Secude

HaloCAD

HaloCAD for SOLIDWORKS PDM 1.3

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 SOLIDWORKS PDM?

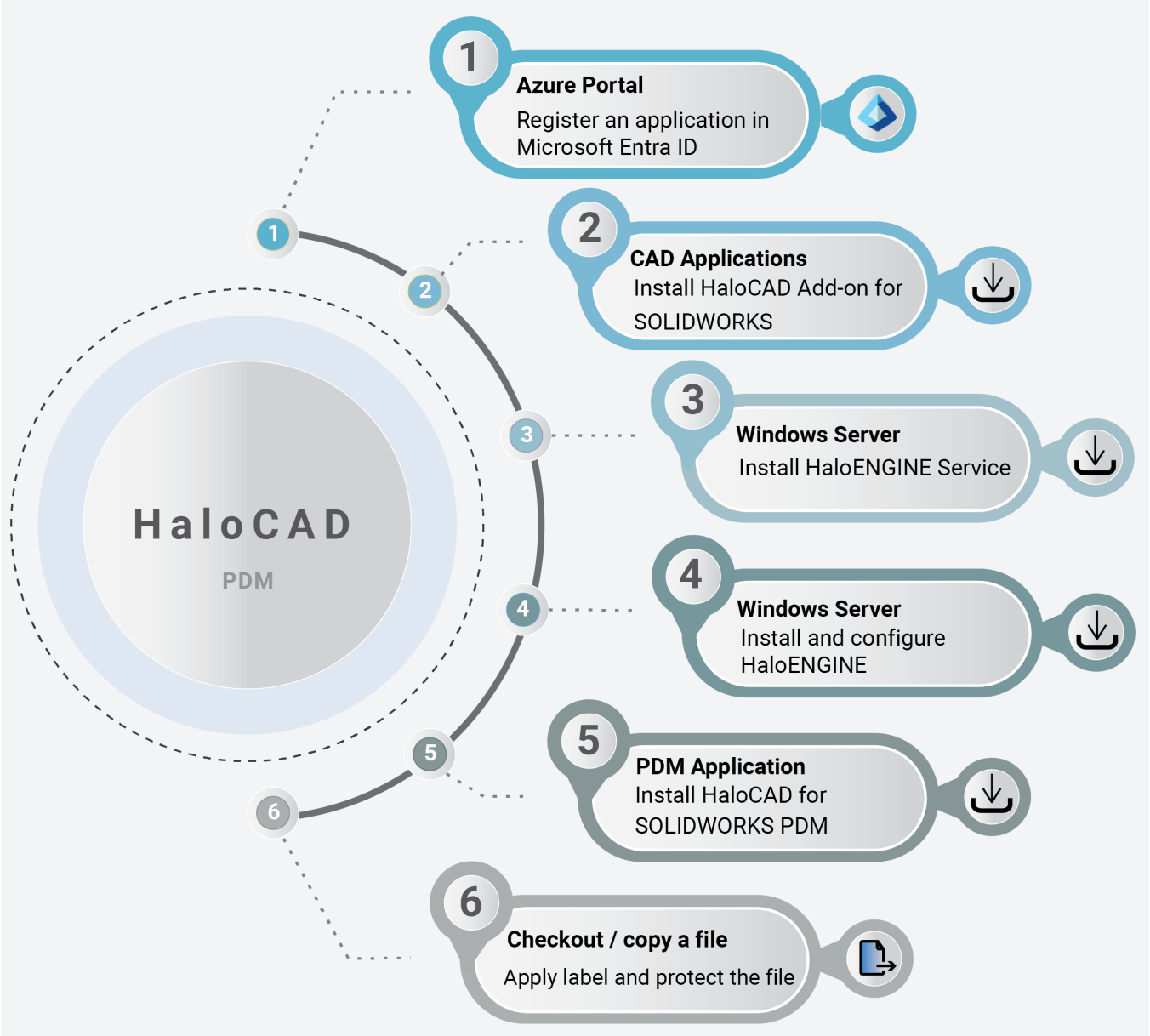
The HaloCAD for SOLIDWORKS Product Data Management (PDM) solution integrates with the respective PDM application and includes the functionality of HaloCAD PROTECT and HaloCAD MONITOR. Files in SOLIDWORKS PDM folders are closely monitored. When a file is cut or copied to a non-SOLIDWORKS PDM folder, HaloCAD 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.

1.3. About this Manual

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

2. Quick Start Installation Summary

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



HaloCAD quick start installation steps with SOLIDWORKS PDM

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`
Step 2 – How to install HaloCAD Add-on for SOLIDWORKS.	`HaloCAD_SOLIDWORKS_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 SOLIDWORKS PDM.	Refer to the current manual.
Step 6 – How to download a protected file.	`HaloCAD_SOLIDWORKS_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.

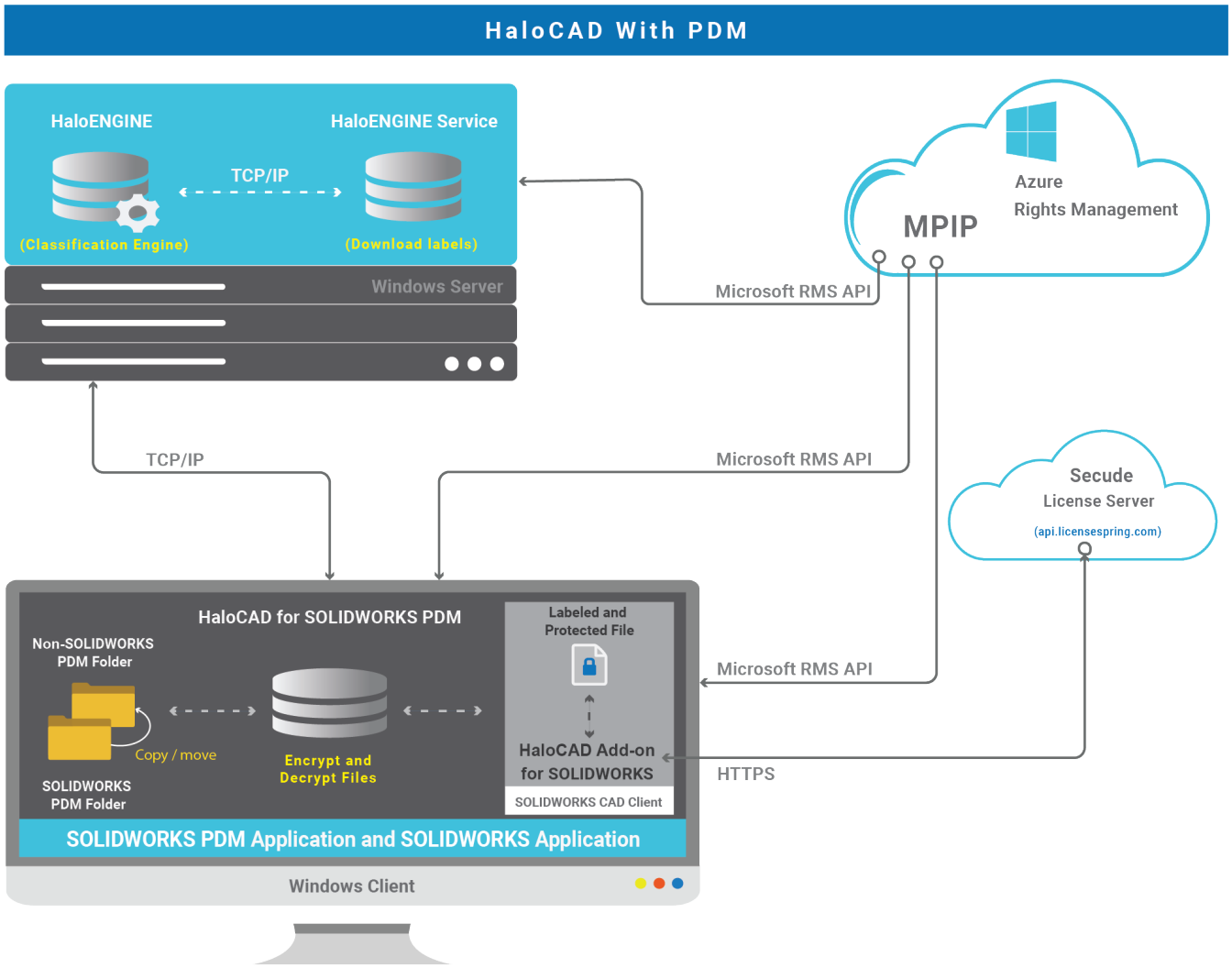
HaloCAD for PDM—This solution includes HaloCAD PROTECT and MONITOR capabilities and interacts with the respective PDM application. Files in SOLIDWORKS PDM folders are closely monitored. When a file is cut or copied to a non-SOLIDWORKS PDM folder, HaloCAD intercepts and protects it before reaching the destination folder. Also, any previously encrypted SOLIDWORKS application files or PDF files copied/moved to the SOLIDWORKS PDM folder will be decrypted and saved.

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 SOLIDWORKS PDM—contains the functionality of HaloCAD PROTECT and MONITOR.
2. HaloCAD Add-on for SOLIDWORKS—reads the protected files, enforces corresponding privileges, and changes MPIP labels.
3. HaloENGINE Server—Significant role where business logic is located. Note: HaloENGINE versions 6.4 and higher are compatible with HaloCAD for SOLIDWORKS PDM.
4. HaloENGINE Service—Downloads labels, which are then used by the Classification Engine in the HaloENGINE.



HaloCAD with PDM

HaloCAD for SOLIDWORKS PDM performs the following functions:

1. Resides in the SOLIDWORKS PDM Client.
2. Watches for cut/copy/paste/send to events in File Explorer (`explorer.exe`).
3. Responsible for obtaining metadata and label information from the HaloENGINE.
4. Responsible for labeling and encrypting files.
5. Responsible for logging HaloCAD component activities to the local log and also for sending audit logs to the HaloENGINE.

HaloCAD Add-on for SOLIDWORKS performs the following functions:

1. Resides in Dassault Systemes 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. Responsible for logging the add-on-related activities.

HaloENGINE performs the following functions:

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

1. Responsible for business logic. The HaloENGINE (classification engine) interprets the metadata collected in SOLIDWORKS PDM 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 retrieving label information from the HaloENGINE Service.
3. Responsible for logging events sent by HaloCAD for SOLIDWORKS PDM.

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). It retrieves MPIP labels from RMS and transmits them to the HaloENGINE.

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. Prerequisites

This section summarizes the prerequisites and dependencies for the installation and configuration of HaloCAD add-ons.

4.1. Register an Application in Microsoft Entra ID

This section will guide you through the steps of registering an application, obtaining the Client ID and Directory ID, and assigning permissions to the application.

Microsoft documentation

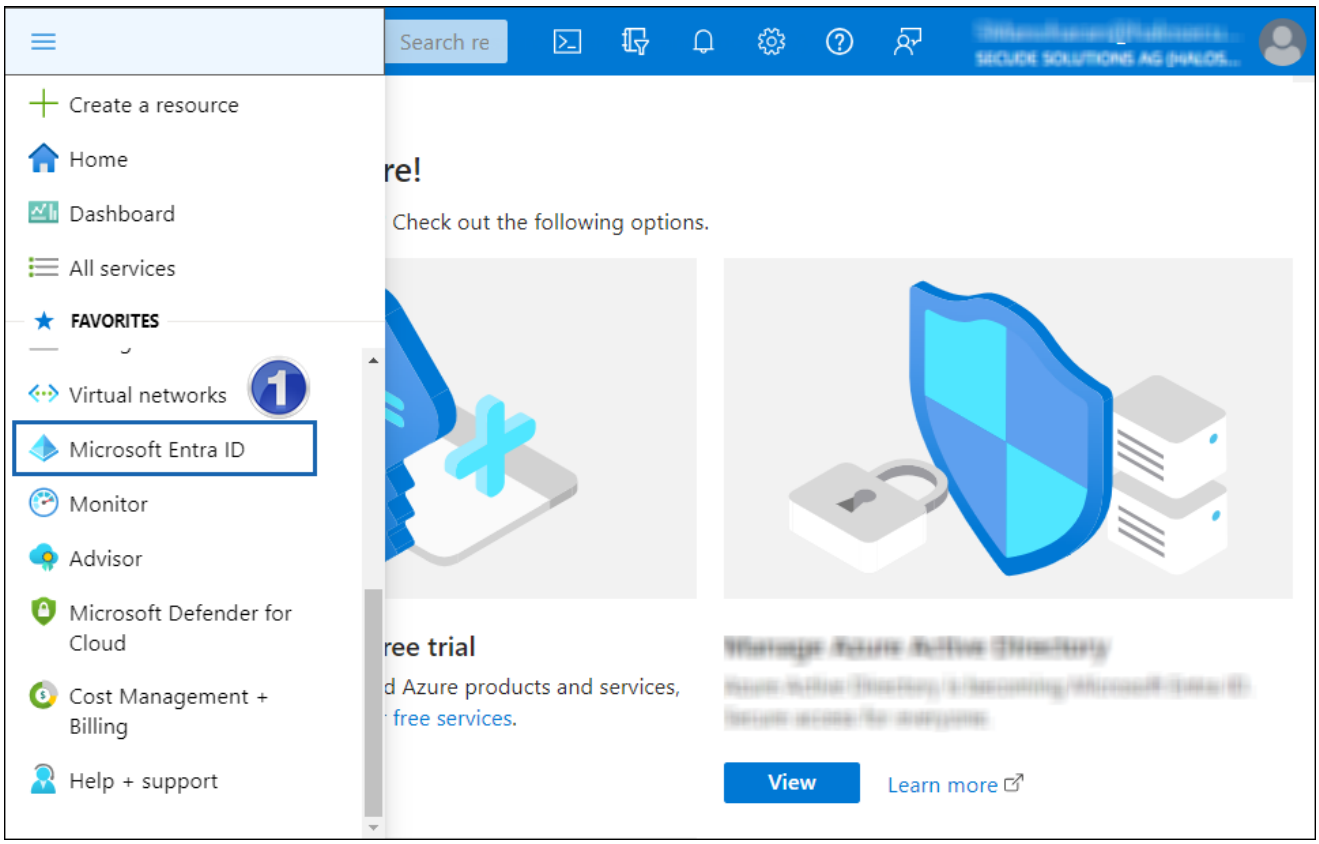
Any application to authenticate via Microsoft Entra ID must be registered in its directory. The information in the Microsoft documentation overrides any information published in this section. Please refer to Microsoft documentation for a comprehensive description.

For demonstration purposes, an application is created in the Azure portal; alternatively, you may create an application using https://entra.microsoft.com.

4.1.1. Create an Application

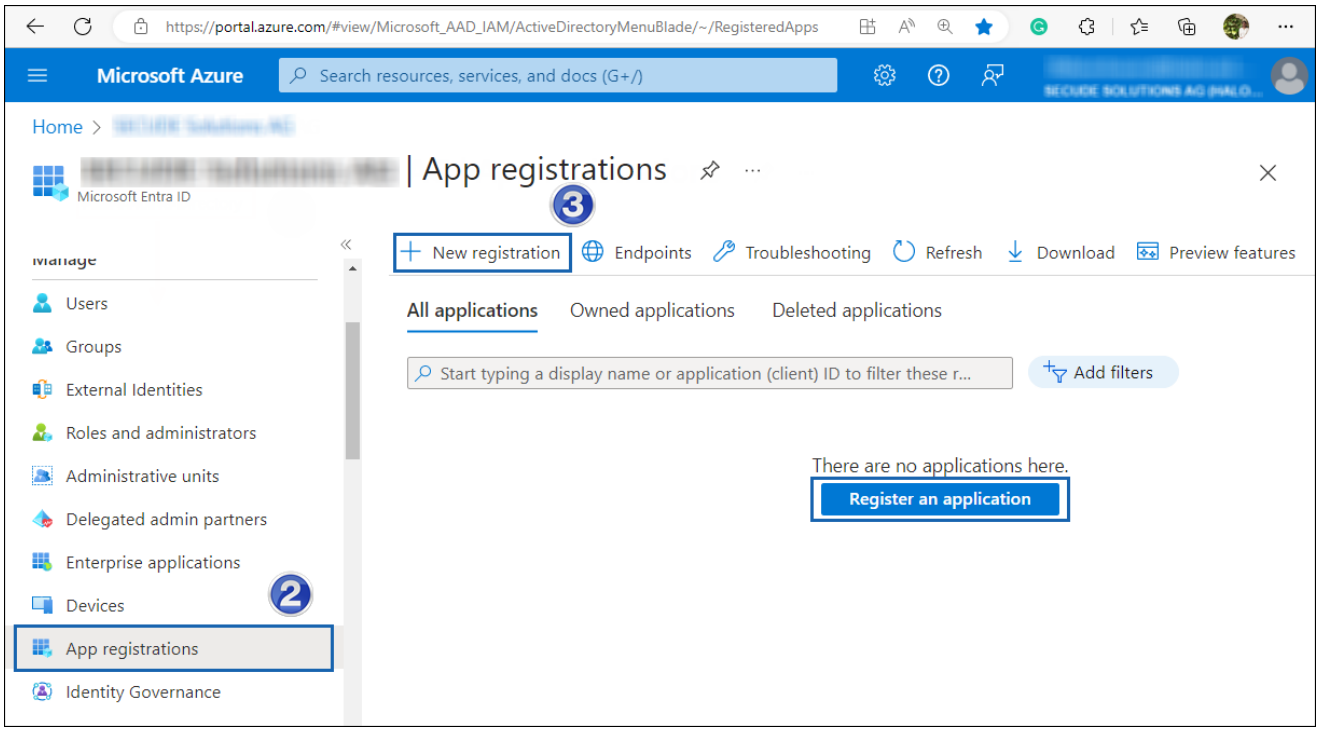
Follow the instructions below to register an application:

1. Sign in to the Microsoft Azure portal using an account with administrator permission.
2. On the portal's **Home** page, under Azure services, or on the left side of the navigation pane, choose **Microsoft Entra ID**.



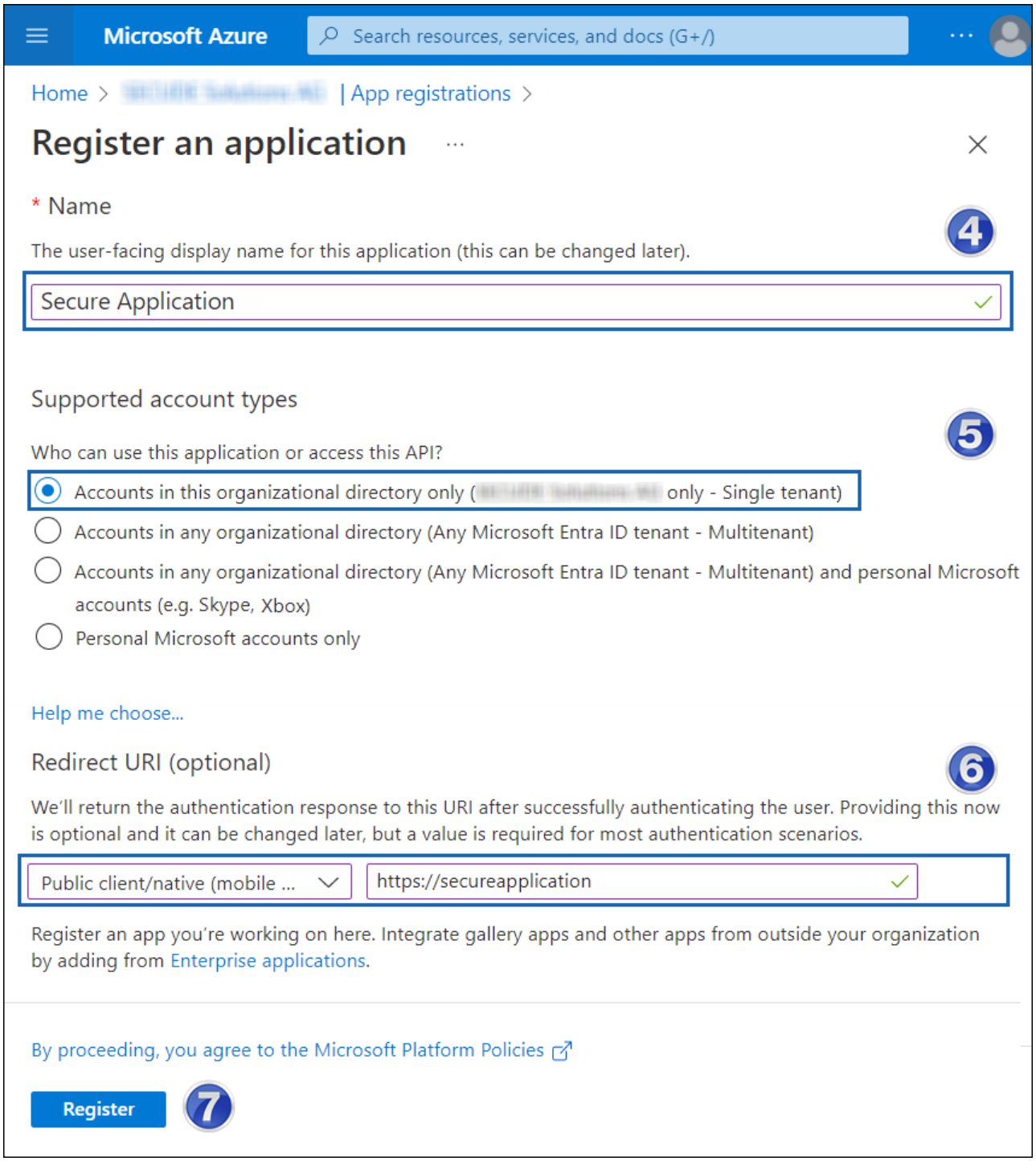
Selecting Microsoft Entra ID

3. On the **Overview page**, in the left navigation pane, click **App registrations**.
4. On the App registrations page, select **New registration** or **Register an Application** (this button appears only if no applications have already been created).



New application registration

5. On the **Register an application** page, enter your application's registration information.



Public client application details

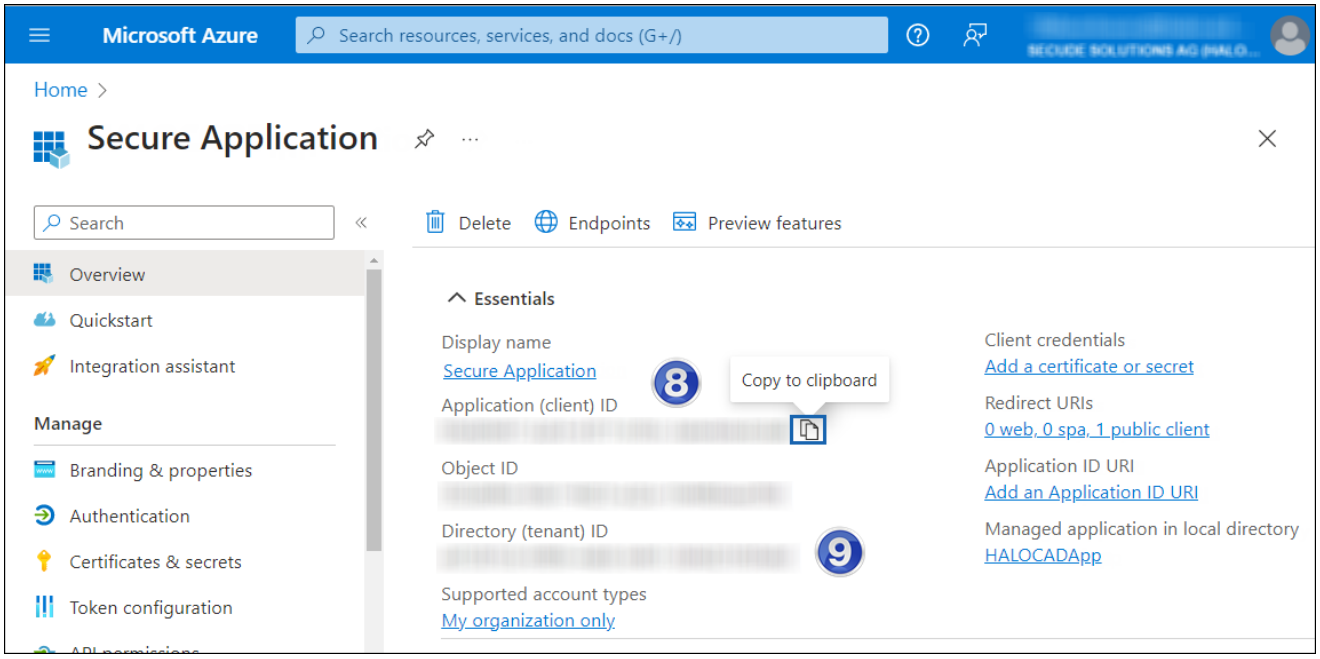
6. In the **Name** section, enter a meaningful application name.
7. Under **Supported account types**, select which account you would like your application to support. For detailed information on these types, please see Microsoft documentation.
   a. To target only accounts that are internal to your organization, select **Accounts in this organizational directory only**.

b. To target only business or educational customers, select **Accounts in any organizational directory**.

c. To target the widest set of Microsoft identities and to enable multitenancy, select **Accounts in any organizational directory and personal Microsoft accounts**.

d. To target the widest set of Microsoft identities, select **Personal Microsoft account only**.

8. Under **Redirect URI**: Select **Public client/native (mobile & desktop)**, and then type a valid redirect URI for your application. For example, `https://localhost`.
9. When finished, click **Register**.
10. An overview page for the new application registration is created and displayed.



Application ID and Tenant ID

11. The following values are shown on the portal once registration is complete. To copy and save the ID value in a text editor, hover your cursor over it and click the **Copy to clipboard** icon.

a. **Application ID** – It is also referred to as **Client ID**.

b. **Directory ID** – It is also referred to as **Tenant ID**.

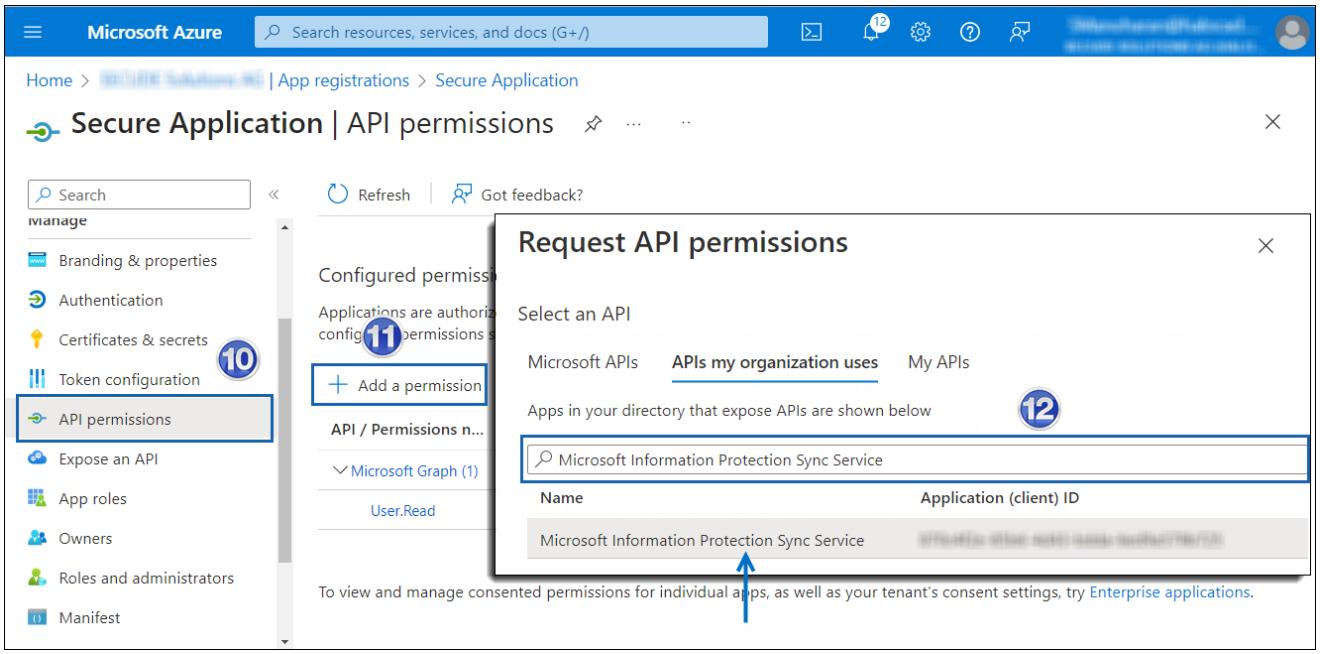
Save the authentication parameters

In a text editor (such as Notepad), copy the values of **Application (client) ID**, **Directory (tenant) ID**, and **Redirect URI**, and save it for initializing the HaloCAD application. Directory (tenant) ID is needed only for single-tenant applications.

4.1.2. Add Required Permissions

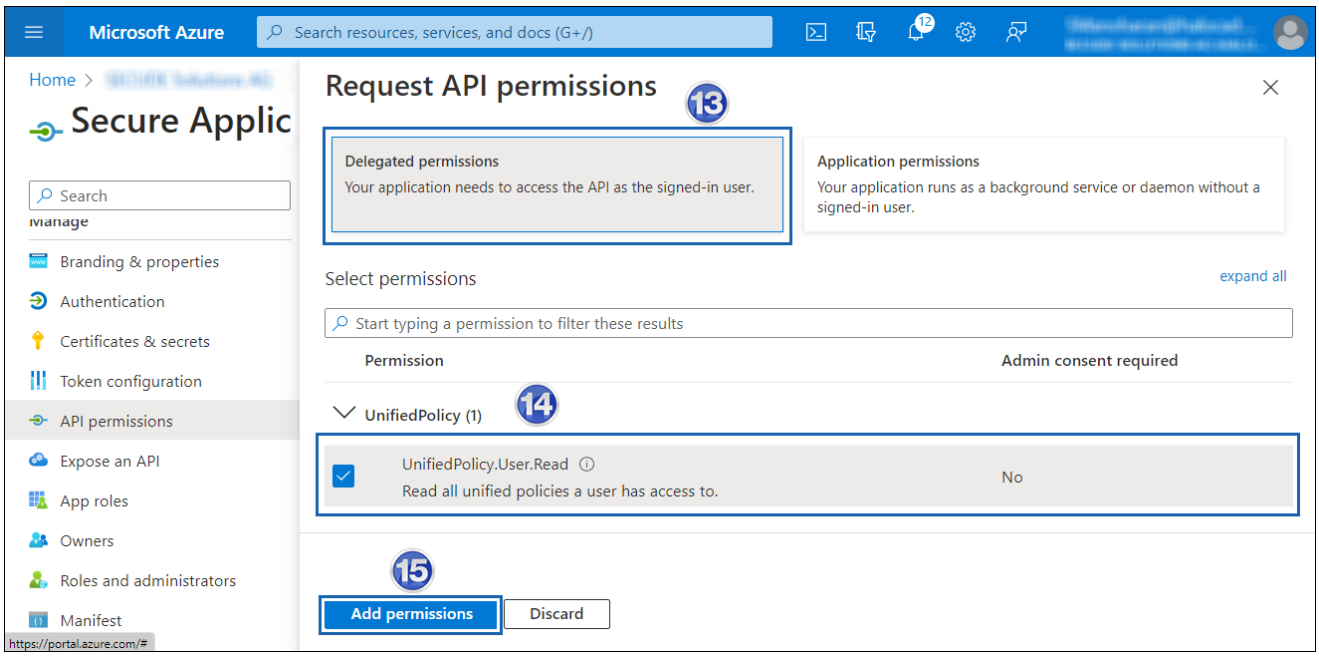
To protect content using MIP SDK, you need to provide the following API permission(s) for the created application ID.

1. In the sidebar of the new application page, select **API permissions**. The **API permissions** page for the new application registration will appear.
2. Click **Add a permission** button. The **Request API permissions** page will appear.
3. Under the **Select an API** setting, select APIs my organization uses. A list appears, containing the applications in your directory that expose APIs.
4. Type in the search box or scroll to find the required API that is mentioned in the below table “Required Permissions”.
5. For example, type "Microsoft Information Protection Sync Service". You can see the API listed as shown in the below figure:



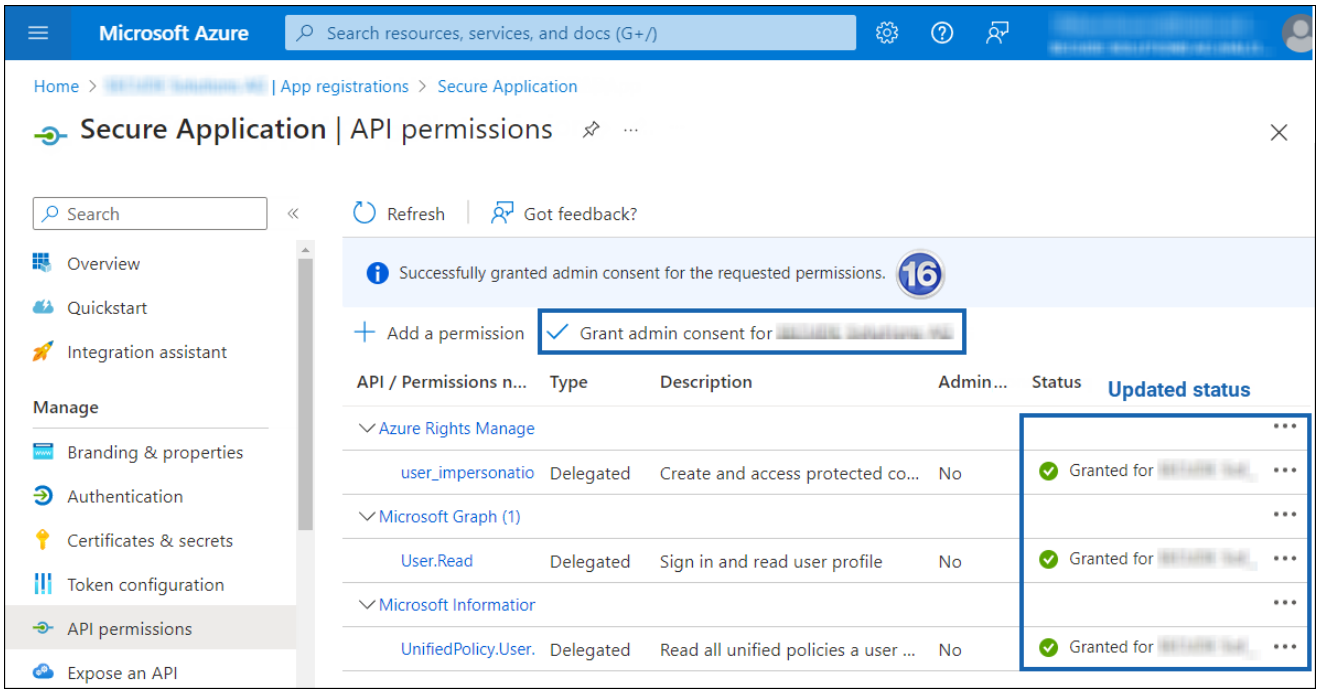
Searching permissions

6. Now, click on the displayed API. You can see two permissions on the page – **Delegated permissions** and **Application permissions**.
7. Click **Delegated permissions** button and then, under the **Permission** section, select the check box against "Read all unified policies a user has access to".



Adding permission

8. Click **Add permissions**. (Repeat the steps outlined above to add the other required permissions listed in the table below.)
9. You will return to the API permissions page, where the permissions have been saved and added to the table.



API Required permissions

10. Click **Grant admin consent** for your company button. You will be prompted to accept the consent confirmation; click **Yes** to the question.
11. The following table lists the required permissions.

API / Permission name	Display Name	Type	Description
Azure Rights Management Services (Microsoft Rights Management Services)	`User_impersonation`	Delegated	Create and access protected content for users
Microsoft Graph	`User.Read`	Delegated	Sign in and read user profile (will be added by default)
Microsoft Information Protection Sync Service	`UnifiedPolicy.User.Read`	Delegated	Read all unified policies a user has access to.

Required permissions

4.2. Create and Configure the Sensitivity Labels

As an administrator, you can create, configure, and publish sensitivity labels for various levels of content sensitivity based on your organization's classification taxonomy. Use names or terms that are familiar to your users. Consider starting with label names like Personal, Public, General, Confidential, and Highly Confidential if you don't already have a taxonomy in place. For more details, please refer to Microsoft online documentation.

5. 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. 2021 SP05.1, version 29.5.1.1 2. 2022 3. 2024 SP 3.1, SP 4.0 4. SolidNetWork License Manager, version 29.51.0001 Supported SOLIDWORKS PDM Client: 1. 2021 SP05.1 2. Supported Operating System: Windows 10, Windows 11, or above with updates installed.
Office 365 Subscription	1. Fully configured Microsoft Purview Information Protection. 2. An Azure subscription is required to use Azure RMS and the MPIP functionality. 3. A working Microsoft Entra ID service must be available. 4. Transport Layer Security (TLS) 1.2 or higher must be enabled to ensure the use of cryptographically secure protocols at all client workstations. 5. To avail revoke access feature, the user should be assigned to Microsoft Purview Information Protection Premium P1/P2 license. (Not required for reader add-on) 6. Audit logging: Your Azure subscription must include Log Analytics on the same tenant as Microsoft Entra ID. 7. Use the option “Public client/native (mobile & desktop)” during application registration in the Azure portal.
Supported file types	`.sldprt`, `.sldasm`, `.prt`, `.asm`, `.slddrw`, `.x_t`, `.tif`, `.dwg`, and `.dxf`
Other components	HaloENGINE (supported from >6.4) and HaloENGINE Service

Requirements

Recommended URLs, addresses, and ports for MPIP

MIP SDK doesn't support the use of authenticated proxies. So, make sure you set the Microsoft 365 endpoints to bypass the proxy. View a list of endpoints at "Microsoft Online Documentation". However, Microsoft recommends the following:

Addresses	Ports
`*.protection.outlook.com` `40.92.0.0/15`, `40.107.0.0/16`, `52.100.0.0/14`, `52.238.78.88/32`, `104.47.0.0/17`, `2a01:111:f403::/48`	TCP 443
`*.aadrm.com`, `*.azurerms.com`, `*.informationprotection.azure.com`, `ecn.dev.virtualearth.net`, `informationprotection.hosting.portal.azure.net`, `*.office.com` (add `substrate.office.com` if you don't want to add all sub-domains), `crl3.digicert.com`, `crl4.digicert.com` .	TCP 443
For event logging `*.events.data.microsoft.com`	TCP 443
National Cloud	**Microsoft Entra ID authentication endpoint**
Microsoft Entra ID for the US Government	`https://login.microsoftonline.us`
Microsoft Entra ID (global service) For details on Microsoft Entra ID endpoints, please refer to "Microsoft Online Documentation".	`https://login.microsoftonline.com`

Recommended endpoints

6. Installing the HaloCAD for SOLIDWORKS PDM

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

6.1. Before you Begin

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

1. Make sure you have administrative access to install the HaloCAD component.
2. Make sure the client computer running the HaloCAD for SOLIDWORKS PDM can connect to the SOLIDWORKS PDM Server.
3. Make sure the machine that is installed with HaloENGINE can reach the machine that is installed with HaloCAD for SOLIDWORKS PDM.
4. Make sure your HaloENGINE complies with 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 admin portal and manually install it in Trusted Root Certification Authorities.

      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 on the SOLIDWORKS PDM server.

6.2. 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 the HaloCAD using command lines.

6.2.1. Graphical Mode

Before you begin

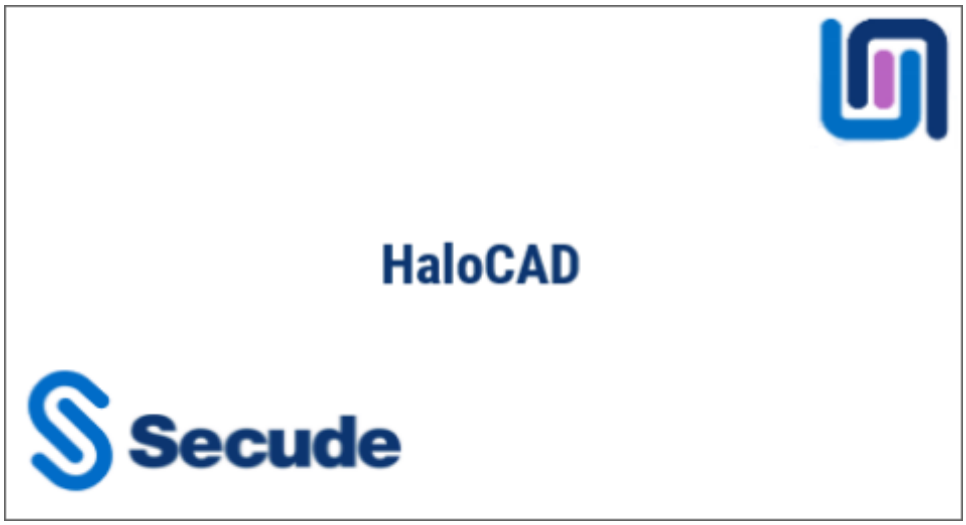
The following prerequisites must be met:

1. A user who installs HaloCAD for SOLIDWORKS PDM must have administrator rights.
2. Make sure that you have tenant details before starting the installation.

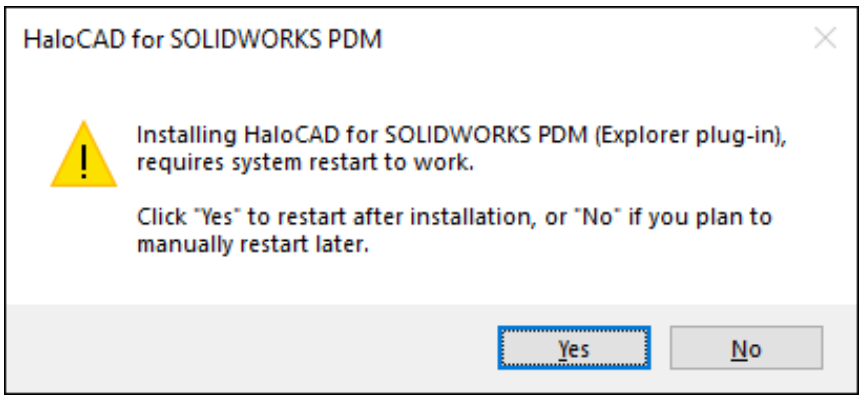
Installation Procedure

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



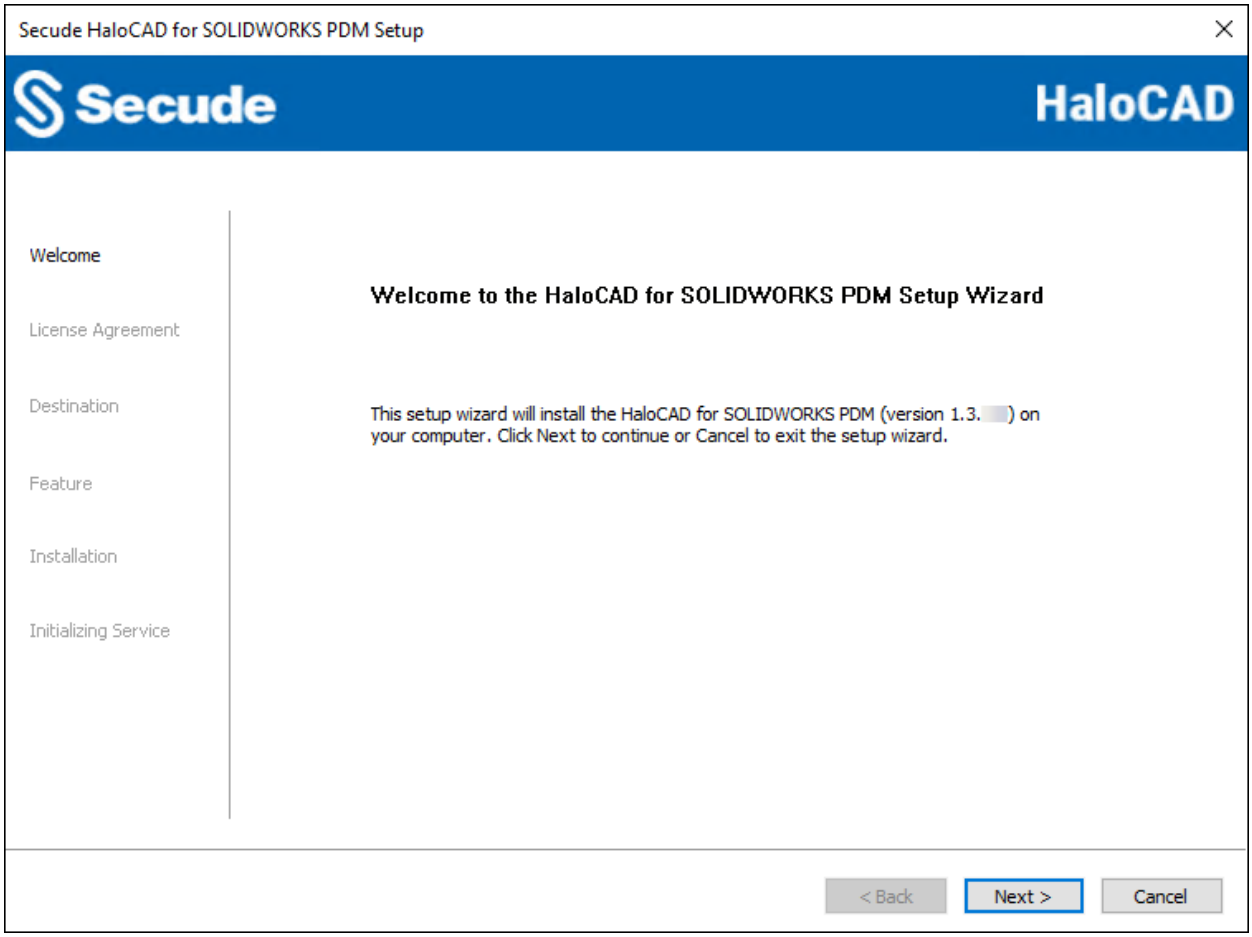
Startup dialog



Restart message

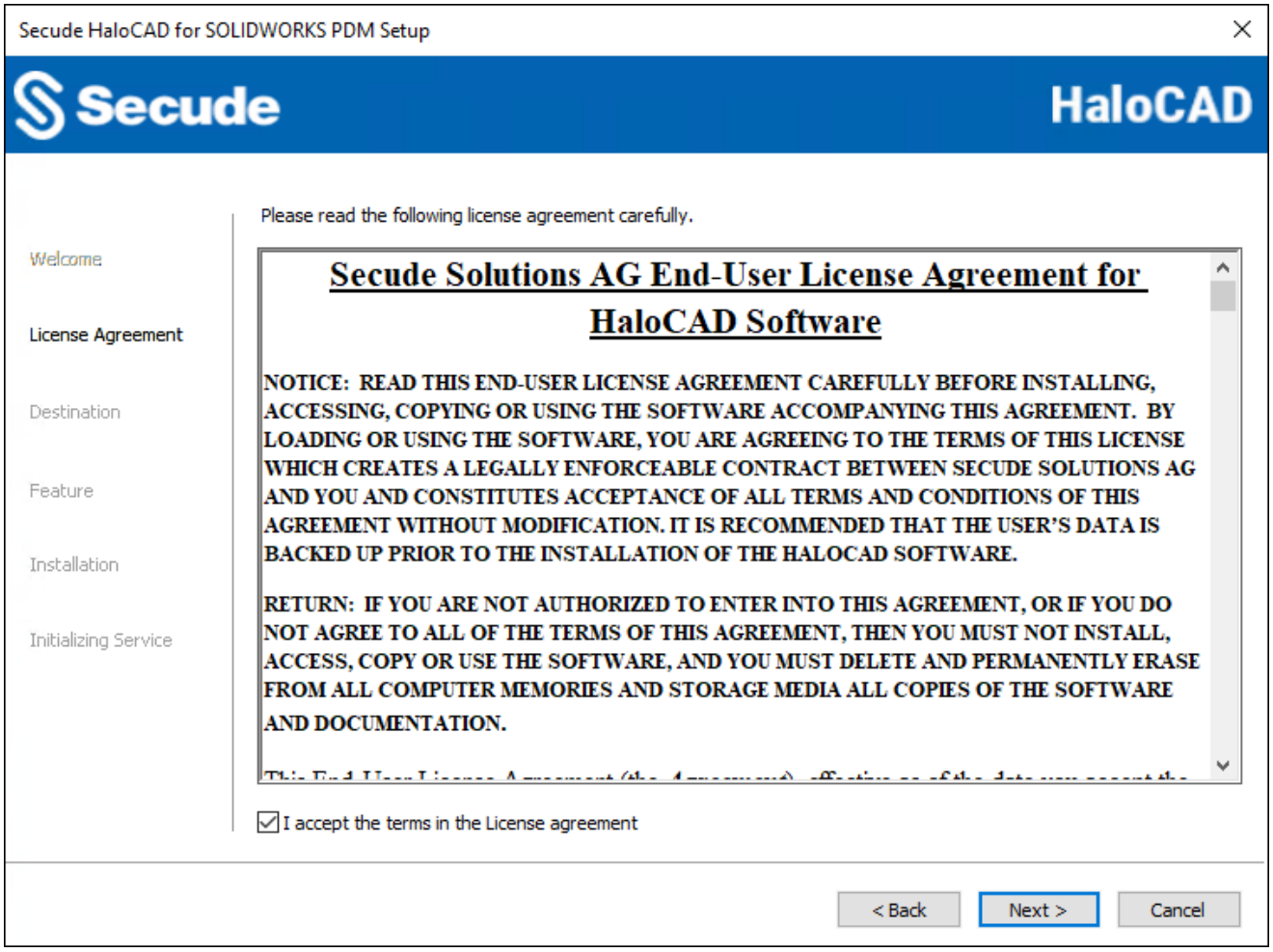
4. To activate the HaloCAD component (Explorer plug-in), you must restart your computer after installing it. To confirm it, you need to choose one of the following options.
   a. By selecting **Yes**, your computer will restart immediately after installing the HaloCAD component.
   b. By selecting **No**, the HaloCAD component will be installed, but you will have to restart your computer manually later. Please note that the HaloCAD component becomes active only after a machine restart.

5. The welcome dialog will appear:



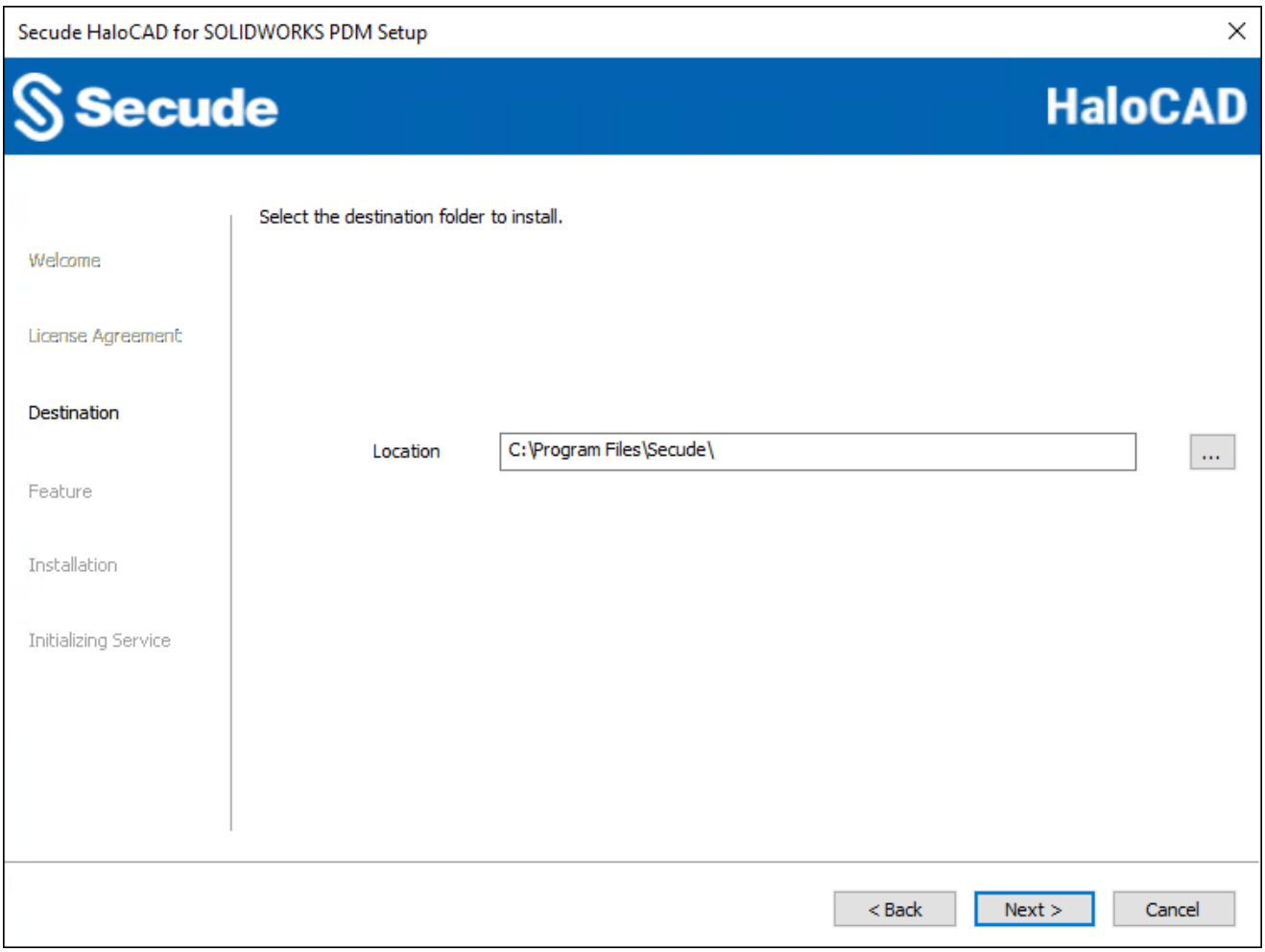
Welcome dialog

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



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**.
9. The destination folder selection dialog will appear:

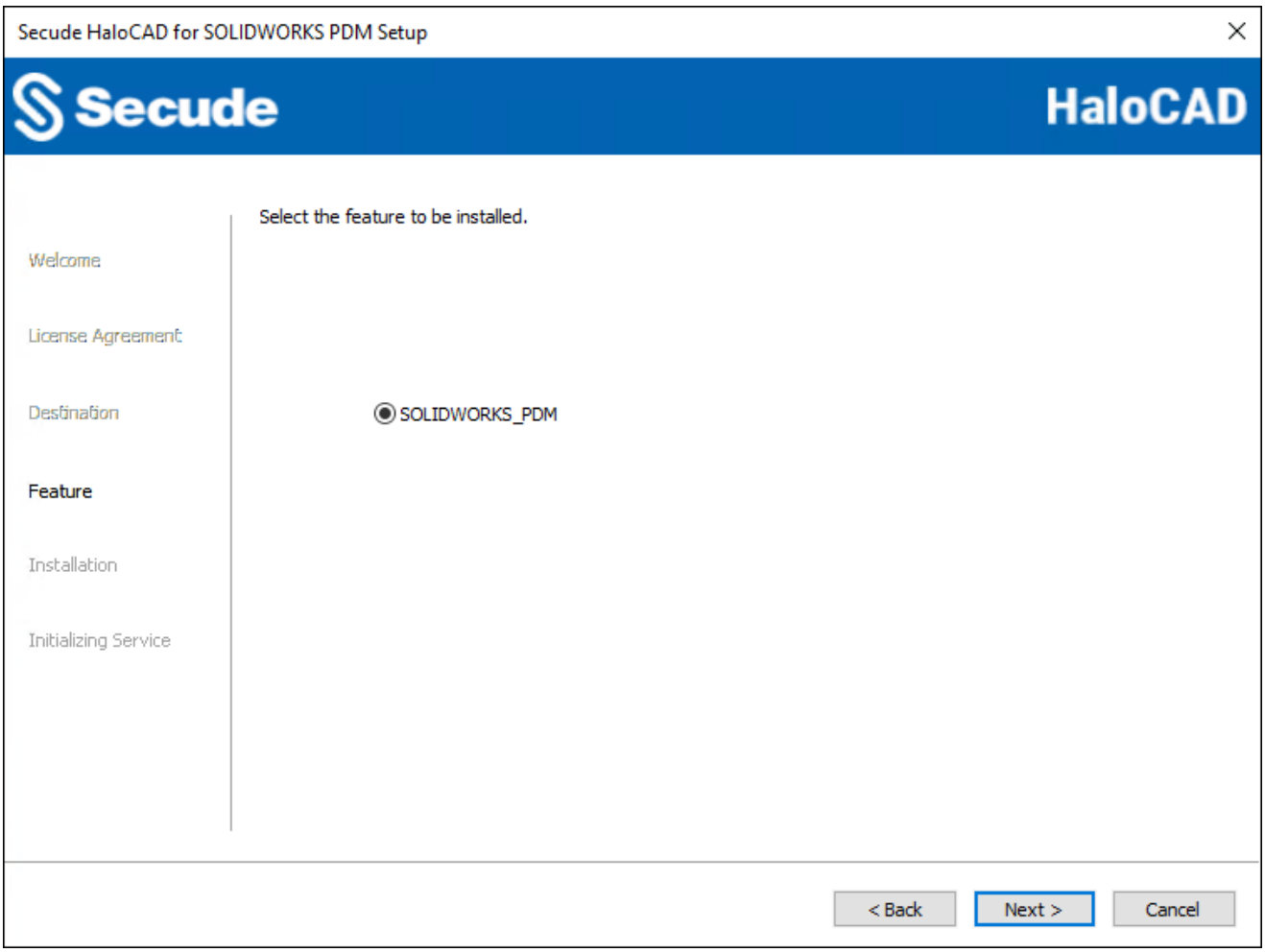


Destination folder selection dialog

a. 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.

b. When you are finished, click **Next**.

10. The feature selection dialog will appear:



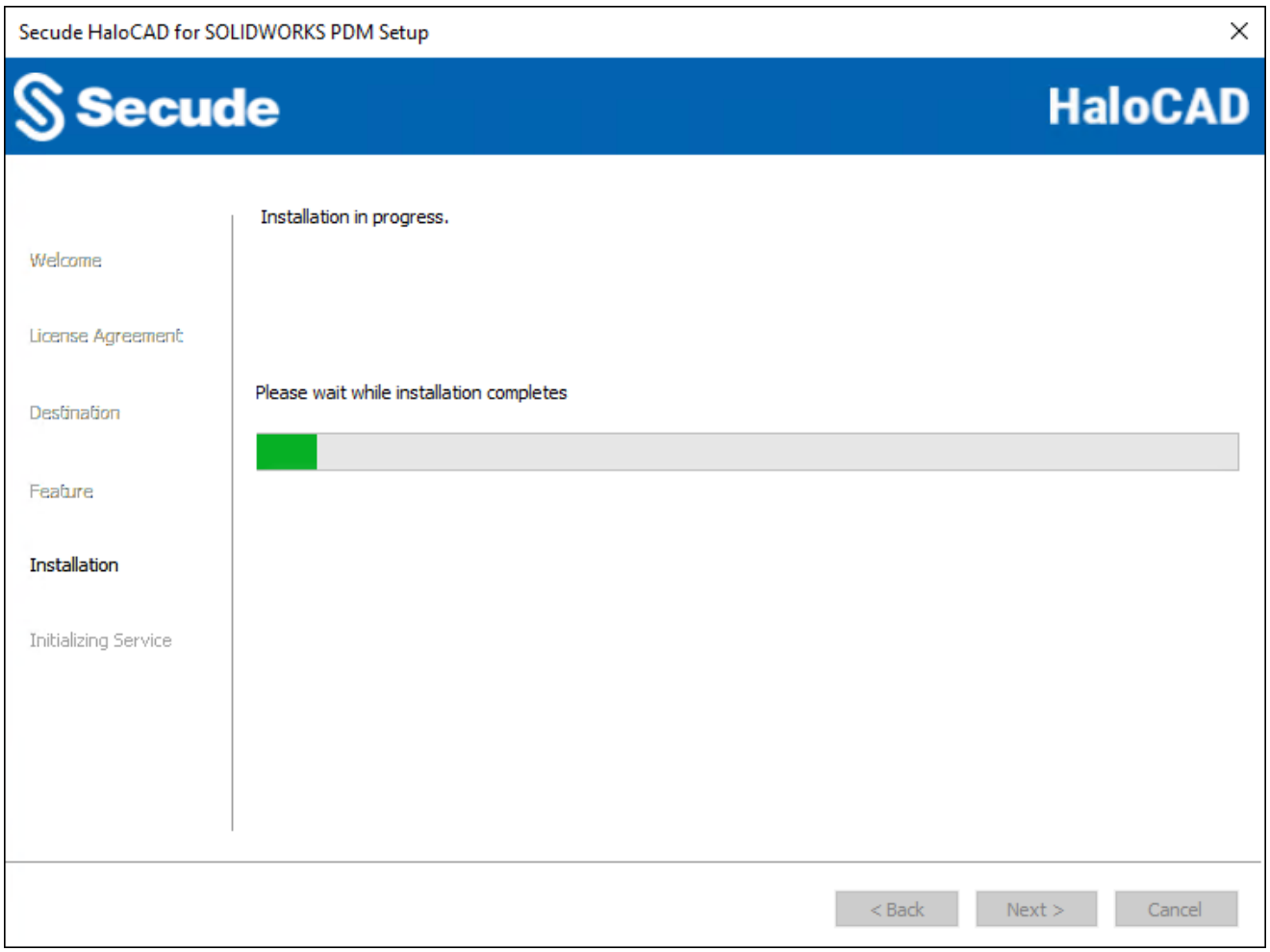
Feature selection dialog

a. By default, **SOLIDWORKS_PDM** option will be selected.

b. If you wish to review or change any settings, click the **Back** button to return to any point in the installation process. Otherwise, click **Next** to allow the setup program to install the application.

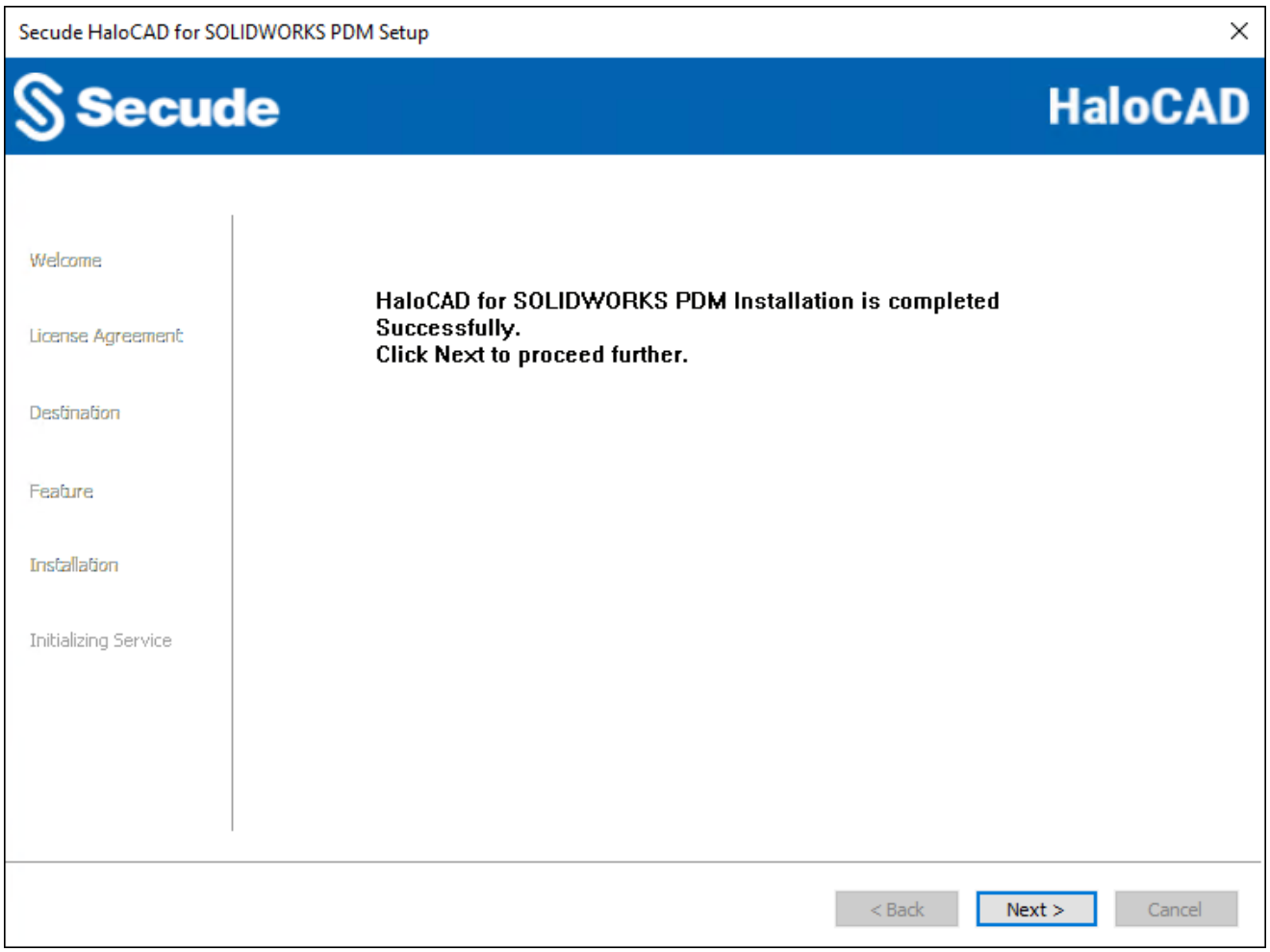
c. Using the **Cancel** button, it is possible to cancel the installation at this point.

11. The installation begins and progress is shown in the dialog.



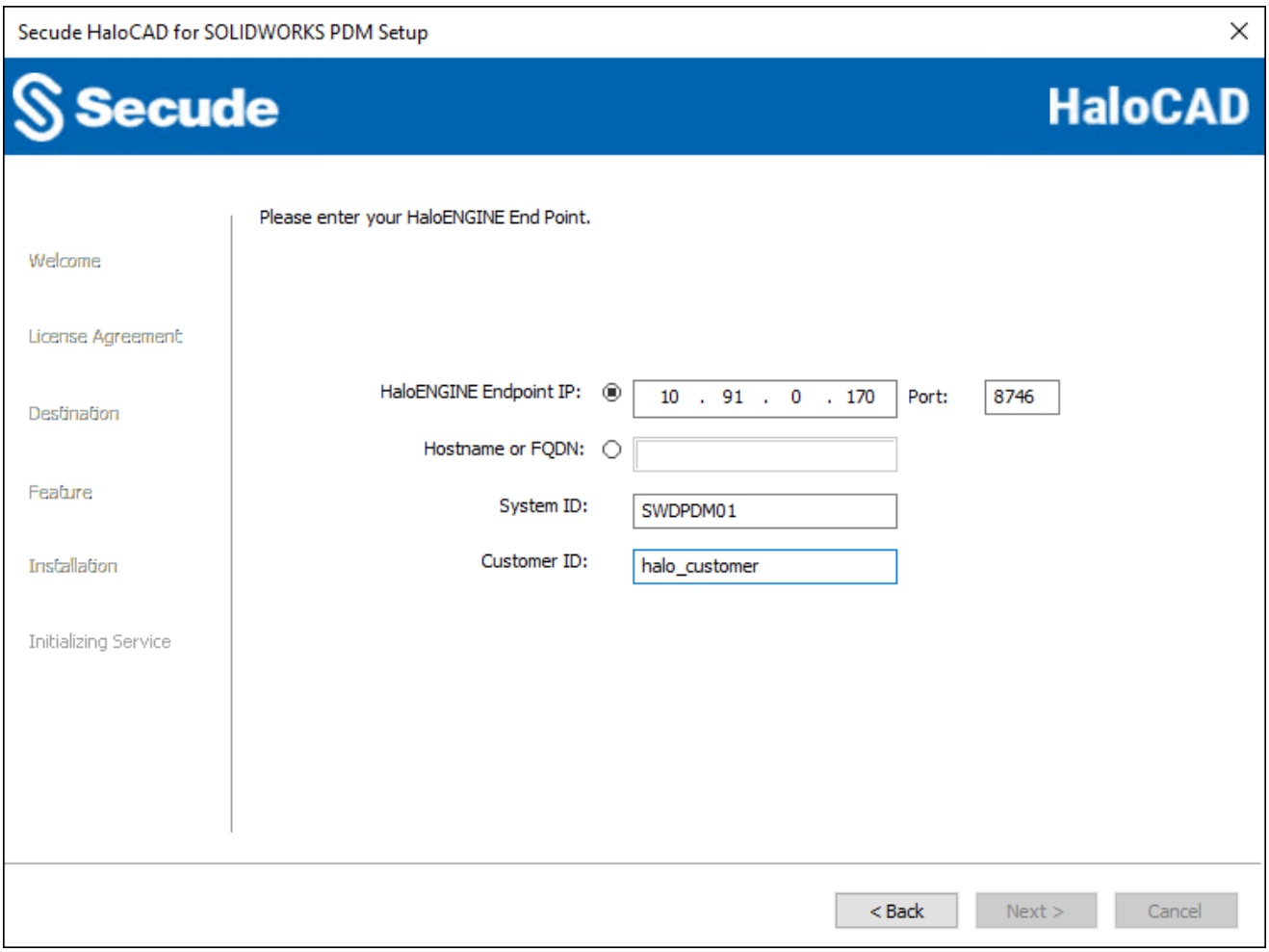
Installation progress dialog

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



Installation completed dialog

13. Click **Next**, and the endpoint dialog will appear.



Endpoint dialog

a. Select either the IP address or the hostname and enter the required details. Enter the IP address of the HaloENGINE in the **HaloENGINE Endpoint IP**. For example, `10.91.0.170`.

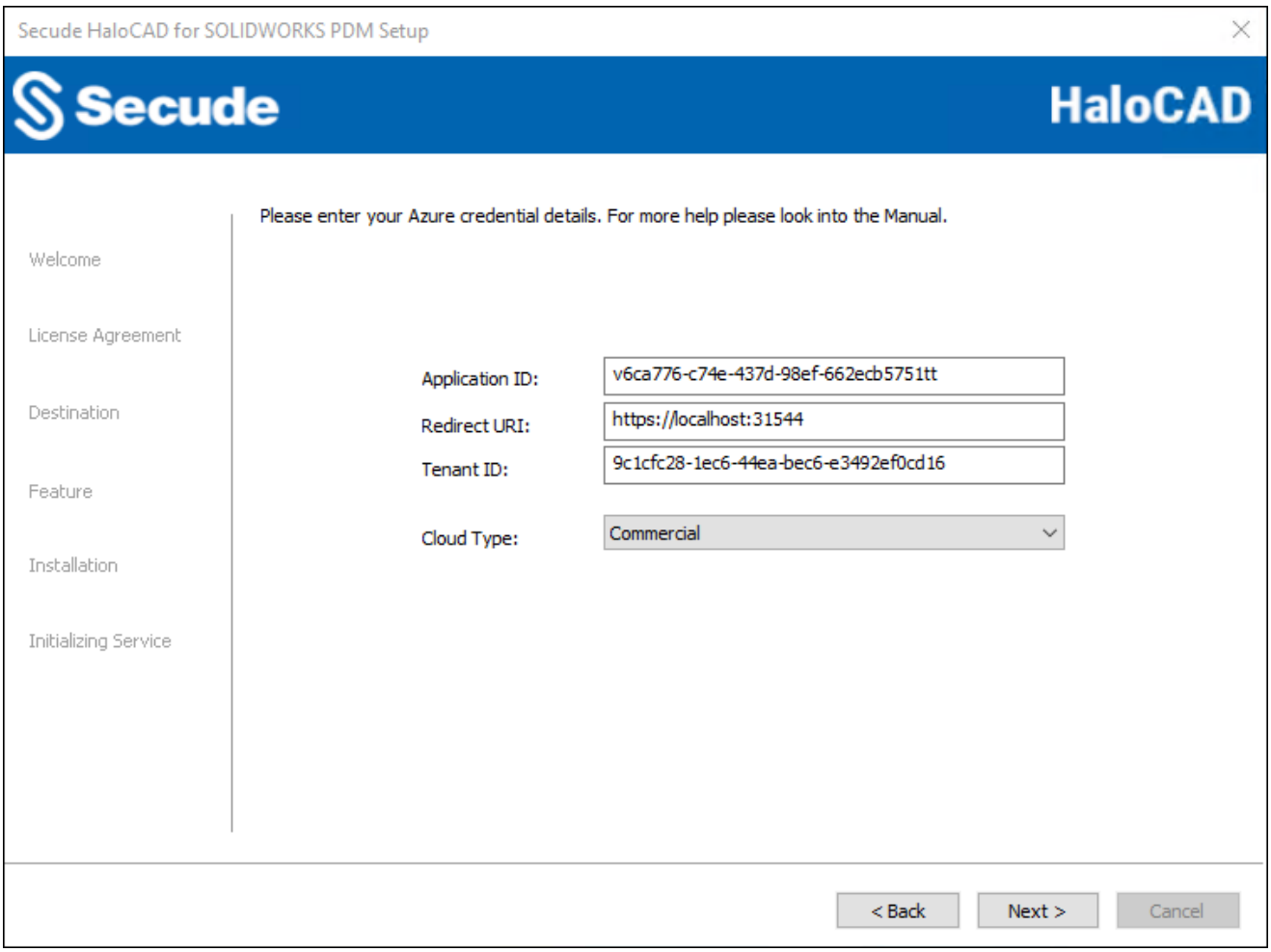
b. Or enter the hostname or fully qualified domain name (FQDN) in **HostName or FQDN**. For example, `SOLIDWORKSServer01.secude.com`. The default port number **8746** will be displayed.

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

d. Enter the **Customer ID** that is assigned for Single Customer mode or Multi-Customer mode in the admin portal. For example, `halo_customer`.

e. At this point, HaloCAD tries to connect to your HaloENGINE. If you enter an invalid endpoint or the Server is not reachable, the installation will be terminated with an error message "*HaloENGINE API endpoint is invalid or not reachable*". In this case, you must return to the previous screen, enter a valid endpoint, confirm that the HaloENGINE is reachable, and then select **Next**.

14. The initialization dialog will appear. To avoid connectivity issues, make sure to enter the correct Azure application registration information in the screen below.



Initialization dialog

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

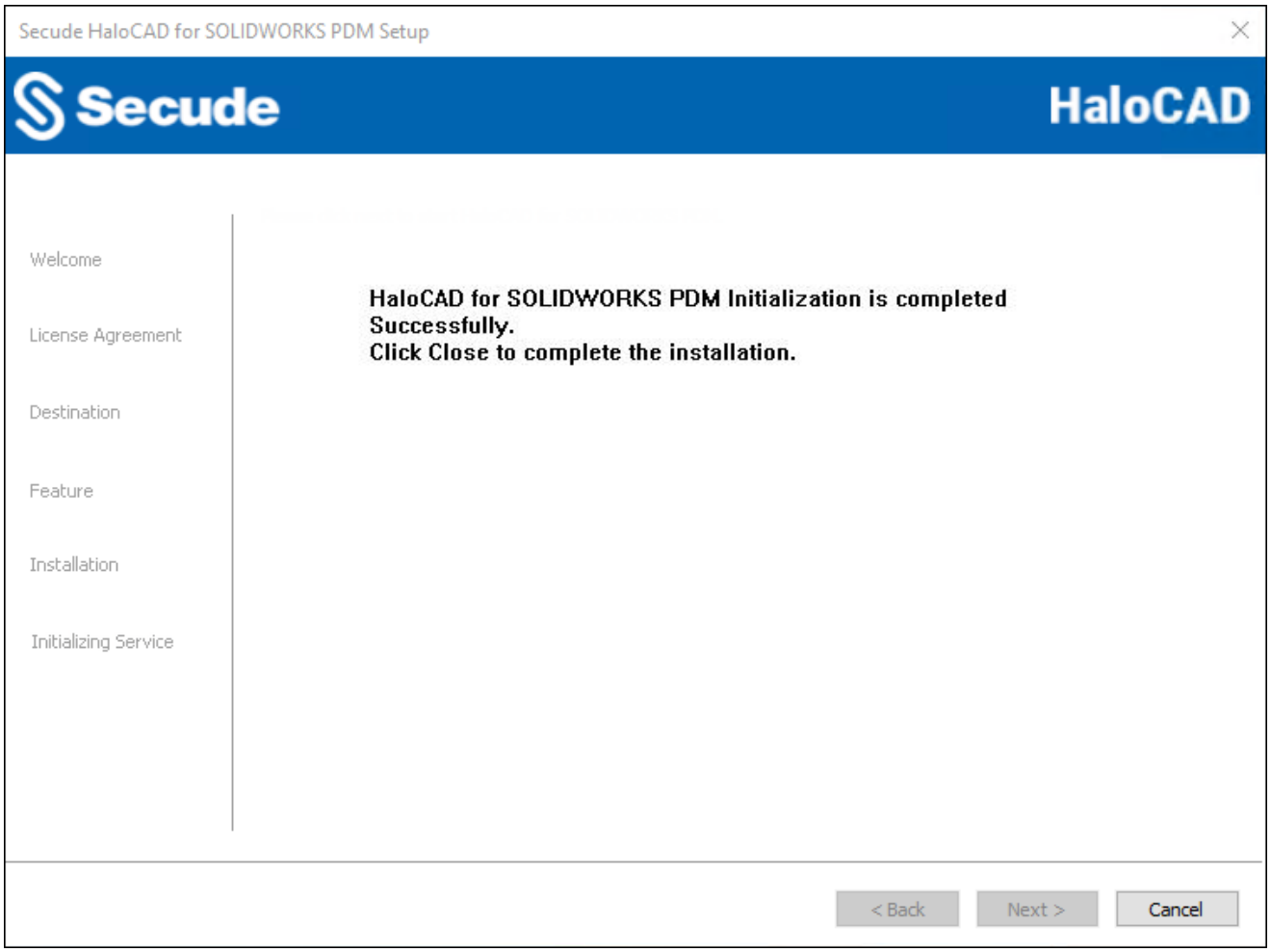
b. **Redirect URI**: Enter the URI that was provided when registering the native application in the Azure portal. For example, `https://localhost`.

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

e. Click **Next**,

15. Once the initialization is completed, you will get the success message as shown below.



Initialization completed dialog

16. Click **Close** to close the installation wizard.
17. Based on the selected option **Yes**, your machine will be restarted automatically. If you have chosen **No**, you must restart it manually.

Post Installation files:

1. You can view the log files at `%AppData%\Roaming\Secude\HaloCAD\SOLIDWORKS PDM\halocad.log`.
2. Also, you can see the configuration information in the registry— `HKEY_LOCAL_MACHINE\SOFTWARE\Secude\HaloCAD for SOLIDWORKS PDM`.
3. To change the HaloENGINE settings, such as endpoints, System ID, and Customer ID, manually edit the registry entries `HKEY_LOCAL_MACHINE\SOFTWARE\Secude\HaloCAD for SOLIDWORKS PDM\ep\HCV`.
   Note: Make a backup of the above registry before editing the entries.

6.2.2. 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>] ]
  HaloCAD_SWPDM_Setup.exe [-uninstall -silent <true|false>]
   ```

4. 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.
5. The following command illustrates how to install HaloCAD using the Azure application details.

   ```
   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/
   ```

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

6.3. Next Step

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

7. Appendix

This section provides supplemental information.

7.1. Enable Support for TLS 1.2 at the Client Workstation for Microsoft Entra ID

To improve the security posture of the tenant, and to remain in compliance with industry standards, Microsoft Entra ID stopped supporting the following Transport Layer Security (TLS) protocols and ciphers:

1. TLS 1.1
2. TLS 1.0
3. 3DES cipher suite (TLS_RSA_WITH_3DES_EDE_CBC_SHA)

In order for the HaloCAD for CAD add-on to be able to authenticate to Microsoft Entra ID, TLS 1.2 must be activated on the respective client workstation. Please see this Microsoft article to enable TLS 1.2.

Microsoft documentation

The information in the Microsoft documentation overrides any information published in this section.

Secude is not liable for changes to the content of this section because it was extracted from the Microsoft article at the time when the HaloCAD manual was prepared. Do check the most recent updates in this regard from the Microsoft documentation.

In summary, the following steps must be performed:

1. Update the Windows Operating System
2. Update .NET Framework
3. Set the following registry settings:

S.No	Windows Registry	Values
1	[HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\.NETFramework\v4.0.30319]	"SystemDefaultTlsVersions"=dword:00000001 "SchUseStrongCrypto"=dword:00000001
2	[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319]	"SystemDefaultTlsVersions"=dword:00000001 "SchUseStrongCrypto"=dword:00000001

Registry entries

7.2. 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 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	1.1.1	https://github.com/openssl	https://github.com/openssl/openssl/blob/master/LICENSE.txt
tbb	2018_20180618oss	https://github.com/oneapi-src/oneTBB	https://github.com/dwaddington/tbb-2018/blob/tbb_2018/LICENSE
MSAL	4.36.1	https://github.com/AzureAD/microsoft-authentication-library-for-dotnet	https://github.com/AzureAD/microsoft-authentication-library-for-dotnet/blob/master/LICENSE
WTL	9.0.4140	https://www.nuget.org/packages/wtl/9.0.4140	https://opensource.org/licenses/cpl1.0.txt

Open-source software

7.3. Metadata

The SOLIDWORKS PDM metadata present in the HaloENGINE is listed in the table below.

SOLIDWORKS PDM Metadata	Use
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

7.4. Download Log Definition

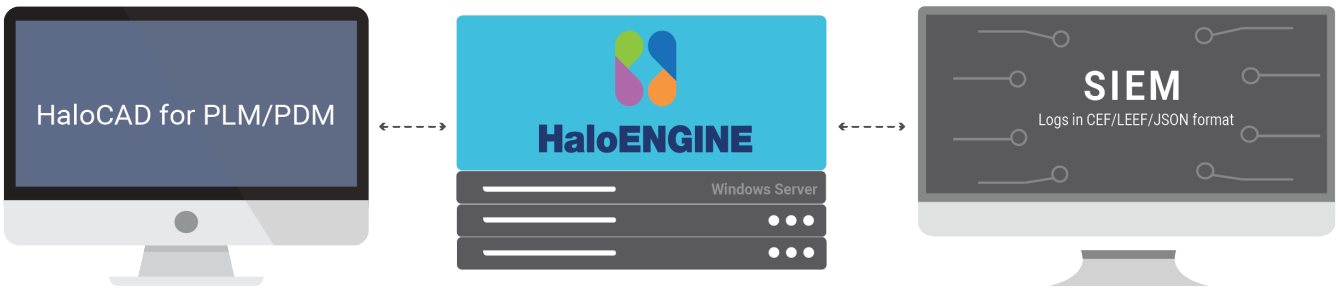
This section explains the log definition for every log format that HaloENGINE supports.

7.4.1. What is SIEM Integration?

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

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

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



Forwarding logs

7.4.2. Why CEF Standard?

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

Syslog and CEF Header

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

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

CEF format

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

CEF format sample

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

```
07:16:20.305 CEF:0|Secude|HaloCAD|6.7.0.3|999|Export
Event|1|deviceCustomDate1Label=exportTime deviceCustomDate1=Oct 15 2024 04:16:17 UTC
externalId=7E68561DA731481BBF9E8009F4B134CA deviceCustomDate2Label=logTime
deviceCustomDate2=Oct 15 2024 05:16:20 UTC act=unblocked;labeled;protected
fname=Part2.SLDPRT filePath=C:\Vault\DEV_TEST fileType=SLDPRT fsize=60137 in=95066
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\=[{ key\=[],
value\=[], type\=[] }] ] 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\=[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

7.4.3. Why LEEF Standard?

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

Syslog and LEEF Header

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

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

LEEF format

```
07:21:57.074 LEEF:2.0|Secude|HaloCAD|6.7.0.3|999|^|exportTime=Oct 15 2024 04:21:54
UTC^eventName=Export Event^externalId=7DB51F158CBE46A39006E32BA33FAA3D^logTime=Oct 15
2024 05:21:57 UTC^act=unblocked;labeled;protected^fname=Part-unprotrcted-
1.SLDPRT^filePath=C:\Vault\DEV_TEST^ftype=SLDPRT^fsize=55728^fdwnsize=90666^shost=SWPD
M_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], destination_attributes=[ {key=[], value=[],
type=[]} ] ]^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=[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`
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|6.6.0.0|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|6.6.0.0|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

7.4.4. Why JSON Standard?

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

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

1. Data is represented in name/value pairs.

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


```
07:33:10.398
{"log_id":"1BFA55EBA318455085A17B7B5CE0E52B","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":[{"type":"","value":"","key":""}],"destination_ip
":"null","os":"Unknown","recipients":[],"browser":"null","device_type":"null","browser
_version":"null","user_agent":"null"},"classification":{"classification_by_system":[],
"classification_by_user":[]},"version":"6.7.0.3","log_time":"Oct 15 2024 05:33:10
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":"","key":"ad_group"}],"bi_info":"nu
ll"},"user_info":{"user_email":"HaloCAD SOLIDWORKS
PDM","user_type":"SOLIDWORKS_PDM","user_name":"secude-
swepdm.com\\Solidworks"},"file_info":{"file_path":"C:\\Vault\\DEV_TEST","file_name":"U
p-prot-
Part1.sldprt","file_type":"SLDPRT","download_file_size":90666,"original_file_size":557
33},"action":["unblocked","labeled","protected"],"export_time":"Oct 15 2024 04:33:06
UTC","event":"Export Event"}
```

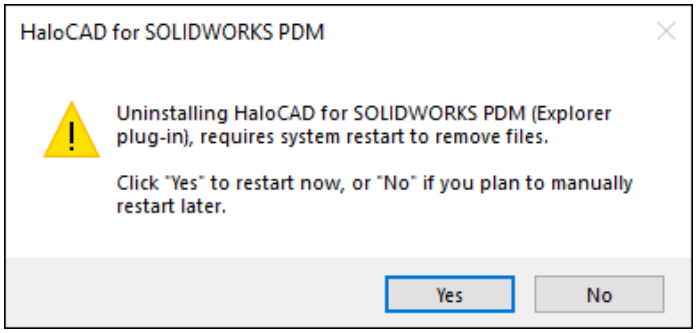

JSON sample

7.5. 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.

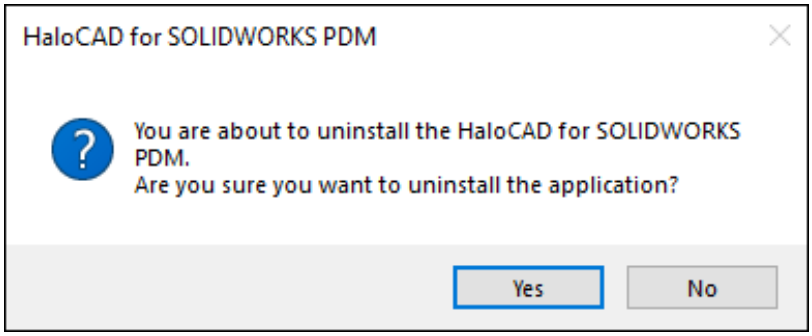
Method #1

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.



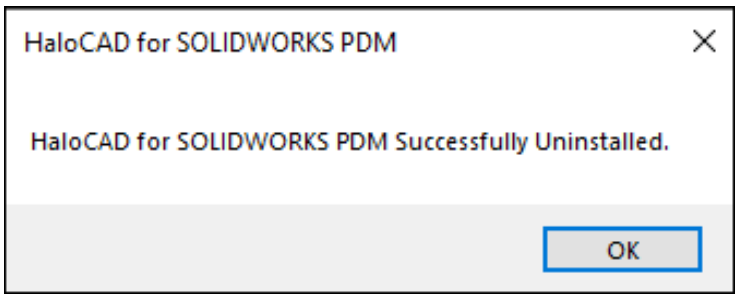
Uninstall Message #1

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 will appear.



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

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.