Secude

HaloCAD

HaloCAD for Autodesk Vault

Installation Manual

Version 3.0

Copyright

© 2025-2026 Secude Solutions AG. All Rights Reserved.

This Secude-branded software and its corresponding documentation are the exclusive property of Secude Solutions AG of Luzern, Switzerland and are protected under the various copyright laws around the world and by various other intellectual property laws. The use of this software and/or its documentation and any copying thereof by end users is subject to the terms of a license agreement with Secude Solutions AG. The wrongful use or copying of this software and/or documentation subjects infringers to both criminal and civil liabilities.

ANY USE, COPYING, REPRODUCTION, ALTERATION, TRANSMISSION, OR TRANSLATION OF THESE MATERIALS, IN WHOLE OR IN PART, IN ANY FORM OR BY ANY MEANS, IS STRICTLY PROHIBITED WITHOUT THE PRIOR WRITTEN PERMISSION OF SECUDE SOLUTIONS AG. IF THIS MATERIAL IS PROVIDED WITH SOFTWARE LICENSED BY SECUDE, THE INFORMATION HEREIN IS PROVIDED SUBJECT TO THE TERMS OF THE WARRANTY PROVIDED WITH THE PRODUCT LICENSE. IF THIS MATERIAL IS NOT PROVIDED WITH LICENSED SOFTWARE, THE INFORMATION HEREIN IS PROVIDED “AS IS” WITHOUT WARRANTY OF ANY KIND. IN EITHER CASE, THERE ARE NO OTHER WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT, OR QUALITY. IN NO EVENT SHALL SECUDE SOLUTIONS AG OR ANY OF ITS AFFILIATES BE LIABLE FOR ANY DIRECT OR INDIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL, PUNITIVE, OR EXEMPLARY DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE MATERIALS AND/OR INFORMATION CONTAINED HEREIN. Some jurisdictions do not allow the exclusion of implied warranties, so the above exclusion may not apply to you.

Secude Solutions AG takes reasonable measures to ensure the quality of the data and other information produced herein. However, these materials may contain technical inaccuracies or typographical errors, and are not guaranteed to be error-free. Information may be changed or updated without notice. Secude Solutions AG has no obligation to update these materials based on changes to its products or services or those of third parties. Secude Solutions AG may also make improvements or changes to the products or services described in this information at any time without notice. Secude Solutions AG frequently releases new versions and updates to its software, and therefore images shown in this document may be slightly different from what you see on screen.

As with any security product, Secude Solutions AG highly recommends the back up of data as well as passwords on a regular basis. Secude Solutions AG is not responsible for the loss of passwords or data that cannot be retrieved based upon a user’s failure to adhere to stringent backup and safe-keeping conventions.

Contact

Secude Solutions AG

Murbacherstrasse 19

6003 Luzern, Switzerland

Mail: info@secude.com

Support

Web: https://support.secude.com

Mail: support@secude.com

Table of Contents

1. INTRODUCTION 1

2. HOW HALOCAD FOR PLM PROTECTS DATA 2

2.1. About this Manual 3

2.2. Reference Manuals 4

2.3. Component Functions 5

3. INSTALLING THE HALOCAD FOR AUTODESK VAULT 7

3.1. System Requirements 7

3.2. Prerequisites 8

3.2.1. Conditions for Running the HaloENGINE GenNXT Tomcat Service 9

3.3. Installation Modes 12

3.3.1. Graphical Mode 12

3.3.2. Silent Mode 18

4. CONFIGURING THE HALOCAD PROXY 20

4.1. Configuration Using Tool (GUI) 20

4.2. Configuration Using the Command Line 25

5. CONFIGURING THE TOMCAT SERVICE 28

5.1. WinHTTP Proxy Settings 31

6. TESTING THE (REVERSE) PROXY CONFIGURATION 32

7. UPDATING THE HALOCAD CONFIGURATION 33

8. APPENDIX 34

8.1. Failover Mechanism for HaloENGINE GenNXT in HaloCAD for PLM 34

8.2. Third-Party Libraries 36

8.3. Autodesk Vault Metadata Definitions 38

8.4. Uninstalling the HaloCAD for Autodesk Vault 39

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 in industries such as automotive, aviation, and high-tech create and manage intellectual property (IP) through engineering drawings. These drawings are created digitally using computer-aided design (CAD) applications and are often shared with external users for business collaboration. It is important to understand the risks associated with sharing sensitive business information. Protecting sensitive engineering data requires comprehensive security measures. HaloCAD is a data protection solution that helps organizations protect sensitive engineering data.

2. How HaloCAD for PLM Protects Data

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

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

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

2.1. About this Manual

This manual describes the installation and configuration procedures specific to HaloCAD for Autodesk Vault.

Reference

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

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

2.2. Reference Manuals

The following table describes the HaloCAD documentation set and the information available in each manual.

For information on	Refer to
Step 1: Verify the supported operating systems, file types, and CAD applications.	`HaloCAD_AutodeskVault_ReleaseNotes_EN_Online.pdf`
Step 2: Review the prerequisites before installation, including: • Registering an Application in Microsoft Entra ID - Web • HaloCAD Architecture • Office 365 Subscription Details • Recommended URLs, Addresses, and Ports for MPIP • Enable Support for TLS 1.2 at the Client Workstation for Microsoft Entra ID	`HaloCAD_Technical_Reference_Manual_EN_Online.pdf`
Step 3: Install the HaloCAD Add-on for AutoCAD/Inventor.	1. `HaloCAD_AutoCAD_Manual_Installation_EN_Online.pdf` 2. `HaloCAD_Inventor_Manual_Installation_EN_Online.pdf`
Step 4: Install and configure HaloENGINE GenNXT.	`HaloENGINEGenNXT_Manual_Installation_EN_Online.pdf`
Step 5: Install and configure HaloCAD for Autodesk Vault.	Refer to the current manual.
Step 6: Understand the protection and decryption workflow.	`HaloCAD_AutodeskVault_Manual_Operations_EN_Online.pdf`

HaloCAD reference documentation

2.3. Component Functions

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

1. HaloCAD Add-on for AutoCAD or HaloCAD Add-on for Inventor
2. HaloCAD for Autodesk Vault
3. HaloENGINE GenNXT
4. Microsoft Purview Information Protection

The following sections describe the functions of each component.

HaloCAD Add-on for AutoCAD and HaloCAD Add-on for Inventor

- **HaloCAD Add-on for AutoCAD** - Operates within Autodesk AutoCAD.
- **HaloCAD Add-on for Inventor** - Operates within Autodesk Inventor.
- Receives protected files from Autodesk Vault and displays their associated labels while enforcing permissions.
- Logs all add-on related activities for auditing purposes.

HaloCAD for Autodesk Vault

- It can be hosted on the Autodesk Vault PLM Server or on a Windows server with the possibility to access the Autodesk Vault server.
- It is a proxy component that listens for check-in and check-out actions initiated via the PLM Vault server.
- Connects to Microsoft Purview Information Protection to download sensitivity labels.
- Collects metadata for the user-selected file.
- Obtains action and label information for the selected file from HaloENGINE GenNXT.
- Encrypts the file and forwards the file stream to the CAD client during check-out operations.
- Decrypts the file and stores the unprotected file in the PLM Vault during check-in operations.
- Logs HaloCAD for Autodesk Vault activities to the local log and sends monitoring logs to HaloENGINE GenNXT.

HaloENGINE GenNXT

- Is a Java-based server component that exposes a web service to HaloCAD for Autodesk Vault.
- Connects to Microsoft Purview Information Protection to download sensitivity labels and make them available for configuration.
- Implements business logic.
- Logs events received from HaloCAD for Autodesk Vault.

Microsoft Purview Information Protection

HaloCAD integrates with Microsoft Purview Information Protection to protect sensitive documents. Microsoft Purview Information Protection is an enterprise document security solution that ensures only authorized users can open protected content while controlling the actions they can perform, such as printing, editing, or saving. Even if sensitive data is accidentally or maliciously disclosed, unauthorized users cannot view the content in clear text.

Microsoft Documentation

This manual assumes that Microsoft Purview Information Protection is already configured and that you are familiar with the Microsoft Entra admin center and related concepts. If you are new to Microsoft Purview Information Protection, refer to the Microsoft documentation for setup and configuration instructions.

3. Installing the HaloCAD for Autodesk Vault

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

3.1. System Requirements

The following table lists the system requirements for installing and running HaloCAD for Autodesk Vault.

Components	Details
Supported Windows Server	Windows Server 2022 and above with updates installed.
Supported file types	1. AutoCAD file types 2. Inventor file types 3. PDF 4. MS Office native file types
Other requirements	Install HaloENGINE GenNXT and HaloCAD for Autodesk Vault separately on Windows servers.

Requirements

3.2. Prerequisites

Before installing HaloCAD for Autodesk Vault, ensure that the following prerequisites are met.

1. Ensure that you have administrative access before performing most system and dataset tasks.
2. Ensure that the client computer running the HaloCAD Add-on for Autodesk and Inventor can connect to the Autodesk Vault Server.
3. Ensure that your HaloENGINE GenNXT meets the requirements listed below:
   a. License file (enabled with AUTODESK_VAULT client type).
   b. Proper action rules
4. Ensure that you have a user account with document-consuming permissions on the Vault Server.
   a. You can add an existing user account to a specific Autodesk Vault.
   b. Or create a new user account and add it to the specific Autodesk Vault by logging in **Autodesk Vault** > **Tools** > **Administration** > **Global Settings** > **Security** > **Users** > in the **User Management** window, click **New User** (enter required details), and click the **Vaults** button to select all the Vaults listed.
5. Ensure that your Microsoft Entra ID application information is available. Refer to the Technical Reference Manual for more information.
6. Ensure that the certificate required for MPIP authentication is installed in the **Local Computer** certificate store, along with the Root CA and Intermediate CA certificates.
   a. If the certificate is CA-signed, install all related certificates in their respective stores (Root, Intermediate, and Personal).
   b. If the certificate is self-signed, install it in both the Trusted Root Certification Authorities and Personal stores of the Local Computer.
7. Ensure that an authentication approach is selected for HaloENGINE GenNXT and HaloCAD for Autodesk Vault PLM: **Self-Signed Certificate** or **CA-Signed Certificate**.
   a. For a **Self-Signed Certificate**, export the public key of the HaloENGINE GenNXT server's self-signed certificate and install it in **Trusted Root Certification Authorities** on the system where HaloCAD for Autodesk Vault is installed.
   b. For a **CA-signed certificate**, install the **Root CA certificate** in **Trusted Root Certification Authorities** on the system where HaloCAD for Autodesk Vault is installed. If an intermediate CA is used, ensure that the **intermediate CA certificate** is also available on the client system to validate the certificate chain.

8. If you want to implement a failover mechanism in HaloENGINE GenNXT, please refer to the section "Failover Mechanism for HaloENGINE GenNXT in HaloCAD for PLM".
9. Ensure that HaloCAD for Autodesk Vault and HaloENGINE GenNXT are installed using the same Azure tenant details. A mismatch in tenant details causes configuration errors.
10. To improve performance, configure MPIP labels to allow offline access. In the Microsoft Entra admin center, navigate to **Information Protection** > **Sensitivity labels** > select a label > **Items** > **Access control** > **Allow offline access**, and select **Always**. Note: Allowing offline access can affect revocation. Consider this impact when configuring the offline access setting. For more information, see the Microsoft documentation, Restrict access to content by using sensitivity labels to apply encryption.

3.2.1. Conditions for Running the HaloENGINE GenNXT Tomcat Service

Before running the HaloENGINE GenNXT Tomcat Service, ensure that the following prerequisites are met.

3.2.1.1. Deny log on as a service policy

If the service runs under a specific user account or 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 is restricted by this policy, the following error message appears when starting the HaloENGINE GenNXT Tomcat Service: "*Error 1069: The service did not start due to a logon failure.*"

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

During installation, HaloENGINE GenNXT retrieves the required Microsoft Entra ID application details and certificate thumbprint. When the HaloENGINE GenNXT Tomcat Service starts, it connects to the MPIP services by using the details provided 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 during installation must match the thumbprint of the certificate installed in the **Local Computer** certificate store.

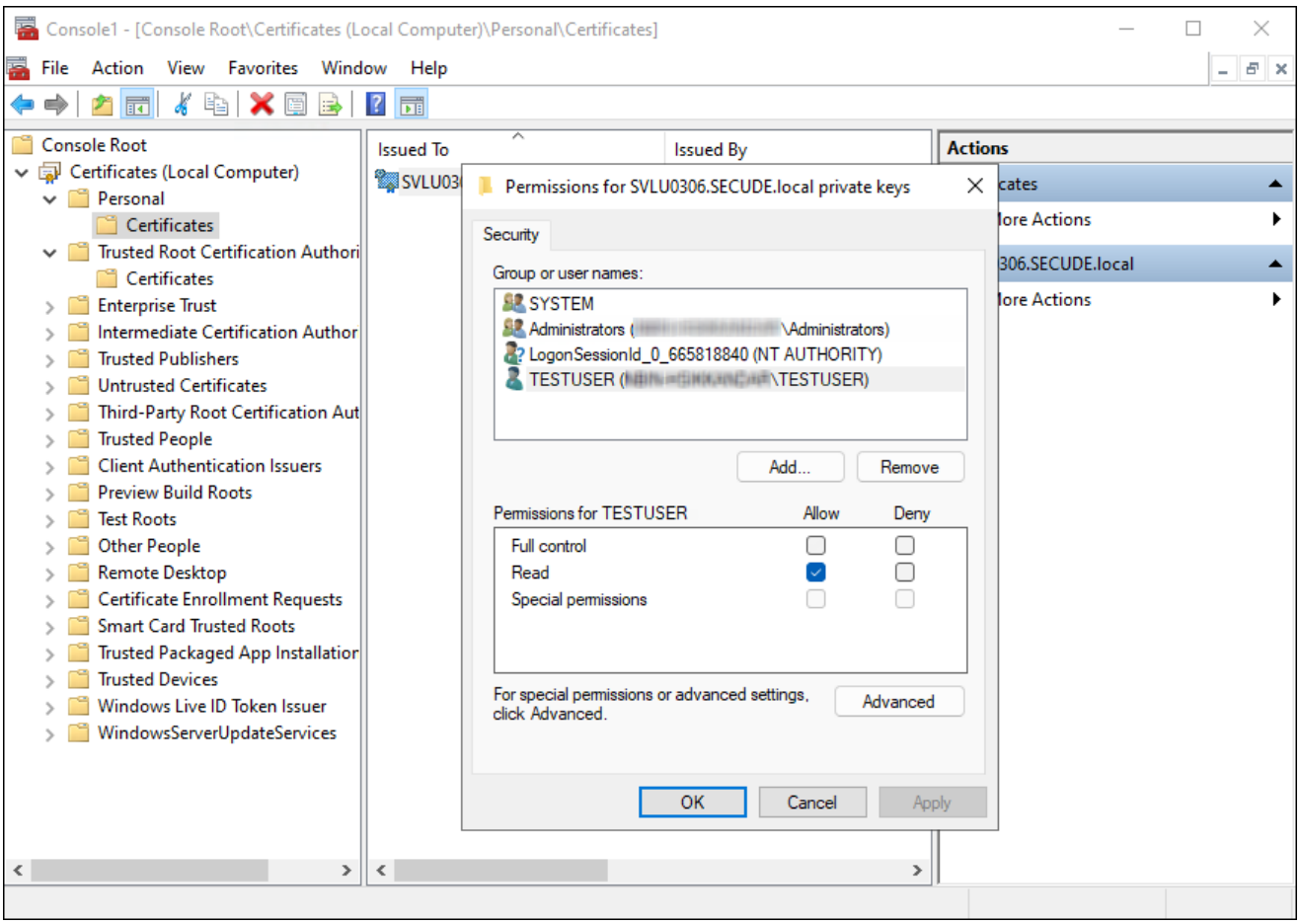
If the service runs under a non-administrative user account, the user might not have sufficient permissions to access the certificate's private key when the certificate is installed in the **Local Computer** certificate store. This restriction prevents successful authentication with MPIP services. To resolve this issue, grant the user **Read** permission to access the certificate's private key by following the procedure below. Any errors encountered during this process are recorded in the log file. If the verification succeeds, the service continues with initialization.

Prerequisites

- The required certificates (certificate used by MPIP service, root CA, and intermediate CA) are installed.
- The private key is stored in the Windows Certificate Store under **Local Computer**.
- You have administrator privileges to perform the configuration.

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. Select **Computer account**, click **Next**, select **Finish**, and then click **OK**.
6. In the left navigation pane, 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-administrator 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

Result

The specified non-administrative user can access the certificate's private key, allowing the HaloENGINE GenNXT Tomcat Service to authenticate successfully with MPIP services.

3.3. Installation Modes

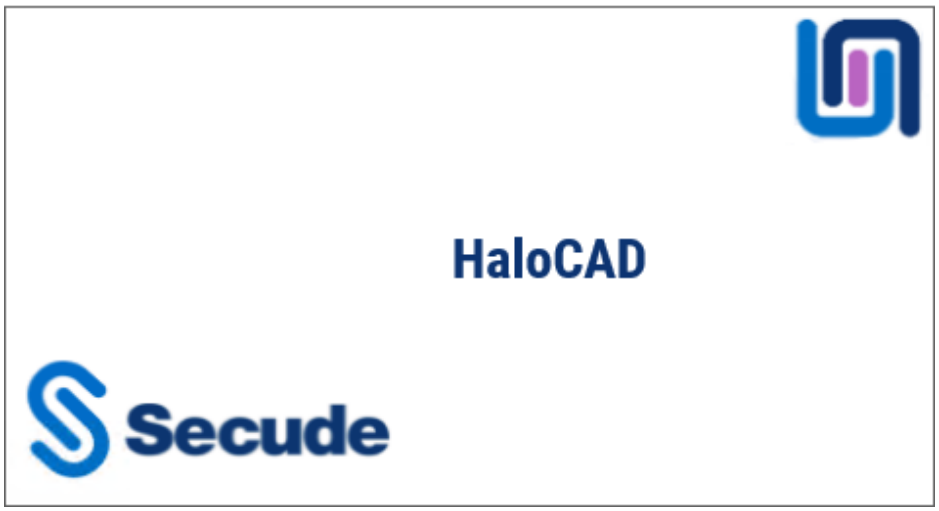
HaloCAD for Autodesk Vault supports the following installation modes:

1. **Graphical Mode**
   Graphical mode is an interactive installation method that uses a wizard-based graphical user interface.
2. **Silent Mode**
   Silent mode is a non-interactive installation method that installs HaloCAD for Autodesk Vault by using command-line options.

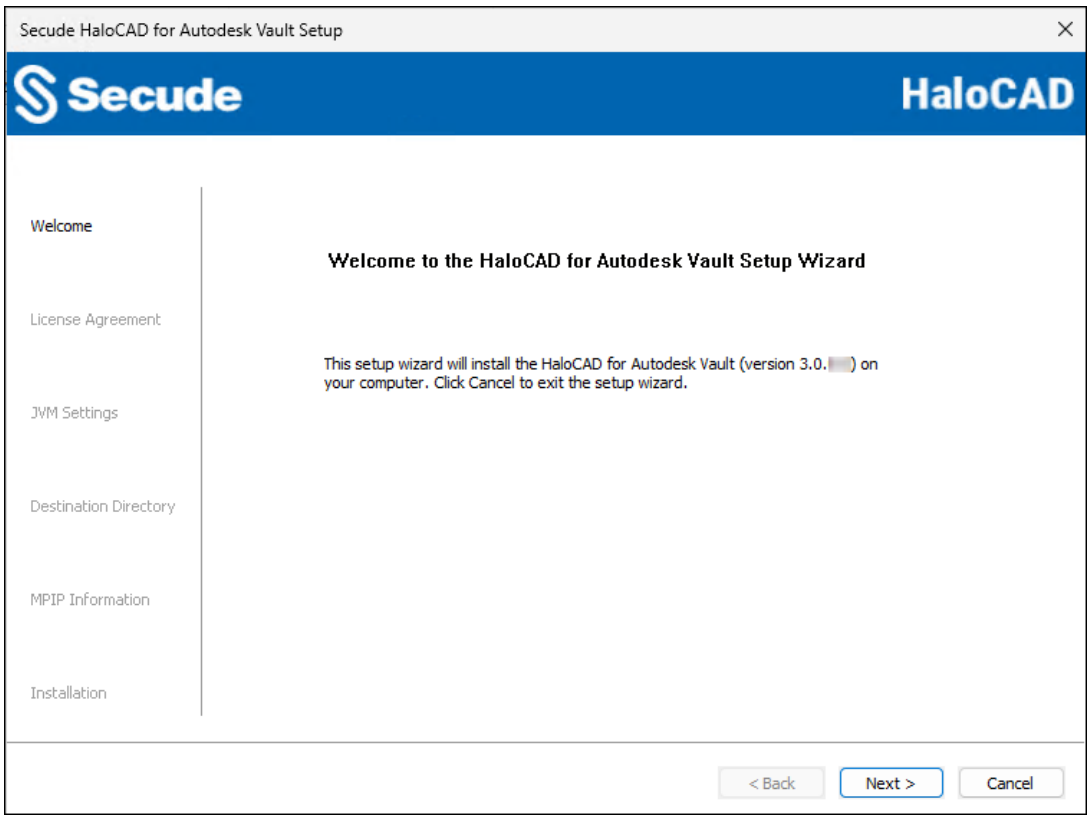
3.3.1. Graphical Mode

Install the HaloCAD component using the GUI-based setup program that is provided in the installation package.

1. To begin the interactive installation, double-click the `HaloCAD_Autodesk_Vault_Setup.exe` installer. Depending on your Windows security settings, a security warning similar to *"Do you want to allow the following program to make changes to this computer?"* may appear. If prompted, click **Yes** to continue the installation.
2. When the installer starts, the **Startup** dialog appears, then the **Welcome** dialog.

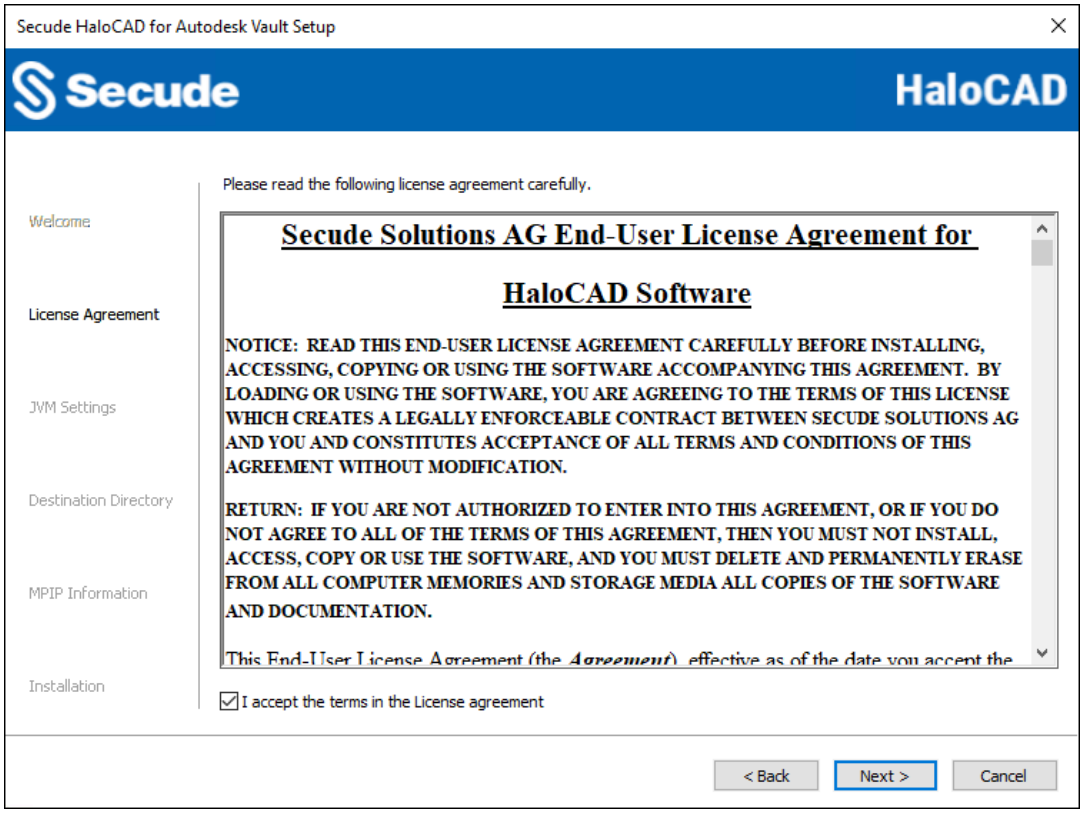


Startup dialog



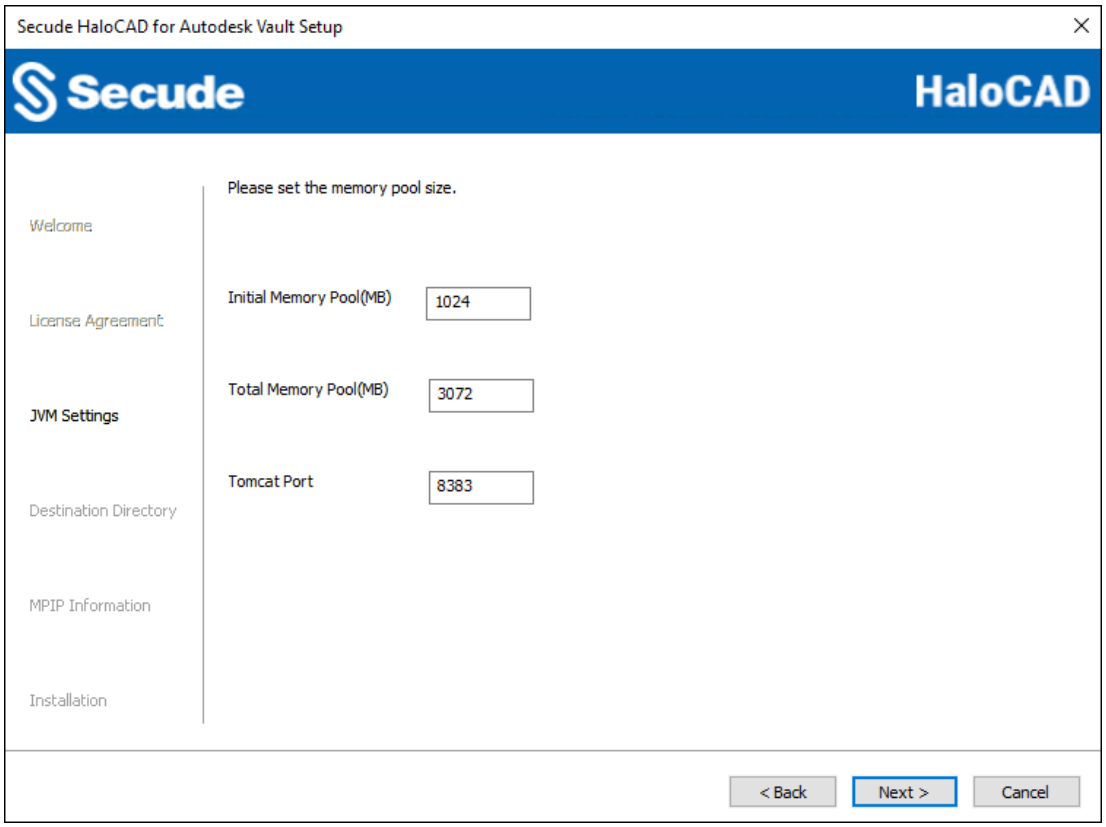
Welcome dialog

3. Click **Next** to continue.
4. The **License Agreement** dialog appears.



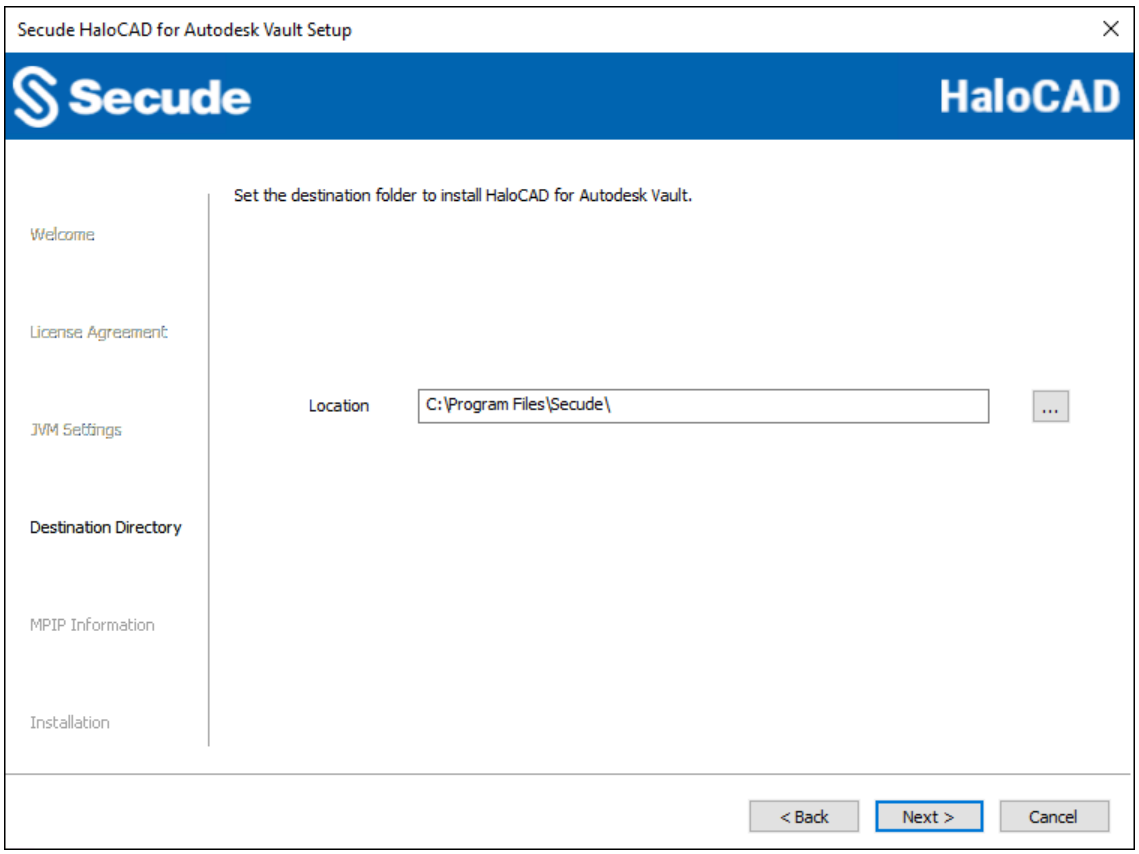
End-User License Agreement Dialog

5. Read the **End-User License Agreement**. If you agree to the terms, select **I accept the terms in the License Agreement**, and then click **Next**.
6. The **JVM Settings** dialog appears.



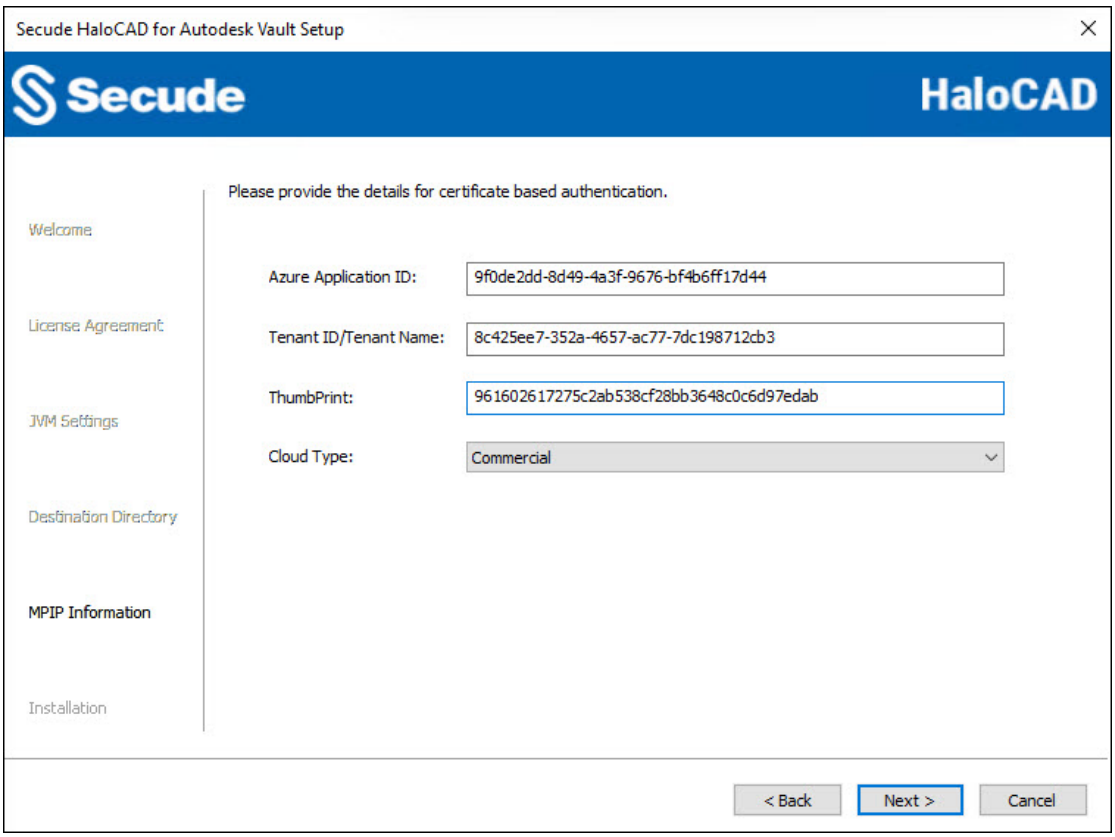
Tomcat pool size configuration dialog

7. Enter the amount of memory you want to allocate to change the **Initial Memory Pool and Total Memory Pool** preset values. Note: Ensure that the Total Memory Pool does not exceed the System's available 3/4th RAM. The default **Tomcat port** is 8383. You can, however, change the port number; it must be greater than 999 and less than or equal to 65535.
8. Click **Next**.
9. The **Destination Directory** dialog appears.



Destination directory dialog

10. By default, the application files are installed in the following directory: `C:\Program Files\Secude\`. To install HaloCAD for Autodesk Vault in a different location, click **Browse** and select the required directory.
11. Click **Next.**
12. The **MPIP Information** dialog appears. To avoid errors, 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 Application ID of the registered application in the Microsoft Entra admin center. 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`).

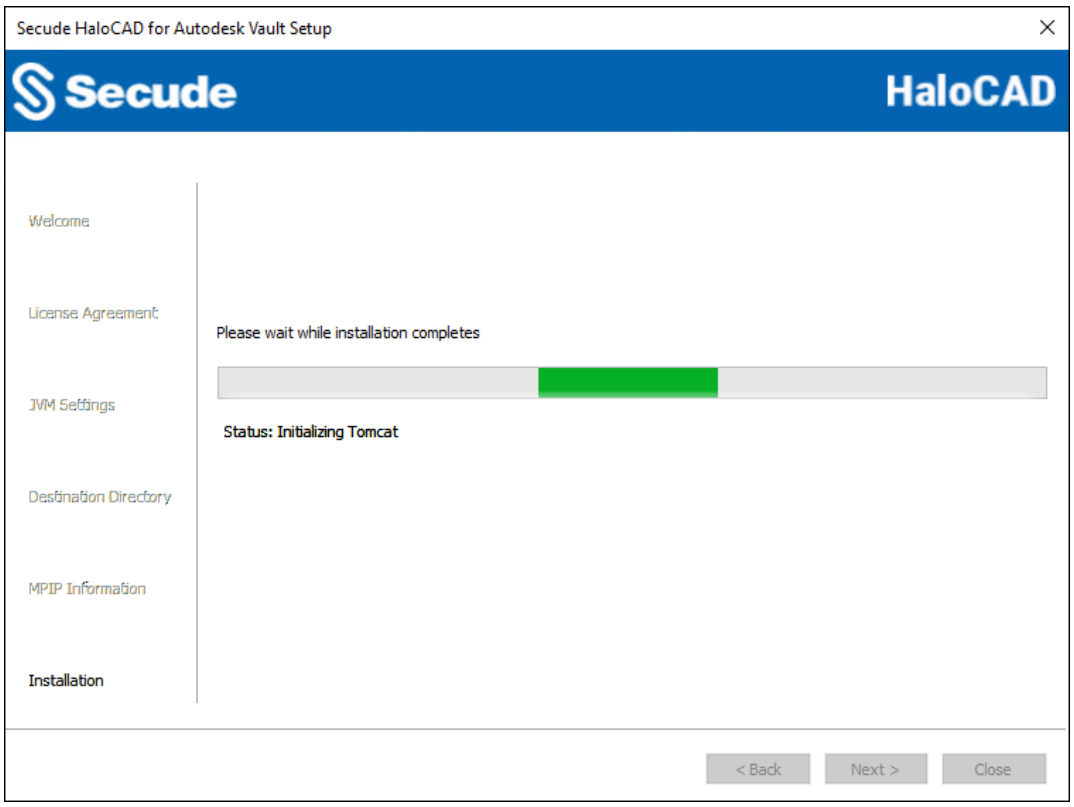
c. **Thumbprint**: Enter the thumbprint of the MPIP authentication certificate installed in the **Local Computer** certificate store. For example, `9d2fdcae3f6ea56f773df54d877ca09b34fca202`.

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. To return to a previous step in the installation, click **Back** (optional).

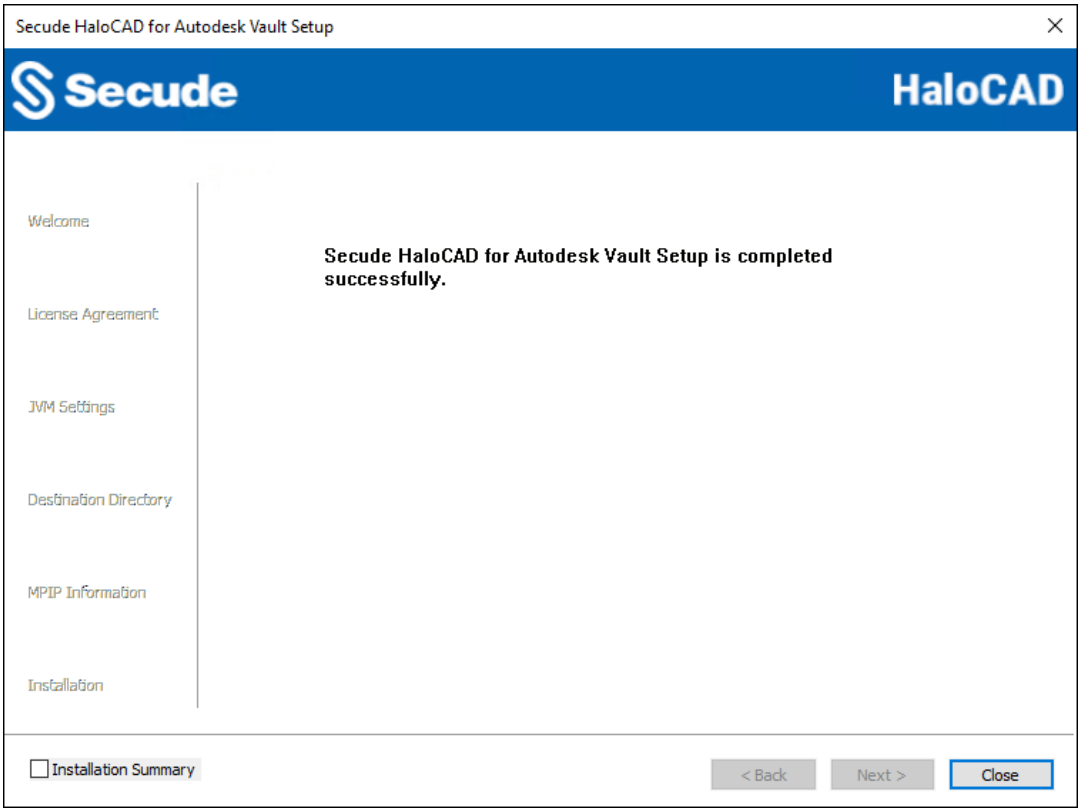
f. Click **Next**.

13. The installation begins, and the progress is displayed in the **Installation** dialog.



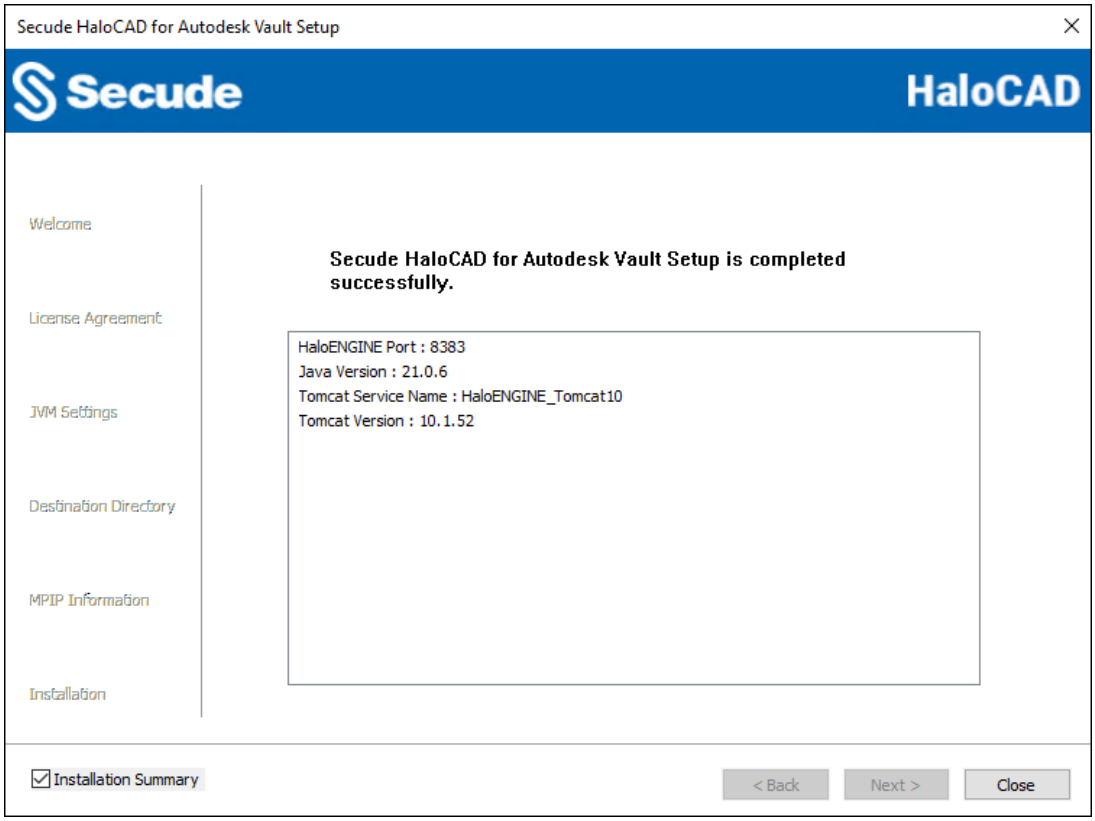
Installation dialog

14. When the installation is complete, a confirmation message appears indicating that the HaloCAD for Autodesk Vault component has been successfully installed.



Installation completed dialog

15. On the setup wizard, you can see the **Installation Summary** option. To view the summary, select the **Installation Summary** check box. The installation details will be summarized in the right-side pane.



Summary dialog

16. Click **Close** to exit the installation wizard.

3.3.2. Silent Mode

In addition to Graphical Mode, you can install the HaloCAD for Autodesk Vault component in **Silent Mode**. Silent Mode does not require user interaction or display a user interface. It enables you to install by using command-line options.

1. Open the Command Prompt with elevated rights (Run as Administrator).
2. Navigate to the directory that contains the HaloCAD for Autodesk Vault installer.
3. To view the available **Silent Mode** options, run the following command:

   Type `HaloCAD_Autodesk_Vault_Setup.exe -help`

   Press `Enter`

   Output

   ...

   ```
   HaloCAD_Autodesk_Vault_Setup.exe -install -initmempool <Initial memory pool size in MB(s).
   Minimum size is 128 MB> -totalmempool <Total memory pool size in MB(s).
   ```

```
Maximum size is 3/4 of total RAM size.> -dir <destination_directory> -port
<range_1_to_65535> -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_Autodesk_Vault_Setup.exe -uninstall
```

4. The following command shows how to install and initialize HaloCAD.

```
HaloCAD_Autodesk_Vault_Setup.exe -install -initmempool 1024 -totalmempool 2048 -dir
"C:\Program Files\Secude" -applicationid 9f0de2dd-8d49-4a3f-9676-bf4b6ff17d44 -
tenantid 8c425ee7-352a-4657-ac77-7dc198712cb3 -thumbprint
961602617275c2ab538cf28bb3648c0c6d97edab -cloudtype "Commercial"
```

5. Press `Enter`.

Result

The installation is complete.

Certificate update

If you update or renew the client certificate, restart the HaloENGINE GenNXT Tomcat service for the changes to take effect.

4. Configuring the HaloCAD Proxy

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

4.1. Configuration Using Tool (GUI)

Prerequisites: Ensure that HaloCAD for Autodesk Vault is installed before proceeding.

Follow these steps to configure the settings through the GUI:

Step 1. Run the HaloCAD Configuration Tool.

1. Navigate to the installation directory. By default, the directory is: `C:\Program Files\Secude\HalocadVault\config`.
2. Do one of the following:
   - Double-click the JAR file `HaloCAD-for-Autodesk-Vault-config-<version>.jar`
   - Open **Command Prompt** as an administrator, type the following command, and then press **Enter**.

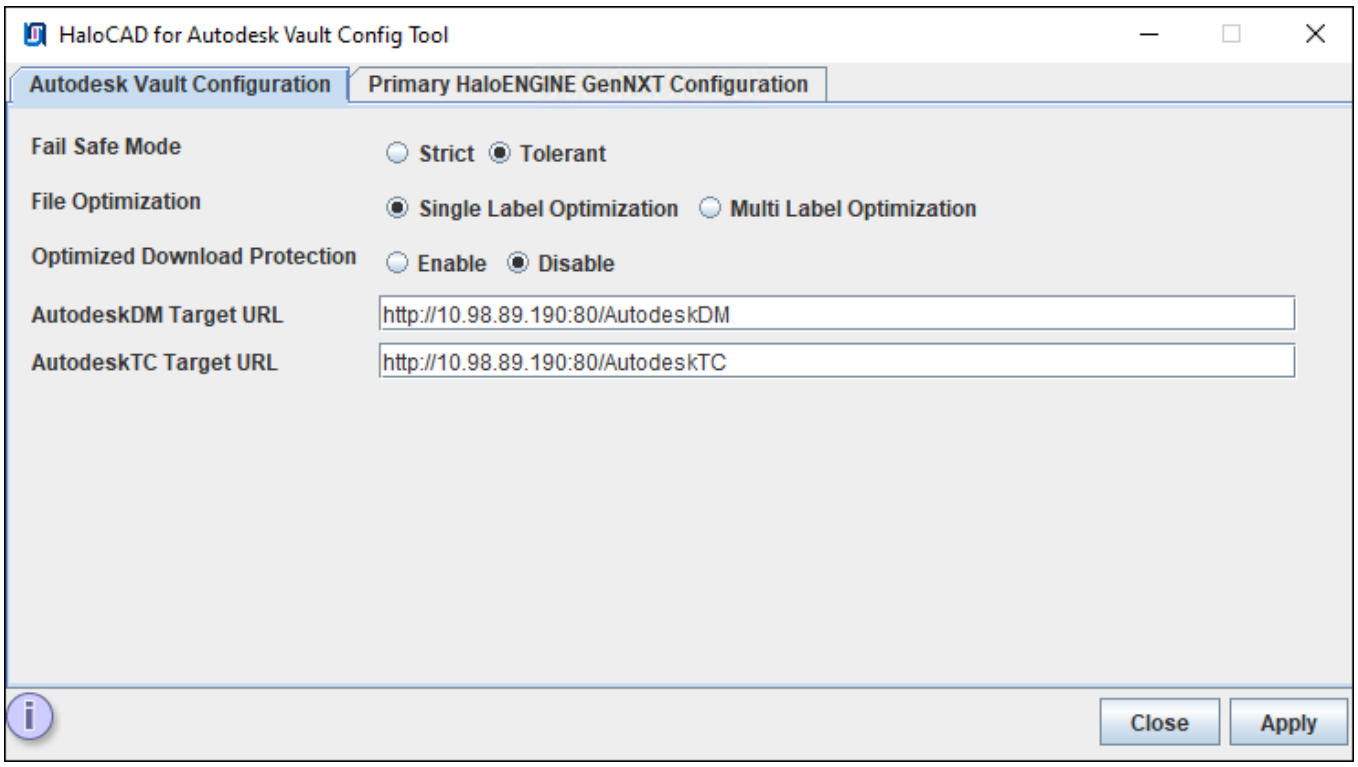
     Syntax: `<pathtojar>java -jar HaloCAD-for-Autodesk-Vault-config-<version>.jar`

     For example: `C:\Program Files\Secude\HalocadVault\config>java -jar HaloCAD-for-Autodesk-Vault-config-<version>.jar`

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

Step 2. Enter the **Autodesk Vault Configuration** Settings.

Select the **Autodesk Vault Configuration** tab, and then enter the following information.



Autodesk Vault configuration tab

1. **Fail-Safe Mode**: The **Fail Safe Mode** controls the system behavior when inconsistencies prevent the specified protection from being applied (for example, conflicting configurations, unreachable server components, or returned error messages). Select one of the following options:
   a. **Strict:** Blocks file uploads and downloads whenever an error occurs.
   b. **Tolerant (default):** Allows file uploads and downloads even when an error occurs.
2. **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.
3. **Optimized Download Protection:** When this option is enabled (disabled by default), during the download of assembly files (for example, a parent ASM with dependent files), the smallest single file is protected and delivered to the user's download location. The remaining files are then automatically protected at the user's download location by the HaloCAD for PLM Client.
4. **AutodeskDM Target URL**: Enter the AutodeskDM Target URL on which your Autodesk Vault is hosted. For example, `http://10.98.89.190:80/AutodeskDM`.

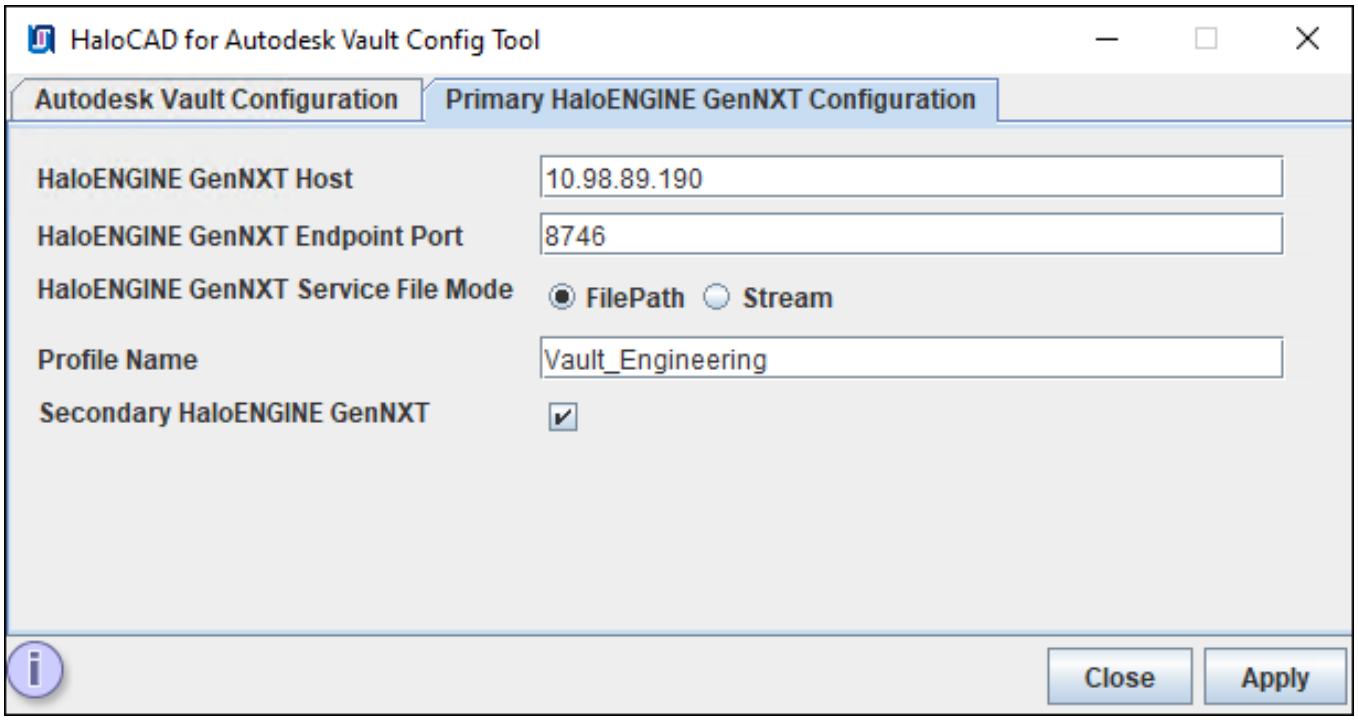
5. **AutodeskTC Target URL**: Enter the AutodeskTC Target URL on which your Autodesk Vault Thin Client is installed. For example,`http://10.98.89.190:80/AutodeskTC`.
6. Click **Apply**. If required values are missing, a red tooltip message appears. Enter the missing information and click **Apply** to continue.

Result:

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

Step 3. HaloENGINE GenNXT Configuration

Select the **Primary HaloENGINE GenNXT Configuration** tab, and then enter the following information.



Primary HaloENGINE GenNXT configuration tab

1. **HaloENGINE GenNXT Host**: Enter the IP address or fully qualified domain name (FQDN) of the HaloENGINE GenNXT server. Example, `10.98.89.190`
2. **HaloENGINE GenNXT Endpoint Port**: Enter the endpoint port used to access HaloENGINE GenNXT. For example, `8746`
3. **HaloENGINE GenNXT Service File Mode**: Select the file transmission method.
   a. **FilePath (default):** Stores the file in a local temporary location for the encryption and decryption process. The file path is used for file transfer.
   b. **Stream:** Transfers the file as a sequence of bytes.

4. **Profile Name**: Enter the profile name configured in the Admin Portal. For example, `Vault_Engineering`.
5. **Secondary HaloENGINE GenNXT**: To configure a failover mechanism, select the **Secondary HaloENGINE GenNXT** check box. HaloCAD supports connection failover between two HaloENGINE GenNXT instances. For more information, please refer to the section "Failover Mechanism for HaloENGINE GenNXT in HaloCAD for PLM".
6. Click **Apply**. If required values are missing, a red tooltip message appears. Enter the missing information and click **Apply** to continue.

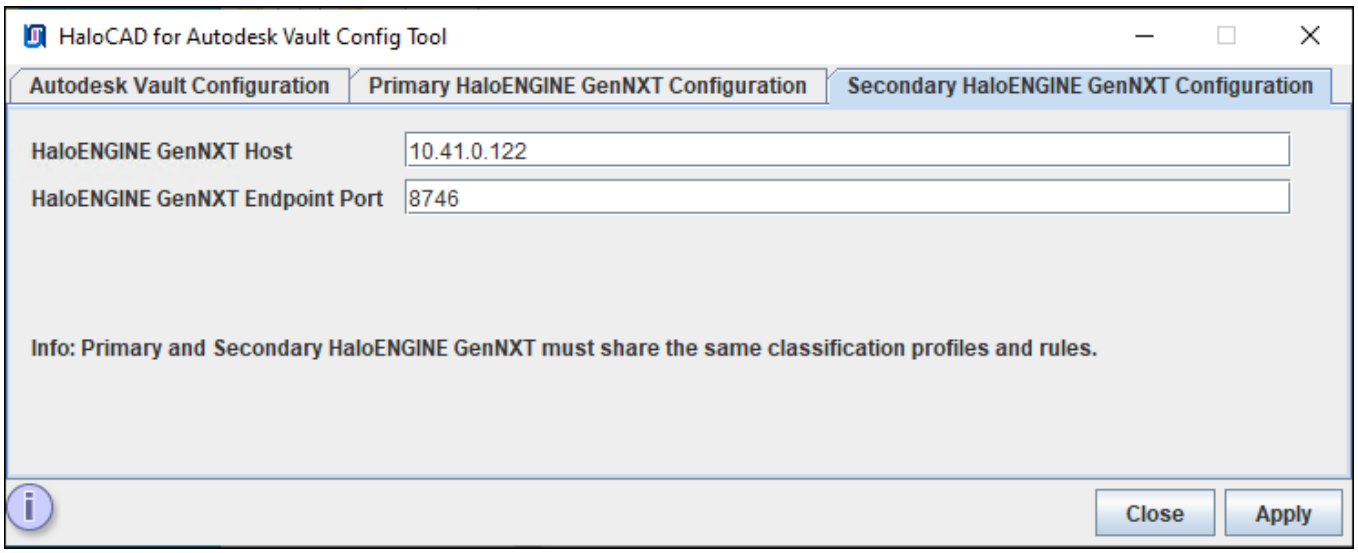
Result:

- A confirmation message dialog box appears.
- Click **OK** to close the dialog box.
- If you have selected the **Secondary HaloENGINE GenNXT** option, you can notice that the **Secondary HaloENGINE GenNXT Configuration** tab has been added to the configuration tool, as shown in Step 4 below.

Step 4. Select the **Secondary HaloENGINE GenNXT Configuration** tab, and then enter the following information.

Skip this step if you are not configuring a secondary HaloENGINE GenNXT. This step is required only if you want to use the failover mechanism.

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



Secondary HaloENGINE GenNXT configuration tab

1. **HaloENGINE GenNXT Host**: Enter the IP address or fully qualified domain name (FQDN) of the HaloENGINE GenNXT server. For example, `10.41.0.122`.
2. **HaloENGINE GenNXT Endpoint Port**: Enter the endpoint port used to access HaloENGINE GenNXT. For example, `8746`
3. Click **Apply**. If required values are missing, a red tooltip message appears. Enter the missing information and click **Apply** to continue.

Result:

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

Step 5. Restart the Tomcat Service.

Restart the HaloENGINE GenNXT Tomcat Service after making any configuration changes.

4.2. Configuration Using the Command Line

This section describes an alternative method for configuring HaloCAD for Autodesk Vault and HaloENGINE GenNXT parameters by using the command line.

Prerequisite: Ensure that HaloCAD for Autodesk Vault is installed.

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

1. Open a command prompt and navigate to the destination folder, type `java -jar HaloCAD-for-Autodesk-Vault-config-<version>.jar -shell`, and press **Enter**.

```
C:\Program Files\Secude\HalocadVault\config>Java -jar HaloCAD-for-Autodesk-Vault-
 config-<version>.jar -shell
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
HaloCAD for Autodesk Vault
Config Path: C:\Program Files\Secude\HalocadVault\config
1. Autodesk Vault Configuration
2. Primary HaloENGINE GenNXT Configuration
0. Exit
Note: If an invalid value is entered, the default value will be applied.
Please choose an option:1
--------------------------------------------------------------------------------
Autodesk Vault Configuration
--------------------------------------------------------------------------------
Fail Safe Mode: (Default:Tolerant) :
1. Tolerant
2. Strict
Please choose an option: 1

File Optimization: (Default:Single Label Optimization)
1. Multi Label Optimization
2. Single Label Optimization
Please choose an option: 1

Optimized Download Protection: (Default:Disable)
1. Enable
2. Disable
Please choose an option: 2

Enter the AutodeskDM Target URL :http://10.98.89.190:80/AutodeskDM

Enter the AutodeskTC Target URL :http://10.98.89.190:80/AutodeskTC
Saved Successfully.
--------------------------------------------------------------------------------
```

```
Autodesk Vault Configuration
Fail Safe Mode          :Tolerant
File Optimization       :Multi Label Optimization
Optimized Download Protection       :Disable
AutodeskDM Target URL   :http://10.98.89.190:80/AutodeskDM
AutodeskTC Target URL   :http://10.98.89.190:80/AutodeskTC

1. Modify all configuration
2. Modify the particular configuration
3. Back to main menu
0. Exit
Please choose an option: 3
--------------------------------------------------------------------------------
1. Autodesk Vault Configuration
2. Primary HaloENGINE GenNXT Configuration
0. Exit
Note: If an invalid value is entered, the default value will be applied.
Please choose an option:2
--------------------------------------------------------------------------------
Primary HaloENGINE GenNXT Configuration
HaloENGINE GenNXT Host IP           :
HaloENGINE GenNXT Endpoint Port     :
HaloENGINE GenNXT Service Mode      :Local
HaloENGINE GenNXT Service File Mode:File Path
Profile Name                  :
Secondary HaloENGINE GenNXT         :Disable Secondary HaloENGINE GenNXT

1. Modify all configuration
2. Modify the particular configuration
3. Back to main menu
0. Exit
Please choose an option: 1
--------------------------------------------------------------------------------
Primary HaloENGINE GenNXT Configuration

Enter the Primary HaloENGINE GenNXT Host:10.98.89.198

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

Enter the Profile Name:Vault_Engineering

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

```
Please choose an option: 1
Saved Successfully.
--------------------------------------------------------------------------------
Primary HaloENGINE GenNXT Configuration
HaloENGINE GenNXT Host IP          :10.98.89.198
HaloENGINE GenNXT Endpoint Port    :8746
HaloENGINE GenNXT Service Mode     :Local
HaloENGINE GenNXT Service File Mode:File Path
Profile Name                        :Vault_Engineering
Secondary HaloENGINE GenNXT        :Disable Secondary HaloENGINE GenNXT

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

2. Click **Close** to close the command prompt.

5. Configuring the Tomcat Service

During installation, the Microsoft Entra ID application details initialize the **HaloENGINE GenNXT Tomcat service**. After successful authentication, the sensitivity labels are retrieved automatically.

Default locations of log files

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

Default locations

Use `heslibconfig.exe` to update MPIP-related settings, such as the Application ID, Tenant ID, thumbprint, and cloud type.

To update your Microsoft Entra ID application details, follow the procedure below.

1. Open the Command Prompt with elevated rights (Run as Administrator).
2. Navigate to the directory where `heslibconfig.exe` is located.
3. 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>
   heslibconfig.exe -testprotection <label_id>
   ```
4. To display the labels, enter the following command:

   ```
   heslibconfig.exe -testmip
   ```

   MPIP initializes, and the labels are fetched.
5. To update the JSON file, enter the following command:

   ```
   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 to `...\config\HaloENGINESVC.json`.

6. To verify that protection is successful, enter the following command:

```
heslibconfig.exe -testprotection ttf1473d-74f4-47ca-9843-e735f94fa797
```

MPIP initializes, and the sample file `testfile.txt` is protected with the label ID.

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 GenNXT 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.
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.

Name	Description
	• 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.
enabledke	Double Key Encryption • 0 (default value)—Disables the DKE functionality in the HaloENGINE GenNXT Tomcat Service. • 1 (On)—Enables the DKE functionality in the HaloENGINE GenNXT Tomcat Service. Please be aware that DKE labels are only visible when DKE functionality is enabled.
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.

Name	Description
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 GenNXT Tomcat Service creates a template file in the tmp\GUID folder (which can be located in the HaloENGINE GenNXT 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 GenNXT Tomcat service configuration

5.1. 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 GenNXT Tomcat Service ensures that the configured proxy settings are applied.

6. Testing the (Reverse) Proxy Configuration

To verify the proxy configuration, follow the instructions below:

1. Open **Autodesk Vault Professional Client** or any **Vault** plugin-loaded application**.**
2. Login to Autodesk Vault, server pointing to the proxy port (tomcat port).

Next Steps

HaloCAD has been set up in your environment and is ready to protect file downloads. Please refer to the Operations Manual for more details. If you are not yet familiar with labels, you might need to consult the Microsoft online reference at this point.

7. Updating the HaloCAD Configuration

You can update the configuration at any time by using the HaloCAD Configuration Tool (GUI). Using the same tool, you can change the current settings whenever you wish. Follow Step 1, update the settings, and then restart the Tomcat Service.

8. Appendix

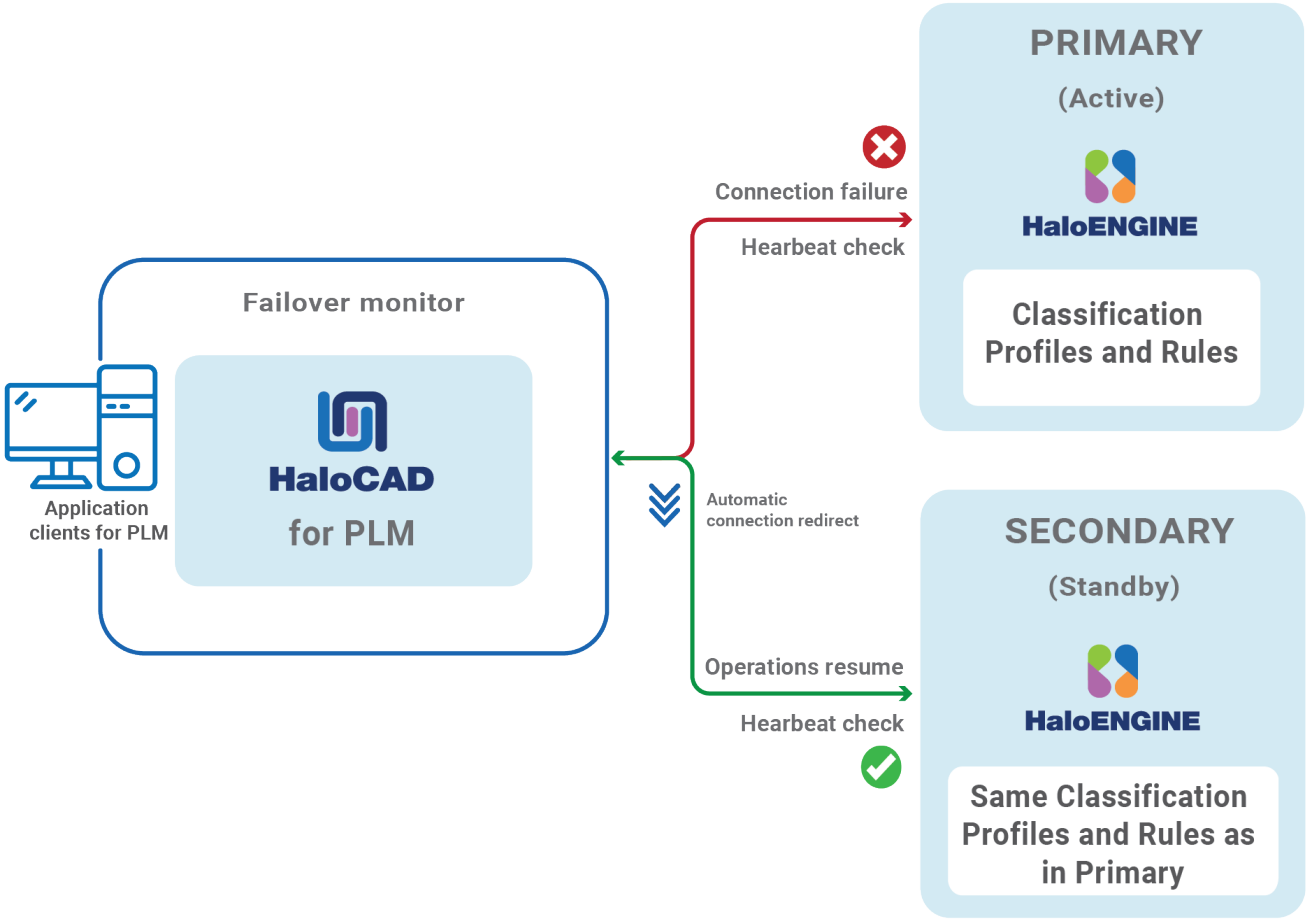
This section provides supplemental information.

8.1. Failover Mechanism for HaloENGINE GenNXT in HaloCAD for PLM

Server failover between two systems supports uninterrupted operation and service reliability in the event of a failure. The server failover configuration is **active-standby**, where the primary server is **active,** and the secondary server is **standby**.

HaloCAD for PLM supports connection failover between two HaloENGINE GenNXT instances. The failover mechanism provides the following benefits:

1. **High Availability**: If the primary HaloENGINE GenNXT fails, the secondary HaloENGINE GenNXT takes over, reducing downtime and maintaining continuous operation.
   Example: Assume that your business process requires no downtime.
   As part of the business security policy, the administrator configures **Fail-Safe Mode** as **Strict** to block file uploads or downloads whenever an error occurs. If HaloENGINE GenNXT encounters an unexpected issue and fails to obtain label information, file uploads or downloads are prevented. In such cases, the HaloENGINE GenNXT failover mechanism handles the situation without affecting the end user. If the primary HaloENGINE GenNXT connection fails, HaloCAD detects the failure and immediately switches to the secondary HaloENGINE GenNXT to continue providing services.
   Once the primary HaloENGINE GenNXT is restored, it remains in standby while the secondary HaloENGINE GenNXT remains active. If the secondary HaloENGINE GenNXT fails, the primary HaloENGINE GenNXT takes over operations again.



Failover Mechanism for HaloENGINE GenNXT in HaloCAD for PLM

2. **Redundancy**: Provides redundancy by ensuring that another HaloENGINE GenNXT is always available to take over if the primary HaloENGINE GenNXT fails. This minimizes the possibility of a single point of failure.
3. **Data Integrity and Consistency**: In the event of a failure, the failover mechanism helps ensure that data remains consistent and that file upload and download activities are not lost. This is crucial for systems that rely on high data security.

Failover Mechanism Requirement

1. **Network Infrastructure:** Deploy the secondary HaloENGINE GenNXT on a separate network segment from the primary HaloENGINE GenNXT.
2. **Data Replication:** Ensure that both HaloENGINE GenNXT use the same classification profiles and rules.

8.2. 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 Autodesk Vault are shown in the table below.

Library names	Versions	Source Code URLs	License Links
HTTP-Proxy-Servlet		https://github.com/mitre/HTTP-Proxy-Servlet	https://github.com/mitre/HTTP-Proxy-Servlet/blob/master/LICENSE.txt
httpmime	4.5.+	https://mvnrepository.com/artifact/org.apache.httpcomponents/httpmime	http://www.apache.org/licenses/LICENSE-2.0.txt
mail	1.6.2	https://mvnrepository.com/artifact/javax.mail/mail	Common Development and Distribution License (CDDL) v1.0 https://glassfish.dev.java.net/public/CDDLv1.0.html
commons-io	2.+	https://mvnrepository.com/artifact/commons-io/commons-io	https://www.apache.org/licenses/LICENSE-2.0.txt
jakarta.servlet-api	5.0.0.0	https://mvnrepository.com/artifact/jakarta.servlet/jakarta.servlet-api/5.0.0	https://www.eclipse.org/legal/epl-2.0/
jna	5.8.0	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	5.8.0	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

Library names	Versions	Source Code URLs	License Links
activation	1.2.0	https://mvnrepository.com/artifact/javax.activation/activation	https://glassfish.dev.java.net/public/CDDLv1.0.html
jaxws-api	2.3.1	https://mvnrepository.com/artifact/javax.xml.ws/jaxws-api	https://github.com/javaee/jax-ws-spec/blob/master/LICENSE.md
jaxws-ri	4.0.1	https://mvnrepository.com/artifact/com.sun.xml.ws/jaxws-ri/4.0.1	https://oss.oracle.com/licenses/CDDL+GPL-1.1
rt	2.3.0	https://mvnrepository.com/artifact/com.sun.xml.ws/rt	https://oss.oracle.com/licenses/CDDL+GPL-1.1
stax2-api	4.0.0	https://mvnrepository.com/artifact/org.codehaus.woodstox/stax2-api	http://www.opensource.org/licenses/bsd-license.php
MIP SDK	1.18.124	https://learn.microsoft.com/en-us/information-protection/develop/version-release-history	https://docs.microsoft.com/en-us/information-protection/develop/
MSAL	4.82.1	https://github.com/AzureAD/microsoft-authentication-library-for-dotnet	https://github.com/AzureAD/microsoft-authentication-library-for-dotnet/blob/master/LICENSE
Spdlog	1.15.3	-	https://github.com/gabime/spdlog

Third-party libraries

8.3. Autodesk Vault Metadata Definitions

The table below lists the Autodesk Vault metadata available in the HaloENGINE GenNXT.

Autodesk Vault Metadata	Use
lifecycle_state	Derivation from the lifecycle of Autodesk Vault data. (For example, work-in-progress, review, and released)
file_type	Derivation from file type. File types of AutoCAD, Inventor, and MS Office native file types. (For example, `dwg`, `ipt`, and `iam`)
folder_name	Derivation from the folder name in the Autodesk Vault server. (For example, `$/DESIGNS/INVENTOR FILES/Jet Engine Model/Workspace/Design Accelerator`)
preexpression_custom_pre-expression	Derivation from custom pre-expression. 1. Yes 2. No

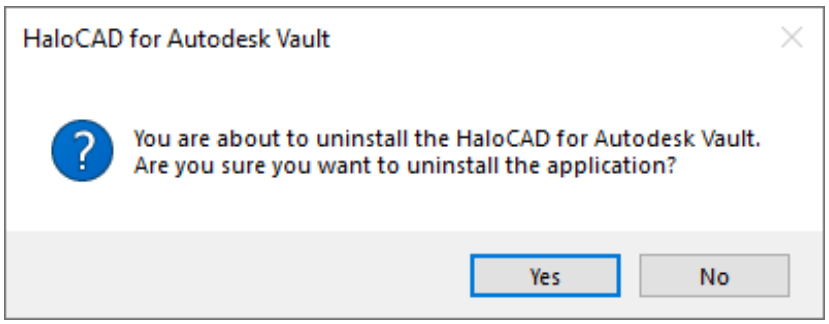
Autodesk Vault metadata

8.4. Uninstalling the HaloCAD for Autodesk Vault

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

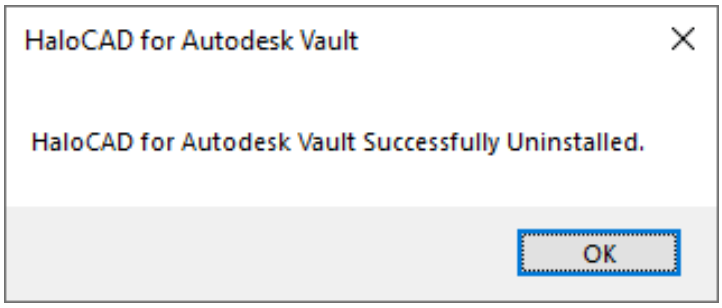
Method #1

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

Result

- The HaloCAD component is successfully uninstalled.
- Click **OK** to close the dialog.
- The uninstallation process is complete.
- **Alternative method:** Open **Command Prompt** as Administrator, then run this command:
  `HaloCAD_Autodesk_Vault_Setup.exe -uninstall`

Index

C

Cad 1

D

Dke 28

E

Endpoint 20

F

Fail-safe 20
File-optimization 20

H

Haloproxy 7

M

Mpip 1

P

Pii 28
Profile-name 20

R

Root-ca 7

S

Secondary_haloengine 20
Server 7

T

Thumbprint 7
Tls 7

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.