Secude

HaloCAD

HaloCAD for SOLIDWORKS PDM

Installation Manual

Version 1.6

Copyright

Contact

Secude Solutions AG

Murbacherstrasse 19

6003 Luzern, Switzerland

Mail: info@secude.com

Support

Web: https://support.secude.com

Mail: support@secude.com

Table of Contents

Typographic Conventions

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

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

1. Introduction

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

1.1. How does HaloCAD for SOLIDWORKS PDM protect your Data??

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

Files in SOLIDWORKS PDM folders are closely monitored. When a file is cut or copied to a non-SOLIDWORKS PDM folder, HaloCAD intercepts it and protects it in the background on the fly before reaching the destination folder. Furthermore, any previously protected SOLIDWORKS application files or PDF files copied to the SOLIDWORKS PDM folder will be decrypted and saved. Thus, the data is always secure, no matter where the file is saved outside of SOLIDWORKS PDM. The cut or copy events are monitored and logged in a log file.

1.2. About this Manual

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

Reference

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

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

1.3. Reference Manuals

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

For information on	Refer to
Step 1: For details on supported operating systems, file types, and CAD applications, see the Release Notes.	`HaloCAD_SOLIDWORKSPDM_ReleaseNotes_EN_Online.pdf`
Step 2: Prerequisites 1. Before installing, it is recommended that you fulfill the prerequisites, such as registering an application in Microsoft Entra ID. 2. HaloCAD Architecture 3. Registering an Application in Microsoft Entra ID - Public client/native 4. Office 365 Subscription Details 5. Recommended URLs, Addresses, and Ports for MPIP 6. Enable Support for TLS 1.2 at the Client Workstation for Microsoft Entra ID 7. Secure Installation (Recommended)	`HaloCAD_Technical_Reference_Manual_EN_Online.pdf`
Step 3: Install HaloCAD Add-on for SOLIDWORKS	`HaloCAD_SOLIDWORKS_Manual_Installation_EN_Online.pdf`
Step 4: Install and configure HaloENGINE	`HaloENGINE_Manual_Installation_EN_Online.pdf`
Step 5: Install and configure HaloCAD for SOLIDWORKS PDM	`Refer to the current manual.`
Step 6: Workflow illustrating protection and decryption	`HaloCAD_SOLIDWORKS_Manual_Operations_EN_Online.pdf`

HaloCAD reference documentation

1.4. Component Functions

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

1. HaloCAD Add-on for SOLIDWORKS
2. HaloCAD for SOLIDWORKS PDM
3. HaloENGINE
4. Microsoft Purview Information Protection

The following list outlines the functions of each component.

HaloCAD for SOLIDWORKS PDM performs the following functions:

1. Resides on the server hosting SOLIDWORKS PDM Client.
2. Watches user-initiated cut, copy, paste, and Send to events in Windows File Explorer (`explorer.exe`).
3. Collects metadata for the user-selected file.
4. Obtains action and label information for the user-selected file from HaloENGINE for file processing.
5. Responsible for labeling and encrypting files.
6. Logs HaloCAD for SOLIDWORKS PDM component activities to the local log and sends monitor logs to the HaloENGINE.

HaloCAD Add-on for SOLIDWORKS performs the following functions:

1. Operates within the Dassault Systèmes SOLIDWORKS application.
2. It is responsible for protecting newly created files that are exported or saved to non-SOLIDWORKS PDM folders and displaying the permission label with enforcement.
3. Logs all add-on–related activities for auditing purposes.

HaloENGINE performs the following functions:

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

Microsoft Purview Information Protection

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

Microsoft documentation

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

2. 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
SOLIDWORKS PDM	SOLIDWORKS PDM Server: 1. 2022 2. 2024 SP 4.0 3. 2025 SP 1.2 4. SolidNetWork License Manager, version 29.51.0001 Supported SOLIDWORKS PDM Clients: 1. 2022, 2024, 2025 2. Supported Operating System: Windows 11 or above with installed updates.
Supported file types	`.sldprt`, `.sldasm`, `.prt`, `.asm`, `.slddrw`, `.x_t`, `.tif`, `.dwg`, and `.dxf`
Other components	HaloENGINE

Requirements

3. Installing the HaloCAD for SOLIDWORKS PDM

This chapter walks through the process of installing and configuring the HaloCAD for SOLIDWORKS PDM.

3.1. Before you begin

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

1. Ensure that you have administrative access to install the HaloCAD component.
2. Ensure that the client computer running the HaloCAD for SOLIDWORKS PDM can connect to the SOLIDWORKS PDM Server.
3. Ensure that the machine with HaloENGINE installed can reach the machine where HaloCAD for SOLIDWORKS PDM is installed.
4. Ensure that your HaloENGINE meets the requirements listed below:
   a. License file (enabled with SOLIDWORKS_PDM system type).
   b. Proper action rules
   c. System Unique ID (assigned to the specific SOLIDWORKS PDM Server)
   d. Select one of the following approaches for authentication.
      Self-signed Certificate: Download the server certificate (`HaloENGINEServer.cer`) from the HaloENGINE Admin portal and manually install it on the SOLIDWORKS PDM client machine under Trusted Root Certification Authorities, where HaloCAD for SOLIDWORKS PDM is also installed.

      Company-Owned Signed Certificate: If you already have a certificate, you can import it into the admin portal. Please refer to the HaloENGINE Manual for additional details. Make sure your company's Root CA is installed in Trusted Root Certification Authorities. In this case, there is no need to install the server certificate (`HaloENGINEServer.cer`) on the SOLIDWORKS PDM client machine.
5. Ensure that both HaloCAD for SOLIDWORKS PDM and HaloENGINE are installed with the same Directory (Tenant) ID. A mismatch in the Directory (Tenant) ID will result in configuration errors.
6. Ensure that your Microsoft Entra ID application information is available when the setup process prompts for a manual installation. Alternatively, for a safe and automatic installation, use `hc.conf.enc`. For more details, please refer to the Technical Reference Manual.

3.2. Installation Modes

You can install the add-on 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**

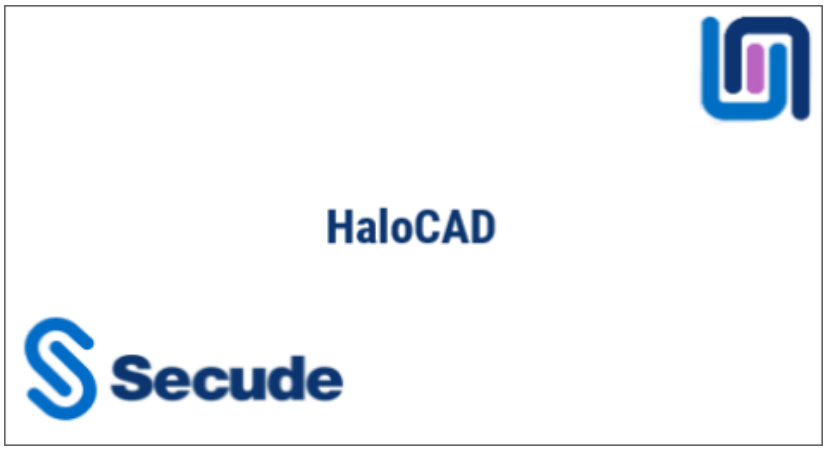
   Silent-mode installation is a non-interactive method of installing HaloCAD using command lines.

3.2.1. Graphical Mode

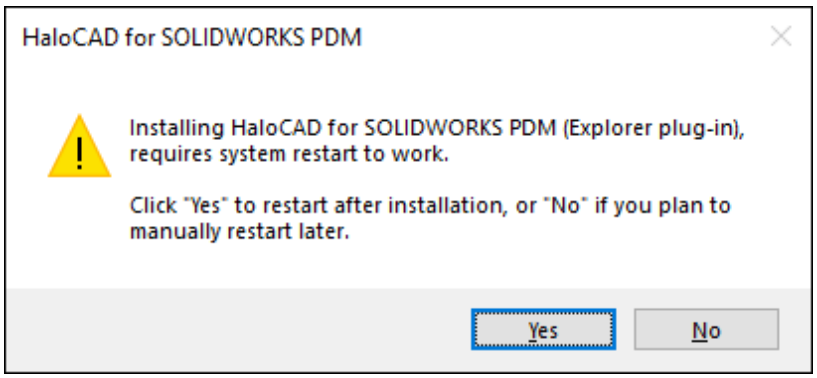
Installation Procedure

Follow the steps below to install SOLIDWORKS PDM using the GUI-based setup application included in the installation package.

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



Startup dialog

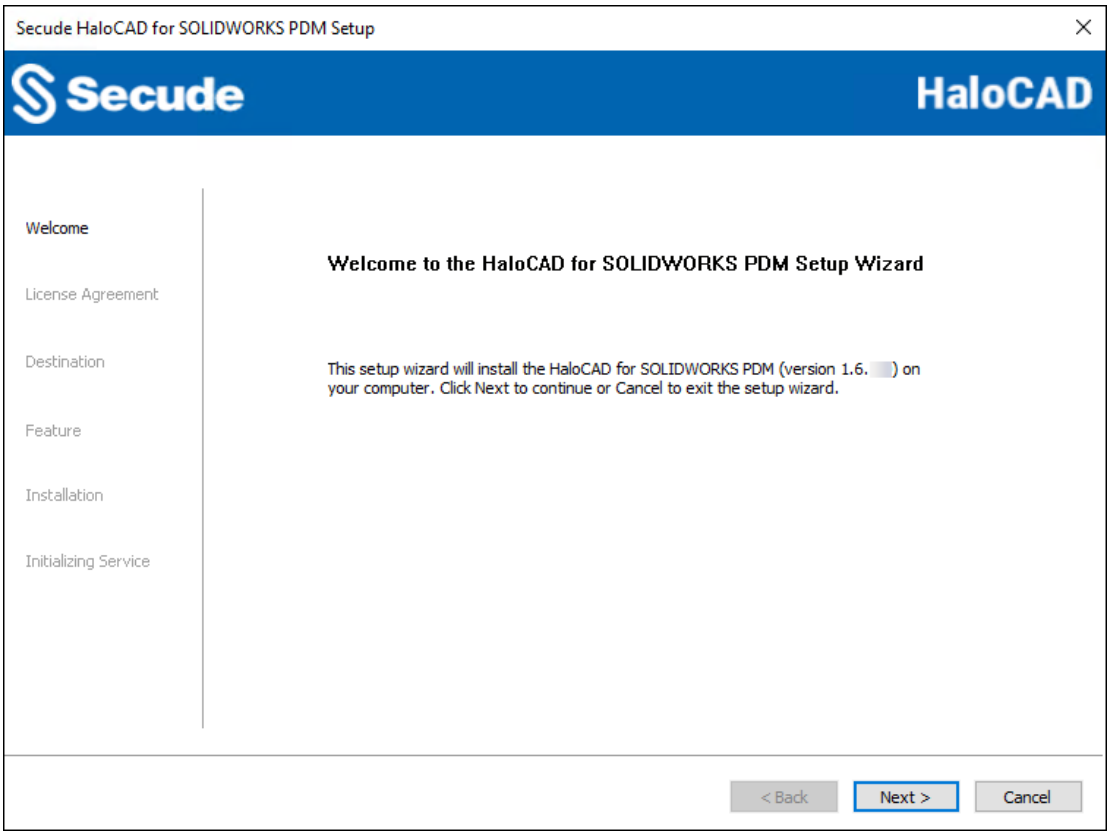


Restart message

4. To activate the HaloCAD component (Explorer plug-in), you must restart your computer after installation. When prompted, choose one of the following options:
   a. **Yes** – The computer will restart automatically after the HaloCAD component is installed.
   b. **No** – The HaloCAD component will be installed, but you must restart the computer manually later.

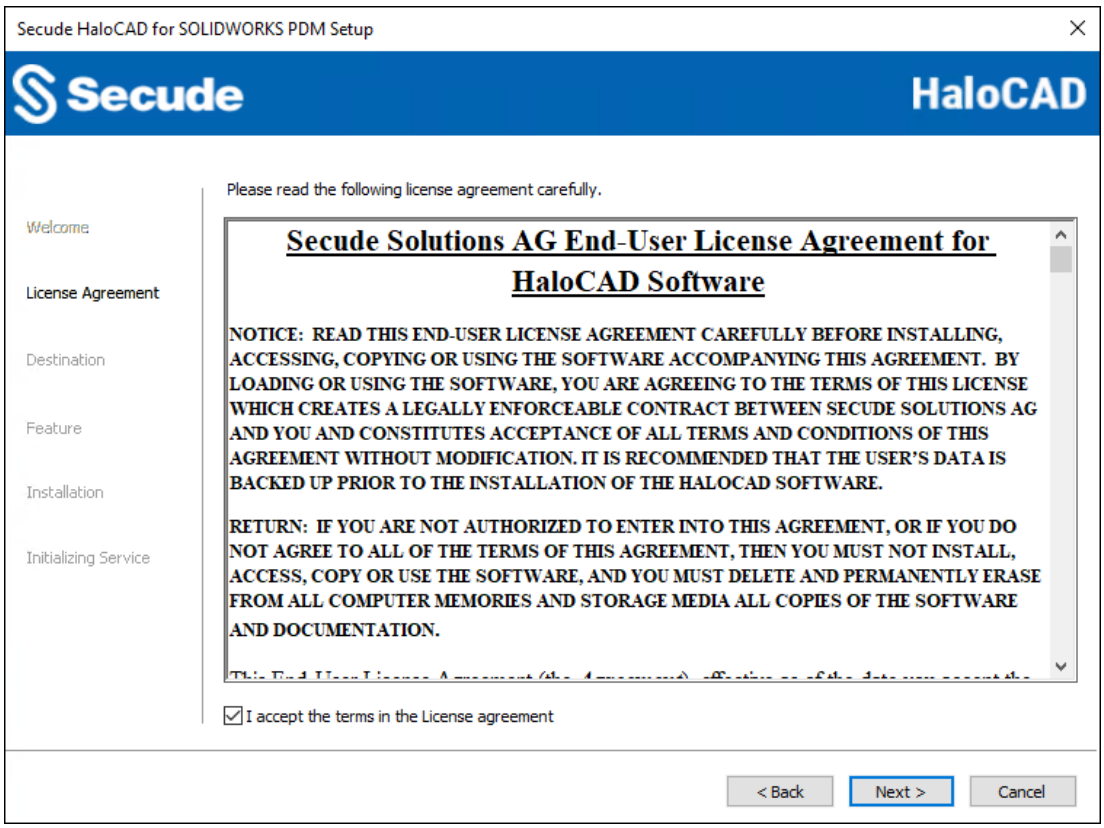
Note: The HaloCAD component becomes active only after the system is restarted.

5. After choosing an option in the restart prompt, the **Welcome** dialog appears.



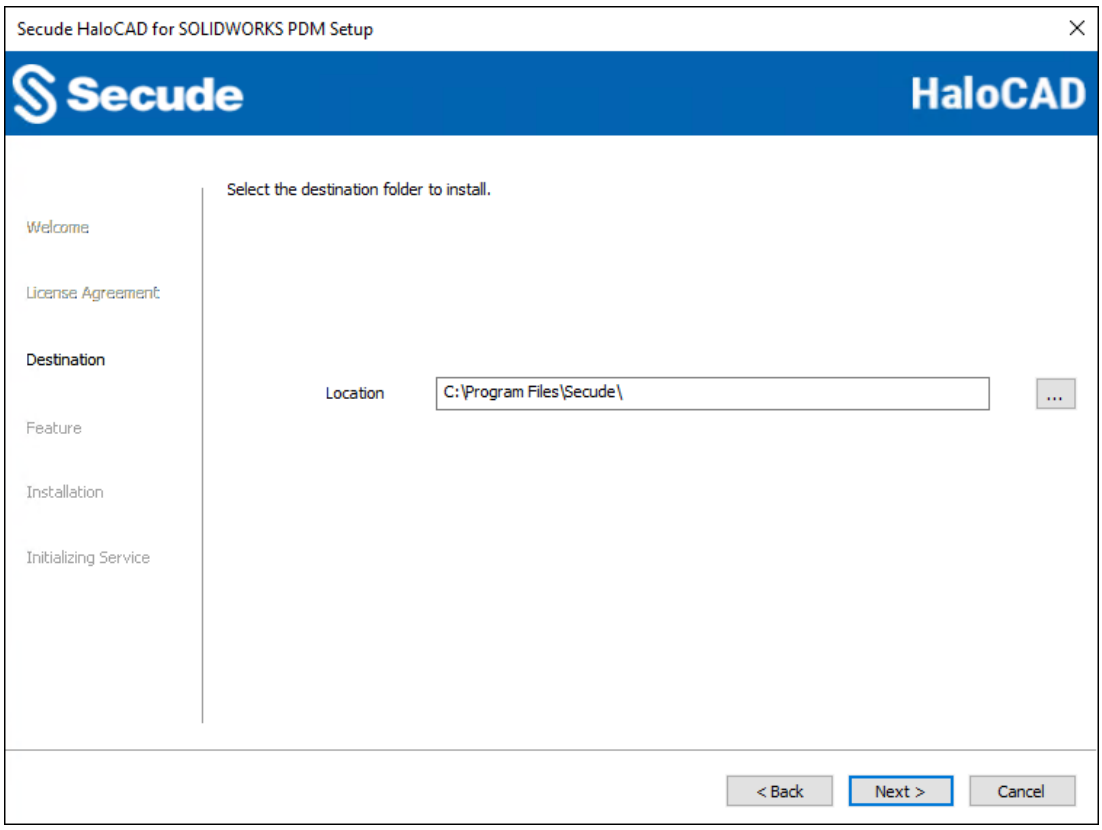
Welcome dialog

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



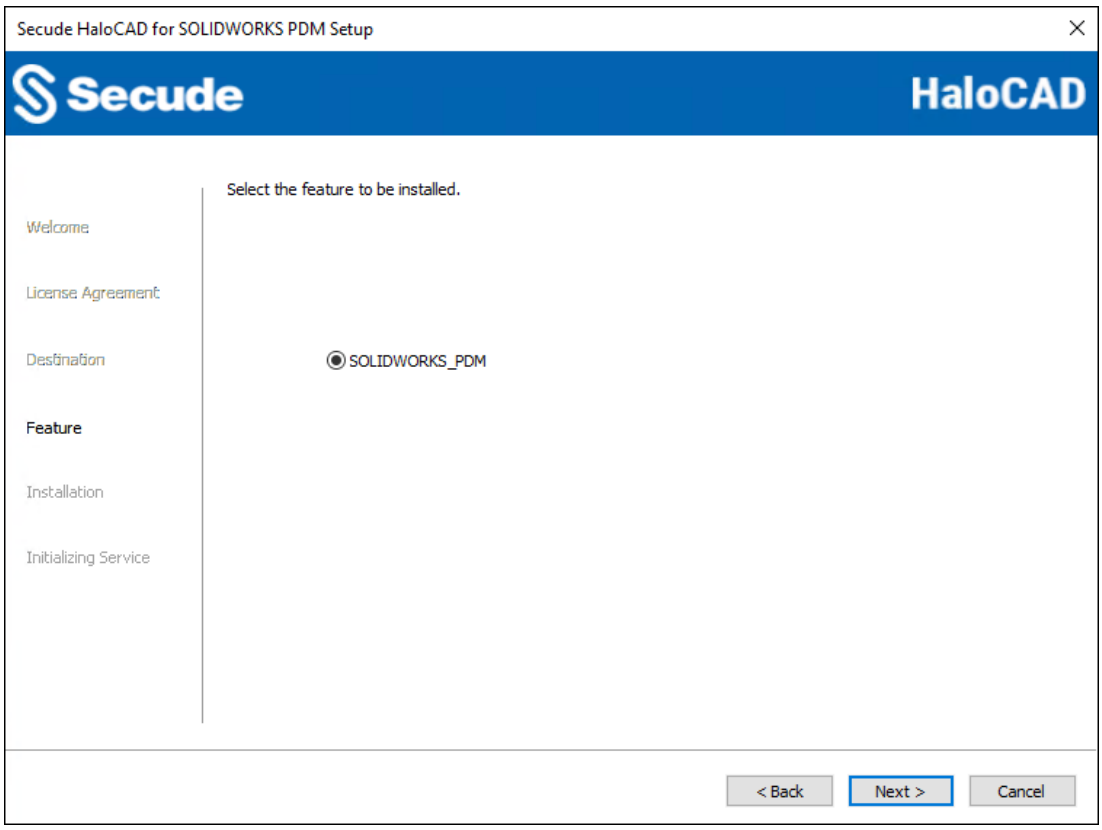
End-User License Agreement dialog

8. Read the **End-User License Agreement**. If you agree, select **I accept the terms in the License Agreement**, and click **Next** to continue.
9. The destination folder selection dialog appears:



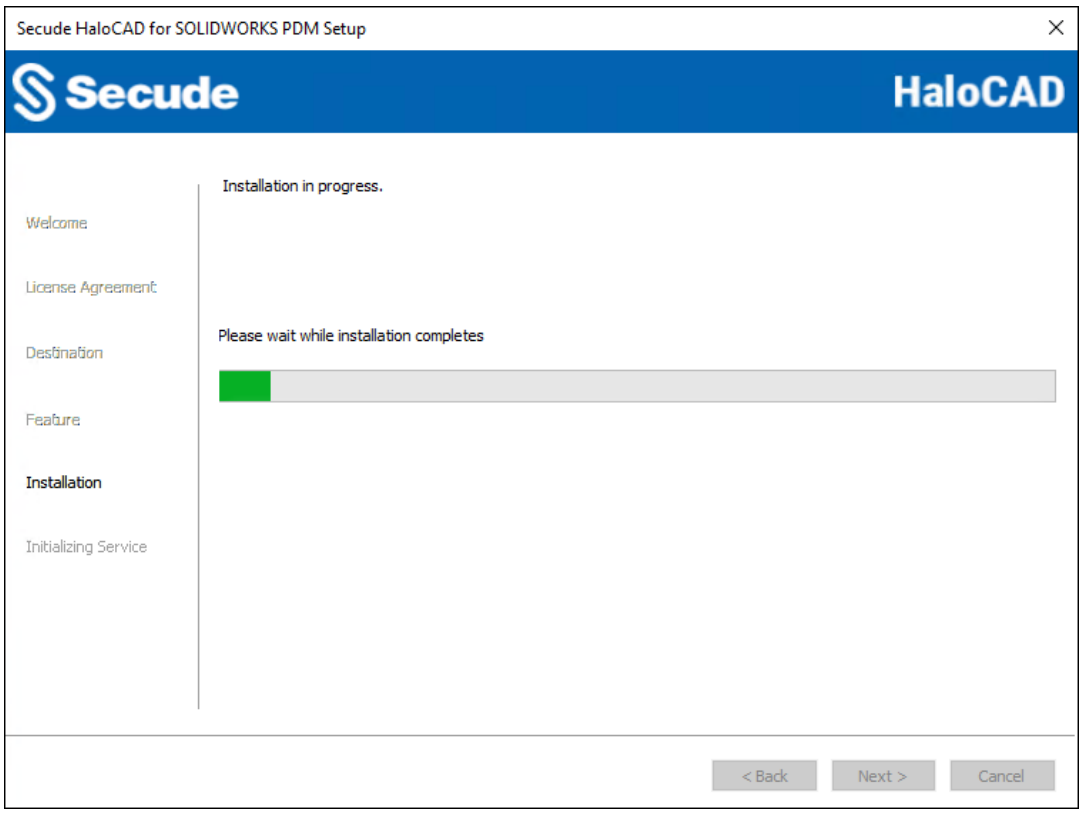
Destination folder selection dialog

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. When you are finished, click **Next**.
11. The feature selection dialog appears.



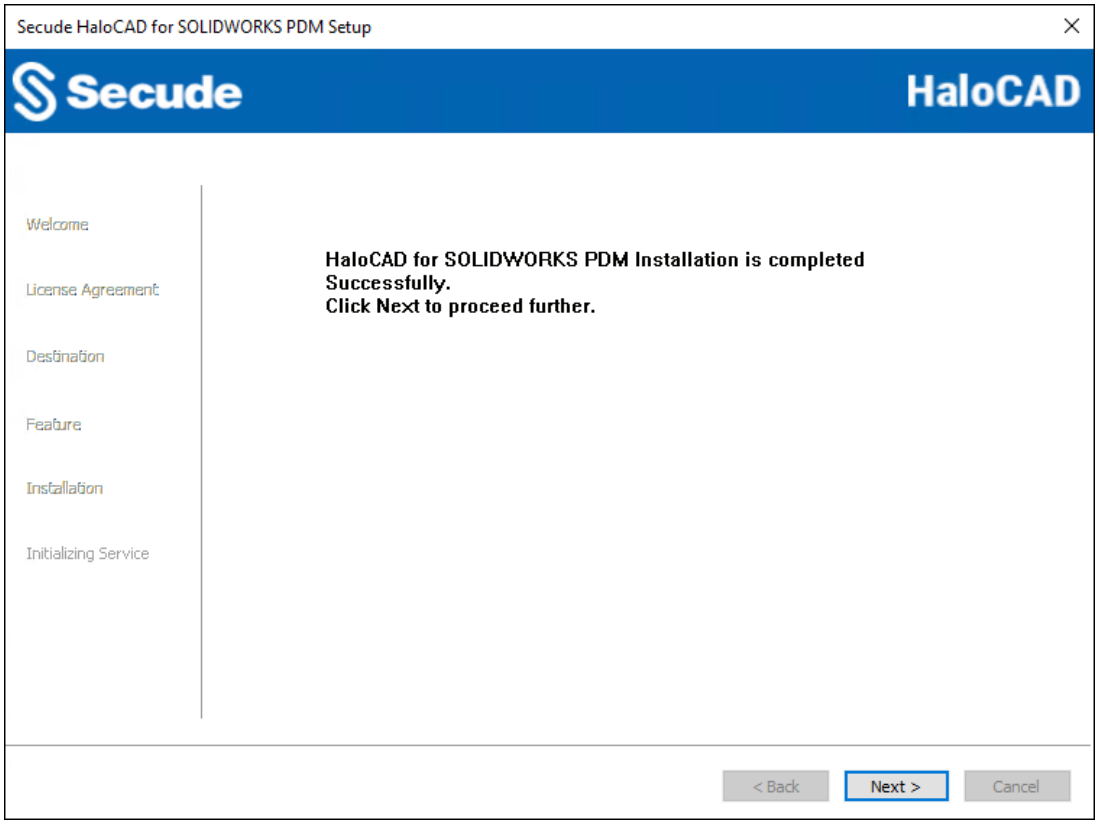
Feature selection dialog

12. By default, the **SOLIDWORKS_PDM** option is selected.
13. To review or change settings, click **Back** to return to a previous step in the installation process. Otherwise, click **Next** to begin installing the application. To cancel the installation at this stage, click **Cancel**.
14. The installation begins, and the progress is displayed in the dialog.



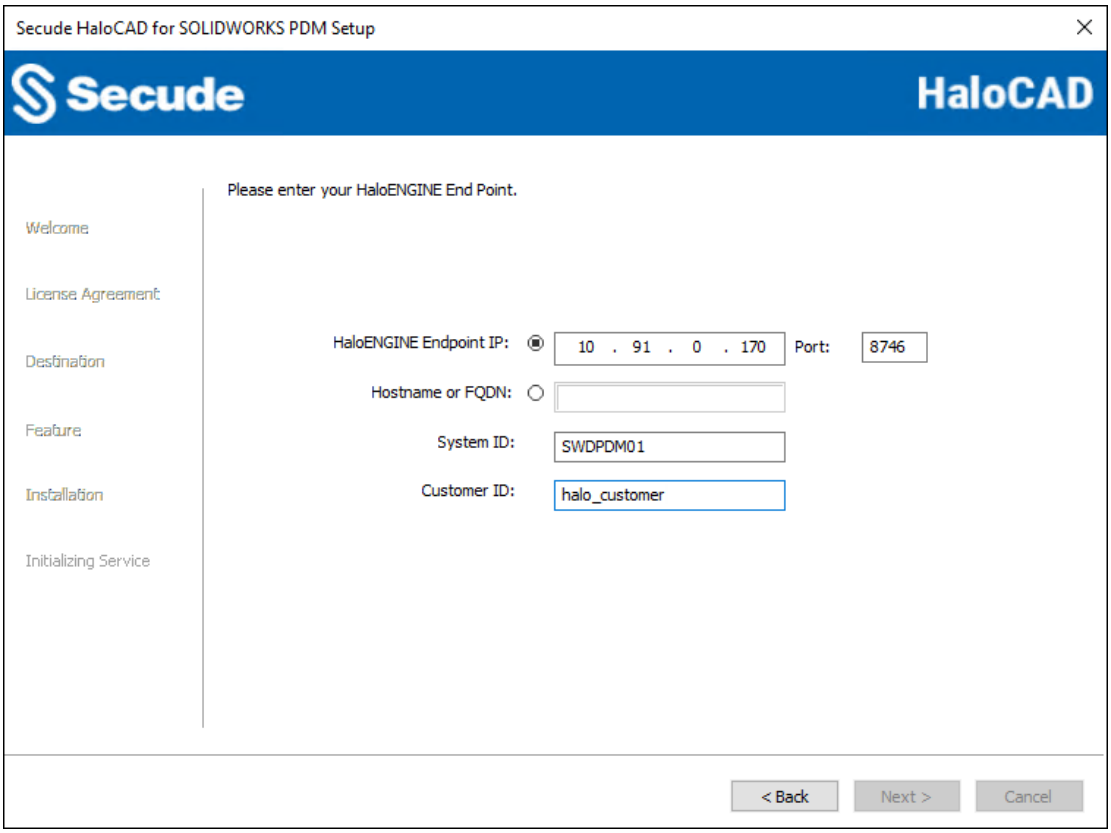
Installation progress dialog

15. When the installation is complete, a message appears confirming that the HaloCAD component has been successfully installed.



Installation completed dialog

16. Click **Next** to display the endpoint dialog.



Endpoint dialog

a. Choose either the IP address or the hostname and provide the relevant information. In the **HaloENGINE Endpoint IP** field, type the HaloENGINE's IP address. For example, 10.91.0.170. Alternatively, type the fully qualified domain name (FQDN) or hostname into the **Hostname** or **FQDN** fields. For example, `SOLIDWORKSServer01.secude.com`. The default port number **8746** will be displayed; however, you can enter your HaloENGINE port number instead.

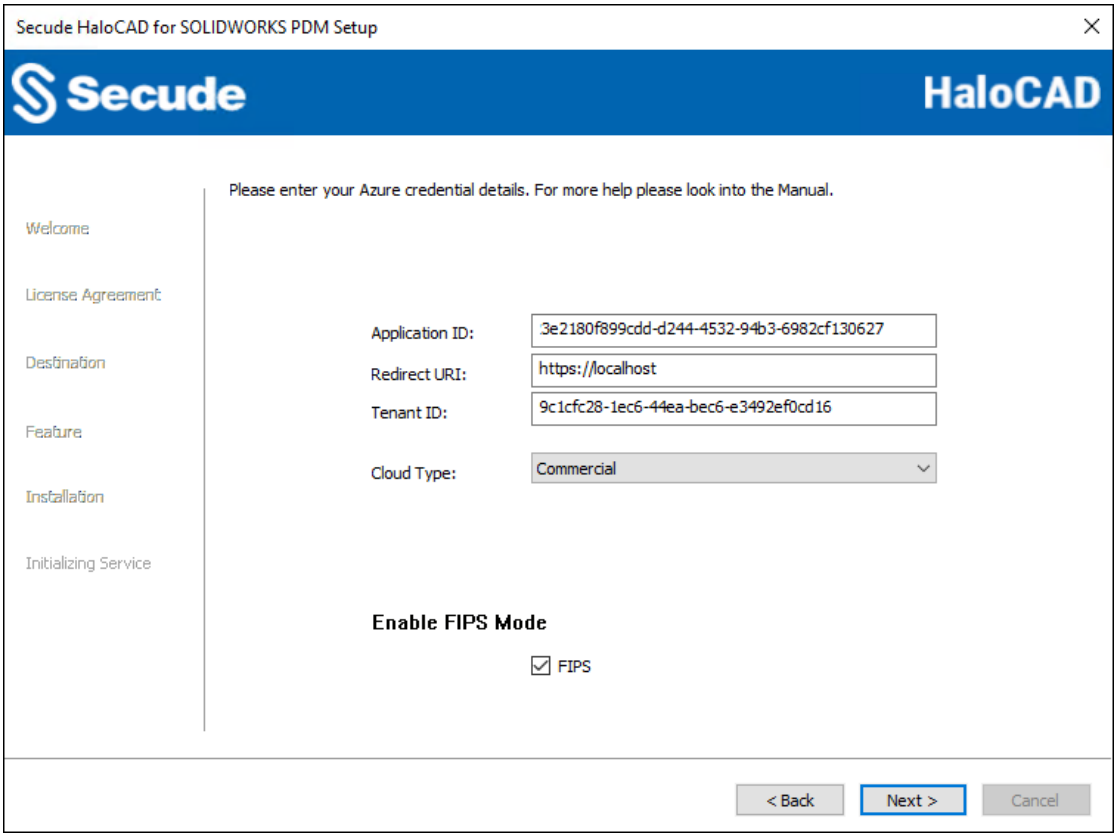
b. Enter the unique ID of SOLIDWORKS PDM in the **System ID**, which is assigned in the HaloENGINE Admin Portal. For example, `SWDPDM01`.

c. Enter the **Customer ID** that is assigned in the admin portal. For example, `halo_customer`.

d. At this stage, HaloCAD attempts to connect to the HaloENGINE. If an invalid endpoint is entered or the HaloENGINE server cannot be reached, the installation is terminated with the error message "*HaloENGINE API endpoint is invalid or not reachable*." In this case, go back to the previous screen, provide a valid endpoint, confirm that the HaloENGINE is reachable, and then select **Next**.

17. The initialization dialog appears. To prevent connectivity issues, ensure that the correct Microsoft Entra ID application details are entered on the screen. Note**:** If the `hc.conf.enc` file is included with

the installer, this initialization screen is skipped and only the completion dialog is shown. The initialization screen appears only when the `hc.conf.enc` file is not present in the installer folder.



Initialization dialog

a. **Application ID**: Enter the unique identifier of your registered application. For example, `v6ca776-c74e-437d-98ef-662ecb5751tt`

b. **Redirect URI**: Enter the URI that was provided when registering the native application in the Azure portal. For example, `https://localhost`.

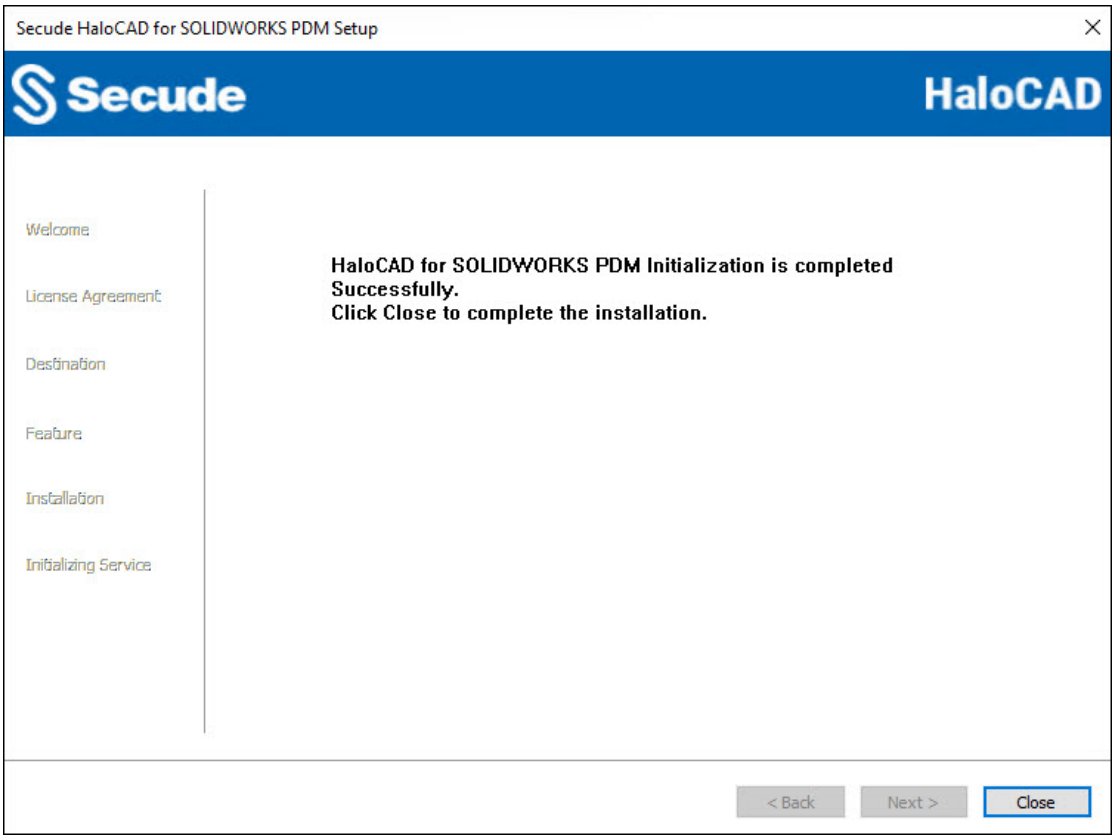
c. **Tenant ID:** If the registered application is **Single tenant**, you need to enter the globally unique identifier of your tenant if not, you can leave it empty. For example, `9c1cfc28-1ec6-44ea-bec6-e3492ef0cd16`

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

e. **Enable Federal Information Processing Standards (FIPS)**: Enable this option to use encryption algorithms that comply with FIPS standards. When enabled, MPIP uses only FIPS-compliant encryption algorithms, and when disabled, it uses standard encryption algorithms. If this option was not enabled during installation, it can later be enabled through a registry entry.

f. Click **Next**.

18. Once the initialization is complete, a success message appears as shown below.



Initialization completed dialog

19. Click **Close** to close the installation wizard.
20. Based on the selected option in the initial prompt displayed when clicking the installer:
    - If you choose **Yes**, your machine will restart automatically.
    - If you choose **No**, you must restart it manually.

Post Installation files

- View log files at: `%AppData%\Roaming\Secude\HaloCAD\SOLIDWORKS PDM\halocad.log`
- HaloCAD stores configuration settings in the Windows registry at `HKEY_LOCAL_MACHINE\SOFTWARE\Secude\HaloCAD for SOLIDWORKS PDM`; do not modify registry values unless required. Only the `enable_fips` setting may be changed (`true`: MPIP uses FIPS-compliant encryption algorithms; `false`: MPIP uses standard encryption algorithms).

- To update HaloENGINE settings (such as endpoints, System ID, or Customer ID), edit: `HKEY_LOCAL_MACHINE\SOFTWARE\Secude\HaloCAD for SOLIDWORKS PDM\ep\HCADSWPDM`
- Back up the registry before modifying any entries.

3.2.2. Silent Mode

Besides graphical mode, the add-on can be installed in silent mode, which does not require user involvement or display a user interface. It is a convenient way to streamline installation using the command at once.

1. Open the Command Prompt with elevated rights (Run as Administrator).
2. Navigate to the add-on installer directory.
3. To know the list of options available in silent mode, follow the steps given below:

   Type `HaloCAD_SWPDM_Setup.exe -help`

   Press `Enter`

   Output

   ...

   ```
   HaloCAD_SWPDM_Setup.exe [-install [-solidworkspdmshield] [-dir
   <destination_directory>]
   [<ApplicationID> <Redirect URI> <TenantID/Name>] <haloengine_api_endpoint>
   <haloengine_api_port> <haloengine_api_SystemId> <haloengine_api_CustomerId>
   <RestartRequired <true|false>> <Cloud Type
   ("Commercial"|"Custom"|"Germany"|"US_DoD"|"US_GCC"|"US_GCC_High"|"US_Sec"|"US_Nat"|"C
   hina_01"|"")>
   [(if Custom) <Protection Cloud Url> <Policy Cloud Url>] [enablefipsmode
   <true|false>]]
   For Silent Mode Installation if ENC file already exists in the same location
   HaloCAD_SWPDM_Setup.exe [-install [-solidworkspdmshield] [-dir
   <destination_directory>] <haloengine_api_endpoint> <haloengine_api_port>
   <RestartRequired <true|false>> <haloengine_api_SystemId> <haloengine_api_CustomerId>
   <enablefipsmode <true|false>>]
   HaloCAD_SWPDM_Setup.exe [-uninstall -silent <true|false>]
   ```

   Note: By selecting `true`, your computer will restart immediately after installing the HaloCAD component. If you select `false`, the HaloCAD component will be installed, but you must restart your computer manually later. Please note that the HaloCAD component becomes active only after a machine restart.

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

   ```
   HaloCAD_SWPDM_Setup.exe -install -solidworkspdmshield -dir "C:\Program Files\Secude"
   v6ca776-c74e-437d-98ef-662ecb5751tt https://localhost 9c1cfc28-1ec6-44ea-bec6-
   e3492ef0cd16 10.41.14.69 8746 SWPDM01 halo_customer true Custom https://api.aadrm.com
   https://dataservice.protection.outlook.com -enablefipsmode true
   ```

5. The example below shows how to install the add-on using the `hc.conf.enc` file located in the same installation location.

   ```
   HaloCAD_SWPDM_Setup.exe -install -solidworkspdmshield -dir "C:\Program Files\Secude"
   10.41.0.116 8746 false SWPDM01 halo_customer -enablefipsmode true
   ```

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

Next Step

After the installation is complete, you can view the HaloCAD-protected files. Please refer to the Operations Manual for more information.

4. Appendix

This section provides supplemental information.

4.1. Third-Party Libraries

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

The third-party libraries and dependencies used by HaloCAD for SOLIDWORKS PDM are shown in the table below.

Library	Version	Source Code	License Link
Mhook	2.5.1	https://github.com/apriorit/mhook	https://github.com/apriorit/mhook#license
Protobuf Library	3.15.6	https://github.com/protocolbuffers/protobuf	https://github.com/protocolbuffers/protobuf/blob/master/LICENSE
JSON Parser	3.11.3	https://github.com/nlohmann/json	https://github.com/nlohmann/json/blob/develop/LICENSE.MIT
OpenSSL	3.4.1	https://github.com/openssl	https://github.com/openssl/openssl/blob/master/LICENSE.txt
tbb	2021.6.0	https://github.com/oneapi-src/oneTBB	https://github.com/dwaddington/tbb-2018/blob/tbb_2018/LICENSE
MSAL	4.72.1	https://github.com/AzureAD/microsoft-authentication-library-for-dotnet	https://github.com/AzureAD/microsoft-authentication-library-for-dotnet/blob/master/LICENSE
WTL	10.0.10320	https://www.nuget.org/packages/wtl/10.0.10320	https://opensource.org/licenses/cpl1.0.txt
MIP SDK	1.18.103	https://learn.microsoft.com/en-us/information-protection/develop/version-release-history	https://docs.microsoft.com/en-us/information-protection/develop/

Third-party libraries

4.2. Metadata Definition

The table below lists the SOLIDWORKS PDM metadata available in the HaloENGINE.

SOLIDWORKS PDM Metadata	Use
author_name	Derivation from the Web2 client interface Items author.
domain_name	Derivation from the network domain name associated with the current user. (For example, `SZVLU100.com`)
file_type	Derivation from file type. File types of SOLIDWORKS.
user_name	Derivation from machine logged-on user. (For example, John and Derek)
client_hostname	Derivation from the computer where SOLIDWORKS PDM is installed. (For example, `SZVLU100.com`)
current_state	Derivation from the file's status as set in SOLIDWORKS PDM. (For example, Approved and Waiting for approval)
project_name	The name of the project from which the saved file is derived. (For example, CMS Turbo Engine)
ad_group	Derivation from the domain groups. (For example, Domain Users and Superusers)
folder_path	Derivation from folder name in SOLIDWORKS PDM server. (For example, `C:/<Folder>`). Please note that files cannot be encrypted if the folder name (`folder_path`) is specified with a backslash "****", such as `C:\folder1\folder2`. Therefore, it is advised to configure with a forward slash "**/**", such as `C:/folder1/folder2`.
preexpression_custom_pre-expression	Derivation from custom pre-expression 1. Yes 2. No

SOLIDWORKS PDM metadata

4.3. Download Log Definition

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

4.3.1. 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

4.3.2. Why CEF Standard?

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

Syslog and CEF Header

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

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

CEF format

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

CEF format sample

Format	Description	Example
Prefix	Syslog applies a prefix to each message, no matter which device it arrives from, that contains the date and hostname.	`10:29:48.486`
Header	Version is an integer and identifies the version of the CEF format. The current CEF version is 0 (CEF:0).	`CEF:0`
	Device Vendor, Device Product, and Device Version are strings that uniquely identify the type of sending device.	`|Secude|HaloCAD|6.10.0.0|`
	• Device Event Class ID is a unique identifier per event-type. • This can be a string or an integer. Device Event Class ID identifies the type of event reported.	`100` (User download)

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

```
08:39:03.330 CEF:0|Secude|HaloCAD|6.10.1.0|999|Export
Event|1|deviceCustomDate1Label=exportTime deviceCustomDate1=Apr 20 2026 06:39:00 UTC
externalId=0DF7C1E33D5F45399B2160CF12AFE58E deviceCustomDate2Label=logTime
deviceCustomDate2=Apr 20 2026 06:39:03 UTC act=unblocked;labeled;protected
fname=Part2.SLDPRT filePath=C:\Vault\TEST2025\PDM fileType=SLDPRT fsize=60007
in=112247 shost=SWPDM_CLIENT_ID duser=secude-swepdm.com\Solidworks,type:SOLIDWORKS_PDM
dst=null requestClientApplication=[null] cs2Label=DataDestination cs2=[
platform\=[Unknown], browser\=[], browser_version\=[null], device_type\=[null],
terminal_id\=[WSLU0305.secude-swepdm.com], destination_attributes\=[] ]
cs3Label=DataOrigin cs3=[ source_type\=[PLM], system_name\=[SWPDM_CLIENT_ID],
client_type\=[SOLIDWORKS_PDM], plm_info\=[{ key\=[project_name], value\=[], type\=[]
}, { key\=[current_state], value\=[Under Editing], type\=[] }, { key\=[author_name],
value\=[Admin], type\=[] }, { key\=[ad_group], value\=[], type\=[] }]]
cs4Label=ClassifyProtectionData cs4=[ policy_id\=[d7e95033-e7f1-4218-8941-
7d60d8e9cf69], policy_name\=[CADSecured], policy_type\=[company_policy],
error\=[false], author\=[HaloCAD SOLIDWORKS PDM] ]
```

CEF sample

4.3.3. 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

```
08:46:36.432 LEEF:2.0|Secude|HaloCAD|6.10.1.0|999|^|exportTime=Apr 20 2026 06:46:34
UTC^eventName=Export Event^externalId=C1F399AD53FD44CCB48E844476B749DA^logTime=Apr 20
2026 06:46:36
UTC^act=unblocked;labeled;protected^fname=Part2.SLDPRT^filePath=C:\Vault\TEST2025\PDM^
ftype=SLDPRT^fsize=60007^fdwnsize=112247^shost=SWPDM_CLIENT_ID^usrName=secude-
swepdm.com\Solidworks,type:SOLIDWORKS_PDM^dst=null^usrAgent=[null]^dataDestination=[
platform=[Unknown], browser=[], browser_version=[null], device_type=[null],
terminal_id=[WSLU0305.secude-swepdm.com] ]^dataOrigin=[ source_type=[PLM],
system_name=[SWPDM_CLIENT_ID], client_type=[SOLIDWORKS_PDM], plm_info=[
{key=[project_name], value=[], type=[]}, {key=[current_state], value=[Under Editing],
type=[]}, {key=[author_name], value=[Admin], type=[]}, {key=[ad_group], value=[],
type=[]} ] ]^classifyProtectionData=[ policy_id=[d7e95033-e7f1-4218-8941-
7d60d8e9cf69], policy_name=[CADSecured], policy_type=[company_policy], error=[false],
author=[HaloCAD SOLIDWORKS PDM] ]
```

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 versions of the LEEF format that is used for the event, for example, `LEEF:2.0|Vendor|Product|Version|EventID|`
	Product name	A text string that identifies the product that sends the event log to QRadar, for example, `LEEF:2.0|Secude|HaloCAD|6.10.0.0|100|`
	Product version	A string that identifies the version of the software or appliance that sends the event log, for example, `LEEF:2.0|Secude|HaloCAD|6.10.0.0|100|`
	EventID	A unique identifier for an event.
	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

4.3.4. Why JSON Standard?

The JSON format is a lightweight text-based interchange format used for serializing and transmitting structured data over a 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).

```
08:54:54.906
{"log_id":"9190E95919EB46B4B501B445463C5BE3","product":"HaloCAD","source_host":{"shost
":"SWPDM_CLIENT_ID"},"protection":{"policy_id":"d7e95033-e7f1-4218-8941-
7d60d8e9cf69","extended_tags":[],"policy_name":"CADSecured","error":false},"destinatio
n_info":{"hostname":"WSLU0305.secude-
swepdm.com","destination_attributes":[],"destination_ip":"null","os":"Unknown","recipi
ents":[],"browser":"null","device_type":"null","browser_version":"null","user_agent":"
null"},"classification":{"classification_by_system":[],"classification_by_user":[]},"v
ersion":"6.10.1.0","log_time":"Apr 20 2026 06:54:54
UTC","event_id":999,"data_origin":{"generic_info":"null","sap_info":"null","system_nam
e":"SWPDM_CLIENT_ID","pre_process_info":[],"source_type":"PLM","client_type":"SOLIDWOR
KS_PDM","plm_info":[{"type":"","value":"","key":"project_name"},{"type":"","value":"Un
der
Editing","key":"current_state"},{"type":"","value":"Admin","key":"author_name"},{"type
":"","value":"","key":"ad_group"}],"bi_info":"null"},"user_info":{"user_email":"HaloCA
D SOLIDWORKS PDM","user_type":"SOLIDWORKS_PDM","user_name":"secude-
swepdm.com\\Solidworks"},"file_info":{"file_path":"C:\\Vault\\TEST2025\\PDM","file_nam
e":"Part2.SLDPRT","file_type":"SLDPRT","download_file_size":112247,"original_file_size
":60007},"action":["unblocked","labeled","protected"],"export_time":"Apr 20 2026
06:54:52 UTC","event":"Export Event"}
```

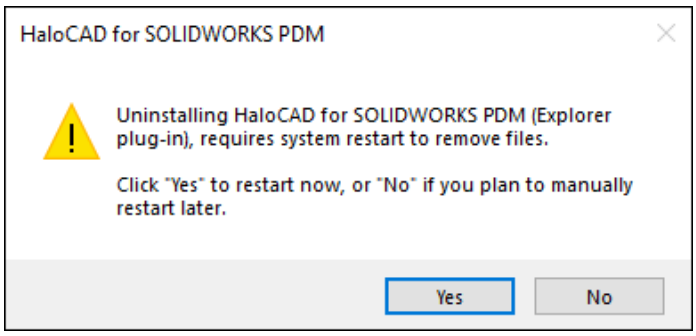

JSON sample

4.4. Uninstalling the HaloCAD for SOLIDWORKS PDM

When you no longer use HaloCAD for SOLIDWORKS PDM, you may uninstall the application. Uninstalling removes all files and registry settings that were added to your computer during the initial installation.

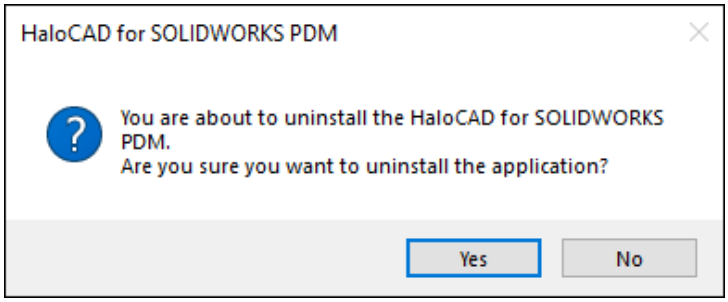
Method #1

1. Click **Start** menu > go to **Control Panel** > **Programs** > **Programs and Features** > **Uninstall a Program** > select **HaloCAD for SOLIDWORKS PDM** application from the list > right-click and select **Uninstall** option or double-click on the installer `HaloCAD_SWPDM_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 add-on.
3. The warning message shown below will appear.



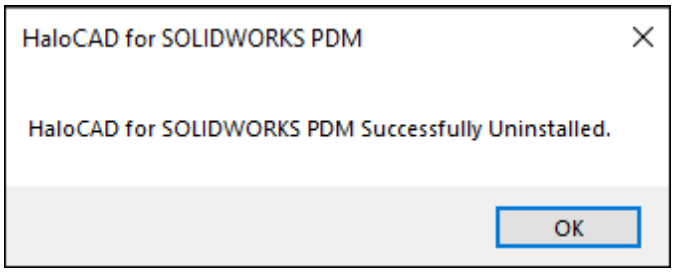
Uninstall Message #1

4. Uninstalling HaloCAD for SOLIDWORKS PDM (Explorer plug-in) requires your computer to restart to confirm that all files have been completely removed.
    a. By selecting **Yes**, your computer will restart immediately after removing the HaloCAD component.
    b. By selecting **No**, the HaloCAD component will be uninstalled, but you must restart your computer manually later.
5. The following notification will ask you to confirm the uninstall, whether you have chosen **Yes** or **No** in the previous message.



Uninstall Message #2

6. Click **Yes** to begin the uninstallation. If you choose **No**, the uninstalling process will end.
7. The following confirmation message appears.



Uninstall Message #3

8. The HaloCAD component has been uninstalled successfully. Click **OK** to close the dialog.
9. Please be patient while your system restarts.

Method #2

The following is an example of uninstalling the HaloCAD for SOLIDWORKS PDM using the command line.

1. Open a command prompt.
2. Navigate to the add-on installer directory.

   Example: `HaloCAD_SWPDM_Setup.exe -uninstall -silent true`
3. The uninstalling process is complete.

Index

www.secude.com

About Secude

Secude, a trusted Microsoft and Siemens Digital Industries Software partner, is a global leader in Zero Trust data protection and data governance.

Our solutions extend Microsoft Purview Information Protection (MPIP) to secure sensitive files—including CAD and PLM assets—from the moment of creation. By embedding persistent protection and access controls directly into design and engineering data, we help enterprises prevent Intellectual Property (IP) theft, data leakage, reputational damage, and compliance risks. With operations in Europe, North America, and Asia, Secude supports global manufacturers, defense contractors, and AEC firms in implementing robust IT security strategies across the product lifecycle and digital supply chain.