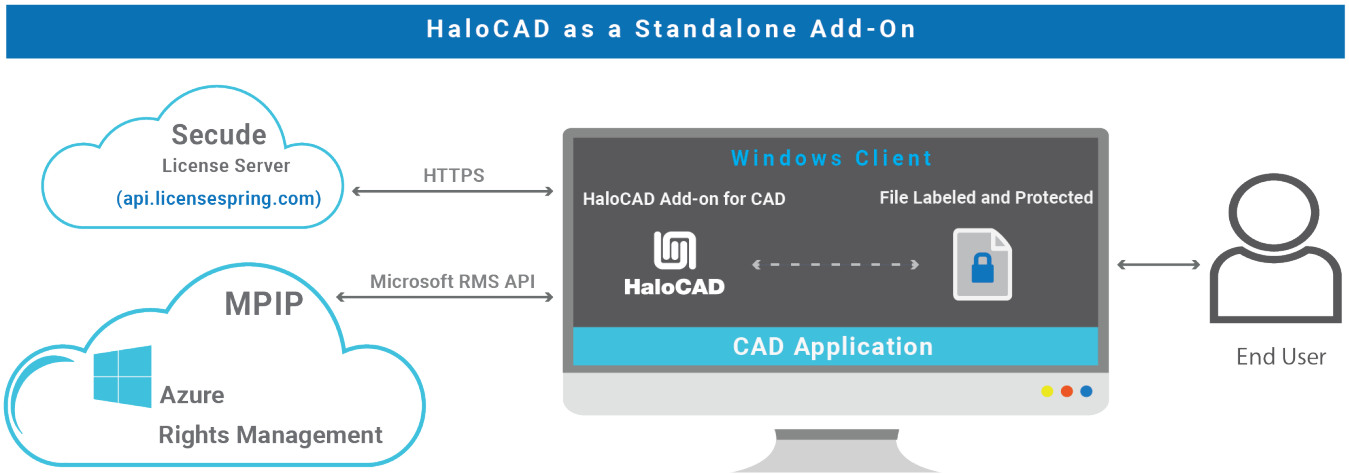
For comprehensive details, please refer to the respective manuals as per your PLM environment:

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

HaloCAD Extension—HaloCAD extends its support to read the MPIP-protected files through a free-of-charge standalone HaloCAD Reader Add-on.

3.1. HaloCAD Add-on for CAD

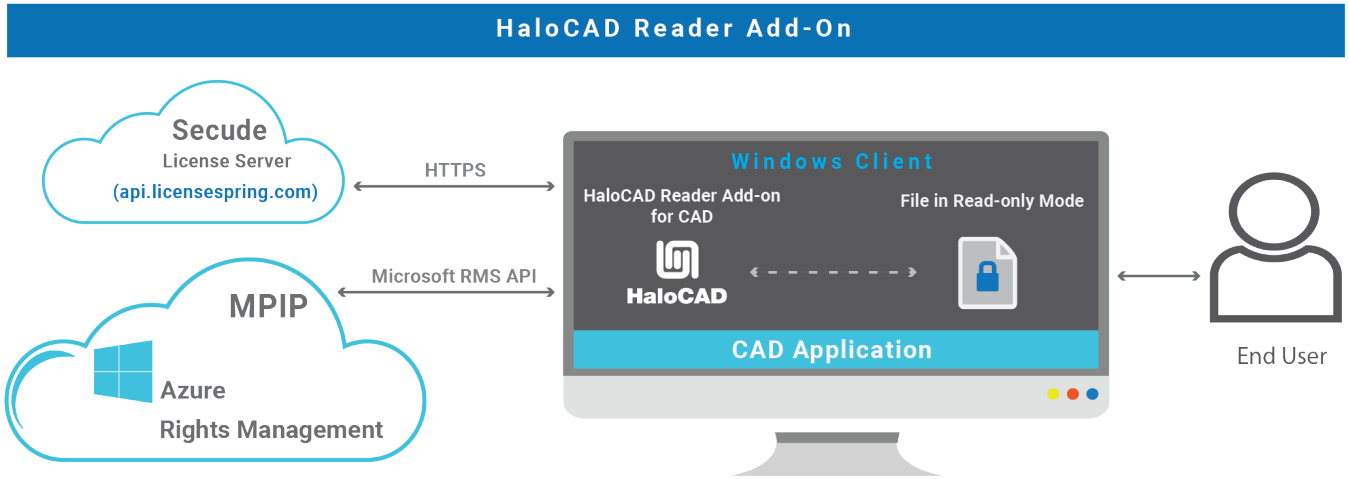
HaloCAD Add-on for CAD leverages Microsoft Purview Information Protection solution to provide persistent document security. During the process of creating a new CAD file, the user downloads MPIP labels using valid credentials, selects a suitable label, and applies it to the file. In the standalone add-on, there is no automation available here as setting labels takes place manually. Protected files can only be opened and modified by authorized users and thus, protection remains even when the file is accessed by multiple users. 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

3.2. HaloCAD Reader Add-on for CAD

Secude offers a standalone reader add-on for the CAD application that allows you to 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. The following figure shows the HaloCAD Reader Add-on for CAD. Note: When a HaloCAD MPIP-protected file is shared with partners/suppliers, they don't need to install HaloCAD Add-on for CAD on their machines, instead just this simple reader add-on is sufficient.



HaloCAD Reader Add-on for CAD

Microsoft documentation

This manual assumes that you already have a complete setup of Microsoft Purview Information Protection and you 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.

4. Prerequisites

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

4.1. Register an Application in Microsoft Entra ID

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

Microsoft documentation

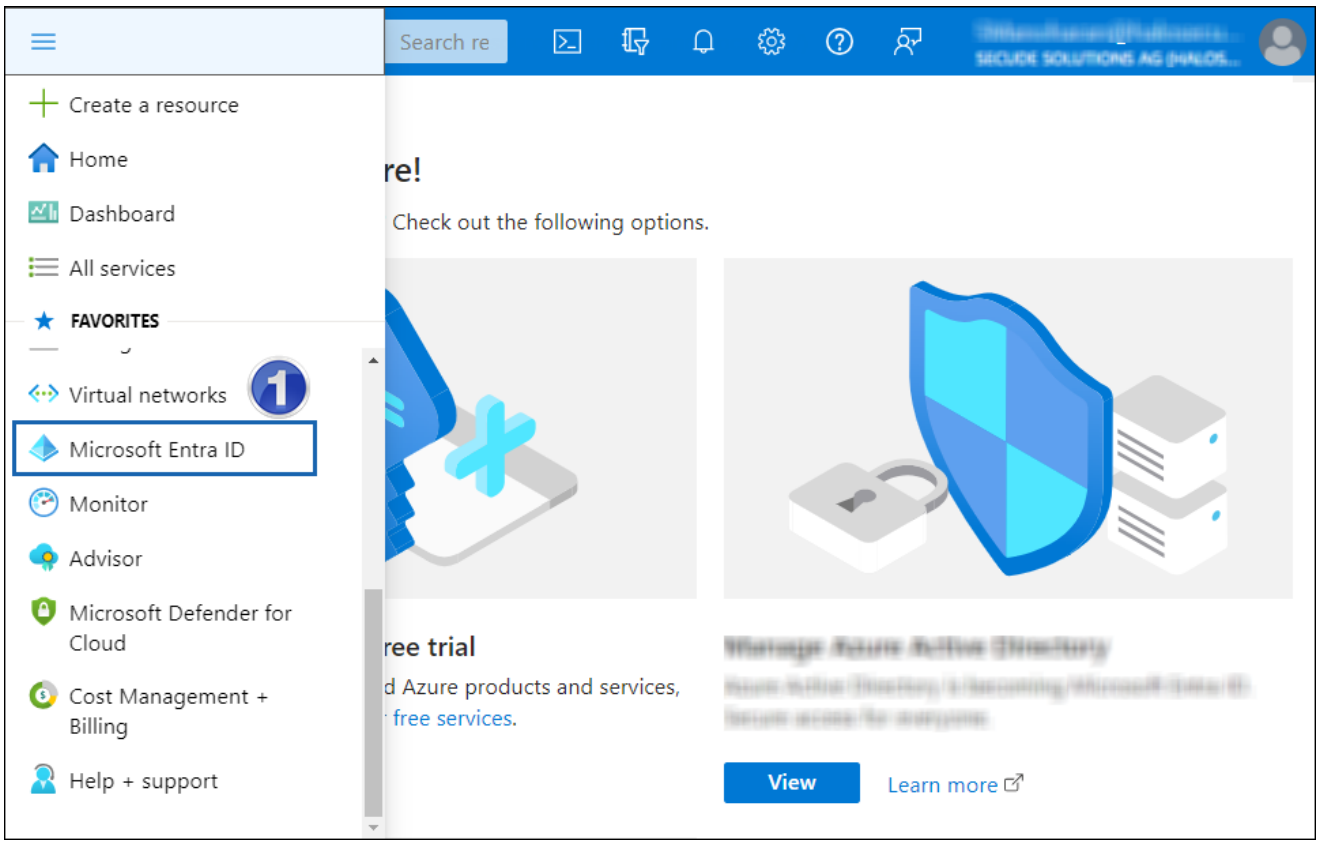
Any application to authenticate via Microsoft Entra ID must be registered in its directory. The information in the Microsoft documentation overrides any information published in this section. Please refer to Microsoft documentation for a comprehensive description.

For demonstration purposes, an application is created in the Azure portal; alternatively, you may create an application using https://entra.microsoft.com.

4.1.1. Create an Application

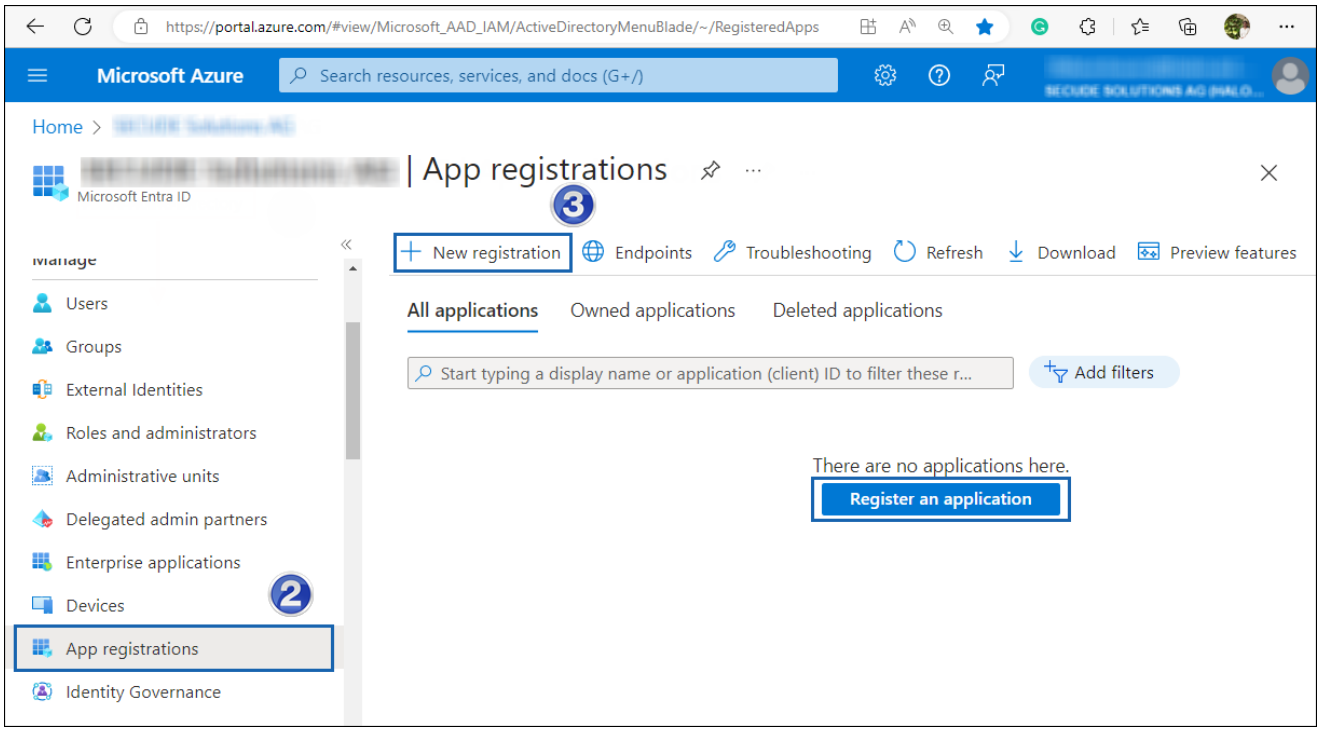
Follow the instructions below to register an application:

1. Sign in to the Microsoft Azure portal using an account with administrator permission.
2. On the portal's **Home** page, under Azure services, or on the left side of the navigation pane, choose **Microsoft Entra ID**.



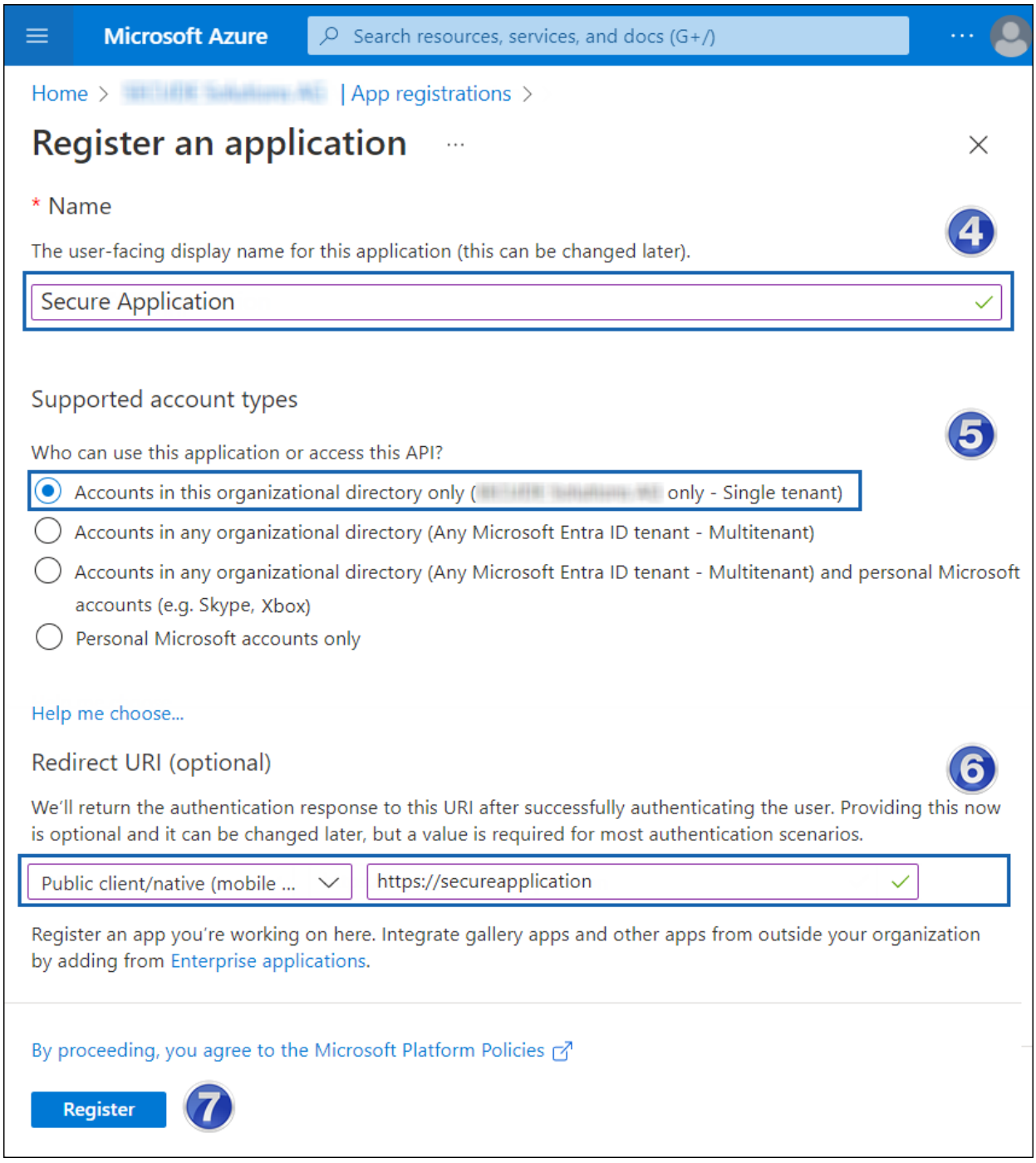
Selecting Microsoft Entra ID

3. On the **Overview page**, in the left navigation pane, click **App registrations**.
4. On the App registrations page, select **New registration** or **Register an Application** (this button appears only if no applications have already been created).



New application registration

5. On the **Register an application** page, enter your application's registration information.



Public client application details

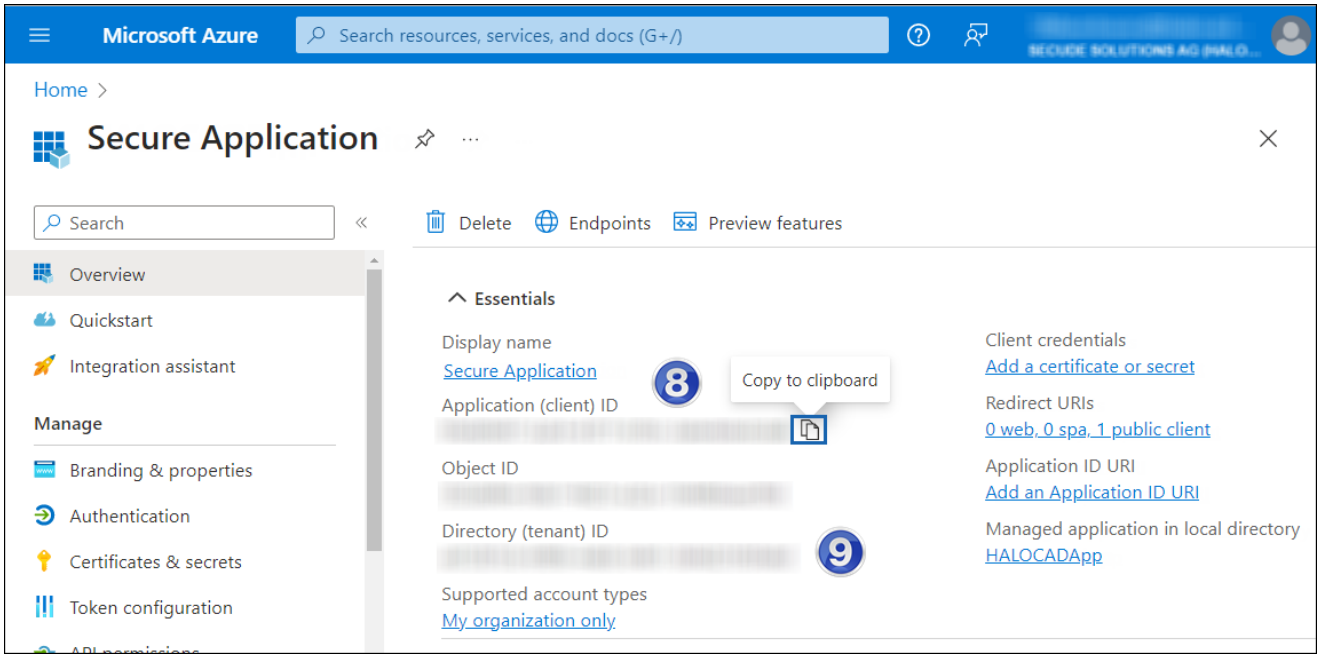
6. In the **Name** section, enter a meaningful application name.
7. Under **Supported account types**, select which account you would like your application to support. For detailed information on these types, please see Microsoft documentation.
   a. To target only accounts that are internal to your 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**.

8. Under **Redirect URI**: Select **Public client/native (mobile & desktop)**, and then type a valid redirect URI for your application. For example, `https://localhost`.
9. When finished, click **Register**.
10. An overview page for the new application registration is created and displayed.



Application ID and Tenant ID

11. The following values are shown on the portal once registration is complete. To copy and save the ID value in a text editor, hover your cursor over it and click the **Copy to clipboard** icon.

a. **Application ID** – It is also referred to as **Client ID**.

b. **Directory ID** – It is also referred to as **Tenant ID**.

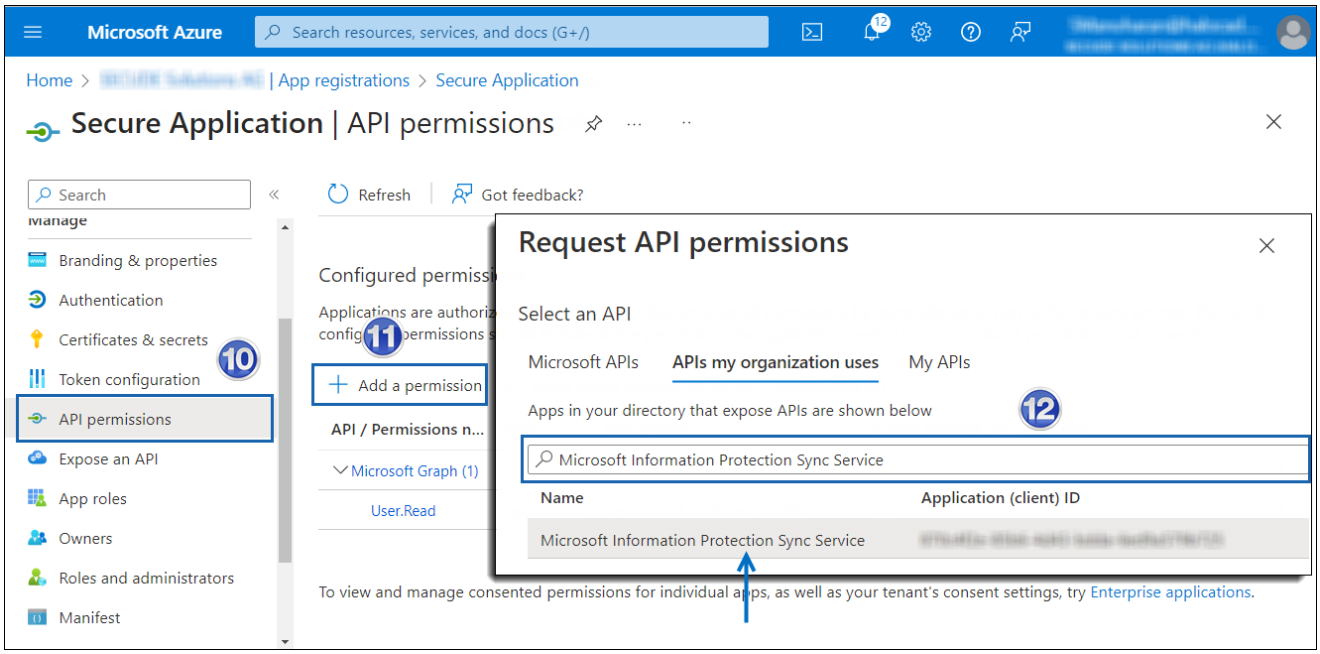
Save the authentication parameters

In a text editor (such as Notepad), copy the values of **Application (client) ID**, **Directory (tenant) ID**, and **Redirect URI**, and save it for initializing the HaloCAD application. Directory (tenant) ID is needed only for single-tenant applications.

4.1.2. Add Required Permissions

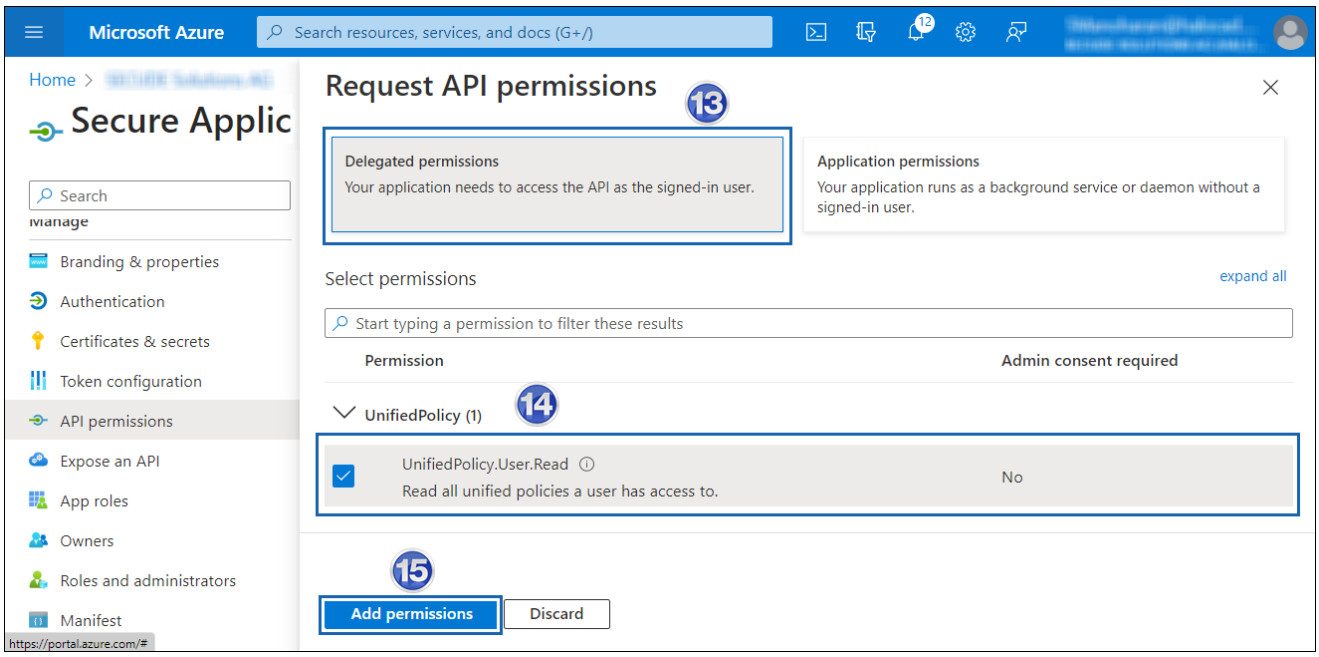
To protect content using MIP SDK, you need to provide the following API permission(s) for the created application ID.

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 below table “Required Permissions”.
5. For example, type "Microsoft Information Protection Sync Service". You can see the API listed as shown in the below figure:



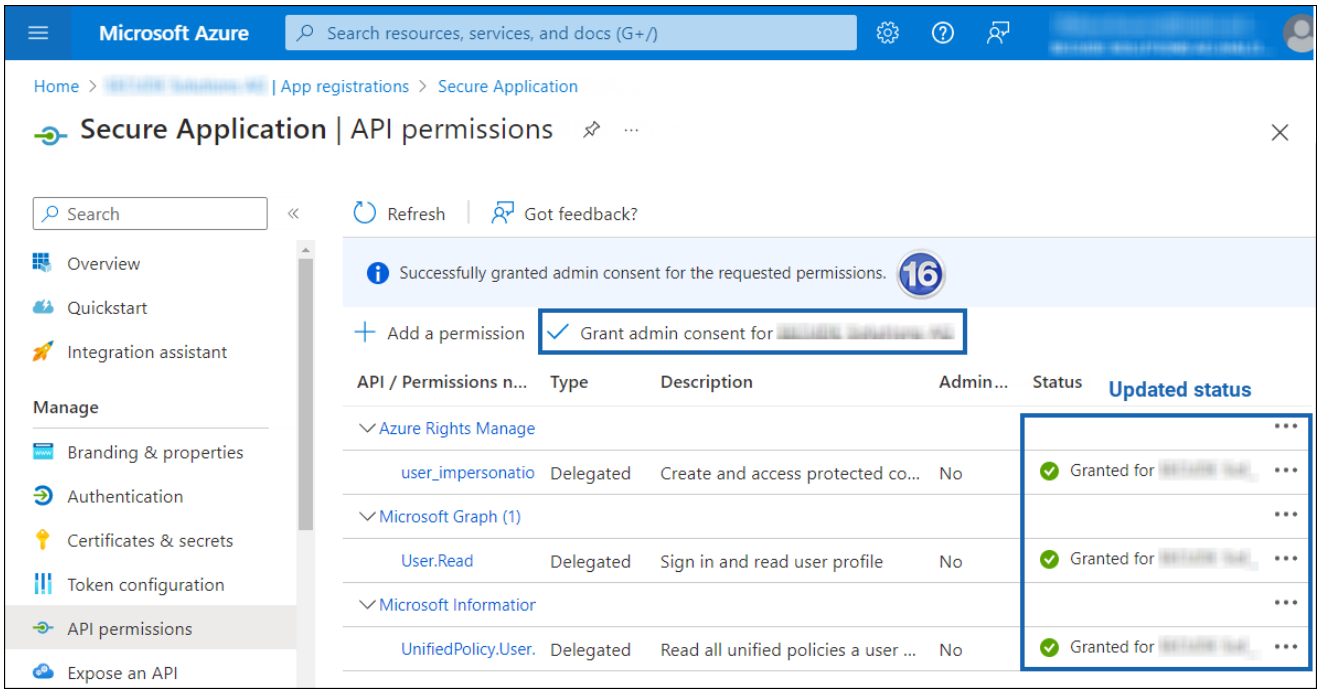
Searching permissions

6. Now, click on the displayed API. You can see two permissions on the page – **Delegated permissions** and **Application permissions**.
7. Click **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. You will return to the API permissions page, where the permissions have been saved and added to the table.



API Required permissions

10. Click **Grant admin consent** for your company button. You will be prompted to accept the consent confirmation; click **Yes** to the question.
11. 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

4.2. Create and Configure the Sensitivity Labels

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

4.3. Office 365 Subscription Details

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

4.4. Recommended URLs, Addresses, and Ports for MPIP

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

Addresses	Ports
`*.protection.outlook.com` `40.92.0.0/15`, `40.107.0.0/16`, `52.100.0.0/14`, `52.238.78.88/32`, `104.47.0.0/17`, `2a01:111:f403::/48`	TCP 443
`*.aadrm.com`, `*.azurerms.com`, `*.informationprotection.azure.com`, `ecn.dev.virtualearth.net`, `informationprotection.hosting.portal.azure.net`, `*.office.com` (add `substrate.office.com` if you don't want to add all sub-domains), `crl3.digicert.com`, `crl4.digicert.com` .	TCP 443
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

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

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

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

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

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

Microsoft documentation

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

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

In summary, the following steps must be performed:

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

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

Registry entries

5. License Activation

A license for a product is necessary for access to features and support, legal compliance, security, and reliability. The primary Secude licensing method uses a Key-based license that regulates and allows access to the application's features. Therefore, to enable features, we suggest obtaining the license key from Secude support before installing HaloCAD.

Key-based License

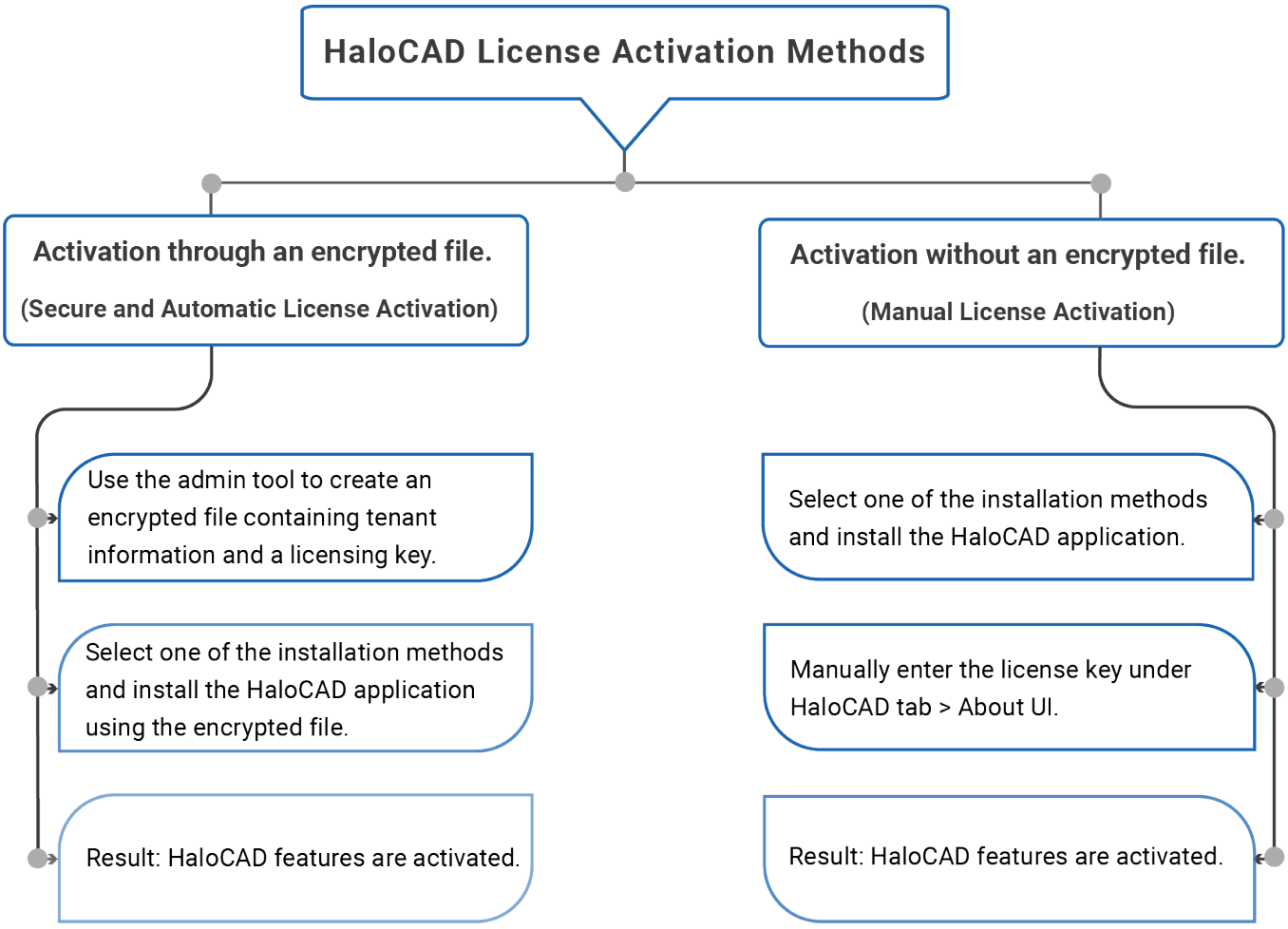
Upon purchase or registration with Secude, a special "license key" is provided to the user to control the use of the application. The license key, which is an alphanumeric code, must be provided by the administrator when the application is installed or activated. By entering this key, the entire functionality of HaloCAD is unlocked, and the user's authorization to use it is validated.

> 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 includes generating an encrypted configuration file with the license key and Azure application details. Using this file, the installer will complete the installation, application initialization, and license activation automatically. Refer to the section "Secure Installation" for more information.
2. **UI-based manual license activation**: This provides a straightforward installation method without automatic license activation. The license must be manually activated by the administrator. Refer to the section "UI-based Manual License Activation" for more information.
3. **License activation through silent mode command line parameters:**
    a. Uses the encrypted configuration file to initialize the application and activate the license automatically.
    b. Installation without the configuration file, in which the application is initialized and the license is manually activated.
    c. For additional information on silent mode, see the section "Silent Mode" in the HaloCAD Installation Manual.
4. **License activation via System Center Configuration Manager (SCCM)**: For deploying and activating the HaloCAD add-on throughout an organization, an encrypted configuration file (containing the license key information and Azure application details) is used together with the installer. Refer to the section "System Center Configuration Manager" for more information. 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

6. Secure Installation (Recommended)

As a best practice, any application secrets should not be shared with end-users, third parties, or any trusted vendors. However, to avail of HaloCAD features (standard add-on and reader add-on) there is a need 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 Azure application specifics (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

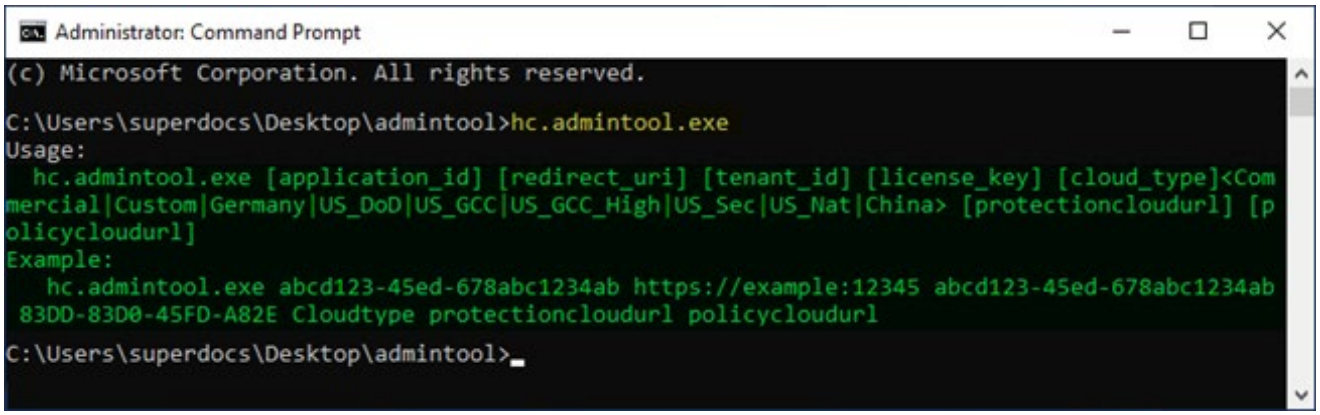
The HaloCAD product package comprises an additional component—`hc.admintool.exe`.

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

1. Azure application details for initialization
2. Cloud type details
3. A license key

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 command

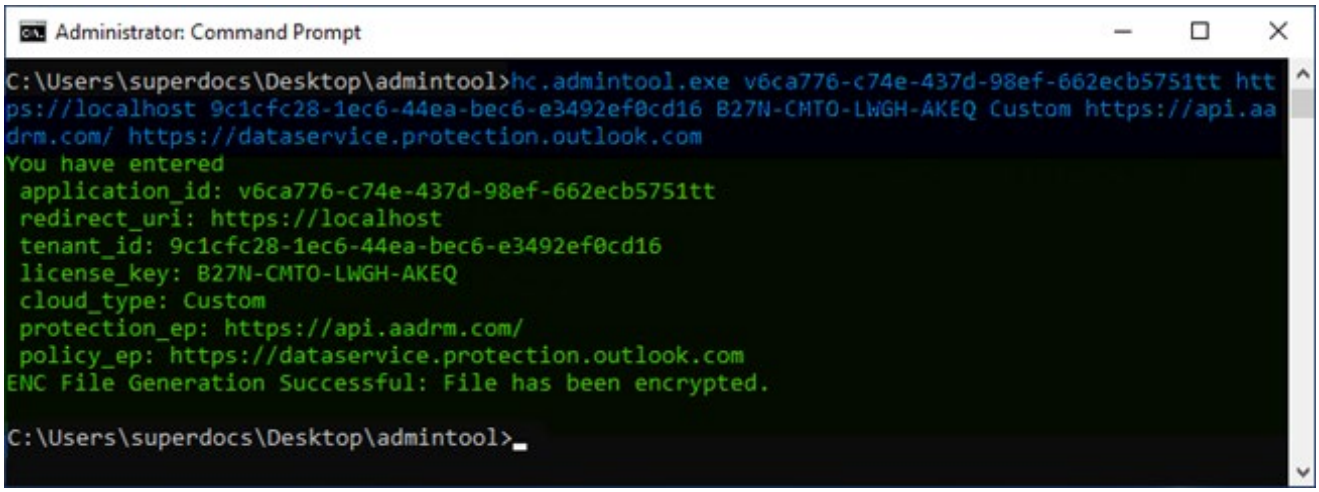
4. Enter the required details. For example,

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

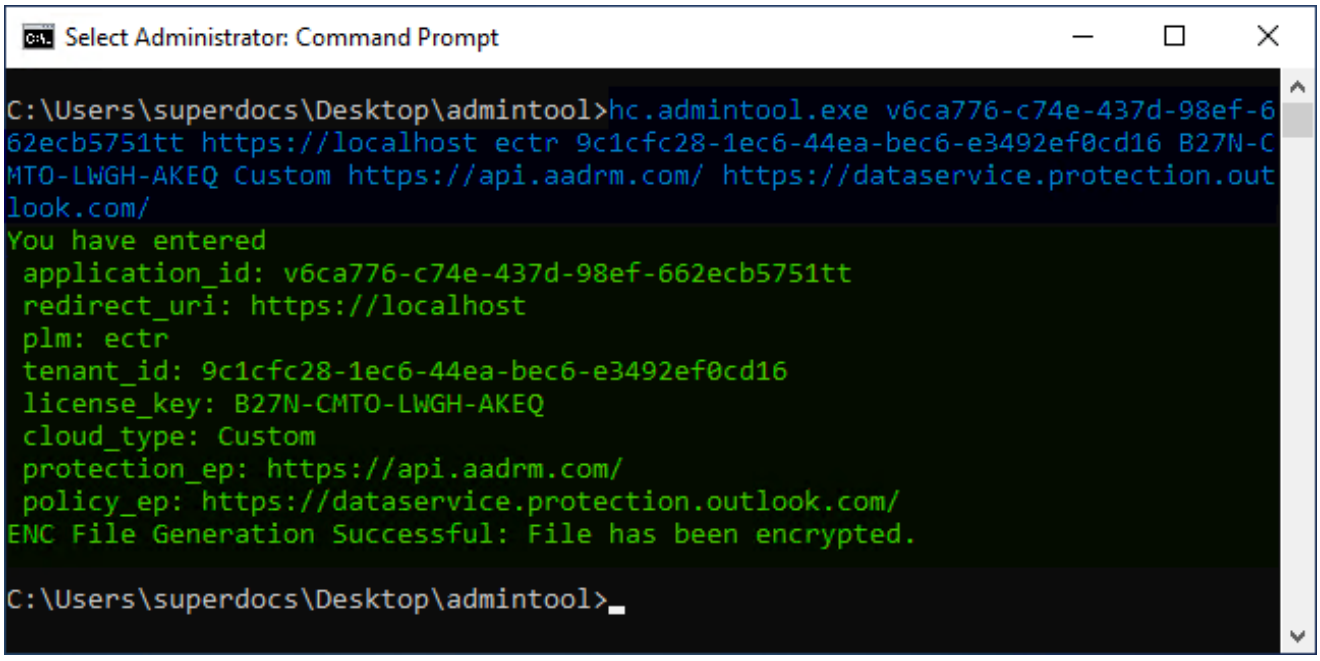
   Cloud type: US_DoD - `hc.admintool.exe v6ca776-c74e-437d-98ef-662ecb5751tt https://localhost 9c1cfc28-1ec6-44ea-bec6-e3492ef0cd16 B27N-CMTO-LWGH-AKEQ US_DoD`

   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 look as follows:



Admin tool output



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

Results:

a. The JSON file `hc.conf.json` will be replaced by an encrypted file `hc.conf.enc`.

b. Now, you can share the configuration file with external users. Using this file, users can install the HaloCAD add-on on their workstations seamlessly with no additional details.

c. Always make sure to create the configuration file using the `hc.admintool.exe` that is included in the installation package. Any configuration file created by prior releases will not work.

What to do next

1. Place the encrypted file `hc.conf.enc` along with the HaloCAD installer.
2. To begin the interactive installation, double-click the installer and follow the instructions as mentioned in the Installation Manual of your purchased add-on.
3. By reading data from the `hc.conf.enc` file, the installer activates the license and bypasses the "Initialization" screen where it would ask for Azure details.

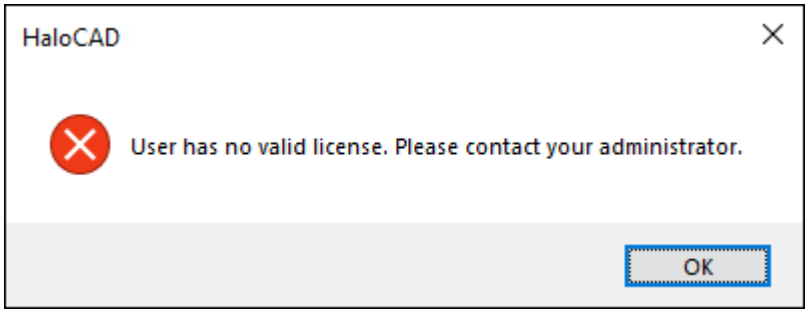
7. UI-based Manual License Activation

This section describes how to activate a license using the HaloCAD user interface.

Prerequisite: Make sure that the HaloCAD installation is complete as explained in the section “Graphical Mode”.

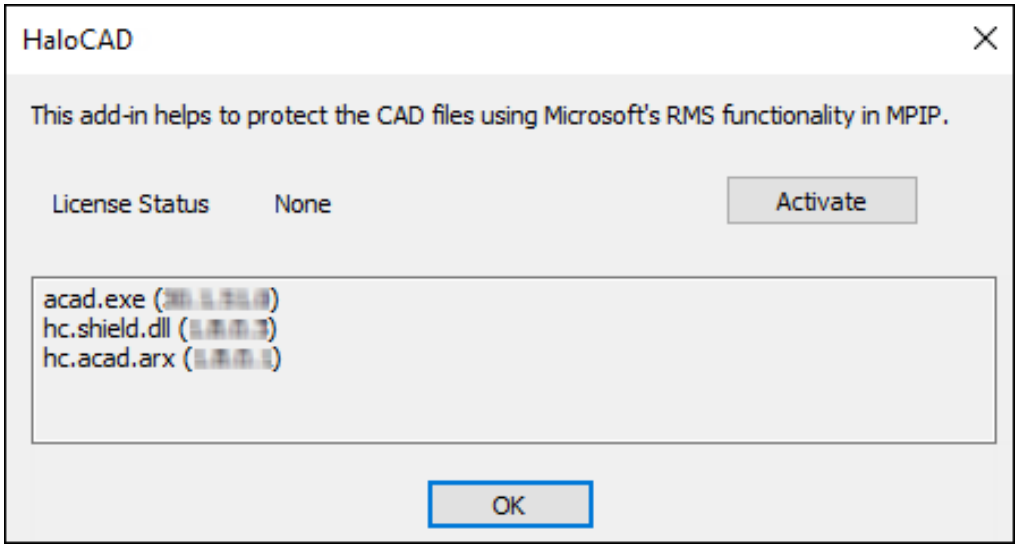
To complete the license activation, carry out the following steps:

1. Open the CAD application.
2. HaloCAD programmatically sends a license validation request to Secude's License Manager, and the following warning message appears:



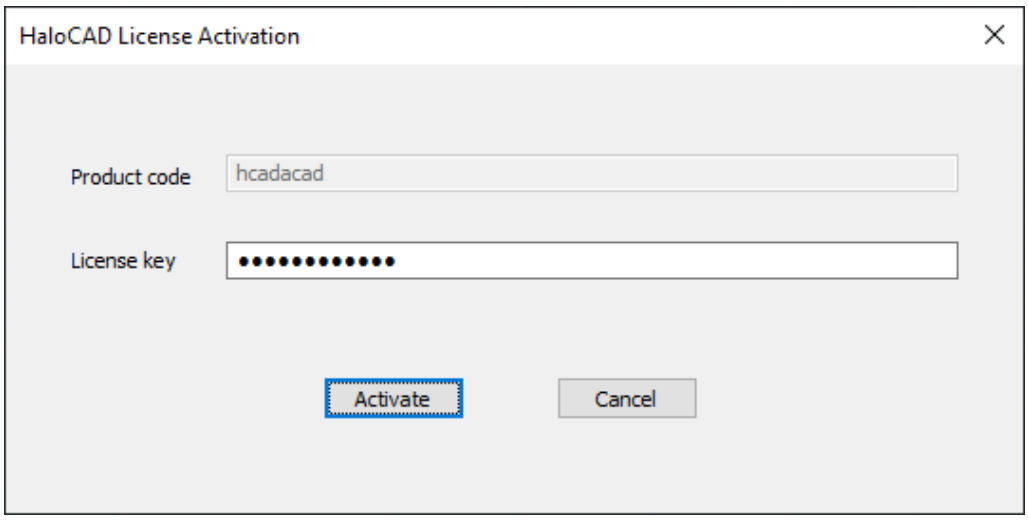
HaloCAD license warning message

3. Click **OK**.
4. Go to the **HaloCAD** tab and click **About** to see the status of your license. Note: If **None** is displayed, your license has not yet been activated.



License status - None

5. Click **Activate**.
6. The *HaloCAD License Activation* screen will appear.

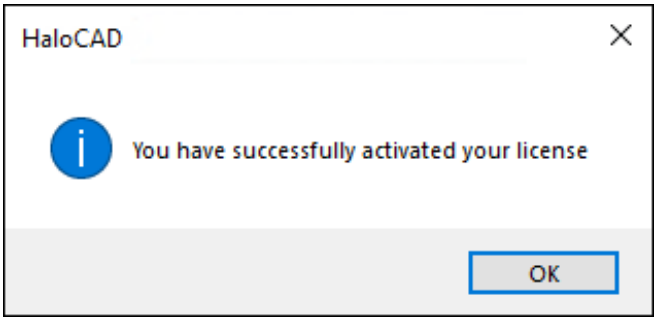


HaloCAD activation screen

7. Enter the license key provided for the standard add-on. Ensure that you enter the license key given for the reader add-on when using the reader add-on. Interchanging license keys results in activation failure.
8. Click **Activate**.

   Results:

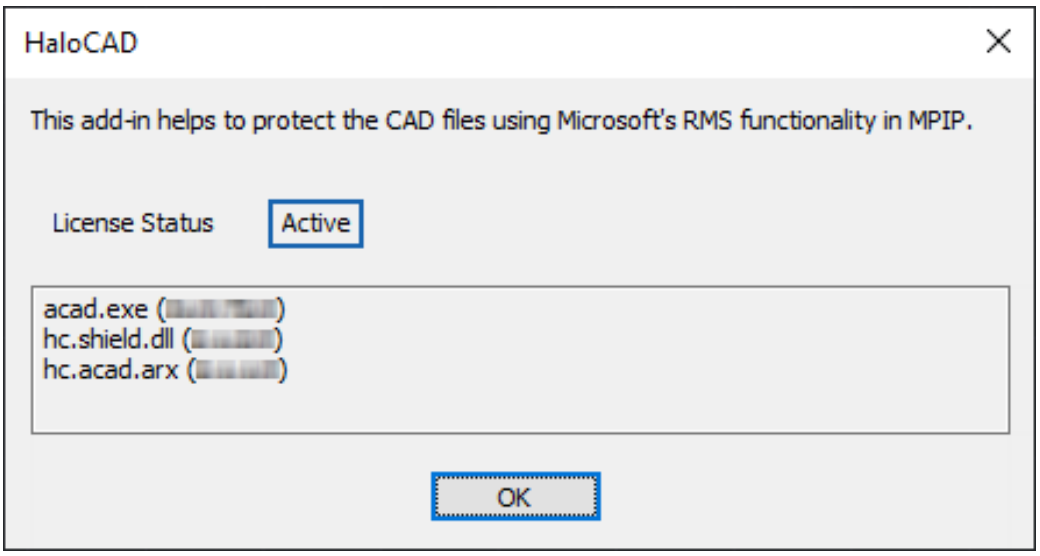
   a. You will receive the below confirmation message:



Activation success message

   b. Click **OK**.

   c. As a result, the **License Status** in the **About** screen will become **Active**.



License status - Active

Related tasks:

a. If you click on the pencil icon (**Click to change label**) to label the file, HaloCAD will prompt you about the **Microsoft Sign-In Assistant**. Click **OK** and sign in with your credentials.

b. After successfully authenticating, the labels can be retrieved from the Azure RMS, and the HaloCAD Ribbon is activated. For more details, please refer to the Operations Manual.

8. License Expiry

The license will expire once the date is reached, and launching the CAD application will result in the following HaloCAD warning message: "*The license is invalid.*" After clicking **OK**, you will get another warning message stating *"User has no valid license. Please contact your administrator"*. Therefore, you must acquire a new license to renew it.

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.

   Results:

   a. The HaloCAD license key is now automatically activated.

   b. 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.

   Results:

   a. The HaloCAD license key is now manually activated.

   b. You can start protecting CAD files.

9. Appendix

Open-source Software

Third-party software/code is included or bundled with Secude's products according to its appropriate license. Secude conducts testing to make sure the third-party products are compatible with and perform as intended with Secude applications. The third-party libraries and dependencies used by the 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	4.59.0	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
MIP SDK	1.15.94	https://learn.microsoft.com/en-us/information-protection/develop/version-release-history	https://docs.microsoft.com/en-us/information-protection/develop/
Licensespring	7.28.1	-	-

Open-source software

Index

Secude

www.secude.com

About Secude

Secude, a Microsoft and SAP Partner, is a global leader for Zero Trust Data-centric security and Enterprise Digital Rights Management (EDRM) solutions.

For more than 25 years Secude has been trusted by many Fortune 500 and DAX-listed companies for architecting, implementing, and protecting their data. Our data-centric security professionals apply their passion and deep domain expertise to provide a holistic approach to protect priceless Intellectual Property (IP) in CAD & SAP based collaborations and supply chains.

With branches in Europe, North America and Asia, Secude supports customers with the implementation of IT security strategies through a global network.