Secude

HaloCAD

HaloCAD Add-on for Solid Edge

Operations Manual

Version 2.4

Copyright

Contact

Secude Solutions AG

Murbacherstrasse 19

6003 Luzern, Switzerland

Mail: info@secude.com

Support

Web: https://support.secude.com

Mail: support@secude.com

Table of Contents

Typographic Conventions

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

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

1. About this Manual

This manual provides comprehensive guidelines and step-by-step instructions for working with **HaloCAD solutions (Label** and **Protect)**. For information on deployment and configuration, refer to the **Installation Manual** included in the product package.

2. General FAQs

This section answers the most frequently asked questions (FAQs). For additional inquiries, please contact your sales representative or the support team.

1. **What does HaloCAD provide for an organization?**
   HaloCAD solution protects engineering CAD files and enforces security across their entire lifecycle.
2. **How many variants does HaloCAD have?**
   HaloCAD is available in three variants:
   a. HaloCAD Add-on for CAD applications – a standalone add-on
   b. HaloCAD for PLM
   c. HaloCAD Reader Add-on for CAD applications
3. **What is the difference between the HaloCAD Add-on for CAD and the HaloCAD for PLM?**
   HaloCAD Add-on for CAD is a standalone solution for organizations that do not store CAD files in PLM. It enforces protection through user engagement.
   HaloCAD for PLM integrates with the respective PLM application and includes the capabilities of HaloCAD PROTECT and HaloCAD MONITOR. The MPIP label is applied automatically, based on the rules defined in the Classification Engine, without requiring user intervention.
4. **What distinguishes the HaloCAD Reader add-on from the HaloCAD Standalone (full add-on)?**
   HaloCAD Standalone Add-on (Full Version) protects CAD files using Microsoft Purview Information Protection solution. This version is licensed.
   HaloCAD Reader Add-on allows viewing of files protected by the HaloCAD Standalone Add-on. This version is free of charge.
5. **What languages are supported by the HaloCAD add-on?**
   Currently, the HaloCAD add-on only supports English.
6. **Does the HaloCAD Add-on support all native CAD file types?**
   Yes, the HaloCAD Add-on supports all CAD native file types.
7. **What happens if an unauthorized person tries to open a HaloCAD-protected CAD file?**
   The process begins with user authentication, which verifies the user's identity. If authentication fails, an error message is displayed, and access is denied.
8. **Who decides what labels should be used for various CAD drawings and how they are managed in the background?**
   An administrator manages labels (user rights) in the Microsoft Purview portal, while engineers can create profiles, classification schemas, and action rules based on the sensitivity of their data.

9. **What if I don't want a certain file to be protected?**

   If you do not want the file to be protected, you can apply the **“No Protection”** label, which does not include any policy settings.

10. **Can I create my own labels?**

    Yes, HaloCAD allows users to create custom permission labels.

3. How does it work?

This chapter provides a high-level explanation of the underlying processes and interactions between the system components to help you understand how HaloCAD protects sensitive data.

3.1. License Enforcement

After installation, HaloCAD programmatically sends a license validation request to Secude's License Manager when a user attempts to start a session for the first time by opening the CAD application. Based on the administrator's installation method, one of the following scenarios applies:

Case 1:

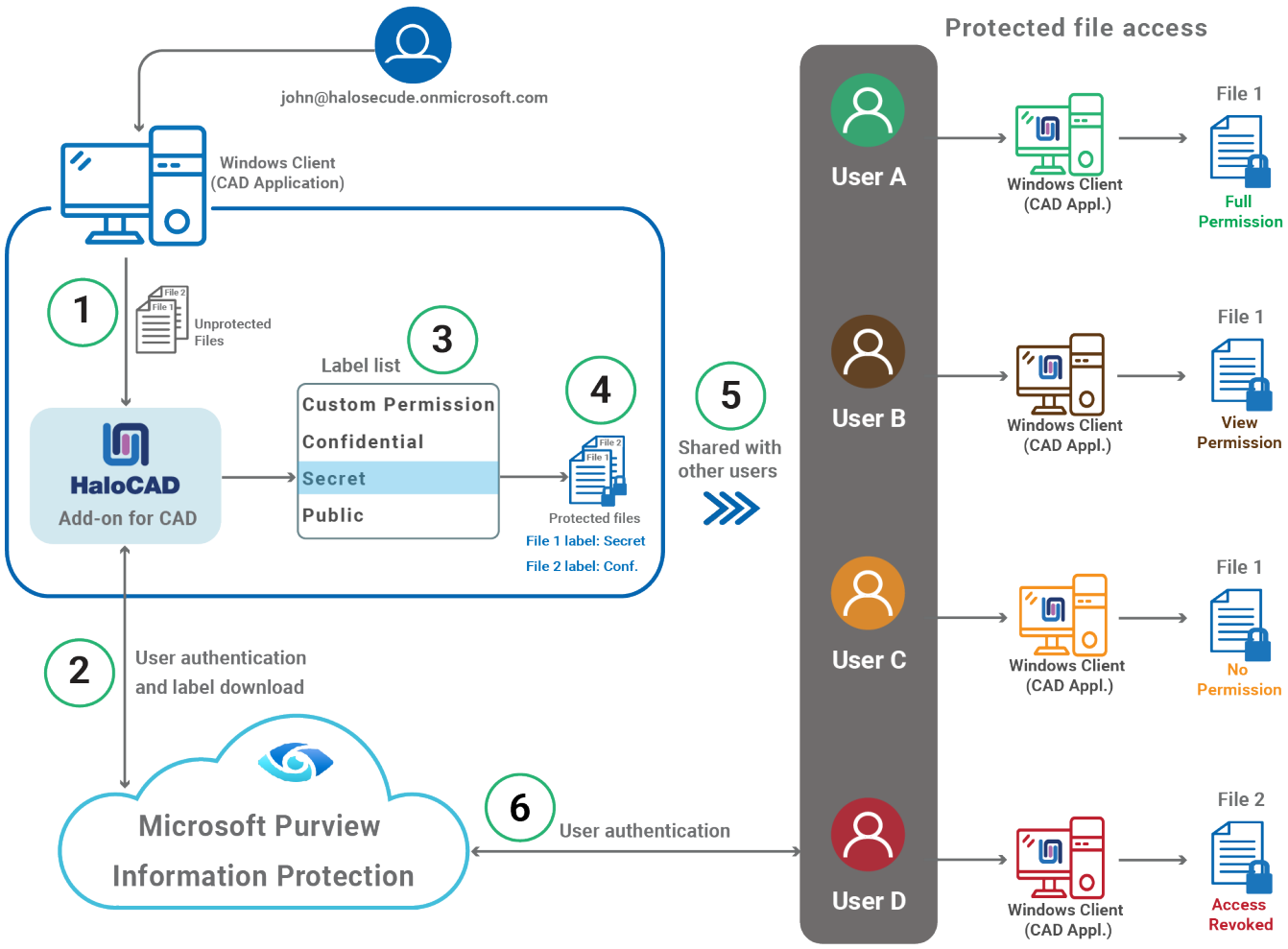
If the license is activated automatically during the installation process, the user can continue using all HaloCAD features without interruption.

Case 2:

If the license has not been activated, the user will receive an error message and will be unable to access HaloCAD features. For information on license activation, refer to the **License Activation** section of the Technical Reference Manual.

3.2. Applying Protection using HaloCAD Add-on

At a high level, HaloCAD workflow involves the following steps:



HaloCAD protection

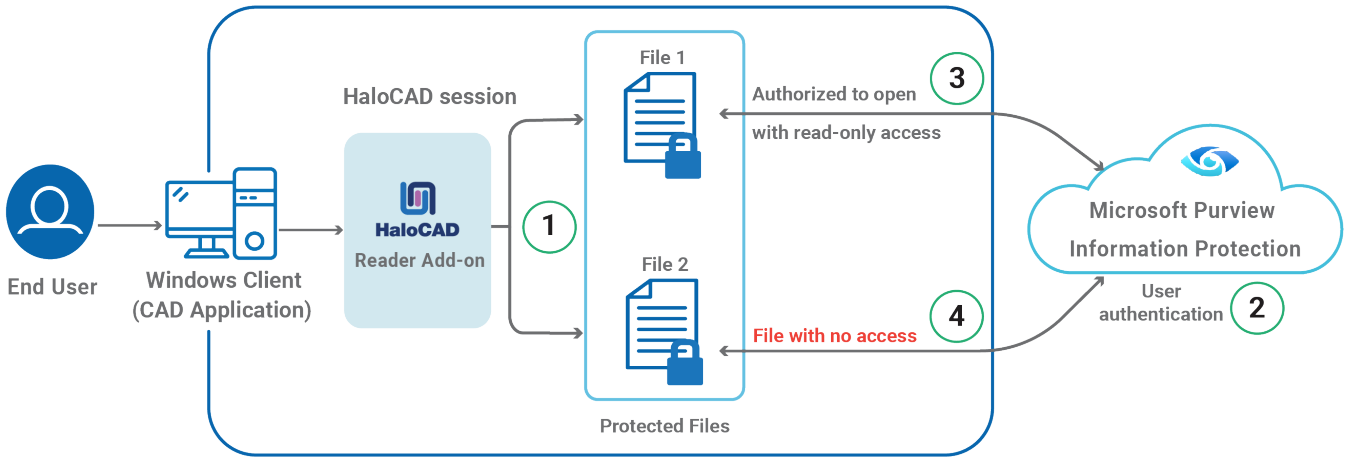
1. To create new CAD files, the user launches the CAD application and logs into the HaloCAD session for the first time.
2. HaloCAD connects to the Microsoft Entra tenant. In this manual, `halosecude.onmicrosoft.com` is used as an example tenant.
   a. Microsoft Entra ID prompts the user for authentication.
   b. After successful authentication, Microsoft Purview Information Protection (MPIP) labels are downloaded for the logged-in user (`john@halosecude.onmicrosoft.com`).
3. File protection: The user (John) selects and applies two different labels to two separate files.
4. HaloCAD enforces document protection based on the selected label. When a sensitivity label is applied, it is stored in the document metadata, and the corresponding protection settings are enforced to secure the content.
5. **File-Sharing**: Assume that `john@halosecude.onmicrosoft.com` shares the files with multiple users. **Users A**, **B**, and **C** receive **File 1**, while **User D** receives **File 2**.

6. Content consumption: Users A, B, C, and D attempt to access the protected files. Microsoft Entra ID authenticates each user, and the file opens upon successful authentication. Access permissions such as **View, Edit, Print, Copy, Export,** and **Change** are granted based on the applied label. Different permission levels may be assigned to individual users or user groups.
   Note: The user who initializes HaloCAD is considered the author and is granted full access rights to the document. For more information on labels, refer to the Microsoft documentation.
   a. File 1 - Full access is granted to `User A@halosecude.onmicrosoft.com`.
   b. File 1 - Read-only (view-only) access is granted to `User B@halosecude.onmicrosoft.com`.
   c. File 1 - `User C@halosecude.onmicrosoft.com` is denied access and cannot open the file.
   d. File 2 - Access was previously granted to `User D@halosecude.onmicrosoft.com` but has been revoked due to risky or suspicious activity.

Logged-in user (HaloCAD session)
In this document, the term “logged-in user” refers to the individual or user account that launches the CAD application and signs in to Microsoft Entra ID through the Microsoft Sign-In application. This may differ from the operating system user currently signed in. Collectively, this is referred to as the “HaloCAD session.”

3.3. Viewing a Protected File Via the HaloCAD Reader Add-on

At a high level, HaloCAD workflow involves the following steps:



HaloCAD Reader Add-on

1. The user selects two files that are protected by HaloCAD.
2. When the user logs in to the HaloCAD session for the first time, a connection to Microsoft Purview Information Protection is required. Microsoft Entra ID authenticates the user.

3. HaloCAD indicates that the files can be opened only in read-only mode. In this scenario, the user is authorized to open File 1.
4. File 2 does not open because the user does not have the required permissions.

By design, saving is restricted once a protected file is opened in a session to prevent protected content from being copied to an unprotected file. HaloCAD shows a restriction message. In a fresh session, unprotected files can be created and saved without any restrictions.

4. Get Started with HaloCAD

This section describes how to protect Solid Edge files, open a protected file, and use the HaloCAD Reader add-on.

4.1. Permission Levels and Usage Rights

4.1.1. Basic Permissions

The following table lists the basic permissions and the usage rights that they contain:

S.No	Permission Level	Usage Rights (Allowed Recipient Actions)
1	View	Open and read the data (also known as “Read-only”). It includes Zoom and view from different angles (for CAD file types).
2	Edit	Edit the file and save it
3	Copy	Extract data (including screen captures) from the file into the same or another file.
4	Print	Print the content
5	Export	Save the content to a different filename (Save As). Also includes “Export to PDF”.
6	Change Rights	Changing the label that is applied to a file includes removing protection and saving it as an unprotected file.
7	Owner (Full Control rights)	Grants all rights to the file and all available actions can be performed. Also includes the following permissions: 1. Remove protection 2. Relabel a file

Basic Permissions

Author (creator) of a file

The author of a file has all the rights and actions mentioned in the above table. Also includes the following permissions:

1. Open file after the expiry date
2. Revoke access

4.1.2. Custom Permissions

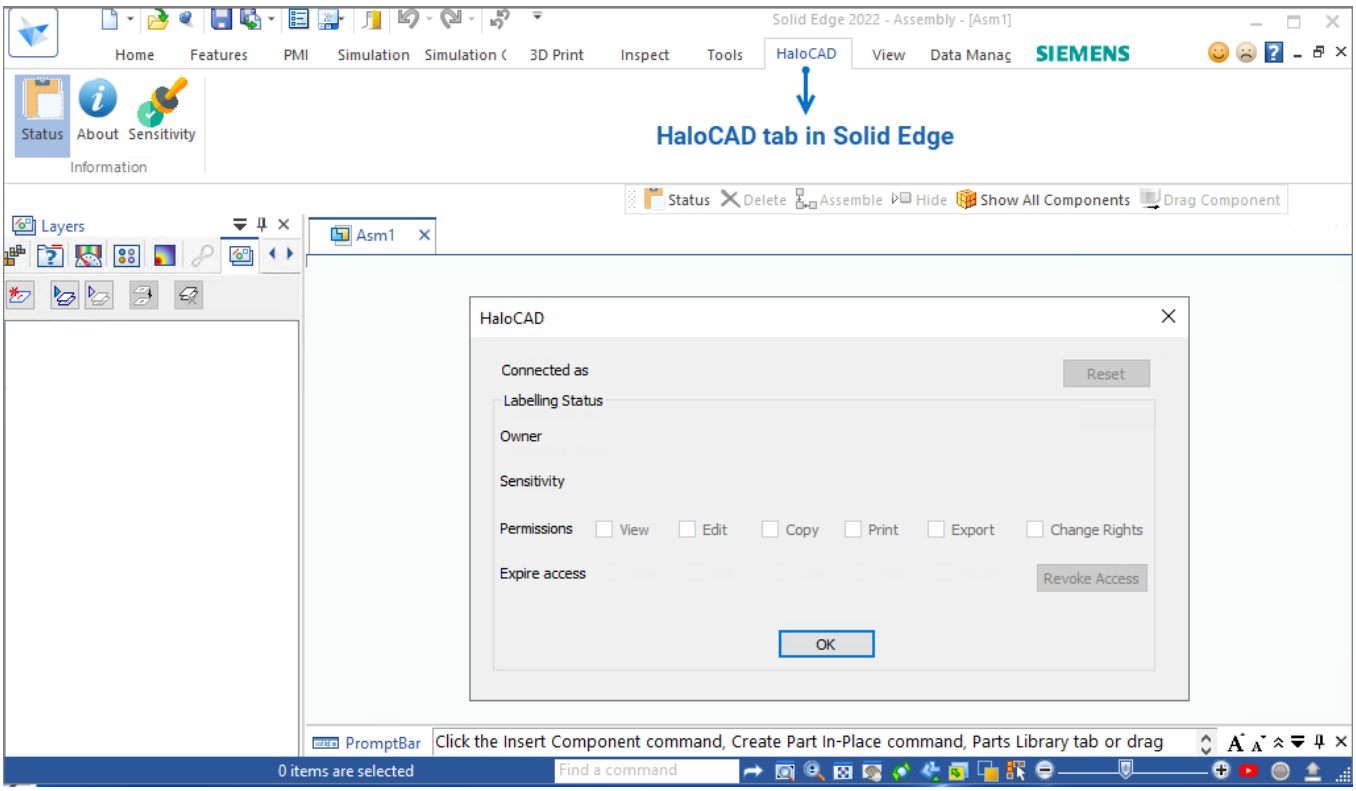
The following table lists the custom permissions and the usage rights that they contain:

S.No	Permission Level	Usage Rights (Allowed Recipient Actions)
1	Viewer	Open and read the data (also known as “Read-only”). It includes Zoom and view from different angles.
2	Reviewer	Viewer’s allowed permissions plus: 1. Edit 2. Save the file
3	Co-Author	Reviewer’s allowed permissions plus: 1. Print 2. Extract data (including screen captures) from the file into the same or another file.
4	Co-Owner	Co-Author’s allowed permissions plus: 1. Export 2. Change Rights
5	Only for me	Grants all rights to the file and all available actions can be performed only by the author of the file.

Custom Permissions

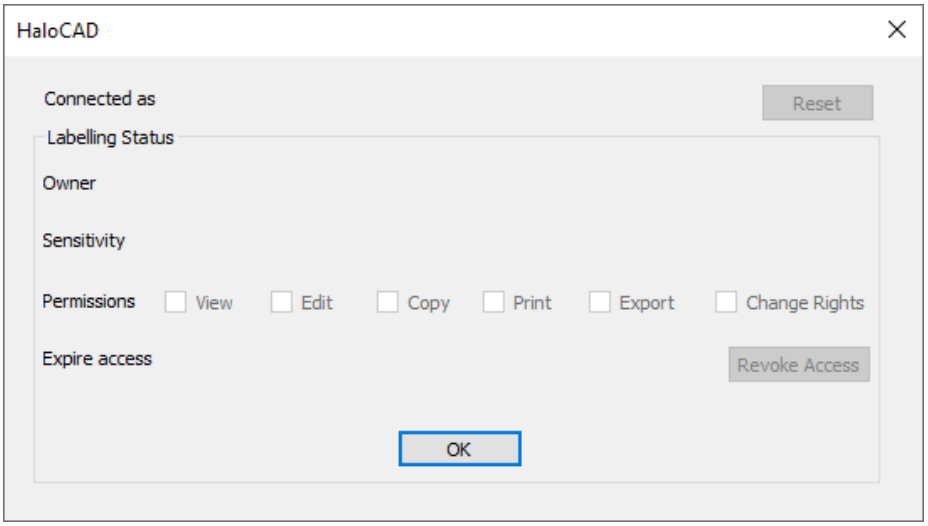
4.2. HaloCAD Screen Introduction

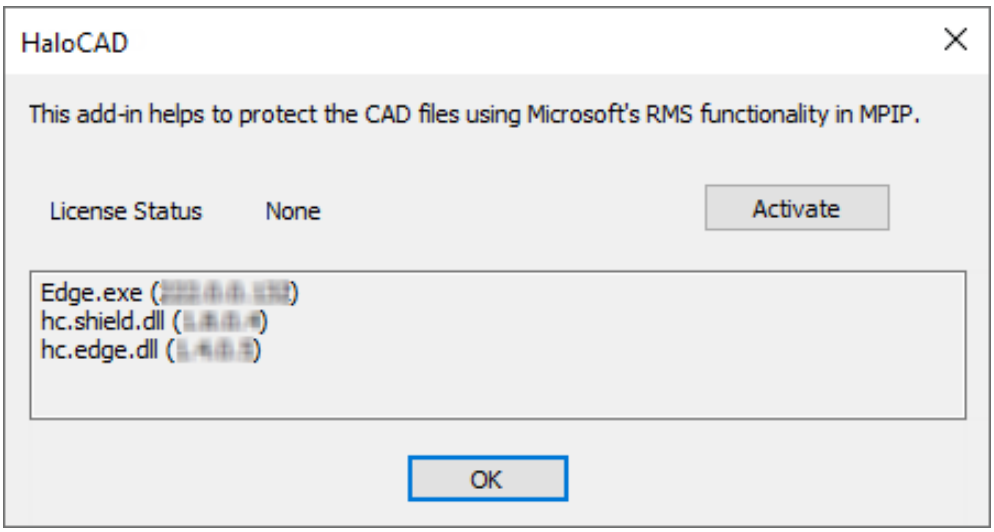
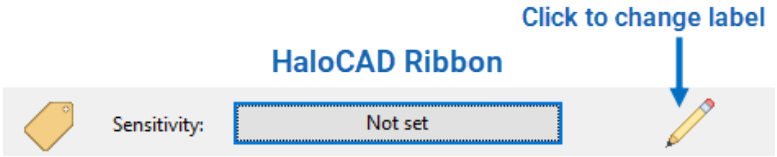
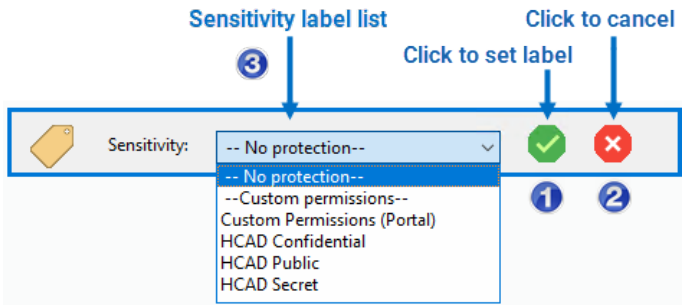
After installing the HaloCAD add-on, the HaloCAD tab appears in the CAD application, as shown in the figure below:



HaloCAD in Solid Edge application

The following table provides a brief description of each HaloCAD menu element.

S.No	Icon	Description
1		The **Status** icon displays the status of the file.  1. **Connected as**: Name of the logged-in user 2. **Owner**: Author of the document 3. **Sensitivity**: Name of the label applied 4. **Permissions**: Rights on the file

S.No	Icon	Description
		5. **Expire access**: Displays the details of how long a user can access the labeled file 6. **Revoke Access** button: Revokes access granted for a protected document 7. **Reset** button: Logs off a user from the current active session. The button will be disabled unless the user logs in again
2		The **About** icon displays the application version and license information. For details on license activation, refer to the “License Activation” section of the Technical Reference Manual. 
3		The **sensitivity** icon enables and disables the **HaloCAD** ribbon.  **Pencil icon** - **Click to change label**: 1. Downloads the available labels. 2. Allows changing an applied label. 

S.No	Icon	Description
		1. **Green check mark - Click to set label** icon - applies the selected label or removes the existing label. 2. **Red cross mark - Click to cancel** icon - cancels the selected label. 3. **Sensitivity** label list - displays the labels.

Overview of screen elements

4.3. How to Protect a CAD File?

Prerequisites

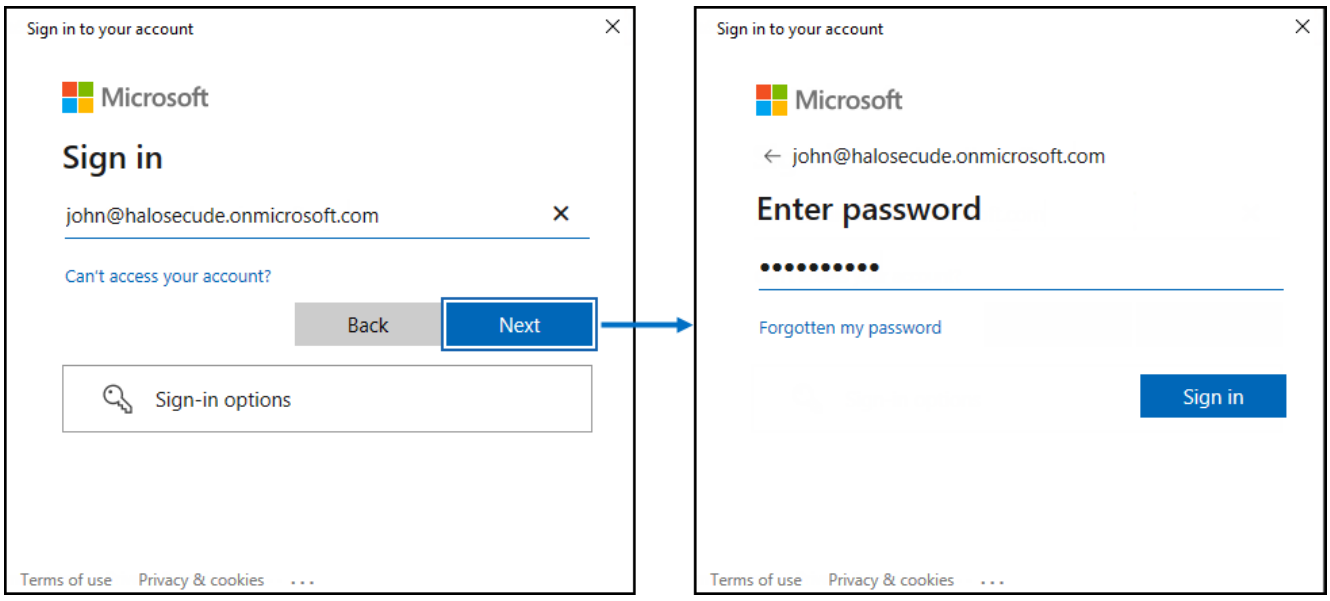
- To protect organizational data by using sensitivity labels, configure protection settings for each label in the **Microsoft Purview portal**.
- To set a default label for documents, configure the following setting in the **Microsoft Purview portal**: Go to **Label policies** > **Settings** > **Documents** > **Default settings for documents** > **Apply a default label to documents**, and then select a label from the list.

To protect a CAD file, perform the following steps:

1. Open the Solid Edge application, and then open an existing file or create a new file.
2. For new or unprotected files, the **Sensitivity** status displays **Not set** if no default label is configured in the policy. If a default label is configured, the configured default label is displayed. In this example, no default label is set.
3. On first login, HaloCAD prompts for **Microsoft Sign-In Assistant** authentication.

Microsoft Sign-In Assistant invoking message

4. Click **OK** and enter your credentials.

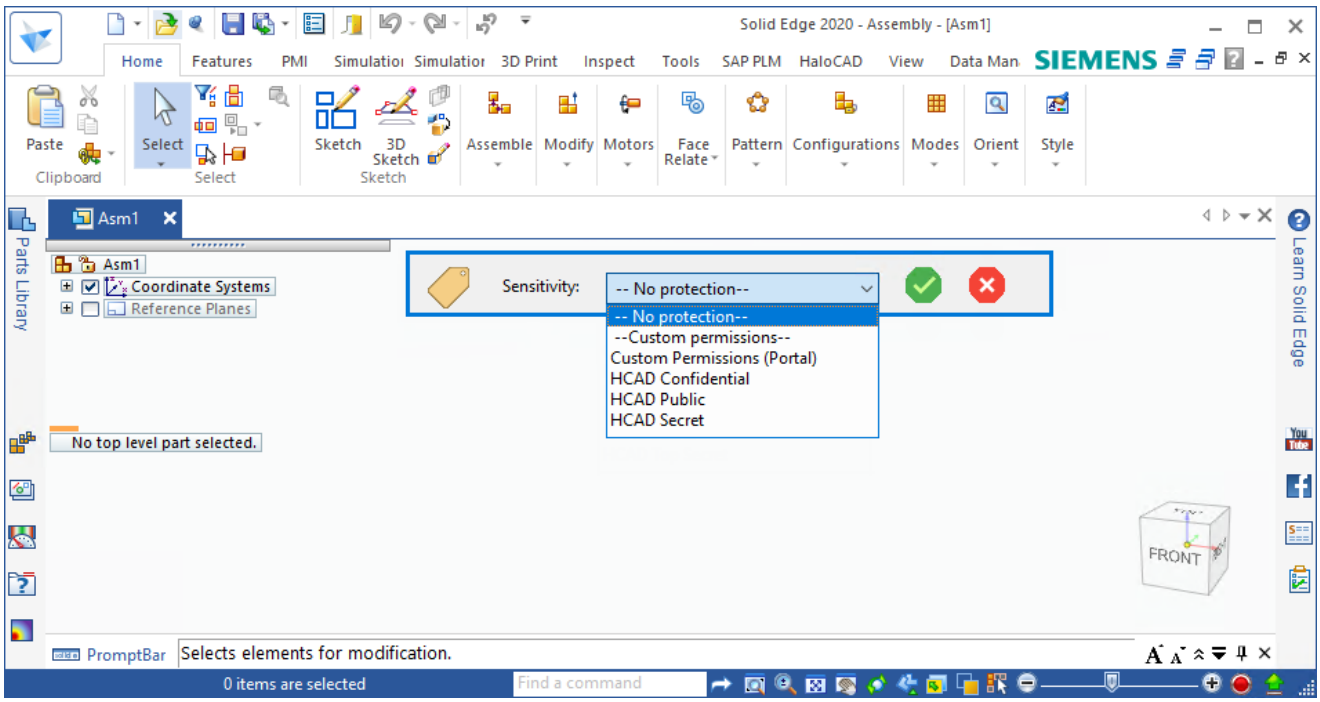


Authentication sign-in prompt

5. After authentication, HaloCAD connects to Microsoft Entra ID and caches the user credentials.
6. Go to the **HaloCAD** tab and click **Sensitivity**.
7. To apply the label to the active document, click the pencil icon (**Click to change label**).
8. A notification appears indicating that labels are being downloaded from Microsoft Purview Information Protection.

Fetching the labels

9. From the **Sensitivity** list, select a label, and then click the green check mark (**Click to set label**) to confirm the selection.

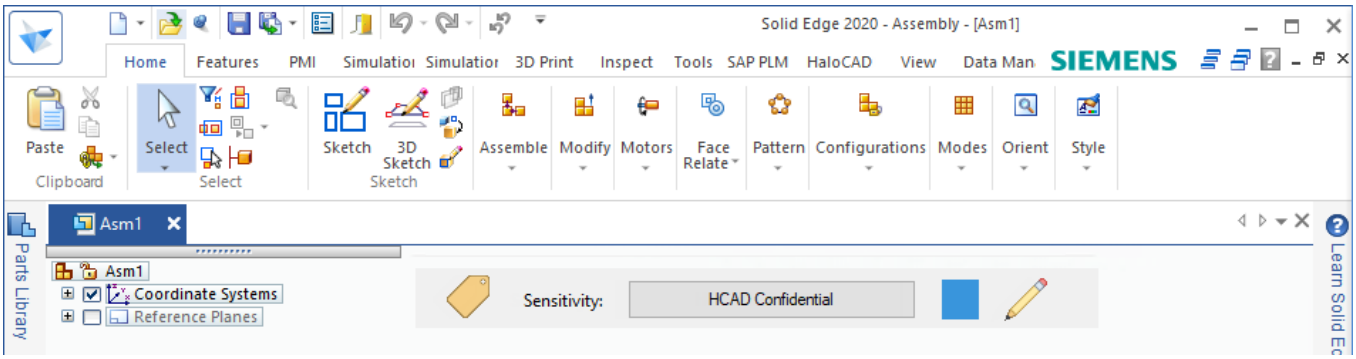


Downloaded labels for the signed-in user

10. For a new file, click **Save** and specify a file name.
11. For an existing file, an additional save action is not required. When the label is applied by clicking the **Click to set label** (check mark) icon, the file is saved automatically.

Result

- The selected label is applied to the active document.
- The selected label is displayed on the HaloCAD ribbon, along with the color configured in the Microsoft Purview portal.
- To clear the credential cache, click **Reset** in the **Status** UI.



File with applied label

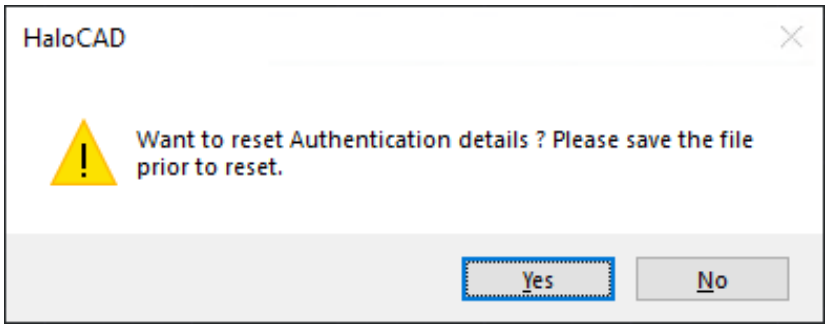
4.3.1. Cancel, Remove, Relabel, and More

1. **Canceling Label Selection**: If you have selected an incorrect label, you can cancel it by clicking the red cross icon (**Click to Cancel**). This will remove only the selected label that has not yet been applied to the file.
2. **Removing Protection**: To remove an existing label and keep the file unprotected, select the **No Protection** label from the list. Note: Whenever you change a label, click the green check mark icon (**Click to set label**) to apply the updated label. The file will be saved, and the label will be applied to the active document.
3. **Relabeling**: If you want to apply a different label or modify protection settings (Custom Permissions) after a label has already been applied, first click the pencil icon (**Click to change label**) and then select a new label from the list. For more details, refer to "Example 9: Custom Permissions Label".
4. **Revoke Access** - If an author does not want a user to access the shared file for security reasons, you can prohibit it by clicking **Revoke Access** in the **Status** UI. Please refer to the section "Example 12: Revoke a File".

4.3.2. Log out an Active User

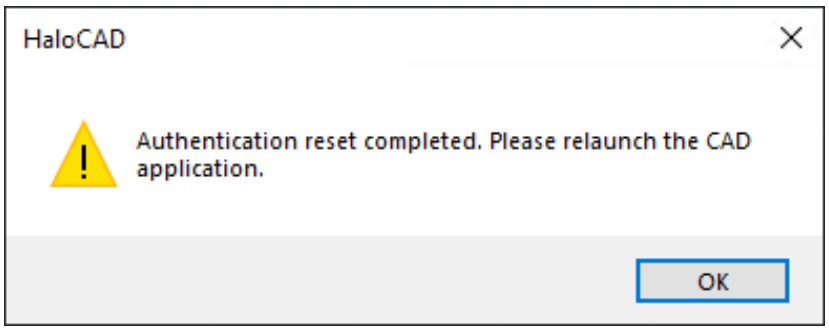
This section describes how to log out the currently active user from HaloCAD. Logging out ends the active session and allows another user to log in.

1. Go to the **HaloCAD** tab > click **Status** > click **Reset**.
2. When the following message appears, click **Yes**.



Clear cached credentials #1

3. When the next message appears, click **OK**.



Clear cached credentials #2

4. Restart the application.

Result

- After relaunching the application, users can log in to a new HaloCAD session using their credentials.
- If you do not relaunch the CAD application, HaloCAD displays the following message: *"For HaloCAD to work properly you should relaunch the application now"*.
- Click **OK**, and then relaunch the application.

Next step

1. **Log in after reset:** After restarting the application, when you open a protected file or click the pencil icon (**Click to change label**), HaloCAD prompts you to use the Microsoft Sign-In Assistant. Click **OK**, and then sign in with your credentials.

Microsoft Sign-In Assistant invoking message

2. For more information about HaloCAD functionality, see **Common scenarios**.

4.4. How to Export a Protected CAD File to a PDF File?

To convert / export / save a protected file as PDF:

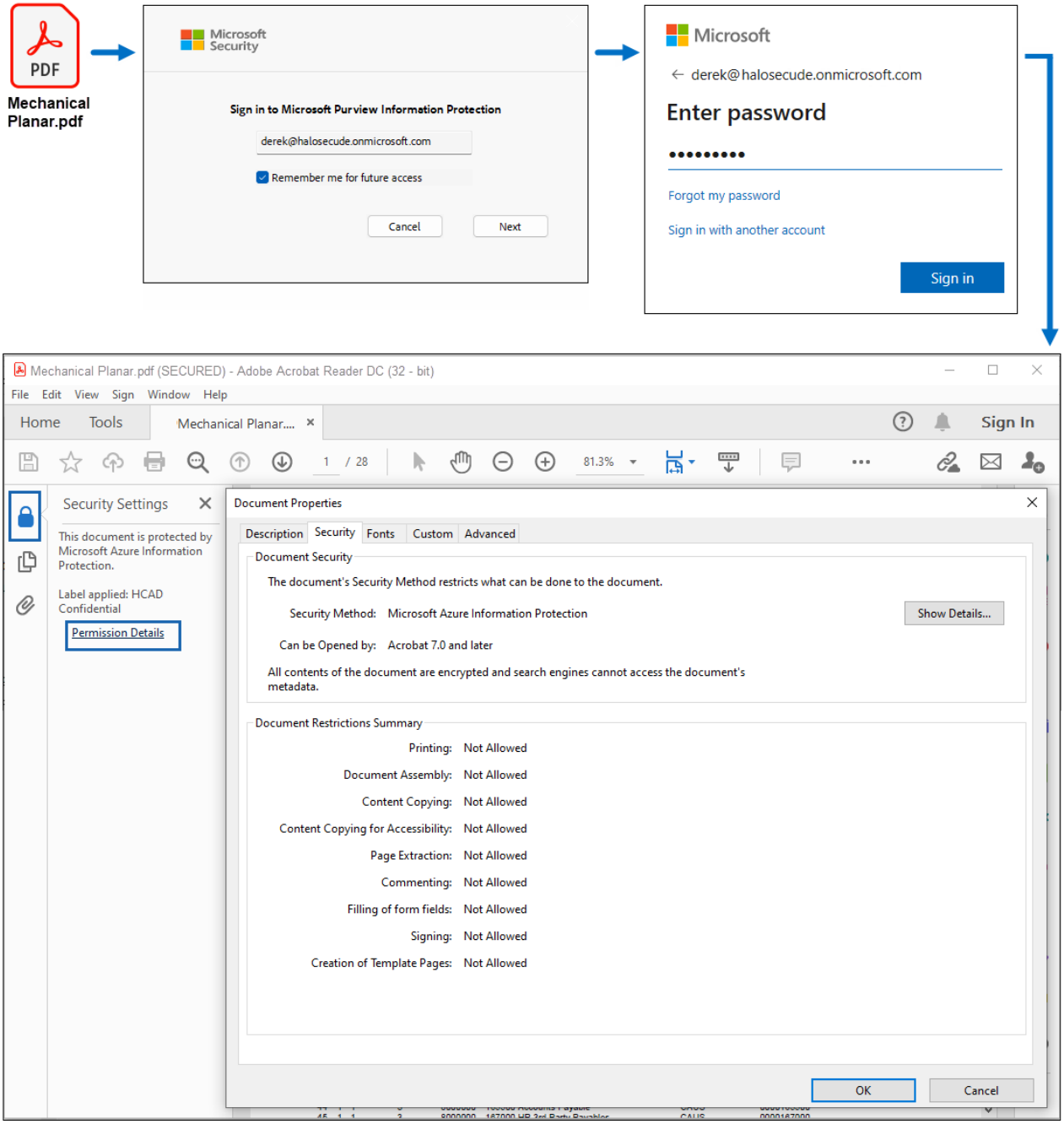
1. Go to the **Solid Edge Application Button** > click **Save As** > In the **Save as Type** list select **Adobe Acrobat Documents (*.pdf)** > click **Save**.
2. Or, go to the **Solid Edge Application Button** > click **Paper Print** > in the **Printer** list select **Microsoft Print to PDF >** click **Print** > choose a location and enter a file name, and click **Save**.

Result: An exported PDF file is saved with protection.

The protected file may need to be viewed after being exported. To open a protected file, follow the instructions below:

Prerequisite: Ensure that the latest version of Acrobat Reader DC or Acrobat DC is installed.

1. Double-click the protected file or open the **Adobe** application, go to the **File** menu > **Open** > browse, and select the file.
2. Microsoft Sign-in prompts you to provide your credentials.
3. Enter the credentials and click **Sign in**.



Protected PDF File

4. To the question "*Do you want to stay signed in?*", answer **Yes**.

Result:

- Upon successful authentication, the protected file is opened.
- If authentication fails, access to the file is blocked.

Next step

To see the actual permissions that are applied to the file, do one of the following:

- Click on the lock icon > **Permission Details** > **Document Properties** screen > click **Show Details**.
- Click **File** > **Properties** > click **Security** tab > **Document Properties** screen > click **Show Details**.

4.5. How to View a Protected File in HaloCAD Reader?

The reader add-on is intended for customers who do not have the full HaloCAD solution installed. Secude provides this viewer program to enable end users to view HaloCAD-protected files without having to install the standard (full) version of the HaloCAD solution on their desktops.

Reader add-on vs HaloCAD Standard add-on

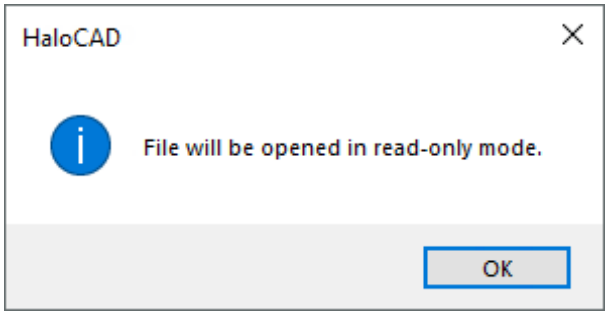
Both add-ons use the Microsoft Purview Information Protection security solution. However, the reader add-on cannot function as a HaloCAD Standard add-on; it is limited to opening and reading CAD files that are protected by the Standard/Full add-on.

Prerequisite: Make sure that the HaloCAD Reader Add-on for Solid Edge is installed.

1. Double-click the protected file.
2. HaloCAD will prompt you about the Microsoft Sign-In Assistant before allowing you to access the file.
3. Click **OK**. Enter the credentials and click **Sign in**. (However, you do not require this validation if your cached account information is available.)

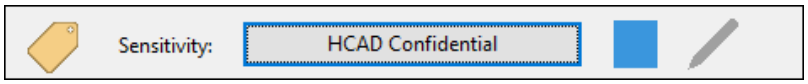
Result:

- A read-only version of the file opens with the following message.



HaloCAD reader message

- Click **OK** on the HaloCAD reader message.
- You can also observe the disabled pencil icon (**Click to change label**) in the Sensitivity ribbon, along with disabled tabs, panels, and buttons in the CAD application, as well as disabled permissions such as edit, copy, print, export, and change rights options.



Disabled Click to change label icon

Next step

The reader add-on gives you the following options, similar to the standard add-on:

- To view the file's permissions, click the **Status** icon.
- To log out an active user from a HaloCAD session, click the **Reset** icon.

5. Common Scenarios

This section presents common scenarios for illustrative purposes and provides general guidelines.

5.1. Concept: Sensitivity Labels

MPIP labels can be customized to meet the requirements of each organization. These labels are defined and managed directly in the Microsoft Purview portal, and the HaloCAD Add-on retrieves them for user selection. When a sensitivity label is applied, the associated permission levels are automatically enforced on the document; any rights that are not explicitly granted are not assigned to the user. For example, a label applied to a CAD file with view-only permission allows users to view the content without any additional rights.

1. Let's say, for example, that you set up a label with the "Viewer" permission. In this case, the user will be able to view MPIP-protected content, but the following actions and menus will be disabled:
   a. Pencil icon - **Click to change label** in the HaloCAD Sensitivity ribbon.
   b. All tabs, panels, and buttons in the CAD application.
   c. Edit, Copy, Print, Export, Change Rights, and Revoke options in the **Status** UI. Refer to Example 1.
2. In contrast to the previous point, if you configure a label with 'Co-Owner' permission, the user will have full access to the file, including the ability to view, edit content, print, copy, and export the file, as well as change rights (labels). Refer to Example 2.
3. For more details on labels, please refer to Microsoft Documentation.

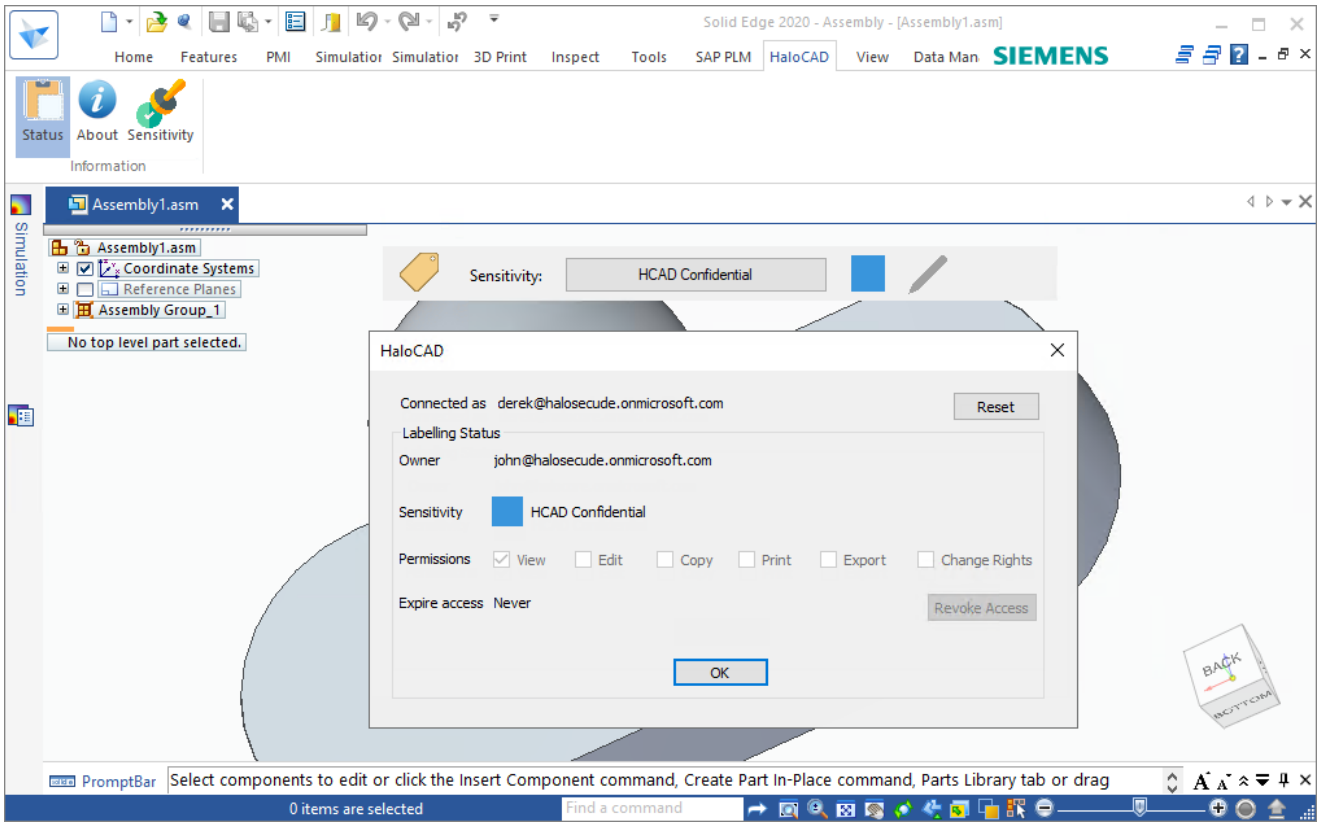
5.2. How to Open a Protected CAD File?

Follow the procedure below to view the protected file:

1. Click the protected file to open it.
2. When a labeled file is opened for the first time, a connection to the Microsoft Entra tenant is requested via the Microsoft Sign-In Assistant.
3. Click **OK** when prompted that the Microsoft Sign-In Assistant will be invoked and user credentials will be cached.
4. Follow the on-screen instructions to complete the authentication process.
5. After successful authentication, the file opens.
6. Access results for the same document may vary based on the applied policy settings. Please refer to the following examples.

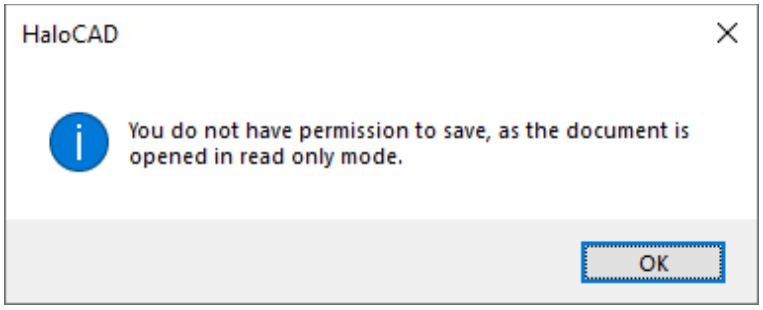
5.2.1. Example 1: Label with Read-only Access

1. The MPIP label **HCAD Confidential** is applied to the following file. This label allows the logged-in (connected) user to view the file while restricting all other operations.
2. To view the applied label and your file permissions, click the **HaloCAD** tab and then select **Status**.



User with restricted access #1

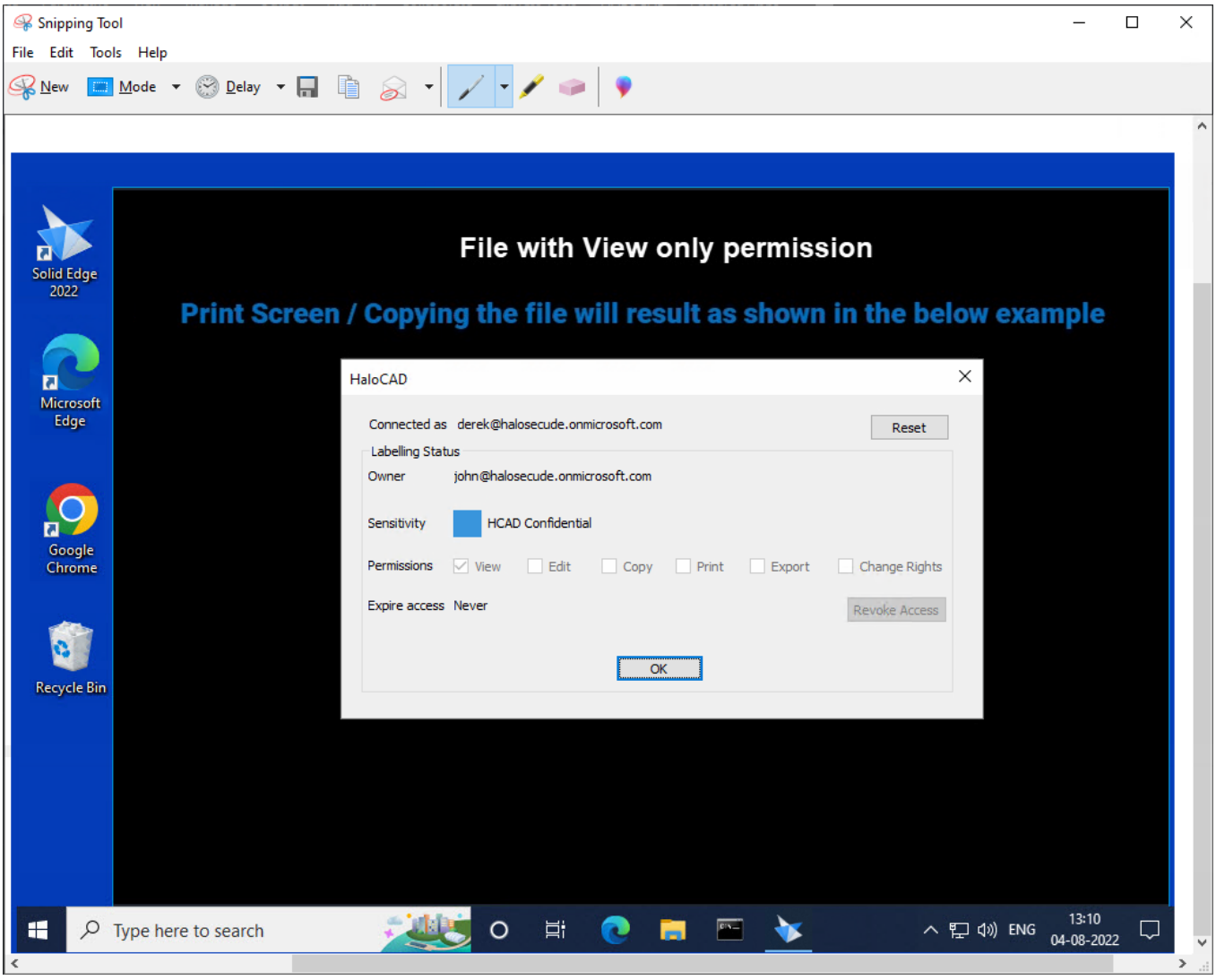
3. In case you try to save the drawing while closing, you will receive the following HaloCAD pop-up.



User with restricted access #2

Behavior When Attempting to Copy, Save, or Capture Screen Data

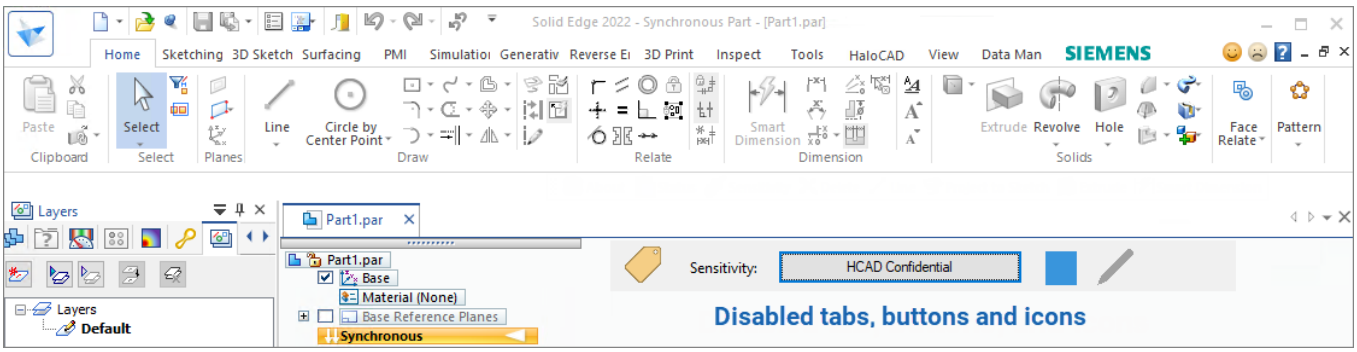
One of the most common ways confidential information is compromised is by copying it (Ctrl + C) or capturing it using tools such as Print Screen or the Snipping Tool and then transmitting it elsewhere. To prevent this, when a label without the **Copy** usage right is applied, the entire content is blanked out during copy or screen-capture attempts. Similarly, when the user clicks the **File** menu, options such as **Save**, **Print**, and other related actions are disabled because the user does not have the required authorization to perform these operations.



HaloCAD prevents copying data

What Happens if You Try to Relabel with Read-Only Permission?

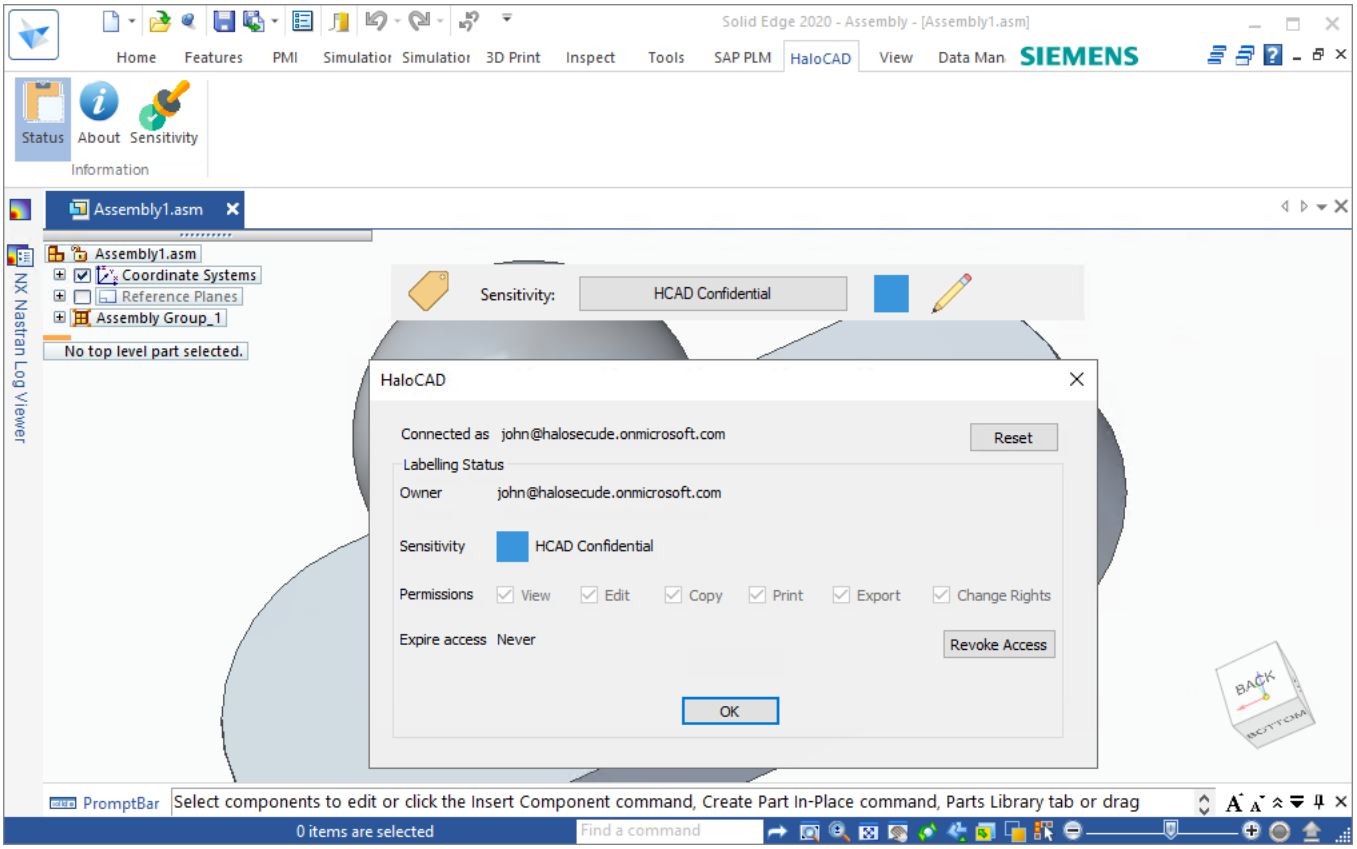
With "Read-only / View" rights, you are only allowed to view the content; all other options, including the tab, panel, button, and pencil icon - **Click to change label** on the HaloCAD Sensitivity ribbon, are disabled. As a result, the imposed protection cannot be relabeled or removed.



Disabled tab, buttons, and icons

5.2.2. Example 2: Label with Full Control Access

The file shown below is labeled **HCAD Confidential**, which grants the user full access, therefore, all menus are enabled in the file. To view the applied label and your file permissions, click the **HaloCAD** tab and then select **Status**.



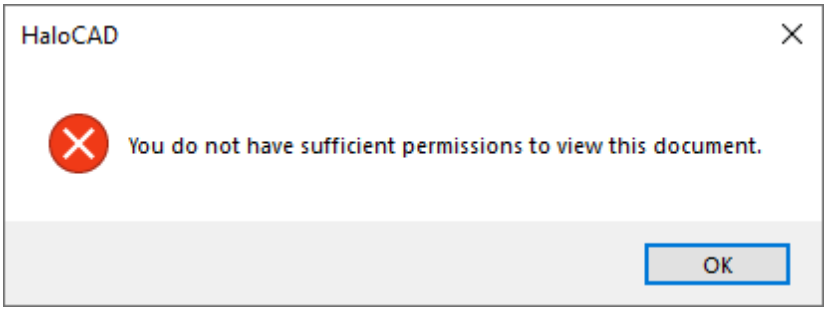
User with full access

What Happens if You Try to Relabel with Co-Owner Permission?

With "Co-Owner" rights, you have complete control over the content and can relabel or remove the protection as needed by clicking the pencil icon - **Click to change label** on the HaloCAD Sensitivity ribbon.

5.2.3. Example 3: Unauthorized User Access

An unauthorized user who double-clicks on a protected CAD file receives the warning shown below. Note: An unauthorized user is anyone who is not listed in the allowed user list configured within the Microsoft Purview Information Protection sensitivity label.



Unauthorized user opening a protected file

5.2.4. Example 4: Labeling Dependent (Protected and Unprotected) Files

Assume there is a protected Parent Assembly file. Now, import protected and unprotected part or sub-assembly files to it. You will receive the below-shown message in two scenarios: when you save the parent file, and if the parent file is relabeled after saving.

Labeling the unprotected and protected child files

You must confirm the following action to take effect:

If **Yes**:

- All associated unprotected child files receive the Assembly file's label.
- Already protected child files are relabeled with the Assembly file's label.
- If a child file does not have Owner or Co-owner rights, the Parent label cannot be imposed on the file.

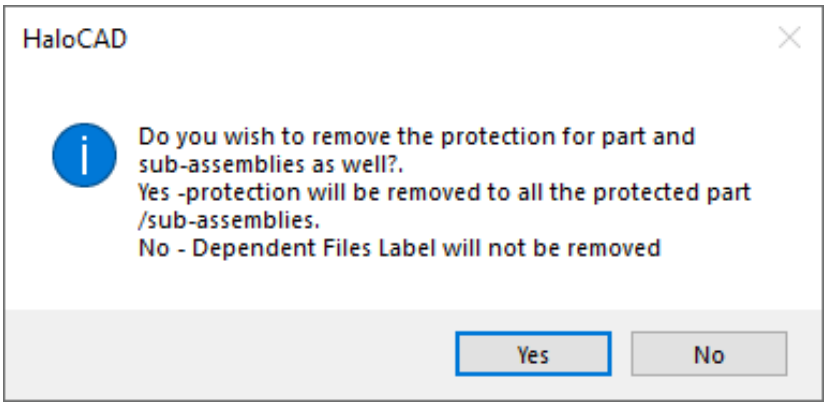
If **No**:

- Only unprotected files receive protection.

- Existing protected child files remain unchanged.

5.2.5. Example 5: Removing Protection from Assembly and Part Files

Assume that a protected Parent Assembly file contains part or sub-assembly files. To keep the file unprotected, remove the existing label and apply the **--No Protection--** label to the Parent Assembly file. The following message appears:



Removing protection from protected part files

You must confirm the following action to take effect:

If **Yes**:

- All associated protected child file labels are removed, and the files are unprotected.
- If a child file does not have Owner or Co-owner rights, protection cannot be removed from the file.

If **No**:

- Only the Parent Assembly file label is removed, and the file is unprotected.
- The labels on the existing protected child files remain unchanged.

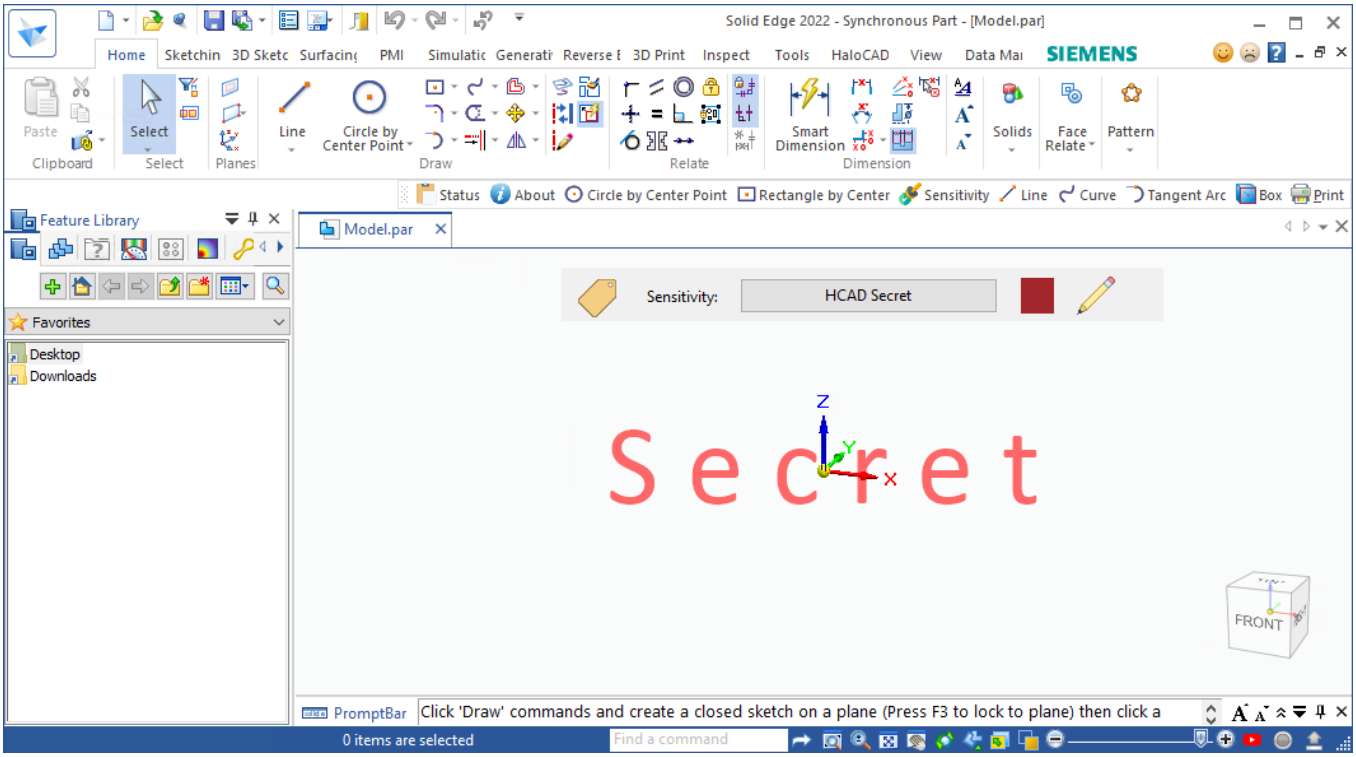
5.2.6. Example 6: Labeling Dependent (Unprotected) Files

Assume that a Parent Assembly file contains dependent parts or sub-assembly files that are unprotected, while the Parent Assembly file may be protected or unprotected. When you relabel the Parent Assembly file, the following message appears. Click **OK** to protect both the Parent Assembly file and the dependent files with the same label.

Labeling unprotected child files

5.2.7. Example 7: Label with Content Marking

Applying a watermark indicates what type of content it is and how it should be handled, and its presence in a file serves as a constant reminder to the user that the file contains sensitive information. The file below is labeled **HCAD Secret** and bears the watermark **Secret**.



Content with watermark

5.2.8. Example 8: Other Use Case Scenarios

5.2.8.1. Importing a file with a restricted/least permission label

A restricted/least permission label refers to a label with the lowest permission, such as view-only access rights. A full permission label has full access rights, such as Edit, Export, Change Rights, and so on. The least permission label functionality is only available for Asm files.

1. **Case 1** - When you import a dependent part or sub-assembly file protected with a “restricted permission” label into a parent assembly file protected with a “full permission” label, the following HaloCAD pop-up message appears as *“Please confirm applying least permission label from import file? Yes - Current file will be updated with import file label “XXXXXXX”. No - Import operation will be cancelled.”*
   a. If **Yes**, then the imported dependent part file’s label will be applied to the parent assembly file. For example, **HCAD Public** label with view rights will be applied.
   b. If **No**, then the import will be blocked, and the parent assembly file will remain unchanged.
2. **Case 2** - When you import a dependent part or sub-assembly file protected with a “full permission” or “restricted permission” label into a parent assembly file that is unprotected, the HaloCAD pop-up message appears as described in Case 1 above. The response (Yes or No) process will also follow the same procedure as in Case 1.
3. **Case 3** - When you import a dependent part or sub-assembly file protected with a “full permission” label into a parent assembly file protected with a “restricted permission” label, the import is allowed and no label changes occur in the parent assembly file.

In addition, when an assembly file is opened, all linked part or sub-assembly files are checked to determine the least restrictive permission among them. If any part or sub-assembly file has the lowest permission level, the parent assembly file adopts that restriction. For example, if a part file is set to 'view-only,' the assembly file is also enforced to 'view-only' upon opening.

5.2.8.2. Labeling a File Without Protection

Compared to a standard MPIP label, a **label-only MPIP label** adds metadata to a file without applying protection. In this context, *label-only* refers solely to metadata classification. The key difference between a standard **MPIP label** and a **label-only MPIP label** is that the standard label includes encryption and protection options, whereas the label-only variant does not. As a result, a **label-only MPIP label** can be applied to files that do not require protection but still need to be labeled for classification purposes.

Prerequisite: Make sure the **Control access** check box under the **Choose protection settings for the types of items you selected** page is unchecked while defining the label-only in the Microsoft Purview portal.

Other key points

1. When a label-only MPIP label is applied to a file, the suffix (**Label Only**) is appended to the label name. For example, if the label name defined in the portal is **HCAD Metadata**, it appears as **HCAD Metadata (Label Only)** after being applied to the file.

MPIP label-only

2. **Full rights**: A file with this label allows a user to have full rights on it.
3. **Notifications**: Similar to a standard MPIP label, the user will receive notifications when label-only is applied to a top-level parent file.
4. **With the HaloCAD Add-on**: The label details will be displayed in the Status UI, just like a standard MPIP label.
5. **Without the HaloCAD Add-on**: A file with a label-only MPIP label will behave like any other unprotected CAD file.
6. **Properties**: To see label details, follow the instructions below:
   a. Go to the **Data Management** tab > click **File Properties.**
   b. Under the **Property** tab, click on **Custom** node to view the author name, label ID, and label name.
   c. Furthermore, if watermarking is configured in this label, the **Custom** node displays additional information such as the font color, font name, font size, layout, and text.

5.2.9. Example 9: Custom Permissions Label

Difference Between Sensitivity Labels and Custom Permissions

Sensitivity Labels

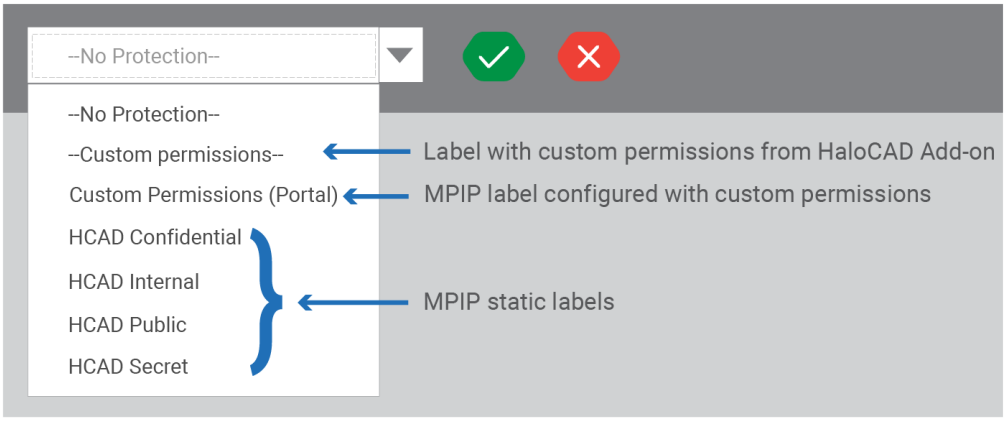
Sensitivity Labels are defined and managed by an organization's administrator in the Microsoft Purview portal. Each label includes a predefined set of permissions and is also referred to as administrator-defined permissions.

Custom Permissions

Custom Permissions are user-selectable permission sets available in the HaloCAD application UI. These permissions are defined by users and are also referred to as user-defined permissions.

5.2.9.1. Protection using Custom Permissions from Microsoft Purview Portal

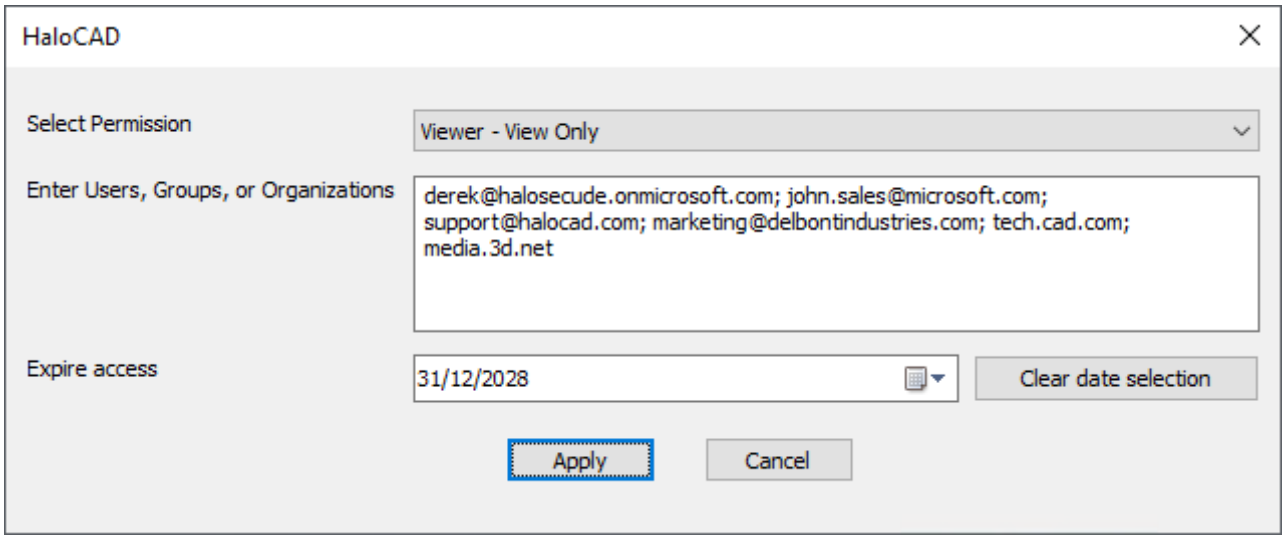
Prerequisite: Make sure the custom permissions label in the portal is set to **Let users assign permissions when they apply the label**.



Custom permissions and other labels

Follow the procedure to apply the custom permissions label:

1. Open the Solid Edge application, click **New**, select a template, and then create objects.
2. Click the **Click to change label** icon.
3. When HaloCAD downloads the labels, custom permission labels (from the Microsoft Purview portal and user-defined labels) are listed in the Sensitivity ribbon.
4. For illustration, the custom permission label from Microsoft Purview is named **Custom Permissions (Portal)**.
5. Select the **Custom Permissions (Portal)** label from the list and click the green check mark (**Click to set label icon**).
6. The HaloCAD screen appears, as shown below.



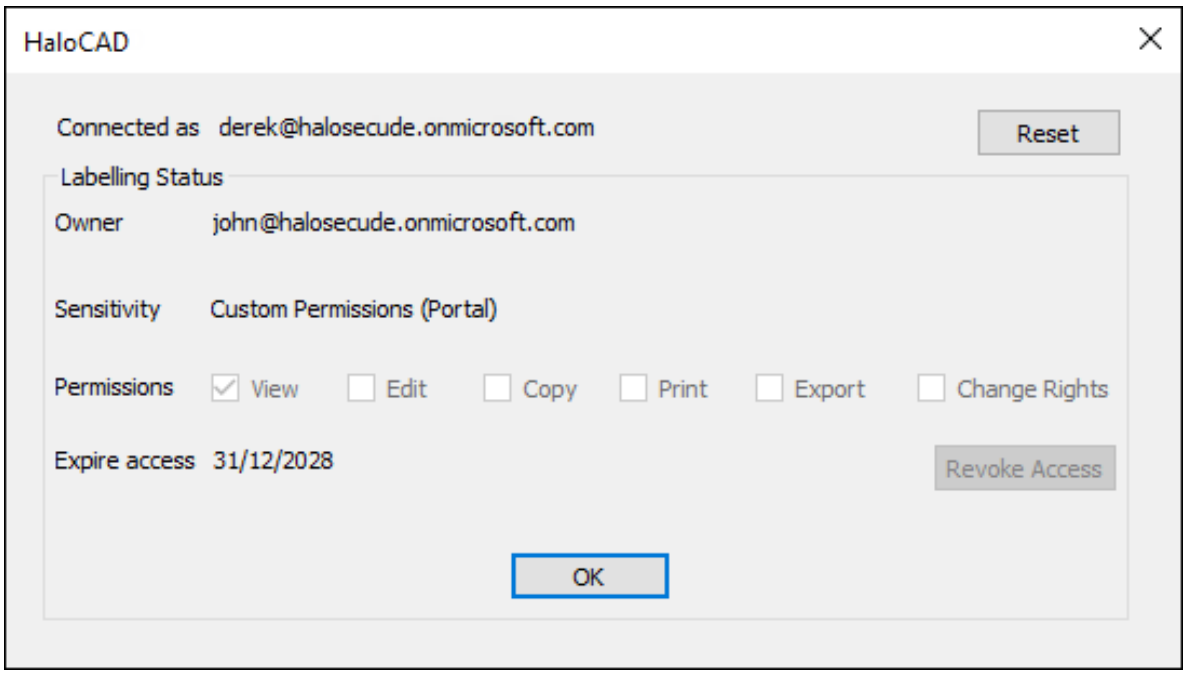
HaloCAD Custom permissions

7. From the **Select Permission** list, choose the level of access you want users to have when protecting the file: (Viewer - View Only / Reviewer - View, Edit / Co-Author - View, Edit, Copy, Print / Co-Owner - All Permissions / Only for me).
8. In **Enter Users, Groups, or Organizations**, specify who should have access to the file. Enter individual email addresses, group email addresses, or an organization domain, separated by commas, spaces, or semicolons.
9. In the **Expire Access** field, specify how long the labeled file can be accessed. Select **Never** for unlimited access, suitable for less sensitive content. For highly sensitive content, select an expiry date so that recipients (other than the owner) cannot access the file after that date.
10. Click the **Clear date selection** option to clear the previous date selection.
11. Click **Apply** to confirm the protection settings.

Result: The label is applied to the file.

What happens when a user opens a custom permissions–labeled file?

Based on the user's permissions, the file can be accessed accordingly. Note: The author of the document always has full rights to the file and can access it at any time, regardless of any custom permissions or expiry date configured in the label. The following example shows a label with custom permissions.



User with custom permission

5.2.9.2. Protection using Custom Permissions (User-defined Permissions) via HaloCAD Add-on

In comparison to the previous section, the HaloCAD add-on also supports a **Custom Permissions** label. However, this label is defined at the application level within HaloCAD and is not obtained from the Microsoft Purview portal. The process for applying this label is the same as described in the previous section.

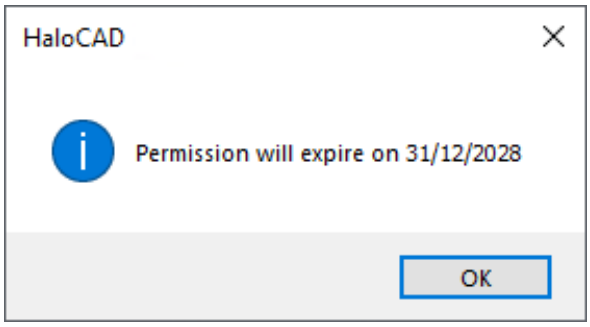
5.2.10. Example 10: Set an Expiration Date for File Access

Prerequisites:

1. Ensure that the expiration date is configured in the Microsoft Purview portal when using a static MPIP label.
2. Ensure that the expiration date is configured in the Custom Permissions label when using it via the Microsoft Purview portal or the HaloCAD add-on.

5.2.10.1. Why is File Expiration Necessary?

When files are shared with external vendors, access may continue even after a contract ends, creating security risks. To prevent this, set an expiration date on the file. This is a recommended practice when working with vendors or contractors. For example, if a file is shared with an expiration date of 31/12/2028, business partners will not be able to open it after that date. Each time the file is opened, HaloCAD displays the file's validity.



Validity of the file

5.2.10.2. What Happens When a File Expires?

When a user opens a file that has reached its expiration date in their current time zone, the labeled file cannot be opened. HaloCAD will prompt a message "*You do not have sufficient permissions to view this document*". This behavior is like unauthorized file access, as described in the section "Example 3: Unauthorized User Access".

5.2.10.3. How to Open an Expired File

Recipients cannot open an expired file. Only the file author can access it. If a recipient needs continued access, they must contact the author to obtain a new copy of the file with an updated expiration date.

5.2.11. Example 11: Remove protection from a file

To remove a label from a protected file, you must either be the file's owner or have full permission to remove protection.

5.2.12. Example 12: Revoke a File

Prerequisite: Ensure that the user who wants to revoke a file has the required license, as specified in the Release Notes under the Requirements section.

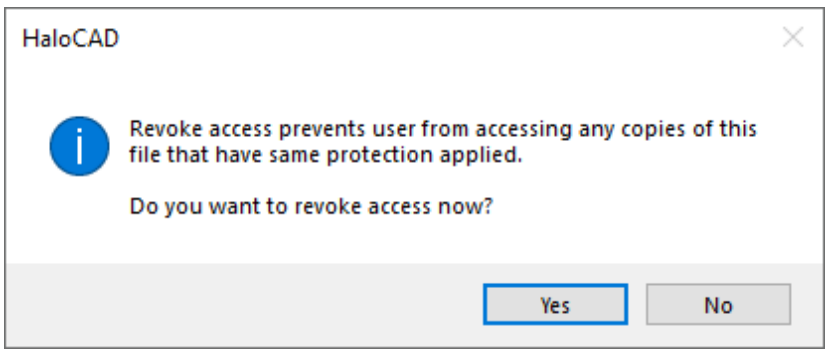
Revoke Feature: MPIP provides a revoke feature that prevents any new access attempts to a protected file, restricting access to all users except the author. Note that revoking access removes permissions for all users associated with that label.

5.2.12.1. Why Should a User Revoke a File?

A user may revoke access to a sensitive file if it was sent by mistake, accessed from a suspicious location, leaked, or if a recipient no longer requires access. In these scenarios, the author can immediately prevent further access by revoking the file. Note: Revoking does not delete the shared file, but users will no longer be able to open it. The **Revoke Access** button is available on the HaloCAD status screen.

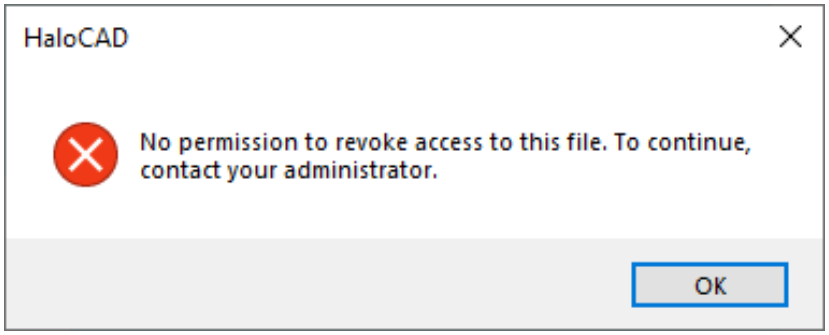
5.2.12.2. How to Revoke a File?

1. To revoke a file, go to the **HaloCAD** tab > click **Status** > click the **Revoke Access** button. The following message will appear:



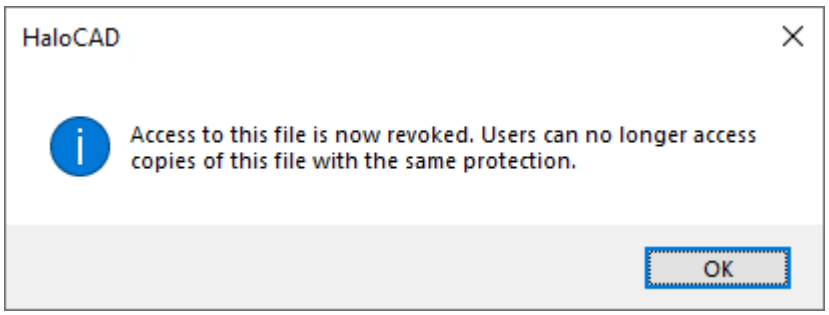
Revoke access message #1

2. Click **Yes** to confirm revoking access and continue with step 3. If you do not have the required license, it is not possible to revoke a file. In this instance, HaloCAD will show the alert as follows:



Access denied when revoking a file

3. The following message will appear:



Revoke access message #2

4. Click **OK** and save the file.

Result:

- Access to the file is revoked.
- Users who previously had access to the document can no longer open it.

5.2.12.3. What Happens if a User Attempts to Open the Revoked File?

Once the file is revoked, the user cannot open it, although the user has accessed it before. HaloCAD shows a generic message as "*You do not have sufficient permissions to view this document.*" This behavior is like unauthorized file access, as described in the section "Example 3: Unauthorized User Access".

MIP SDK

A revoked file can be accessed by the same user if it was previously opened by the same user in the same HaloCAD session. This is due to the actual behavior of the MIP SDK if you have defined the sensitivity label with the two options **Allow offline access** and **Users have offline access to the content for this many days,** the configured offline access allows users to continue to access the revoked file until the offline policy period ends.

5.2.12.4. What Happens if a User Changes the Label?

Assume User A shares a sensitive file with User B.

Case 1: If User B makes copies of the original document, revoking file access by User A will also revoke all copies, since the label remains unchanged.

Case 2: If User A has not revoked access and User B (with full rights) changes the label, revoking file access will not apply to that modified copy. However, the original document will still be revoked.

5.2.12.5. How to Open the Revoked File?

A recipient cannot open a revoked file. Only the file author can access it. If a recipient needs access, they must contact the author to obtain a new copy of the file.

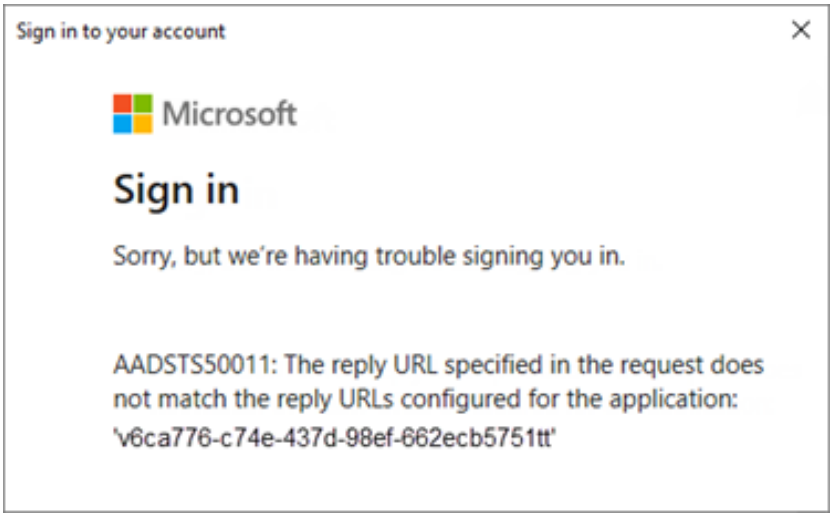
6. Troubleshooting

This chapter will help you overcome the most common problems with the HaloCAD solution.

6.1. Cannot Sign in to Microsoft Sign-In Assistant

Symptoms

The user login fails with the following error message.



Microsoft Sign-in error message

Background

The above error occurs when a user logs in to a HaloCAD session using Microsoft Sign-In Assistant.

Probable Cause

As the Redirect URL specified in the request does not match the URL configured for the registered application, Microsoft Sign-in fails.

Corrective Action

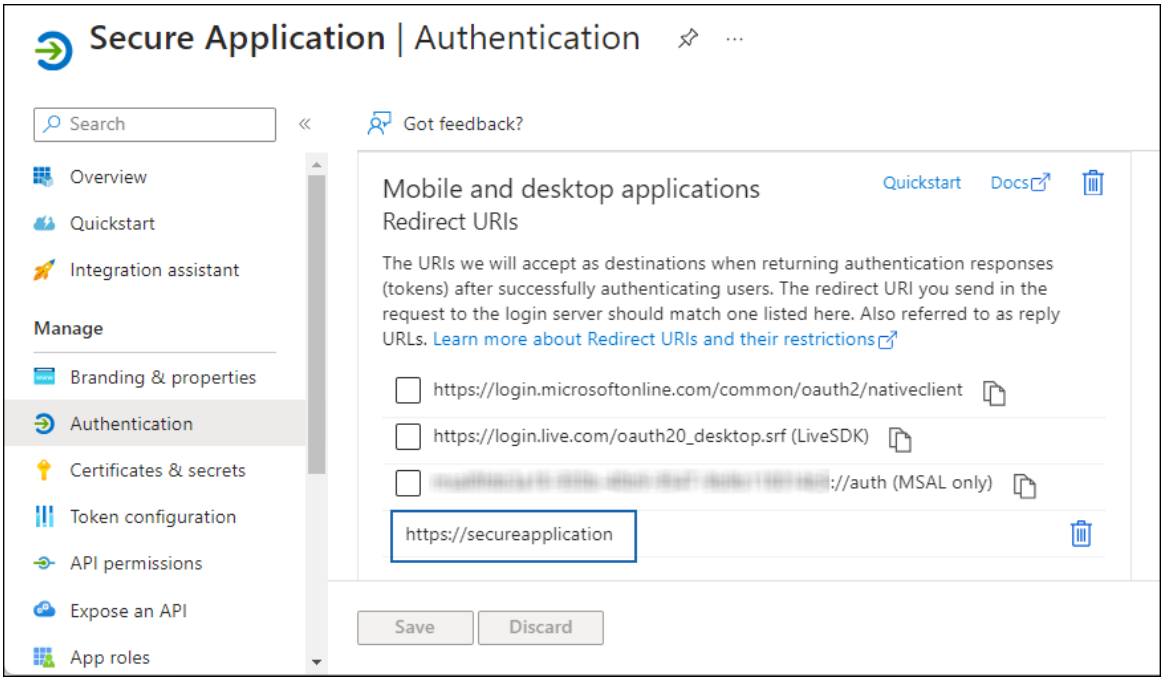
1. **Case 1:** An incorrect Redirect URI was entered during the HaloCAD installation.
   a. Reinstall the HaloCAD Add-on using the correct **Redirect URI**.
   b. Launch the CAD application, click the pencil icon (**Click to change label**), and sign in using the Microsoft Sign-In Assistant.
2. **Case 2**: Redirect URIs use an improper scheme (such as `http://contoso.com`)
   a. Log in to the Microsoft Azure portal.
   b. On the home page, click the **Show Portal Menu** icon, then select **Microsoft Entra ID**.
   c. Under the **Manage** section on your tenant's **Overview** page, choose **App registrations**.

d. Click **All Applications**, and enter your application name in the search bar.

e. From the list, select your application.

f. Click the **Redirect URIs** link or select **Authentication** from the **Manage** section on the application overview page.

g. Verify that the reply URL begins with https://. If it does not, update it to https and save the changes.



Incorrect Redirect URIs

h. Now, sign in using the Microsoft Sign-In Assistant.

3. **Case 3**: Tenant ID provided for multi-tenant application

a. Reinstall the HaloCAD Add-on without entering the **Tenant ID**.

b. Open the CAD application, click the pencil icon (**Click to change label**), and sign in using the Microsoft Sign-In Assistant.

6.2. Labels are not Getting Downloaded in the HaloCAD Session

Symptoms

The user could not download labels.

Background

The user logs in successfully in the HaloCAD session, but cannot download labels.

Probable Cause

Improper label configuration in the Microsoft Purview portal.

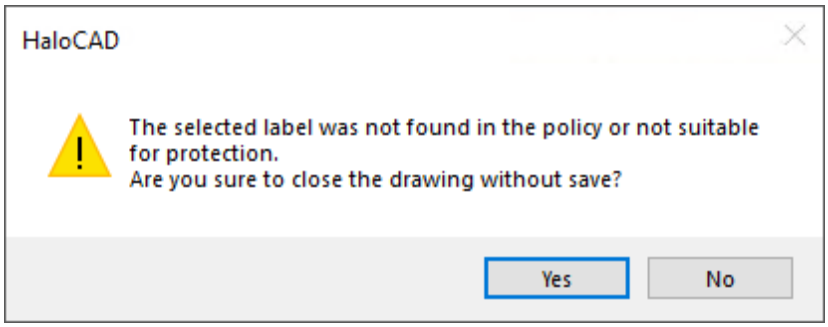
Corrective Action

1. Log in to the Microsoft Purview portal as a global administrator.
2. Ensure that the labels are configured to apply protection.
3. Verify that the user has the required policy to use the label.
4. For more details, refer to the Microsoft documentation.

6.3. Label not Found in the Policy

Symptoms

HaloCAD prompts the following message:



Label not found error message

Background

The above message is shown when you apply a label to a file and save it.

Probable Cause

Improper label configuration.

Corrective Action

Request your Microsoft Purview portal administrator to review the label and publish label policies.

6.4. Double Key Encryption Label could not be Applied

Symptoms

HaloCAD prompts the following message:

DKE label error message

Background

The above message is shown when you apply a Double Key Encryption (DKE) label to a file and save it.

Probable Cause

This issue occurs if the DKE service is stopped or unavailable.

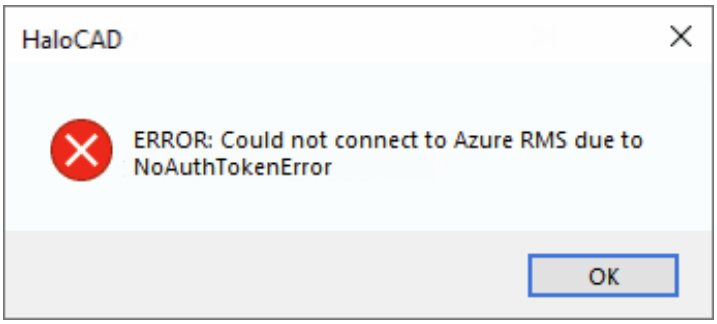
Corrective Action

Make sure that the DKE service on the client's computer is active and accessible online.

6.5. Could not Connect to MPIP – Case 1

Symptoms

HaloCAD prompts the following message:



MPIP connection warning message #1

Background

The above error occurs when a user logs in to the HaloCAD session via Microsoft Sign-In Assistant.

Probable Cause

This issue occurs if one or more of the following conditions are true:

1. **Case 1**: You have entered the incorrect **Application (client) ID**, **Directory (tenant) ID**, and **Redirect URI**.
2. **Case 2**: You have closed the Microsoft Sign-In Assistant dialog unknowingly.

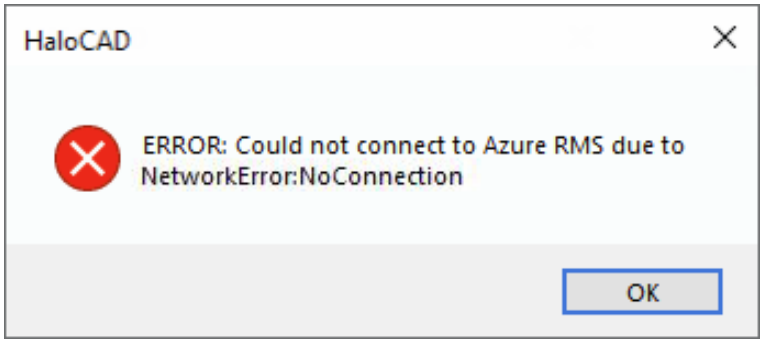
Corrective Action

1. **Case 1**: Make sure the correct values of **Application (client) ID**, **Directory (tenant) ID**, and **Redirect URI** are entered during the initialization.
2. **Case 2**: Relaunch the application and enter user credentials in the Microsoft Sign-In Assistant dialog.

6.6. Could not Connect to MPIP – Case 2

Symptoms

HaloCAD prompts the following message:



MPIP connection warning message #2

Background

The above error occurs when a user logs in to the HaloCAD session via Microsoft Sign-In Assistant.

Probable Cause

The most likely cause of this issue is that your network is preventing you from connecting to Microsoft Purview Information Protection.

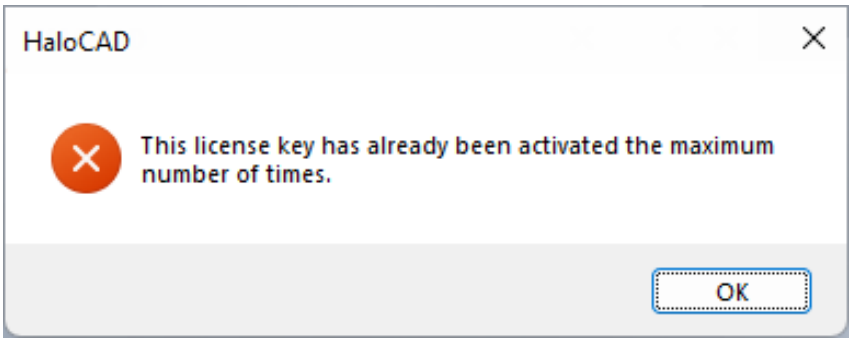
Corrective Action

1. Review your firewalls or network infrastructure to establish a connection with Azure.
2. Check if your proxy limits the URL.

6.7. HaloCAD Activation Fails

Symptoms

HaloCAD prompts the following message:



HaloCAD Activation warning message

Background

The above message is shown when you try to activate HaloCAD on a system.

Probable Cause

After a successful license activation, the license status changes to **Active**, and the **Total activations** count in Secude's License Server Manager increases by one. The total activation count increments with each activation.

For example, if you purchased ten HaloCAD licenses, you can activate HaloCAD up to ten systems. After the tenth activation, attempting to activate HaloCAD on another system will fail, and the License Server Manager will display an error indicating that the maximum number of activations has been reached.

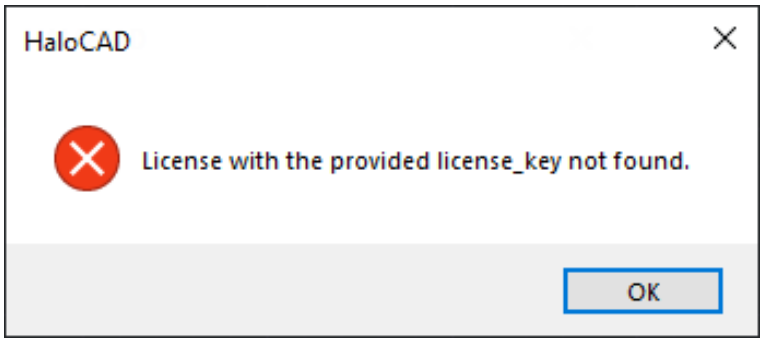
Corrective Action

1. **Action 1:** Uninstall one or more HaloCAD add-ons that were previously activated on a CAD system, and then activate the license on the required CAD system.
2. **(Or) Action 2:** Purchase an additional HaloCAD license.
3. After completing the action, activate the license.

6.8. Incorrect License Key Error Message

Symptoms

HaloCAD prompts the following message:



Incorrect license activation message

Background

The above message is shown when you try to activate HaloCAD on a system.

Probable Cause

There are various possible reasons, including a license key associated with another HaloCAD, an incorrect key, or an invalid key.

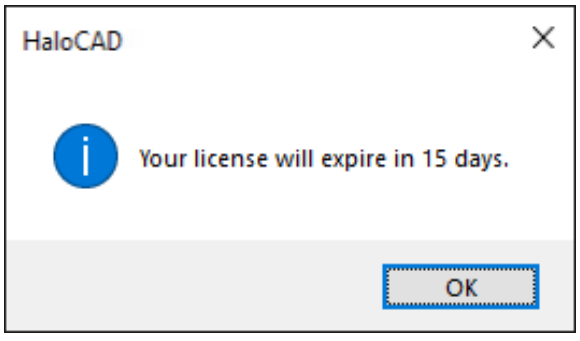
Corrective Action

Make sure to enter the correct licensing key, unique to this add-on, before activating it.

6.9. Why Am I Getting License Expiration Notifications?

Symptoms

HaloCAD prompts the following message:



HaloCAD notification

Background

The above notification occurs once a day when a user logs into the HaloCAD session.

Probable Cause

When you run the CAD application and see a HaloCAD expiration alert, it means action is required to continue using the add-on.

Each license has an end date defined at the time of issue. When the license is within 30 days of expiry, the License Manager triggers daily notifications in HaloCAD. For example, if the license expires on September 30, 2028, notifications will begin appearing once per day starting September 1, 2028.

Corrective Action

1. Purchase a new HaloCAD license or renew the existing license.
2. Activate the license.

6.10. Other License-Related Error Messages

HaloCAD License Error Messages	Root Cause	Correction Action
The license validity period has expired	When your license had just expired.	Please contact Secude's representative to receive a new license.
The license is not enabled.	When you try to activate a license key that is already disabled on the License portal.	Please contact Secude's representative to enable the license.
This device is blacklisted.	When your device is blocked in the license portal for a specific reason.	Please contact Secude's representative to enable the device.
This license cannot be activated before the start date: yyyy-mm-dd.	When attempting to activate a license before its start date.	Please make sure the license is activated on the start date.
Date header is not valid or set in past.	When the date or time on the machine is incorrect.	Please make sure that the machine installed with the HaloCAD add-on is synchronized with the current date and time.

License-related error messages

7. Technical Support

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

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

Contact Technical Support

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

Additional Resources

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

Documentation Feedback

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

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

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

Secude

www.secude.com

About Secude

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

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