Secude

HaloCAD

HaloCAD for Teamcenter 2.5

Installation Manual

Copyright

© 2023-2024 Secude Solutions AG. All Rights Reserved.

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

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

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

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

Contact

Secude Solutions AG

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: `hcsadm.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 Contains detailed information about a topic and are of direct importance to the subject at hand. 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 industries, such as automotive, aviation, high tech, and even fashion, 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. By implementing comprehensive security measures you can significantly reduce the risks and safeguard your data.

1.1. How does HaloCAD Protect your Data?

HaloCAD effortlessly integrates Microsoft Purview Information Protection (MPIP), formerly known as Microsoft Information Protection (MIP), the leading technology for Enterprise Digital Rights Management (EDRM). It acts as a shield for your CAD files by automatically labeling them with MPIP and manages data assets across your environment.

It offers access to MPIP-protected files, including label handling and privilege enforcement. CAD users will not notice any differences in the handling of CAD files because they take place in the background. By seamlessly attaching MPIP labels to the CAD files while they are being created, it provides end-to-end security for those files.

1.2. What is HaloCAD for PLM?

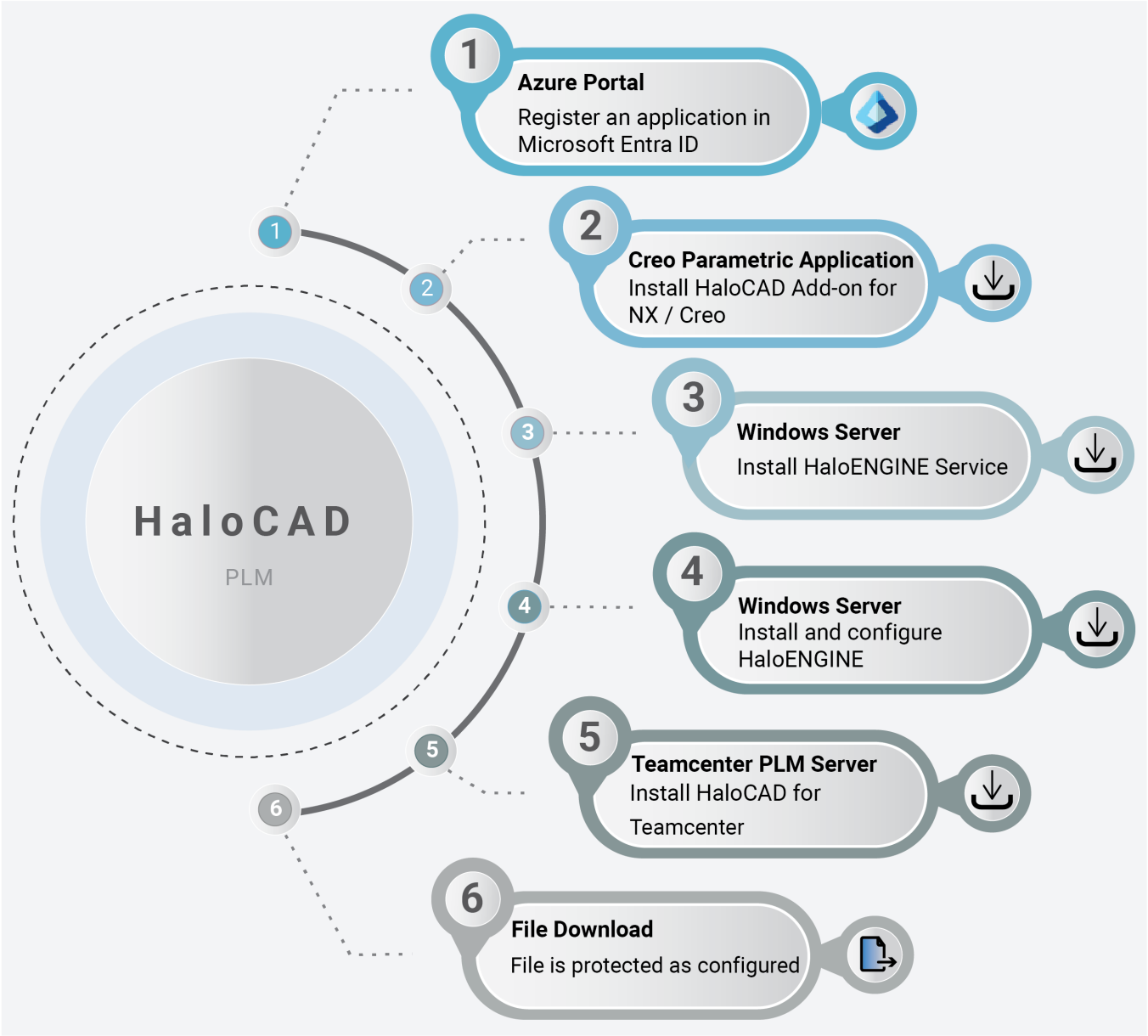
The HaloCAD for PLM solution integrates with the respective PLM application and includes the functionality of HaloCAD PROTECT and HaloCAD MONITOR. Files are automatically protected during the access/download or check-out process and are stored unprotected back into the PLM Vault during the upload/check-in process.

1.3. About this Manual

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

2. Quick Start Installation Summary

The following image shows the high-level idea of setting up HaloCAD.



HaloCAD quick start installation steps with PLM

Reference Manuals

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

Component	Refer to
Step 1 – How to register an application in Entra ID.	`HaloCAD_Technical_Reference_Manual_EN_Online.pdf`

Component	Refer to
Step 2 – How to install HaloCAD Add-on for NX/Creo.	1. `HaloCAD_NX_Manual_Installation_EN_Online.pdf` 2. `HaloCAD_Creo_Manual_Installation_EN_Online.pdf`
Step 3 – How to install HaloENGINE.	`HaloENGINE_Manual_Installation_EN_Online.pdf`
Step 4 – How to install HaloENGINE Service.	`HaloENGINE_Manual_Installation_EN_Online.pdf`
Step 5 – How to install HaloCAD for Teamcenter.	Refer to the current manual.
Step 6 – How to download a protected file.	`HaloCAD_Teamcenter_Manual_Operations_EN_Online.pdf`

HaloCAD documentation

3. HaloCAD Architecture

HaloCAD is available in three variants:

HaloCAD Add-on for CAD—A standalone solution that contains the HaloCAD PROTECT feature. It enables CAD applications to use MPIP directly with user interaction.

HaloCAD for PLM—This solution includes HaloCAD PROTECT and MONITOR capabilities and interacts with the respective PLM application. HaloCAD for Teamcenter actively monitors file access, upload, and download events while running in the background. During a file upload, HaloCAD examines to see if the file is already encrypted, and if so, it decrypts and then allows the file to get check-in to the PLM Vault. In the event of a file access/download, the selected file is automatically protected. HaloCAD operates independently throughout the check-in and check-out process in accordance with the rules stated in the Classification Engine. Please note that currently, Teamcenter PLM protects NX, Creo, MS Office, and PDF files.

Supported PLM Multi-CAD Integrations:

1. HaloCAD for Teamcenter—Siemens NX Integration
2. HaloCAD for Teamcenter—PTC Creo Integration

HaloCAD Extension—HaloCAD extends its support to read the MPIP-protected files through a free-of-charge standalone HaloCAD Reader Add-on.

Components of HaloCAD

The following section explains about components of HaloCAD.

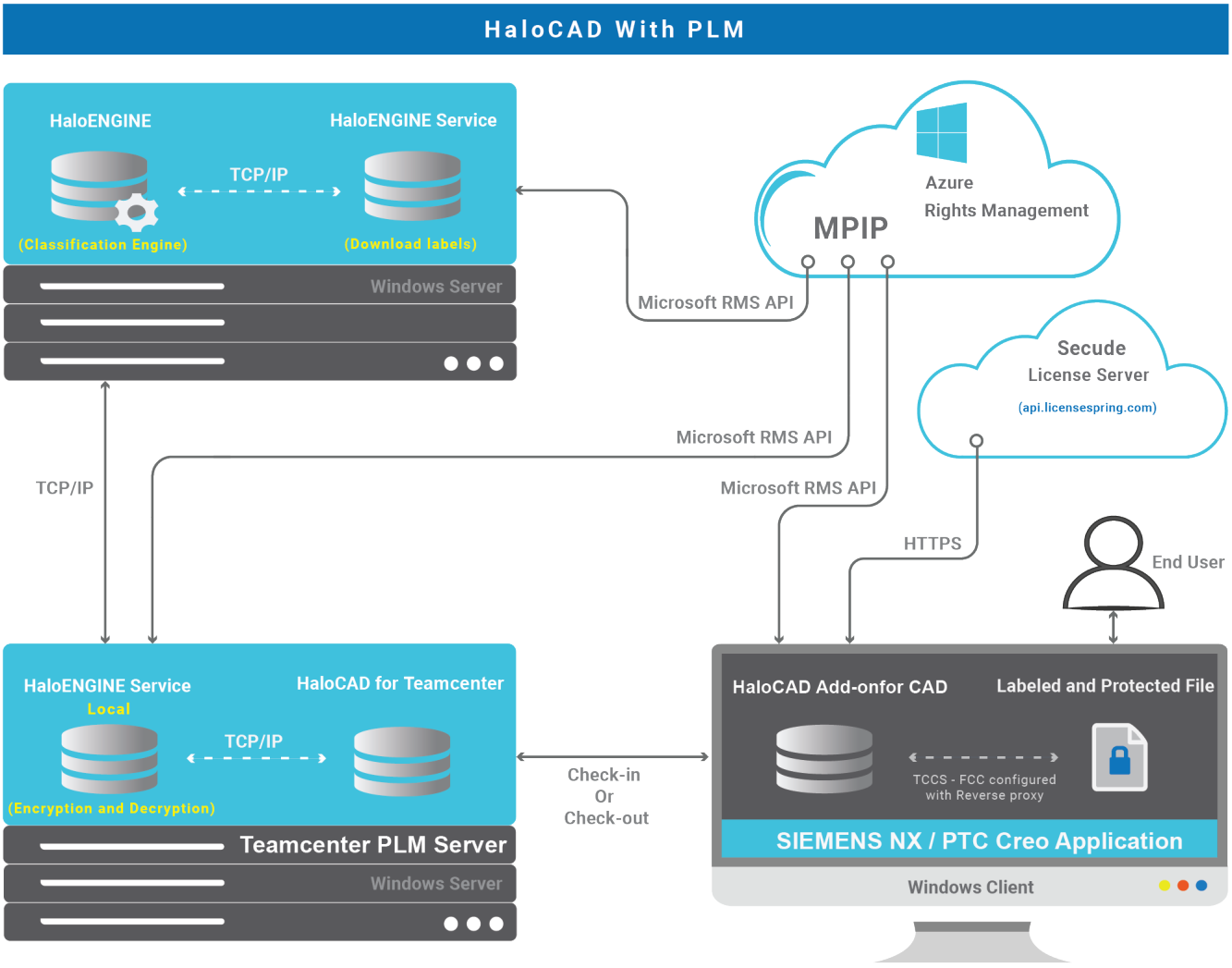
1. HaloCAD for Teamcenter—a proxy component that contains the functionality of HaloCAD PROTECT and MONITOR.
2. HaloCAD Add-on for CAD—reads the protected files, enforces corresponding privileges, and changes MPIP labels.
3. HaloENGINE—Significant role where business logic is located.
4. HaloENGINE Service —Serves file processing (encryption and decryption). Based on the PLM configuration (Local mode or Remote mode), the place of file processing differs.
   a. With **Local** mode, HaloENGINE Service and HaloCAD for Teamcenter should be installed on the same server machine, or these two components can be installed on the same server machine where Teamcenter PLM is installed. For file encryption and decryption, HaloCAD for Teamcenter interacts with the HaloENGINE Service.
   Whereas the HaloENGINE and a second HaloENGINE Service must be configured on another server machine, and this second HaloENGINE Service is primarily responsible for downloading

labels from Azure RMS.

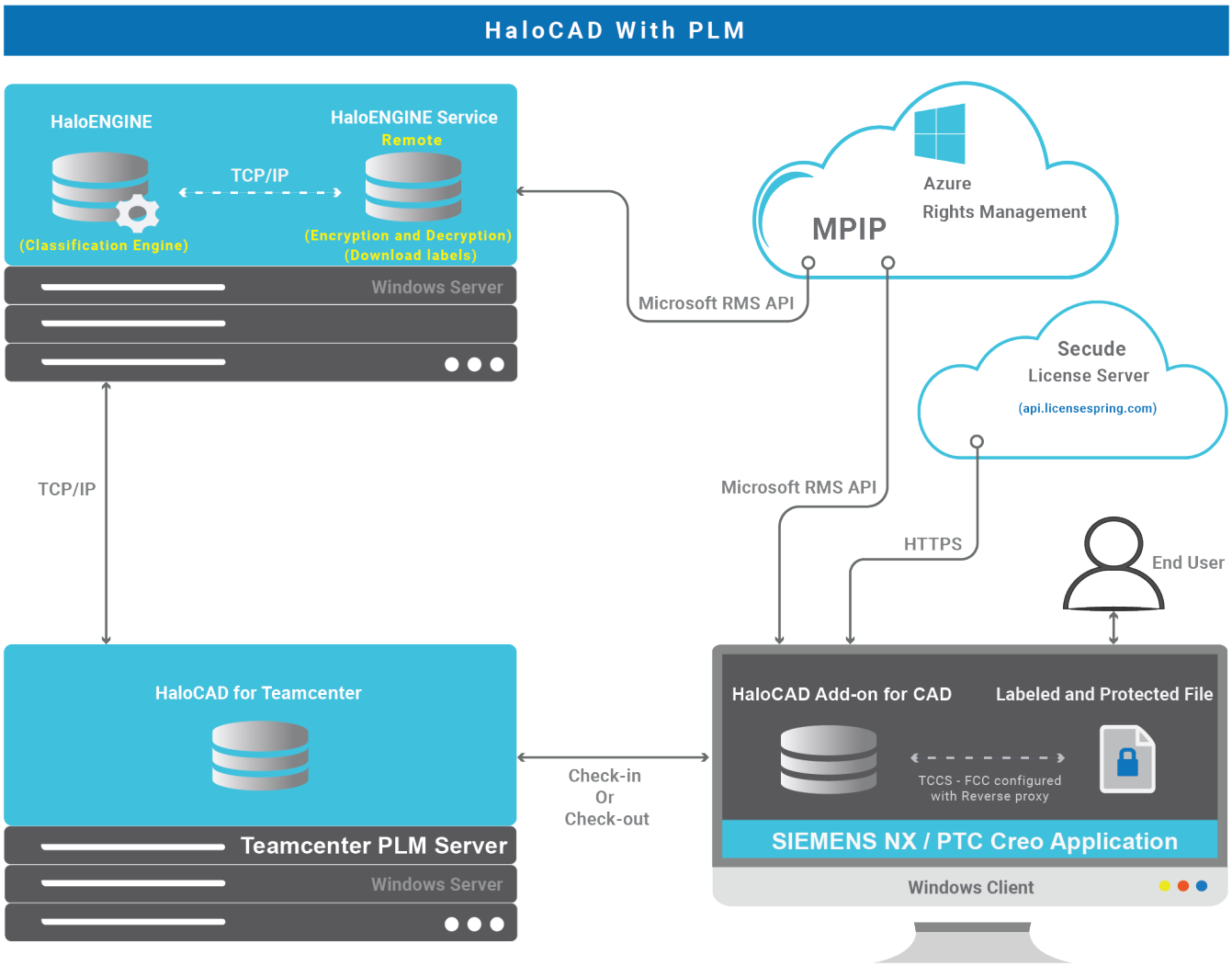
b. With **Remote** mode, HaloCAD for Teamcenter is installed on a separate server machine and communicates with the HaloENGINE to get the file encrypted/decrypted by the HaloENGINE Service, which is installed locally on the HaloENGINE installed machine.

c. During a file check-in/check-out action, the HaloCAD for Teamcenter add-on actively listens to the request and collects the metadata, and sends it to the HaloENGINE for label derivation. The file, along with the derived information, is then passed to the local HaloENGINE Service or HaloENGINE (to remote HaloENGINE Service) for file processing (encryption/decryption).

d. The only difference between local mode and remote mode is where encryption/decryption occurs.



HaloCAD with PLM (Local)



HaloCAD with PLM (Remote)

HaloCAD Add-on for NX and **HaloCAD Add-on for Creo** perform the following functions:

1. **HaloCAD Add-on for NX** - Resides in Siemens NX application.
2. **HaloCAD Add-on for Creo** - Resides in Creo application.
3. Responsible for receiving the protected file from Teamcenter and displaying the label with permission enforcement.
4. Responsible for forwarding the encrypted file stream (if labeled) to HaloCAD for Teamcenter.
5. Responsible for logging the add-on-related activities.

HaloCAD for Teamcenter performs the following functions:

1. Resides in Siemens Teamcenter PLM Server (as shown in the image above).
2. Responsible for listening to check-in and check-out actions via AWC browser / RAC session /other clients (MS Office, Creo, and NX).

3. Remote mode: Responsible for the collection of metadata and label information from the HaloENGINE and then sending the file via the HaloENGINE to the (remote) HaloENGINE Service for file processing.
4. Local mode: Responsible for the collection of metadata and label information from the HaloENGINE and then forwarding the file directly to the (local) HaloENGINE Service for file processing either in “File path” or “Stream”.
5. Responsible for receiving the encrypted file via the HaloENGINE (in remote mode) and from the HaloENGINE Service (in local mode) during the check-out process.
6. Responsible for logging HaloCAD component activities to the local log and also for sending audit logs to the HaloENGINE.

HaloENGINE performs the following functions:

HaloENGINE is a Java-based server component that exposes a web service to HaloCAD for Teamcenter.

1. Responsible for business logic. The HaloENGINE (classification engine) interprets the metadata collected in Teamcenter PLM and makes all decisions. The action derivation is based on the rules generated with metadata, which are captured during a file download.
2. Responsible for forwarding the file stream to the HaloENGINE Service for encryption (in Remote mode) during check-out action.
3. Responsible for forwarding the file stream to the HaloENGINE Service for decryption in remote mode if the file is already protected during the check-in process.
4. Responsible for logging events sent by HaloCAD for Teamcenter.

HaloENGINE Service performs the following functions:

HaloENGINE Service, a Windows service, is responsible for communicating with HaloENGINE via TCP/IP. It is the only component that directly communicates with the Azure Right Management Service (Azure RMS).

1. Responsible for fetching the MPIP labels.
2. Responsible for protecting the file that the HaloENGINE or Proxy (in local mode) sends to it, based on the defined MPIP label.
3. Responsible for decrypting a protected file while uploading.

Microsoft Purview Information Protection

HaloCAD solution effortlessly integrates Microsoft Purview Information Protection 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.

4. Installing the HaloCAD for Teamcenter

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

4.1. 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.

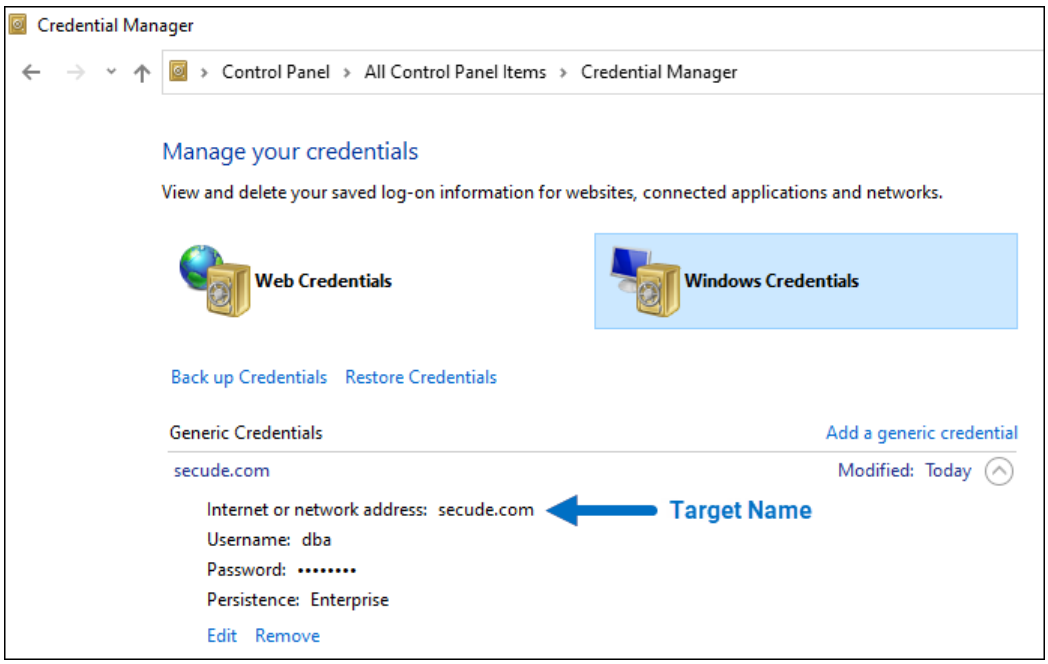
Components	Details
Supported Operating System	Windows Server 2016 and above
Supported Teamcenter versions	1. Teamcenter 13.x, 14.x 2. Teamcenter 2312
Supported file types	1. NX file types 2. Creo file types 3. PDF 4. MS Office native file types
Other components	HaloENGINE and HaloENGINE Service

Requirements

4.2. Prerequisites

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

1. Make sure you have administrative access before performing the most of system and dataset tasks.
2. Make sure the client computer running the HaloCAD Add-on for NX or the HaloCAD Add-on for Creo can connect to the Teamcenter Server.
3. Make sure your HaloENGINE complies with the requirements listed below:
   a. License file (enabled with TEAMCENTER system type).
   b. Proper action rules
   c. Client certificate (`.JKS`)
4. Make sure that the following **system variables** are set:
   a. **Default_Transient_Server** – The default transient file server location.
      - `Default_Transient_Server=http://<host>:<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>:<port>/tc/fms`
      - For example, `Fms_BootStrap_Urls=http://tclu0310.secude.local:8080/tc/fms`
5. Make sure to have an entry in **Credential Manager** which will be used during the HaloCAD component configuration. To do so, go to **Control Panel** > **User Accounts** > **Credential Manager** > **Manage Windows Credentials** > **Add a Generic Credential**, enter all the required details, and save the entry.
6. The credentials are stored in **Windows Vault**. The following figure shows a sample entry for the Credential Manager.



Entry in Credential Manager

7. Make sure to log in to Teamcenter using the service user in client SOA (which is added in **Credential Manager**), and we recommend that the user is assigned with “read” permission.
8. If you want to implement a failover mechanism in HaloENGINE, please refer to the section “Failover Mechanism for HaloENGINE in HaloCAD for PLM”.

4.3. Installation Modes

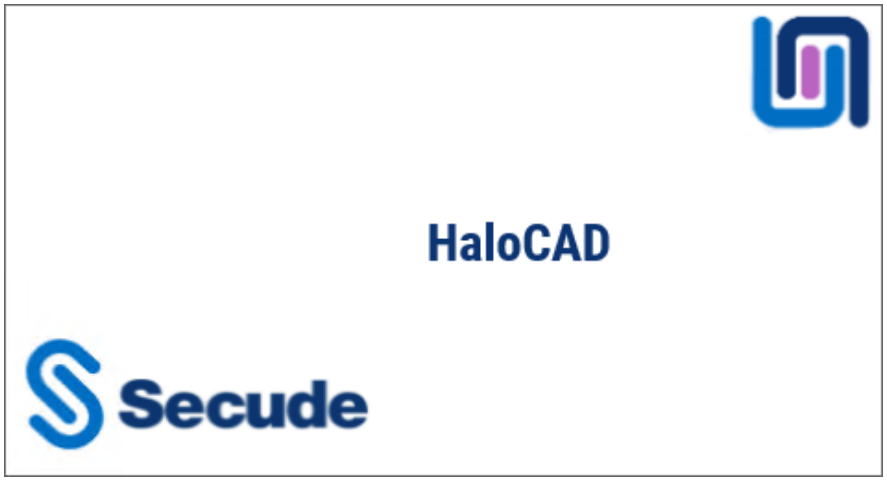
You can install the HaloCAD component in the following modes:

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.

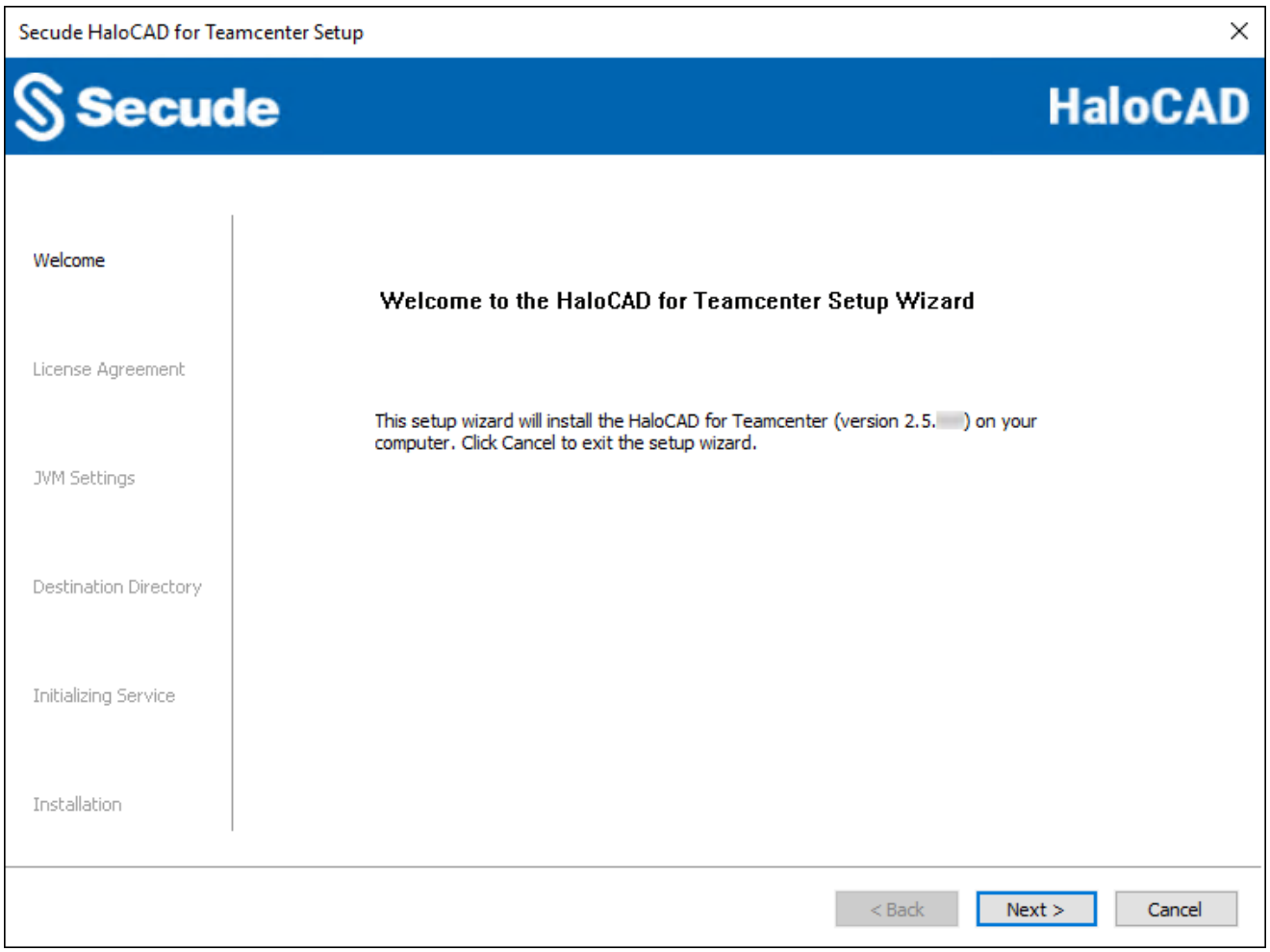
4.3.1. Graphical Mode

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, you will see the startup dialog followed by the welcome dialog:

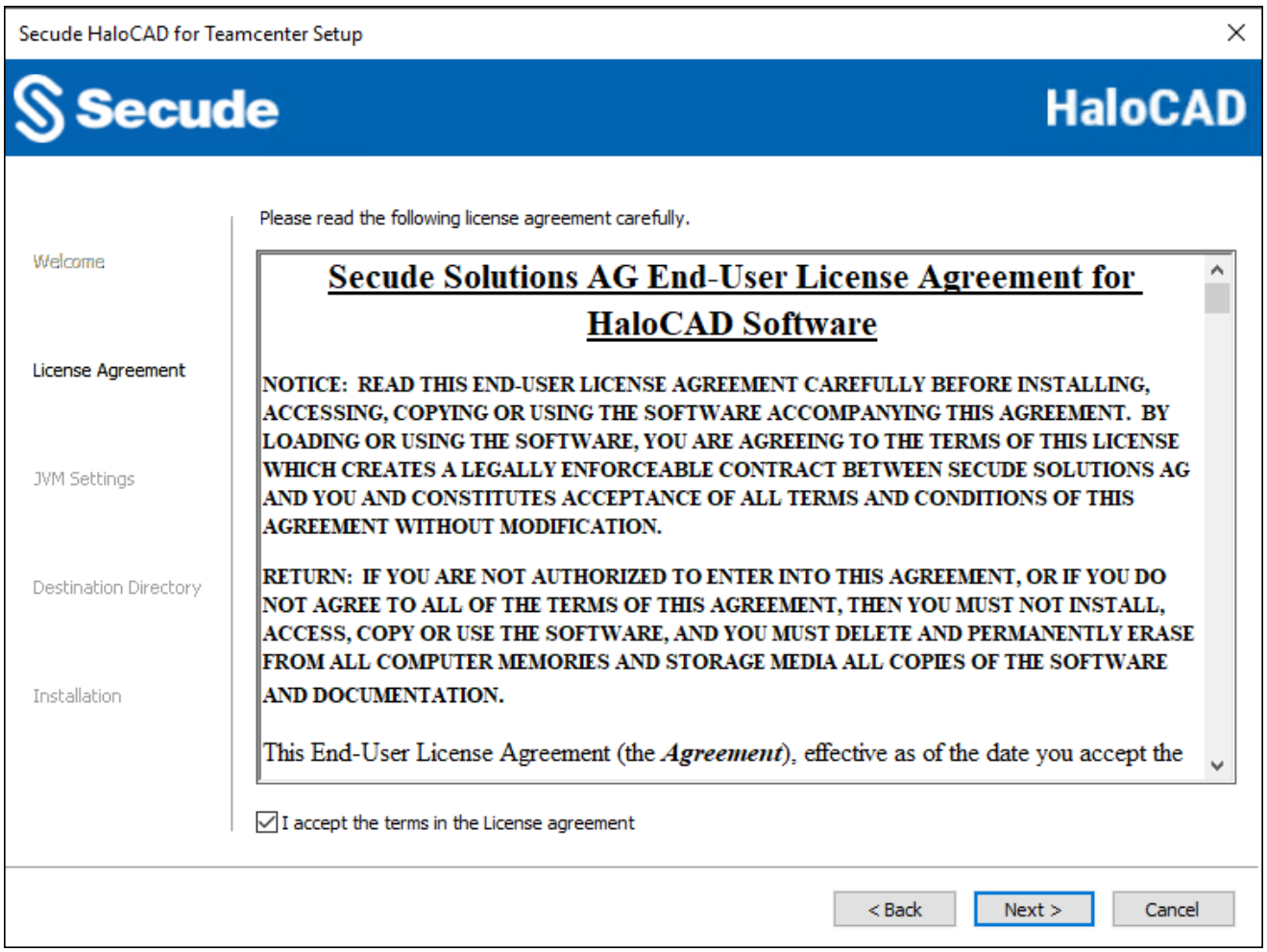


Startup Dialog



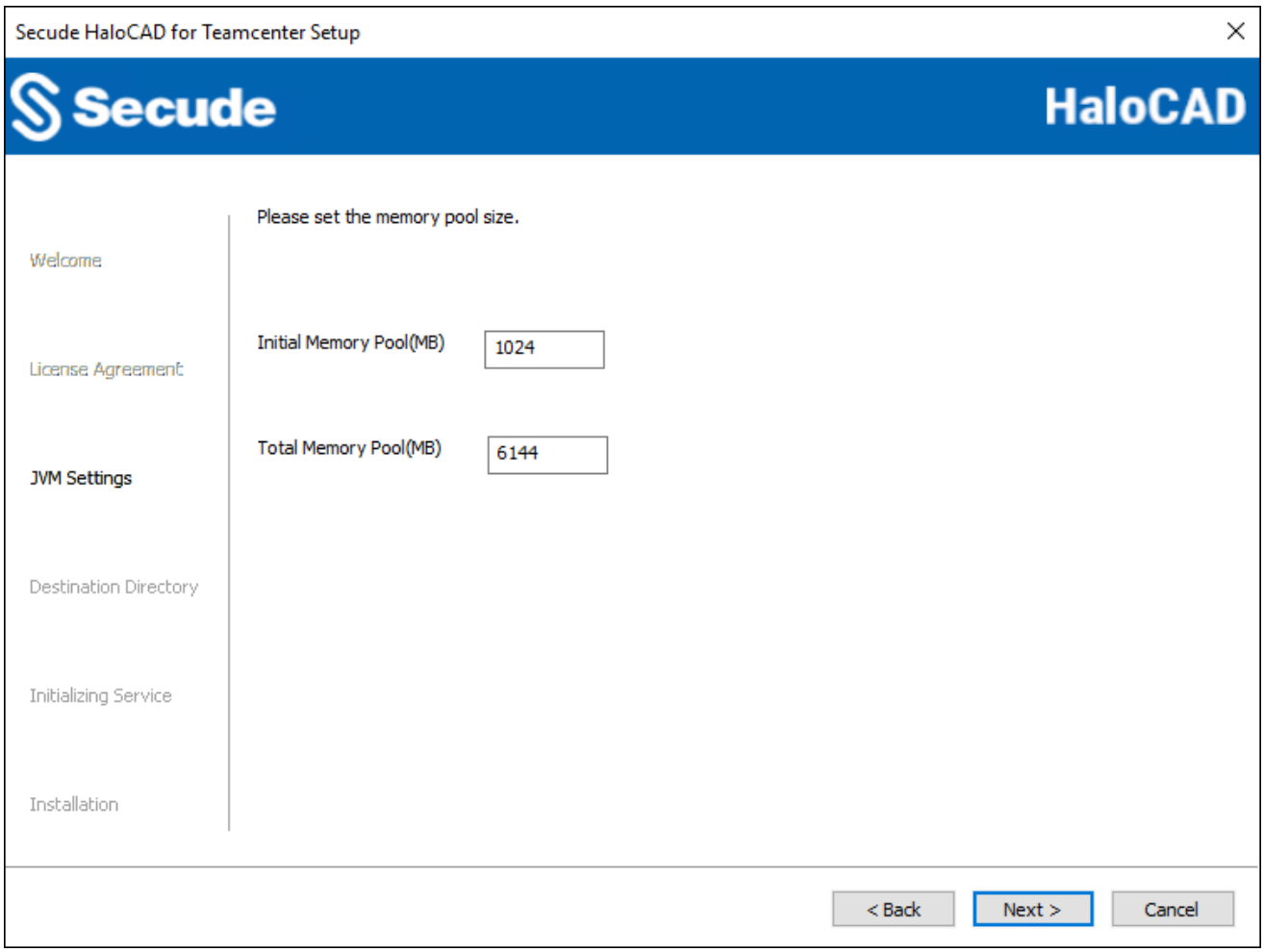
Welcome Dialog

4. Click **Next** to continue the installation.
5. The end-user license agreement dialog will appear:



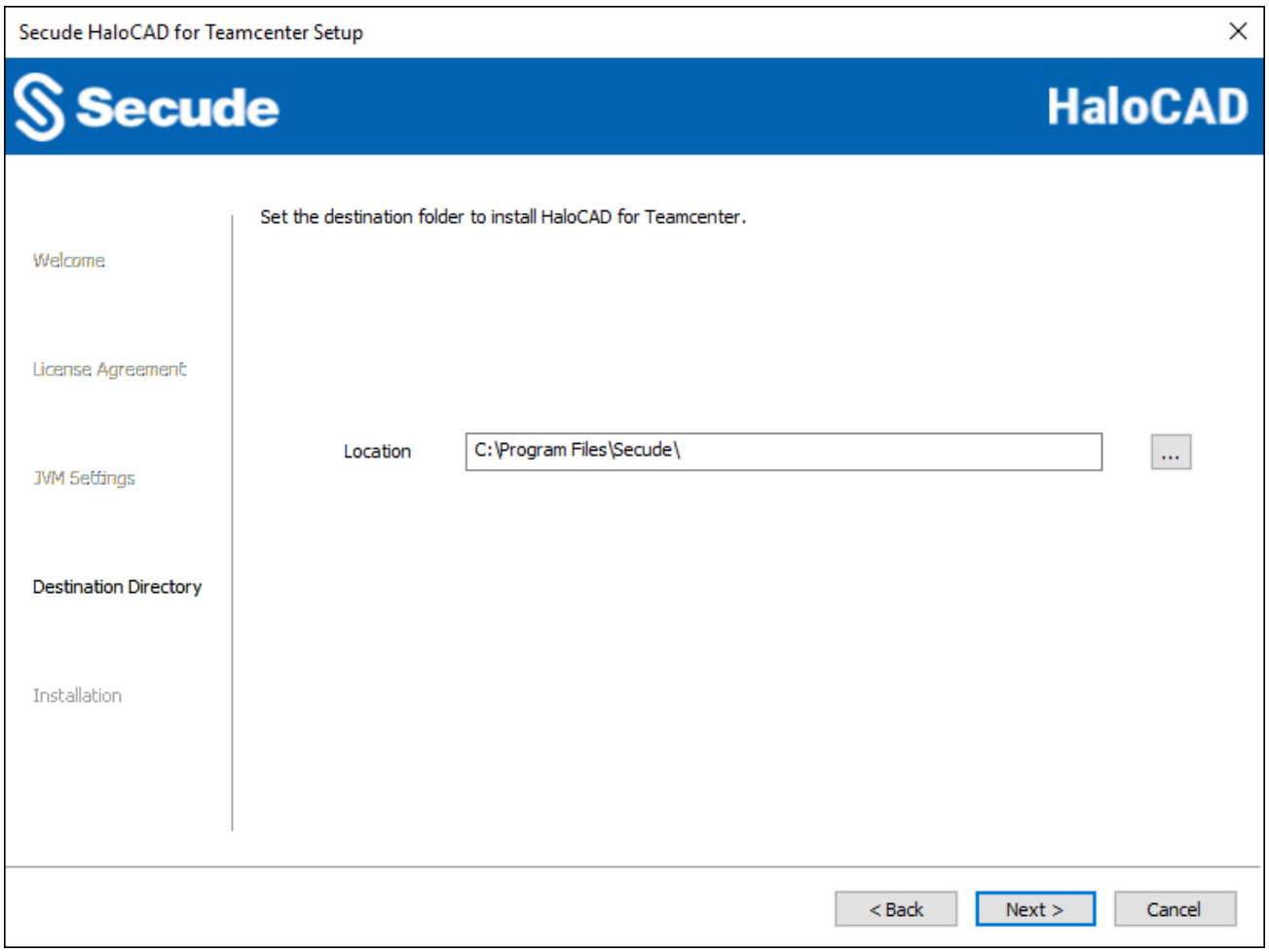
End-User License Agreement Dialog

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



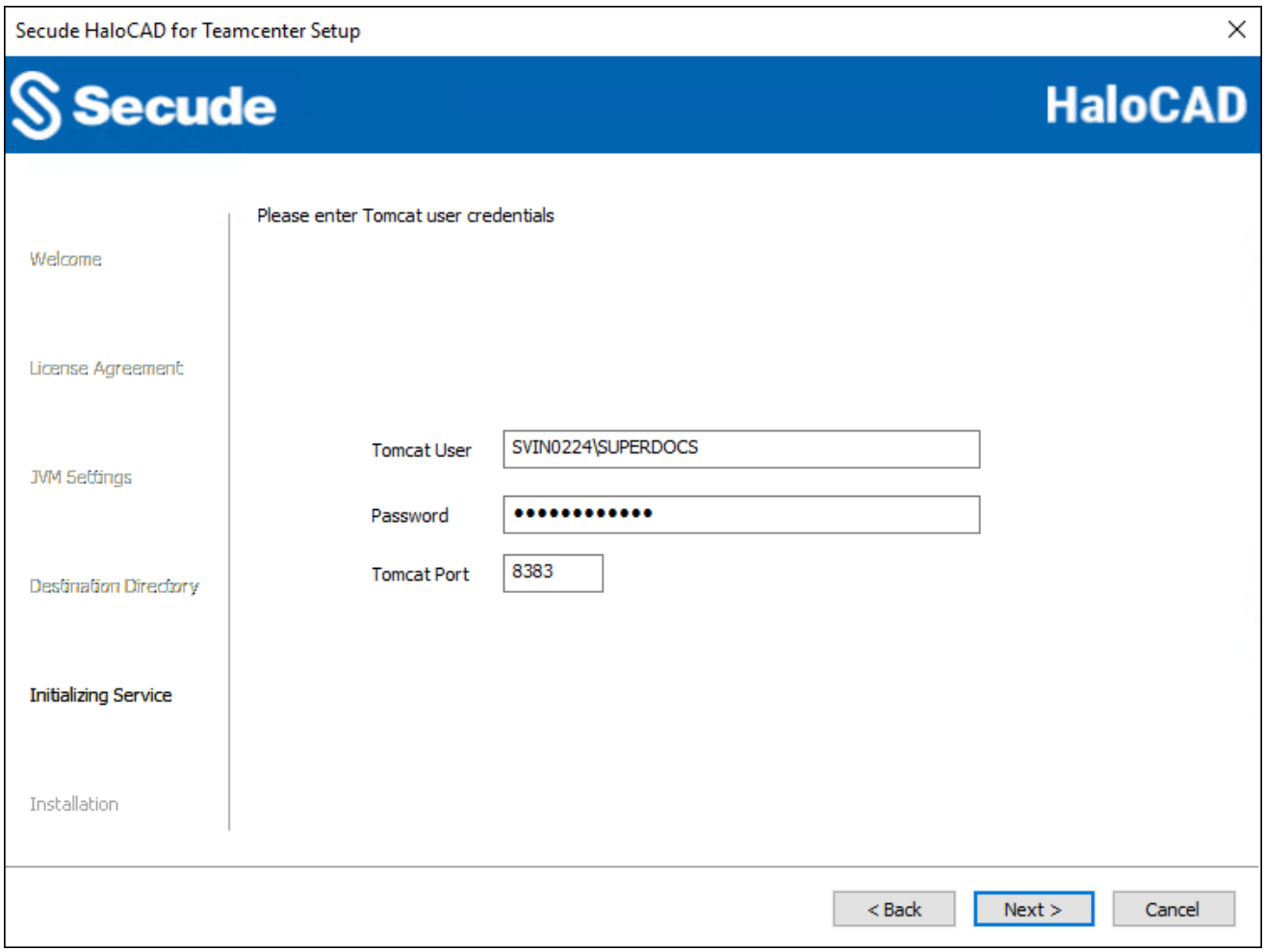
Tomcat pool size configuration dialog

8. Enter the amount of memory you want to allocate to change the preset values for the **Initial Memory Pool** and **Total Memory Pool**. Note: Ensure that the Total Memory Pool does not exceed the System's available 3/4th RAM.
9. Click **Next**. The destination folder selection dialog will appear:



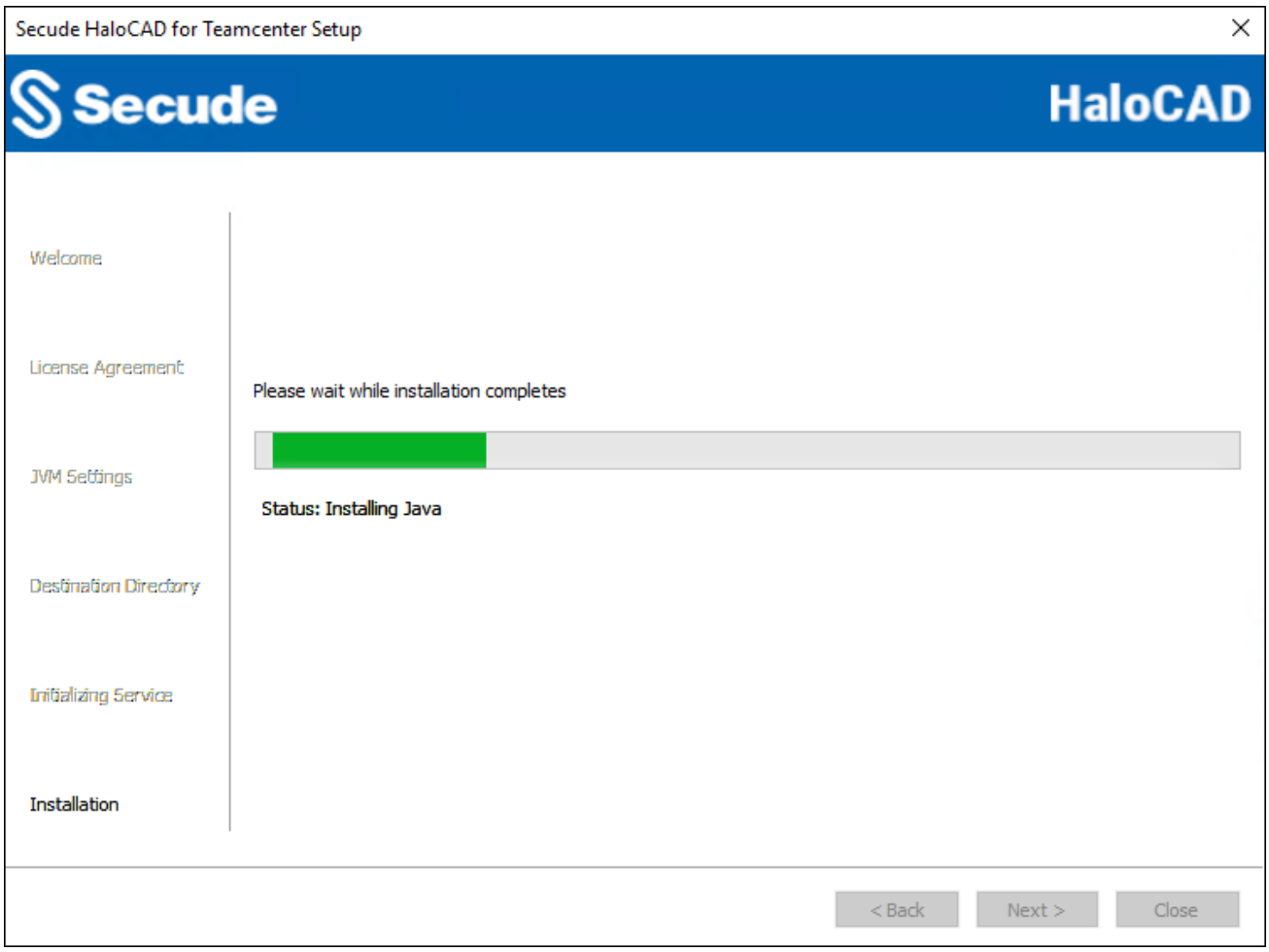
Destination folder selection dialog

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. Note: If HaloENGINE Service and/or HaloENGINE are already installed, you cannot change the destination folder. The browse button becomes disabled. Click **Next** to allow the Setup program to install the HaloCAD component.
11. To return to any point in the installation process, click the **Back** button (optional).
12. The Tomcat user credential dialog will appear:



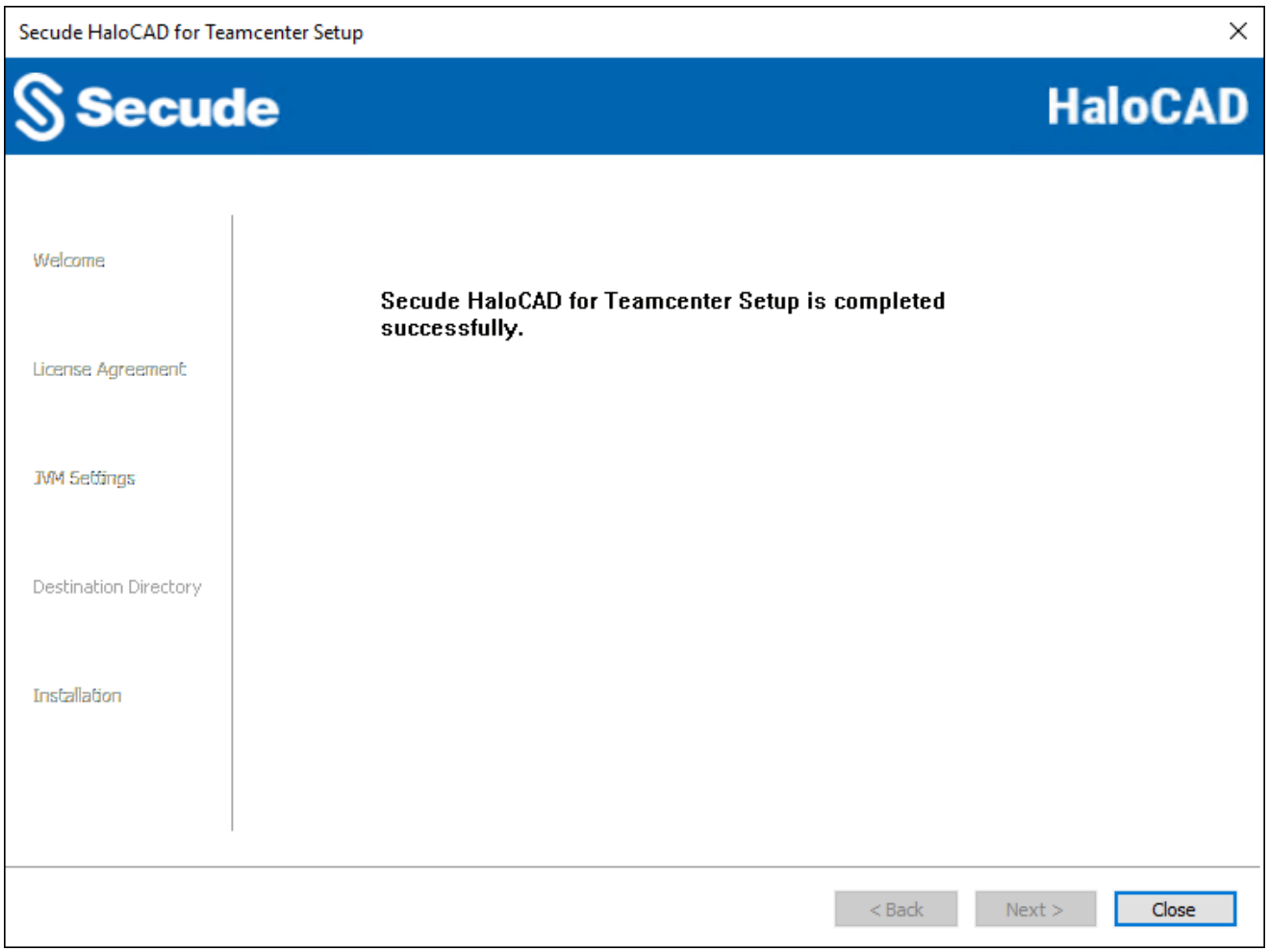
Tomcat user credential dialog

13. To configure the Tomcat service, enter the following details:
    a. If the computer is connected to a domain you need to enter a domain name first followed by the user name and password in the **Tomcat User** text box. For example, `[Domain Name]\[User]`, `SECUDE.TC\Admin`.
    b. On a non-domain joined computer, you need to enter the machine name first followed by the user name and password in the **Tomcat User** text box. For example, `[Machine Name]\[User]`, `SECUDEdesk\Admin`.
    c. **Tomcat Port**: The default port is 8383. You can, however, change the port number; it must be greater than 999 and less than or equal to 65535.
14. The installation begins and progress is shown in the dialog.



Installation progress dialog

15. When the installation is completed, you will see a message confirming that the HaloCAD component has been successfully installed.



Installation completed dialog

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

Post-Installation files:

The following files and directories can be found in both the default and user-specified installation locations:

1. Configuration Tool—`C:\Program Files\Secude\HaloCADTeamcenter\config\halocad-teamcenter-config-<version>.jar`. This tool is explained in the next section "Configuring the HaloCAD Proxy".
2. Java-related files—`C:\Program Files\Secude\secude-jre`
3. Tomcat Related files—`C:\Program Files\Secude\Tomcat`
4. Log file—`C:\Program Files\Secude\Tomcat\logs\haloproxy.log`

4.3.2. 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 -help
   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> -username <keep-empty-quotes> -password <user-domain-password>
   HaloCAD_Teamcenter_Setup.exe -uninstall
   ```
4. The following command illustrates how to install the HaloCAD component.

   ```
   HaloCAD_Teamcenter_Setup.exe -install -initmempool 1024 -totalmempool 2048 -dir
   "C:\Program Files\Secude" -port 8383 -username "" -password "Sample@123"
   ```
5. Press `Enter`.
6. The installation is complete.

5. 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.

5.1. Configuration Using Tool (GUI)

Step 1. Stop the Tomcat Service.

Use `services.msc` to stop the service.

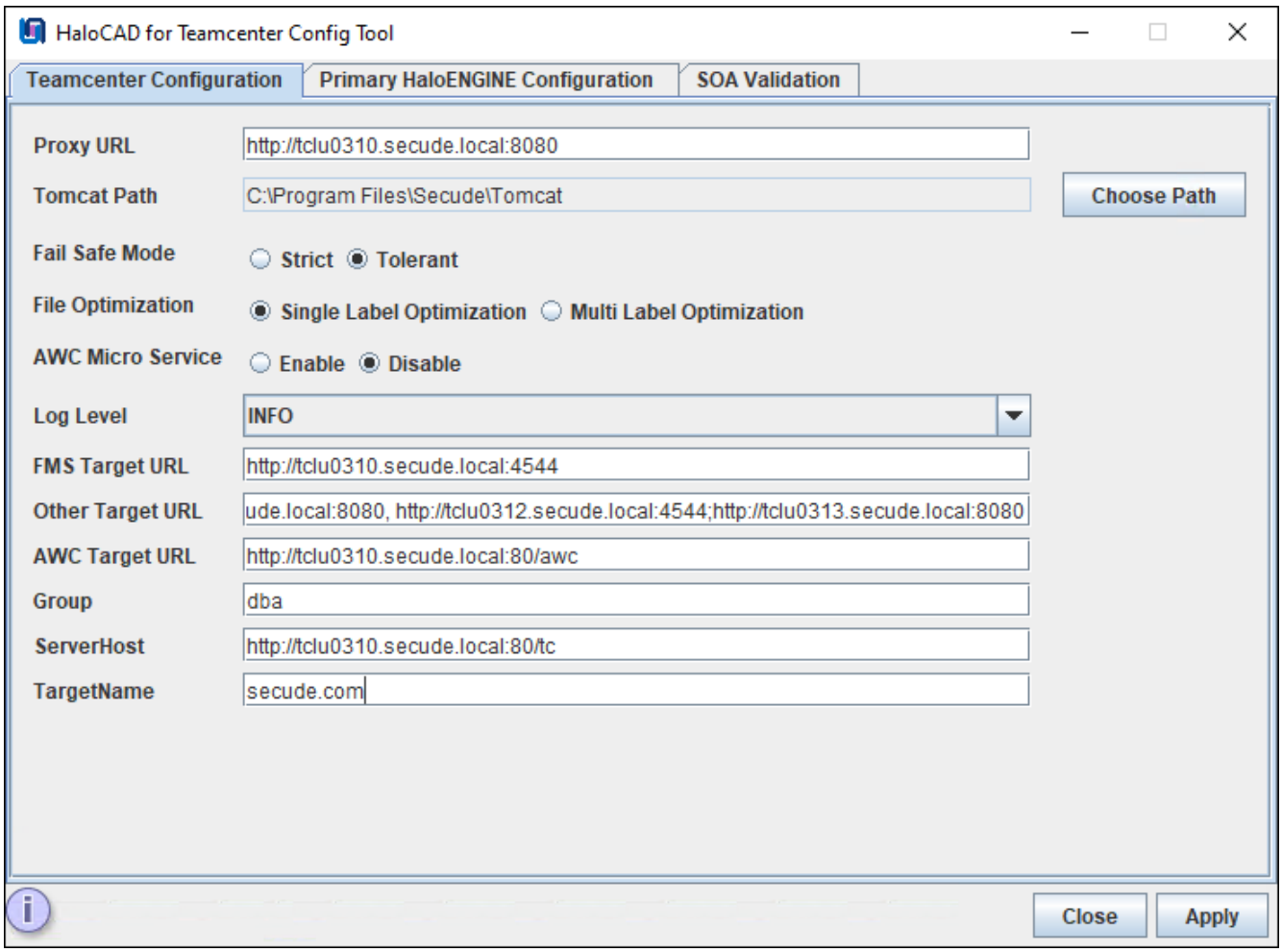
Step 2. Run the HaloCAD Config tool.

1. Go to the default installation directory `C:\Program Files\Secude\HaloCADTeamcenter\config`.
2. Double-click on the `halocad-teamcenter-config-<version>.jar` file or run the jar file in a **Command Prompt** using administrator privileges. In the latter case, you must type the following command and press **Enter**.

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

   For example: `java -jar C:\Program Files\Secude\HaloCADTeamcenter\config\halocad-teamcenter-config-<version>.jar`
3. The *HaloCAD for Teamcenter Config Tool* window will appear.

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



Teamcenter Configuration tab

1. **Proxy URL**: Enter the URL where the proxy (HaloCAD component) is installed. For example, `http://tclu0310.secude.local:8080`
2. **Tomcat Path**: Click **Choose Path** to browse and select the path of the **Tomcat** home directory. 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 taken into account and applied to all dependent files.

b. **Multi-Label Optimization:** Each file type group label defined in the classification engine is taken into account and assigned to the appropriate group with 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 = 8080 you may use a different port for AWC Proxy Port 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 as per 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. **TargetName**: Enter the network address that is added in the **Credential Manager** as TargetName. For example, `secude.com`.
12. Click **Apply**. Any missing values will be indicated with a red tool tip message. This indicates that you need to enter and click **Apply**.

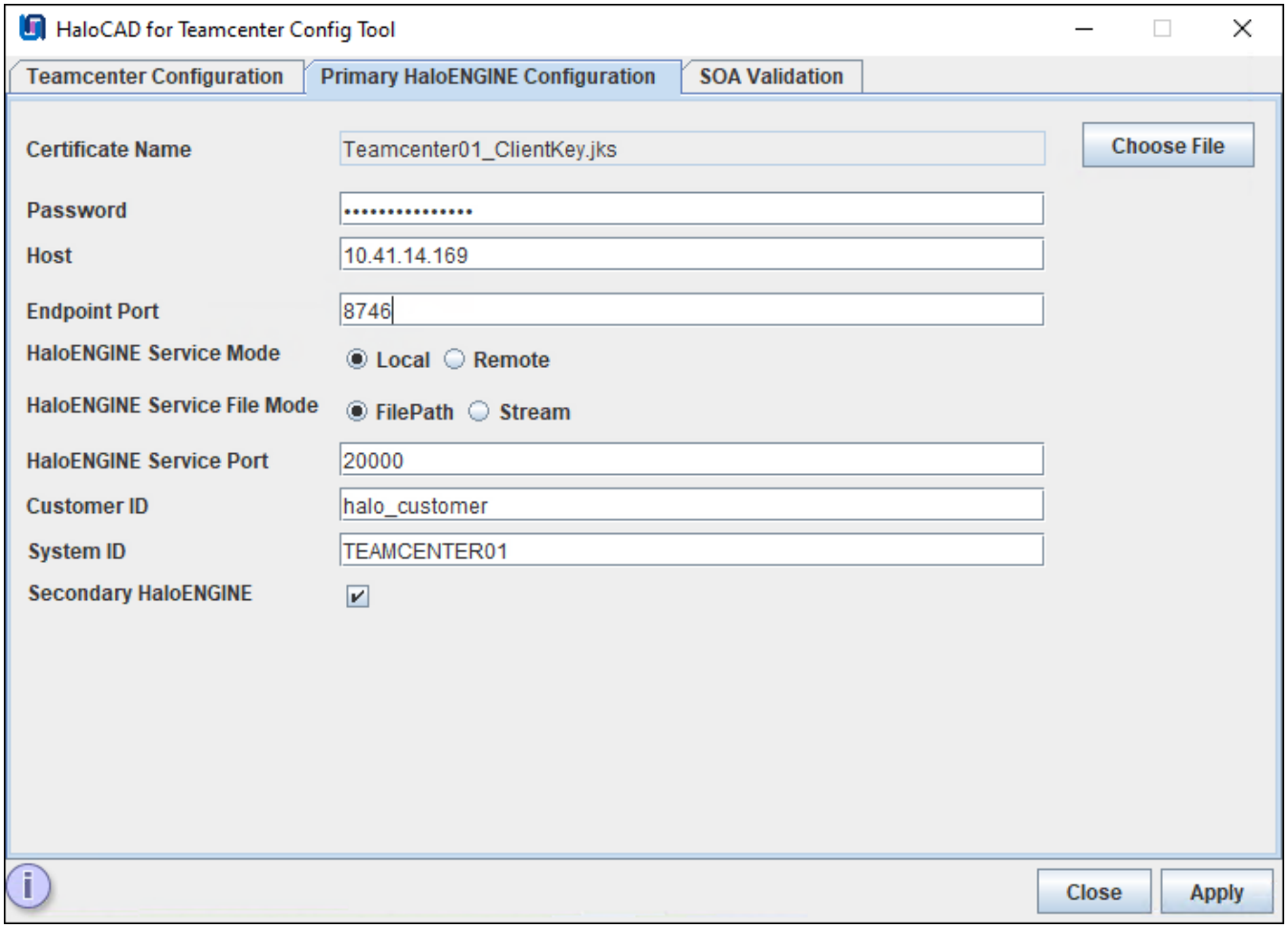
    Results:

    a. A progress bar indicates that "*Restarting Tomcat Service*" is being performed.

    b. A confirmation message dialog box will appear.

    c. Click **OK** on the confirmation 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, generated by the HaloENGINE Admin Portal (through which communication is established between primary HaloENGINE and Teamcenter). For example, `Teamcenter01_ClientKey.jks`

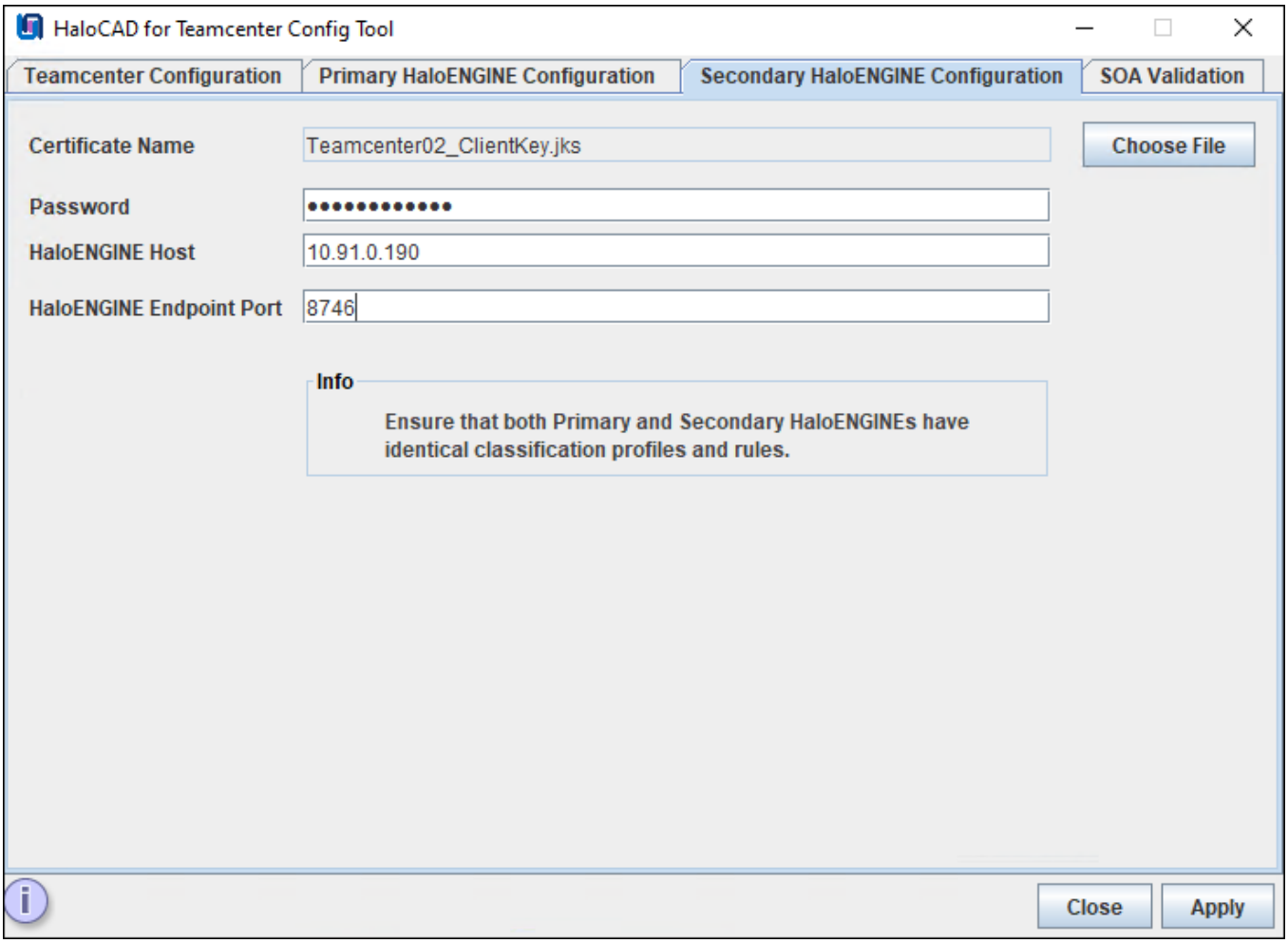
2. **Password**: Enter the password of the selected client Keystore. For example, `ckpass`
3. **Host**: Enter the IP address/FQDN of HaloENGINE. For example, `10.41.14.169`
4. **Endpoint Port**: Enter the Endpoint Port where the service is accessed by this client application. For example, `8746`
5. **HaloENGINE Service Mode**: Select the location where the HaloENGINE Service is installed.
   a. **Local (default)**: Select if HaloENGINE Service and HaloCAD for Teamcenter are installed on the same machine on which Teamcenter PLM is installed. If you choose **Local**, you must select the file transmission method in the **HaloENGINE Service File Mode** (**Filepath** / **Stream**) and then enter the port number in the **HaloENGINE Service Port** text box.
   b. **FilePath (default)**: File stored in a local temporary location for encryption and decryption process. Here, file path information is used for transferring.
   c. **Stream**: File as a sequence of bytes.
   d. **HaloENGINE Service Port**: Enter the port assigned to the HaloENGINE Service during the installation. By default, HaloENGINE Service uses port `20000`.
   e. **Remote**: Select if HaloENGINE Service and HaloCAD for Teamcenter are installed on different machines.
6. **Customer ID**: Enter the **Customer ID** that is assigned for Single Customer mode or Multi-Customer mode 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".
9. Click **Apply**. Any missing values will be indicated with a red tool tip message. This indicates that you need to enter and click **Apply**.

   Results:
   a. A progress bar indicates that "*Restarting Tomcat Service*" is being performed.
   b. A confirmation message dialog box will appear.
   c. Click **OK** on the confirmation dialog box.
   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 below in Step 2c.

Step 2c. Check the connection status on the *Secondary HaloENGINE configuration* tab.

If you haven't selected the Secondary HaloENGINE option in the Teamcenter Configuration tab, skip this step. 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 Teamcenter]. For example, `Teamcenter02_ClientKey.jks`
2. **Certificate Password**: Enter the password of the selected client Keystore. For example, `Key$T#1234`
3. **HaloENGINE Host**: Enter the IP address/FQDN of HaloENGINE. For example, `10.91.0.190`
4. **HaloENGINE Endpoint Port**: Enter the endpoint port from which HaloENGINE can be accessed. For example, `8746`
5. Click **Apply**. Any missing values will be indicated with a red tool tip message. This indicates that you need to enter and click **Apply**.

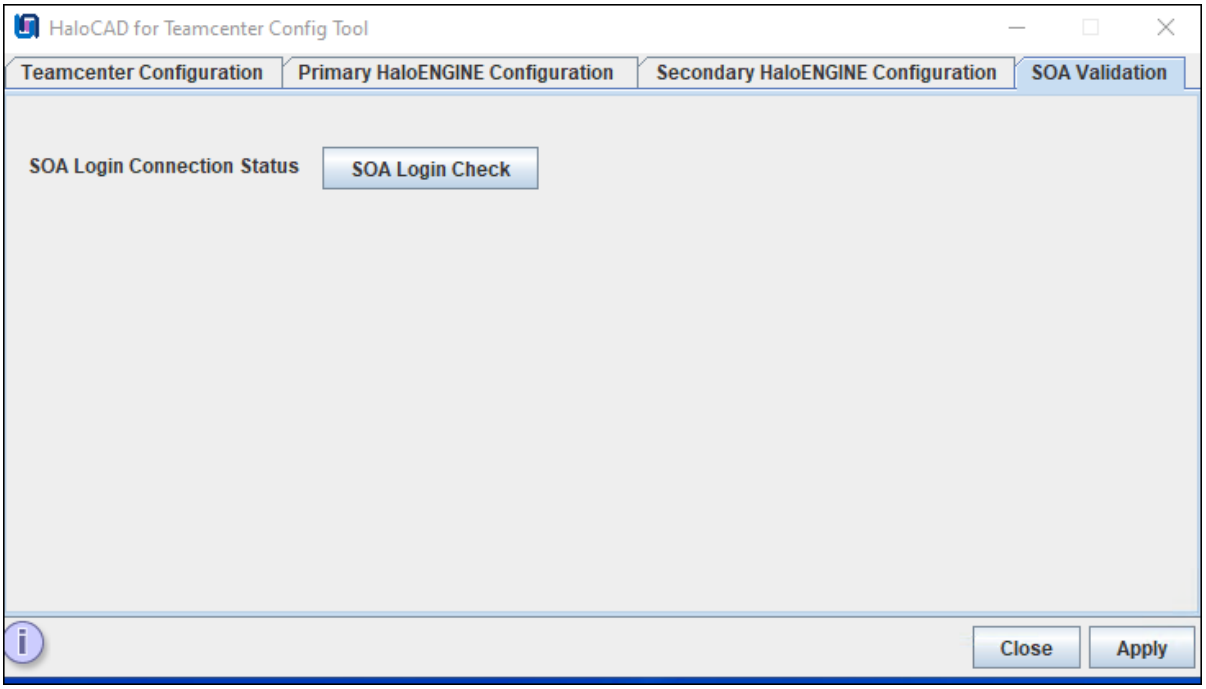
Results:

a. A progress bar indicates that "*Restarting Tomcat Service*" is being performed.

b. A confirmation message dialog box will appear.

c. Click **OK** on the confirmation dialog box.

Step 2d. Check the connection status on the *SOA Validation* tab.



SOA Validation tab

1. Press the **SOA Login Check** button to confirm the SOA credential configuration.
2. Click **Apply**. Any missing values will be indicated with a red tool tip message. This indicates that you need to enter and click **Apply**.

   Results:

   a. A progress bar indicates that "*Checking SOA logging connection status*" is being performed.

   b. A confirmation message dialog is displayed if the connection is successful. Click **OK** on the confirmation dialog box.

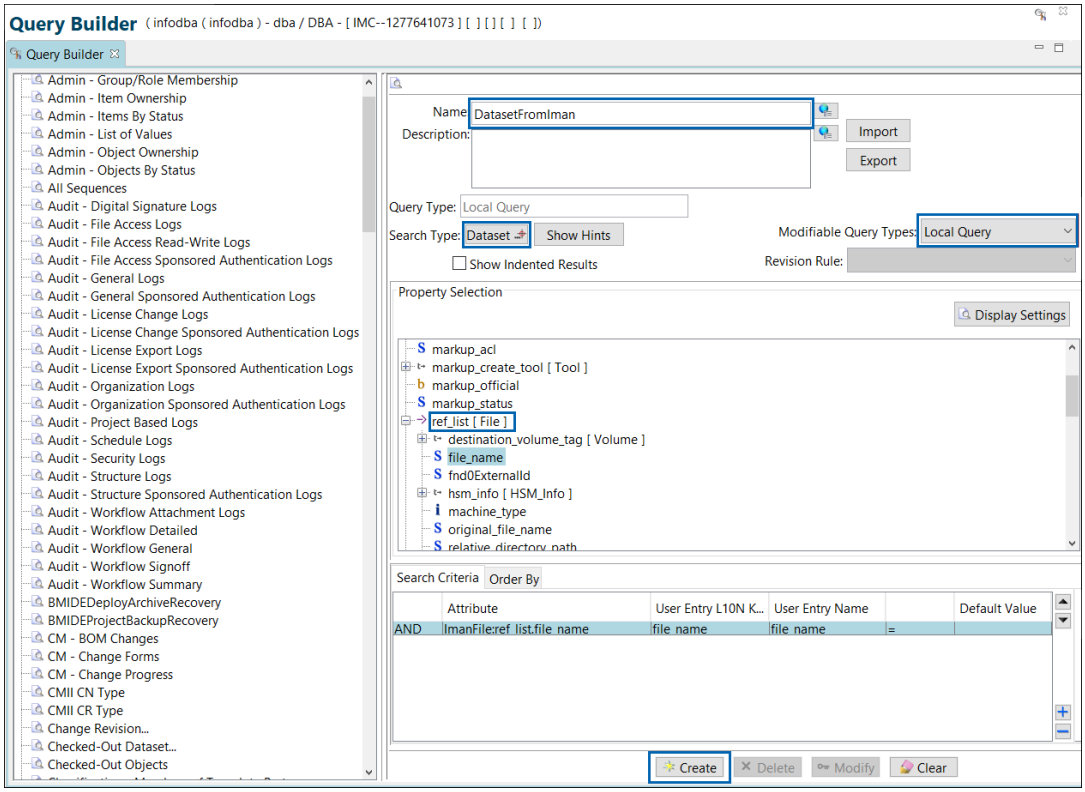
   c. Click **Close** to close the **HaloCAD for Teamcenter Config Tool** window.

Related task: If there is an error in the connection, you will receive the appropriate warning. Please follow the message and try again.

5.2. 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.

5.3. 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 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 privilege 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 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 privilege and add the following line along with the port number as shown in the below example:
      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.

5.4. 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 Teamcenter has been installed.

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

1. Open a command prompt and navigate to the destination folder and 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
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 Target name:
secude.com
Restarting Tomcat Service. Please wait.
Tomcat restarted successfully
--------------------------------------------------------------------------------
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
Target Name                     :secude.com

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
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\superdocs\Desktop\SM\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

HaloENGINE Service: (Default:Local)
1. Local
2. Remote

Please choose an option:
1

HaloENGINE Service File Mode: (Default:File Path)
```

```
1. File Path
2. Stream

Please choose an option:
1

Enter the HaloENGINE Service Port: (Default:20000)
20000

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

Please choose an option:
1
Restarting Tomcat Service. Please wait.
Tomcat restarted successfully
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               :Local
HaloENGINE Service File Mode     :File Path
HaloENGINE Service Port          :20000
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
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
SOA login is successful

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

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

6. 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.

6.1. FMS Proxy

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.

6.2. AWC Proxy

To verify the AWC configuration, follow the instructions below:

1. From the browser, open the AWC link. For example,
    a. Without Microservice: `<http://localhost:<AWC> Port>/awc`
    b. With Microservice: `<http://localhost:<awc> port>`

    Result: This will launch the AWC login page.
2. If you can sign in and view the Active Workspace, it confirms that the AWC is accessible via 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.

7. Updating the HaloCAD Configuration

You can update the configuration at any time by using the HaloCAD Configuration Tool (GUI).

8. 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.

9. Appendix

This section provides supplemental information.

9.1. Supported FMS Configurations

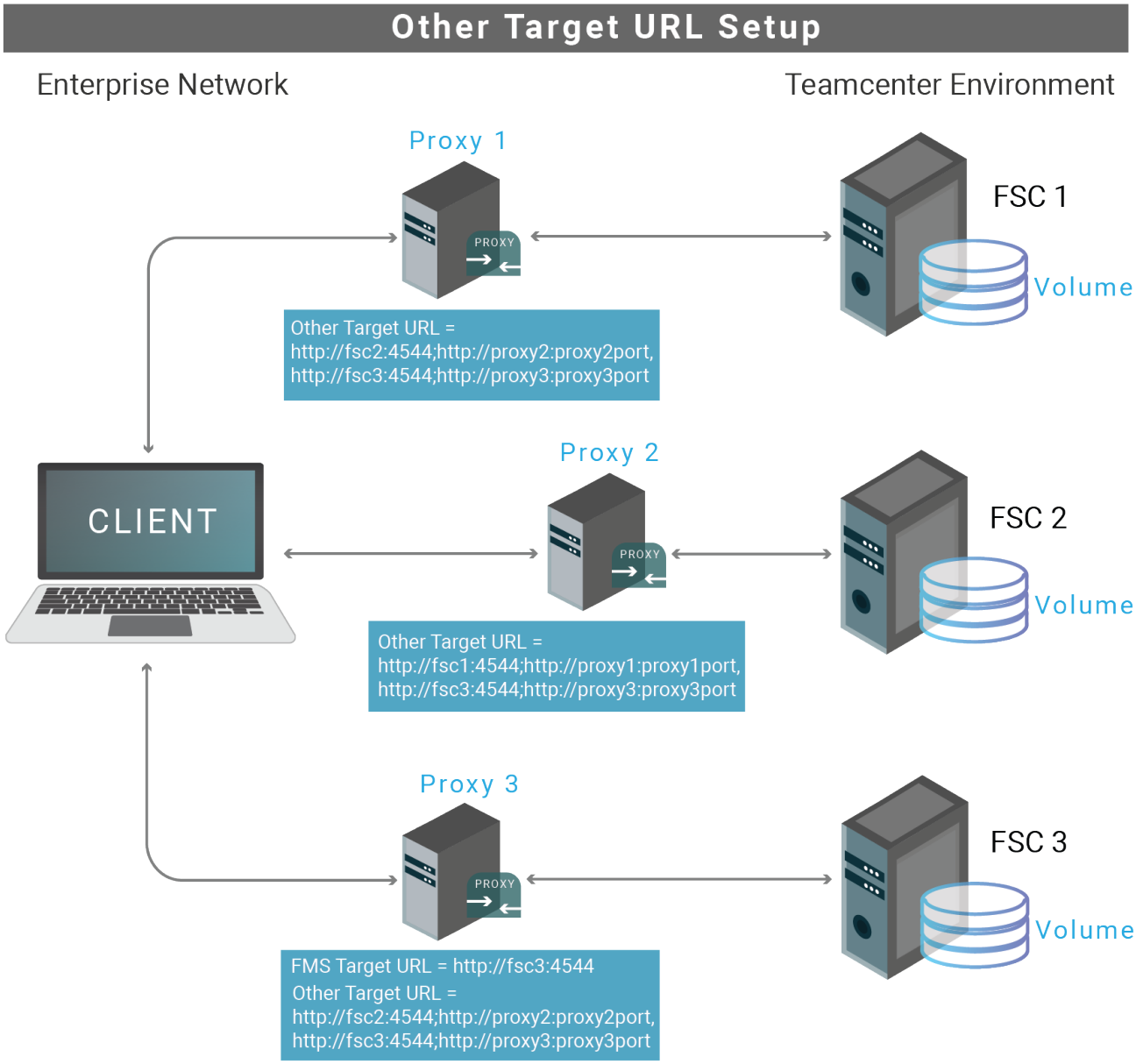
Teamcenter supports various FMS configurations based on the volume of files to be stored, how often files are accessed by clients, and client geographical location (remote).

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" />
```

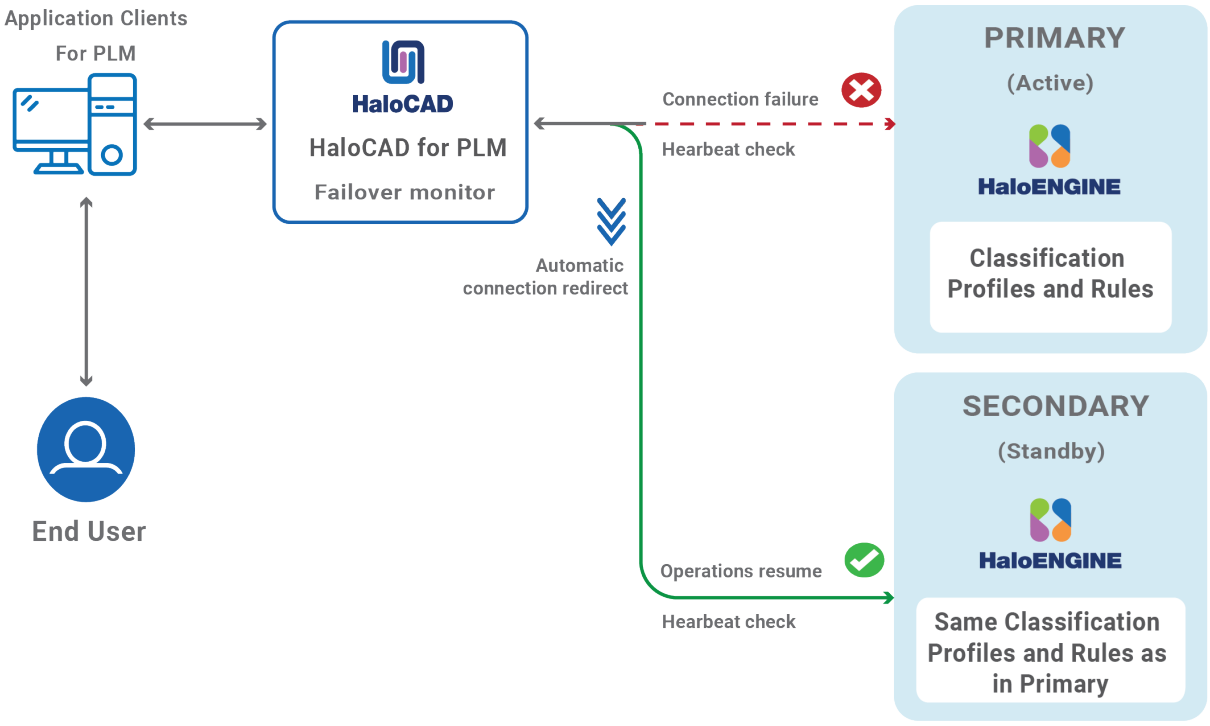
```
<transientvolume id="7f16bd0578697f1eb1bbb4b5020aadef" enterpriseid="-1234567890"
 root="D:\\Temp\\transientVolume_usprd01" priority="0" />
</fsc>
<fsc id="PUN-FMS_YUN_WEB20P_usprd01" address="http://PUN-FMS-WEB:4544"
 ismaster="false">
<transientvolume id="8c425ee7352a4657ac777dc198712cb3" enterpriseid="-1234567890"
 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>
```

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

9.3. Open-source Software

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
javax.mail	1.5.+	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	3.1.+	https://mvnrepository.com/artifact/javax.servlet/javax.servlet-api	https://glassfish.dev.java.net/nonav/public/CDDL+GPL.html
jna	5.6.0	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	5.6.0	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

Open-source software

9.4. Metadata

The Teamcenter metadata present in the HaloENGINE is listed in the table below.

Teamcenter metadata	Use
user_role	Derivation from 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 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)
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)

Teamcenter metadata	Use
preexpression_custom_pre-expression	Derivation from custom pre-expression. 1. Yes 2. No

Teamcenter metadata

9.5. Download Log Definition

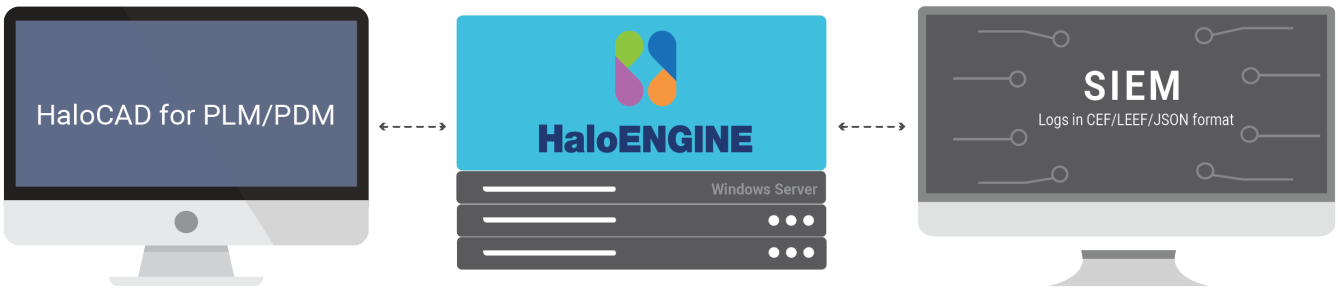
This section explains the log definition for every log format that HaloENGINE supports.

9.5.1. 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

9.5.2. 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|6.7.0.0|`
	• Device Event Class ID is a unique identifier per event-type.	`100` (User download)

Format	Description	Example
	• This can be a string or an integer. Device Event Class ID identifies the type of event reported.	
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

```
23:27:06.496 CEF:0|Secude|HaloCAD|6.7.0.3|100|user
download|1|deviceCustomDate1Label=exportTime deviceCustomDate1=Oct 18 2024 06:27:04
UTC externalId=CDF1138FA859429BB0EDE5E49A61A60C deviceCustomDate2Label=logTime
deviceCustomDate2=Oct 18 2024 06:27:06 UTC act=unblocked;labeled;protected
fname=Installation of Postgres.docx
filePath=FMS_SHA256_SIGNATURE=b7c7ed99efb4c45949d2d8993bc10df328af20137c4c43b11a1f3d84
7b1eb71e3189819770608bfc02ea51fed89f94e8e96b16f1cdbd2d436569a2c1ee42749a;\dba_66f105e2
\testpr_wor_39v0blkatzbz1.docx fileType=docx fsize=26907 in=65536 shost=TC11
duser=infodba,type:DBA;PartnerContractAdmin dst=10.41.0.123
requestClientApplication=[null] cs2Label=DataDestination cs2=[ platform\=[Unknown],
browser\=[FMS-FCC/2312 (bd:20240607)], browser_version\=[null], device_type\=[null],
terminal_id\=[SVLU0309], destination_attributes\=[{ key\=[client_ip],
value\=[10.41.0.123], type\=[null] }, { key\=[client_host], value\=[SVLU0309],
type\=[null] }] ] cs3Label=DataOrigin cs3=[ source_type\=[PLM], system_name\=[TC11],
client_type\=[TEAMCENTER], plm_info\=[{ key\=[original_file_name],
```

```
value\=[Installation of Postgres.docx], type\=[null] }, { key\=[folder_name],
value\=[dba_66f105e2], type\=[null] }, { key\=[ip_clearance], value\=[secret],
type\=[null] }, { key\=[gov_clearance], value\=[super-secret], type\=[null] }, {
key\=[user_def_group], value\=[dba], type\=[null] }]] cs4Label=ClassifyProtectionData
cs4=[ policy_id\=[d7e95033-e7f1-4218-8941-7d60d8e9cf69], policy_name\=[CADSecured],
policy_type\=[company_policy], error\=[false], author\=[HaloENGINE Service] ]
```

CEF sample

9.5.3. 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

```
23:39:56.735 LEEF:2.0|Secude|HaloCAD|6.7.0.3|100|^|exportTime=Oct 18 2024 06:39:55
UTC^eventName=user download^externalId=BE041836AC4C4AC4B41468F7594E04DC^logTime=Oct 18
2024 06:39:56 UTC^act=unblocked;labeled;protected^fname=Installation of
PostgresPro.docx^filePath=FMS_SHA256_SIGNATURE=39aa1a2af568f8425e06c0a10b184024ecd91d7
bf971a08c8cc3d848f31b19ff41932e34513160eb70908e79a1f0911a0d64005b74b1d5e4e74791e74422b
d7f;\dba_66f105e2\testse_wor_2a209p0augghq.docx^ftype=docx^fsize=26907^fdwnsize=65536^
shost=TC11^usrName=infodba,type:DBA;PartnerContractAdmin^dst=10.41.0.123^usrAgent=[nul
l]^dataDestination=[ platform=[Unknown], browser=[FMS-FCC/2312 (bd:20240607)],
browser_version=[null], device_type=[null], terminal_id=[SVLU0309],
destination_attributes=[ {key=[client_ip], value=[10.41.0.123], type=[null]},
{key=[client_host], value=[SVLU0309], type=[null]} ] ]^dataOrigin=[ source_type=[PLM],
system_name=[TC11], client_type=[TEAMCENTER], plm_info=[ {key=[original_file_name],
value=[Installation of PostgresPro.docx], type=[null]}, {key=[folder_name],
value=[dba_66f105e2], type=[null]}, {key=[ip_classification], value=[top-secret],
```

```
type=[null]}, {key=[ip_clearance], value=[secret], type=[null]},
{key=[gov_classification], value=[gov-secret], type=[null]}, {key=[gov_clearance],
value=[super-secret], type=[null]}, {key=[user_def_group], value=[dba], type=[null]} ]
]^classifyProtectionData=[ policy_id=[d7e95033-e7f1-4218-8941-7d60d8e9cf69],
policy_name=[CADSecured], policy_type=[company_policy], extendedTags=[
message=[Success] ], 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|6.7.0.0|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|6.7.0.0|100|`
	EventID	A unique identifier for an event.
	Delimiter Character	Pipe Specifies an alternative delimiter to the attributes. You can use a single character or the hex value for that character. The hex value can be represented by the prefix 0x or x, followed by a series of 1-4 characters (0-9A-Fa-f).

Format	Description	Example
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

9.5.4. 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).


```
23:43:17.215
{"log_id":"52F42C05D96E47E2B924F43949019909","product":"HaloCAD","source_host":{"shost
":"TC11"},"protection":{"policy_id":"d7e95033-e7f1-4218-8941-
7d60d8e9cf69","extended_tags":[{"value":"Success","key":"message"}],"policy_name":"CAD
Secured","error":false},"destination_info":{"hostname":"SVLU0309","destination_attribu
tes":[{"value":"10.41.0.123","key":"client_ip"},{"value":"SVLU0309","key":"client_host
"}],"destination_ip":"10.41.0.123","os":"Unknown","recipients":[],"browser":"FMS-
FCC/2312
(bd:20240607)","device_type":"null","browser_version":"null","user_agent":"null"},"cla
ssification":{"classification_by_system":[],"classification_by_user":[]},"version":"6.
7.0.3","log_time":"Oct 18 2024 06:43:17
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":"Installation of
PostgresPsdvsdvro.docx","key":"original_file_name"},{"value":"dba_66f105e2","key":"fol
der_name"},{"value":"secret","key":"ip_clearance"},{"value":"gov-
secret","key":"gov_classification"},{"value":"super-
```

```
secret","key":"gov_clearance"},{"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=0c04162c53b229ac792980b676324fcf5fa4ad5456a20d84df39a7
e1c2843459ef585b9aac8d4b8e701874f1fe2c59090dc7a1be78a9dfbaa781b106c20b0cfa;\\dba_66f10
5e2\\testes_wor_2si09p0auggl3.docx","file_name":"Installation of
PostgresPsdvsdvro.docx","file_type":"docx","download_file_size":65536,"original_file_s
ize":26907},"action":["unblocked","labeled","protected"],"export_time":"Oct 18 2024
06:43:15 UTC","event":"user download"}
```


JSON format

9.6. Deactivating the HaloCAD for Teamcenter

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

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 at 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 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".

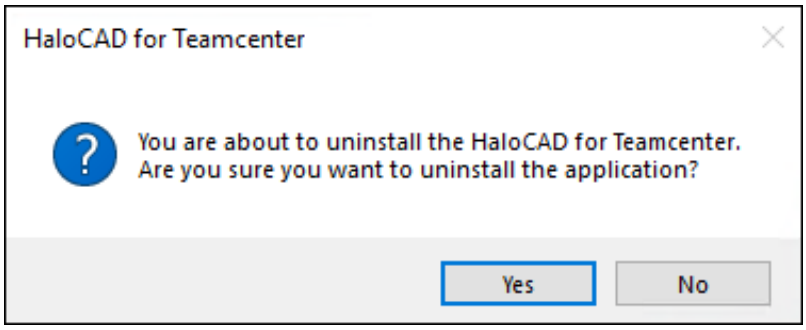
9.7. Uninstalling the HaloCAD for Teamcenter

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!*"

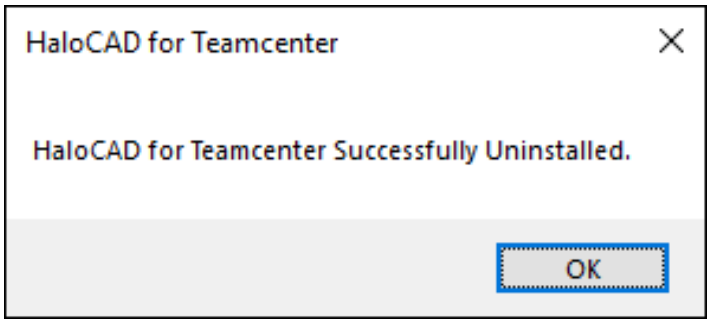
Method #1

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 will appear.



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 Microsoft and SAP Partner, is a global leader for Zero Trust Data-centric security and Enterprise Digital Rights Management (EDRM) solutions.

For more than 25 years Secude has been trusted by many Fortune 500 and DAX-listed companies for architecting, implementing, and protecting their data. Our data-centric security professionals apply their passion and deep domain expertise to provide a holistic approach to protect priceless Intellectual Property (IP) in CAD & SAP based collaborations and supply chains.

With branches in Europe, North America and Asia, Secude supports customers with the implementation of IT security strategies through a global network.