Secude

HaloCAD

HaloCAD for Autodesk Vault

Installation Manual

Version 2.7

Copyright

Contact

Secude Solutions AG

Landenbergstrasse 34

6005 Luzern

Switzerland

Tel: +41 41 510 70 70

Mail: info@secude.com

Support

Web: https://support.secude.com

Mail: support@secude.com

Table of Contents

Typographic Conventions

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

Convention	Description
Boldface type	• Items you must select, such as menu options, command buttons, or items in a list. • Titles of sections, sub-sections, etc.
Italic type	• To emphasize a word • Error messages • Table and Figure captions
`Consolas Font`	• Package names • Filenames and directory names • XML element names and attribute names • Parameters • File type • Code examples Example: `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 Autodesk Vault.

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_AutodeskVault_ReleaseNotes_EN_Online.pdf`
Step 2: Prerequisites 1. Before installing, it is recommended that you fulfill the prerequisites, such as registering an application in 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 AutoCAD/Inventor.	1. `HaloCAD_AutoCAD_Manual_Installation_EN_Online.pdf` 2. `HaloCAD_Inventor_Manual_Installation_EN_Online.pdf`
Step 4: Install and configure HaloENGINE.	`HaloENGINE_Manual_Installation_EN_Online.pdf`
Step 5: Install and configure HaloCAD for Autodesk Vault.	Refer to the current manual.
Step 6: Workflow illustrating protection and decryption	`HaloCAD_AutodeskVault_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 CAD
2. HaloCAD for Autodesk Vault
3. HaloENGINE
4. Azure RMS

The following list outlines the functions of each component.

HaloCAD Add-on for AutoCAD and Inventor performs the following functions:

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

HaloCAD for Autodesk Vault performs the following functions:

1. It can be hosted on the Autodesk Vault PLM Server or on a Windows server with the possibility to access the Autodesk Vault server.
2. It is a proxy component that listens for check-in and check-out actions initiated via the PLM Vault server.
3. Connects with Azure Rights Management Service (Azure RMS) to retrieve MPIP 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 Autodesk Vault component activities to the local log and sends monitor logs to the HaloENGINE.

Recommendations for improving performance

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 Autodesk Vault.
2. Connects with Azure RMS to download MPIP labels and make them available for configuration.
3. Implements business logic.
4. Logs events received from HaloCAD for Autodesk Vault.

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 Autodesk Vault

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

2.1. System Requirements

The following system requirements table specifies the minimum and recommended technical specifications, such as software and network resources, necessary to run the product.

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
Office 365 Subscription	1. Fully configured Microsoft Purview Information Protection. 2. An Azure subscription is required to use Azure RMS and the MPIP functionality. 3. A working Microsoft Entra ID service must be available. 4. Transport Layer Security (TLS) 1.2 or higher must be enabled to ensure the use of cryptographically secure protocols at all client workstations. 5. To avail the revoke access feature, the user should be assigned to the Microsoft Purview Information Protection Premium P1/P2 license. (Not required for reader add-on) 6. Audit logging: Your Azure subscription must include Log Analytics on the same tenant as Microsoft Entra ID. 7. Register an application to get the Application (client) ID and Tenant ID in the Azure portal.

Components	Details
	Select the option **Web** during application registration. Refer to the Technical Reference Manual for details on TLS 1.2 and application registration.
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. Make sure you have administrative access before performing most of the system and dataset tasks.
2. Make sure the client computer running the HaloCAD Add-on for AutoCAD/Inventor can connect to the Autodesk Vault Server.
3. Make sure your HaloENGINE complies with the requirements listed below:
   a. License file (enabled with AUTODESK_VAULT system type).
   b. Proper action rules
   c. Client certificate (`.JKS`)
4. Make sure to have a user account with document-consuming rights in 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 on the **Vaults** button to select all the Vaults listed.
5. If you want to implement a failover mechanism in HaloENGINE, please refer to the section "Failover Mechanism for HaloENGINE in HaloCAD for PLM".
6. Ensure that both HaloCAD for Autodesk Vault and HaloENGINE are installed using the same Azure tenant details. A mismatch in the tenant details will result in configuration errors.
7. 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 Azure tenant 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.

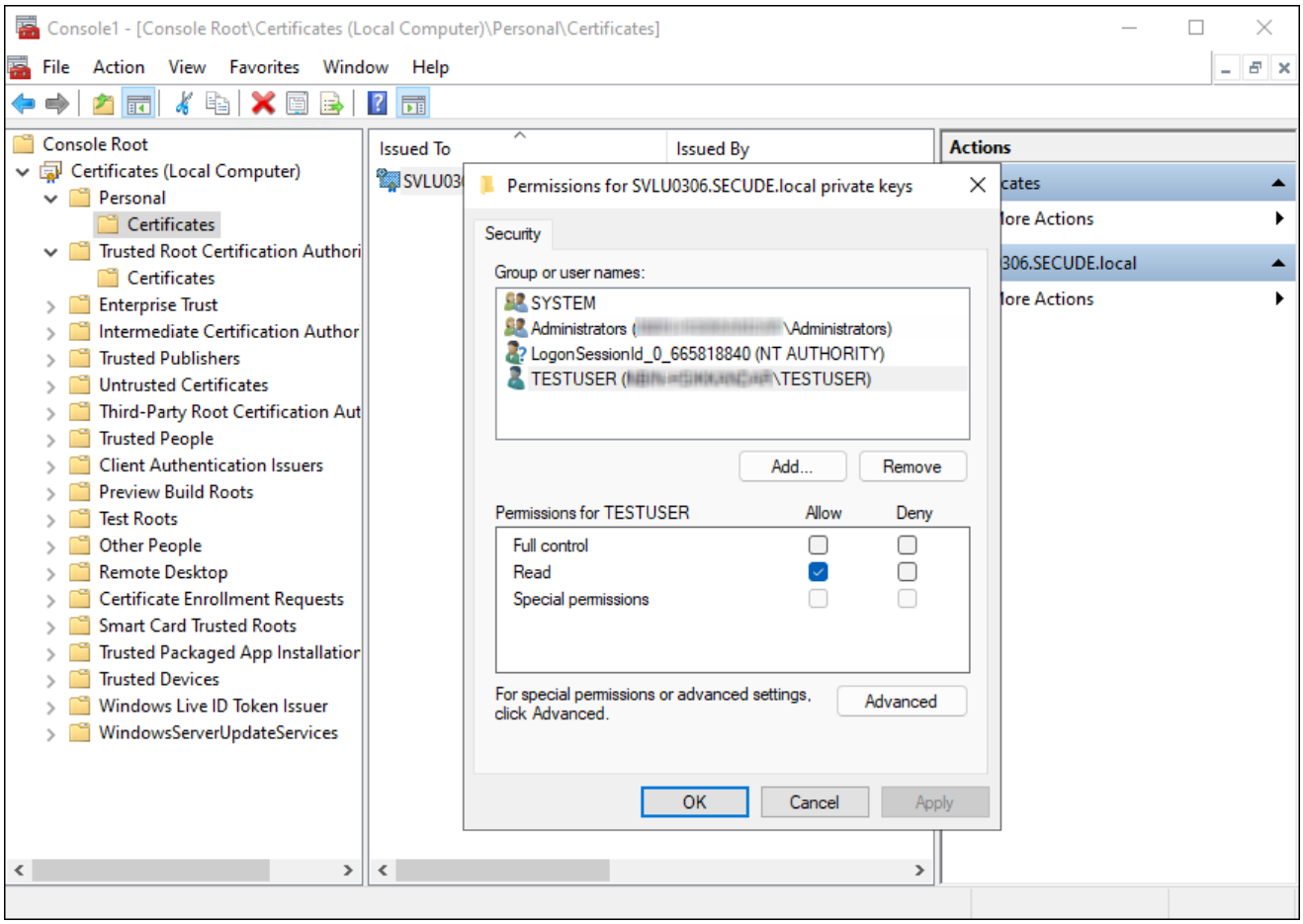
Prerequisites

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. Installation Modes

You can install the HaloCAD 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 component using command lines.

Prerequisites

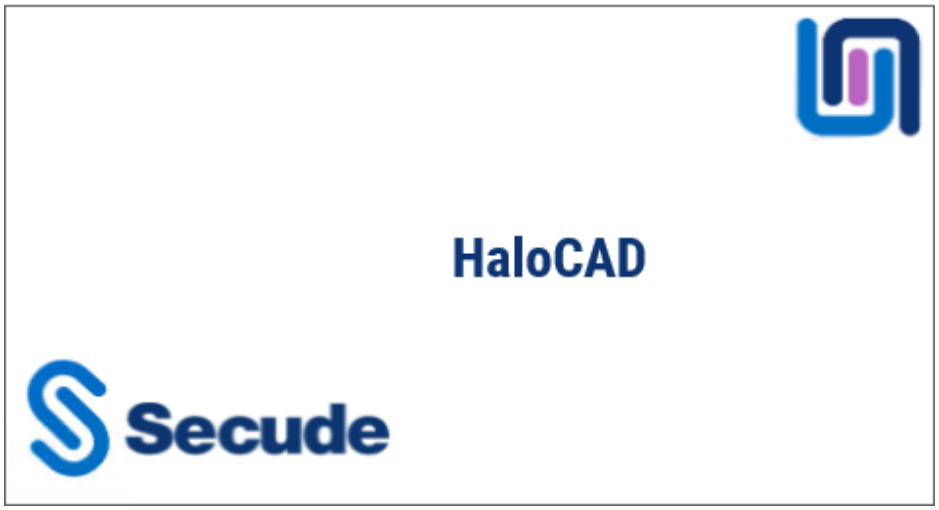
Before installing HaloCAD, ensure that the following requirements are met:

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.

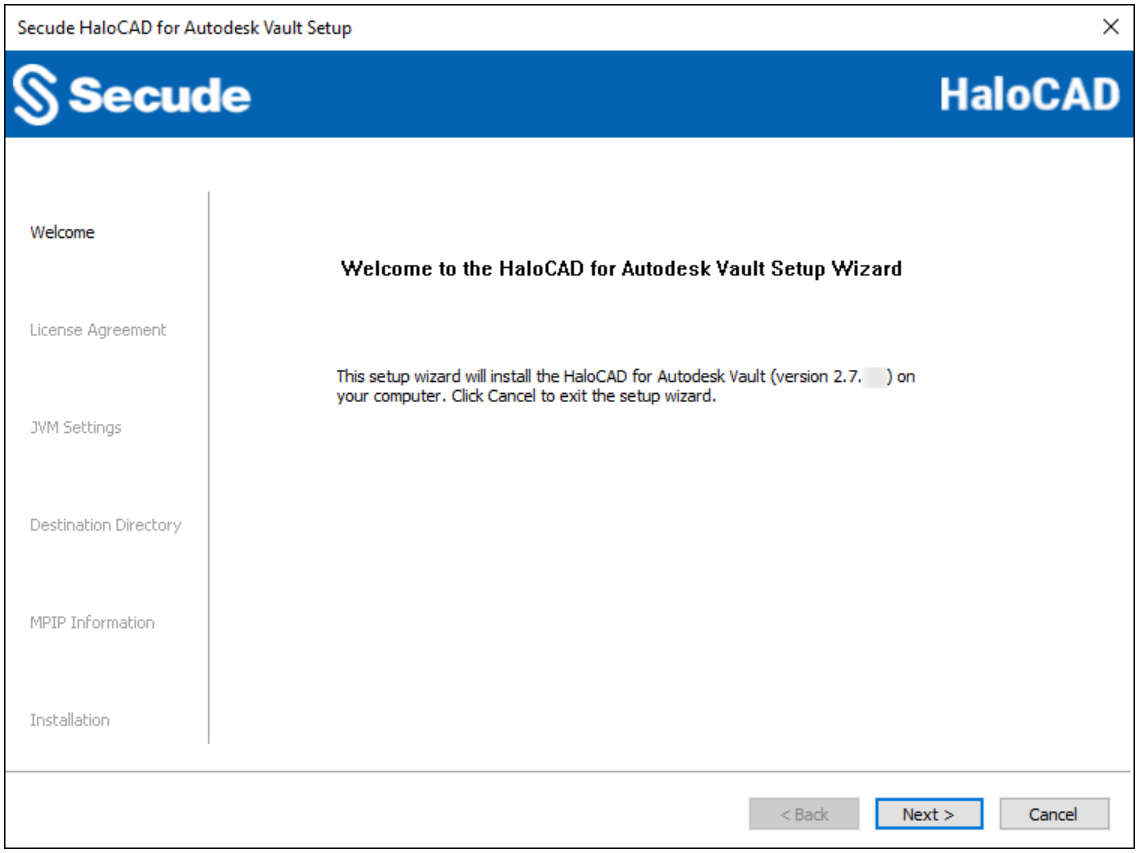
2.3.1. Graphical Mode

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 installer `HaloCAD_Autodesk_Vault_Setup.exe` file.
2. 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.
3. When the installer starts, the **Startup** dialog appears, followed by the **Welcome** dialog.

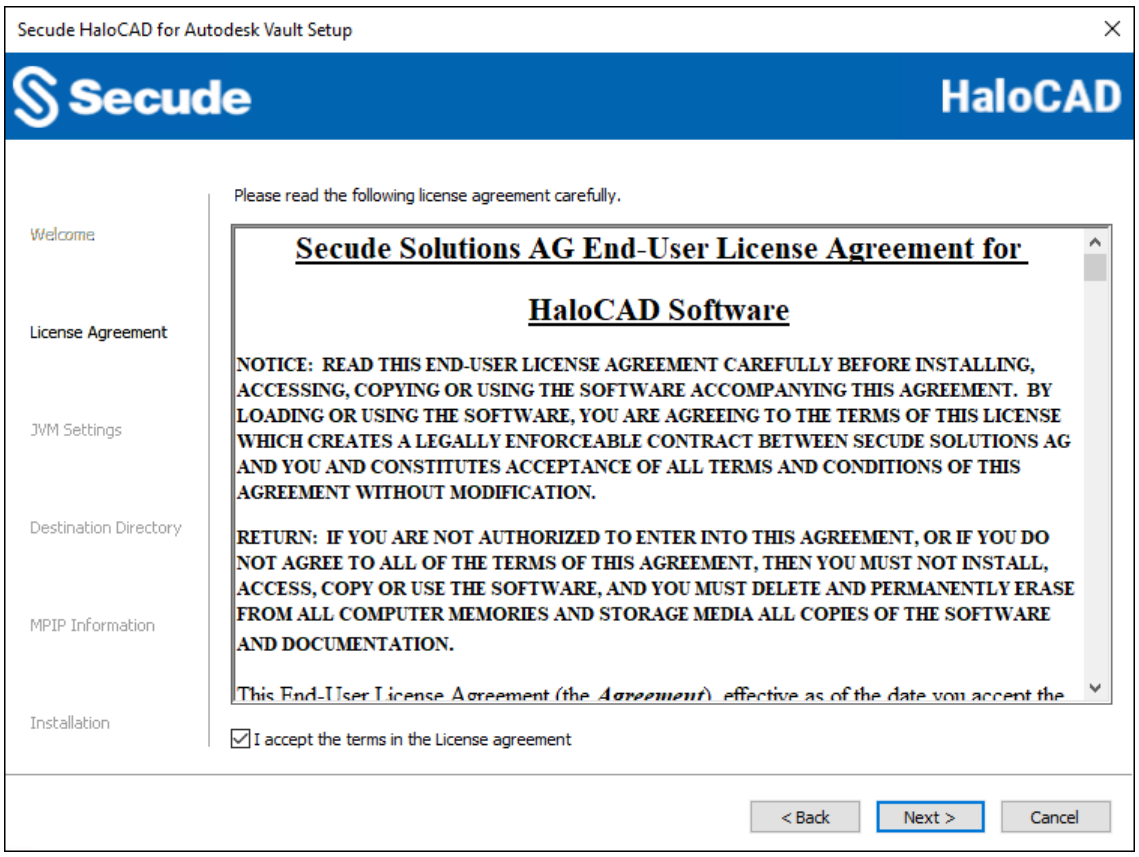


Startup Dialog



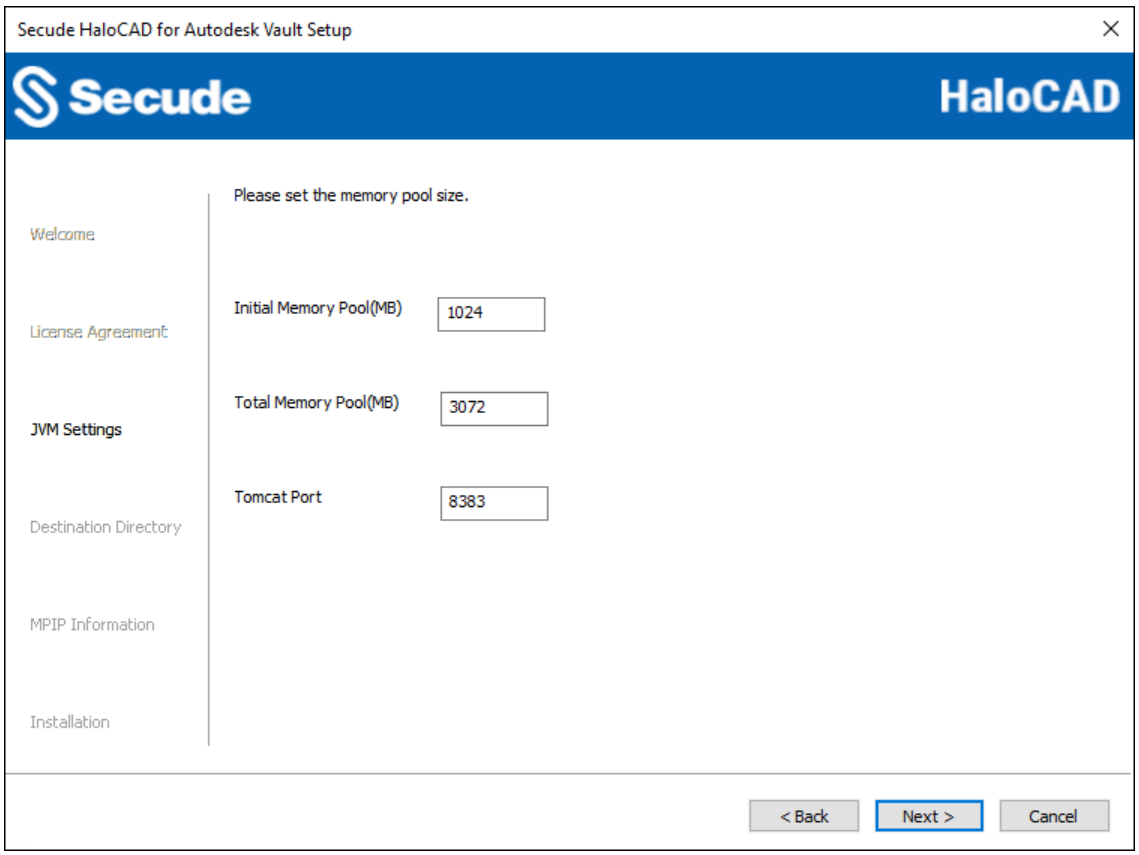
Welcome Dialog

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



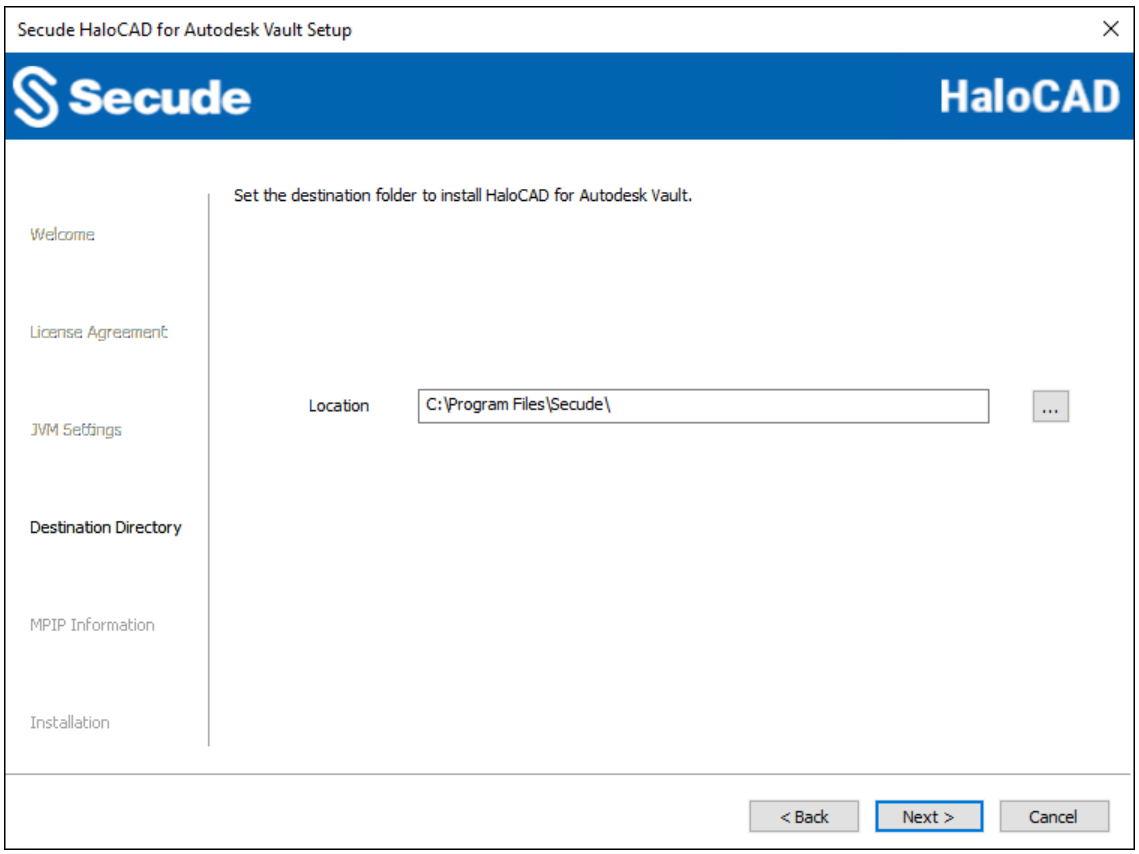
End-User License Agreement Dialog

6. Read the **End-User License Agreement**. If you agree, select **I accept the terms in the License Agreement**, and click **Next** to continue.
7. The Tomcat memory pool size configuration dialog appears.



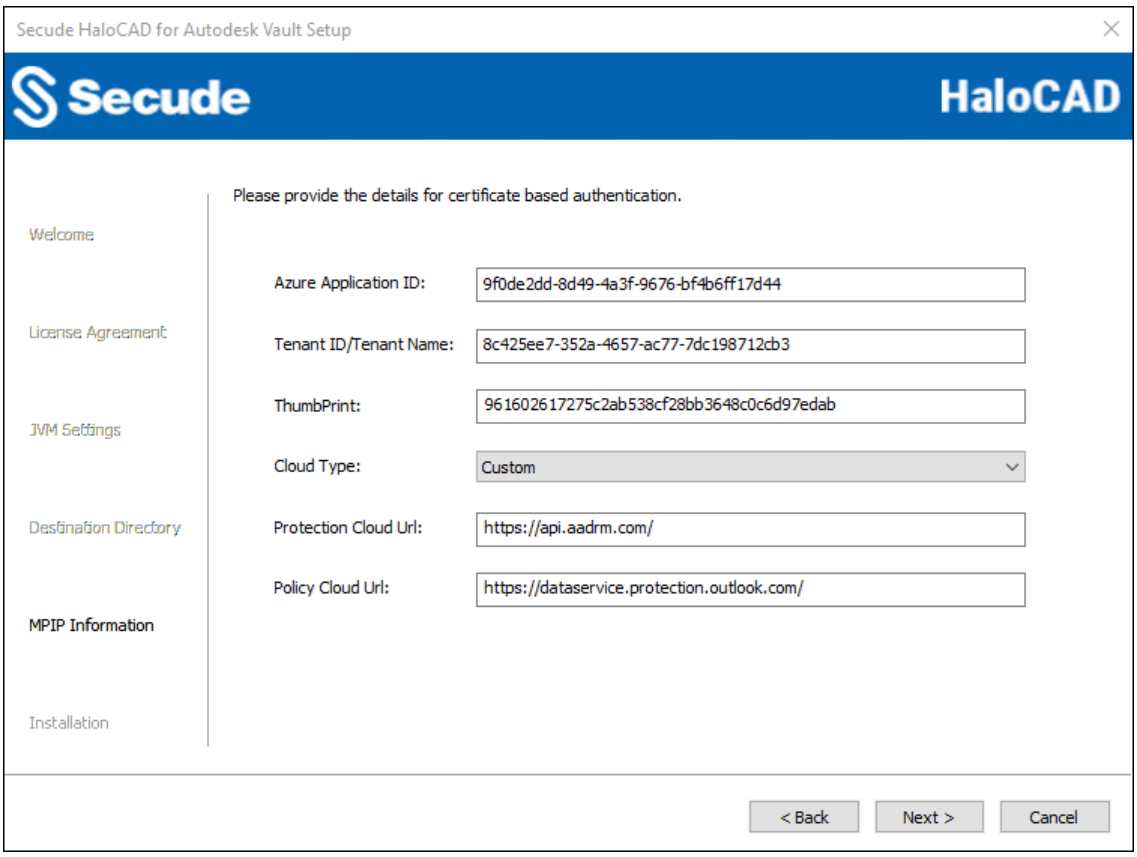
Tomcat pool size configuration dialog

8. 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.
9. Click **Next**. The destination folder selection dialog will appear:



Destination folder selection dialog

10. By default, application files are stored in the program files directory (`C:\Program Files\Secude\`). If you would like to choose an alternate location, click the **Browse** button and select your location preference. To return to any point in the installation process, click the **Back** button (optional).
11. Click **Next** to allow the Setup program to install the HaloCAD component.
12. The certificate-based authentication dialog appears. To avoid errors, please ensure that you enter the correct Azure application registration details in the installation wizard.



Certificate-based authentication dialog

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

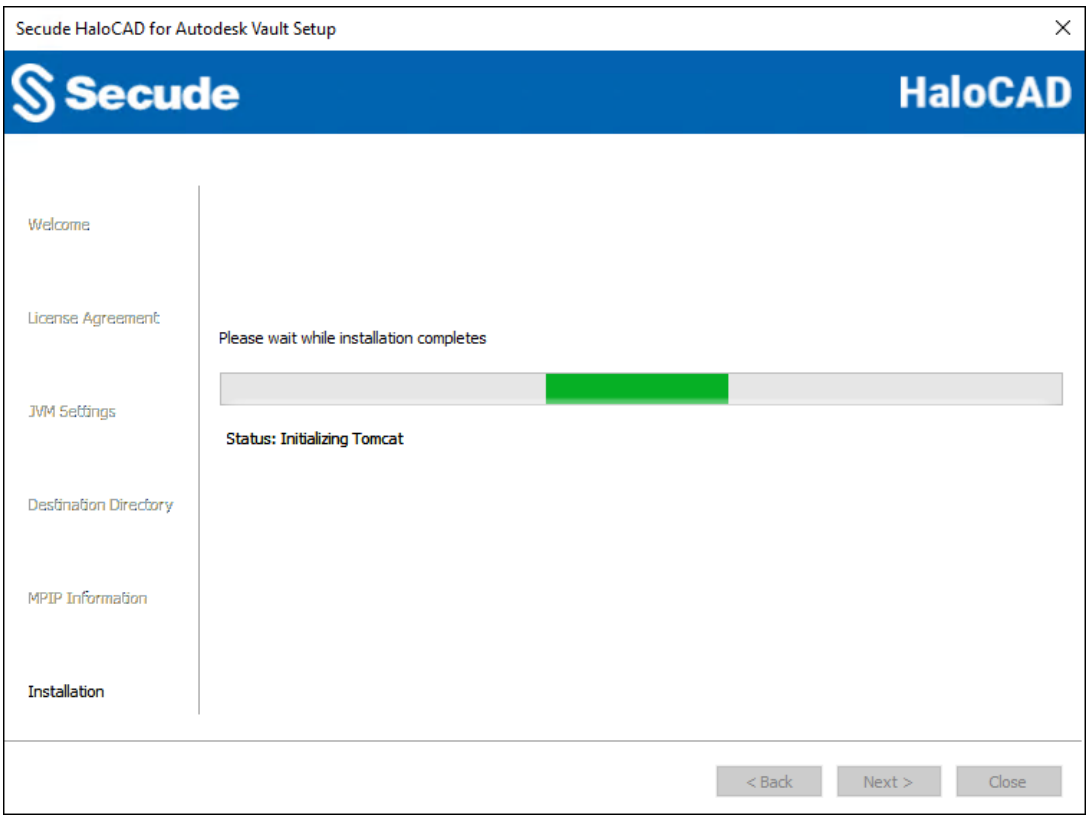
b. **Tenant ID/Tenant Name**: Enter your Microsoft Entra tenant name (for example, `contoso.onmicrosoft.com`) or its tenant ID (for example, `8c425ee7-352a-4657-ac77-7dc198712cb3`)

c. **Thumbprint**Error! Bookmark not defined.: Enter the thumbprint of the MPIP authentication certificate installed in the **Local Computer** certificate store.

d. **Cloud Type**: By default, Commercial will be set. However, based on your Azure subscription and configuration, you can change the cloud type from the list — Commercial / Custom / Germany / US_DoD / US_GCC / US_GCC_High / US_Sec / US_Nat / China_01. In the case of **Custom** cloud type, you need to enter the appropriate URLs in **Protection Cloud URL** (for example, `https://api.aadrm.com`) and **Policy Cloud URL** (for example, `https://dataservice.protection.outlook.com`).

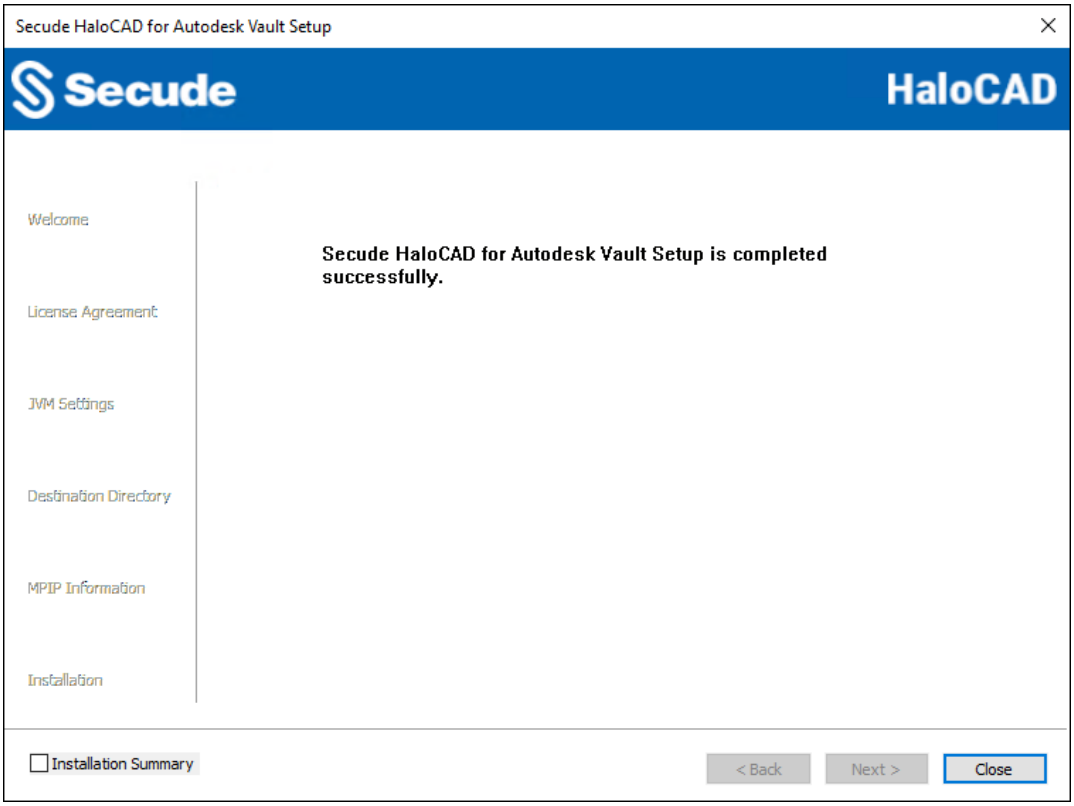
e. Click **Next**.

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



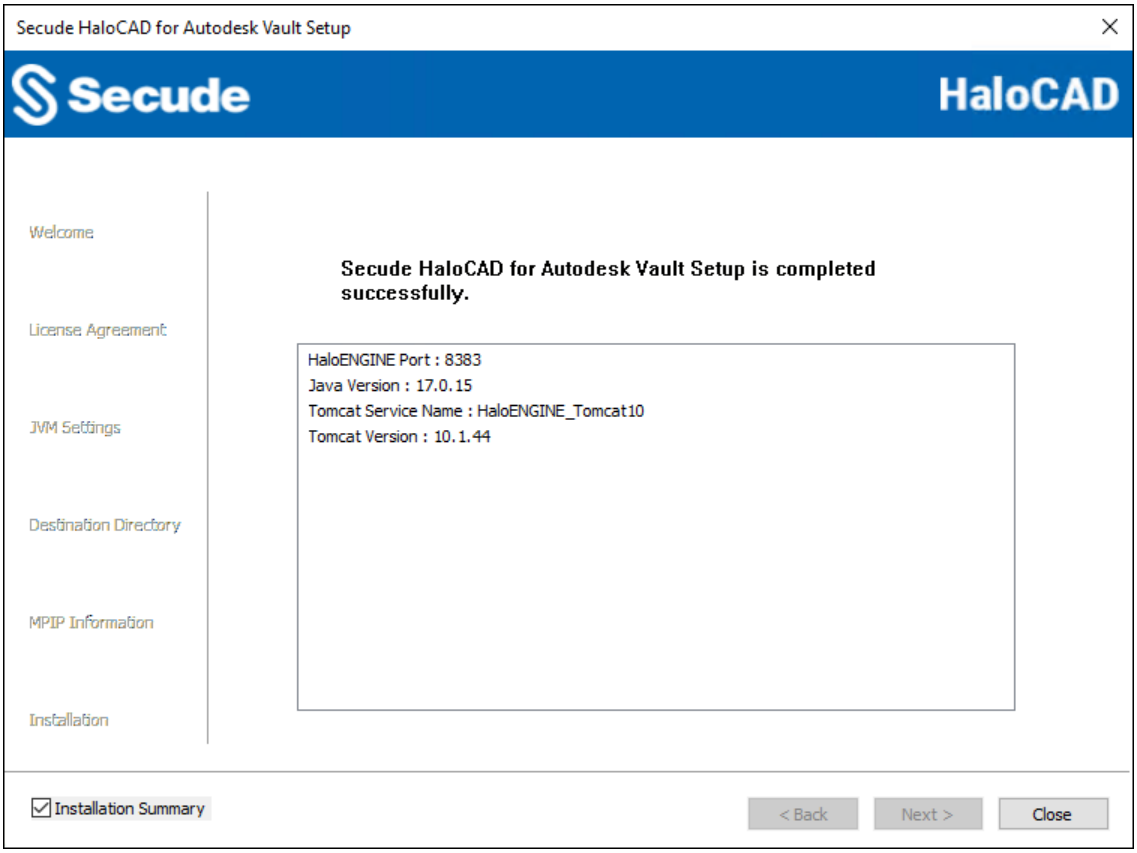
Installation progress dialog

14. When the installation is complete, a message appears confirming that the HaloCAD 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 with preinstalled HaloENGINE dialog

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

2.3.2. Silent Mode

Besides graphical mode, the HaloCAD 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 component installer.
3. To know the list of options available in silent mode, follow the steps given below:

   Type `HaloCAD_Autodesk_Vault_Setup.exe -help`

   Press `Enter`

   Output

   ...

   ```
   HaloCAD_Autodesk_Vault_Setup.exe -help
   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 Custom https://api.aadrm.com
https://dataservice.protection.outlook.com
```

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

3. Configuring the HaloCAD Proxy

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

3.1. 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. Stop the Tomcat Service.

Use `services.msc` to stop the service.

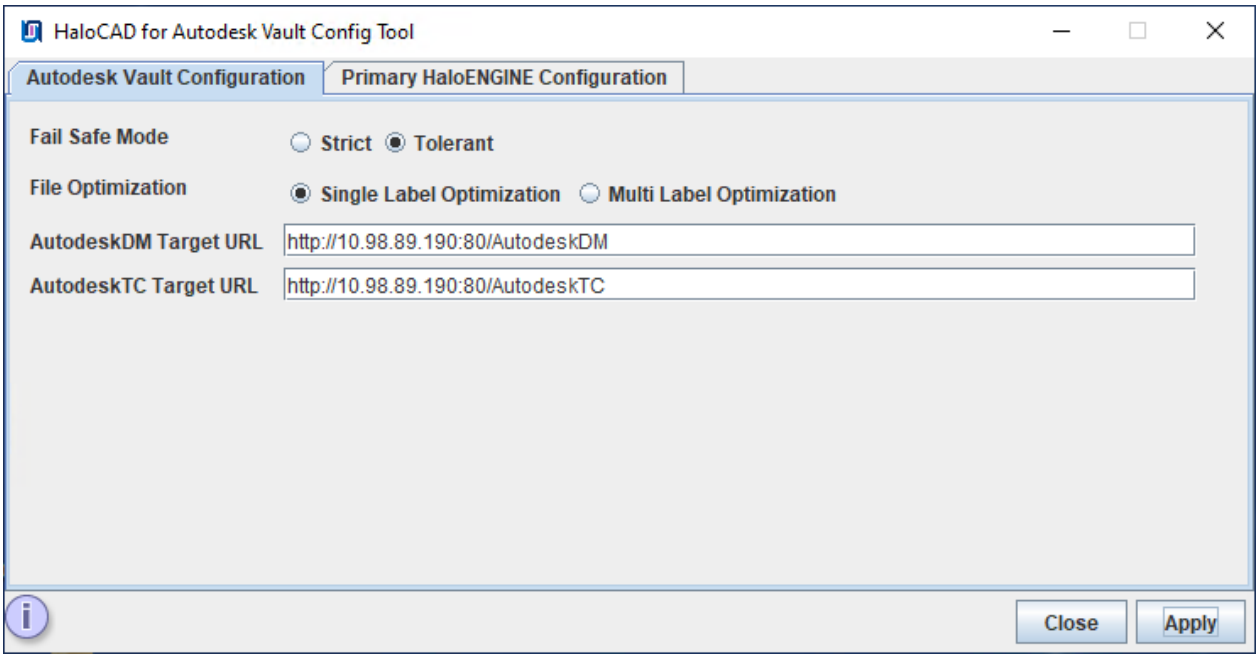
Step 2. Run the HaloCAD Configuration Tool.

1. Navigate to the destination folder you specified during installation. The default folder is `C:\Program Files\Secude\HalocadVault\config`.
2. To run, either double-click the `HaloCAD-for-Autodesk-Vault-config-<version>.jar` file or open Command Prompt with administrative privileges and execute the following syntax.

   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`
3. The *HaloCAD for Autodesk Vault Config Tool* window appears as shown in the figure below.

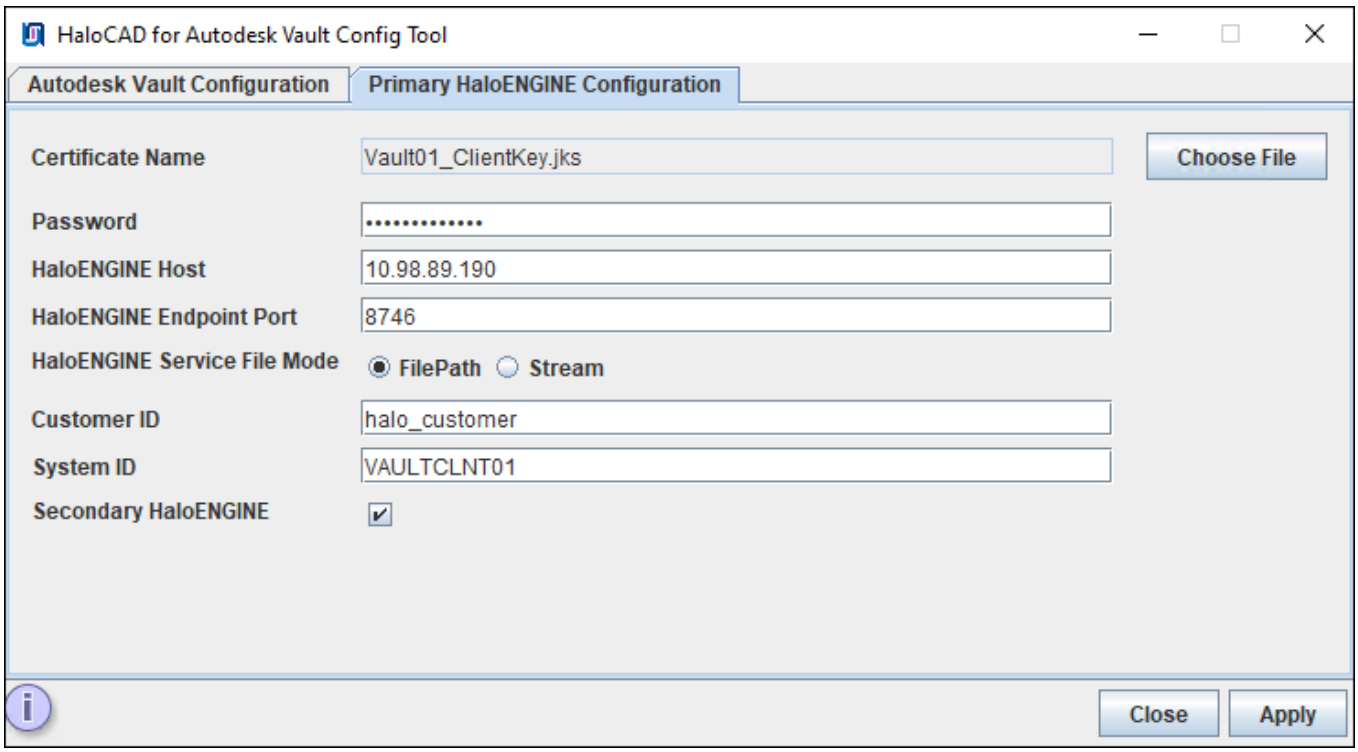
Step 2a. Enter the following details under the *Autodesk Vault Configuration* tab.



Autodesk Vault 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 is blocked whenever any error occurs.
   b. **Tolerant (default)**: The file upload or download will be allowed, 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. **AutodeskDM Target URL**: Enter the AutodeskDM Target URL on which your Autodesk Vault is hosted. For example, `http://10.98.89.190:80/AutodeskDM`.
4. **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`.
5. Click **Apply**. A red tooltip message appears if any required values are missing. Enter the missing information and click **Apply** to continue.
   Results:
   a. A confirmation message dialog box appears.
   b. Click **OK** to close the dialog box.

Step 2b. Enter the following information under the *Primary HaloENGINE Configuration* tab.



Primary 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 the HaloENGINE and Autodesk Vault). Example, `Vault01_ClientKey.jks`
2. **Password**: Enter the password of the selected client Keystore. Example, `Key$T#123`
3. **HaloENGINE Host**: Enter the IP address/FQDN of HaloENGINE. Example, `10.98.89.190`
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 Autodesk Vault Server's hostname, and the same must be entered in the **System Unique ID** (HaloENGINE admin portal). For example, `VAULTCLNT01`.
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.

   Results:

   a. A confirmation message dialog box appears.

   b. Click **OK** to close the dialog box.

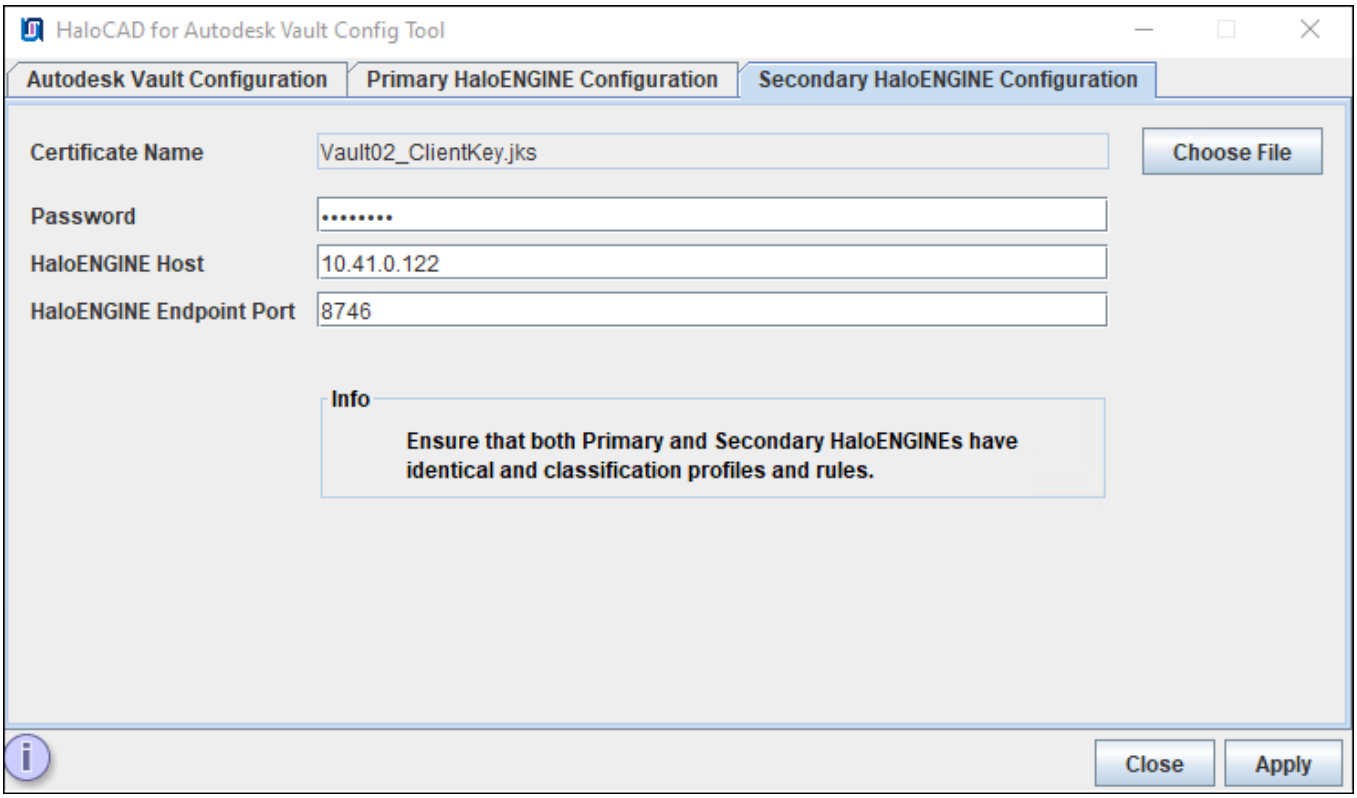
   c. After successful configuration, the configuration tool will create a `config.properties` file in `C:\Program Files\Secude\HalocadVault\config`.

   d. If you have selected the **Secondary HaloENGINE** option, you can notice that the **Secondary HaloENGINE Configuration** tab has been added to the configuration tool, as shown in *Step 2c* below.

Step 2c. Enter the following information under the *Secondary HaloENGINE Configuration* tab.

You can skip this step if you haven't chosen the Secondary HaloENGINE option. This step is only necessary if you want to use the failover mechanism.

Prerequisite: Ensure that the secondary HaloENGINE uses the same configuration profiles and rules as the primary HaloENGINE. Thus, when the primary HaloENGINE fails, the secondary HaloENGINE immediately takes over, assuring continuous operation.



Secondary 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 (secondary) and Autodesk Vault]. For example, `Vault02_ClientKey.jks`
2. **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, `10.41.0.122`.
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.

   Results:

   a. A confirmation message dialog box appears.

   b. Click **OK** to close the dialog box.

Step 3. Start the Tomcat Service.

3.2. 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 Autodesk Vault has been 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 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

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
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 Configuration
0. Exit
Note: If an invalid value is entered, the default value will be applied.
Please choose an option:2
--------------------------------------------------------------------------------
Primary HaloENGINE Configuration
Certificate Name            :
HaloENGINE Host IP          :
HaloENGINE Endpoint Port    :
HaloENGINE Service Mode     :Local
HaloENGINE Service File Mode:File Path
Customer ID                 :halo_customer
System ID                   :
Secondary HaloENGINE        :Disable Secondary HaloENGINE

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

```
0. Exit
Please choose an option: 1
--------------------------------------------------------------------------------
Primary HaloENGINE Configuration
Enter the Primary Certificate Path:
 C:\Users\Administrator\Desktop\Certs\Vault01_ClientKey.jks

Enter the Primary certificate Password:

Enter the Primary HaloENGINE Host:10.98.89.190

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

Enter the Customer ID:halo_customer

Enter the System ID:VAULTCLNT01

Secondary HaloENGINE: (Default:Disable Secondary HaloENGINE)
1. Disable Secondary HaloENGINE
2. Enable Secondary HaloENGINE
Please choose an option: 1
Saved Successfully.
--------------------------------------------------------------------------------
Primary HaloENGINE Configuration
Certificate Name            :Vault01_ClientKey.jks
HaloENGINE Host IP          :10.98.89.190
HaloENGINE Endpoint Port    :8746
HaloENGINE Service Mode     :Local
HaloENGINE Service File Mode:File Path
Customer ID                 :halo_customer
System ID                   :VAULTCLNT01
Secondary HaloENGINE        :Disable Secondary HaloENGINE

1. Modify all configuration
2. Modify the particular configuration
3. Back to main menu
0. Exit
Please choose an option:
```

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

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\HalocadVault\HaloENGINEService\lib\heslibconfig.exe`
MIP logs	`C:\Program Files\Secude\HalocadVault\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.
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.

Name	Description
	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.
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.

Name	Description
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

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.

5. 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.

6. 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 2, update the settings, and then restart the Tomcat Service.

7. Appendix

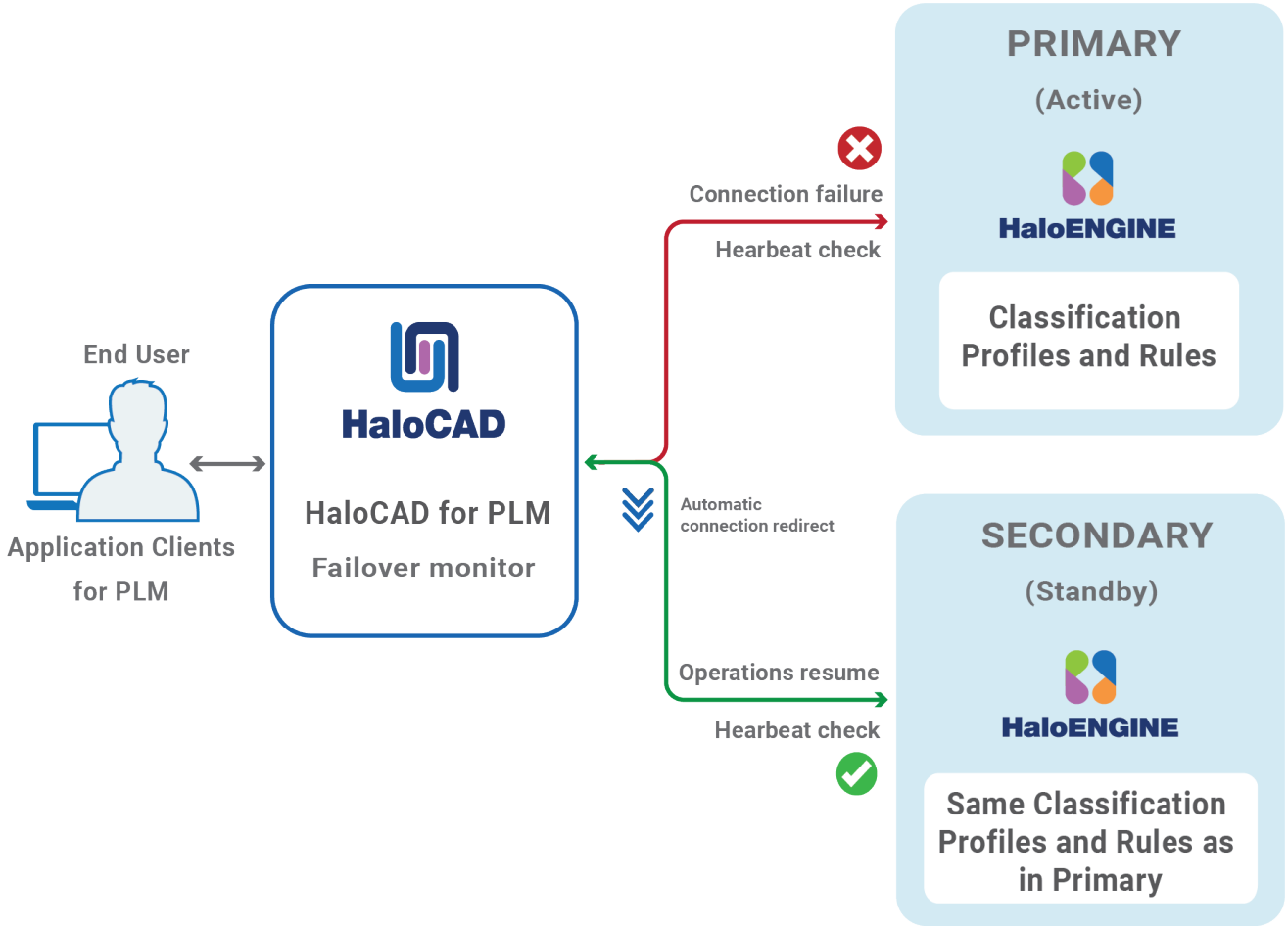
This section provides supplemental information.

7.1. 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. Make sure the secondary HaloENGINE has HaloENGINE service installed as well.
3. Data replication: Both HaloENGINEs must have the same classification profiles and rules.

7.2. 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	Version	Source Code	License Link
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	1.4.1	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
javax.servlet-api	3.1.+	https://mvnrepository.com/artifact/javax.servlet/javax.servlet-api	https://glassfish.dev.java.net/nonav/public/CDDL+GPL.html
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	Version	Source Code	License Link
activation	1.1.1	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	1.17.158	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
Spdlog	1.15.3	-	https://github.com/gabime/spdlog

Third-party libraries

7.3. Metadata Definition

The Autodesk Vault metadata present in the HaloENGINE is listed in the table below.

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 folder name in 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

7.4. Download Log Definition

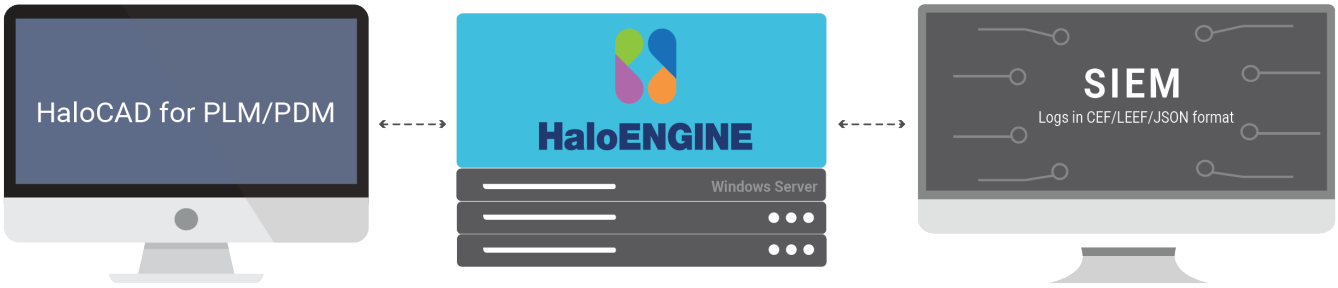
This section explains the log definition for every log format that HaloENGINE supports.

7.4.1. 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, 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

7.4.2. 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|6.9.0.0|`
	• 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. 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.	Please refer to the following table.

CEF Header details

```
06:40:10.457 CEF:0|Secude|HaloCAD|6.9.1.0|100|user
download|1|deviceCustomDate1Label=exportTime deviceCustomDate1=Oct 21 2025 13:40:10
UTC externalId=39BE6C83F24145FDBB254225210C8BBA deviceCustomDate2Label=logTime
deviceCustomDate2=Oct 21 2025 13:40:10 UTC act=unblocked;labeled;protected
fname=commandshell_testing.txt filePath=$/TestDocument/commandshell_testing.txt
fileType=txt fsize=24455 in=59411 shost=Vault duser=Administrator,type:Administrator
dst=10.91.0.1 requestClientApplication=[null] cs2Label=DataDestination cs2=[
platform\=[Windows NT], browser\=[VP], browser_version\=[null], device_type\=[null],
terminal_id\=[10.91.0.1], destination_attributes\=[{ key\=[client_ip],
value\=[10.91.0.1], type\=[null] }, { key\=[client_host], value\=[10.91.0.1],
type\=[null] }] ] cs3Label=DataOrigin cs3=[ source_type\=[PLM], system_name\=[Vault],
client_type\=[AUTODESK_VAULT], plm_info\=[{ key\=[document_id], value\=[3880],
type\=[null] }, { key\=[document_type], value\=[txt], type\=[null] }, {
key\=[document_number], value\=[3880], type\=[null] }, { key\=[document_version],
value\=[2], type\=[null] }]] cs4Label=ClassifyProtectionData cs4=[
policy_id\=[d7e95033-e7f1-4218-8941-7d60d8e9cf69], policy_name\=[CADSecured],
policy_type\=[company_policy], error\=[false], author\=[HALOCORE Service] ]
```

CEF sample

7.4.3. 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

```
06:46:33.771 LEEF:2.0|Secude|HaloCAD|6.9.1.0|100|^|exportTime=Oct 21 2025 13:46:33
UTC^eventName=user download^externalId=FC0969BA9740443F87D22C19C77848F6^logTime=Oct 21
2025 13:46:33
UTC^act=unblocked;labeled;protected^fname=commandshell_testing.txt^filePath=$/TestDocu
ment/commandshell_testing.txt^ftype=txt^fsize=24455^fdwnsize=59411^shost=Vault^usrName
=Administrator,type:Administrator^dst=10.91.0.1^usrAgent=[null]^dataDestination=[
platform=[Windows NT], browser=[VP], browser_version=[null], device_type=[null],
terminal_id=[10.91.0.1], destination_attributes=[ {key=[client_ip], value=[10.91.0.1],
type=[null]}, {key=[client_host], value=[10.91.0.1], type=[null]} ] ]^dataOrigin=[
source_type=[PLM], system_name=[Vault], client_type=[AUTODESK_VAULT], plm_info=[
{key=[document_id], value=[3880], type=[null]}, {key=[document_type], value=[txt],
type=[null]}, {key=[document_number], value=[3880], type=[null]},
{key=[document_version], value=[2], type=[null]} ] ]^classifyProtectionData=[
policy_id=[d7e95033-e7f1-4218-8941-7d60d8e9cf69], policy_name=[CADSecured],
policy_type=[company_policy], extendedTags=[ message=[Success] ], error=[false],
author=[HALOCORE Service] ]
```

LEEF sample

Format	Description	Example
Syslog Header	The Syslog header contains the timestamp.	`17:10:28.743`
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, `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|6.9.0.0|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|6.9.0.0|100|`
	EventID	A unique identifier for an event.

Format	Description	Example
	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

7.4.4. 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).

```
06:42:42.296
{"log_id":"ED65FA85D02C4BB4AFAC41D1297679D5","product":"HaloCAD","source_host":{"shost
":"Vault"},"protection":{"policy_id":"d7e95033-e7f1-4218-8941-
7d60d8e9cf69","extended_tags":[{"value":"Success","key":"message"}],"policy_name":"CAD
Secured","error":false},"destination_info":{"hostname":"10.91.0.1","destination_attrib
utes":[{"value":"10.91.0.1","key":"client_ip"},{"value":"10.91.0.1","key":"client_host
"}],"destination_ip":"10.91.0.1","os":"Windows
NT","recipients":[],"browser":"VP","device_type":"null","browser_version":"null","user
_agent":"null"},"classification":{"classification_by_system":[],"classification_by_use
r":[]},"version":"6.9.1.0","log_time":"Oct 21 2025 13:42:42
UTC","event_id":100,"data_origin":{"generic_info":"null","sap_info":"null","system_nam
e":"Vault","pre_process_info":[],"source_type":"PLM","client_type":"AUTODESK_VAULT","p
lm_info":[{"value":"3880","key":"document_id"},{"value":"txt","key":"document_type"},{
"value":"3880","key":"document_number"},{"value":"2","key":"document_version"}],"bi_in
fo":"null"},"user_info":{"user_email":"HALOCORE
Service","user_type":"Administrator","user_name":"Administrator"},"file_info":{"file_p
ath":"$/TestDocument/commandshell_testing.txt","file_name":"commandshell_testing.txt",
"file_type":"txt","download_file_size":59411,"original_file_size":24455},"action":["un
blocked","labeled","protected"],"export_time":"Oct 21 2025 13:42:41 UTC","event":"user
download"}
```

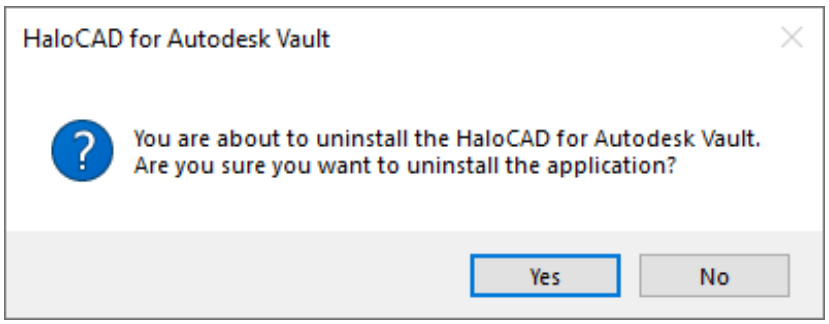

JSON sample

7.5. Uninstalling the HaloCAD for Autodesk Vault

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.

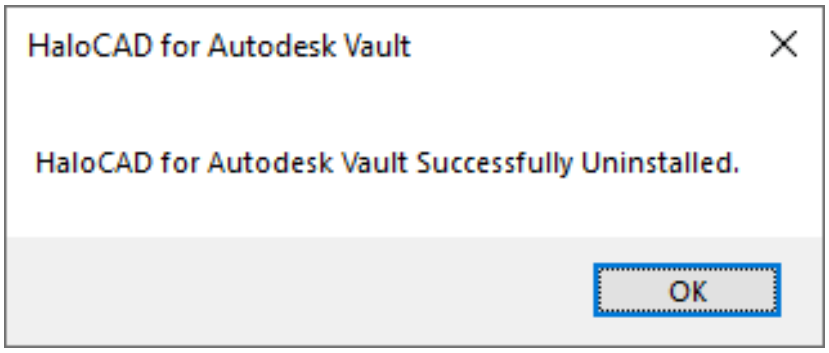
Method #1

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

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

Method #2

The HaloCAD component can be removed using the command line, as illustrated in the sample below.

1. Open a command prompt.

2. Navigate to the HaloCAD component's directory.

   Example: `HaloCAD_Autodesk_Vault_Setup.exe -uninstall`

3. The uninstalling process is complete.

Index

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.