Secude

HaloCAD

HaloCAD for Teamcenter

Installation Manual

Version 2.8

Copyright

Contact

Secude Solutions AG

Murbacherstrasse 19

6003 Luzern, Switzerland

Mail: info@secude.com

Support

Web: https://support.secude.com

Mail: support@secude.com

Table of Contents

Typographic Conventions

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

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

1. Introduction

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

1.1. How does HaloCAD for PLM protect your Data?

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

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

1.2. About this Manual

This manual provides step-by-step guidance for installing and configuring HaloCAD for Teamcenter.

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_Teamcenter_ReleaseNotes_EN_Online.pdf`
Step 2: Prerequisites 1. Before installing, it is recommended that you fulfill the prerequisites, such as registering an application in Microsoft Entra ID 2. HaloCAD Architecture 3. Registering an Application in Microsoft Entra ID - Web 4. Office 365 Subscription Details 5. Recommended URLs, Addresses, and Ports for MPIP 6. Enable Support for TLS 1.2 at the Client Workstation for Microsoft Entra ID	`HaloCAD_Technical_Reference_Manual_EN_Online.pdf`
Step 3: How to install HaloCAD Add-on for NX	`HaloCAD_NX_Manual_Installation_EN_Online.pdf`
Step 4: Install and configure HaloENGINE	`HaloENGINE_Manual_Installation_EN_Online.pdf`
Step 5: Install and configure HaloCAD for Teamcenter	Refer to the current manual.
Step 6: Workflow illustrating protection and decryption	`HaloCAD_Teamcenter_Manual_Operations_EN_Online.pdf`

HaloCAD reference documentation

1.4. Component Functions

Supported PLM CAD Integration: HaloCAD for Teamcenter—Siemens NX Integration

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

1. HaloCAD Add-on for NX
2. HaloCAD for Teamcenter
3. HaloENGINE
4. Microsoft Purview Information Protection

The following list outlines the functions of each component.

1. HaloCAD Add-on for NX - Operates within the Siemens NX application.
2. Receives protected files from Teamcenter and displays their associated labels while enforcing permissions.
3. Logs all add-on–related activities for auditing purposes.

HaloCAD for Teamcenter performs the following functions:

1. It resides on the same network as the Siemens Teamcenter PLM server and acts as a proxy for client traffic to the PLM server
2. It is a proxy component that listens for check-in and check-out actions initiated by the user via AWC browser / RAC session /other clients (MS Office or NX).
3. Connects to Microsoft Purview Information Protection to download sensitivity labels for file processing.
4. Collects metadata for the user-selected file.
5. Obtains action and label information for the user-selected file from HaloENGINE for file processing.
6. Performs encryption and forwards the file stream to the CAD client during check-out operations.
7. Performs decryption and stores the unprotected file in the PLM Vault during check-in operations.
8. Logs HaloCAD for Teamcenter component activities to the local log and sends monitor logs to the HaloENGINE.

Recommendations for improving performance

MPIP offline access

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

HaloENGINE performs the following functions:

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

Microsoft Purview Information Protection

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

Microsoft documentation

This manual assumes that you already have a complete setup of Microsoft Purview Information Protection and you are familiar with using the Microsoft Purview portal and related concepts. If you are new, you can refer to Microsoft's online documentation for setup and configuration.

2. Installing the HaloCAD for Teamcenter

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

2.1. System Requirements

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

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

Requirements

2.2. Prerequisites

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

1. Ensure that you have administrative access to install the HaloCAD component.
2. Ensure that the client computer running the HaloCAD Add-on can connect to the Teamcenter Server.
3. Ensure that your HaloENGINE meets the requirements listed below:
   a. License file (enabled with TEAMCENTER system type).
   b. Proper action rules
   c. Client certificate (`.JKS`)
4. Ensure that the following system variables are set:
   a. **Default_Transient_Server** – The default location of the transient file server.
      - `Default_Transient_Server=http://<host>:<proxy port>/tc/fms`
      - For example, `Default_Transient_Server=http://tclu0310.secude.local:8080/tc/fms`
   b. **Fms_BootStrap_Urls** – The FMS server that manages file downloads.
      - `Fms_BootStrap_Urls=http://<host>:<proxy port>/tc/fms`

- For example, `Fms_BootStrap_Urls=http://tclu0310.secude.local:8080/tc/fms`

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

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

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

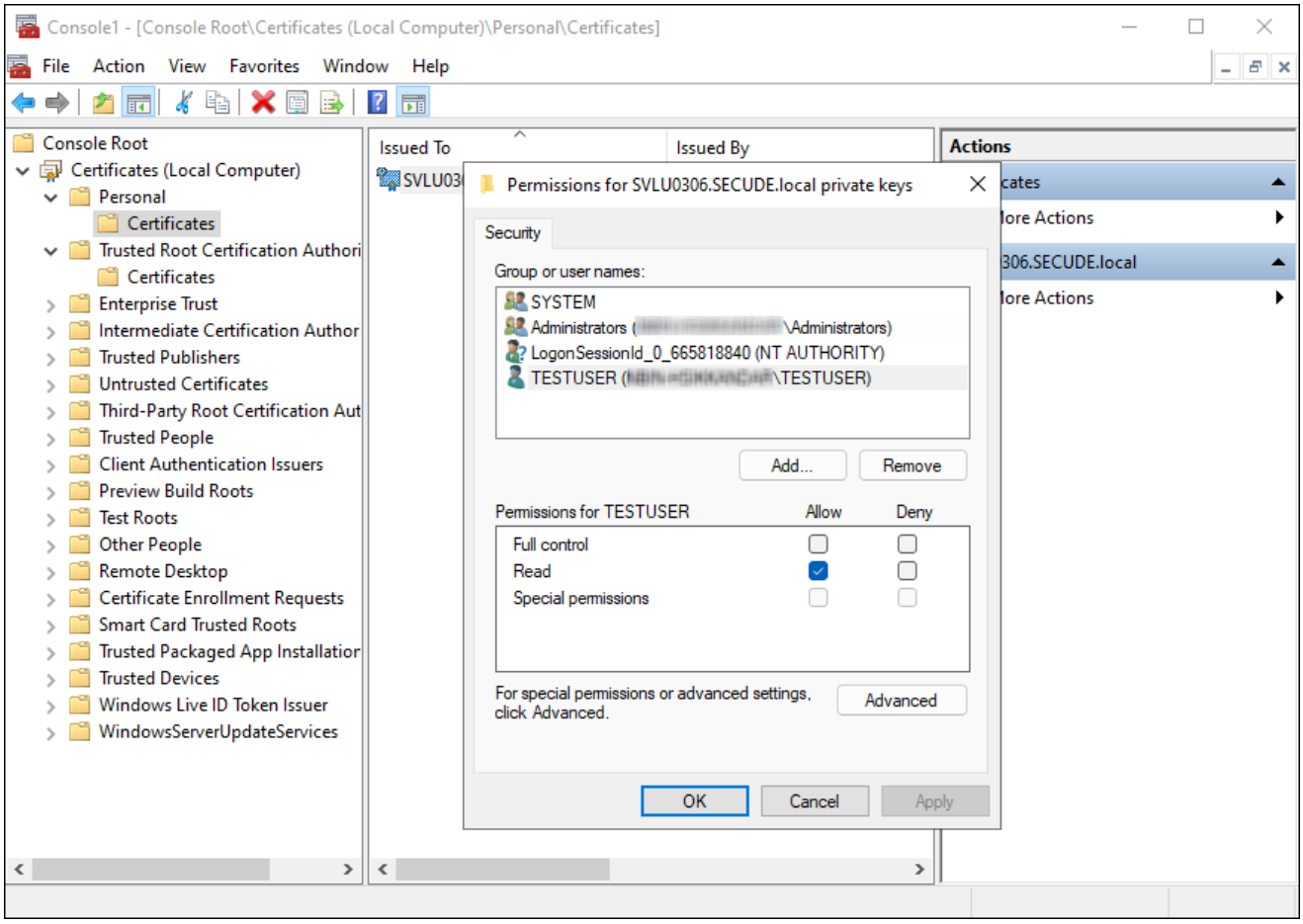
Prerequisites

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

Follow the procedure below to grant read access:

1. Open **Certificate Manager** as Administrator.

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



Granting private key access to a non-admin user

2.3. 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

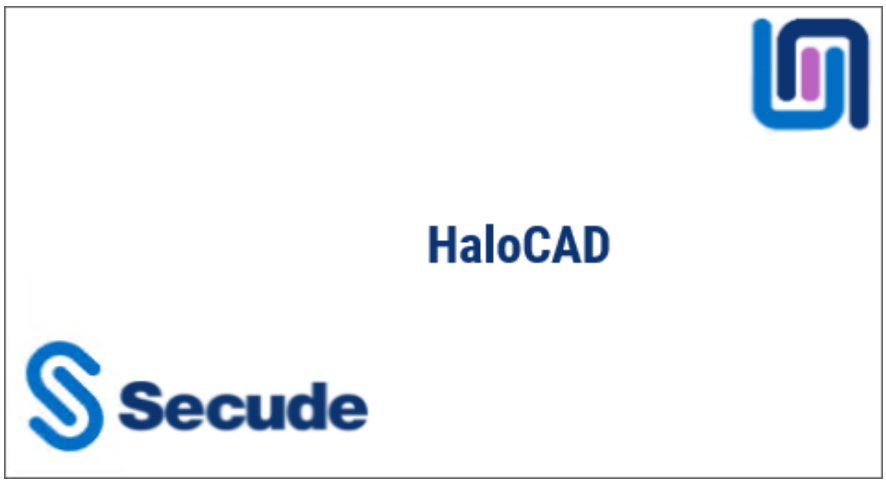
Before installing HaloCAD, ensure that the following requirements are met:

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 installing HaloCAD must have administrator privileges.

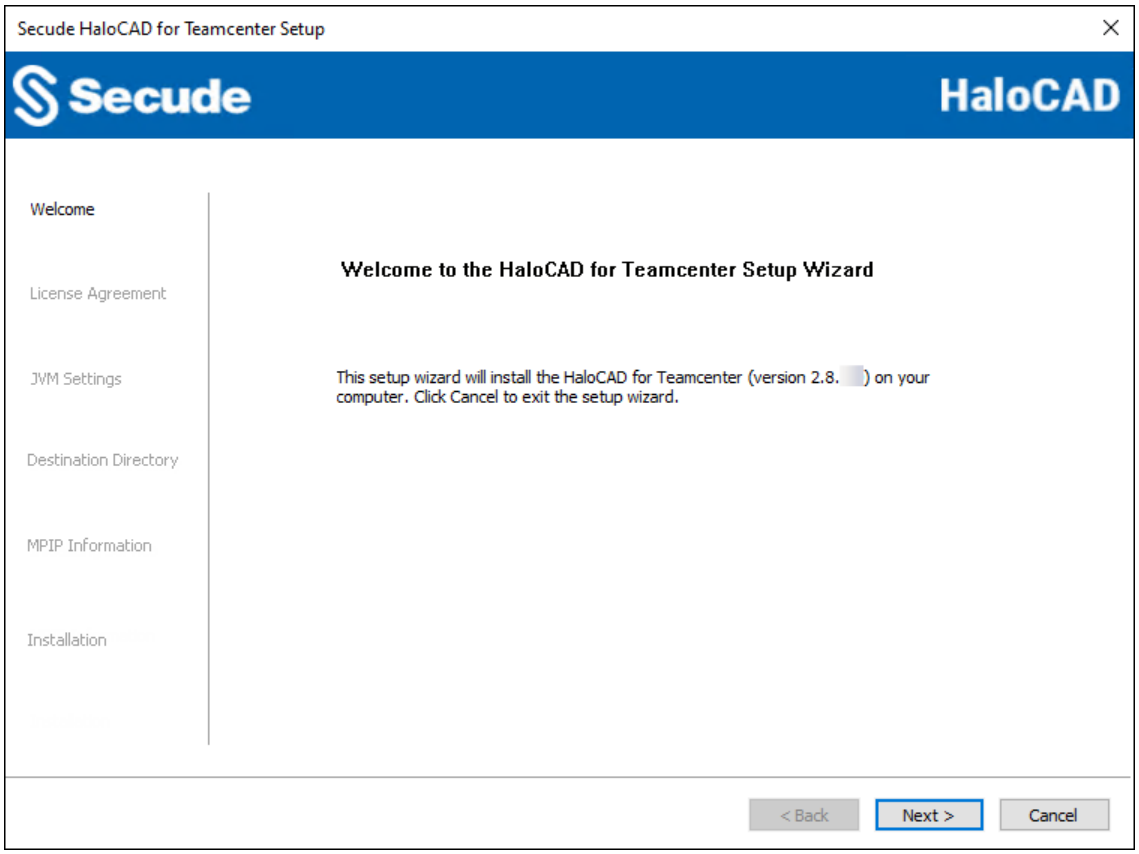
2.3.1. Graphical Mode

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

1. To begin the interactive installation, double-click the installer `HaloCAD_Teamcenter_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.

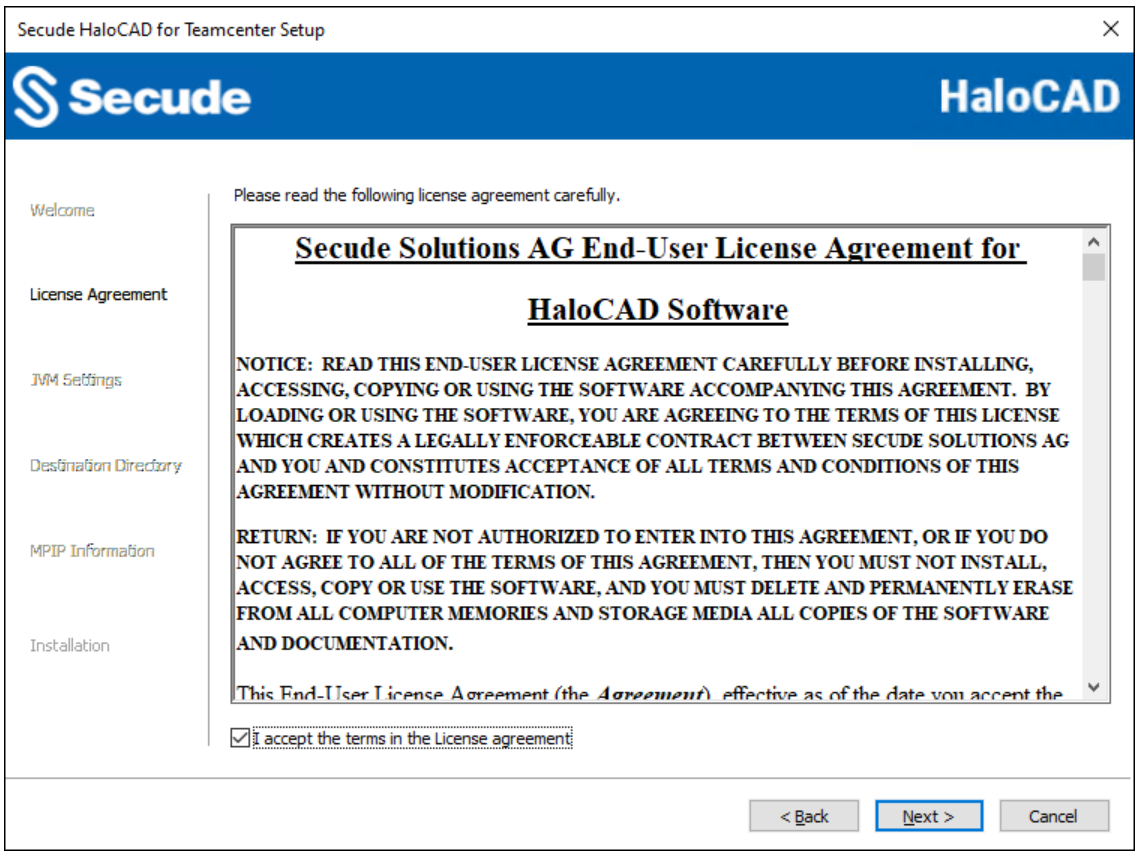


Startup Dialog



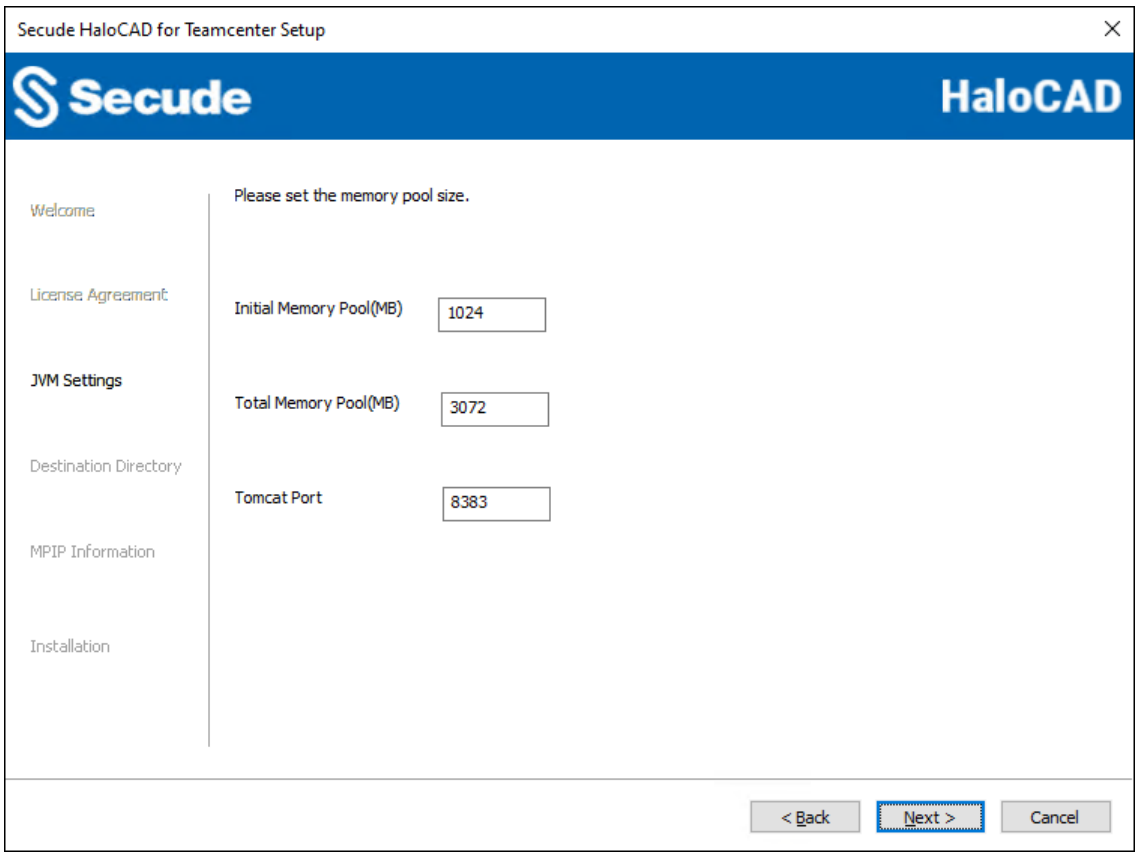
Welcome Dialog

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



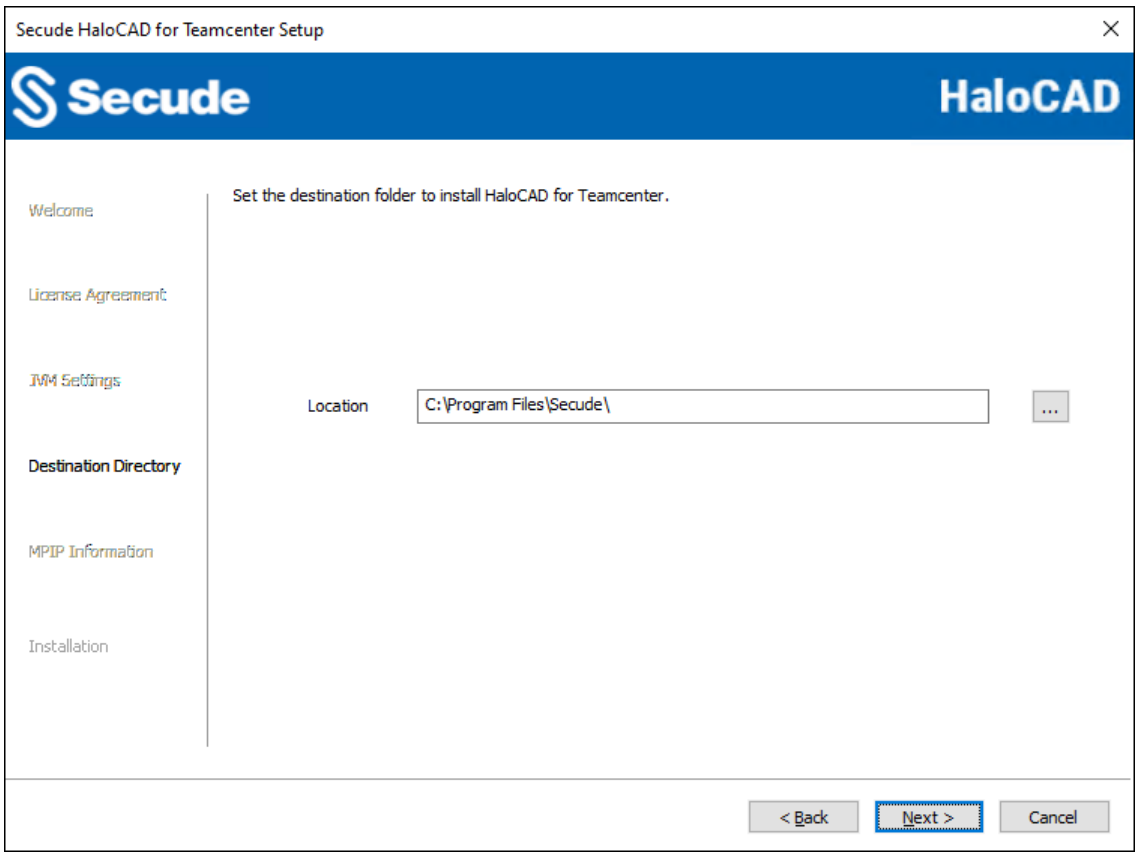
End-User License Agreement Dialog

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.



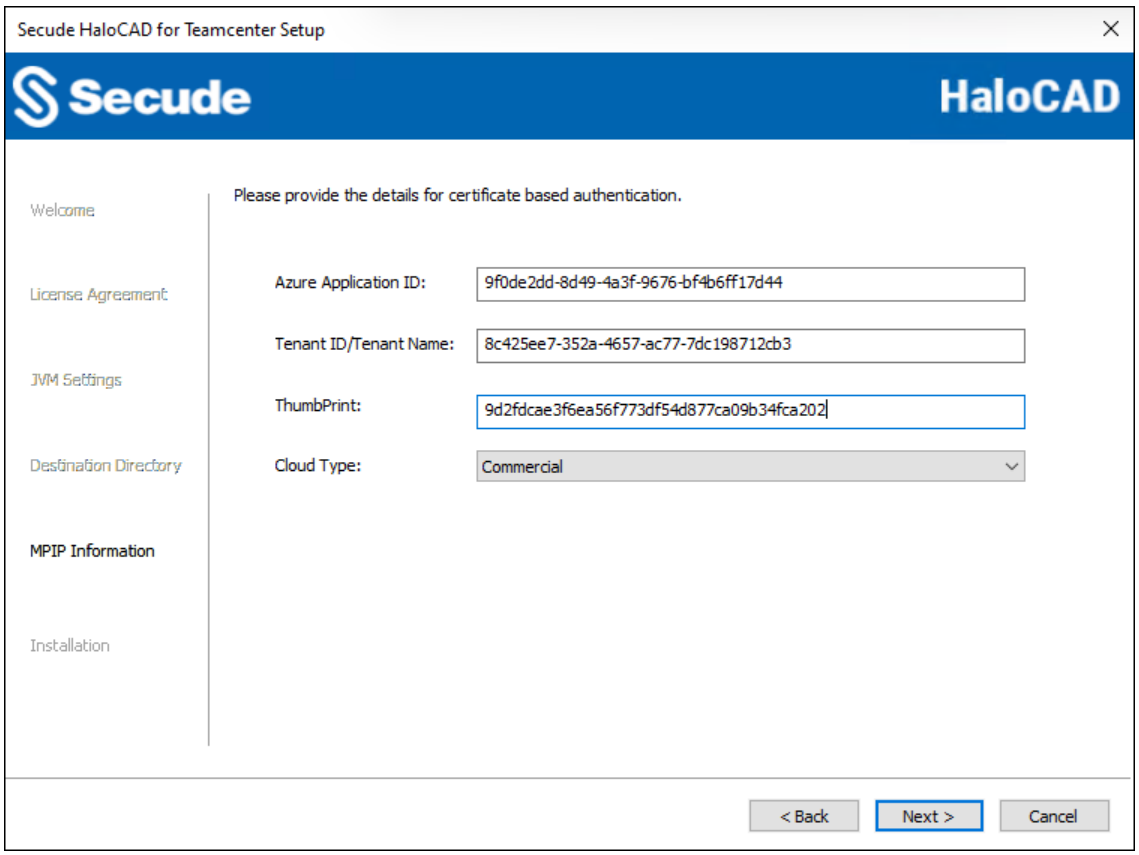
Tomcat pool size configuration dialog

8. Specify the amount of memory to modify the preset values for the **Initial Memory Pool**, **Total Memory Pool**, and **Tomcat Port**. The default port is **8383**; however, you can change the port number. The port value must be greater than **999** and less than or equal to **65535**. Note: Ensure that the **Total Memory Pool** does not exceed three-fourths (3/4) of the system's available RAM.
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 Microsoft Entra ID application details in the installation wizard.



Certificate-based authentication dialog

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

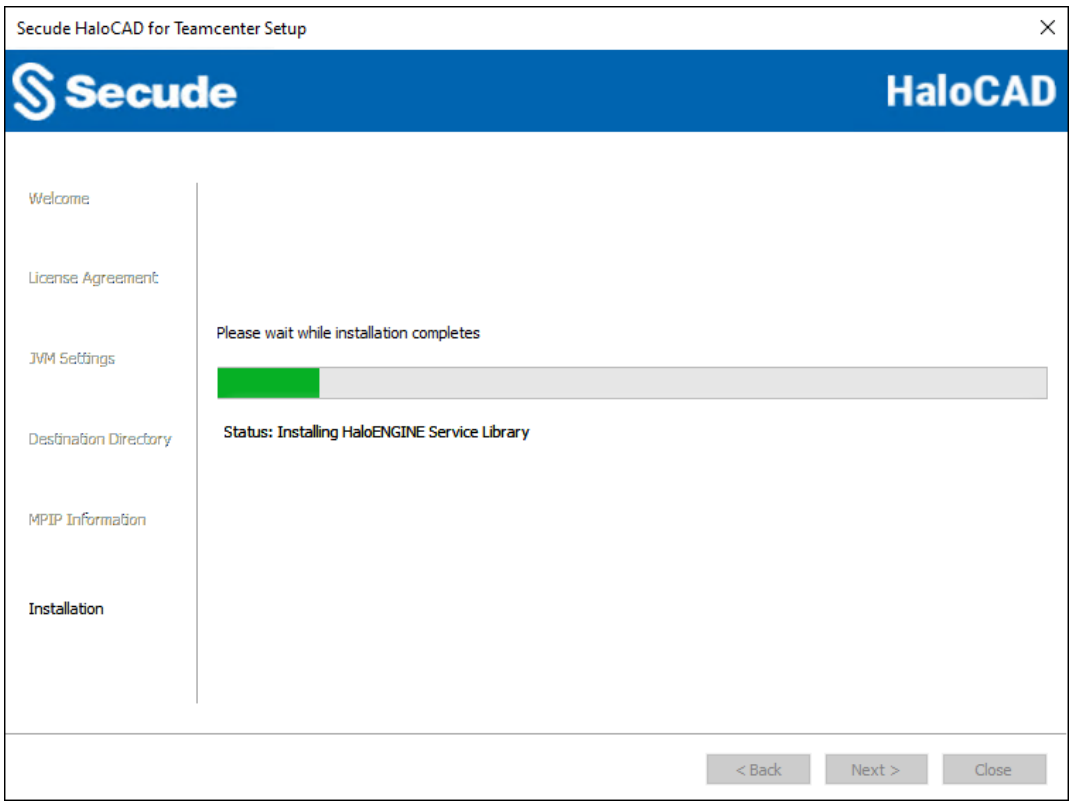
b. **Tenant ID/Tenant Name**: Enter your Microsoft Entra tenant name (for example, `contoso.onmicrosoft.com`) or its tenant ID (for example, `8c425ee7-352a-4657-ac77-7dc198712cb3`).

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

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

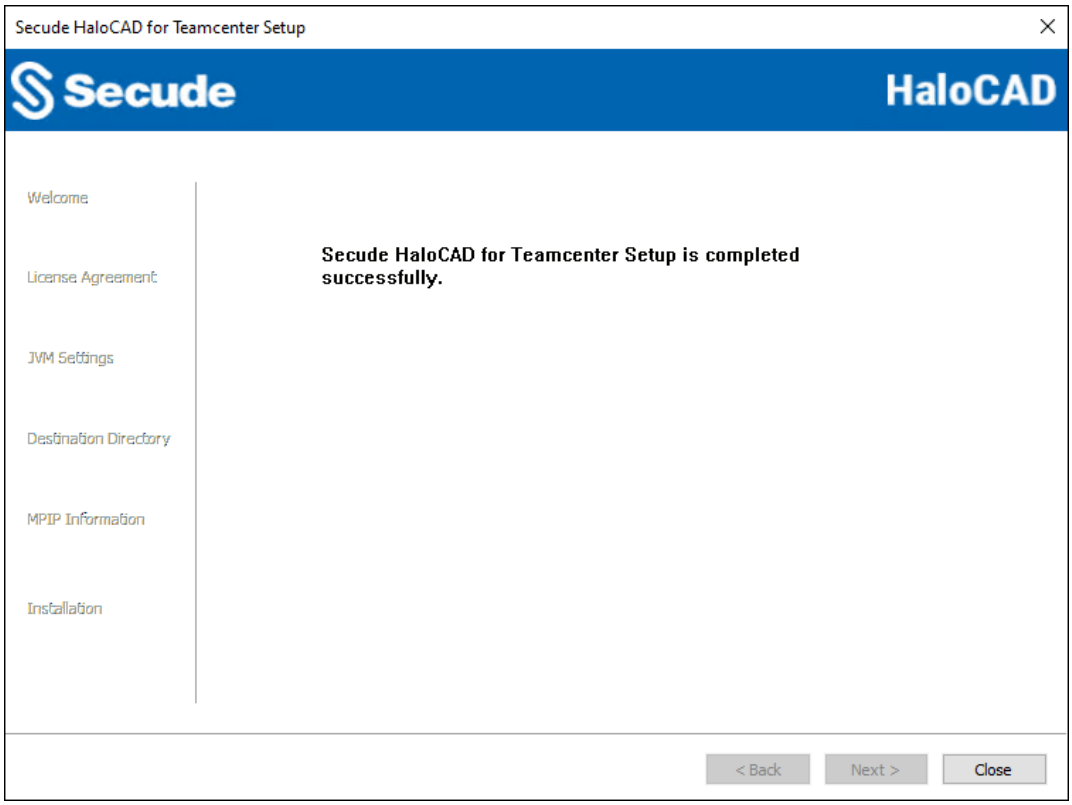
e. Click **Next**.

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. 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_Teamcenter_Setup.exe -help`

   Press `Enter`

   Output

   ...

   ```
   HaloCAD_Teamcenter_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_Teamcenter_Setup.exe -uninstall
   ```
4. The following command shows how to install and initialize HaloCAD.

   ```
   HaloCAD_Teamcenter_Setup.exe -install -initmempool 1024 -totalmempool 2048 -dir
   "C:\Program Files\Secude" -port 8383 -applicationid "9f0de2dd-8d49-4a3f-9676-
   bf4b6ff17d44" -tenantid "8c425ee7-352a-4657-ac77-7dc198712cb3" -thumbprint
   "961602617275c2ab538cf28bb3648c0c6d97edab" -cloudtype "Commercial"
   ```
5. Press `Enter`.
6. The installation is complete.

3. Configuring the HaloCAD Proxy

This section explains how to configure HaloCAD and HaloENGINE parameters using both command-line and GUI methods, as well as Dataset and TCCS configurations.

3.1. Configuration Using Tool (GUI)

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

Follow these steps to configure the settings through the GUI:

Step 1. Run the HaloCAD Config tool.

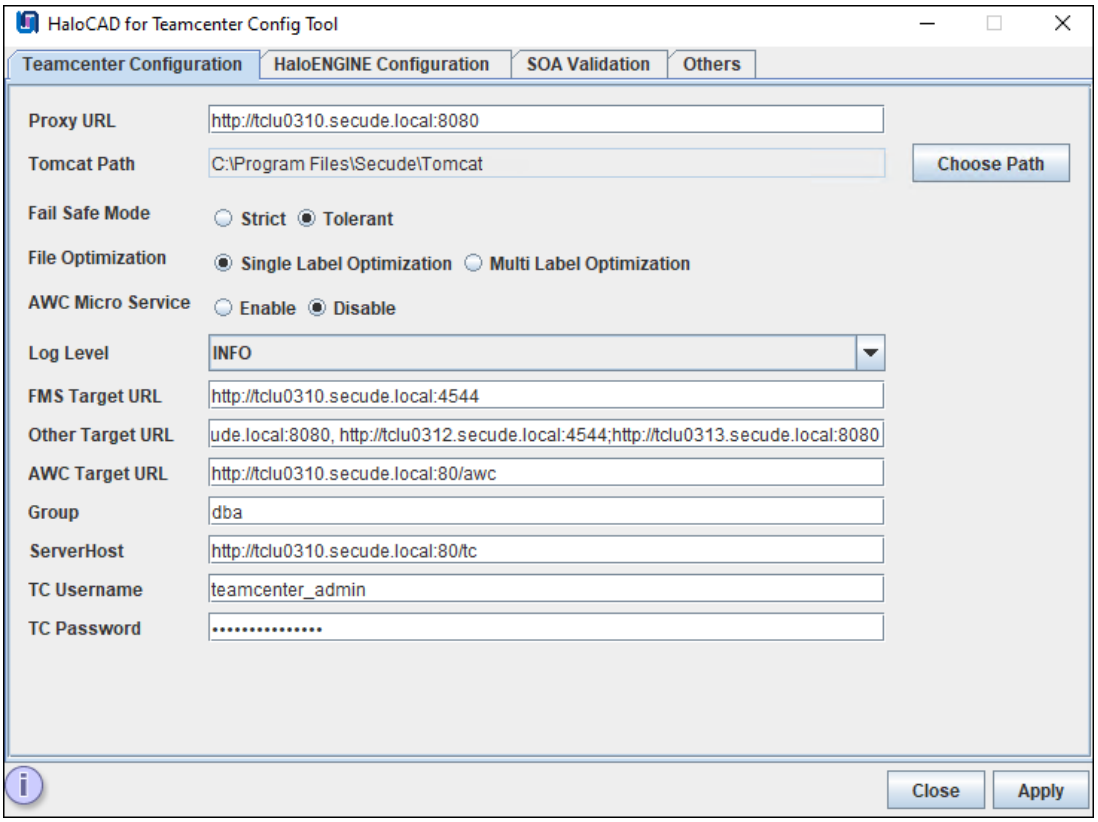
1. Go to the default installation directory `C:\Program Files\Secude\HaloCADTeamcenter\config`.
2. To run, either double-click the `halocad-teamcenter-config-<version>.jar` file or open Command Prompt with administrative privileges and execute the following syntax.

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

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

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

Step 2. Enter the following information under the Teamcenter Configuration tab.



Teamcenter Configuration tab

1. **Proxy URL**: Enter the URL of the proxy (HaloCAD component) installation. For example, `http://tclu0310.secude.local:8080`
2. **Tomcat Path**: Click **Choose Path** to browse and select the **Tomcat** home directory path. For example, `C:\Program Files\Secude\Tomcat`
3. **Fail-Safe Mode**: The Fail-Safe Mode controls the system's behavior in case of inconsistencies that prevent the specified protection from being applied (conflicting configuration, server component unreachable, or returning an error message, etc.). You can define any one of the following:
   a. **Strict**: The file upload or download will be blocked whenever any error occurs.
   b. **Tolerant** (default): The file upload or download will be allowed, even when an error occurs.
4. **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.
5. **AWC Micro Service**: To communicate with Teamcenter via **Microservices**, enable this option.
   AWC 5.x with Microservice:
   a. If you use Microservices for AWC, enable the option **AWC Micro Service** and provide the port number in **AWC Proxy Port**. Please use a different port number for the Proxy URL and AWC Proxy Port.
   b. For Example, if your Proxy URL is 8080, you may use a different port for the AWC Proxy Port, such as 8081.
   c. To access AWC, use `http://hostname:awcproxyport`. For example, `http://svlu0309:8081`

   AWC 4.x without Microservice:
   a. Here, to use AWC without Microservice, disable the option **AWC Micro Service**.
   b. To access AWC, use `http://hostname:proxyport/awc`. For example, `http://svlu0309:8080/awc`
6. **Log Level**: Select a log level of your choice.
   a. **INFO**: A standard log level that highlights the progress of the application.
   b. **ERROR**: Logs error events that prevent program execution.

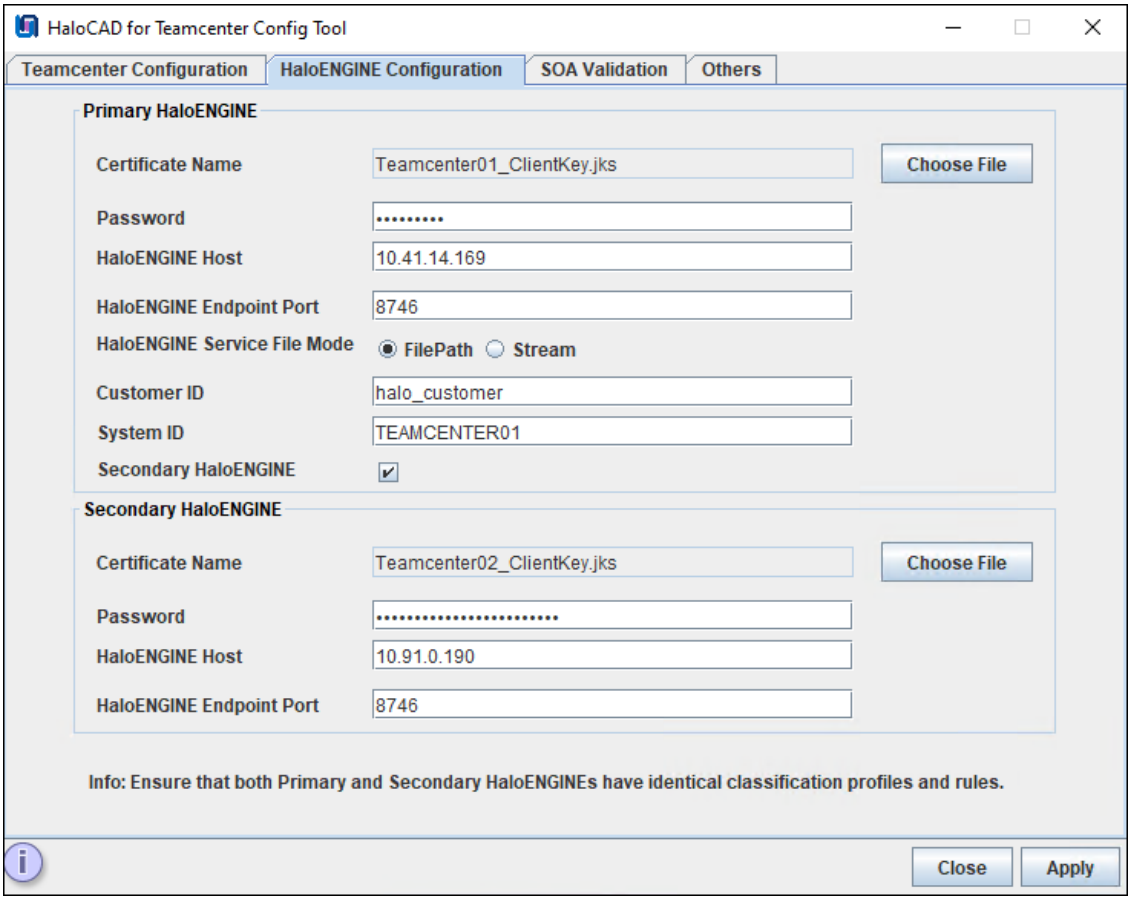
c. **DEBUG**: Logs detailed tracing messages. It should be used for information that may be required for diagnosing issues and troubleshooting. The log level is set to "DEBUG" by default. The log rollover period is configured to 24 hours, which means that every 24 hours, a new log file with the file format `haloproxy.<yyyy-MM-dd>.log` is generated.

7. **FMS Target URL**: Enter the URL of the Teamcenter Server where the file download needs to be protected. For more details, please refer to the section "Appendix". For example, `http://tclu0310.secude.local:4544`
8. **Other Target URL**: In case of multiple FSC configurations, enter other URLs as given in the following format `http://<fmstarget url_1>;http://<proxy url_1>,http://<fmstarget url_2>; http://<proxy url_1>`. For more details, please refer to the section "Appendix". Example, `http://tclu0317.secude.local:4544/;http://tclu0310.secude.local:8080, http://tclu0312.secude.local:4544;http://tclu0313.secude.local:8080`
   AWC Target URL: Enter AWC's URL.
   a. Without Microservice: `http://tclu0310.secude.local:80/awc`
   b. With Microservice: `http://tclu0310.secude.local:3000`
9. **Group**: Enter the name of the group. For example, `dba`.
10. **ServerHost**: Enter your Teamcenter URL. For example, `http://tclu0310.secude.local:80/tc` or `http://tclu0310.secude.local:7001/tc`.
11. **TC Username**: Enter the Teamcenter username. For example, teamcenter_admin.
12. **TC Password**: Enter the Teamcenter password.
13. Click **Apply**. A red tooltip message appears if any required values are missing. Enter the missing information and click **Apply** to continue.

Result:

- A progress bar indicates that the "*Restarting Tomcat Service*".
- A confirmation message dialog box appears.
- Click **OK** to close the confirmation dialog box.

Step 3. Go to the **HaloENGINE Configuration** tab, and then enter the following information.



HaloENGINE Configuration tab

Primary HaloENGINE Configuration

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 the primary HaloENGINE and Teamcenter). For example, `Teamcenter01_ClientKey.jks`
2. **Password**: Enter the password of the selected client Keystore. For example, `ckpass`
3. **Host**: Enter the IP address/FQDN of HaloENGINE. For example, `10.41.14.169`
4. **Endpoint Port**: Enter the Endpoint Port where the service is accessed by this client application. 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**: System Unique ID must be the Teamcenter Server's hostname that is added as the FMS target in the proxy configuration. For example, `TEAMCENTER01`
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".

Secondary HaloENGINE Configuration

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.

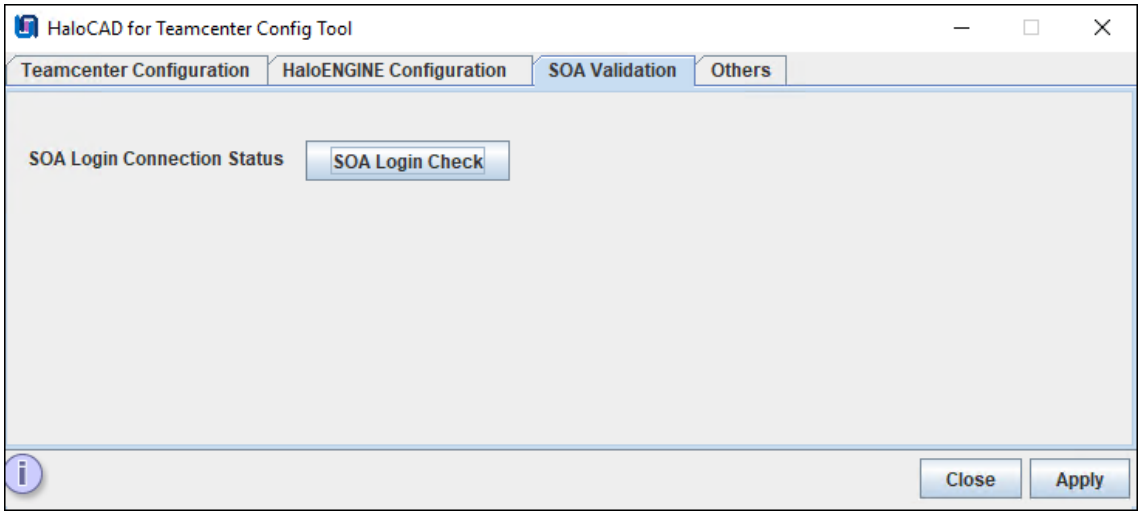
Prerequisite: Ensure that the secondary HaloENGINE uses the same configuration profiles and rules as the primary HaloENGINE. Thus, when the primary HaloENGINE fails, the secondary HaloENGINE immediately takes over, assuring continuous operation.

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 Teamcenter]. For example, `Teamcenter02_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, `10.91.0.190`
4. **HaloENGINE Endpoint Port**: Enter the endpoint port from which HaloENGINE can be accessed. For example, `8746`
5. Click **Apply**. A red tooltip message appears if any required values are missing. Enter the missing information and click **Apply** to continue.

Result:

- A progress bar indicates that the "*Restarting Tomcat Service*".
- A confirmation message dialog box appears.
- Click **OK** to close the confirmation dialog box.

Step 4. Go to the **SOA Validation** tab and check the connection status.



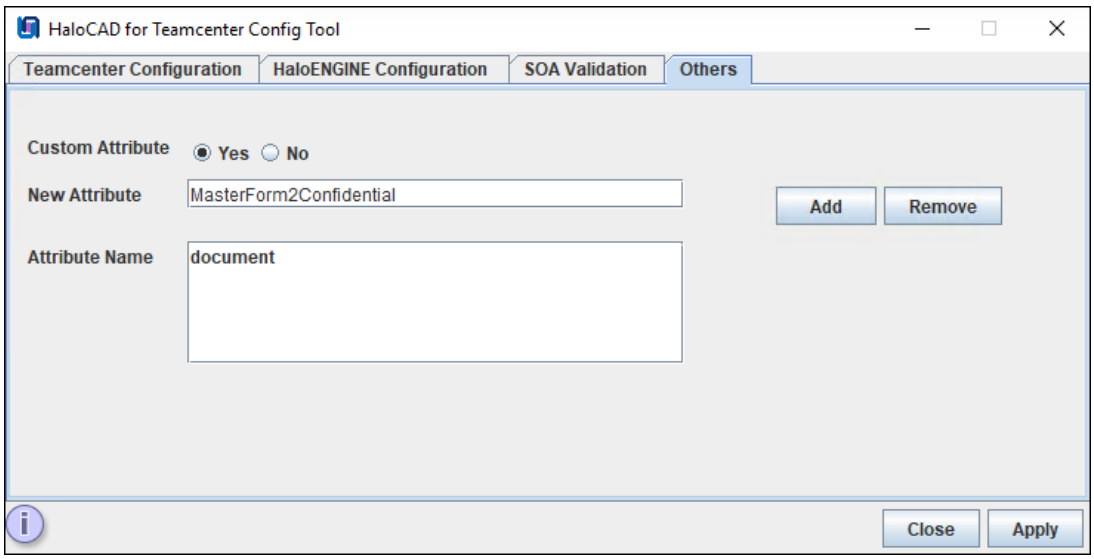
SOA Validation tab

1. Press the **SOA Login Check** button to confirm the SOA credential configuration.
2. Click **Apply**. A red tooltip message appears for any missing values. Enter the required information and click **Apply** to continue.

Result:

- A progress bar indicates that "*Checking SOA Login connection status*" is in progress.
- If the connection is successful, a confirmation message dialog box appears. Click **OK** to close the dialog box.
- If the connection fails, an appropriate warning message appears. Follow the on-screen instructions and try again.

Step 5. Go to the **Others** tab, and then enter the following information.



Others tab

1. **Custom Attribute**
    a. If you do not want to use custom attributes, click **Apply**, and then close the configuration tool window.
    b. If you want to use custom attributes, choose **Yes** in **Custom Attribute**, and then fill out the following information.
2. **New Attribute**: Enter the name of an attribute and then click **Add**. Enter the exact custom property name that was provided during the custom property configuration. For example, the **document** is a new attribute added to the list.
3. The attribute will be added to the **Attribute Name** list.
4. Click **Apply**. A red tooltip message appears for any missing values. Enter the required information and click **Apply** to continue.

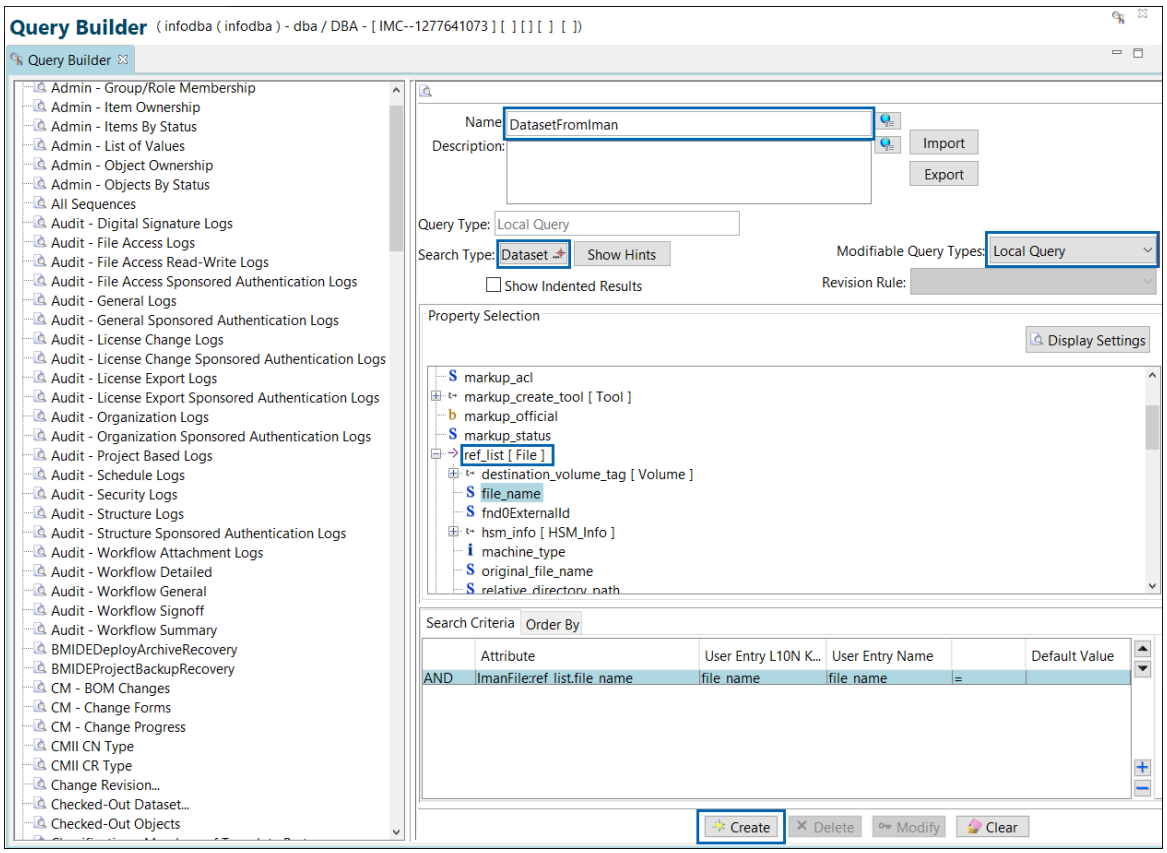
Result:

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

3.2. Dataset Configuration - DatasetFromIman

The following steps are to be carried out by a user with DBA privileges on the Teamcenter server. For illustration, the user account **Infodba** is used.

1. Click the **Query Builder** icon in the navigation pane.
2. Click on **Saved Queries**. A new query page will appear, and you need to enter the following details.
    a. Enter **DatasetFromIman** in the **Name** text box.
    b. In **Search Type**, select **Dataset** from the list.
    c. In **Modifiable Query Types**, select **Local Query** from the list.
    d. Under the **Properties Selection** section, double-click on the property **ref_list**. The **Business Type Selection Dialog** will appear.
    e. You need to search for **ImanFile** and double-click on it. It will be added to the property.
    f. The property name will now appear as **ref_list [File]**.
    g. Under **ref_list [File]**, double-click on **file_name**. You can see the attributes being displayed in the **Search Criteria** section.



Adding a new query - DatasetFromIman

3. Click **Create**.

   Result: The query is saved and added to the Query Builder list.

3.3. TCCS Configuration

The following procedure explains how to change the File Management System (FMS) master file and FMS client cache (FCC) file in the Teamcenter client communication system (TCCS). We recommend that you make a backup of the current two XML files.

1. **Step 1**. Modify the FMS master file.

   a. Go to Siemens installed location `<Installed_Path>\Siemens\Teamcenter12\fsc\fmsmaster_FSC_<ComputerName>_Teamcenter.xml>.`

   For example, `C:\Program Files\Siemens\Teamceter12\fsc\fmsmaster_FSC_tclu0310_Teamcenter.xml`

b. Open the XML file with administrator privileges and add the following line after `<fscgroup id="mygroup"> tag` along with the port number as shown in the example below:
Line format:`<loadbalancer id="ReverseProxy" address="<host>:<port>/tc/fms/" />`
For Example, `<loadbalancer id="ReverseProxy" address="http://tclu0310.Secude.local:8080/tc/fms/" />`

c. Save the file.

2. **Step 2**. Modify the FCC file.

a. Go to the Siemens installed location `<Installed_Path>\Siemens\Teamcenter12\tccs\fcc.xml>`.
For example, `C:\Program Files\Siemens\Teamceter12\tccs\fcc.xml`

b. Open the XML file with administrator privileges and add the following line along with the port number as shown in the example below:
Line format: `<parentfsc address="http://<host>:<port>/tc/fms" priority="0" transport="lan"/> <assignment address="parentfsc address">`
For Example, `<parentfsc address=http://tclu0310.Secude.local:8080/tc/fms priority="0" transport="lan"/> <assignment mode = "parentfsc">`

c. Save the file.

3. **Step 3**. Restart the Siemens service.

a. Restart the Teamcenter FSC Service (**FSC_<serverhostname>_Teamcenter**) via the **Windows Services Manager**.

b. Please note that whenever XML files are modified, the FSC service should be restarted.

3.4. Configuration Using the Command Line

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

Prerequisite: Ensure HaloCAD for Teamcenter is installed.

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

1. Open a command prompt, navigate to the destination folder, then type java -jar halocad-teamcenter-config-<version>.jar -shell and press **Enter**.

```
C:\Program Files\Secude\HaloCADTeamcenter\config>java -jar halocad-teamcenter-
 config-<version>.jar -shell
------------------------------------------------------------------
------------------------------------------------------------------
```

```
HaloCAD for Teamcenter
Config Path: C:\Program Files\Secude\HaloCADTeamcenter\config
1. Teamcenter Configuration
2. Primary HaloENGINE Configuration
3. SOA Validation
4. Others
0. Exit
Note: If an invalid value is entered, the default value will be applied.
Please choose an option:1

------------------------------------------------------------------


------------------------------------------------------------------
Teamcenter Configuration:
------------------------------------------------------------------
Enter the Proxy URL:
http://tclu0310.secude.local:8080

Enter the Tomcat path:
C:\Program Files\Secude\Tomcat

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

Please choose an option:
1

Fail Optimization: (Default:Single Label Optimization)
1. Multi Label Optimization
2. Single Label Optimization

Please choose an option:1

Awc Microservice: (Default:AWC Disable)
1. AWC Enable
2. AWC Disable

Please choose an option:
2

Log Level: (Default:INFO)
1. INFO
2. DEBUG
```

```
3. ERROR

Please choose an option:
2

Enter the FMS Target URI:
http://tclu0310.secude.local:4544

Enter the AWC Target URI:
http://tclu0310.secude.local:80/awc

Enter the Group Name:
dba

Enter the Serverhost:
http://tclu0310.secude.local:80/tc

Enter the TC Username:
teamcenter_admin

Enter the TC Password:

-----------------------------------------------------------------
Teamcenter Configuration:

Proxy URL                       :http://tclu0310.secude.local:8080
Tomcat Path                     :C:\Program Files\Secude\Tomcat
Fail Safe Mode                  :Tolerant
Fail Optimization               :Multi Label Optimization
Awc Microservice                :AWC Disable
Log Level                       :DEBUG
FMS Target URL                  :http://tclu0310.secude.local:4544
AWC Target URL                  :http://tclu0310.secude.local:80/awc
Group Name                      :dba
Server host                     :http://tclu0310.secude.local:80/tc
TC UserName                     :teamcenter_admin

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

Please choose an option:
3
```

```
--------------------------------------------------------------------------------
1. Teamcenter Configuration
2. Primary HaloENGINE Configuration
3. SOA Validation
4. Others
0. Exit
Note: If an invalid value is entered, the default value will be applied.
Please choose an option:2
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
Certificate Configuration:
--------------------------------------------------------------------------------
Enter the Primary Certificate Path:
C:\Users\Administrator\Desktop\Certs\Teamcenter01_ClientKey.jks
File name:Teamcenter01_ClientKey.jks.

Enter the Primary certificate Password:

Enter the Primary HaloENGINE Host:
10.41.14.169

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

Enter the Customer ID:
halo_customer

Enter the System ID:
TEAMCENTER01

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

Please choose an option:
1
Saved Successfully.
--------------------------------------------------------------------------------
Primary HaloENGINE Configuration:

Primary Certificate Name         :Teamcenter01_ClientKey.jks
Primary HaloENGINE Host          :10.41.14.169
Primary HaloENGINE Endpoint Port :8746
HaloENGINE Service File Mode     :File Path
```

```
Customer ID                     :halo_customer
System ID                       :TEAMCENTER01
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:
3
--------------------------------------------------------------------------------
1. Teamcenter Configuration
2. Primary HaloENGINE Configuration
3. SOA Validation
4. Others
0. Exit
Note: If an invalid value is entered, the default value will be applied.
Please choose an option:3
--------------------------------------------------------------------------------

--------------------------------------------------------------------------------
SOA Login connection status:
--------------------------------------------------------------------------------
1. Check SOA connection status
0. Exit

Please choose a valid option:1
Checking Teamcenter Login status, Please wait.
Oct 25, 2024 3:11:58 AM com.secude.halocad.teamcentercmd.AppXSessionCMD loginShell
INFO: TC--> Login successful

1. Check Status again
2. Back to main menu
0. Exit

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

```
Please choose an option:4
--------------------------------------------------------------------------------
Others...
Custom Attribute                :No

1. Custom Attribute
2. Back to main menu
0. Exit

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

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

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

Name	Description
databoundary	Audit and telemetry events are sent to the nearest collector, where these events are stored and processed. Other options: 1. Asia 2. Europe_MiddleEast_Africa 3. European_Union 4. North_America For example, if your AIP administrator sets North_America, the HaloENGINE Tomcat Service forces all telemetry and audit data to go directly to North America.
enabledke	Double Key Encryption • 0 (default value)—Disables the DKE functionality in the HaloENGINE Tomcat Service. • 1 (On)—Enables the DKE functionality in the HaloENGINE Tomcat Service. Please be aware that DKE labels are only visible when DKE functionality is enabled.
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 Proxy Configurations

When you have completed your proxy configuration as described in the previous sections, you need to verify that it works properly by performing the following steps.

5.1. Verify FMS Proxy Configuration

To verify the FMS configuration, follow the instructions below:

1. Go to `<installed_path>\Teamcenter12\tccs\bin`, and execute **CMD** with administrator privilege.
2. Type `fccstat.exe -stop` and press **Enter**. You will receive a confirmation message as "– *fccstat -stop: FCC Stopped.*" This confirms that the server has stopped.
3. Type `fccstat.exe -status` and press **Enter**. You will receive a confirmation message "– *fccstat -status: FCC Offline.*" This confirms that the server went offline.
4. Now, type `fccstat.exe -start` and press **Enter**. You will receive a confirmation message "– *fccstat -start: FCC Started.*" This confirms that the server has started successfully.
5. Type `fccstat.exe -status` and press **Enter**. You will receive a confirmation message "– *fccstat -status: FCC Status... with configured Haloproxy port number.* This confirms that the server is connected to the client. In case, if you have entered the "**Other Target URL**" field, then that URL must be updated along with the proxy in the `fccstat` command.

Result:

```
C:\Users\Teamcenter>cd %fms_home%
C:\Program Files\Siemens\Teamcenter12\tccs>cd bin
C:\Program Files\Siemens\Teamcenter12\tccs\bin>fccstat.exe -stop
fccstat -stop:
FCC Stopped.
C:\Program Files\Siemens\Teamcenter12\tccs\bin>fccstat.exe -status
fccstat -status: FCC Offline.
C:\Program Files\Siemens\Teamcenter12\tccs\bin>fccstat.exe -start
fccstat -start:
FCC Started.
C:\Program Files\Siemens\Teamcenter12\tccs\bin>fccstat.exe -start
fccstat -status:
Cache:
segment: 1 files, 360448 bytes, 0 hits, 0 misses.
read: 0 files, 0 bytes, 0 hits, 0 misses.
write: 0 files, 0 bytes.
Clients:
1 Client connections established.
3 Client request messages processed.
```

```
    2 Client response messages processed.
    0 Client status messages processed.
    0 Client error messages processed.
    Background:
    0 background file download requests received.
    Servers:
    0 segments downloaded.
    0 files downloaded.
    0 files uploaded.
    <site=?>
    0: Assigned FSC 'http://tclu0310.Secude.local:8080/tc/fms/-
     1824758811/mygroup/FSC_tclu0310_Teamcenter_3' is currently active.
```

6. If you do not receive the confirmation message, then you need to review the settings.

5.2. Verify AWC Proxy Configuration

1. Open the AWC link in a browser:
   a. Without Microservice: `http://localhost:<AWC_Port>/awc`
   b. With Microservice: `http://localhost:<AWC_Port>`
2. The AWC login page is displayed.
3. Sign in and verify that the Active Workspace loads successfully.
4. Successful access confirms that AWC is reachable through Haloproxy.

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).

7. Troubleshooting

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

Timeout Error in Haloproxy

Symptom

The following error message is logged.

```
INFO - Request Object--> 000846__ugp_5gt06yo91w79s.prt
INFO - Request Object--> listda_exc_kwx04mk93neia.xlsx
ERROR - java.lang.InterruptedException
ERROR - java.lang.InterruptedException
```

Background

Restarted Tomcat Service

Probable Cause

The most likely cause is to restart the Tomcat Service in the middle of the SOA service operation. Unfortunately, SOA could not stop its tasks from being processed due to which it took to longer time to get the data and ended up with the above error.

Workaround

Restart the Tomcat again and please note not to stop the service while SOA is in operation.

8. Appendix

This section provides supplemental information.

8.1. Supported FMS Configurations

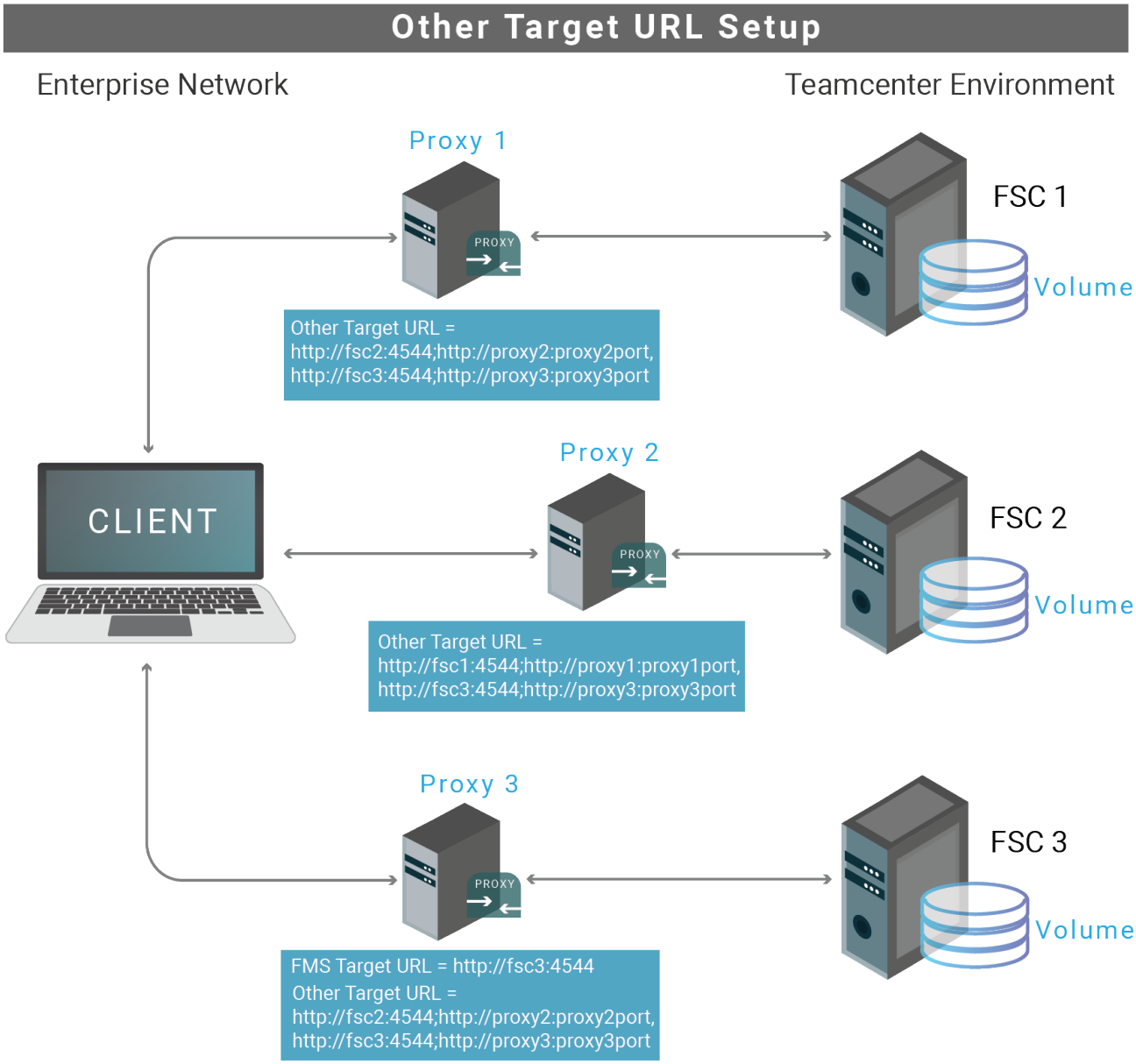
Teamcenter supports various FMS configurations based on the volume of files to be stored, how often files are accessed by clients, and client geographical location (remote).

For illustration purposes, the supported configurations are listed below:

1. **Single FSC**
   a. **With single volume** – Typically for simple deployment. Teamcenter provides a single FSC that mounts a single volume. In this case, enter the URL in the "FMS Target URL".
   b. **With multiple volumes** – A standard small or medium deployment with a large volume of file storage. In this case, each volume will have an entry under this FSC. Here, enter the URL in the "FMS Target URL" field.
   c. A sample of the FMS master file is shown below for illustration purposes:

```
<fscgroup id="mygroup">
<loadbalancer id="ReverseProxy" address="http://SAMPLE.local:8080/tc/fms" />
<fsc id="FSC_SAMPLE_Teamcenter_3" address="http://SAMPLE.local:4544"
ismaster="true">
<volume id="9c1cfc281ec644eabec6" enterpriseid="-1234567890" root="C:\Program
Files\Siemens\volume" priority="0" />
<transientvolume id="v6ca776c74e437d98ef662ecb5751tt" enterpriseid="-1234567890"
root="C:\\Temp\\transientVolume_Teamcenter" />
</fsc>
```

2. **Multiple FSCs with Multiple Volumes** – Numerous files are accessed simultaneously by the clients from more than one FSC or a single file from any one of the configured FSC. For instance, in the below case, a client is configured to connect with more than one FSC. Therefore, you must specify the details in the Other Target URL field.



Other Target URL Setup

A sample of the FMS master file is shown below for illustration purposes:

```
<fscgroup id="mygroup">
<loadbalancer id="ReverseProxy" address="http://PUN-FMS:8080/tc/fms"/>
<fsc id="PUN-FMS_usprd01" address="http://PUN-FMS:4544" ismaster="true">
<volume id="123d0000000f8c9bd0d7" enterpriseid="-1234567890"
 root="E:\Siemens\usprd01_vols\dba_vol1" priority="0" />
<volume id="456a000001388c9bd0d7" enterpriseid="-1234567890"
 root="E:\Siemens\usprd01_vols\lyn_vol1" priority="0" />
<volume id="7898001339268c9bd0d7" enterpriseid="-1234567890"
 root="F:\Siemens\usprd01_vols\dba_vol2" priority="0" />
<volume id="0123001339268c9bd0d7" enterpriseid="-1234567890"
 root="F:\Siemens\usprd01_vols\lyn_vol2" priority="0" />
```

```
<transientvolume id="7f16bd0578697f1eb1bbb4b5020aadef" enterpriseid="-1234567890"
 root="D:\\Temp\\transientVolume_usprd01" priority="0" />
</fsc>
<fsc id="PUN-FMS_YUN_WEB20P_usprd01" address="http://PUN-FMS-WEB:4544"
 ismaster="false">
<transientvolume id="8c425ee7352a4657ac777dc198712cb3" enterpriseid="-1234567890"
 root="D:\\Temp\\transientVolume_usprd01" priority="0" />
</fsc>
<fsc id="PUN-FMS_YUT_usprd01" address="http://PUN-FMS-YUT:4544" ismaster="true">
<volume id="c07e4bfa95a44a0894b0" enterpriseid="-1234567890"
 root="D:\Siemens\usprd01_vols\YUT_vol1" priority="0" />
</fsc>
<fsc id="PUN-FMS_YRT_usprd01" address="http://PUN-FMS-YRT:4544" ismaster="true">
<volume id="9c1cfc281ec644eabec6" enterpriseid="-1234567890"
 root="D:\Siemens\usprd01_vols\YRT_vol1" priority="0" />
</fsc>
<clientmap subnet="127.0.0.1" mask="0.0.0.0">
<assignedfsc fscid="PUN-FMS_YUN_WEB20P_usprd01" priority="0" />
</clientmap>
</fscgroup>
```

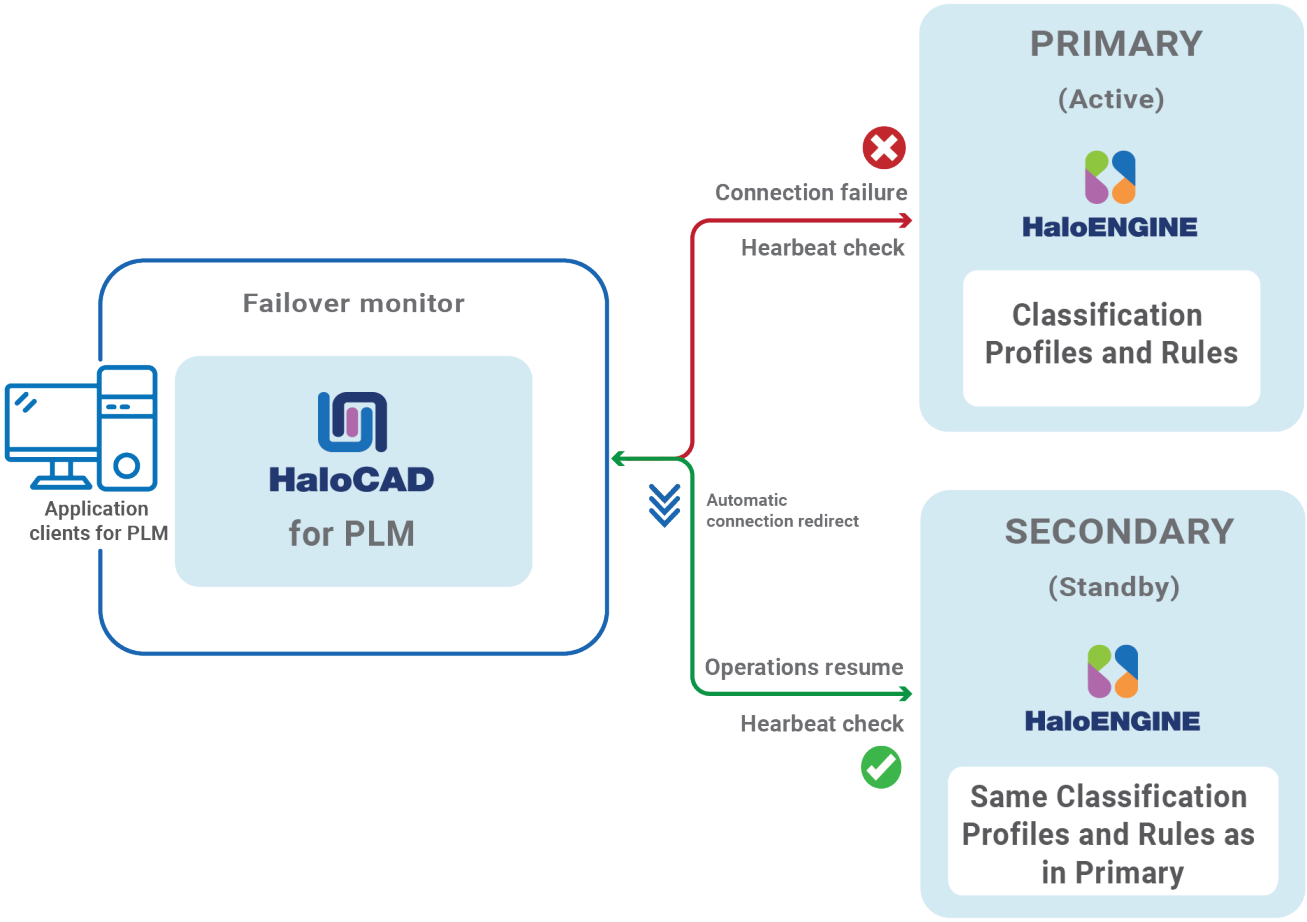
8.2. Failover Mechanism for HaloENGINE in HaloCAD for PLM

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

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

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

is any failure in the secondary HaloENGINE, the primary HaloENGINE will again take over the operations.



Failover Mechanism for HaloENGINE in HaloCAD for PLM

2. **Redundancy**: It provides redundancy, which means there is always another HaloENGINE ready to take over if the primary one fails. This minimizes the possibility of a single point of failure.
3. **Data Integrity and Consistency**: In the event of a failure, the failover technique can help guarantee that data is consistent and file upload/download activities are not lost, which is crucial for systems that rely on high data security.

Failover Mechanism Requirement

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

8.3. Third-Party Libraries

Third-party software/code is included or bundled with Secude's products according to its appropriate license. Secude conducts testing to make sure the third-party products are compatible with and perform as intended with Secude applications.

The third-party libraries and dependencies used by HaloCAD for Teamcenter 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
httpclient	4.5.+	https://mvnrepository.com/artifact/org.apache.httpcomponents/httpclient	http://www.apache.org/licenses/LICENSE-2.0.txt
mail	2.1.1	https://mvnrepository.com/artifact/javax.mail/mail	http://www.sun.com/cddl https://glassfish.java.net/public/CDDL+GPL_1_1.html
commons-io	2.+	https://mvnrepository.com/artifact/commons-io/commons-io	https://www.apache.org/licenses/LICENSE-2.0.txt
javax.servlet-api	5.0.0	https://mvnrepository.com/artifact/javax.servlet/javax.servlet-api	https://glassfish.dev.java.net/nonav/public/CDDL+GPL.html
jna	5.13.0	https://mvnrepository.com/artifact/net.java.dev.jna/jna	http://www.apache.org/licenses/LICENSE-2.0.txt http://www.gnu.org/licenses/licenses.html

Library	Version	Source Code	License Link
jna-platform	5.13.0	https://mvnrepository.com/artifact/net.java.dev.jna/jna-platform	http://www.apache.org/licenses/LICENSE-2.0.txt http://www.gnu.org/licenses/licenses.html
MIP SDK	1.18.103	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

8.4. Metadata Definition

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

Teamcenter metadata	Use
user_role	Derivation from the user role. Multiple roles may be assigned to a single user. (For example, Designer and Engineer)
user_def_group	Derivation from a group of users who log in. (For example, a user from the Engineering group)
gov_clearance	Derivation from a specific object based on value or licensing value. (For example, secret - single value field)
ip_clearance	Derivation from intellectual property (IP) classification values and clearance levels assigned to data objects and users for IP access evaluation. (For example, super-secret - single value field)

Teamcenter metadata	Use
user_name	Derivation from Teamcenter logged-in users. (For example, John and Derek)
file_type	Derivation from file type and Teamcenter object data. (NX file types and MS Office native file types) (For example, prt, asm, and XLSX)
gov_classification	Derivation from a Teamcenter object based on its value or license value. (For example, secret - single value field)
obj_project_names	Derivation from Teamcenter object data. The object could be used in several projects. (For example, project1; project2- multi-value- field)
ip_classification	Derivation from Teamcenter's intellectual property (IP). (For example, secret, internal, and confidential - single value field)
preexpression_custom_pre-expression	Derivation from custom pre-expression. 1. Yes 2. No

Teamcenter metadata

8.5. Download Log Definition

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

8.5.1. What is SIEM Integration?

SIEM, which stands for Security Information and Event Management, is a comprehensive approach to managing an organization's security information and events. SIEM integration refers to the process of incorporating SIEM solutions into an organization's existing IT infrastructure to enhance its ability to monitor, detect, and respond to security incidents. To support this approach, 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

8.5.2. Why CEF Standard?

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

Syslog and CEF Header

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

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

CEF format

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

CEF format sample

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

```
12:39:08.384 CEF:0|Secude|HaloCAD|6.10.1.0|106|user
upload|1|deviceCustomDate1Label=exportTime deviceCustomDate1=Apr 16 2026 07:09:08 UTC
externalId=453FFC46378F471BA774D309DB99AA54 deviceCustomDate2Label=logTime
deviceCustomDate2=Apr 16 2026 07:09:08 UTC
act=unblocked;unlabeled;decrypted;protected_originally
fname=checki_exc_4sv09j4bn7aj7.xlsx
filePath=FMS_SHA256_SIGNATURE=9ab166ff5a71001c22d2fc93c3f19077217f61a9142bc6dc5f90a7d9
0a8c848003c66796365c9623698f7a4db018f61e988cce819a4b66de054217c0d65b6c72;\dba_67fe4f61
\checki_exc_4sv09j4bn7aj7.xlsx fileType=xlsx fsize=49395 in=7693 shost=TC11
duser=infodba,type:TEAMCENTER dst=10.41.14.203 requestClientApplication=[null]
cs2Label=DataDestination cs2=[ platform\=[Unknown], browser\=[FMS-FCC/2406
(bd:20240517) FMS-FCC/2406 (bd:20240517)], browser_version\=[null],
device_type\=[null], terminal_id\=[SVLU0310], destination_attributes\=[{
key\=[client_ip], value\=[10.41.14.203], type\=[null] }, { key\=[client_host],
value\=[SVLU0310], type\=[null] }] ] cs3Label=DataOrigin cs3=[ source_type\=[PLM],
system_name\=[TC11], client_type\=[TEAMCENTER], plm_info\=[{ key\=[file_name],
value\=[checki_exc_4sv09j4bn7aj7.xlsx], type\=[null] }, { key\=[folder_name],
value\=[dba_67fe4f61], type\=[null] }, { key\=[ip_classification], value\=[super-
secret], type\=[null] }]] cs4Label=ClassifyProtectionData cs4=[ error\=[false],
author\=[HaloENGINE Service] ]
```

CEF sample

8.5.3. Why LEEF Standard?

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

Syslog and LEEF Header

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

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

LEEF format

```
12:19:21.901 LEEF:2.0|Secude|HaloCAD|6.10.1.0|106|^|exportTime=Apr 16 2026 06:49:21
UTC^eventName=user upload^externalId=1F26CC928AB54656B8202FEA7948C6EA^logTime=Apr 16
2026 06:49:21
UTC^act=unblocked;unlabeled;decrypted;protected_originally^fname=xlsxte_exc_6j409v0bn7
9m8.xlsx^filePath=FMS_SHA256_SIGNATURE=acb57878d26493703ee825e4dc074b06b8ba66b19873bd2
94f159a26d790ba588dc9e01bd566e2d9c9d626df086c717089c356b81056f1cb89b2107708741d6b;\dba
_67fe4f61\xlsxte_exc_6j409v0bn79m8.xlsx^ftype=xlsx^fsize=49392^fdwnsize=7693^shost=TC1
1^usrName=infodba,type:TEAMCENTER^dst=10.41.14.203^usrAgent=[null]^dataDestination=[
platform=[Unknown], browser=[FMS-FCC/2406 (bd:20240517) FMS-FCC/2406 (bd:20240517)],
browser_version=[null], device_type=[null], terminal_id=[SVLU0310],
destination_attributes=[ {key=[client_ip], value=[10.41.14.203], type=[null]},
{key=[client_host], value=[SVLU0310], type=[null]} ] ]^dataOrigin=[ source_type=[PLM],
system_name=[TC11], client_type=[TEAMCENTER], plm_info=[ {key=[file_name],
value=[xlsxte_exc_6j409v0bn79m8.xlsx], type=[null]}, {key=[folder_name],
value=[dba_67fe4f61], type=[null]}, {key=[ip_classification], value=[super-secret],
type=[null]} ] ]^classifyProtectionData=[ error=[false], author=[HaloENGINE Service] ]
```

LEEF format sample

Format	Description	Example
Syslog Header	The Syslog header contains the timestamp.	`14:37:02.651`
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|6.10.0.0|100|`
	Product version	A string that identifies the version of the software or appliance that sends the event log, for example, `LEEF:2.0|Secude|HaloCAD|6.10.0.0|100|`
	EventID	A unique identifier for an event.

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

8.5.4. Why JSON Standard?

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

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

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

```
12:32:13.101
{"log_id":"334957EF6AE34C51881F2FF9ACC7C87F","product":"HaloCAD","source_host":{"shost
":"TC11"},"protection":{"policy_id":"d7e95033-e7f1-4218-8941-
7d60d8e9cf69","extended_tags":[],"policy_name":"CADSecured","error":false},"destinatio
n_info":{"hostname":"SVLU0310","destination_attributes":[{"value":"10.41.14.203","key"
:"client_ip"},{"value":"SVLU0310","key":"client_host"}],"destination_ip":"10.41.14.203
","os":"Unknown","recipients":[],"browser":"FMS-FCC/2406
(bd:20240517)","device_type":"null","browser_version":"null","user_agent":"null"},"cla
ssification":{"classification_by_system":[],"classification_by_user":[]},"version":"6.
10.1.0","log_time":"Apr 16 2026 07:02:13
UTC","event_id":100,"data_origin":{"generic_info":"null","sap_info":"null","system_nam
e":"TC11","pre_process_info":[],"source_type":"PLM","client_type":"TEAMCENTER","plm_in
fo":[{"value":"NewTestNewTomcat.xlsx","key":"original_file_name"},{"value":"dba_67fe4f
61","key":"folder_name"},{"value":"top-
secret","key":"ip_classification"},{"value":"dba","key":"user_def_group"}],"bi_info":"
null"},"user_info":{"user_email":"HaloENGINE
Service","user_type":"DBA;PartnerContractAdmin","user_name":"infodba"},"file_info":{"f
ile_path":"FMS_SHA256_SIGNATURE=0d60b2bef67b10d74626f7cf651d1c47ac8783189fb14d666b1ff9
78bc278bef37d253fbadc6f8c3da642a813be4a617f946d11ba60e40d32032525465ddaed7;\\dba_67fe4
f61\\testne_exc_1xm031cb4ujq6.xlsx","file_name":"NewTestNewTomcat.xlsx","file_type":"x
lsx","download_file_size":44544,"original_file_size":7693},"action":["unblocked","labe
led","protected"],"export_time":"Apr 16 2026 07:02:12 UTC","event":"user download"}
```


JSON format

8.6. Deactivating the HaloCAD for Teamcenter

For any diagnostic testing purposes in connection with HaloCAD, you may need to deactivate HaloCAD for a while. In such cases, follow the procedure below:

1. **Step 1**. Stop **fsc** service.

   Remove the changes done in FMS master file `fmsmaster_FSC_<ComputerName>_Teamcenter.xml`

   For example,

   ```
   <loadbalancer id="ReverseProxy" address="http://tclu0310.Secude.local:8080/tc/fms/" />
   ```

2. **Step 2**. Remove the changes made in the FCC file.

   a. Go to `<installed_path>\Teamcenter12\tccs\bin>`, and execute **CMD** with administrator privilege.

   b. Type `fccstat.exe -stop` and press **Enter**.

c. Remove the changes on the line in the `fcc.xml` file.

d. FCC Line format: `<parentfsc address="http://:/tc/fms" priority="0" transport="lan"/>` `<assignment address="parentfsc address">`

e. Alternatively, you can use the backup files of these two.

3. **Step 3.** Start **fsc** service.

   a. Type `fccstat.exe -start` and press **Enter**.

   b. Type `fccstat.exe -status` and press **Enter**. You will receive a confirmation message without the Haloproxy port number, which confirms that HaloCAD is not active.

4. **Step 4**. Remove the two **system variables** - **Default_Transient_Server** and **Fms_BootStrap_Urls**.
5. **Step 5**. Restart **Server Manager** from `services.msc`.
6. Complete your investigation and then activate it, as described in the section "TCCS Configuration - Step 2".

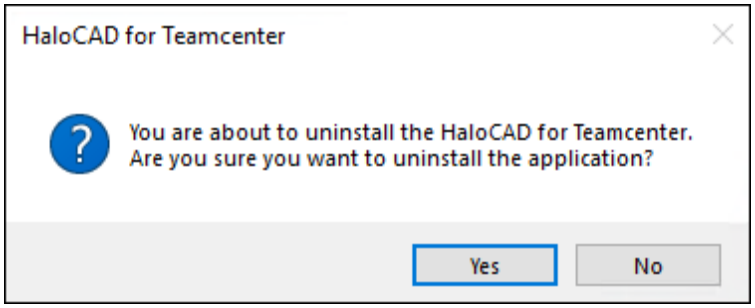
8.7. Uninstalling the HaloCAD for Teamcenter

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

Prerequisite: Make sure to close the configuration tool before performing uninstallation. Otherwise, an error message will appear such as "*Kindly close the running config tool and proceed uninstallation!*"

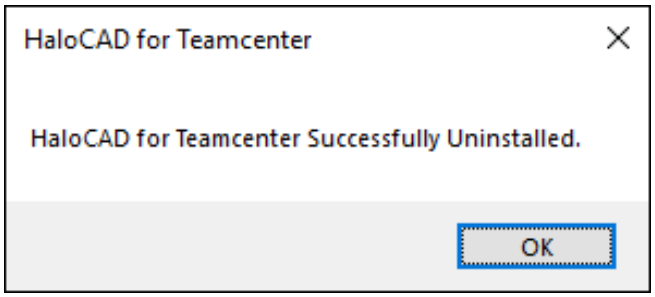
Method #1

1. Click **Start** menu > go to **Control Panel** > **Programs** > **Programs and Features** > **Uninstall a Program** > select **HaloCAD for Teamcenter** application from the list > right-click and select **Uninstall** option or double-click on the installer `HaloCAD_Teamcenter_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. The HaloCAD component has been successfully uninstalled. Click **OK** to close the dialog.
6. The uninstalling process is complete.

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_Teamcenter_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.