Secude

HaloCAD

HaloCAD for Windchill

Installation Manual

Version 2.8

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. Introduction

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

1.1. How does HaloCAD for PLM protect your Data?

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

It provides access to MPIP-protected files, including label handling and privilege enforcement. Any file access actions, such as check-out or export, that may result in a download are intercepted by the HaloCAD for PLM solution, automatically protected based on predefined rules, and then delivered to the end user. Similarly, file access actions such as check-in or upload are intercepted and examined. If a protected file is detected, it is decrypted, and the unprotected file is returned to the PLM vault. For CAD users, the handling of CAD files remains seamless, as these processes occur entirely in the background. By applying MPIP labels, the solution ensures end-to-end security for CAD files, while all upload and download activities are continuously monitored and logged to provide complete traceability.

1.2. About this Manual

This manual walks you through the installation and configuration procedures unique to HaloCAD for Windchill.

Reference

Before proceeding with the instructions in this manual, administrators should:

1. Review the Technical Reference Manual to understand HaloCAD’s architecture and prerequisites.
2. Refer to the Release Notes to verify the supported CAD applications.

1.3. Reference Manuals

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

For information on	Refer to
Step 1: For details on supported operating systems, file types, and CAD applications, see the Release Notes.	`HaloCAD_Windchill_ReleaseNotes_EN_Online.pd`
Step 2: Prerequisites 1. Before installing, it is recommended that you fulfill the prerequisites, such as registering an application in Microsoft Entra ID 2. HaloCAD Architecture 3. Registering an Application in Microsoft Entra ID - Web 4. Office 365 Subscription Details 5. Recommended URLs, Addresses, and Ports for MPIP 6. Enable Support for TLS 1.2 at the Client Workstation for Microsoft Entra ID	`HaloCAD_Technical_Reference_Manual_EN_Online.pdf`
Step 3: How to install HaloCAD Add-on for Creo	`HaloCAD_Creo_Manual_Installation_EN_Online.pdf`
Step 4: Install and configure HaloENGINE	`HaloENGINE_Manual_Installation_EN_Online.pdf`
Step 5: Install and configure HaloCAD for Windchill	`Refer to the current manual.`
Step 6: Workflow illustrating protection and decryption	`HaloCAD_Windchill_Manual_Operations_EN_Online.pdf`

HaloCAD reference documentation

1.4. Component Functions

The following components are involved in HaloCAD architecture when deployed in an integrated environment:

1. HaloCAD Add-on for Creo

2. HaloCAD for Windchill
3. HaloENGINE
4. Microsoft Purview Information Protection

The following list outlines the functions of each component.

HaloCAD Add-on for Creo performs the following functions:

1. Operates within the Creo Parametric application.
2. Receives protected files from Windchill and displays their associated labels while enforcing permissions.
3. Logs all add-on–related activities for auditing purposes.

HaloCAD for Windchill performs the following functions:

1. Resides on the server hosting Windchill PLM Server.
2. Listens for check-in and check-out actions initiated via the browser or Creo.
3. Connects to Microsoft Purview Information Protection to download sensitivity labels for file processing.
4. Collects metadata for the user-selected file.
5. Obtains action and label information for the user-selected file from HaloENGINE for file processing.
6. Performs encryption and forwards the file stream to the CAD client during check-out operations.
7. Performs decryption and stores the unprotected file in the PLM Vault during check-in operations.
8. Logs HaloCAD for Windchill component activities to the local log and sends monitor logs to the HaloENGINE.

Recommendations for improving performance

MPIP offline access

Configure the labels to allow offline access. This must be configured in the Microsoft Purview portal under **Items** > **Allow offline access** > **Always**. Choosing this option could have an effect on the revocation process. Therefore, it needs to be taken into account when choosing the offline access option. Please refer to the Microsoft Documentation "Restrict access to content by using sensitivity labels to apply encryption".

HaloENGINE performs the following functions:

1. HaloENGINE is a Java-based server component that exposes a web service to HaloCAD for Windchill.
2. Connects to Microsoft Purview Information Protection to download sensitivity labels and make them available for configuration.
3. Implements business logic.

4. Logs events received from HaloCAD for Windchill.

Microsoft Purview Information Protection

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

Microsoft documentation

This manual assumes that you already have a complete 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.

2. Installing the HaloCAD for Windchill

This chapter explains the requirements, prerequisites, and how to install HaloCAD for Windchill.

2.1. System Requirements

The following system requirements table outlines the minimum and recommended technical specifications, including software and network resources, required to run the product.

Components	Details
Supported Operating Systems	Windows Server 2022 and above with updates installed.
Supported file types	1. Creo file types 2. MS Office native file types 3. Non-Office file types
Others	Install HaloENGINE and HaloCAD for PLM separately on Windows servers.

Requirements

2.2. Prerequisites

The following preparatory steps or conditions must be met before installing the product.

1. Ensure that you have administrative access to install the HaloCAD component.
2. Ensure that the client computer running the HaloCAD Add-on can connect to the Windchill Server.
3. If you download your files from a Replication Server, install HaloCAD for Windchill on the Replication Server.
4. If you want to use custom attributes as metadata while protecting, make sure the **Type and Attribute Management Utility** page is configured.
5. Ensure that your HaloENGINE meets the requirements listed below:
   a. License file (enabled with WINDCHILL system type).
   b. Proper action rules
   c. Client certificate (`.JKS`)

6. Ensure that `PATH` is added to the **System variable** to run the HaloCAD Configuration Tool:
   For example, `PATH=C:\WINDOWS\system32;C:\WINDOWS;C:\Program Files\Java\jdk1.8.0_241\bin`
7. In a Windchill setup with Single Sign On (SSO) implemented on the master/main server and a replica server connected to it, HaloCAD has a limitation when obtaining metadata from the replica server using SSO-based authentication. In this case, we recommend that you enable split authentication for the HaloCAD rest endpoint. Please refer to the section "Enabling Split Authentication" and for more information, see PTC Knowledge Base Article CS291543.
8. If you want to implement a failover mechanism in HaloENGINE, please refer to the section "Failover Mechanism for HaloENGINE in HaloCAD for PLM".
9. Ensure that both HaloCAD for Windchill and HaloENGINE are installed using the same Azure tenant details. A mismatch in the tenant details will result in configuration errors.
10. Ensure that the previously installed HaloENGINE Service is completely uninstalled.

2.2.1. Conditions for Running the HaloENGINE Tomcat Service

Before you begin, make sure that the following prerequisites are met in your system:

Deny log on as a service policy

If the service is running under a specific user or a specific group, ensure that the user is not restricted by the **Deny log on as a service** policy (Local Security Policy > Security Settings > Local Policies > User Rights Assignment). If the user(s) exist, the "*Error 1069: The Service did not start due to a logon failure*" message appears while running the HaloENGINE Tomcat service.

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

During installation, the HaloENGINE gets the required Microsoft Entra ID application details and certificate thumbprint. When the HaloENGINE Tomcat service starts, it tries to connect to the MPIP services using the details entered during installation. As part of this process, it validates the certificate thumbprint against the certificate installed in the **Local Computer** certificate store. The thumbprint entered in the installation wizard must match the one available in the Local Computer certificate store.

If the service runs under a non-administrative user account, the user may not have sufficient permissions to access the certificate's private keys when the certificate is installed in the Local Computer store. This restriction prevents successful authentication with MPIP services. To resolve this issue, grant the user **Read** permission to access the certificate's private key by following the steps listed below.

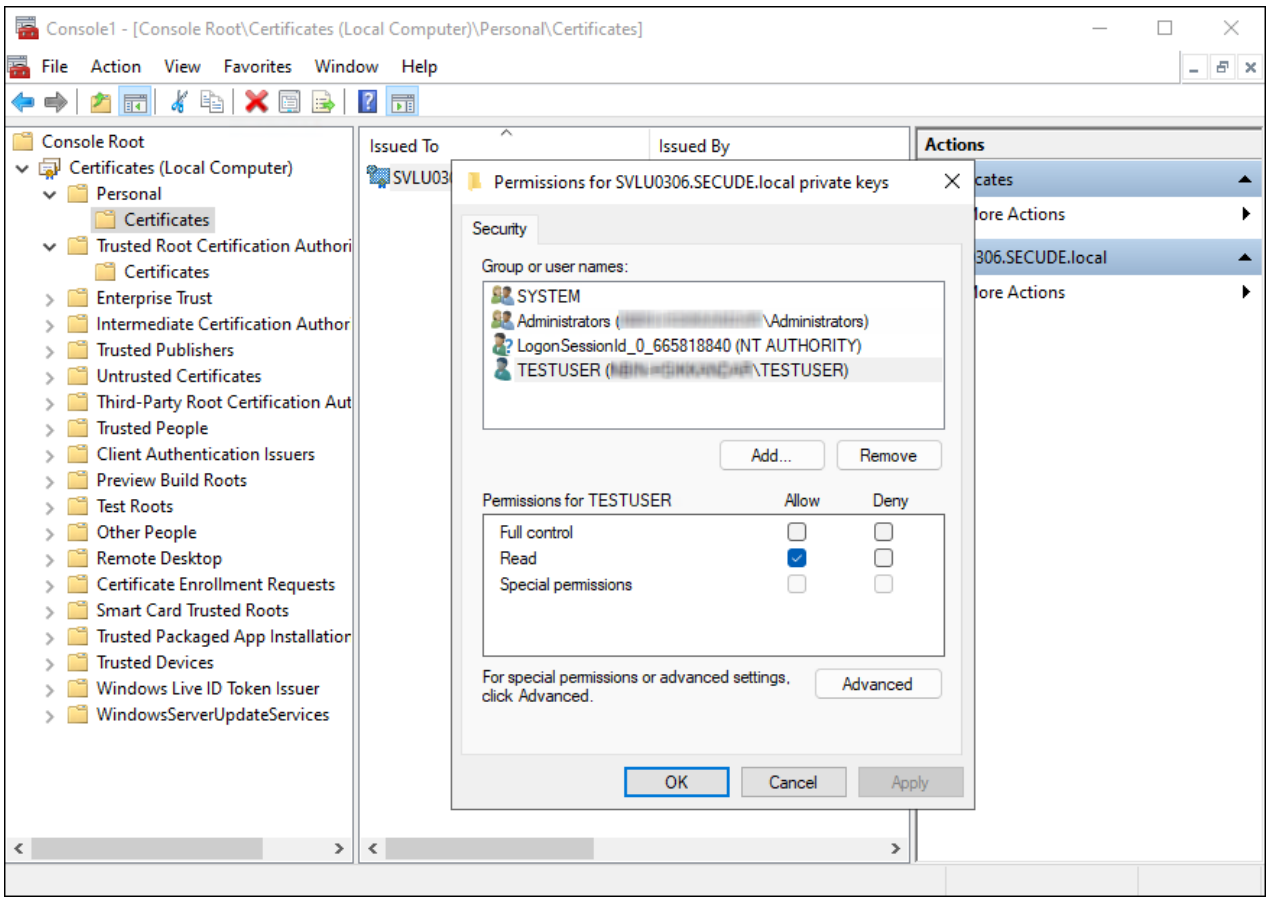
Any errors encountered during this process are recorded in the log file. If the verification succeeds, the service proceeds with initialization.

Prerequisites

1. The required certificates (machine certificate, root CA, and intermediate CA) are already installed.
2. The private key is stored in the **Windows Certificate Store** under **Local Computer**.
3. You have administrative rights to perform the setup.

Follow the procedure below to grant read access:

1. Open **Certificate Manager** as Administrator.
2. Press **Win + R**, type mmc, and press **Enter**.
3. In the console, go to **File** and select **Add/Remove Snap-in**.
4. Select **Certificates** from the list and click **Add**.
5. Choose the **Computer account**, then click **Next**, followed by **Finish**, and then **OK**.
6. In the left panel, expand **Certificates (Local Computer)**, expand **Personal**, and select **Certificates**.
7. Identify the certificate that contains the private key.
8. Right-click the certificate, select **All Tasks**, and then select **Manage Private Keys**.
9. In the **Permissions** window, click **Add** and enter the non-admin username (for example, TESTIL) and click **OK**.
10. Select the **Read** permission, click **Apply**, and then click **OK**.



Granting private key access to a non-admin user

2.3. HaloCAD in Windows Environment

This section explains how to set up HaloCAD for Windchill using an installer for Windows-based Master and Replica Servers. The installer is included in the installation package.

2.3.1. Installation Modes

You can install the HaloCAD for Windchill component in the following modes:

1. **Graphical Mode**
   Graphical mode installation is an interactive, graphical user interface-based method that is driven by a wizard.
2. **Silent Mode**
   Silent-mode installation is a non-interactive method of installing the HaloCAD for Windchill component using command lines.

Prerequisites

Before installing HaloCAD, ensure that the following requirements are met:

1. Azure application registration details: Please refer to the Technical Reference Manual.
2. The certificate required for MPIP authentication must be installed in the Local Computer certificate store, along with the Root CA and Intermediate CA certificates.
   - If the certificate is CA-signed, install all related certificates in their respective stores (Root, Intermediate, and Personal).
   - If the certificate is self-signed, install it in both the Trusted Root Certification Authorities and Personal stores of the Local Computer.
3. Administrator rights: The user performing the HaloCAD installation must have administrator privileges.

   Installer selection: Use the installer based on your PTC Windchill version:

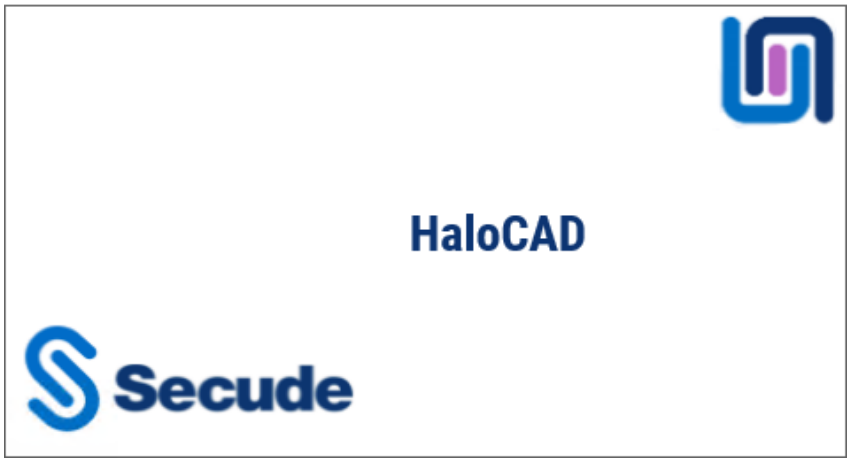
   - For **Windchill 13.1.0.0**, use the installer located in `<Product package>\<Version>\Windchill 13.1.0.0\windows`
   - For **Windchill 13.0.2.0** and **Windchill 13.0.2.4**, use the installer located in `<Product package>\<Version>\Windchill 13.0.2.x\windows`

2.3.1.1. Graphical Mode

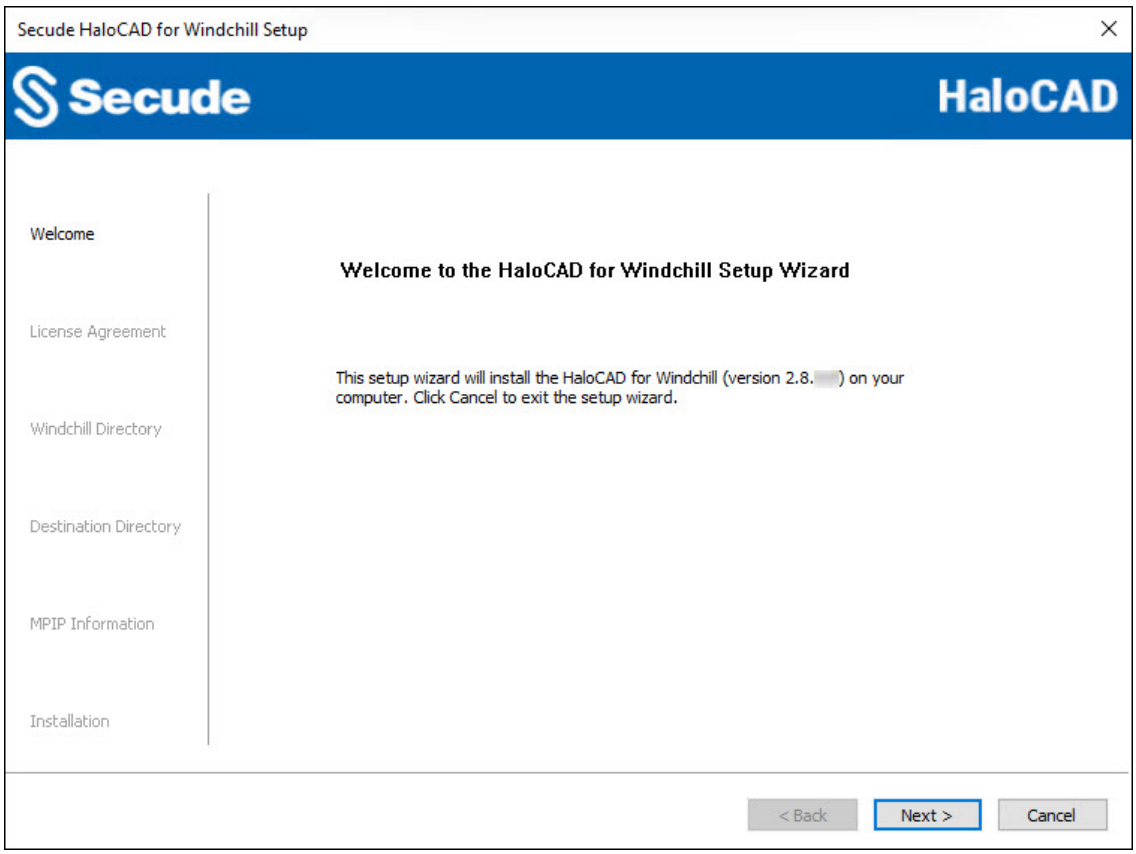
1. To begin the interactive installation, double-click the installer `HaloCAD_Windchill_Setup.exe` file. Depending on your Windows security settings, you may get a warning such as "*Do you want to*

allow the following program to make changes to this computer?". If you get this security warning, click the **Yes** button to continue the installation.

2. When the installer starts, the **Startup** dialog appears, followed by the **Welcome** dialog.

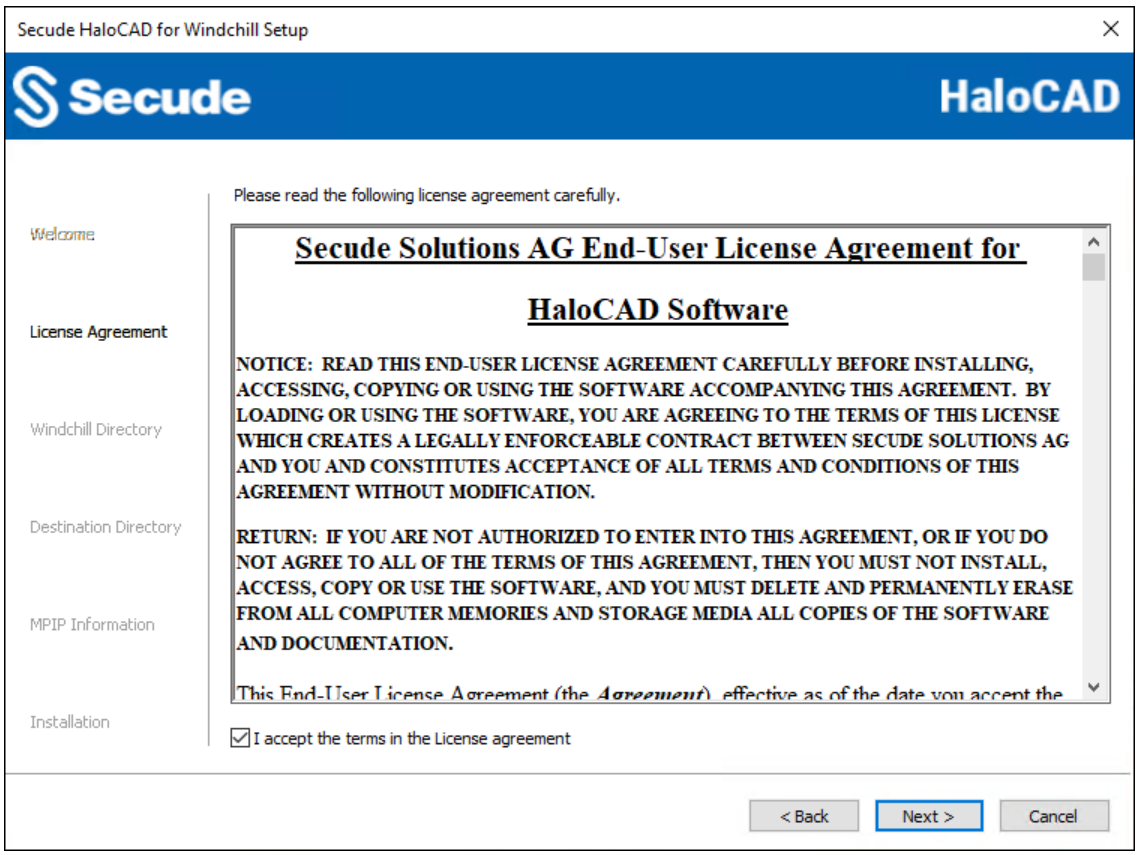


Startup dialog



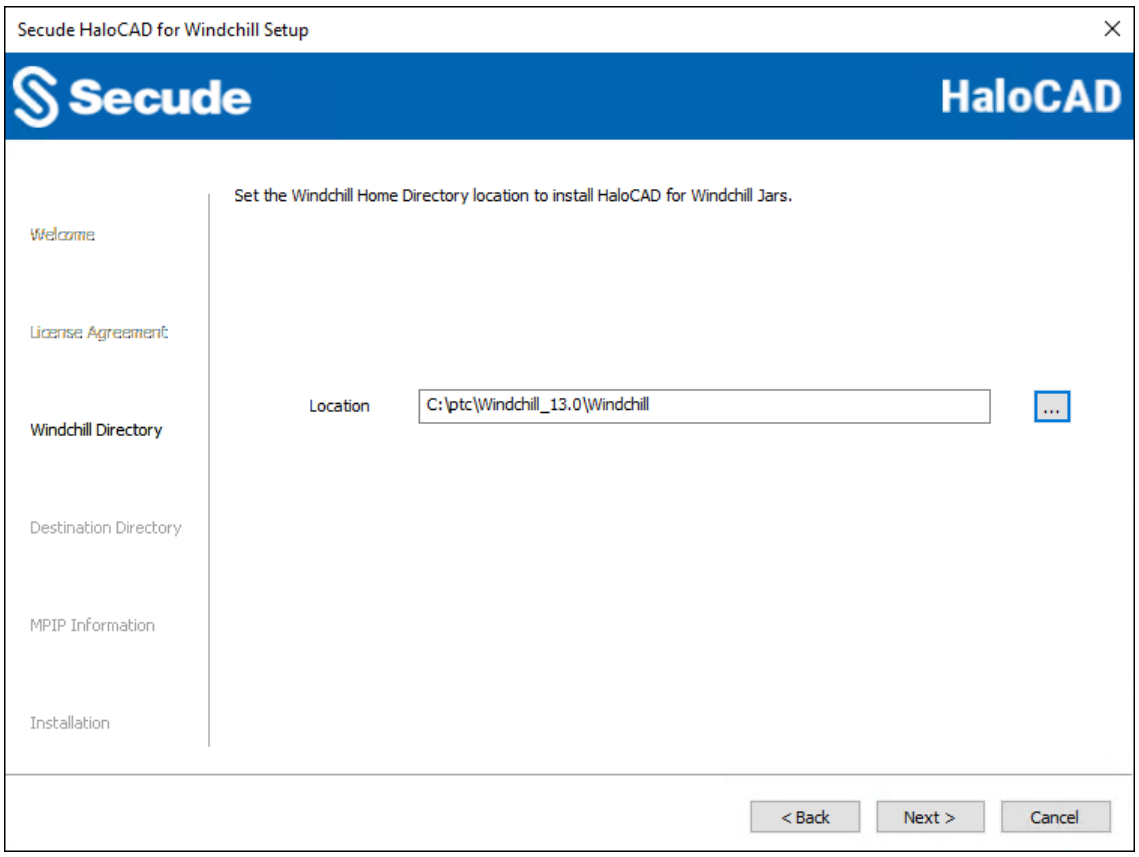
Welcome dialog

3. Click **Next** to continue the installation.
4. The **End-User License Agreement (EULA)** dialog appears.



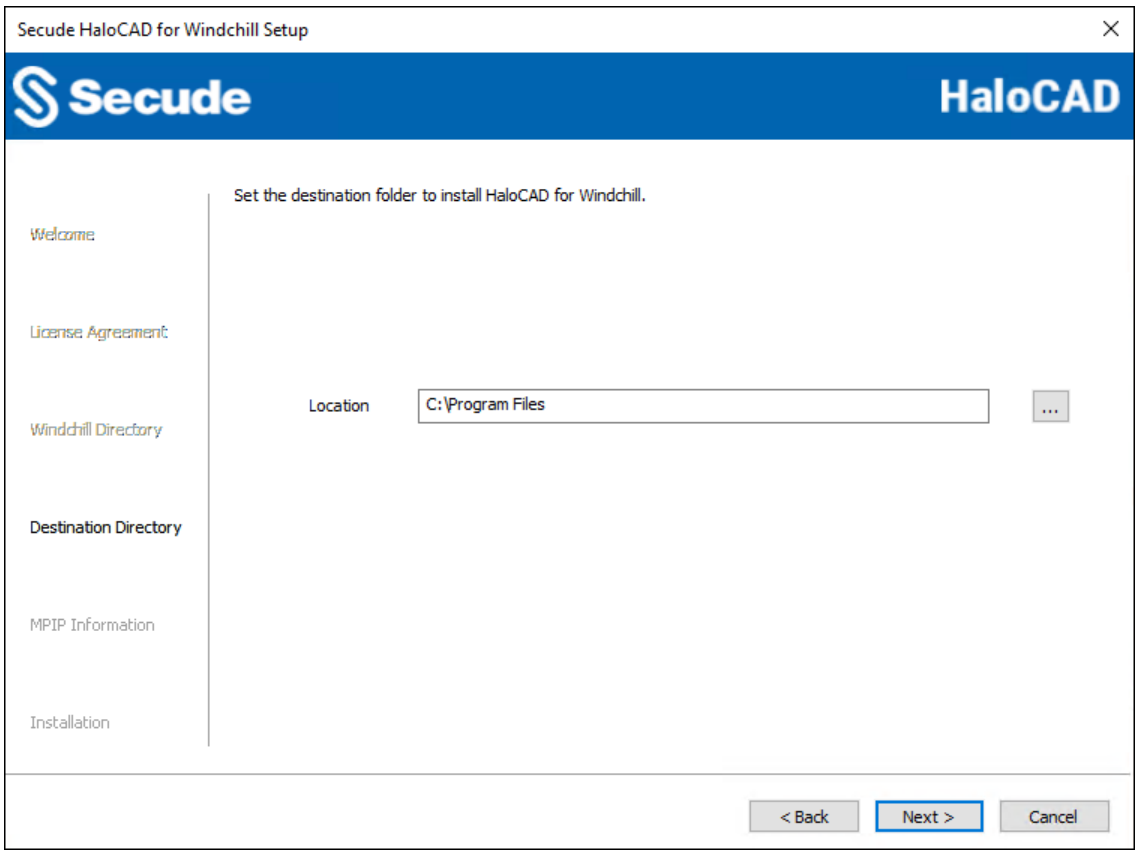
End-User License Agreement dialog

5. Read the **End-User License Agreement**. If you agree, select **I accept the terms in the License Agreement**, and click **Next** to continue.
6. The *Windchill Home Directory location* dialog appears:



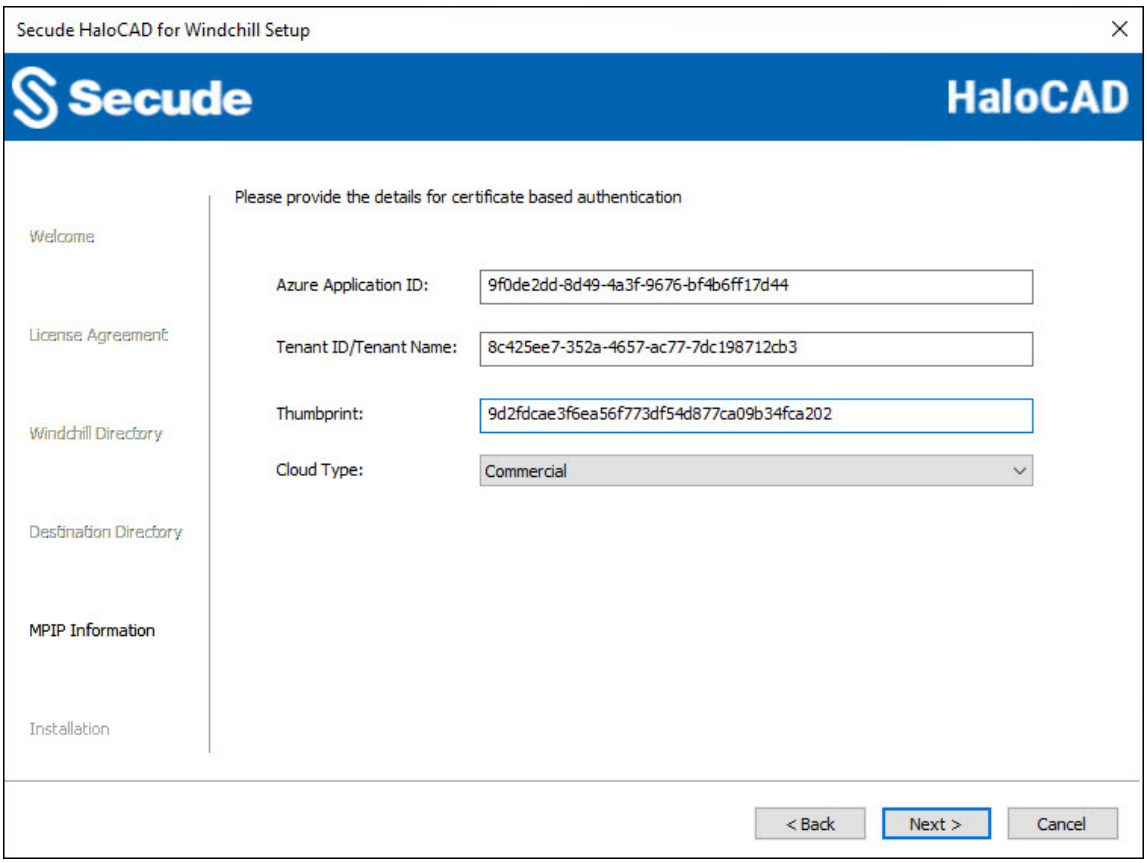
Windchill Home Directory Location dialog

7. Select the Windchill server's home directory in your system and click **Next**. For example, `C:\ptc\Windchill_13.0\Windchill`. Please ensure the correct home directory path is entered; otherwise, the installation will fail and display an error message as "*Windchill Home Directory path is incorrect. So please enter the correct path.*" To return to any point in the installation process, click the **Back** button (optional).
8. The destination folder selection dialog will appear:



Destination folder selection dialog

9. By default, application files are stored in the program files directory (`C:\Program Files`). If you would like to choose an alternate location, click the **Browse** button and select your location preference.
10. The certificate-based authentication dialog appears. To avoid errors, please ensure that you enter the correct Microsoft Entra ID application details in the installation wizard.



Certificate-based authentication dialog

a. **Azure Application ID**: Enter the unique identifier of your registered application. For example, `9f0de2dd-8d49-4a3f-9676-bf4b6ff17d44`

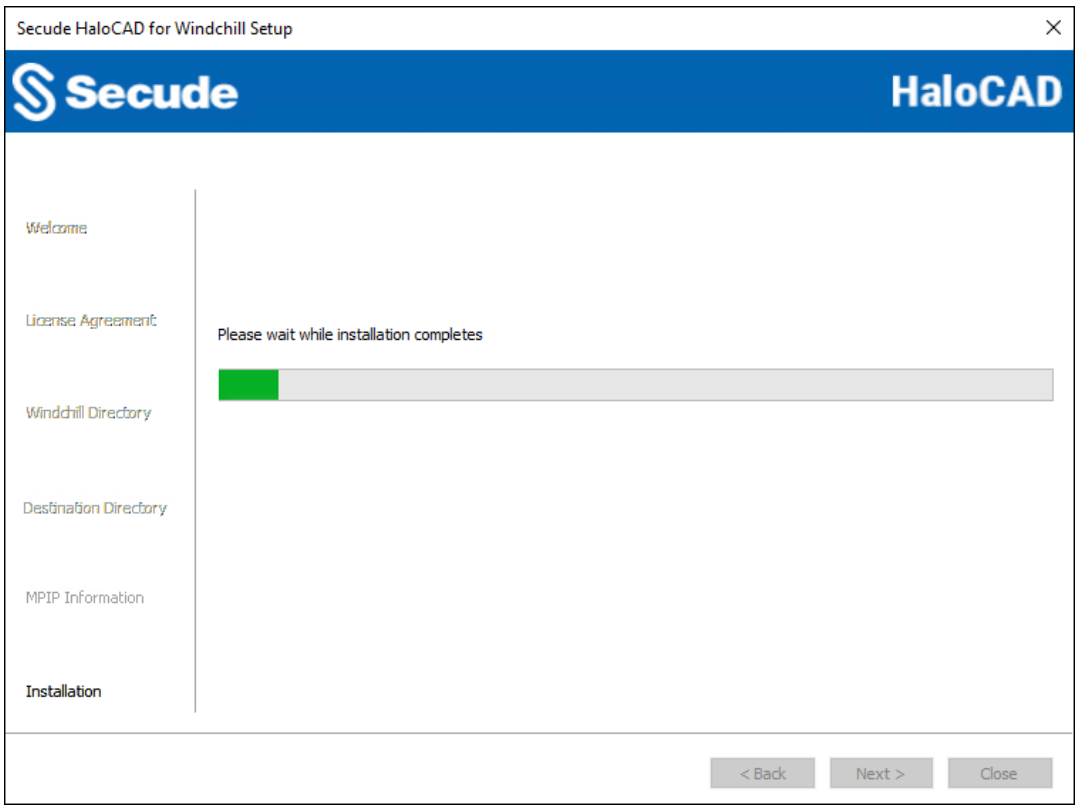
b. **Tenant ID/Tenant Name**: Enter your Microsoft Entra tenant name (for example, `contoso.onmicrosoft.com`) or its tenant ID (for example, `8c425ee7-352a-4657-ac77-7dc198712cb3`).

c. **Thumbprint**: Enter the thumbprint of the MPIP authentication certificate installed in the **Local Computer** certificate store. For example, `9d2fdcae3f6ea56f773df54d877ca09b34fca202`.

d. **Cloud Type**: **Commercial** is selected by default. Based on your Azure subscription and configuration, select the required cloud type from the list: Commercial, Custom, Germany, US_DoD, US_GCC, US_GCC_High, US_Sec, US_Nat, or China_01. If you select **Custom**, enter the appropriate URLs in the **Protection Cloud URL** (for example, `https://api.aadrm.com`) and **Policy Cloud URL** (for example, `https://dataservice.protection.outlook.com`) fields.

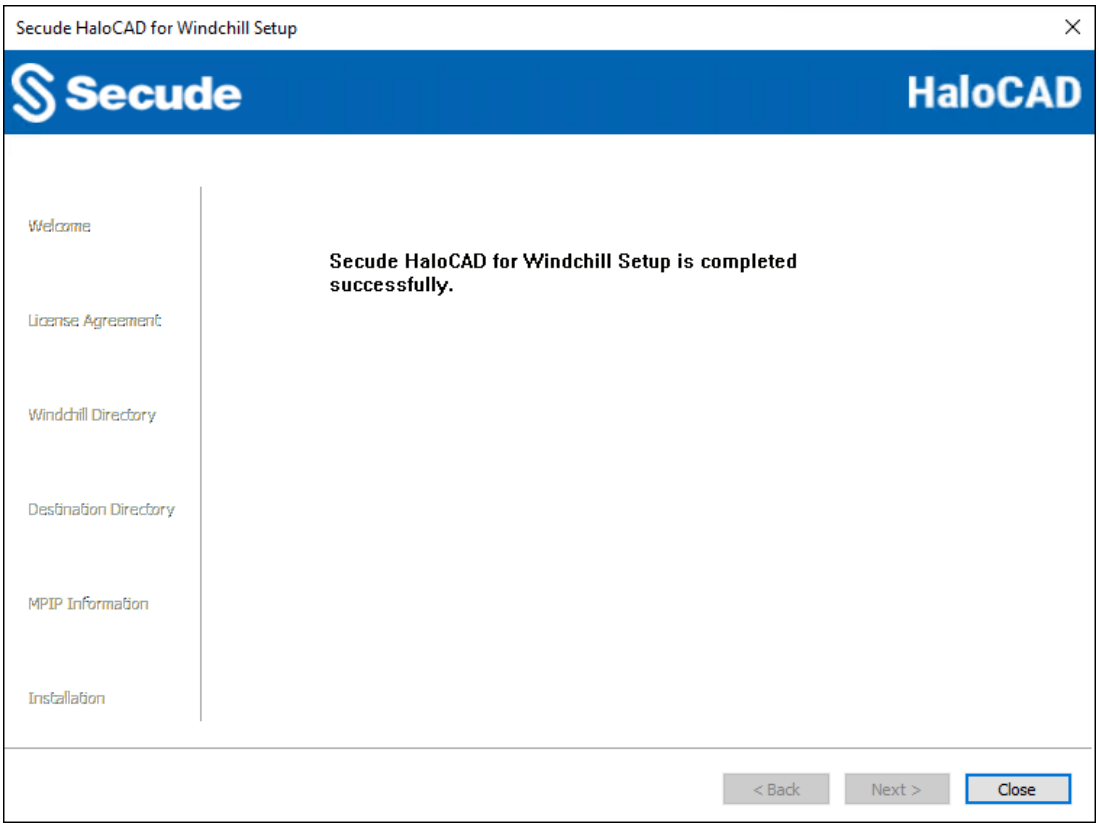
e. Click **Next**.

11. The installation begins, and the progress is displayed in the dialog.



Installation progress dialog

12. When the installation is complete, a message appears confirming that the HaloCAD component has been successfully installed.



Installation completed dialog

13. Click **Close** to close the installation wizard.

2.3.1.2. Silent Mode

Besides graphical mode, the HaloCAD for Windchill component can be installed in silent mode, which does not require user involvement or display a user interface. It is a convenient way to streamline the installation process using commands at once.

1. Open the Command Prompt with elevated rights (Run as Administrator).
2. Navigate to the directory of the HaloCAD for Windchill component installer.
3. To know the list of options available in silent mode, follow the steps given below:

   Type `HaloCAD_Windchill_Setup.exe -help`

   Press `Enter`

   Output

   ...

   ```
   HaloCAD_Windchill_Setup.exe -install -wdir <Windchill_Home_Directory> -dir
   <destination_directory> -applicationid <application_id> -tenantid <tenant_id> -
   thumbprint <thumb_print> -cloudtype
   <(Commercial|Custom|Germany|US_DoD|US_GCC|US_GCC_HIGH|US_Sec|US_Nat|China_01)> (if
   cloudtype is Custom) <protectioncloudurl> <policycloudurl>
   HaloCAD_Windchill_Setup
   ```

4. The following command illustrates how to install the HaloCAD for Windchill component.

   ```
   HaloCAD_Windchill_Setup.exe -install -wdir "C:\ptc\Windchill_13.0\Windchill" -dir
   "C:\Program Files" -applicationid "9f0de2dd-8d49-4a3f-9676-bf4b6ff17d44" -tenantid
   "8c425ee7-352a-4657-ac77-7dc198712cb3" -thumbprint
   "961602617275c2ab538cf28bb3648c0c6d97edab" -cloudtype "Commercial"
   ```

5. Press `Enter`.
6. The installation is complete.

2.3.2. Configuration Methods

This section describes two methods (command line and GUI) for configuring the parameters of HaloCAD for Windchill and HaloENGINE components.

2.3.2.1. Configuration Using Tool (GUI)

Prerequisites: Ensure that HaloCAD for Windchill is installed before proceeding.

Follow these steps to configure the settings through the GUI:

Step 1. Stop PTC Windchill

1. Launch the **Windchill Shell**.
2. Type the stop command `windchill stop` and press **Enter**.

   Result: A confirmation message appears indicating that the Server Manager stopped.

Step 2. Run the HaloCAD for Windchill Configuration Tool.

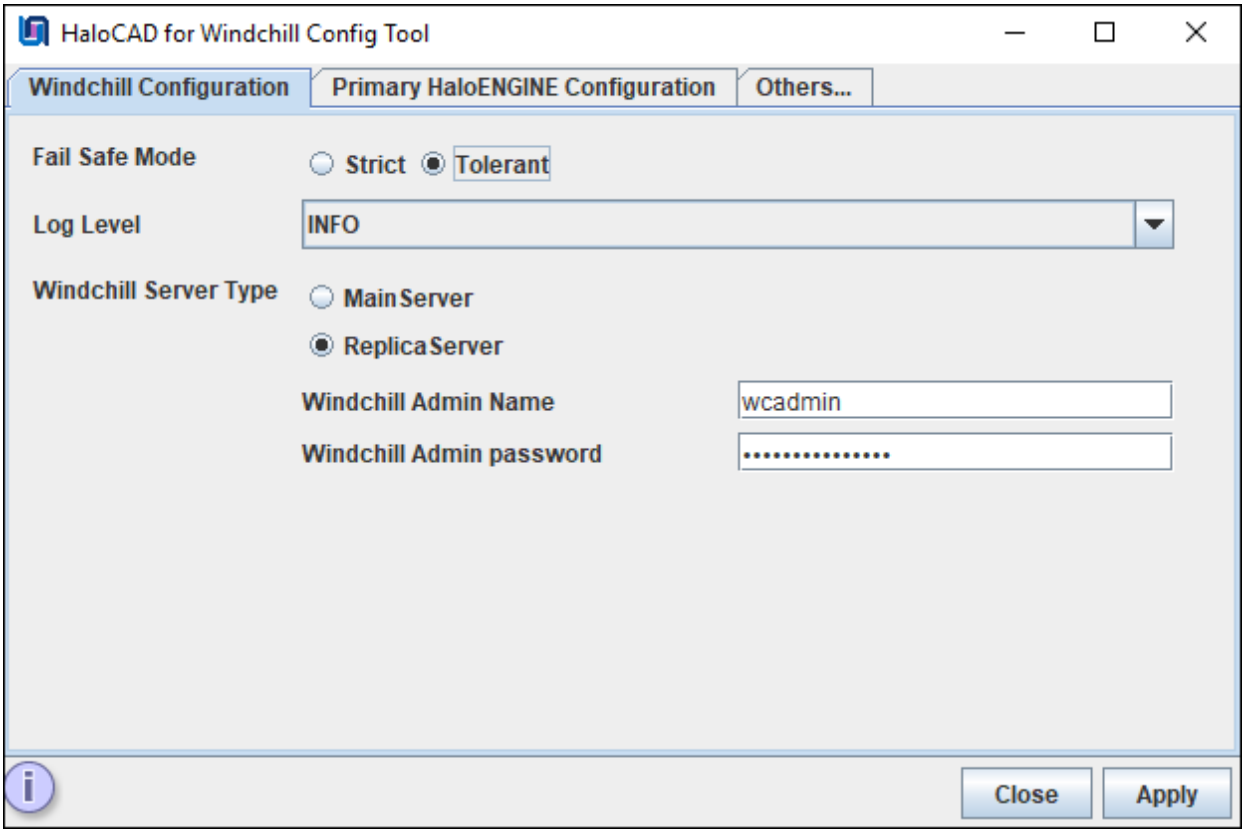
1. Navigate to the destination folder you specified during installation. The default folder is `C:\Program Files\Secude\HaloCADWindchill\config`.
2. Double-click the jar file or type the following syntax and press **Enter** in either the Windows command prompt or Windchill Shell with administrative privileges.

   Syntax: `<pathtojar>java -jar halocad-windchill-config-<version>.jar`

   For example: `C:\Program Files\Secude\HaloCADWindchill\config>java -jar halocad-windchill-config-<version>.jar`

Result: The **HaloCAD for Windchill Config Tool** window is displayed.

Step 3. Enter the following information under the **Windchill Configuration** tab.



Windchill configuration tab

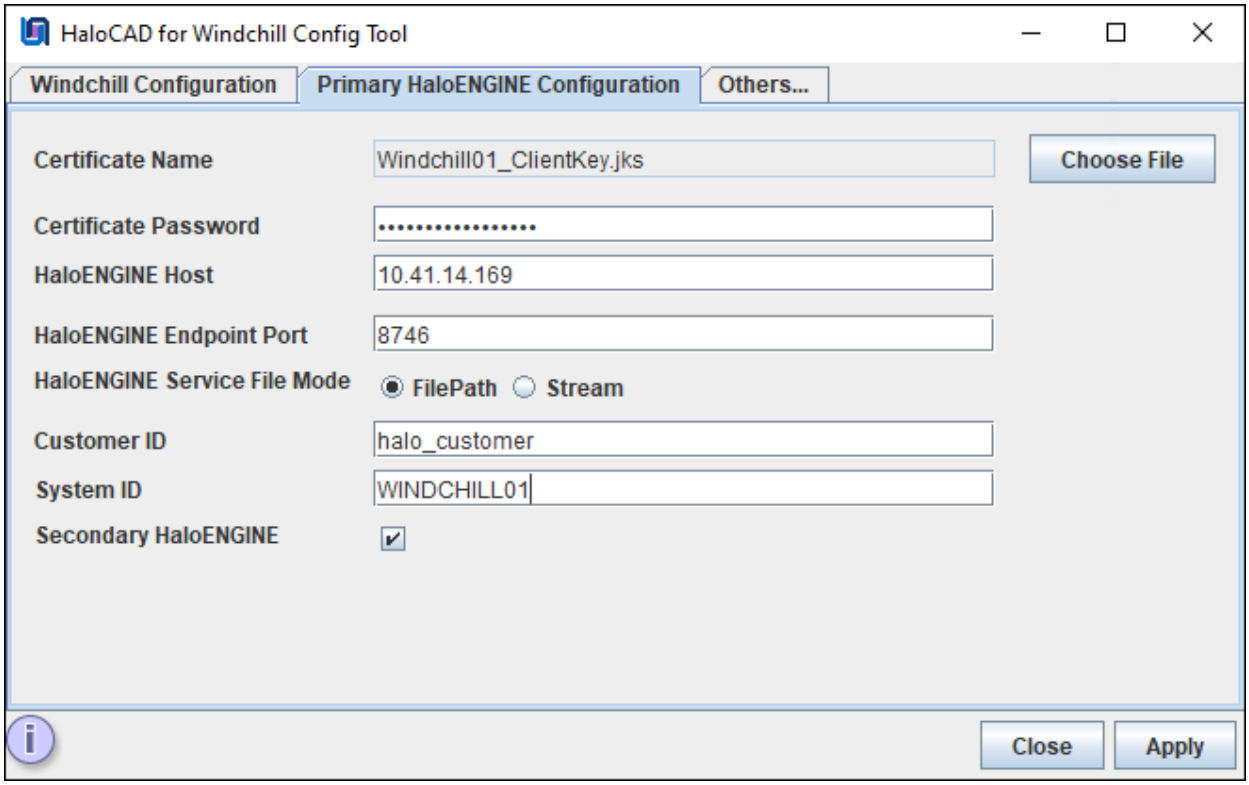
1. **Fail Safe Mode**: The Fail-Safe Mode controls the system's behavior in case of inconsistencies that prevent the specified protection from being applied (conflicting configuration, server component unreachable, or returning an error message, etc.). You can define any one of the following:
   a. **Strict**: The file upload or download will be blocked whenever any error occurs.
   b. **Tolerant** (default): The file upload or download will be allowed, even when an error occurs.
2. **Log Level**: Select a log level of your choice.
   a. **INFO** (default): A standard log level that highlights the progress of the application.
   b. **ERROR**: Logs error events that prevent program execution.
   c. **DEBUG**: Logs detailed tracing messages. It should be used for information required for diagnosing issues and troubleshooting.
3. **Windchill Server Type**: Choose one of the following options based on your environment.
   a. **MainServer**: If you have only the Main Server, select **Main Server** in **Windchill Server Type**. By default, the UI displays **Disable Windchill REST**, indicating that the Windchill REST service is disabled. You can enable it to retrieve application data from the Main Server by selecting **Enable Windchill REST**.

      Note: Enabling the REST service is required only when the Main Server is linked to a Replica Server and files are downloaded from it.
   b. **ReplicaServer**: This option applies to the **Windchill File Server/Windchill Content Cache Server**, which acts as a remote site in the Windchill environment. It is a lightweight server that stores master data but does not host the Windchill database. The master server manages the database metadata and maintains information about the files stored on the File Server. If you select this option, you must configure the following:
      - **Windchill Admin Name**: Enter the administrator's name for the Main Server. For example, `wcadmin`.
      - **Windchill Admin password**: Enter the administrator password.
4. Click **Apply**. A red tooltip message appears if any required values are missing. Enter the missing information and click **Apply** to continue.

Result:

- A confirmation message dialog box appears.
- Click **OK** to close the dialog box.
- The configuration files are generated in the installation directory.

Step 4. Go to the **Primary HaloENGINE Configuration** tab, and then enter the following information.



Primary HaloENGINE configuration tab

1. **Certificate Name**: Click **Choose File** to browse and select the client Keystore in JKS format, generated by the HaloENGINE Admin Portal [through which communication is established between HaloENGINE (primary) and Windchill]. For example, `Windchill01_ClientKey.jks`
2. **Certificate Password**: Enter the password of the selected client Keystore. For example, `Key$T#123`
3. **HaloENGINE Host**: Enter the IP address/FQDN of HaloENGINE. For example, `10.41.14.169`
4. **HaloENGINE Endpoint Port**: Enter the endpoint port from which HaloENGINE can be accessed. For example, `8746`
5. **HaloENGINE Service File Mode**: Select the file transmission method.
   a. **FilePath** (default): File stored in a local temporary location for the encryption and decryption process. Here, file path information is used for transferring.
   b. **Stream**: File as a sequence of bytes.
6. **Customer ID**: Enter the Customer ID that has been assigned in the Admin Portal. For example, `halo_customer`.
7. **System ID**: Enter the Windchill Server's hostname, and the same must be entered in the **System Unique ID** (HaloENGINE admin portal). For example, `WINDCHILL01`

8. **Secondary HaloENGINE**: If you want to set up a failover mechanism in your environment, select this check box. HaloCAD supports connection failover between two HaloENGINEs. For more information, please refer to the section "Failover Mechanism for HaloENGINE in HaloCAD for PLM".
9. Click **Apply**. A red tooltip message appears if any required values are missing. Enter the missing information and click **Apply** to continue.

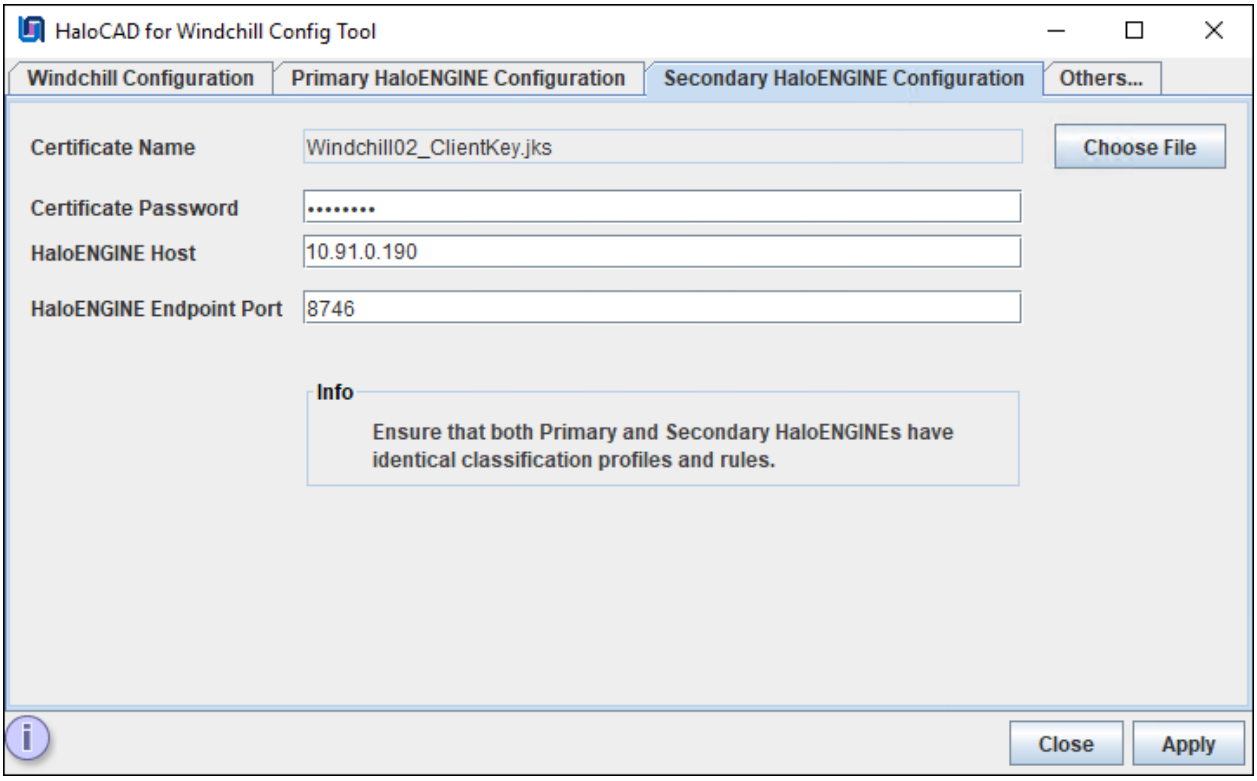
Result:

- A confirmation message dialog box appears.
- Click **OK** to close the dialog box.
- If the **Secondary HaloENGINE** option is selected, the **Secondary HaloENGINE Configuration** tab appears in the Configuration Tool (see step 5). Otherwise, proceed to step 6.

Step 5. Go to the **Secondary HaloENGINE Configuration** tab, and then enter the following information.

If you have not selected the Secondary HaloENGINE option on the Primary HaloENGINE Configuration tab, skip this step. This step is required only if you plan to use the failover mechanism.

Prerequisite: Ensure that the secondary HaloENGINE uses the same configuration profiles and rules as the primary HaloENGINE. This ensures that, if the primary HaloENGINE fails, the secondary HaloENGINE can immediately take over and maintain uninterrupted operation.



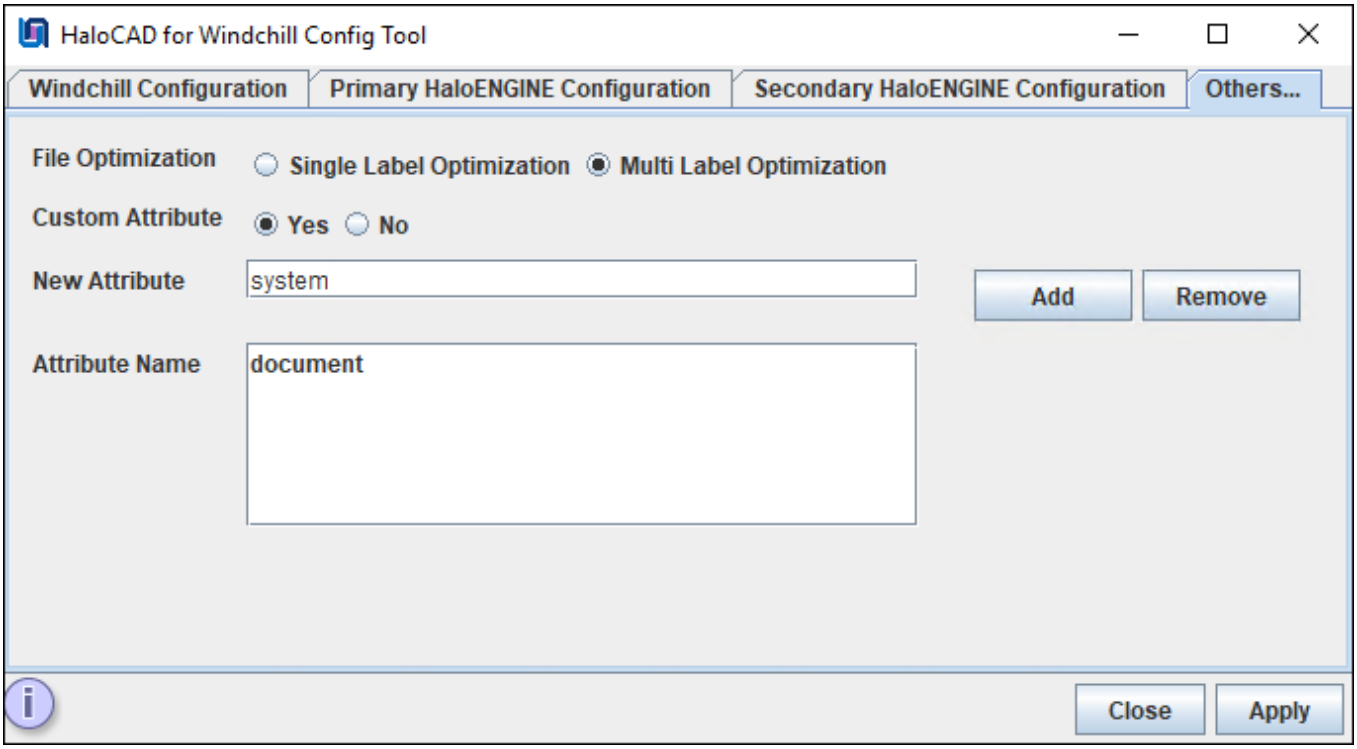
Secondary HaloENGINE configuration tab

1. **Certificate Name**: Click **Choose File** to browse and select the client Keystore in JKS format, which is generated by the HaloENGINE Admin Portal [through which communication is established between HaloENGINE (secondary) and Windchill]. For example, `Windchill02_ClientKey.jks`
2. **Certificate Password**: Enter the password of the selected client Keystore. For example, `Key$T#1234`
3. **HaloENGINE Host**: Enter the IP address/FQDN of HaloENGINE. For example, `10.91.0.190`
4. **HaloENGINE Endpoint Port**: Enter the endpoint port from which HaloENGINE can be accessed. For example, `8746`
5. Click **Apply**. A red tooltip message appears if any required values are missing. Enter the missing information and click **Apply** to continue.

Result:

- A confirmation message dialog box appears.
- Click **OK** to close the dialog box.

Step 6. Go to the **Others** tab, and then enter the following information.



Others tab

1. **File Optimization**: Choose one of the following options for file optimization. By default, **Single Label Optimization** is set.
   a. **Single Label Optimization:** The top-level file label is considered and applied to all dependent files.

b. **Multi Label Optimization:** Each file type group label defined in the Classification Engine is considered and applied to the corresponding group during ASM optimization.

2. **Custom Attribute** (Global Attribute)
   a. If you do not want to use custom attributes, simply click **Apply** and **Close** the configuration tool window.
   b. If you want to use custom attributes, choose **Yes** in **Custom Attribute**, and then fill out the following information.
3. **New Attribute**: Enter the name of an attribute and then click **Add**. For example, the **document** is a new attribute added to the list.
4. The attribute will be added to the **Attribute Name** list.
5. Click **Apply**. A red tooltip message appears if any required values are missing. Enter the missing information and click **Apply** to continue.

Result:

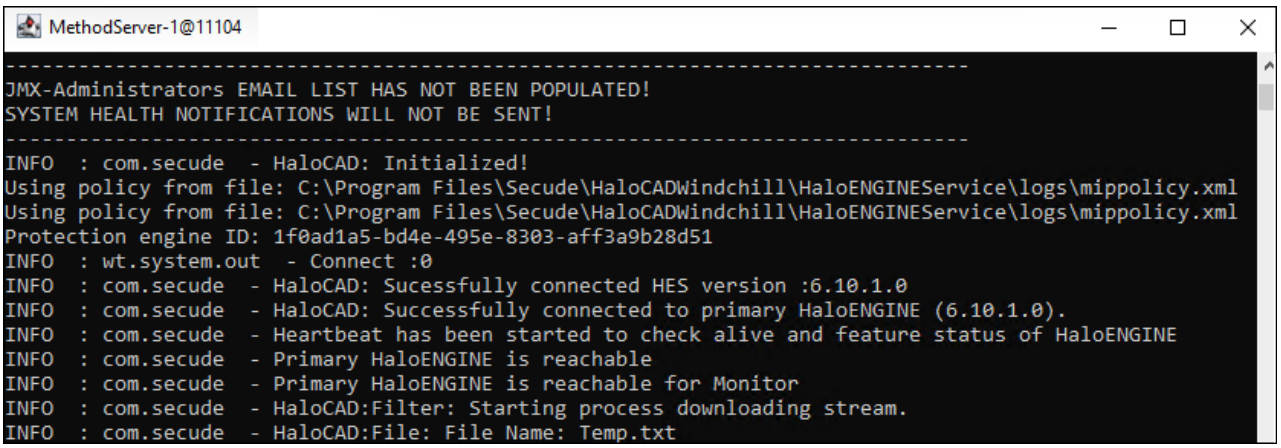
- A confirmation message dialog box appears.
- Click **OK** to close the dialog box.
- Click **Close** to exit the Configuration Tool.
- To remove an attribute from the list, select the attribute, click **Remove**, and then click **Apply** to save the configuration.

Step 7. Start Windchill.

1. Close and reopen the Windchill shell.
2. Type the start command `windchill start` and press **Enter**.

Result:

- A confirmation message appears indicating *"wt.manager.ServerLauncher - Starting Server Manager"*.
- During initialization, the **MethodServer** log displays messages that confirm the configuration was successful.



Sample log file output

Related tasks

- The same logs can be seen in the `MethodServer-xxx-log4j.log` file.
- HaloCAD for Windchill component-related activities are logged in `%WINDCHILL_HOME%\Windchill\logs`.

2.3.2.2. Configuration Using the Command Line

This is an alternative method of configuring the HaloCAD and HaloENGINE parameters using the command line.

Prerequisite: Ensure that HaloCAD for Windchill has been installed.

Follow the command-line instructions. A sample is provided below:

1. Open the Windchill Shell window, type `java -jar halocad-windchill-config-<version no>.jar -shell`, and press **Enter**.

```
C:\Program Files\Secude\HaloCADWindchill\config>java -jar halocad-windchill-config-
 <version>.jar -shell
--------------------------------------------------------------------------------
HaloCAD for Windchill Config Path: C:\Program Files

1. Windchill Configuration
2. Primary HaloENGINE Configuration
3. Others...
0. Exit
Note: If an invalid value is entered, the default value will be applied.

Please choose an option:
1
--------------------------------------------------------------------------------
Windchill Configuration:
```

```
--------------------------------------------------------------------------------
Fail Safe Mode: (Default:Tolerant)
1. Tolerant
2. Strict

Please choose an option:
1

Log Level: (Default:INFO)
1. INFO
2. DEBUG
3. ERROR

Please choose an option:
2

Windchill Server Type: (Default:MainServer)
1. MainServer
2. ReplicaServer

Please choose an option:
1

Windchill REST: (Default:Disable Windchill REST)
1. Disable Windchill REST
2. Enable Windchill REST

Please choose an option:
1
Saved Successfully.
--------------------------------------------------------------------------------
Windchill Configuration:

Fail Safe Mode                  :Tolerant
Log Level                       :DEBUG
Windchill Server Type           :MainServer
Windchill REST                  :Disable Windchill REST

1. Modify all configuration
2. Modify the particular configuration
3. Back to main menu
0. Exit

Please choose an option:
```

```
3
--------------------------------------------------------------------------------
1. Windchill Configuration
2. Primary HaloENGINE Configuration
3. Others...
0. Exit
Note: If an invalid value is entered, the default value will be applied.

Please choose an option:
2
--------------------------------------------------------------------------------
Primary HaloENGINE Configuration:
--------------------------------------------------------------------------------
Enter the Certificate Path:
C:\Users\Administrator\Desktop\Windchill01_ClientKey.jks
File name:Windchill01_ClientKey.jks.

Enter the Certificate Password:

Secondary HaloENGINE: (Default:Disable)
1. Disable
2. Enable

Please choose an option:
1

Enter the HaloENGINE Host:
10.41.14.169

Enter the HaloENGINE Endpoint Port: (Default:8746)
8746

Enter the Customer ID:
halo_customer

Enter the System ID:
WINDCHILL01

HaloENGINE Service File Mode: (Default:File Path)
1. File Path
2. Stream

Please choose an option:
2
```

```
Saved Successfully.
--------------------------------------------------------------------------------
Primary HaloENGINE Configuration:

Certificate Name                :Windchill01_ClientKey.jks
HaloENGINE Host                 :10.41.14.169
HaloENGINE Endpoint Port        :8746
HaloENGINE Service File Mode    :Stream
Customer ID                     :halo_customer
System ID                       :WINDCHILL01
Secondary HaloENGINE            :Disabled

1. Modify all configuration
2. Modify the particular configuration
3. Back to main menu
0. Exit

Please choose an option:
3
--------------------------------------------------------------------------------
1. Windchill Configuration
2. Primary HaloENGINE Configuration
3. Others...
0. Exit
Note: If an invalid value is entered, the default value will be applied.

Please choose an option:
3
--------------------------------------------------------------------------------
Others...

File Optimization               :Single Label Optimization
Custom Attribute                :No

1. File Optimization
2. Custom Attribute
3. Back to main menu
0. Exit

Please choose an option:
2
--------------------------------------------------------------------------------
Custom Attribute: (Default:No)
1. No
```

```
2. Yes

Please choose an option:
1
Custom Attribute Disabled Successfully.
--------------------------------------------------------------------------------
Others...

File Optimization               :Single Label Optimization
Custom Attribute                :No

1. File Optimization
2. Custom Attribute
3. Back to main menu
0. Exit

Please choose an option:
```

2. Click **Close** to close the Windchill Shell.

2.4. Configuring the Tomcat Service

About the Term "HaloENGINE Tomcat Service"

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

During installation, Azure details are provided to initialize the HaloENGINE Tomcat Service. After successful authentication, the labels are fetched automatically. To update MPIP-related details (such as the Application ID), use `heslibconfig.exe`.

Default locations of log files

Name	Default Path
HaloCAD log	`C:\Program Files\Secude\Tomcat\logs\haloproxy.log`.
Configuration tool	`C:\Program Files\Secude\HaloCADWindchill\HaloENGINEService\lib\heslibconfig.exe`
MIP logs	`C:\Program Files\Secude\HaloCADWindchill\HaloENGINEService\logs\mip_cache_storage\mip\logs`

Default locations

To update your Azure details, follow the procedure below.

- Open the Command Prompt with elevated rights (Run as Administrator).
- Navigate to the directory where `heslibconfig.exe` is located.
- To view the list of available options in silent mode, enter the following command:

  Type `heslibconfig.exe -help`

  Press `Enter`

  Output

  ```
  Usage:
  heslibconfig.exe -testmip
  heslibconfig.exe -update -applicationid <application_id> -tenantid <tenant_id> -thumbprint <thumb_print> -cloudtype <(Commercial|Custom|Germany|US_DoD|US_GCC|US_GCC_HIGH|US_Sec|US_Nat|China_01) (if cloudtype is Custom) <protectioncloudurl> <policycloudurl>
  ```
- The following command illustrates how to update json file.

  ```
  heslibconfig.exe -update -applicationid 9f0de2dd-8d49-4a3f-9676-bf4b6ff17d44 -tenantid 8c425ee7-352a-4657-ac77-7dc198712cb3 -thumbprint 961602617275c2ab538cf28bb3648c0c6d97edab -cloudtype Custom https://api.aadrm.com https://dataservice.protection.outlook.com
  ```
- A confirmation message appears stating that the configuration JSON file location has been successfully updated, `...\config\HaloENGINESVC.json`

Configuration change in JSON File

After installation, navigate to the configuration folder`...\HaloENGINEService\config`, and you will find a JSON file that contains the HaloENGINE Tomcat Service configuration properties. Note: From the list of default parameters, only the parameters listed below should be modified, and only when necessary. All other parameters must remain at their default values to ensure proper system functionality and stability.

Name	Description
block_pii	Enable or disable the visibility of Personally Identifiable Information (PII) in the MIP SDK logs. • false—PII will be visible in clear text in the MIP SDK logs. • true—PII will be masked with asterisks in the MIP SDK logs. This helps to protect the PII's confidentiality.

Name	Description
cachetype	MPIP cache storage type used by the service. • In Memory—0, maintains the storage cache in memory in the application. • On Disk—1 (default storage type), stores the database (SQLite3) on disk in the directory provided in the settings object. The database is stored in plaintext. • On Disk Encrypted—2, stores the database (SQLite3) on disk in the directory provided in the settings object. The database is encrypted using OS-specific APIs.
cacheuserlicense	• 0—false, End User License (EUL) will NOT be stored in the MPIP cache storage. • 1—true (default value), End User License (EUL) will be stored in the MPIP cache storage
databoundary	Audit and telemetry events are sent to the nearest collector, where these events are stored and processed. Other options: 1. Asia 2. Europe_MiddleEast_Africa 3. European_Union 4. North_America For example, if your AIP administrator sets North_America, the HaloENGINE Tomcat Service forces all telemetry and audit data to go directly to North America.
enabledke	Double Key Encryption • 0 (default value)—Disables the DKE functionality in the HaloENGINE Tomcat Service. • 1 (On)—Enables the DKE functionality in the HaloENGINE Tomcat Service. Please be aware that DKE labels are only visible when DKE functionality is enabled.

Name	Description
enablefiletracking	To register a protected file to track and revoke. • 0 (default value)—the protected file will not be registered for file tracking and access revocation. • 1—The protected file will be registered for file tracking and access revocation
enableminimaltelemetry	To transmit diagnostic information to Microsoft. • 0 (default value)—all diagnostic events are transmitted. • 1—Minimum diagnostic events are transmitted.
log_level	The available log levels are ERROR, WARNING, INFO, and DEBUG.
log_purge	It indicates removing files older than a defined time frame. By default, the log files older than 7 days will be deleted.
streambuffersize	It is a buffer size used for memory-based encryption with the MIP SDK. When the allotted buffer size is exceeded, an additional memory of stream buffer size is allocated, and this process is repeated until the encryption/decryption operation is completed. The default setting is 10MB.
templatefile_purge	Defines the purge time of template files that are generated for every CAD assembly file (compound file) download. The default value set is one hour. For example, when a file is downloaded at 15:25 hours, the HaloENGINE Tomcat Service creates a template file in the tmp\GUID folder (which can be located in the HaloENGINE Tomcat Service user's profile folder). In the background, it examines and deletes files that have reached the configured time, i.e., after 16:25 hours. Note: This is only applicable in the event of CAD assembly file labeling.

HaloENGINE Tomcat service configuration

2.4.1. WinHTTP Proxy Settings

To allow MIP SDK to use the proxy settings set up in your environment, follow the steps below:

Determine whether the proxy server has been properly set up by running the following command.

```
C:\Windows\system32>netsh winhttp show proxy
```

```
Current WinHTTP proxy settings:

Direct access (no proxy server).
```

If the response to the command is as shown above, it indicates that the proxy server has not been configured in the registry for WinHTTP.

To configure the proxy server for WinHTTP, use the following command:

Syntax: `C:\Windows\system32>netsh winhttp set proxy <proxyservername>:<portnumber>`

Example: `C:\Windows\system32>netsh winhttp set proxy 190.160.166.191:8080`

In this case, the proxy server has been set up with `190.160.166.191:8080`. Once this command is executed successfully, the registry is updated with the proxy server URL, and the HaloENGINE Tomcat Service ensures that the configured proxy settings are applied.

3. Updating the HaloCAD Configuration

In both Windows and Linux environments, you can alter the configuration at any time by using either the HaloCAD Configuration Tool (GUI) or the command line.

4. Appendix

This section provides supplemental information.

4.1. Enabling Split Authentication

In a Windchill setup with Single Sign On (SSO) implemented on the master/main server and a replica server connected to it, HaloCAD has a limitation when obtaining metadata from the replica server using SSO-based authentication.

Split authentication can overcome HaloCAD's limitation in accessing REST calls from the replica server to the main server. All other activities are performed using SSO authentication or customized authentication that the customer uses, except for HaloCAD operations on the replica server.

PTC has recommended this solution, and it can be found in Knowledge Base Article CS291543. The following example shows how to configure split authentication for the HaloCAD Controller endpoint on the main server.

Follow the steps for the configuration:

1. Stop the Windchill and Apache servers.
2. In the HTTPServer directory `<WT_HOME>\HttpServer\conf\conf.d` (for example, `C:\ptc\Windchill_12.0\HTTPServer\conf\conf.d`), create a new configuration file with a number higher than the existing `<number>-app-Windchill-Auth.conf` file. For example, if there is a file with `39-app-Windchill-Auth.conf`, you can create one with `40-app-Windchill-Auth.conf`.
3. Now enter the following values into the file and save it.

```
<LocationMatch ^/+Windchill/+servlet/+HALOCADController(;.*)?>
      AuthName "Windchill"
      AuthType Basic
      AuthBasicProvider Windchill-LDAP
      Require valid-user
</LocationMatch>
```

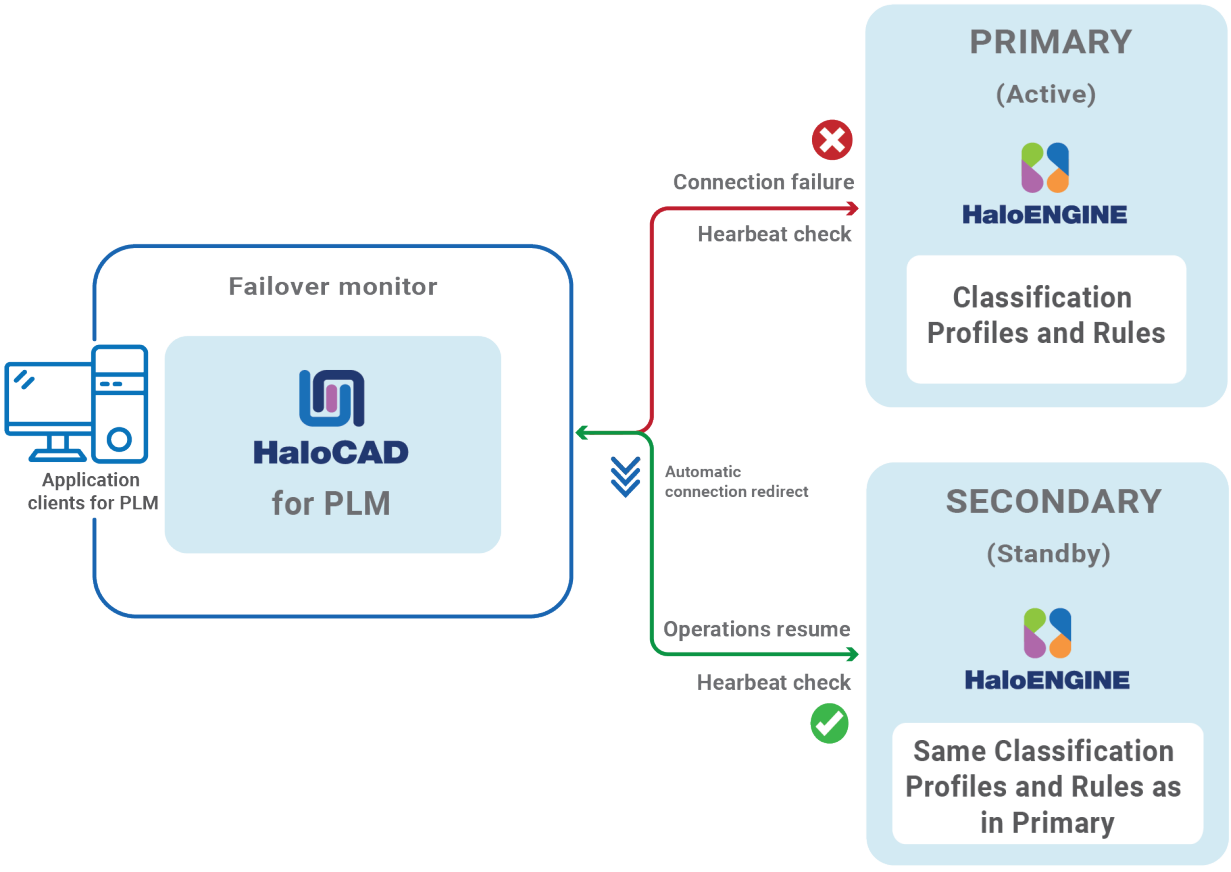
4. Restart the Windchill and Apache servers.

4.2. Failover Mechanism for HaloENGINE in HaloCAD for PLM

Server failover between two systems supports uninterrupted operation and service reliability in case of a breakdown. The server failover configuration is "active-standby," meaning that the primary server is "active", and the secondary server is "standby."

HaloCAD for PLM supports connection failover between two HaloENGINEs. Here's a summary of its purpose:

1. **High Availability**: If the primary HaloENGINE fails, the secondary HaloENGINE will take over, reducing downtime and maintaining continuous operation.
   Example: Let us assume that your business process requires no downtime.
   As per the business security policy, your administrator has configured Fail-Safe Mode as Strict to block any file upload or download whenever an error occurs. If HaloENGINE encounters an unexpected issue, failure to obtain label information will prevent file download or upload. In this instance, the failover mechanism in HaloENGINE will be the ideal option for dealing with such unforeseen scenarios, with no impact on the end user. Thus, even if the primary HaloENGINE connection fails, HaloCAD recognizes the failure and instantly switches to the secondary HaloENGINE to continue providing services.
   Once the primary HaloENGINE is restored, it will be a standby for the secondary HaloENGINE. If there is any failure in the secondary HaloENGINE, the primary HaloENGINE will again take over the operations.



Failover Mechanism for HaloENGINE in HaloCAD for PLM

2. **Redundancy**: It provides redundancy, which means there is always another HaloENGINE ready to take over if the primary one fails. This minimizes the possibility of a single point of failure.

3. **Data Integrity and Consistency**: In the event of a failure, the failover technique can help guarantee that data is consistent and file upload/download activities are not lost, which is crucial for systems that rely on high data security.

Failover Mechanism Requirement

1. Network Infrastructure: Minimal Secondary HaloENGINE needs to be segmented so that the primary and secondary HaloENGINEs don't share the same network.
2. Data replication: Both HaloENGINEs must have the same classification profiles and rules.

4.3. Third-Party Libraries

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 HaloCAD for Windchill are shown in the table below.

Library	Version	Source Code	License Link
commons-io	2.+	https://mvnrepository.com/artifact/commons-io/commons-io	https://www.apache.org/licenses/LICENSE-2.0.txt
jna	5.13.0	https://mvnrepository.com/artifact/net.java.dev.jna/jna	http://www.apache.org/licenses/LICENSE-2.0.txt http://www.gnu.org/licenses/licenses.html
jna-platform	5.13.0	https://mvnrepository.com/artifact/net.java.dev.jna/jna-platform	http://www.apache.org/licenses/LICENSE-2.0.txt http://www.gnu.org/licenses/licenses.html
MIP SDK	1.16.126.0	https://learn.microsoft.com/en-us/information-protection/develop/version-release-history	https://docs.microsoft.com/en-us/information-protection/develop/
MSAL	4.73.1	https://github.com/AzureAD/microsoft-authentication-library-for-dotnet	https://github.com/AzureAD/microsoft-authentication-library-for-dotnet/blob/master/LICENSE

Library	Version	Source Code	License Link
Spdlog	1.15.3	-	https://github.com/gabime/spdlog

Third-party libraries

4.4. Metadata Definition

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

Windchill metadata	Use
server_name	Derivation from server name (FQDN of the Windchill server). (For example, `svin0007.secude.local`)
user_name	Derivation from Windchill logged-in users. (For example, John and Derek)
file_name	Derivation from the file name.
project_name	Derivation from the project name. (For example, Windchill)
product_name	Derivation from product name (For example, Windchill).
lifecycle_template	Derivation from the lifecycle of a file. Lifecycle provides an overview of how business items develop and serves as a model for the commercialization process. The lifecycle templates may be of the following types: Approval, Basic, Default, and so on. (For example, `Pipeline.prt` - Default)
user_role	Derivation from the user role. (For example, Designer and Engineer)
lifecycle_state	Derivation from the lifecycle of a file. Each phase of a lifecycle template is associated with a lifecycle state. There are different kinds of lifecycle states. 1. Approval (template): In work, under review, approved (states) 2. Basic (template): Basic: In work, released, canceled (states) 3. Default (template): Default: In work, under review, released (states)

Windchill metadata	Use
	(For example, `Pipeline.prt`- Default-released)
security_label	Derivation from Windchill access control policy. For more details, please refer to the online PTC Windchill documentation. (For example, Export Control, Corporate Proprietary, and Third Party Proprietary)
file_type	Derivation from file type (Creo file types and MS Office native file types). (For example, sec, prt, asm, xlsx)
library_name	Derivation from the library name. (For example, Density, Wheel, and Pipeline)
workspace_name	Derivation from workspace. (For example, Generic_computer and Drive System)
system_context	Derivation from the origin of the data. (For example, Generic_computer, and Drive System)
preexpression_custom_pre-expression	Derivation from custom pre-expression. 1. Yes 2. No

Windchill metadata

4.5. Download Log Definition

This section explains the log definition for every log format that HaloENGINE supports.

4.5.1. What is SIEM Integration?

SIEM, which stands for Security Information and Event Management, is a comprehensive approach to managing an organization's security information and events. SIEM integration refers to the process of incorporating SIEM solutions into an organization's existing IT infrastructure to enhance its ability to monitor, detect, and respond to security incidents. To support this approach, the HaloENGINE transmits logs in JavaScript Object Notation (JSON), Log Event Extended Format (LEEF), and Common Event Format (CEF).

1. Common Event Format is an open log management standard developed by HP ArcSight. CEF comprises a standard prefix and a variable extension that is formatted as key-value pairs.
2. Log Event Extended Format is a customized event format for IBM Security QRadar. LEEF comprises a LEEF header, event attributes, and an optional Syslog header.
3. JavaScript Object Notation is a lightweight text-based open standard designed for human-readable data interchange.

These logs are forwarded to the communications module, which transmits them to your collection server via UDP or TCP. Ideally, a SIEM (Microsoft Azure Sentinel, Splunk, RSA, and others) server would scan the received messages, sort them, and alert your security team.

Forwarding logs

4.5.2. Why CEF Standard?

The CEF format is an open log management standard that simplifies log management. CEF allows third parties to create their device schemas that are compatible with a standard that is used industry-wide for normalizing security events. Technology companies and customers can use the standardized CEF format to facilitate data collection and aggregation, for later analysis by an enterprise management system. CEF is an extensible, text-based format designed to support multiple device types by offering the most relevant information. It defines the syntax for log records consisting of a standard header and a variable extension, formatted as key-value pairs.

Syslog and CEF Header

The data is normalized and categorized into the ArcSight CEF for easy correlation and analysis. CEF uses Syslog as a transport mechanism. It uses the following format, consisting of a Syslog prefix, a header, and an extension, as shown below. If an event producer is unable to write Syslog messages, it is still possible to write the events to a file.

```
Prefix | Header |[Extension]
```

CEF format

```
10:29:48.486 host CEF:Version|Device Vendor|DeviceProduct|Device Version|Signature ID|Name|Severity|[Extension]
```

CEF format sample

Format	Description	Example
Prefix	Syslog applies a prefix to each message, no matter which device it arrives from, that contains the date and hostname.	`10:29:48.486`
Header	Version is an integer and identifies the version of the CEF format. The current CEF version is 0 (CEF:0).	`CEF:0`
	Device Vendor, Device Product, and Device Version are strings that uniquely identify the type of sending device.	`|Secude|HaloCAD|6.10.0.0|`
	• Device Event Class ID is a unique identifier per event-type. • This can be a string or an integer. Device Event Class ID identifies the type of event reported.	`100` (User download)
Extension	The Extension field contains a collection of key-value pairs. The keys are part of a predefined set. The standard allows for including additional keys as outlined in "ArcSight Extension Dictionary”. An event can contain any number of key-value pairs in any order, separated by spaces (""). If a field contains a space, such as a filename, this is valid and can be logged in exactly that manner.	Please refer to the following table.

Format	Description	Example
	Secude uses only Standard Key Names from ArcSight Extension Directory and no custom extensions. The reason for that is to avoid significant limitations custom extensions will cause.	

CEF Header details

```
14:19:44.920 CEF:0|Secude|HaloCAD|6.10.1.0|100|user
download|1|deviceCustomDate1Label=exportTime deviceCustomDate1=Apr 13 2026 08:49:44
UTC externalId=06474D9CA79844D4BC358CB17F65B6B0 deviceCustomDate2Label=logTime
deviceCustomDate2=Apr 13 2026 08:49:44 UTC act=unblocked fname=Test.txt filePath=New
Product fileType=txt fsize=3049 in=3049 shost=windchill122 duser=wcadmin,type:Product
Manager dst=10.41.13.22 requestClientApplication=[null] cs2Label=DataDestination cs2=[
platform\=[Windows NT], browser\=[Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/146.0.0.0 Safari/537.36],
browser_version\=[null], device_type\=[null], terminal_id\=[10.41.0.112],
destination_attributes\=[{ key\=[client_ip], value\=[10.41.13.22], type\=[null] }, {
key\=[client_host], value\=[10.41.13.22], type\=[null] }] ] cs3Label=DataOrigin cs3=[
source_type\=[PLM], system_name\=[windchill122], client_type\=[WINDCHILL],
plm_info\=[{ key\=[product_name], value\=[New Product], type\=[null] }, {
key\=[system_context], value\=[New Product], type\=[null] }, {
key\=[organization_name], value\=[SECUDE], type\=[null] }, {
key\=[lifecycle_template], value\=[Basic], type\=[null] }, { key\=[lifecycle_state],
value\=[In Work], type\=[null] }]] cs4Label=ClassifyProtectionData cs4=[
policy_id\=[d7e95033-e7f1-4218-8941-7d60d8e9cf69], policy_name\=[CADSecured],
policy_type\=[company_policy], error\=[false], author\=[HaloENGINE Service] ]
```

CEF sample

4.5.3. Why LEEF Standard?

The Log Event Extended Format (LEEF) is a customized event format for IBM Security QRadar that contains readable and easily processed events for QRadar.

Syslog and LEEF Header

The LEEF format consists of a Syslog header, a LEEF header, and event attributes. The Syslog header is an optional field. The Syslog header contains the timestamp and IPv4 address or hostname of the system that sends the event. The LEEF header is a required field for LEEF events. The LEEF header is a pipe delimited (|) set of values that identifies your software or appliance to QRadar. Event attributes identify the payload information of the event that is produced by your appliance or software. Every event attribute is a key-value pair with a tab that separates individual payload events.

```
Syslog Header | LEEF Header |[Event Attributes]
```

LEEF format

```
15:03:24.203 LEEF:2.0|Secude|HaloCAD|6.10.1.0|100|^|exportTime=Apr 15 2026 09:33:24
UTC^eventName=user download^externalId=9BE04917052F4E31B5D0556BD52CD104^logTime=Apr 15
2026 09:33:24 UTC^act=unblocked;protected_originally^fname=file1
(5).docx^filePath=New_Folder^ftype=docx^fsize=11879^fdwnsize=11879^shost=windchill122^
usrName=wcadmin,type:Product Manager^dst=10.41.0.253^usrAgent=[null]^dataDestination=[
platform=[Windows NT], browser=[Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/147.0.0.0 Safari/537.36 Edg/147.0.0.0],
browser_version=[null], device_type=[null], terminal_id=[10.41.0.122],
destination_attributes=[ {key=[client_ip], value=[10.41.0.253], type=[null]},
{key=[client_host], value=[10.41.0.253], type=[null]} ] ]^dataOrigin=[
source_type=[PLM], system_name=[windchill122], client_type=[WINDCHILL], plm_info=[
{key=[product_name], value=[New_Folder], type=[null]}, {key=[system_context],
value=[New_Folder], type=[null]}, {key=[organization_name], value=[SECUDE],
type=[null]}, {key=[lifecycle_template], value=[Basic], type=[null]},
{key=[lifecycle_state], value=[In Work], type=[null]} ] ]^classifyProtectionData=[
policy_id=[d7e95033-e7f1-4218-8941-7d60d8e9cf69], policy_name=[CADSecured],
policy_type=[company_policy], error=[false], author=[HaloENGINE Service] ]
```

LEEF sample

Format	Description	Example
Syslog Header	The Syslog header contains the timestamp.	`03:44:14.061`
LEEF Header	LEEF:version	An integer value that identifies the major and minor version of the LEEF format that is used for the event, for example,

Format	Description	Example
		`LEEF:2.0|Vendor|Product|Version|EventID|`
	Product name	A text string that identifies the product that sends the event log to QRadar, for example, `LEEF:2.0|Secude|HaloCAD|6.10.0.0|100|`
	Product version	A string that identifies the version of the software or appliance that sends the event log, for example, `LEEF:2.0|Secude|HaloCAD|6.10.0.0|100|`
	EventID	A unique identifier for an event.
	Delimiter Character	Pipe Specifies an alternative delimiter to the attributes. You can use a single character or the hex value for that character. The hex value can be represented by the prefix 0x or x, followed by a series of 1-4 characters (0-9A-Fa-f).
Event Attributes	Predefined Key Entries	A set of key-value pairs that provide detailed information about the security event. Each event attribute must be separated by a tab or the delimiter character, but the order of attributes is not enforced.

LEEF Header details

4.5.4. Why JSON Standard?

The JSON format is a lightweight text-based interchange format used for serializing and transmitting structured data over the network connection. Furthermore, it supports Security Information and Event Management solutions (e.g., Microsoft Azure Sentinel, Splunk, etc.,) seamlessly.

JSON syntax is considered as a subset of JavaScript syntax; it includes the following:

1. Data is represented in name/value pairs.
2. Curly braces hold objects and each name is followed by ':'(colon), the name/value pairs are separated by ','(comma).
3. Square brackets hold arrays and values are separated by ','(comma).

```
15:06:52.584
{"log_id":"1BAF4F01FB4046FD8CAE9D976ADB9470","product":"HaloCAD","source_host":{"shost
":"windchill122"},"protection":{"policy_id":"d7e95033-e7f1-4218-8941-
7d60d8e9cf69","extended_tags":[],"policy_name":"CADSecured","error":false},"destinatio
n_info":{"hostname":"10.41.0.122","destination_attributes":[{"value":"10.41.0.253","ke
y":"client_ip"},{"value":"10.41.0.253","key":"client_host"}],"destination_ip":"10.41.0
.253","os":"Windows NT","recipients":[],"browser":"Mozilla/5.0 (Windows NT 10.0;
Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/147.0.0.0 Safari/537.36
Edg/147.0.0.0","device_type":"null","browser_version":"null","user_agent":"null"},"cla
ssification":{"classification_by_system":[],"classification_by_user":[]},"version":"6.
10.1.0","log_time":"Apr 15 2026 09:36:52
UTC","event_id":100,"data_origin":{"generic_info":"null","sap_info":"null","system_nam
e":"windchill122","pre_process_info":[],"source_type":"PLM","client_type":"WINDCHILL",
"plm_info":[{"value":"New_Folder","key":"product_name"},{"value":"New_Folder","key":"s
ystem_context"},{"value":"SECUDE","key":"organization_name"},{"value":"Basic","key":"l
ifecycle_template"},{"value":"In
Work","key":"lifecycle_state"}],"bi_info":"null"},"user_info":{"user_email":"HaloENGIN
E Service","user_type":"Product
Manager","user_name":"wcadmin"},"file_info":{"file_path":"New_Folder","file_name":"Ex2
.txt","file_type":"txt","download_file_size":4526,"original_file_size":4526},"action":
["unblocked","protected_originally"],"export_time":"Apr 15 2026 09:36:51
UTC","event":"user download"}
```


JSON sample

4.6. Uninstalling the HaloCAD Component from Windows

Once you stop using the HaloCAD component, you can uninstall it. Uninstall removes all files and registry settings that were added to your computer at the time of initial installation.

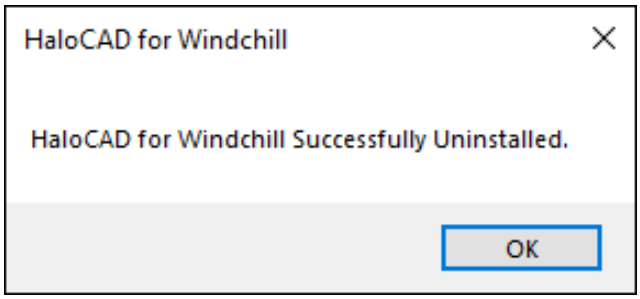
Prerequisite: Make sure to stop the Windchill Server before performing uninstallation. Otherwise, an error message will appear such as "*Windchill Server instance is running. So please stop the server and retry unistallation.*"

1. Click **Start** menu > go to **Control Panel** > **Programs** > **Programs and Features** > **Uninstall a Program** > select **HaloCAD for Windchill** application from the list > right-click and select **Uninstall** option or double-click on the installer `HaloCAD_Windchill_Setup.exe` file.

2. Depending on your Windows security settings, you may get a security warning as "*Do you want to allow the following program to make changes to this computer*?". If you get this security warning, click the **Yes** button to confirm that you want to uninstall the HaloCAD component.
3. The following confirmation message appears.

Uninstall Message #1

4. Click **Yes** to confirm that you want to remove it from the computer.



Uninstall Message #2

Results:

- The HaloCAD component has been successfully uninstalled.
- Click **OK** to close the dialog.
- The uninstalling process is complete.

5. **Alternate option:** Remove the configuration files with the Config tool, then run the following command.

```
HaloCAD_Windchill_Setup.exe -uninstall
```

Index

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.