Secude

HaloCAD

HaloCAD for Autodesk Vault 2.5

Installation Manual

Copyright

Contact

Secude Solutions AG

Landenbergstrasse 34

6005 Luzern

Switzerland

Tel: +41 41 510 70 70

Mail: info@secude.com

Support

Web: https://support.secude.com

Mail: support@secude.com

Table of Contents

Typographic Conventions

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

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

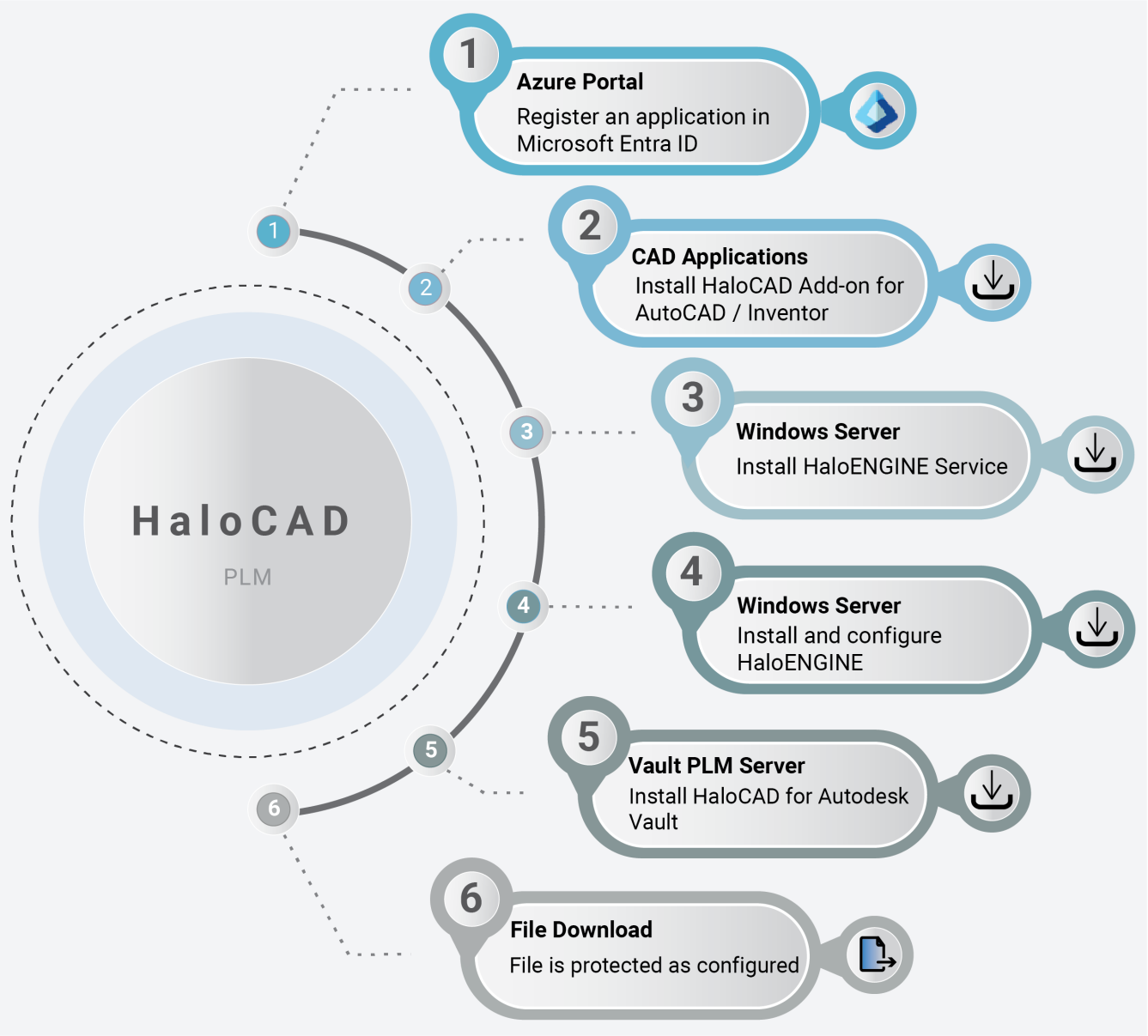
The HaloCAD for PLM solution integrates with the respective PLM application and includes the functionality of HaloCAD PROTECT and HaloCAD MONITOR. Files are automatically protected during the access/download or check-out process and are stored unprotected back into the PLM Vault during the upload/check-in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

1.3. About this Manual

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

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 AutoCAD/Inventor.	1. `HaloCAD_AutoCAD_Manual_Installation_EN_Online.pdf` 2. `HaloCAD_Inventor_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 Autodesk Vault.	Refer to the current manual.
Step 6 – How to download a protected file.	`HaloCAD_AutodeskVault_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 Autodesk Vault 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, Autodesk Vault PLM protects AutoCAD, Inventor, MS Office, and PDF files.

Supported PLM Multi-CAD Integrations:

1. HaloCAD for Autodesk Vault—Autodesk AutoCAD Integration
2. HaloCAD for Autodesk Vault—Autodesk Inventor 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

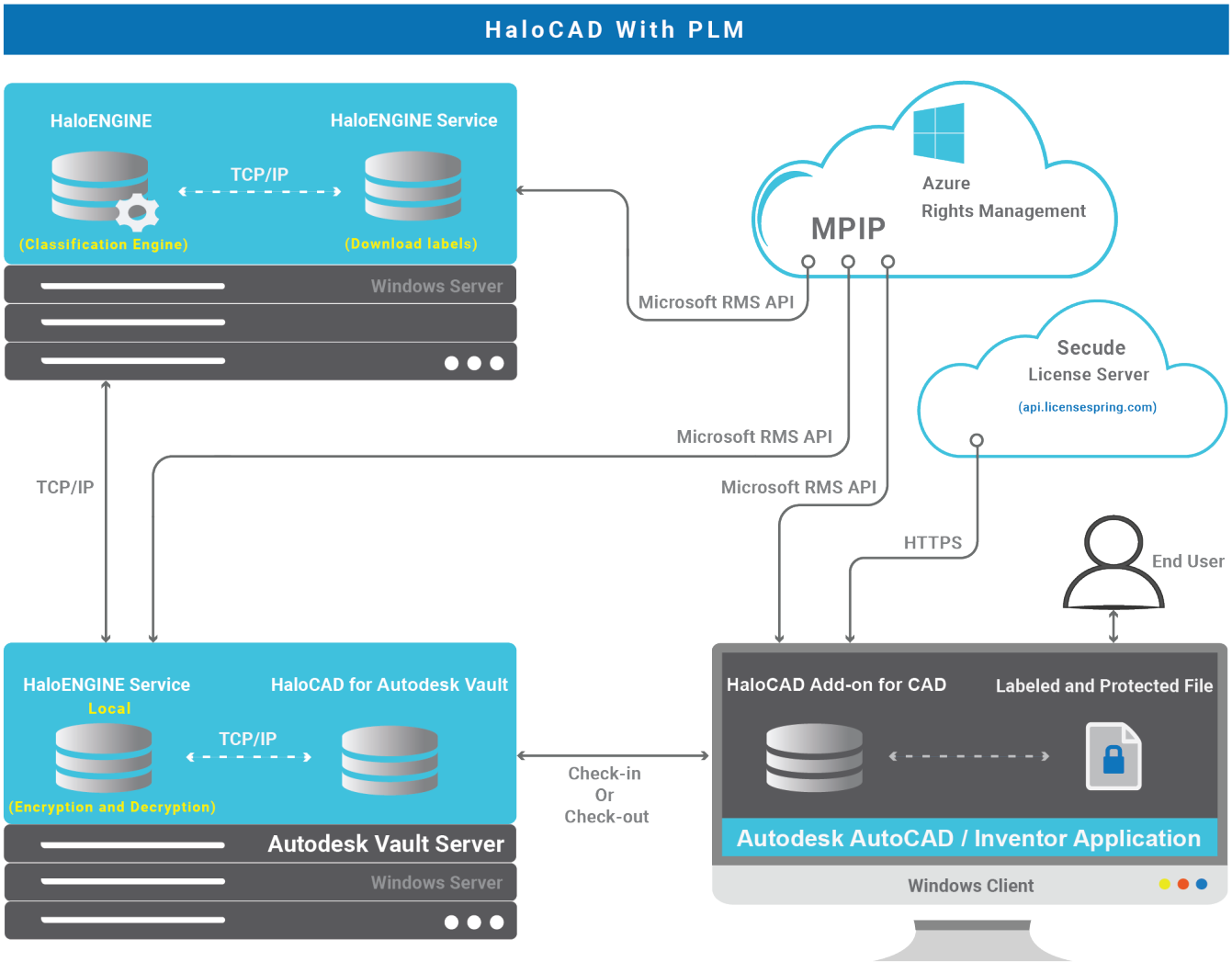
The following section explains about components of HaloCAD.

1. HaloCAD for Autodesk Vault—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 Autodesk Vault should be installed on the same server machine, or these two components can be installed on the same server machine where Autodesk Vault PLM is installed. Whereas 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.

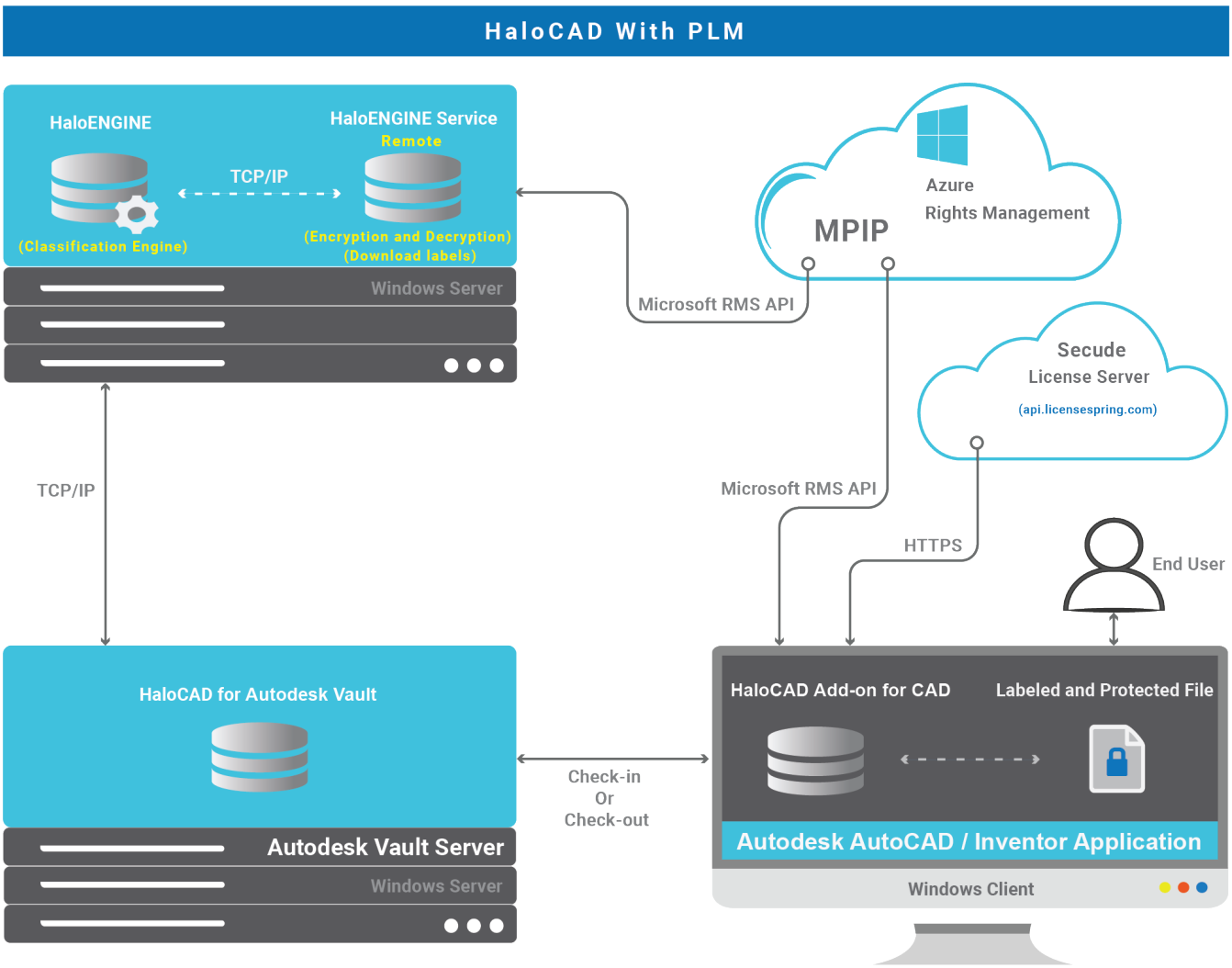
b. With **Remote** mode, HaloCAD for Autodesk Vault is installed on a separate server machine and communicates with the HaloENGINE to get the file encrypted/decrypted by the HaloENGINE Service, which is installed locally on the HaloENGINE installed machine.

c. During a file check-in/check-out action, the HaloCAD for Autodesk Vault 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 AutoCAD and Inventor performs the following functions:

1. Resides in Autodesk AutoCAD and Inventor applications.
2. Responsible for receiving the protected file from the Autodesk Vault and displaying the appropriate label with permission enforcement.
3. Responsible for forwarding the encrypted file stream (if labeled) to HaloCAD for Autodesk Vault.
4. Responsible for logging the add-on-related activities.

HaloCAD for Autodesk Vault performs the following functions:

1. It can be hosted on the Autodesk Vault PLM Server or on a Windows server with the possibility to access the Autodesk Vault server.
2. Listen for check-in and check-out actions through the PLM Vault server.
3. Remote mode: Responsible for the collection of metadata and label information from the HaloENGINE and then sending the file to the (remote) HaloENGINE 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 Autodesk Vault.

1. Responsible for business logic. The HaloENGINE (classification engine) interprets the metadata collected in Autodesk Vault 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 to Autodesk Vault.

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 to PLM.

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 Autodesk Vault

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

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 Windows Server	Windows Server 2016 and above
Supported file types	1. AutoCAD file types 2. Inventor 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 AutoCAD/Inventor can connect to the Autodesk Vault Server.
3. Make sure that the HaloENGINE Service is installed in MPIP mode.
4. Make sure your HaloENGINE complies with the requirements listed below:
   a. License file (enabled with AUTODESK_VAULT system type).
   b. Proper action rules
   c. Client certificate (`.JKS`)
5. Make sure to have a user account with document-consuming rights in the **Vault Server**.
   a. You can add an existing user account to the specific Autodesk Vault.

b. Or create a new user account and add it to the specific Autodesk Vault by logging in **Autodesk Vault** > **Tools** > **Administration** > **Global Settings** > **Security** > **Users** > in the **User Management** window, click **New User** (enter required details) and click on the **Vaults** button to select all the Vaults listed.

6. 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

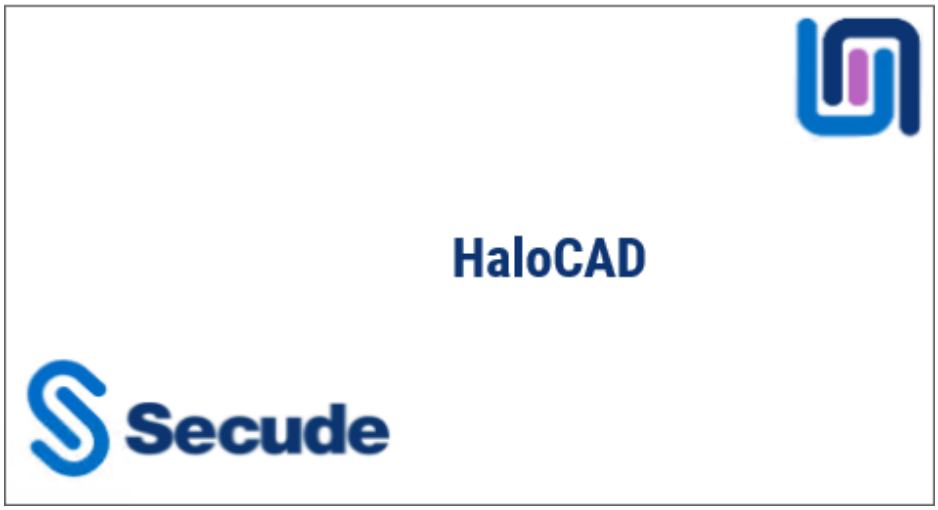
You can install the HaloCAD component in the following modes:

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.

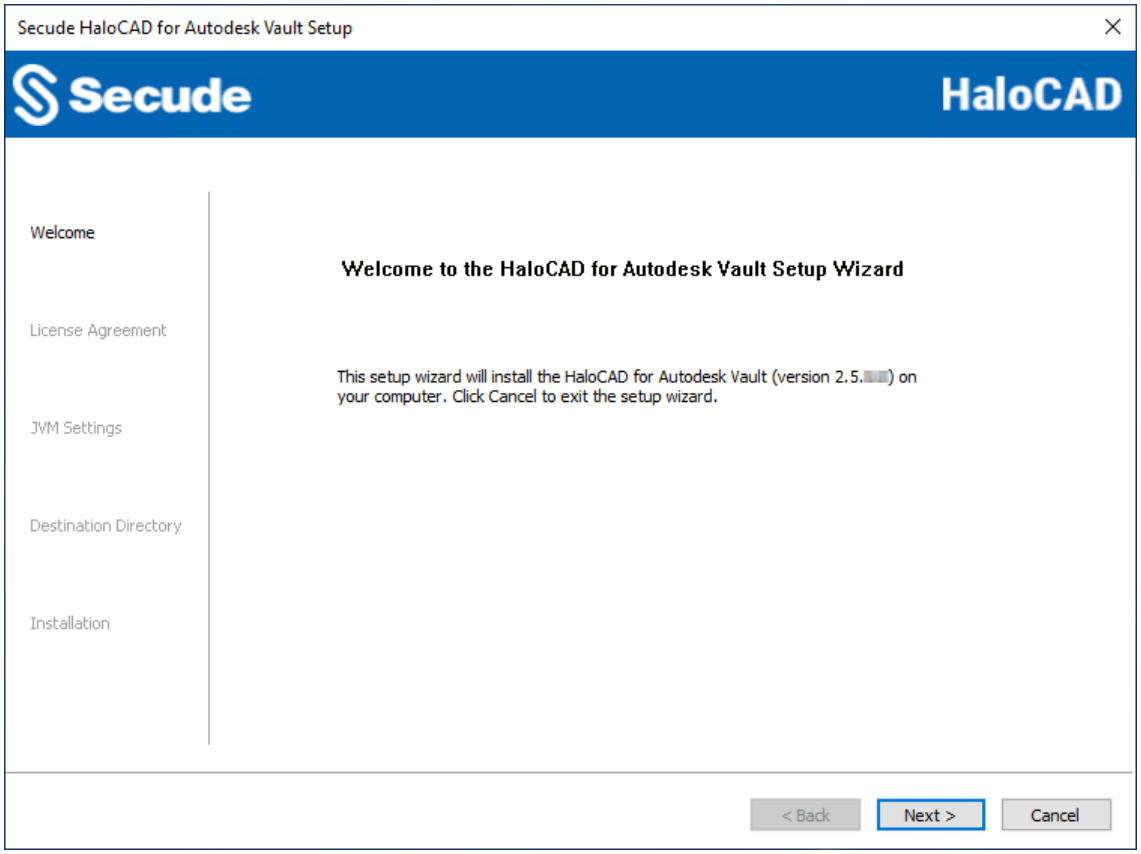
4.3.1. Graphical Mode

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

1. To begin the interactive installation, double-click the installer `HaloCAD_Autodesk_Vault_Setup.exe` file.
2. Depending on your Windows security settings, you may get a warning such as "*Do you want to allow the following program to make changes to this computer?*". If you get this security warning, click the **Yes** button to continue the installation.
3. When the installer starts, you will see the startup dialog followed by the welcome dialog:

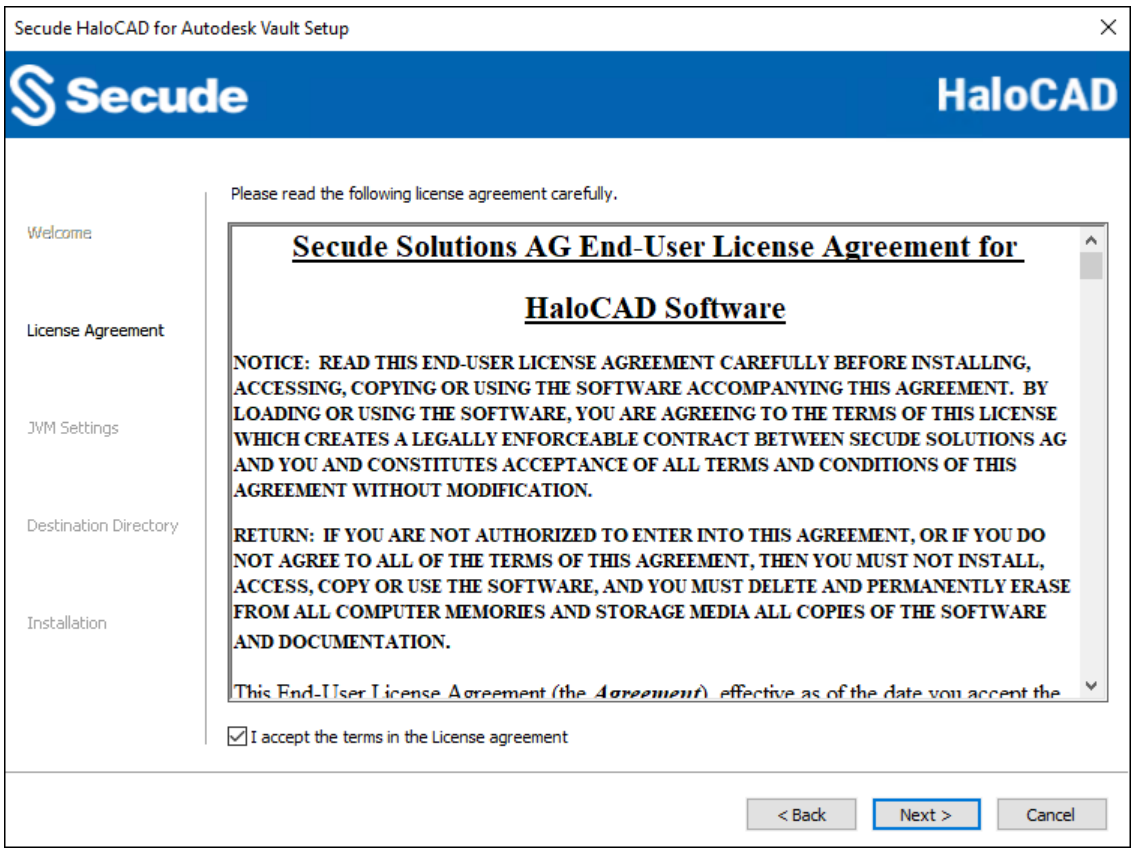


Startup Dialog



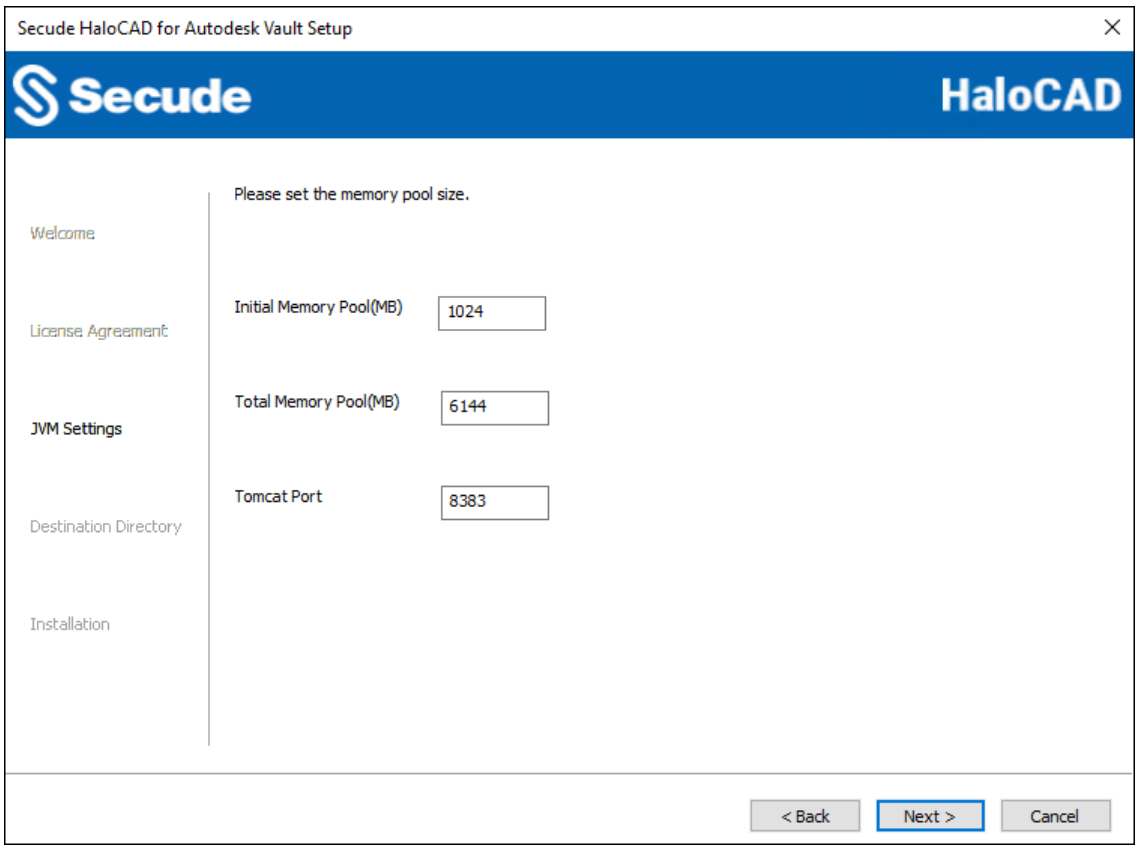
Welcome Dialog

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



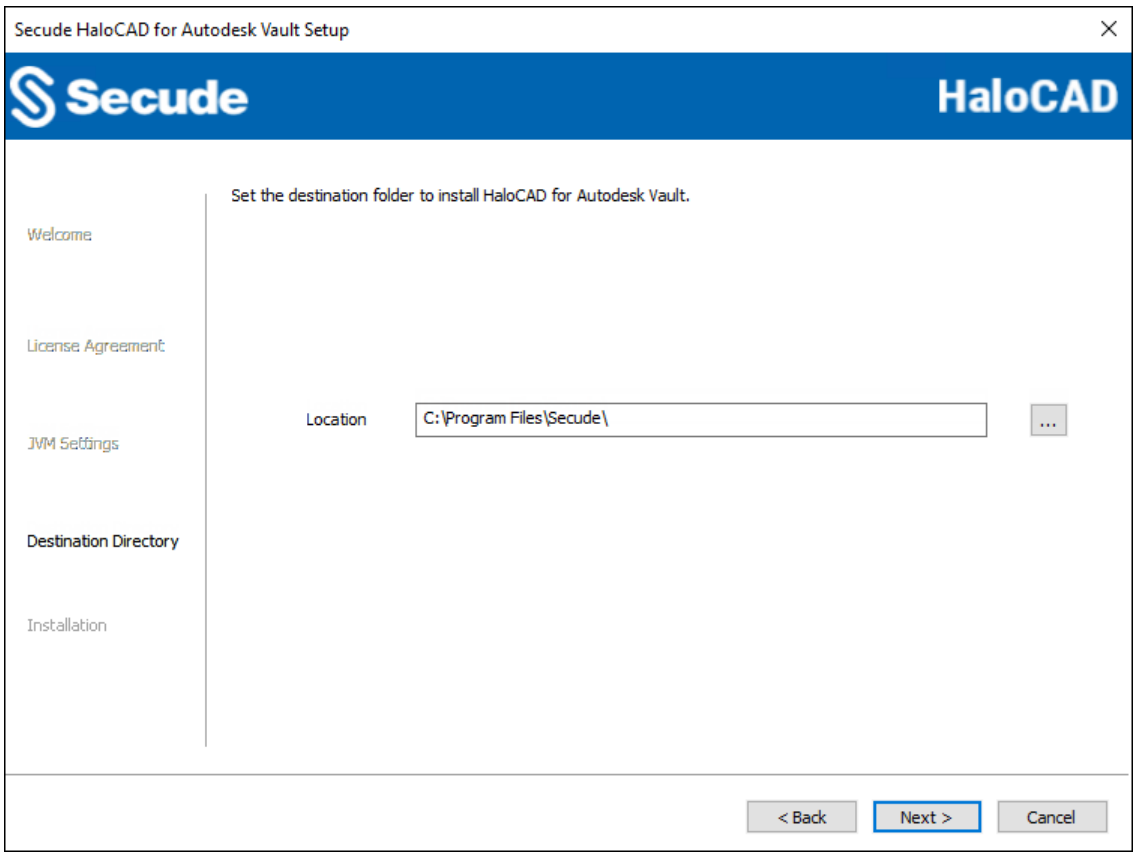
End-User License Agreement Dialog

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:



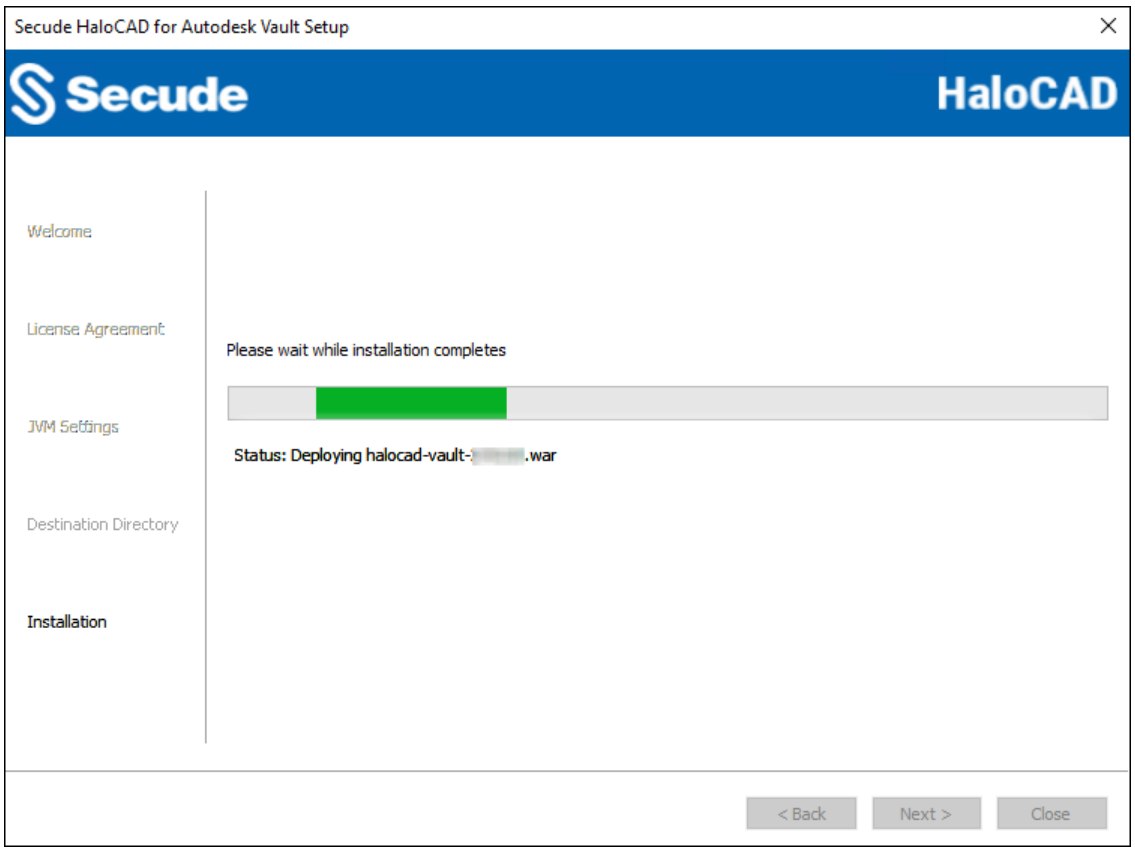
Tomcat pool size configuration dialog

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



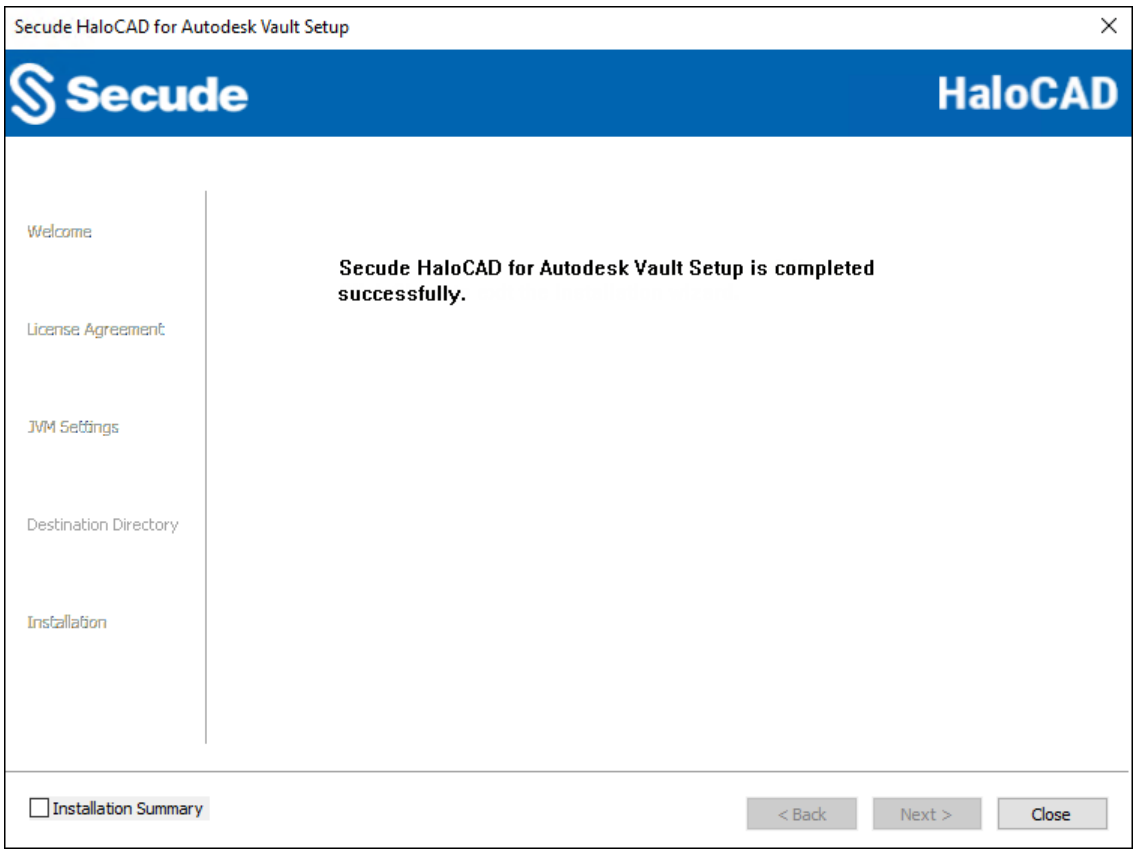
Destination folder selection dialog

10. By default, application files are stored in the program files directory (`C:\Program Files\Secude\`). If you would like to choose an alternate location, click the **Browse** button and select your location preference. 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. To return to any point in the installation process, click the **Back** button (optional).
11. The installation begins and progress is shown in the dialog.



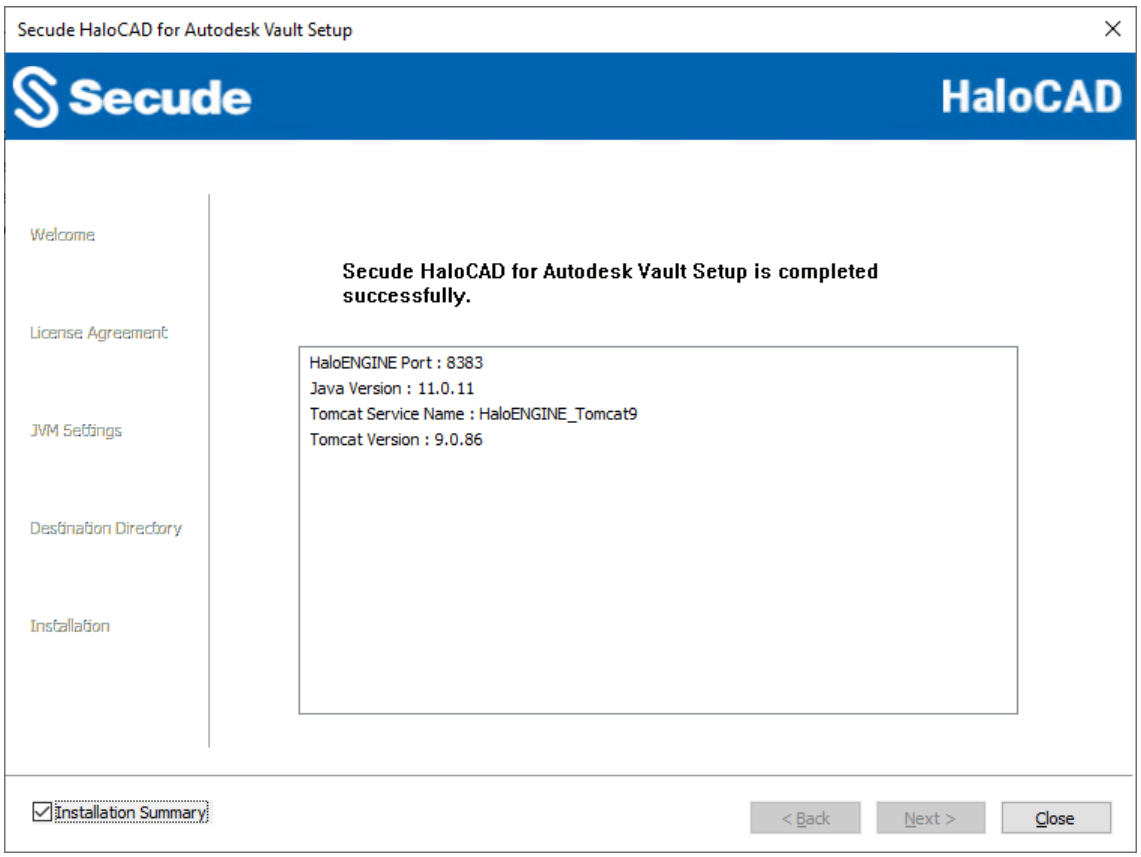
Installation progress dialog

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



Installation completed dialog

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



Summary with preinstalled HaloENGINE dialog

14. Please note that the HaloENGINE information will not be included in the summary if it is not already installed.
15. 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\HalocadVault\config\HaloCAD-for-Autodesk-Vault-config-<version>.jar`. This tool is explained in the next section "Configuring the HaloCAD Proxy".
2. Log file—HaloCAD component-related activities are logged in `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_Autodesk_Vault_Setup.exe -help`

   Press `Enter`

   Output

   ...

   ```
   HaloCAD_Autodesk_Vault_Setup.exe -install -initmempool <Initial memory pool size in MB(s).
   Minimum size is 128 MB> -totalmempool <Total memory pool size in MB(s).
   Maximum size is 3/4 of total RAM size.> -dir <destination_directory> -port <range_1_to_65535>
   HaloCAD_Autodesk_Vault_Setup.exe -uninstall
   ```
4. The following command illustrates how to install the HaloCAD component.

   ```
   SECUDE_HALOCAD_AUTODESK_VAULT_X64.EXE -install -initmempool 1024 -totalmempool 2048 -dir "C:\Program Files\Secude" -port 4444
   ```
5. Press `Enter`.
6. Installation gets completed.

5. Configuring the HaloCAD Proxy

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

5.1. Configuration Using Tool (GUI)

Prerequisite: Ensure that HaloCAD for Autodesk Vault has been installed.

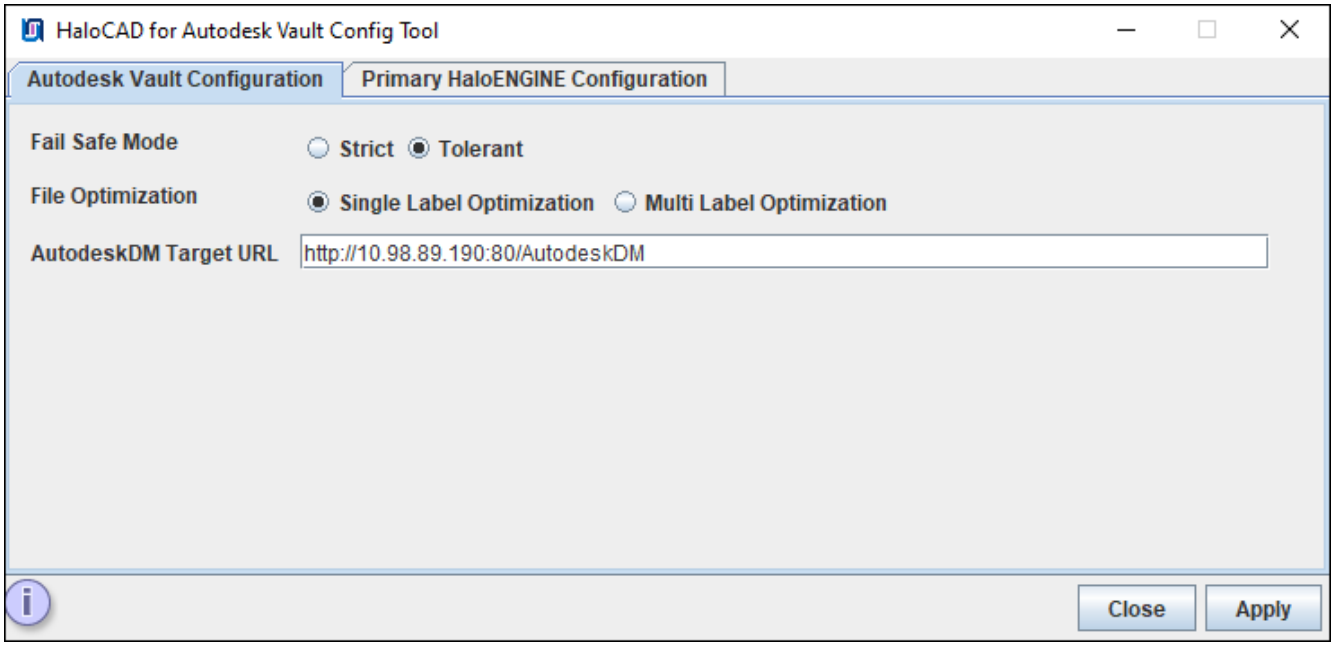
Follow the steps below to configure settings using the GUI.

Step 1. Stop the Tomcat Service.

Step 2. Run the HaloCAD Configuration Tool.

1. Navigate to the destination folder you specified during installation. The default folder is `C:\Program Files\Secude\HalocadVault\config`.
2. Double-click the jar file or type `HaloCAD-for-Autodesk-Vault-config-<version>.jar` and press **Enter** in the **Command Prompt** with administrative privileges.
   Example: `C:\Program Files\Secude\HalocadVault\config>java -jar HaloCAD-for-Autodesk-Vault-config-<version>.jar`
3. The *HaloCAD for Autodesk Vault Config Tool* window will appear.

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

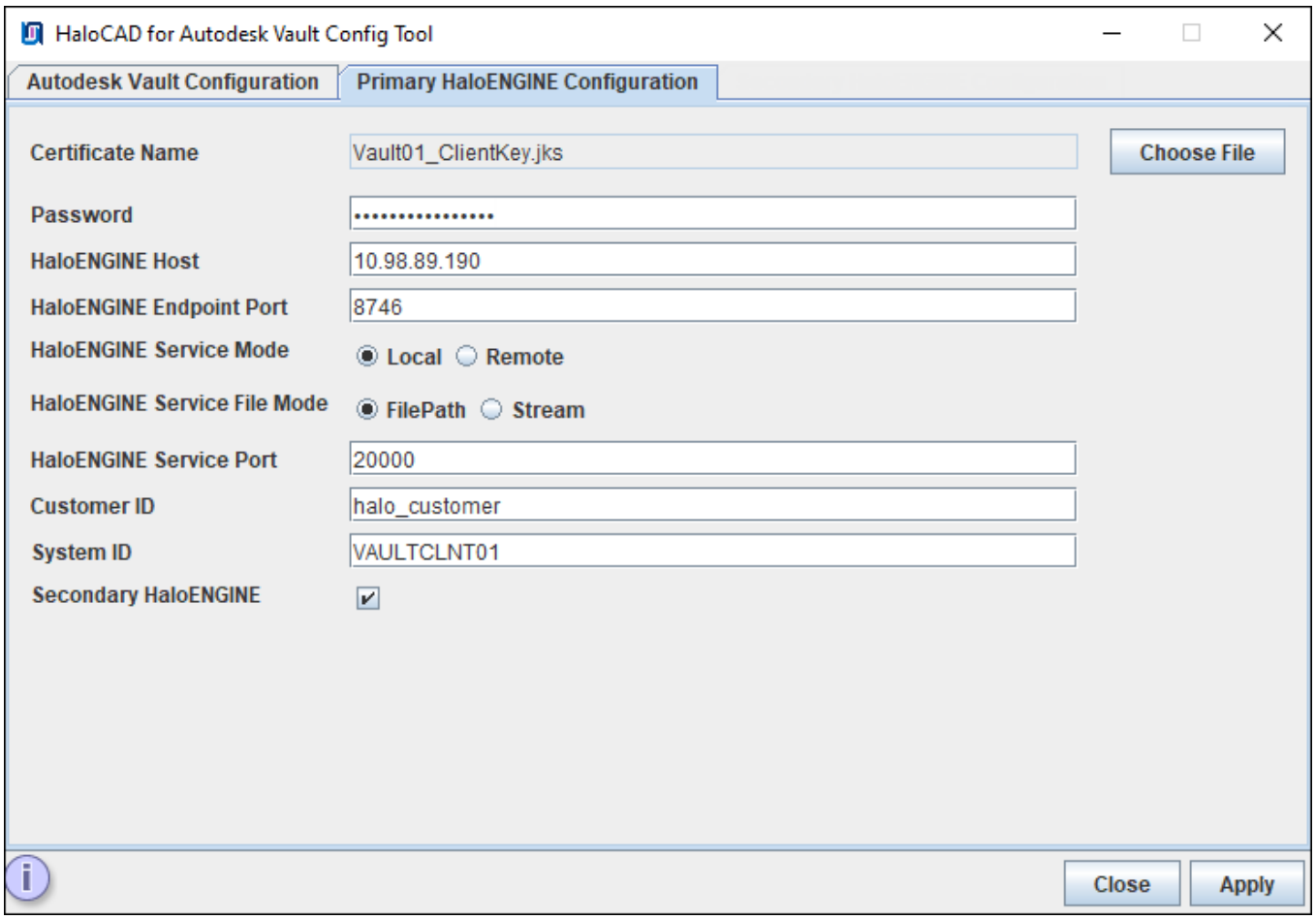


Autodesk Vault configuration tab

1. **Fail-Safe Mode**: The Fail-Safe Mode controls the system's behavior in case of inconsistencies that prevent the specified protection from being applied (conflicting configuration, server component unreachable, or returning an error message, etc.). You can define any one of the following:
   a. **Strict**: The file upload or download is blocked, whenever any error occurs.
   b. **Tolerant (default)**: The file upload or download will be allowed, even when an error occurs.
2. **File Optimization**: Choose one of the following options for file optimization. By default, Single Label Optimization is set.
   a. **Single Label Optimization:** The top-level file label is 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.
3. **AutodeskDM Target URL**: Enter the AutodeskDM Target URL on which your Autodesk Vault is hosted. Example, `http://10.98.89.190:80/AutodeskDM`.
4. 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 confirmation message dialog box will appear.
   b. 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, which is generated by the HaloENGINE Admin Portal (through which communication is established between the HaloENGINE and Autodesk Vault). Example, `Vault01_ClientKey.jks`
2. **Password**: Enter the password of the selected client Keystore. Example, `Key$T#123`
3. **HaloENGINE Host**: Enter the IP address/FQDN of HaloENGINE. Example, `10.98.89.190`
4. **HaloENGINE Endpoint Port**: Enter the Endpoint Port where the service is accessed by this client application. 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 Autodesk Vault are installed on the same machine on which Autodesk Vault is installed. If you choose **Local**, you must select the file transmission method in the **HaloENGINE Service File Mode** (**FilePath**/**Stream**) and enter the port number in the **HaloENGINE Service Port** text box.
      - **FilePath (default)**: File stored in a local temporary location for encryption and decryption process. Here, file path information is used for transferring.
      - **Stream:** File as a sequence of bytes.

- **HaloENGINE Service Port**: Enter the port assigned to the HaloENGINE Service during the installation. By default, HaloENGINE Service uses port `20000`.

b. **Remote**: Select if HaloENGINE Service and HaloCAD for Autodesk Vault 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**: Enter the Autodesk Vault Server's hostname and the same must be entered in the **System Unique ID** (HaloENGINE admin portal). For example, `VAULTCLNT01`.
8. **Secondary HaloENGINE**: If you want to set up a failover mechanism in your environment, select this check box. HaloCAD supports connection failover between two HaloENGINEs. For more information, please refer to the section "Failover Mechanism for HaloENGINE in HaloCAD for PLM".
9. Click **Apply**. 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 confirmation message dialog box will appear.

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

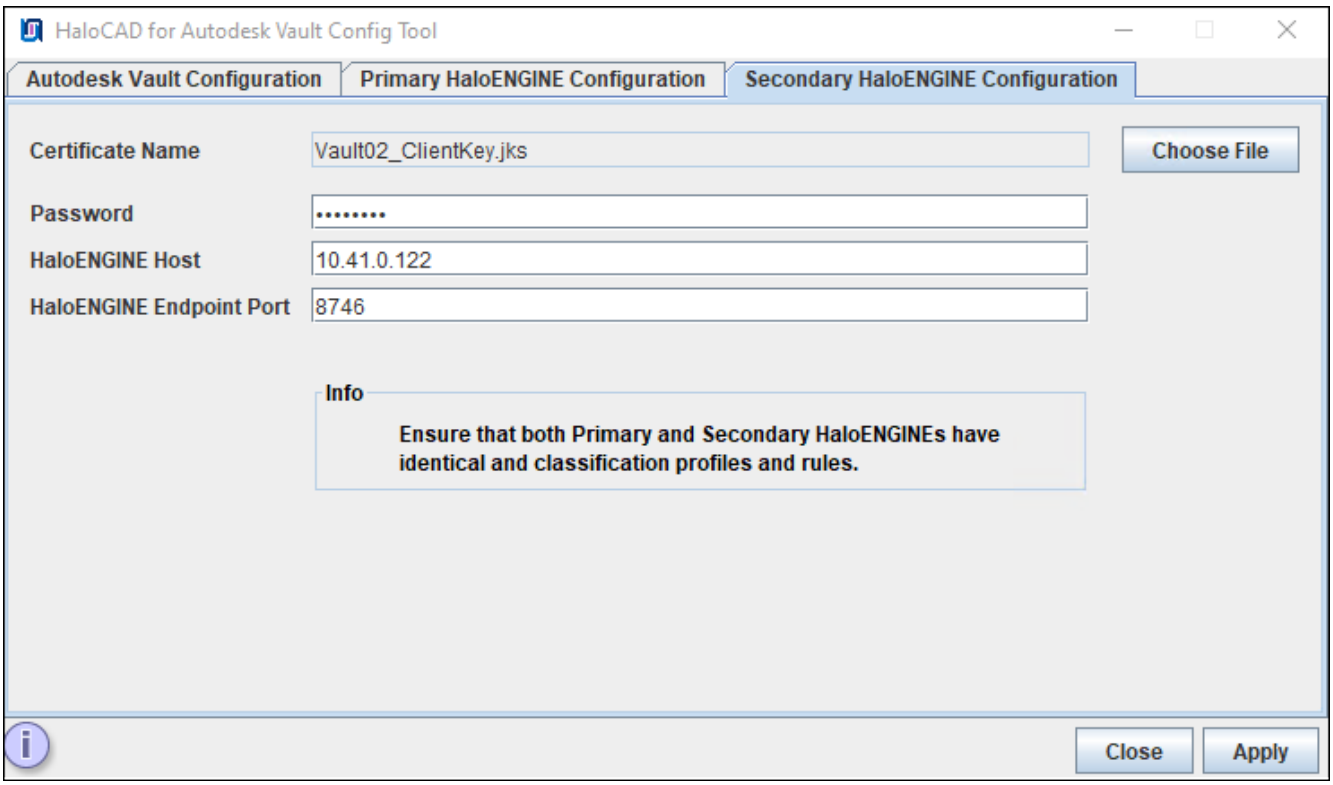
   c. After successful configuration, the configuration tool will create a `config.properties` file in `C:\Program Files\Secude\HalocadVault\config`.

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

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

If you haven't selected the Secondary HaloENGINE option in the Autodesk Vault 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 Autodesk Vault]. For example, `Vault02_ClientKey.jks`
2. **Password**: Enter the password of the selected client Keystore. For example, `Key$T#1234`
3. **HaloENGINE Host**: Enter the IP address/FQDN of HaloENGINE. For example, `10.41.0.122`.
4. **HaloENGINE Endpoint Port**: Enter the endpoint port from which HaloENGINE can be accessed. For example, `8746`
5. Click **Apply**. 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 confirmation message dialog box will appear.

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

Step 3. Start the Tomcat Service.

5.2. Configuration Using the Command Line

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

Prerequisite: Ensure that HaloCAD for Autodesk Vault has been installed.

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

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

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

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

Enter the AutodeskDM Target URL :http://10.98.89.190:80/AutodeskDM
Saved Successfully.
--------------------------------------------------------------------------------
Autodesk Vault Configuration
Fail Safe Mode          :Tolerant
File Optimization       :Multi Label Optimization
AutodeskDM Target URL   :http://10.98.89.190:80/AutodeskDM

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

```
0. Exit
Please choose an option: 3
--------------------------------------------------------------------------------
1. Autodesk Vault Configuration
2. Primary HaloENGINE Configuration
0. Exit
Note: If an invalid value is entered, the default value will be applied.
Please choose an option:2
--------------------------------------------------------------------------------
Primary HaloENGINE Configuration
Certificate Name            :
HaloENGINE Host IP          :
HaloENGINE Endpoint Port    :
HaloENGINE Service Mode     :Local
HaloENGINE Service File Mode:File Path
HaloENGINE Service Port     :20000
Customer ID                 :halo_customer
System ID                   :
Secondary HaloENGINE        :Disable Secondary HaloENGINE

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

Please choose an option: 1
--------------------------------------------------------------------------------
Primary HaloENGINE Configuration
Enter the Primary Certificate Path:
 C:\Users\superdocs\Desktop\SM\Vault01_ClientKey.jks

Enter the Primary certificate Password:

Enter the Primary HaloENGINE Host:10.98.89.190

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

Enter the Customer ID:halo_customer

Enter the System ID:VAULTCLNT01

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

```
Please choose an option: 1

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

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

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

6. Testing the (Reverse) Proxy Configuration

To verify the proxy configuration, follow the instructions below:

1. Open **Autodesk Vault Professional Client** or any **Vault** plugin-loaded application**.**
2. Login to Autodesk Vault, server pointing to the proxy port (tomcat port).
3. You can see the logs in `C:\Program Files\Secude\Tomcat\logs\haloproxy.log`.

Next Steps

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

7. Updating the HaloCAD Configuration

You can update the configuration at any time by using the HaloCAD Configuration Tool (GUI). Using the same tool, you can change the current settings whenever you wish. Follow Step 2, update the settings, and then restart the Tomcat Service.

8. Appendix

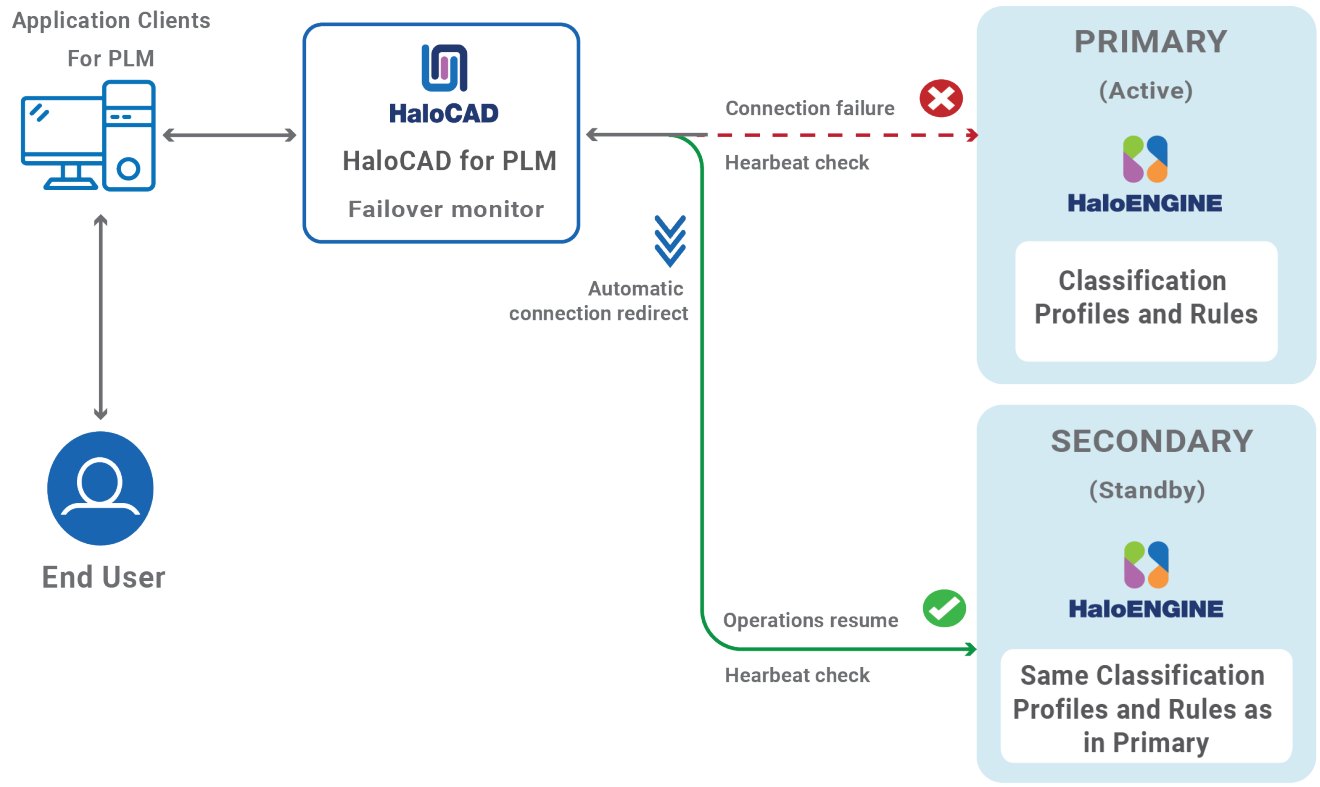
This section provides supplemental information.

8.1. Failover Mechanism for HaloENGINE in HaloCAD for PLM

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

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

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



Failover Mechanism for HaloENGINE in HaloCAD for PLM

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

Failover Mechanism Requirement

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

8.2. 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 Autodesk Vault are shown in the table below.

Library	Version	Source Code	License Link
HTTP-Proxy-Servlet		https://github.com/mitre/HTTP-Proxy-Servlet	https://github.com/mitre/HTTP-Proxy-Servlet/blob/master/LICENSE.txt
httpmime	4.5.+	https://mvnrepository.com/artifact/org.apache.httpcomponents/httpmime	http://www.apache.org/licenses/LICENSE-2.0.txt
javax.mail	1.4.1	https://mvnrepository.com/artifact/javax.mail/mail	Common Development and Distribution License (CDDL) v1.0 https://glassfish.dev.java.net/public/CDDLv1.0.html
commons-io	2.+	https://mvnrepository.com/artifact/commons-io/commons-io	https://www.apache.org/licenses/LICENSE-2.0.txt
javax.servlet-api	3.1.+	https://mvnrepository.com/artifact/javax.servlet/javax.servlet-api	https://glassfish.dev.java.net/nonav/public/CDDL+GPL.html
jna	5.8.0	https://mvnrepository.com/artifact/net.java.dev.jna/jna	http://www.apache.org/licenses/LICENSE-2.0.txt http://www.gnu.org/licenses/licenses.html
jna-platform	5.8.0	https://mvnrepository.com/artifact/net.java.dev.jna/jna-platform	http://www.apache.org/licenses/LICENSE-2.0.txt http://www.gnu.org/licenses/licenses.html
activation	1.1.1	https://mvnrepository.com/artifact/javax.activation/activation	https://glassfish.dev.java.net/public/CDDLv1.0.html

Library	Version	Source Code	License Link
jaxws-api	2.3.1	https://mvnrepository.com/artifact/javax.xml.ws/jaxws-api	https://github.com/javaee/jax-ws-spec/blob/master/LICENSE.md
jaxws-ri	4.0.1	https://mvnrepository.com/artifact/com.sun.xml.ws/jaxws-ri/4.0.1	https://oss.oracle.com/licenses/CDDL+GPL-1.1
rt	2.3.0	https://mvnrepository.com/artifact/com.sun.xml.ws/rt	https://oss.oracle.com/licenses/CDDL+GPL-1.1
stax2-api	4.0.0	https://mvnrepository.com/artifact/org.codehaus.woodstox/stax2-api	http://www.opensource.org/licenses/bsd-license.php

Open-source software

8.3. Metadata

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

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

Autodesk Vault Metadata

8.4. Download Log Definition

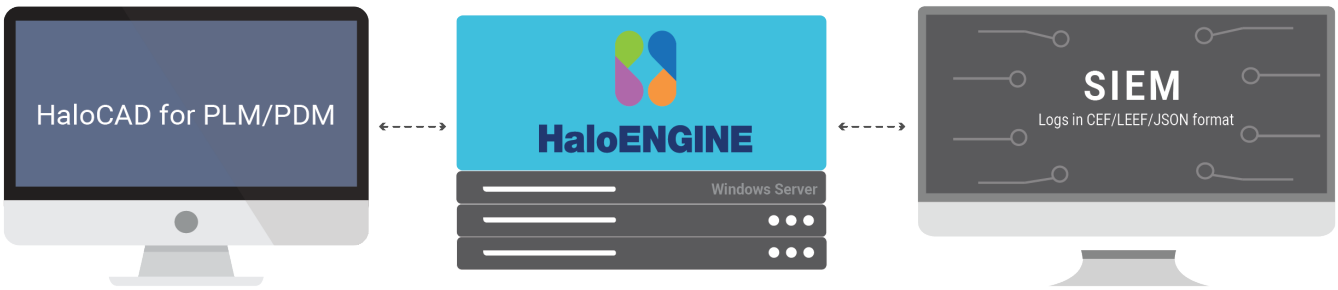
This section explains the log definition for every log format that HaloENGINE supports.

8.4.1. What is SIEM Integration?

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

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

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



Forwarding logs

8.4.2. Why CEF Standard?

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

Syslog and CEF Header

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

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

CEF format

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

CEF format sample

Format	Description	Example
Prefix	Syslog applies a prefix to each message, no matter which device it arrives from, that contains the date and hostname.	`10:29:48.486`
Header	Version is an integer and identifies the version of the CEF format. The current CEF version is 0 (CEF:0).	`CEF:0`
	Device Vendor, Device Product, and Device Version are strings that uniquely identify the type of sending device.	`|Secude|HaloCAD|6.7.0.0|`
	• 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)

Format	Description	Example
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

```
22:15:39.569 CEF:0|Secude|HaloCAD|6.7.0.0|100|user
download|1|deviceCustomDate1Label=exportTime deviceCustomDate1=Aug 23 2024 05:20:42
UTC externalId=BF735B9B56B7450D88AEBE6C387E2229 deviceCustomDate2Label=logTime
deviceCustomDate2=Aug 23 2024 05:15:39 UTC act=unblocked;labeled;protected
fname=Inventorlog.txt filePath=$/DOCS/Inventorlog.txt fileType=txt fsize=275787
in=310655 shost=vault duser=Administrator,type:Administrator;Security
Administrator;Change Order Editor (Level 1);Admin;Product Manager dst=10.41.0.253
requestClientApplication=[null] cs2Label=DataDestination cs2=[ platform\=[Windows NT],
browser\=[VP], browser_version\=[null], device_type\=[null],
terminal_id\=[10.41.0.253], destination_attributes\=[{ key\=[client_ip],
value\=[10.41.0.253], type\=[null] }, { key\=[client_host], value\=[10.41.0.253],
type\=[null] }] ] cs3Label=DataOrigin cs3=[ source_type\=[PLM], system_name\=[vault],
plm_info\=[{ key\=[document_id], value\=[52450], type\=[null] }, {
key\=[document_type], value\=[txt], type\=[null] }, { key\=[document_number],
value\=[52450], type\=[null] }, { key\=[document_version], value\=[1], type\=[null]
}]] cs4Label=ClassifyProtectionData cs4=[ policy_id\=[d7e95033-e7f1-4218-8941-
7d60d8e9cf69], policy_name\=[CADSecured], policy_type\=[company_policy],
error\=[false], author\=[HALOCORE Service] ]
```

CEF sample

8.4.3. Why LEEF Standard?

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

Syslog and LEEF Header

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

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

LEEF format

```
22:33:59.265 LEEF:2.0|Secude|HaloCAD|6.7.0.0|100|^|exportTime=Aug 23 2024 05:39:01
UTC^eventName=user download^externalId=BD0B92DF9C39460D8BC5EADF67E03041^logTime=Aug 23
2024 05:33:59
UTC^act=unblocked;labeled;protected^fname=Inventorlog.txt^filePath=$/DOCS/Inventorlog.
txt^ftype=txt^fsize=275787^fdwnsize=310655^shost=vault^usrName=Administrator,type:Admi
nistrator;Security Administrator;Change Order Editor (Level 1);Admin;Product
Manager^dst=10.41.0.253^usrAgent=[null]^dataDestination=[ platform=[Windows NT],
browser=[VP], browser_version=[null], device_type=[null], terminal_id=[10.41.0.253],
destination_attributes=[ {key=[client_ip], value=[10.41.0.253], type=[null]},
{key=[client_host], value=[10.41.0.253], type=[null]} ] ]^dataOrigin=[
source_type=[PLM], system_name=[vault], plm_info=[ {key=[document_id], value=[52450],
type=[null]}, {key=[document_type], value=[txt], type=[null]}, {key=[document_number],
value=[52450], type=[null]}, {key=[document_version], value=[1], type=[null]} ]
]^classifyProtectionData=[ policy_id=[d7e95033-e7f1-4218-8941-7d60d8e9cf69],
policy_name=[CADSecured], policy_type=[company_policy], extendedTags=[
message=[Success] ], error=[false], author=[HALOCORE Service] ]
```

LEEF sample

Format	Description	Example
Syslog Header	The Syslog header contains the timestamp.	`17:10:28.743`

Format	Description	Example
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).
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

8.4.4. Why JSON Standard?

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

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

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


```
00:25:43.525
{"log_id":"3206B00A024E44C7BE398ACE213FF26B","product":"HaloCAD","source_host":{"shost
":"vault"},"protection":{"policy_id":"d7e95033-e7f1-4218-8941-
7d60d8e9cf69","extended_tags":[{"value":"Success","key":"message"}],"policy_name":"CAD
Secured","error":false},"destination_info":{"hostname":"10.41.0.253","destination_attr
ibutes":[{"value":"10.41.0.253","key":"client_ip"},{"value":"10.41.0.253","key":"clien
t_host"}],"destination_ip":"10.41.0.253","os":"Windows
NT","recipients":[],"browser":"VP","device_type":"null","browser_version":"null","user
_agent":"null"},"classification":{"classification_by_system":[],"classification_by_use
r":[]},"version":"6.7.0.0","log_time":"Aug 23 2024 07:25:43
UTC","event_id":100,"data_origin":{"generic_info":"null","sap_info":"null","system_nam
e":"vault","pre_process_info":[],"source_type":"PLM","plm_info":[{"value":"52450","key
":"document_id"},{"value":"txt","key":"document_type"},{"value":"52450","key":"documen
t_number"},{"value":"1","key":"document_version"}],"bi_info":"null"},"user_info":{"use
r_email":"HALOCORE
Service","user_type":"null","user_name":"null"},"file_info":{"file_path":"$/DOCS/Inven
torlog.txt","file_name":"Inventorlog.txt","file_type":"txt","download_file_size":31065
5,"original_file_size":275787},"action":["unblocked","labeled","protected"],"export_ti
me":"Aug 23 2024 07:30:45 UTC","event":"user download"}
```

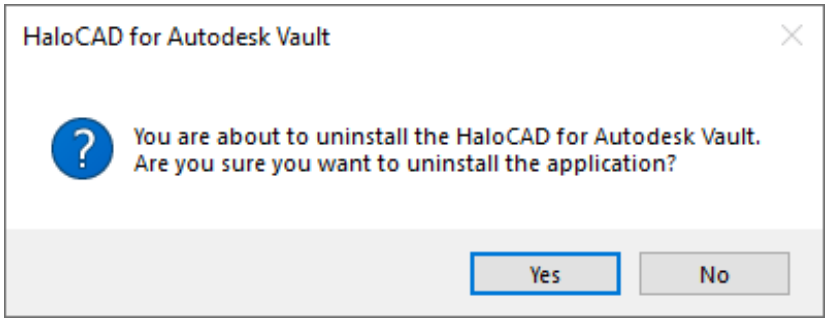

JSON sample

8.5. Uninstalling the HaloCAD for Autodesk Vault

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

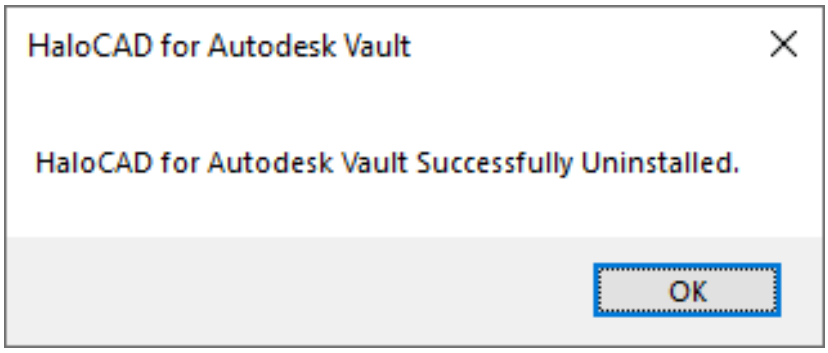
Method #1

1. Click **Start** menu > go to **Control Panel** > **Programs** > **Programs and Features** > **Uninstall a Program** > select **HaloCAD for Autodesk Vault** application from the list > right-click and select **Uninstall** option or double-click on the installer `HaloCAD_Autodesk_Vault_Setup.exe` file.
2. Depending on your Windows security settings, you may get a security warning as "*Do you want to allow the following program to make changes to this computer*?". If you get this security warning, click the **Yes** button to confirm that you want to uninstall the HaloCAD component.
3. The following confirmation message will appear.



Uninstall Message #1

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



Uninstall Message #2

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

Method #2

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

1. Open a command prompt.

2. Navigate to the HaloCAD component's directory.

   Example: `HaloCAD_Autodesk_Vault_Setup.exe -uninstall`

3. The uninstalling process is complete.

Index

Secude

www.secude.com

About Secude

Secude, a 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.