Secude

HaloSHARE

Installation and Configuration Manual

Version 1.0

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 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

HaloSHARE secures internal and external business workflows by providing centralized bulk file protection, including classification, sensitivity labeling, encryption, password-based access control, digital signing, Controlled Unclassified Information (CUI) marking, and watermarking.

HaloSHARE extends Microsoft Purview Information Protection (MPIP) to CAD, Microsoft Office, and non-Office file formats, including text and PDF files stored in shared folders. It protects sensitive data by applying customizable sensitivity labels that support tracking, revocation, and expiration.

1.1. What distinguishes HaloSHARE?

Digital transformation improves supply-chain efficiency, but it also increases the risk of data exposure. When users share unprotected files, organizations face potential data leaks, operational disruption, and financial loss. In shared environments, unauthorized access and accidental file sharing are common risks. To protect business operations without interrupting workflows, project files must be secured by default.

HaloSHARE automatically protects files placed in a predefined local folder (the HaloSHARE radius) on systems where HaloSHARE is installed, such as OneDrive or SharePoint. When a file enters the HaloSHARE radius, HaloSHARE automatically encrypts it to prevent unauthorized access and accidental sharing, both inside and outside the organization.

HaloSHARE also supports watermarking, CUI marking, digital signing, password protection, and metadata tagging. These capabilities enable secure file sharing and tracking while preserving user productivity.

By implementing HaloSHARE, organizations can reduce the risk of data breaches, support compliance with data protection regulations, and eliminate manual file-security processes.

1.2. About this Manual

This guide provides step-by-step instructions for installing and configuring HaloSHARE. It is intended for system administrators and IT professionals responsible for deploying HaloSHARE in an enterprise environment.

The guide covers the following tasks:

- Installing HaloSHARE
- Configuring core features and security settings
- Troubleshooting common issues

1.3. Features

HaloSHARE provides the following capabilities:

- Protects multiple files in folders in bulk.
- Applies label-based protection using Microsoft Purview Information Protection (MPIP) and user-defined custom permissions.
- Lets you customize protection settings for specific file types.
- Enables easy removal of protection and re-labeling of files using existing labels.
- Applies bulk watermarking to sensitive content, with visible, unique, date-stamped sharing indicators to improve security and visibility of ownership.
- Adds custom properties to enhance file security and provide contextual awareness.

1.4. Feature Availability and Setup Requirements

Feature name	Description	Setup requirements
HaloSHARE with MPIP protection	Applies sensitivity labels, supports re-labeling, and performs file encryption and decryption.	Requires a valid license key with MPIP protection enabled.
HaloSHARE with watermark	Adds watermark text as a visual indicator. Supports watermarking for PDF, CAD, and Microsoft Office files.	Requires a valid license key with the watermark feature enabled.
HaloSHARE with compliance marking	Applies CUI markings to PDF and Microsoft Office files.	Requires a valid license key with the CUI feature enabled.
HaloSHARE with password protection	Protects files using a user-defined password.	Requires a valid license key with the Password Protection feature enabled.
HaloSHARE with file signing	Protects files using a digital signature.	Requires a valid license key with the File Signing feature enabled.
HaloSHARE with metadata marking	Embeds user-defined tags into files for classification and tracking.	Requires a valid license key with the Metadata Marking feature enabled.

Feature set up

License Combinations in HaloSHARE

The list above outlines the basic licenses available with HaloSHARE. Depending on user requirements, license combinations are also offered. For example, HaloSHARE protection with watermarking for PDF files, or HaloSHARE watermarking for Office files combined with CUI marking for PDF files.

1.5. General FAQs

This section provides answers to the most frequently asked questions (FAQ). If you have any further inquiries, don't hesitate to get in touch with our sales representative or support team.

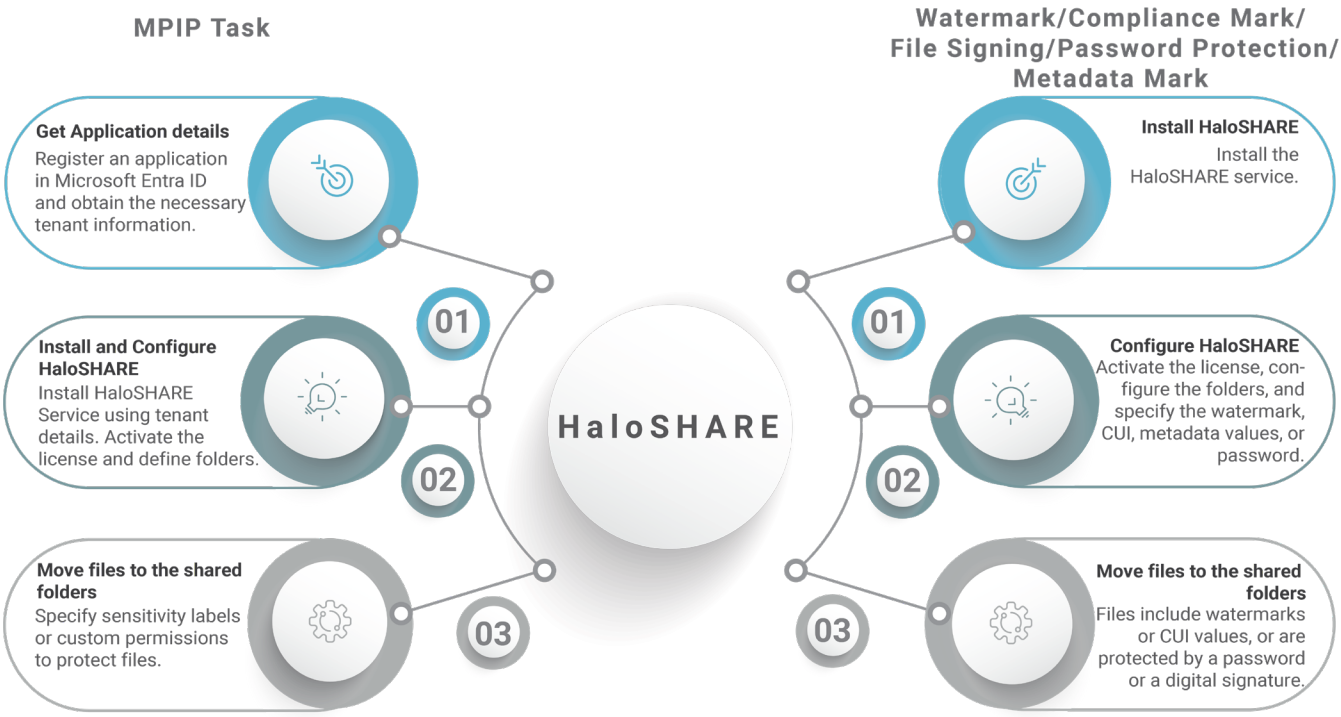
1. **What does HaloSHARE provide for an organization?**
   This labeling solution protects your files and enforces security throughout their full life cycle.
2. **Does it protect all native Computer-Aided Design (CAD) file types?**
   Yes, HaloSHARE supports all CAD native file types.
3. **What happens if an unauthorized person attempts to open a HaloSHARE-labeled file?**
   Initially, user authentication occurs. It is a process of verifying a user's identity. If the user fails authentication, they will be prompted with an error message and denied access.
4. **Who decides what labels should be used for various supplier folders and how they are managed in the background?**
   In an organization, an MPIP administrator is responsible for creating and managing labels (user rights) in the Microsoft Purview portal. The choice of label can be made by engineers or designers who create drawings for a specific supplier.
5. **What if I don't want a certain file type to be protected?**
   HaloSHARE encrypts any file based on the extension specified in the configuration. As a result, you can whitelist file types to be encrypted and blacklist file types by not defining them in the configuration.
6. **Is it possible to apply custom permissions to protect a file?**
   Yes, HaloSHARE allows users to apply custom permissions without using MPIP labels.
7. **How to open a protected CAD file?**
   You can view a Protected CAD file using a HaloCAD Add-on for CAD applications.
8. **How to open a protected PDF file?**
   You can view a protected PDF file using Adobe Acrobat Reader DC/Acrobat DC or the Microsoft Edge browser. Additionally, it can be opened with the Microsoft Purview Information Protection viewer.

9. **How do I view the watermark on a CAD file?**

   When a HaloSHARE-watermarked CAD file is shared with external partners, they can view it by installing the HaloCAD Add-on for CAD applications.

2. Quick Start Installation Summary

The following image shows a high-level overview of installing the HaloSHARE service.



Quick start implementation steps

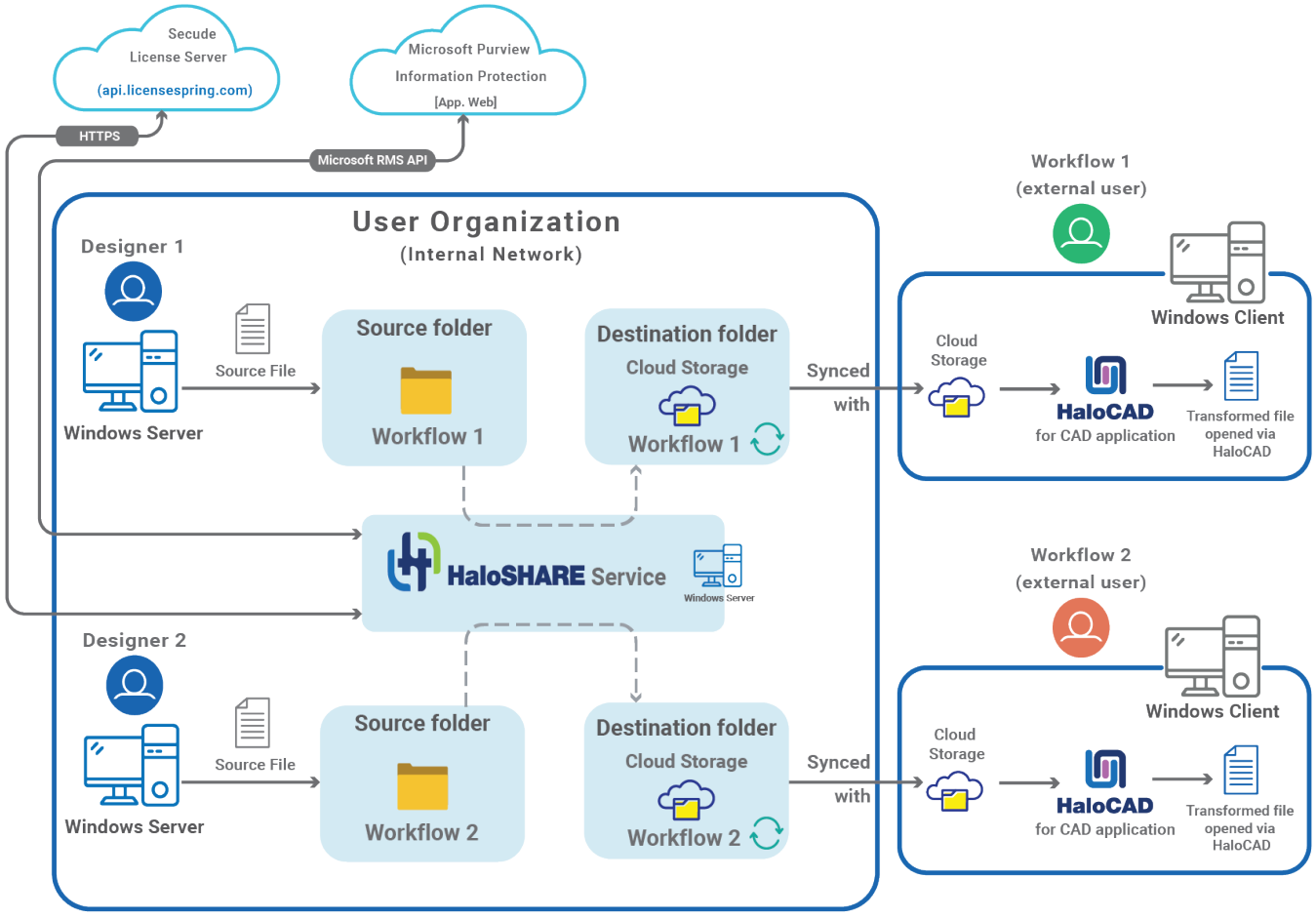
3. Architecture

In the following scenario, designers from an organization share their work with partners. To facilitate this, the HaloSHARE configuration screen allows your administrator to assign source and destination folders for the designer's external partners. The configuration can be set to move files from a source folder to a destination folder, as illustrated below.

Workflow Source Folder (from designer)	Workflow Destination Folder (to external partner)
`C:\Prestin Engineering\External User 1`	`C:\SharePoint\External User 1`
`C:\Prestin Engineering\External User 2`	`C:\OneDrive\External User 2`

Source and destination Folders

At a high level, the HaloSHARE workflow consists of these steps:



Architecture

Shared folder location

An external, user-specific shared folder may be located on OneDrive, SharePoint, or Autodesk Forma (formerly ACC Docs).

Based on the workflow configuration, the following tasks take place:

- **HaloSHARE with MPIP Task**
  HaloSHARE scans the folder and its subfolders for new files, determines whether they need encryption, and applies the appropriate MPIP label or custom permission. The labeled files are then moved to destination folders, typically external user–specific shared folders.
- **HaloSHARE with Watermark Task**
  HaloSHARE scans the folder and its subfolders for new files. When a new file is detected, it is automatically watermarked with user-specified text. The watermarked files are then moved to destination folders, typically external user–specific shared folders.
- **HaloSHARE with Compliance Mark Task**
  HaloSHARE supports Controlled Unclassified Information (CUI) Marking with the Limited Dissemination Control (LDC) or Distribution Statement options. However, neither option can be applied simultaneously to the same file. The first page of the document displays the values for the CUI designation indicator block, as configured.
  HaloSHARE scans the folder and its subfolders for new files. When a new file is detected, it automatically embeds the user-specified CUI values. The CUI-embedded files are then moved to destination folders, typically external, user-specific shared folders.
- **HaloSHARE with File Signing Task**
  HaloSHARE scans the folder and its subfolders for new files. When a new file is detected, HaloSHARE automatically applies a digital signature. The signed files are then moved to the destination folders, typically external user–specific shared folders.
- **HaloSHARE with Password Protection Task**
  HaloSHARE scans the folder and its subfolders for new files. When a new file is detected, HaloSHARE automatically applies a user-defined password. The protected files are then moved to the destination folders, typically external user–specific shared folders.
- **HaloSHARE with Metadata Mark Task**
  HaloSHARE scans the folder and its subfolders for new files. When a new file is detected, it automatically embeds the user-specified metadata values. The embedded metadata files are then moved to destination folders, typically external, user-specific shared folders.

External users, including suppliers, vendors, and external consultants, can access HaloSHARE-protected and watermarked files only through the HaloCAD Add-on. For more details, refer to the HaloCAD manuals.

4. System Requirements

The following table outlines the minimum and recommended technical specifications, including software and network requirements, required to run the product.

Components	Details
Operating System	1. Supported in Microsoft Windows Server 2022 and above. 2. Requires **.NET** Framework 4.6.2 and above. 3. Latest Windows system updates installed.
MPIP task label protection-specific requirements	
Office 365 Subscription	1. An Azure subscription is required to use Azure RMS and the MPIP functionality. 2. A working Microsoft Entra ID service must be available. 3. Microsoft Purview Information Protection must be fully configured. 4. HaloSHARE creates an outbound network communication with Microsoft Azure Services. 5. TLS 1.2 or higher must be enabled to ensure the use of cryptographically secure protocols. 6. Register an application to get the Application (client) ID and Tenant ID in the Azure portal. 7. Refer to the table below, "**Recommended URLs, Addresses, and Ports for MPIP**" to know about the service endpoints.
Supported file types	1. `.dwg`, `.dxf`, `.ipt`, `.iam`, `.idw`, `.ipn`, `.rvt`, `.rfa`, `.prt`, `.asm`, `.drw`, `.frm`, `.mfg`, `.sec`, `.lay`, `.par`, `.dft`, `.eps`, `.emn`, `.emp`, `.psm`, `.jt`, `.sldprt`, `.sldasm`, `.slddrw`, `.slddrt`, `.dgn`, `.step`, `.ige`, `.iges`, `.neu`, `.log`, `.3dm`, `.3ds`, `.acis`, `.amf`, `.catpart`, `.catproduct`, `.cgr`, `.dae`, `.dwf`, `.easm`, `.fcstd`, `.g`, `.gcode`, `.gltf`, `.glb`, `.icd`, `.igs`, `.iv`, `.model`, `.obj`, `.pic`, `.plmxml`, `.sat`, `.smt`,

Components	Details
	`.stl`, `.stp`, `.ste`, `.stpz`, `.tcw`, `.u3d`, `.unv`, `.usdz`, `.vda`, `.pvz`, `.qif`, `.wrl`, `.x_b`, `.x_t`, `.xaml`, `.z3`, and `.zip`. 2. Creo file formats with iteration: `.prt`, `.asm`, `.sec`, `.frm`, `.drw`, `.lay`, `.cem`, `.mfg`, `.neu`, `.log`, and `.pvz`. 3. Microsoft Office and non-Office file formats.
Autodesk Forma specific requirements	
Autodesk Platform Services	Register an application in Autodesk Platform Services to obtain the Client ID and Client Secret.
Watermark task specific requirements	
Supported file types	`.pdf`, `.docx`, `.xlsx`, `.pptx`, `.dwg`, `.rvt`, and `.ifc`.
Supported CAD application for watermark	1. AutoCAD 2023, 2024, 2025, 2026 2. Revit 2023, 2024, 2025, 2026
Application for viewing protected and watermarked files	1. HaloCAD Add-on for CAD application. 2. To view metadata in a Revit application, you need to install the **RevitLookup** tool.
File Signing task specific requirements	
Supported file types	Microsoft Office and PDF file types
Metadata task specific requirements	
Supported file types	Microsoft Office and PDF file types
Password Protection task specific requirements	
Supported file types	Microsoft Office file types
Compliance Mark(Controlled Unclassified Information) task specific requirements	
Supported file types	1. Supported: `.pdf`, `.docx`, and `.pptx` 2. Unsupported: `.xlsx`

Requirements

5. Prerequisites

Before you install the HaloSHARE, there are a few things that you need.

5.1. MPIP Protection

This section is specific to the MPIP feature.

5.1.1. 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.

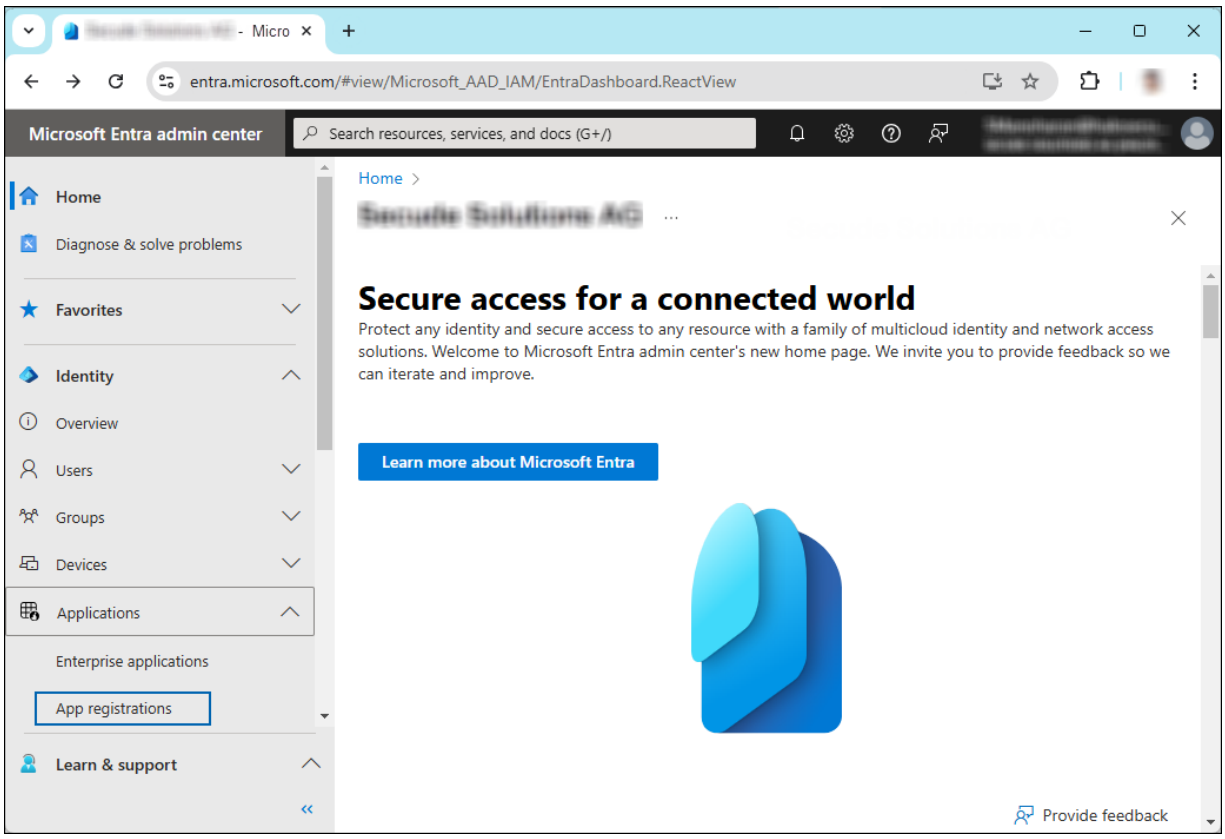
Microsoft documentation
Registering an application in Microsoft Entra ID establishes a trust connection between your application and the identity provider, the Microsoft identity platform.
The information in the Microsoft documentation overrides any information published in this section. For a comprehensive description, refer to Microsoft documentation.

Prerequisite: You must have sufficient permissions to register an application with your Microsoft Entra ID tenant.

5.1.1.1. Create an Application

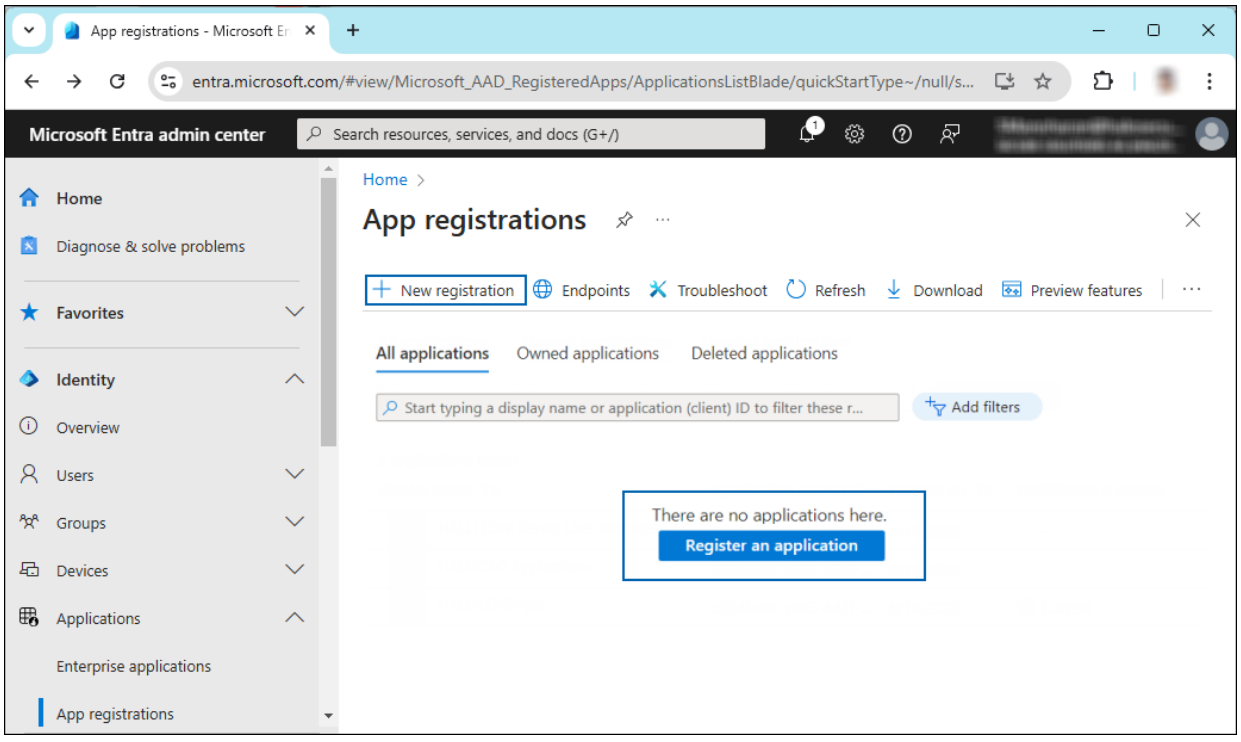
Follow these steps to register the application:

1. Log in to the Microsoft Entra admin center using an account that has administrator privileges.
2. If you have access to multiple tenants, click the Settings icon in the top menu and select the tenant for which you want to register the application from the **Directories + subscriptions** menu.
3. You will be directed to the homepage.



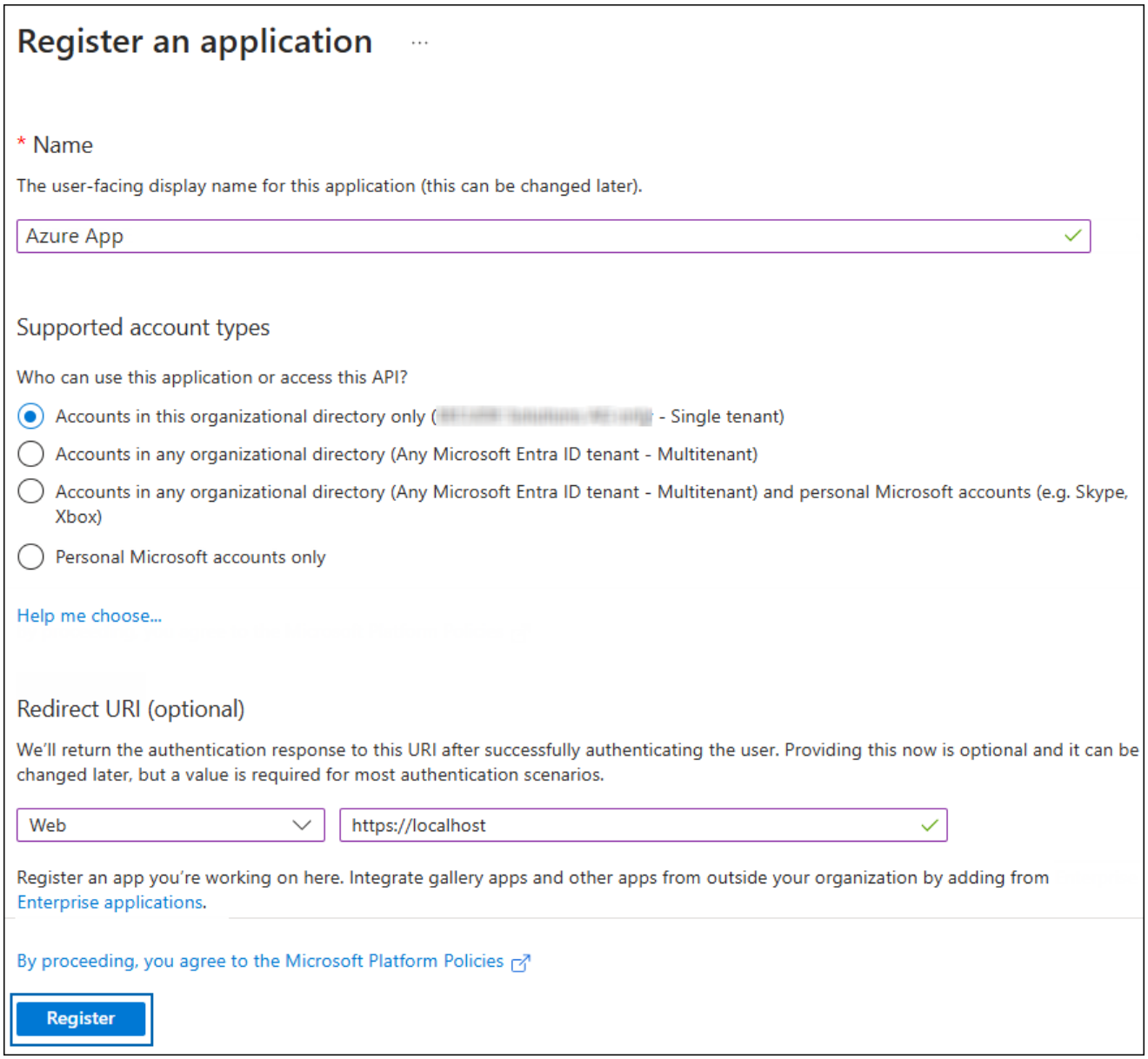
Selecting Microsoft Entra ID

4. On the left side of the navigation pane, click **Identity** > **Applications** > **App registrations**.
5. On the **App registrations** page, click the **New registration** page or **Register an Application** button (this button appears only if no applications have already been created).



New application registration

6. On the **Register an application** page, enter the registration details for your application.



Application details

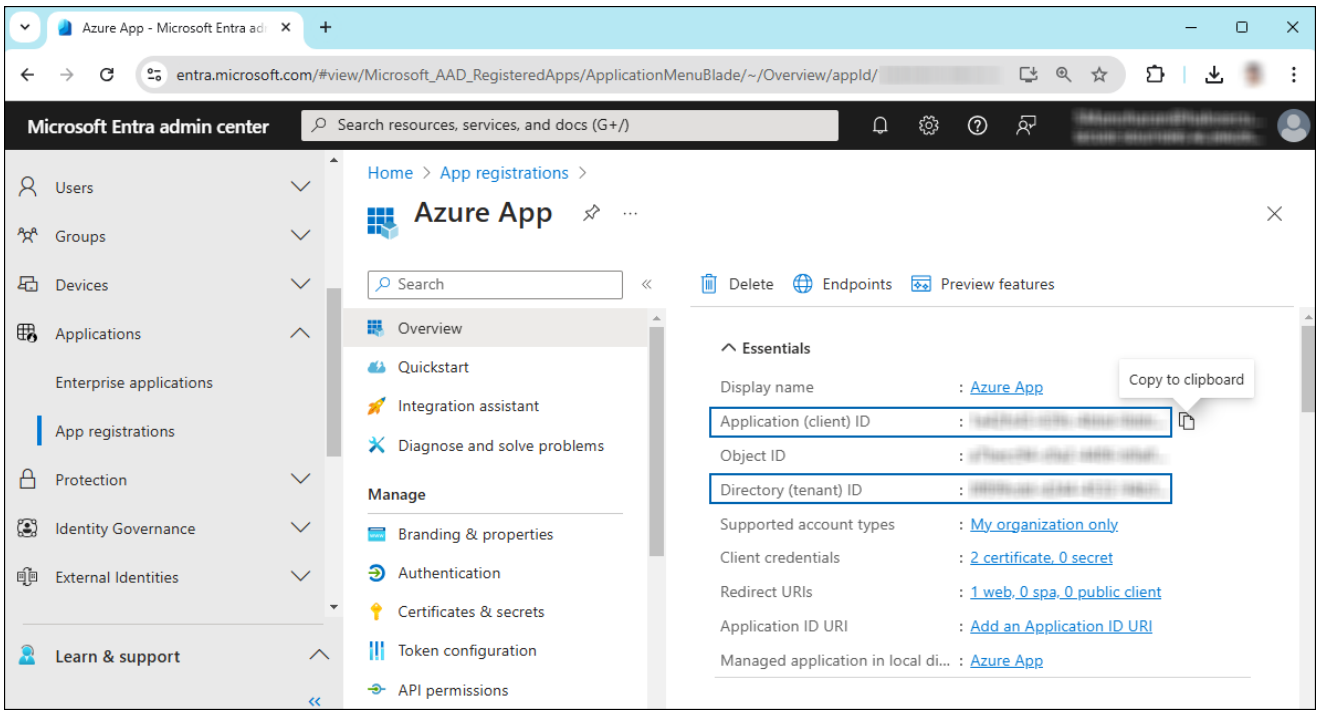
a. In the **Name** field, enter an appropriate application name.

b. Under **Supported account types**, select the option **Accounts in this organizational directory only (single tenant)**. As of now, the HaloSHARE Service supports only a single tenant.

c. Under **Redirect URI**: Select **Web**, and then type a valid redirect URI for your application. For example, `https://localhost`.

d. When finished, click **Register**.

7. The home page of the new application is created and displayed.



Application ID and Tenant ID

8. 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** – also known as **Client ID**.
   b. **Directory ID** – also known as **Tenant ID**.

Save the authentication parameters

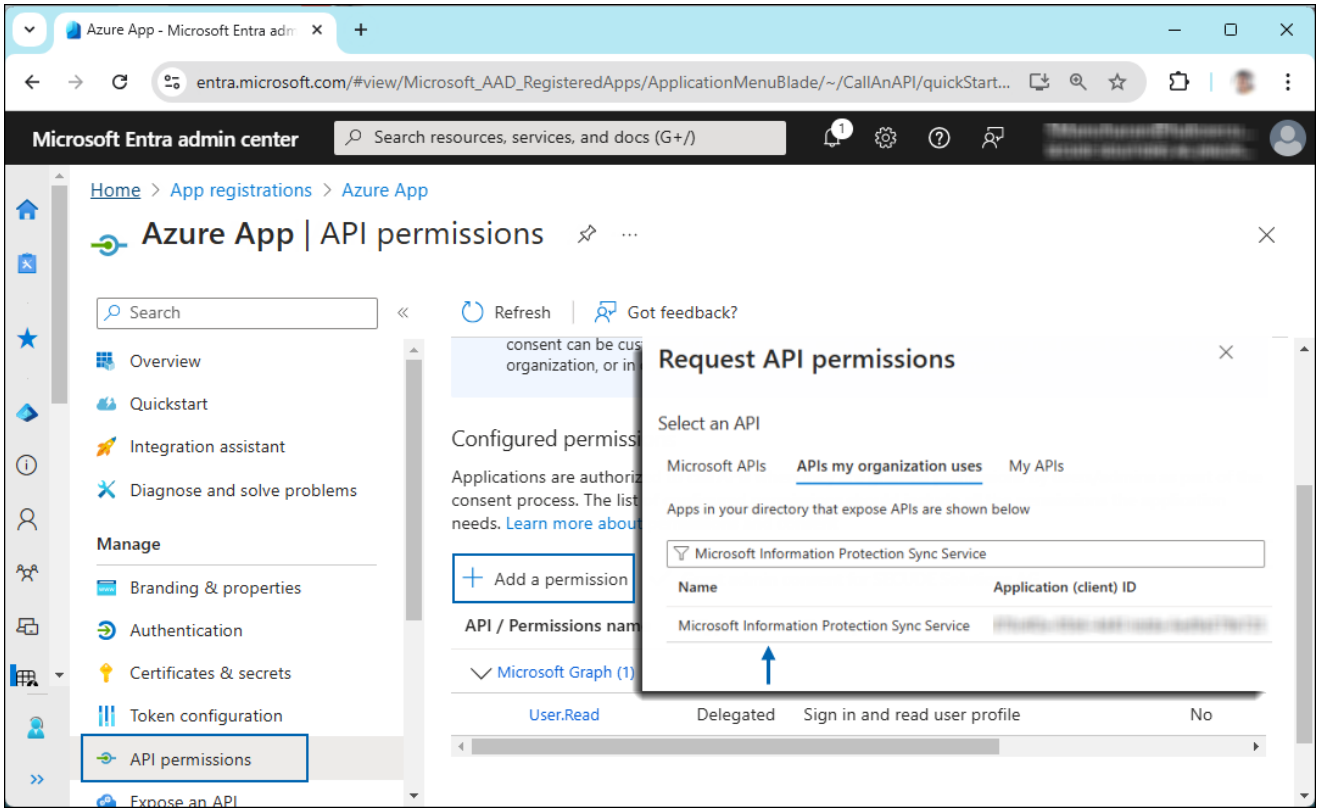
In a text editor (such as Notepad), copy the value of **Application (client) ID** and **Directory (tenant) ID**, and save it for initializing the HaloSHARE.

5.1.1.2. Add Required Permissions

To protect content with MIP SDK, you must provide the necessary API permissions to the application created in the previous section.

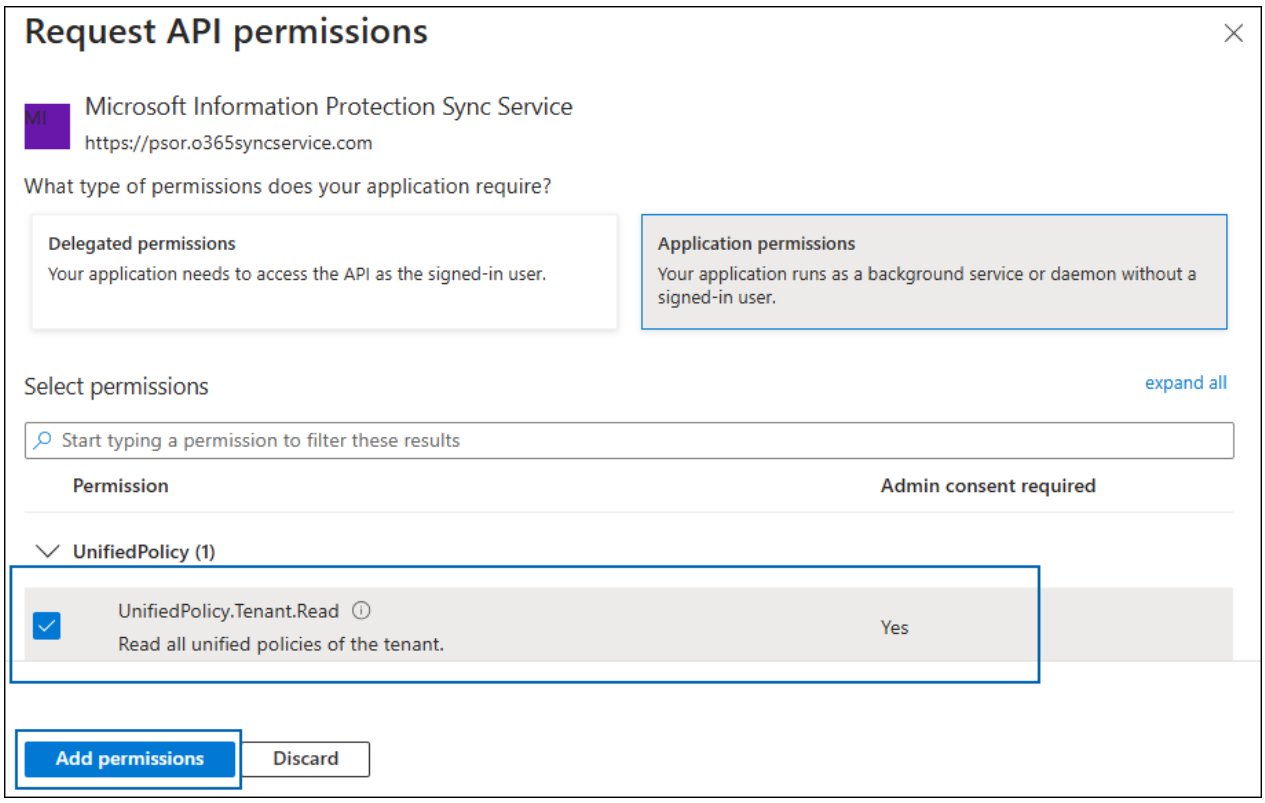
1. In the application page sidebar, select **API permissions**. The **API permissions** page for the new application registration page appears.
2. Click **Add a permission** button. The **Request API permissions** page appears.
3. Under the **Select an API** setting, select **APIs my organization uses**. A list appears containing the applications in your directory that expose APIs.
4. In the search box, type in the name of the permission indicated in the "Required Permissions" table below. Alternatively, you could scroll to find the API.

5. For example, type **Microsoft Information Protection Sync Service** into the search box. The following figure shows how the API is listed:



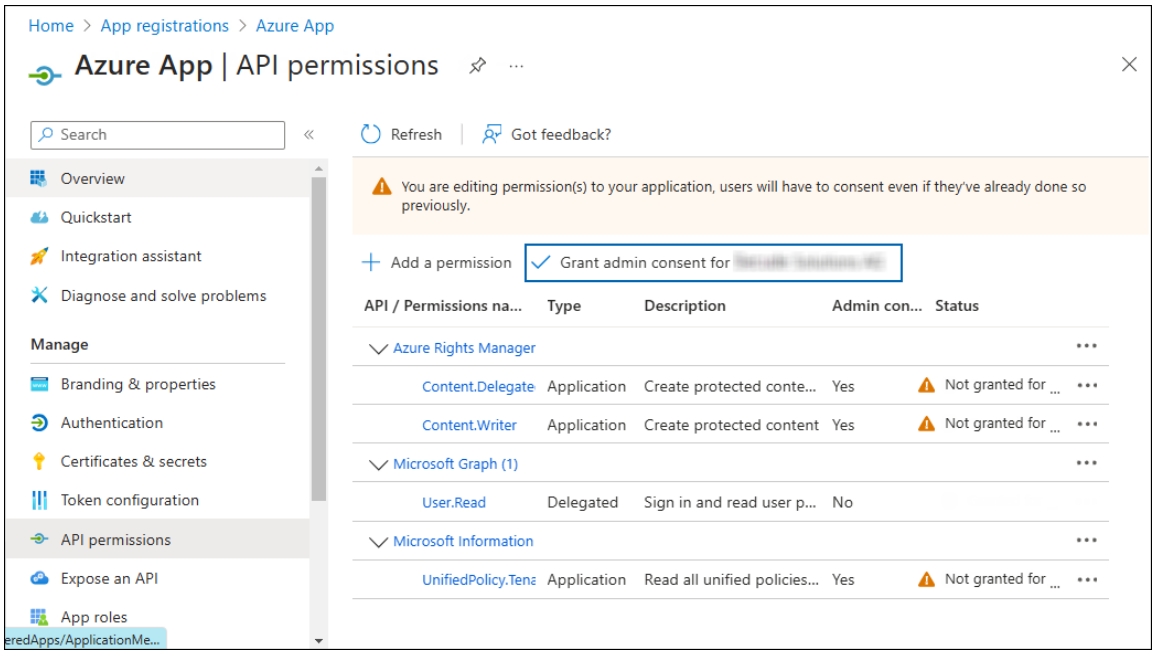
API selection

6. Now, click on the displayed API. You can see two permission types on the page: **Delegated permissions** and **Application permissions**.
7. Click **Application permissions** button and then under the **Permission** section, select the check box near **Read all unified policies of the tenant**.



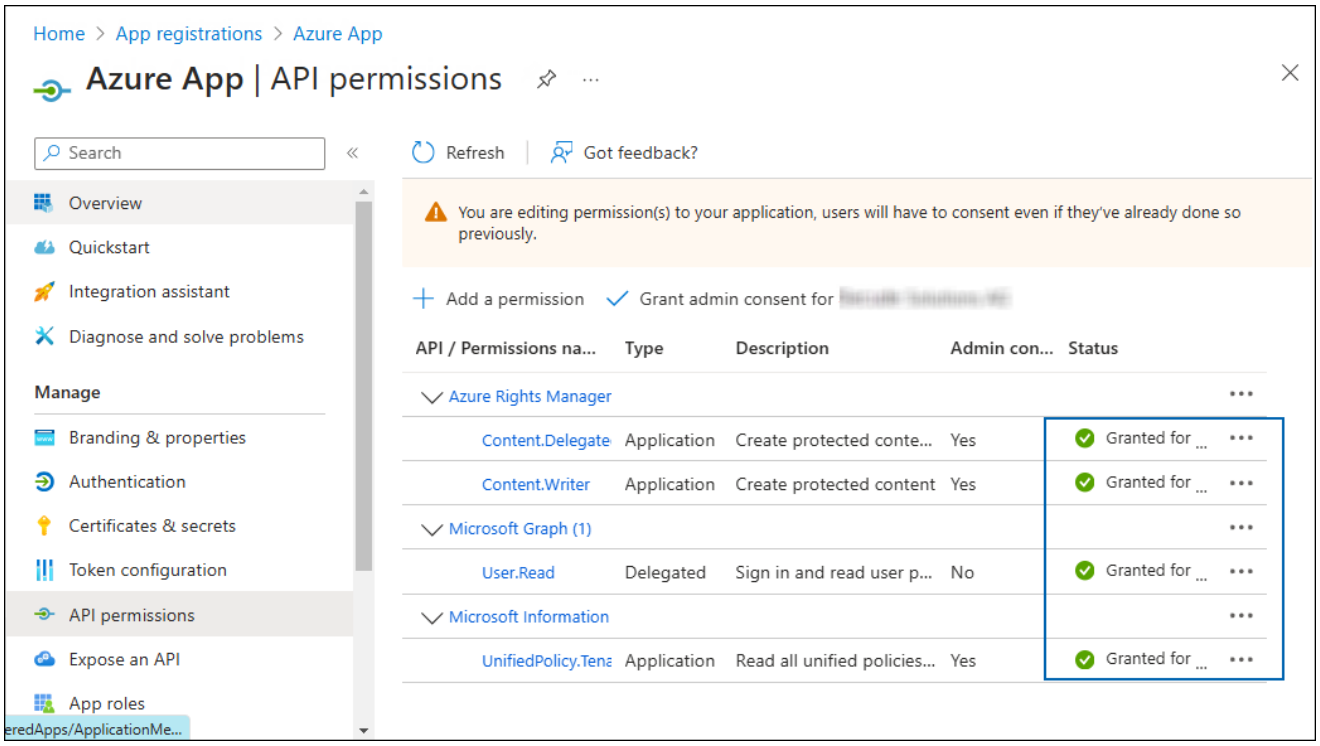
Adding permission

8. Click **Add permissions**.
9. Repeat the steps above to add the other required permissions listed in the “Required permissions” table below.
10. You will be taken back to the **API permissions** page, where the permissions have been saved and added to the table with the status **Not granted**.



Required API Permissions

11. Click **Grant admin consent for your company** button. You will be prompted to accept the consent confirmation; click **Yes** to the question.
12. After accepting the admin consent, the **Status** will change to **Granted**.



API Permissions with admin consent

13. The following table lists the required permissions.

API / Permission Name	Display Name	Type	Description
Microsoft Graph	`User.Read`	Delegated	Sign in and read the user profile. This API permission is added by default, but HaloSHARE does not use it.
Azure Rights Management Services (Microsoft Rights Management Services)	`Content.DelegatedWriter`	Application	Create protected content on behalf of a user
	`Content.Writer`	Application	Create protected content
Microsoft Information Protection Sync Service	`UnifiedPolicy.Tenant.Read`	Application	Read all unified policies of the tenant

Required permissions #1

Additional Permission (Only for Relabeling)

The above permissions are sufficient to apply the MPIP label to a file. In addition, HaloSHARE requires the following superuser privilege to relabel a file if the service is not the owner of the file.

API / Permission Name	Display Name	Type	Description
Azure Rights Management Services (Microsoft Rights Management Services)	`Content.SuperUser`	Application	Read all protected content for this tenant in the Azure portal

Required permissions #2

5.1.1.3. Upload the Certificate in the Azure Portal

HaloSHARE uses certificate-based authentication, so you must enter your certificate information in the registered application.

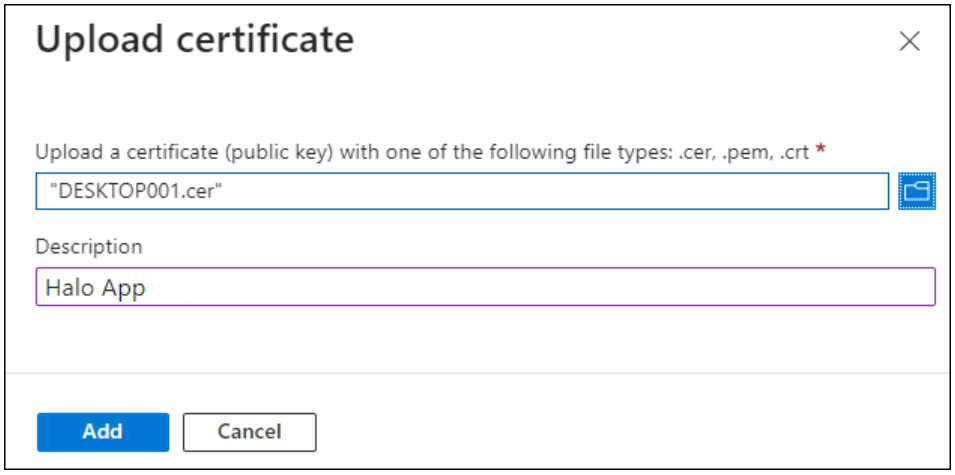
Prerequisites:

1. **Certificate**:
   a. Make sure to have a valid certificate that contains keys such as `-KeyExportPolicy Exportable` and `-KeySpec Signature`.
   b. And that can also be a self-signed certificate. Note: As a best practice and for security reasons, we recommend using a self-signed certificate in a test environment, and NOT recommended for a production environment.
2. **Install the certificate**:
   a. Make sure to install this certificate on a Windows Server machine where HaloSHARE will be installed.
   b. The Certificate Store can be either **Current User** or **Local Computer**.
   c. If it is a self-signed certificate, it should also be installed in the **Trusted Root Certification Authorities** store.
   d. If the certificate is signed, the root CA and any intermediate CA (if applicable) should also be installed in the appropriate trusted store.

To upload the public key of the certificate, follow the steps below:

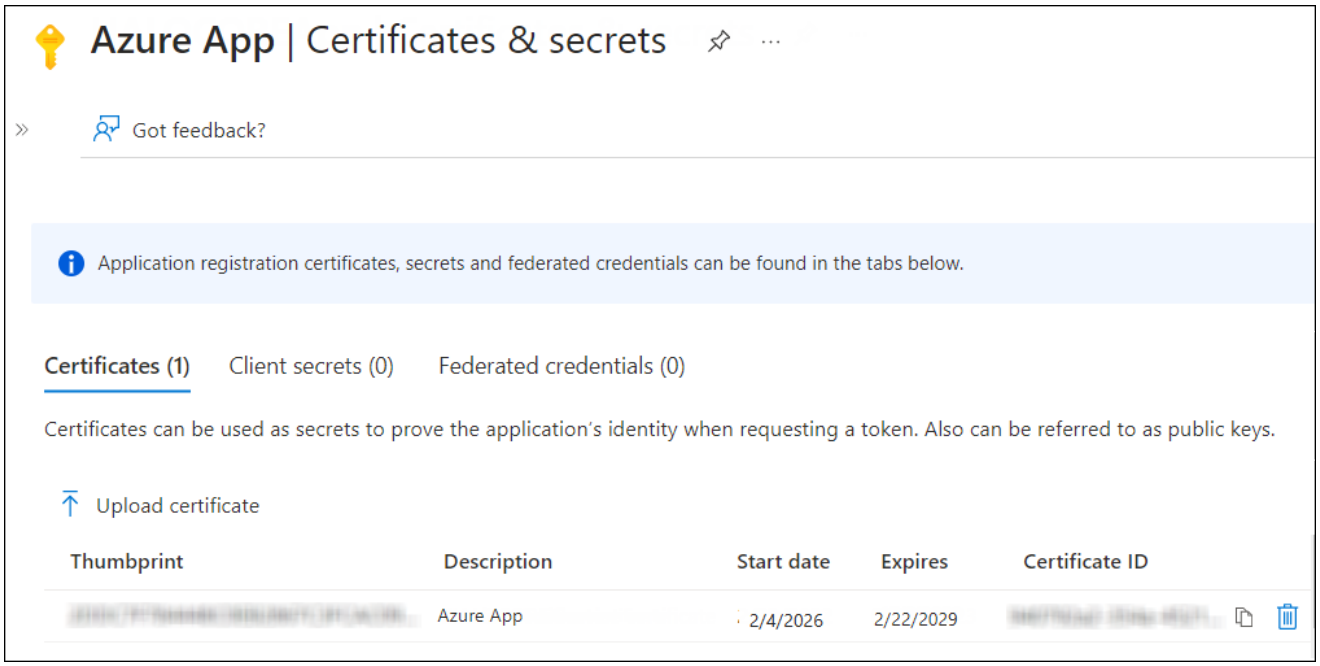
1. In the sidebar of the new application page, select **Certificate & secrets**.

2. Under the **Certificate** section, click **Upload certificate**. The **Upload certificate** dialog appears as shown in the figure below:



Upload certificate #1

3. Click on the folder icon to select the certificate and click **Open**. For illustration purposes, the file `DESKTOP001.cer` is used.
4. Now, click **Add**. The certificate will get uploaded, and its thumbprint will be displayed on the page as shown in the figure below:



Upload certificate #2

5. You are now ready to install the HaloSHARE.

5.1.2. 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.

5.1.3. 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`

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

Registry entries

5.2. Register an application in Autodesk Platform Services

This section describes how to register an application, obtain the Client ID and Client Secret, and assign access permissions.

Prerequisites:

- Ensure that specific URLs and protocols required for Autodesk subscription licensing are allowed through the firewall or proxy system.
- If the computer connects to the internet via a firewall or proxy server, configure the proxy to allow unrestricted and anonymous access to the required domains.
- Allow access to the URL `developer.api.autodesk.com` over port 443 (HTTPS).
  The default ports used are 80 (HTTP) and 443 (HTTPS).
- Ensure access to relevant Certificate Authority (CA) endpoints (for example, `digicert.com`) over port 80 for CRL (Certificate Revocation List) verification.

To complete this setup, you need:

- An APS account
- A developer hub

If you do not have an APS account, start with the section Create an APS account. If you already have an account, continue with Set up a developer hub.

5.2.1. Create an APS Account

If you do not have an Autodesk account, create one as follows:

1. Go to the Autodesk Platform Services website.
2. Click **Sign in** in the upper-right corner.
3. Click **Create account**.
4. Follow the on-screen instructions to complete account setup.

5.2.2. Set up a Developer Hub

A developer hub is used to create and manage APS applications.

- If you are part of a team, your team might already have a developer hub. Ask your team administrator to add you, and then continue with Create an application.
- If your team has an Autodesk Platform Services plan but has not created a developer hub, see Create a developer hub.

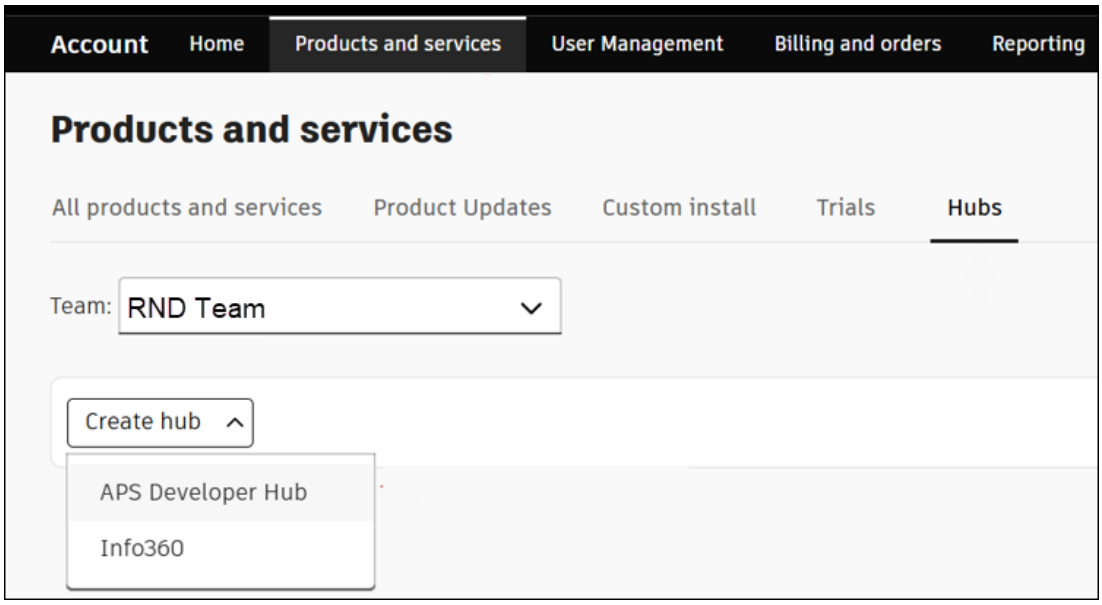
5.2.3. Create a Developer Hub

Prerequisites

- An Autodesk account (created in the previous step)
- An Autodesk team with an APS subscription (Free tier or Paid)

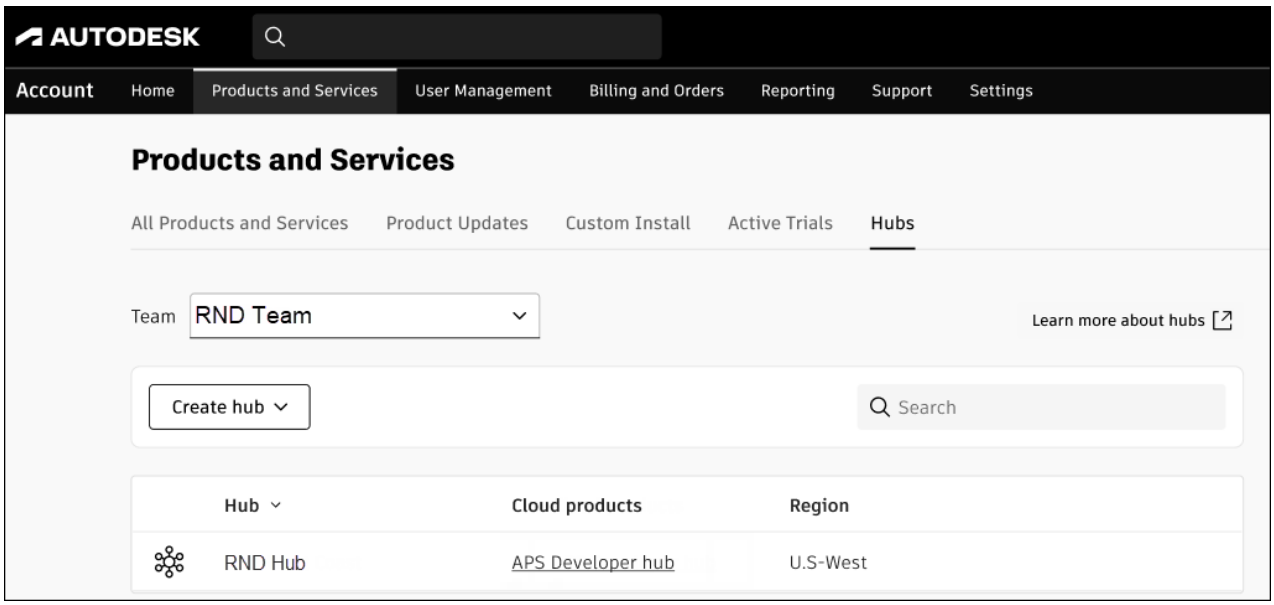
Procedure

1. Log in to https://manage.autodesk.com using your Autodesk Account.
2. Click **Products and Services**, and then select the **Hubs** tab.



Products and Services

3. Choose the **Team** where the APS offering is assigned.
4. From the **Create hub** list, select **APS Developer Hub** as the product.
5. Enter a hub name and, optionally, provide a description. (for example, RND Hub)
6. Click **Create & Activate**.
7. Refresh the page, and then click the hub name to open the developer portal.

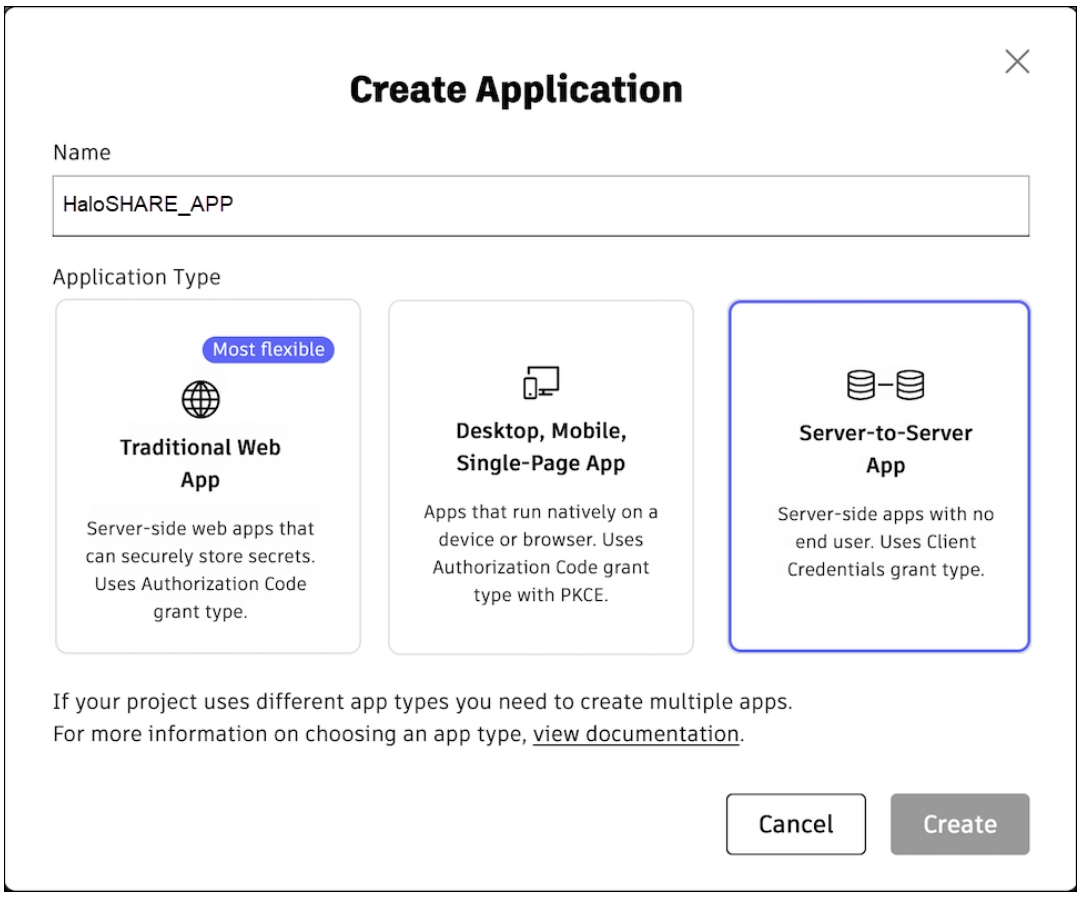


New hub

5.2.4. Create an Application Credentials

To authenticate with APS APIs, you must create an application to obtain the client ID and client secret.

1. Click the APS Developer Hub created in the previous section.
2. On the **Applications** page, click **Create application** in the top right corner.
3. The **Create Applications** window opens.
4. Enter a name for the application (for example, HaloSHARE_App).



Application name

5. The following application types are available. For HaloSHARE, select **Server-to-Server App**.
    - **Traditional Web App** – For applications that run on a server (for example, a web app with a backend server).
    - **Desktop, Mobile, Single-Page App** – For applications that run on a user's device (for example, mobile apps, desktop apps, or browser-based apps).
    - **Server-to-Server App** – For server-side applications that do not require user authentication (for example, background services or daemons).
6. Click **Create**.
7. A confirmation message appears after the settings are successfully saved.
8. Copy the **Client ID** and **Client Secret** from the **App Settings** and use them when configuring HaloSHARE.
9. Under **General Settings**, enter the redirect URI in the **JWKS URI.** For local development, you can use `https://localhost:8080`
10. Under **API Access**, select the **Data Management API** from the list.
11. Click **Save changes**.

5.2.5. Provide access to Autodesk Forma

Some Autodesk products require you to provision access for your application using its Client ID before integration.

Prerequisite: Ensure that you have administrator access to a Forma hub.

1. Log in to your Autodesk Forma hub.
2. Navigate to **Hub Admin**.
3. Select the required project.
4. On the **Hub Admin** page, go to **Custom Integrations**.
5. Click **Add Custom Integration**.
6. In the **Add custom integration** dialog box, enter the following details:
    - Client ID
    - Custom integration name
    - Description
7. Click **Next** and complete the process.

5.3. Watermarking CAD files

1. Ensure CAD applications such as Revit or AutoCAD are installed on the system where HaloSHARE will be installed. This check is necessary because the HaloSHARE installer installs the required watermarking files only if the relevant CAD application files are present.
2. Make sure the SharePoint folder is configured to sync with the mapped local drive. Files marked **Always keep on this device** have a green circle with a white checkmark  . This ensures that files are downloaded automatically to your machine.
3. Before you begin, ensure that the user who is running the service, or the specific group the user belongs to, is not assigned to the **Deny log on as a service** policy (**Local Security Policy** > **Security Settings** > **Local Policies** > **User Rights Assignment**). If the user(s) exist, the **Error 1069: The Service did not start due to a logon failure** message will appear while running the HaloSHARE.
4. **Watermark in Revit**: The **RevitLookup** tool is required to view custom properties (metadata) in Revit. After applying the watermark, navigate to **Revit Lookup** > **Dashboard** > **Schemas** > **HaloMetadataInfo** > **GetElements** > **GetEntity (Schema)** > **Get ()**.

5.4. File Signing Task

For file signing tasks, you can select either **Local Computer** or **Current User** during configuration. Both options have certain restrictions, as described below.

- If you select **Local Computer**, the service running user must have access to the Local Computer certificates or to the specific certificate in the Local Computer store. If the service running user is a local non-admin user, promote the service running user to a local admin user or grant the service running user access to the private key.
- If you select **Current User**, the selected certificate must be installed in the certificate store of the service running user.

5.5. General

1. To install the service, you must have local administrator privileges.
2. To run the service, you can use a user account with administrative privilege or non-administrative privilege.
3. The user who initializes the service should have appropriate permissions on the source and destination folders. In addition, the user running the service should have access to that network location as an IP address. For example, `\\10.0.0.138\foldername`

6. Installing the HaloSHARE

This chapter walks through the process of installing and configuring the HaloSHARE.

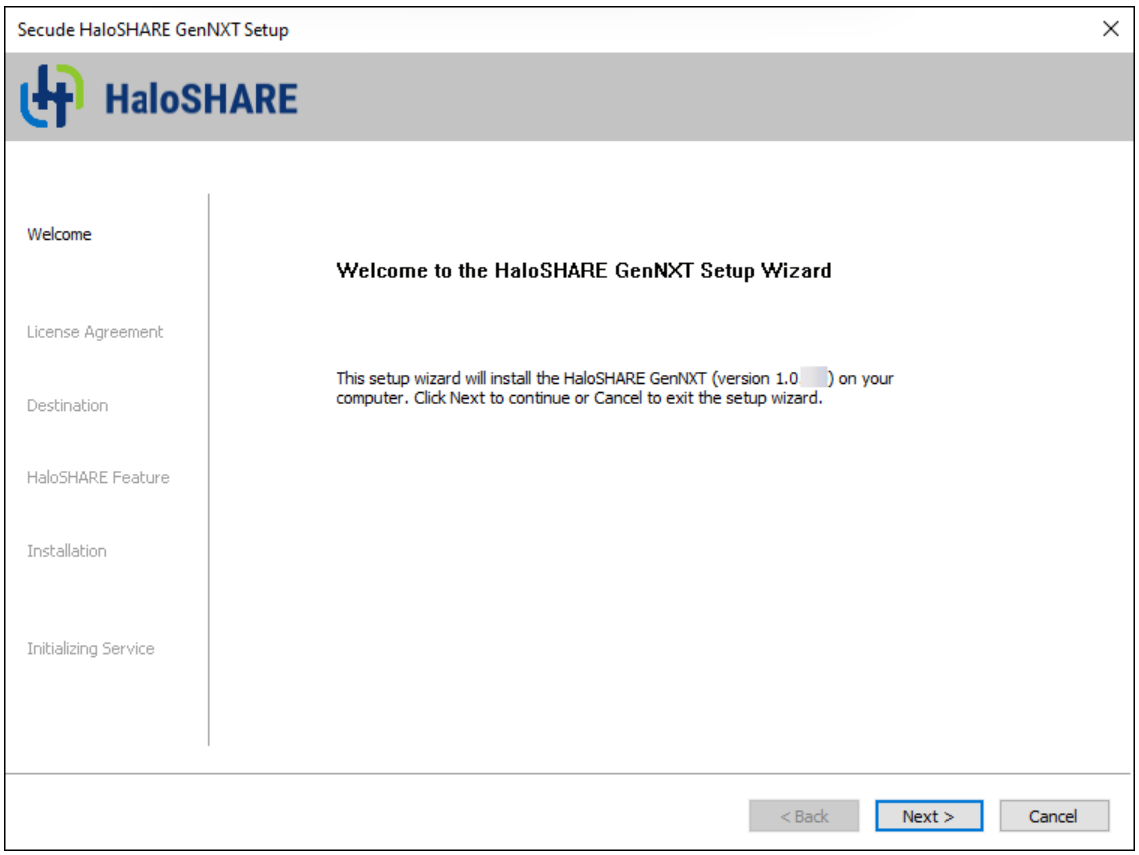
6.1. Interactive Installation

Install HaloSHARE using the GUI-based setup program provided in the installation package. Make sure the user who installs the HaloSHARE has administrator rights.

During installation, MPIP, Watermarking, and CUI Marking are listed as the main features. Selecting Watermarking or CUI Marking automatically includes Metadata, File Signing, and Password Protection capabilities. No separate check boxes are required.

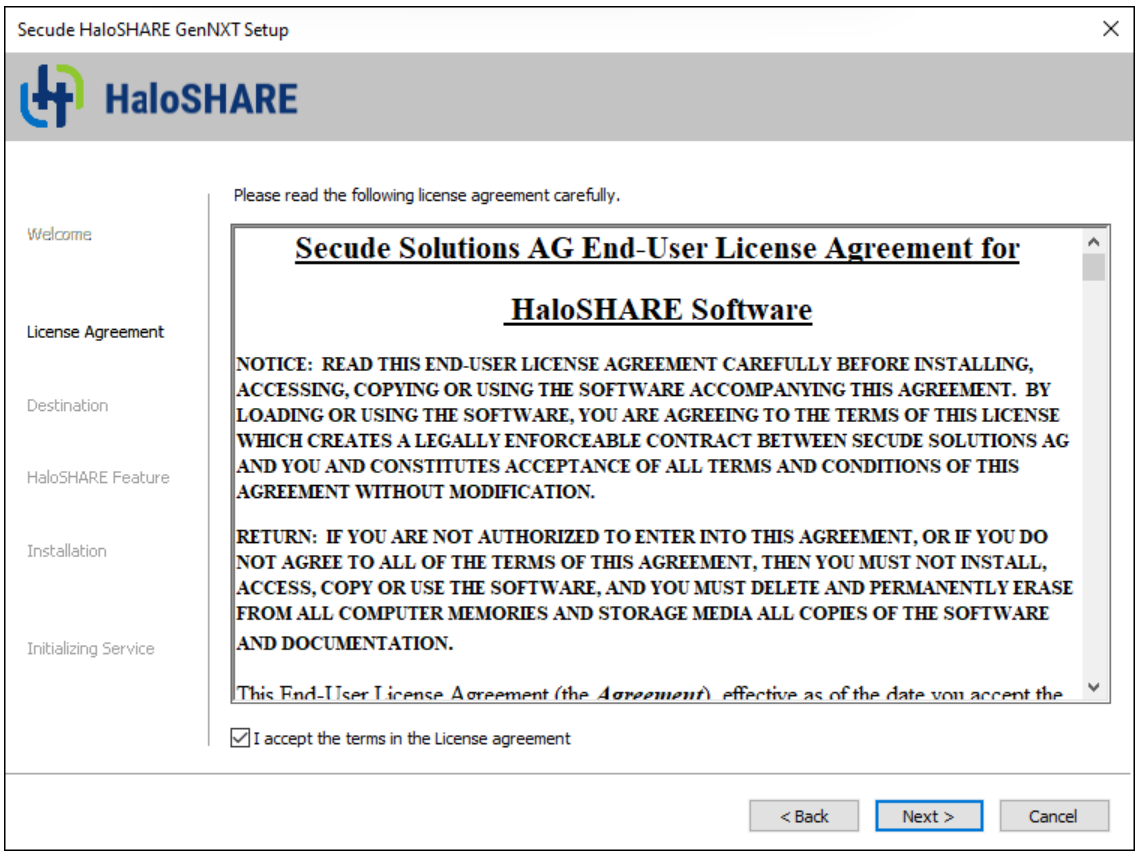
1. To begin the interactive installation, double-click the installer `HaloSHAREGenNXT_Setup.exe` file. Depending on your Windows security settings, a prompt may appear stating, *"Do you want to allow the following program to make changes to this computer?"* If this warning appears, click **Yes** to continue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

Startup dialog



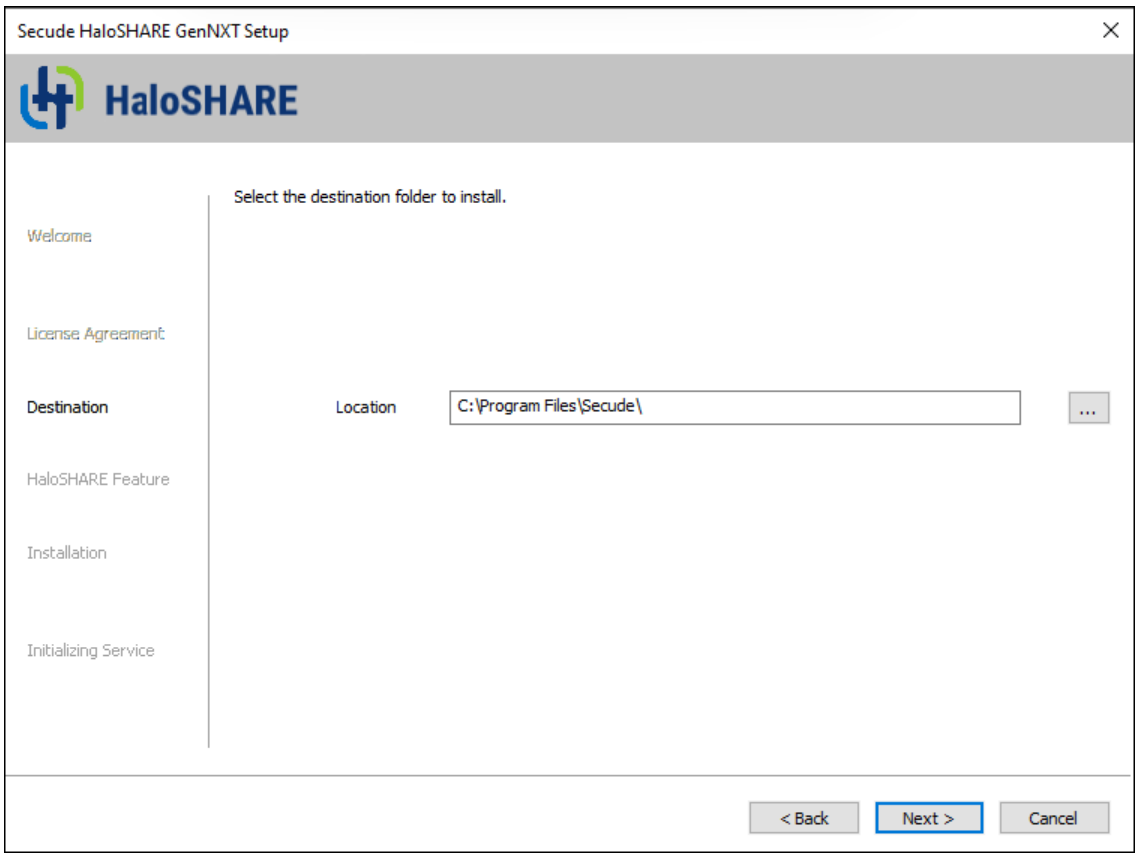
Welcome dialog

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



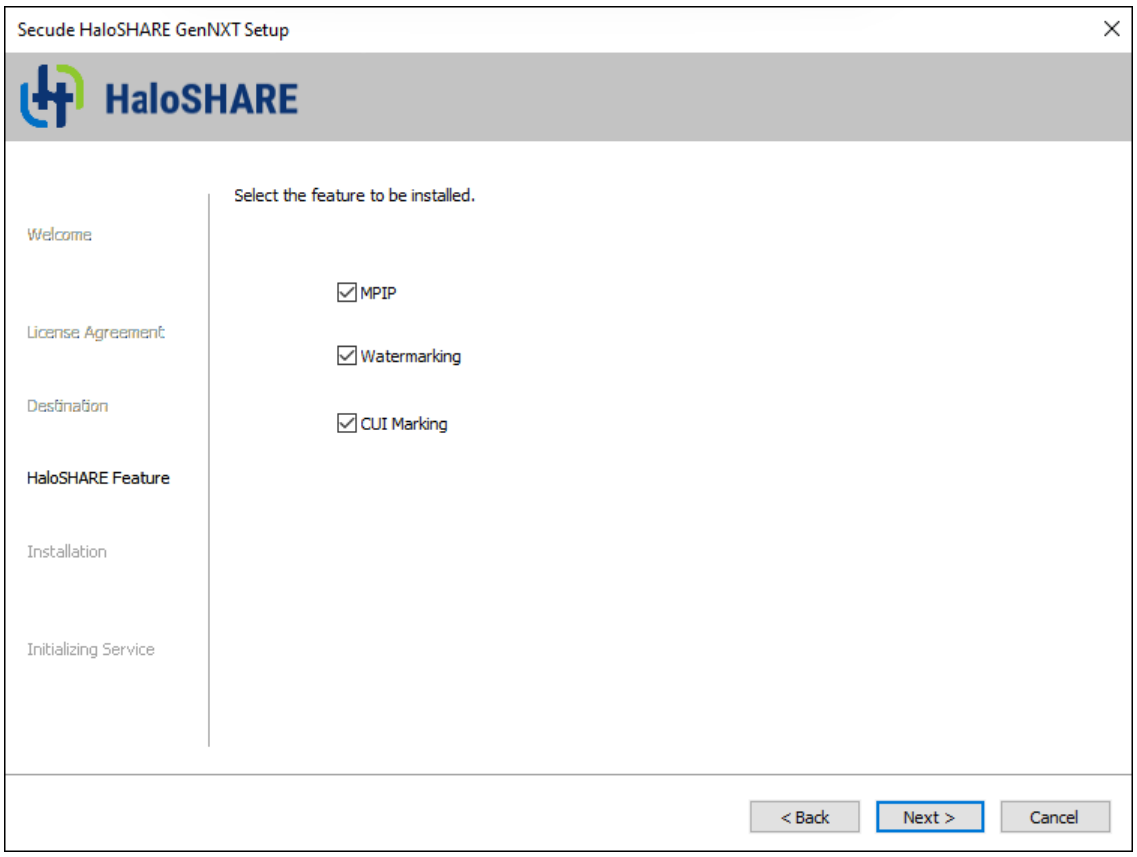
End-user License Agreement dialog

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



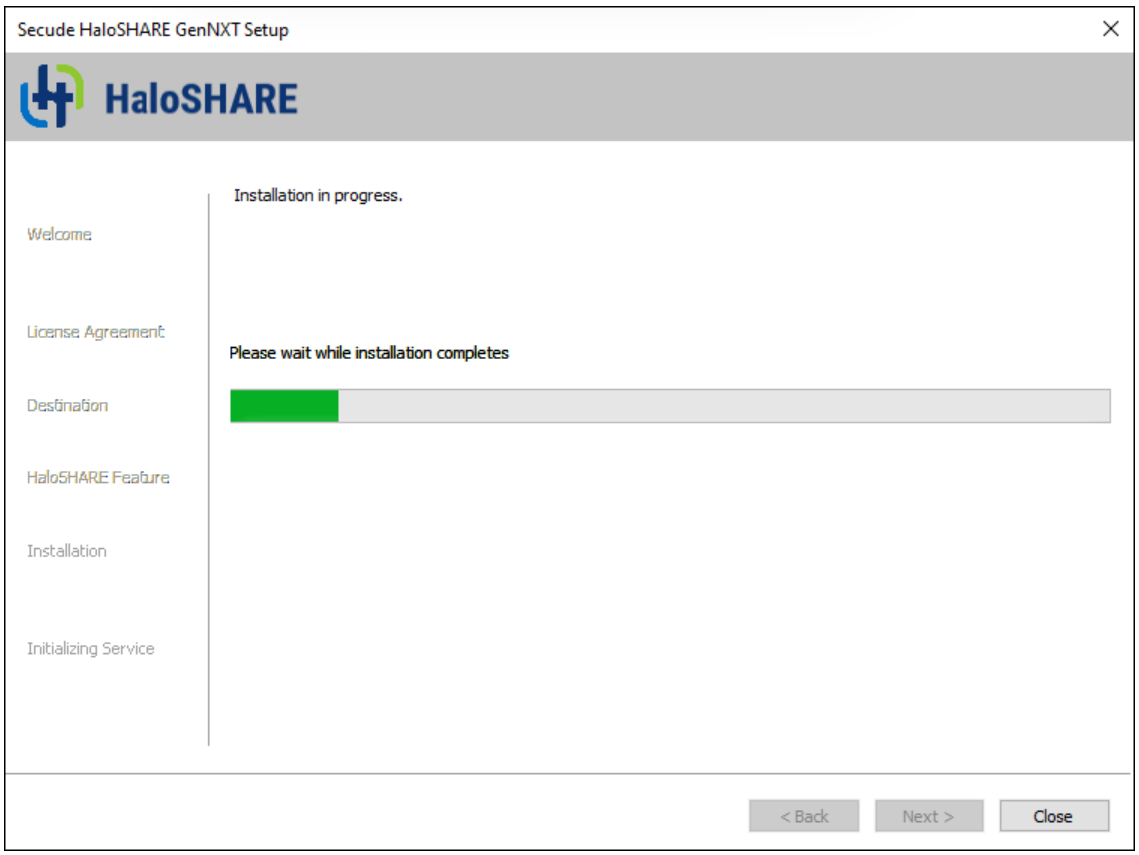
Destination folder selection dialog

7. 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**.
8. The HaloSHARE feature selection dialog appears.



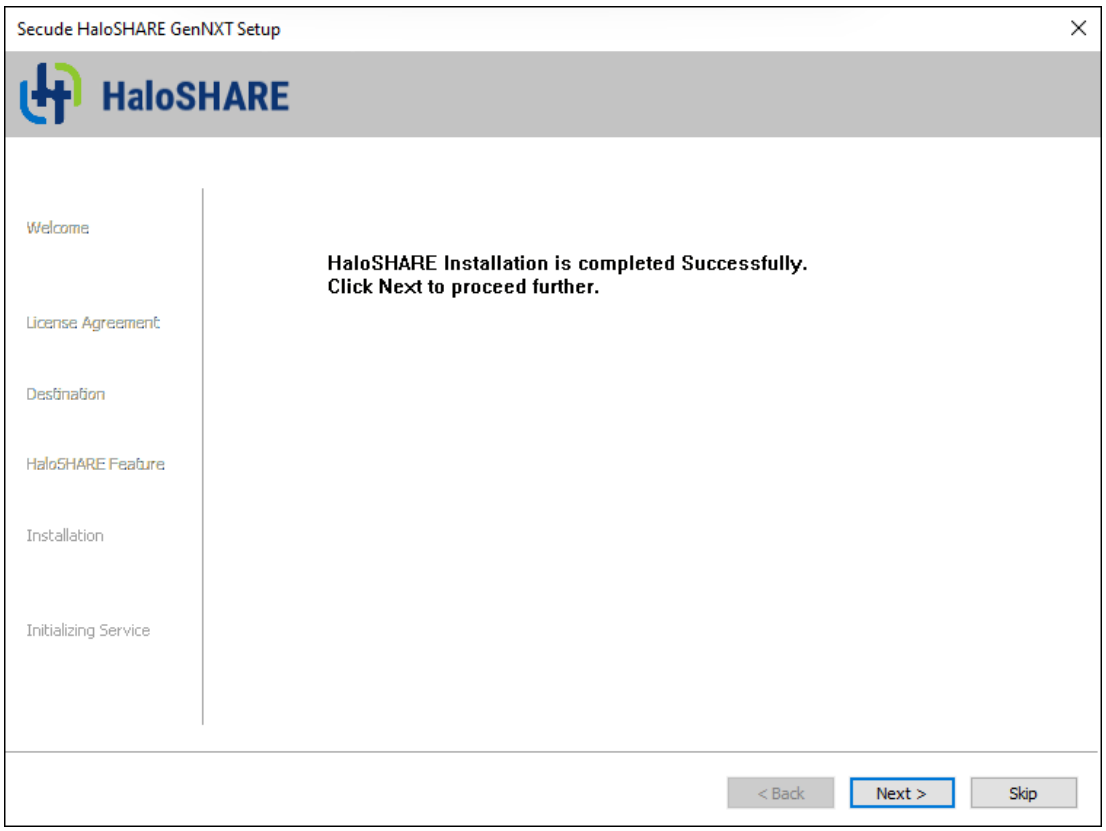
HaloSHARE feature selection dialog

9. You can choose one or more or all of the following options, depending on your requirements.
   a. To apply MPIP labels for file protection, select **MPIP**.
   b. To add a watermark to files, select **Watermarking**.
   c. To add CUI to the files, select **CUI Marking**.
   d. To review or modify the installation settings, click **Back** to return to the previous screens. Click **Next** to continue.
10. The installation begins, and the progress is displayed in the dialog.



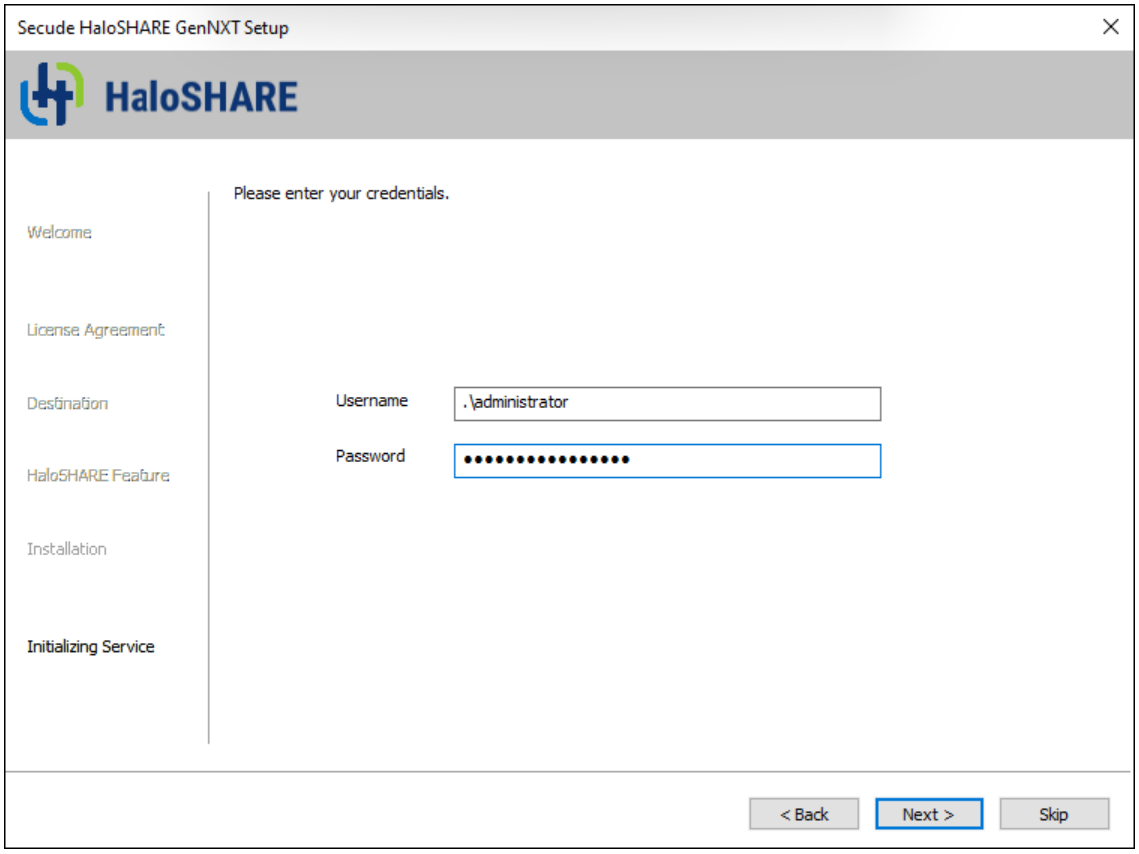
Installation progress dialog

11. Please wait until the installation completes. After the installation finishes, a confirmation message appears indicating that HaloSHARE was installed successfully.



Installation completed dialog

12. Click **Next**. The user credential dialog will appear:



User credential dialog

a. If the computer is connected to a domain and you want to run HaloSHARE on it, you must enter a domain user account and password. For example, `[domain]\[user]`, `hc.test\john`.

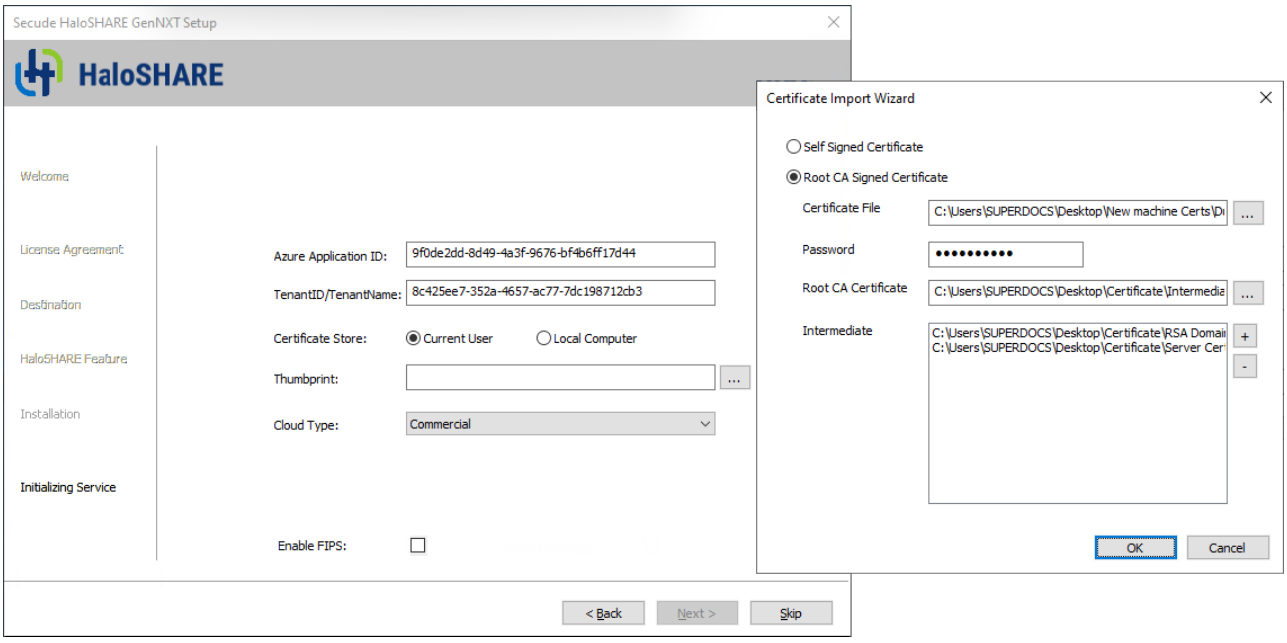
b. On a non-domain-joined computer, you need to enter the username and password of a user. For example, `.\[user]`, `.\john`.

13. Click **Next** to proceed.
14. If you selected **Watermarking**, **CUI Marking**, or both, proceed to Step 16.
15. The following authentication dialog appears when you select **MPIP** alone or with the **Watermarking** or **CUI Marking** options. To avoid errors, ensure that you enter the correct Azure application registration details in the installation wizard.

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

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

c. **Certificate Store**: Select a certificate store (**Current User** or **Local Computer**). When selecting Local Computer, ensure that the user running the service has at least local administrator rights.



Certificate-based authentication dialog

d. **Thumbprint**: If the certificate is already installed, enter the thumbprint manually. If the certificate is not installed, click **Browse** to select the required certificate, as described in Option 1 or Option 2.

e. **Option 1: Self-Signed Certificate**—Select this option if you have a self-signed certificate registered in the Azure portal. Click **Browse** to select the certificate (`.pfx` or `.p12`) and enter the password.

f. **Option 2: Root CA Signed Certificate**—Select this option if you have a certificate signed by a CA. Click **Browse** to select the signed certificate and verify that the certificate path appears in the **Certificate File** field. Enter the password in the **Password** field. Click **Browse** in the **Root CA Certificate** field to select the Root CA certificate (`.cer` or `.crt`). Click **(+) Add** in the **Intermediate CA** field to add intermediate CA certificates. Click **(-) Delete** to remove a certificate from the **Certificate Import Wizard**, and then click **OK** to populate the thumbprint automatically.

g. **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.

h. **Enable Federal Information Processing Standards (FIPS):** If you want to utilize encryption algorithms that comply with FIPS standards, enable this option. By enabling the option, MPIP uses only FIPS-compliant encryption algorithms. If not, MPIP uses standard encryption algorithms. However, FIPS mode can be enabled at any moment using the Administration Manager Tool (`hsadm.exe`). For more details, please refer to the MIP SDK Documentation "MIP SDK FIPS Compliance Statement".

i. Click **Next**.

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

Initialization completed dialog

17. Click **Close** to complete the installation.

Post-installation checks:

1. You can view the log files in the `<YEAR_MM_DD>.hs.log` format (for example, `2026_Feb_25.hs.log`) at `C:\Users\Username(user running service)\AppData\Local\Secude\HaloSHARE\log`.
2. You can view the configuration information in the registry path `HKEY_LOCAL_MACHINE\SOFTWARE\Secude\HaloSHARE`.
3. In MPIP mode, a protected policy XML file will be located at `C:\Users\Public\Secude\HaloSHARE`

6.2. Update from Old to New Version

Prerequisite:

From the installed location, back up the current `haloshare_config.enc` file. It provides the HaloSHARE configuration properties, which will be essential to retain current settings.

1. Uninstall the current version
2. Install the new version
3. Replace the `haloshare_config.enc` file in the folder where HaloSHARE is installed. The default path is `C:\Program Files\Secude\HaloSHARE`.

4. Run `HaloSHAREConfiguration.exe`, select the existing **Workflow Task**, and click **Save**.

To ensure compatibility across versions, after replacing the `haloshare_config.enc` file, select any workflow name or task and click **Save** in the new configuration tool. This step is required to enable continued use of existing configuration files (supplier-based version) with workflow-based versions.

What to do next

After installing HaloSHARE, you need to configure it according to your company's requirements. For instructions, refer to the following chapter.

7. Configuring the HaloSHARE

Using the configuration tool, you can quickly set up HaloSHARE.

7.1. Administration

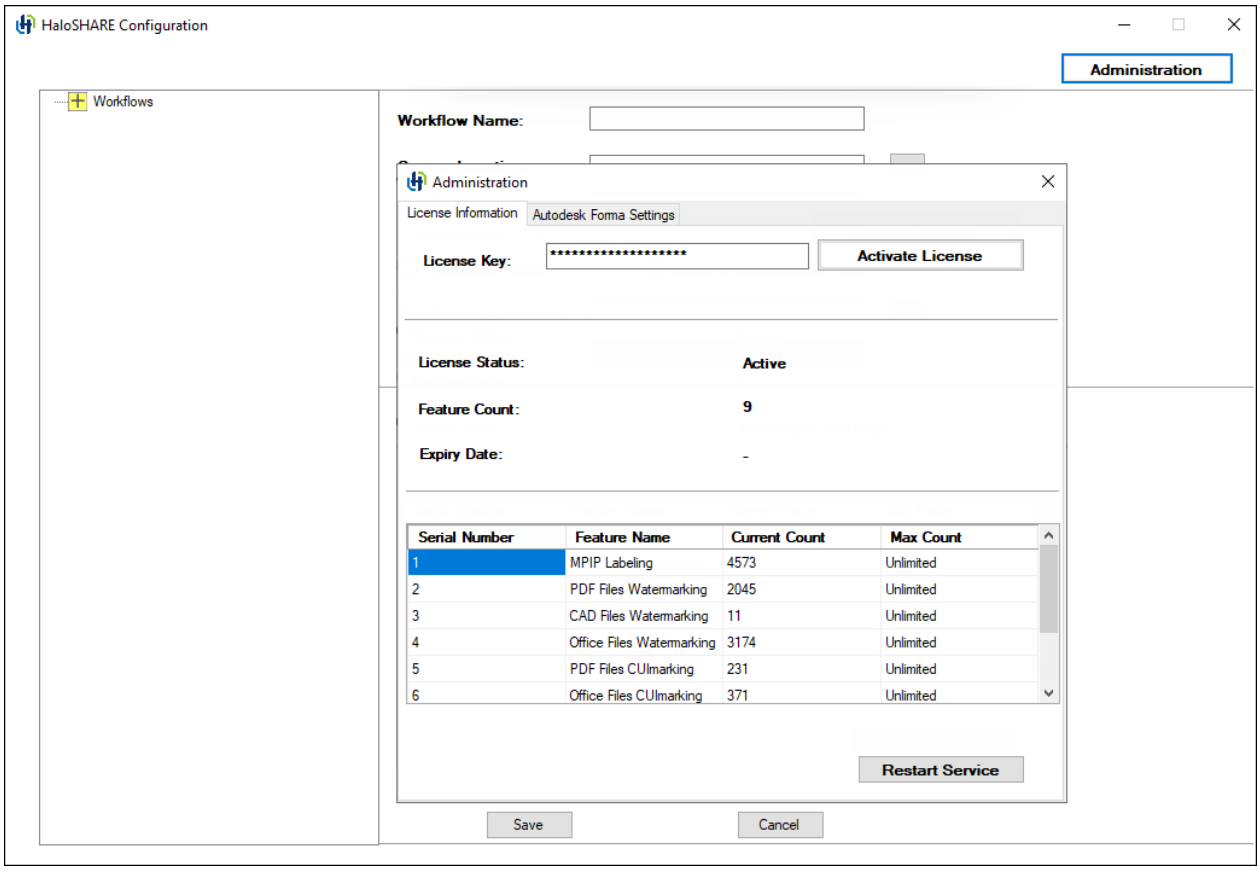
HaloSHARE uses a key-based license to control application features. Obtain the license key from Secude Support before installing HaloSHARE. After installation, enter the license key in the configuration tool to activate HaloSHARE and enable all features.

> This document does not cover all the specifics of purchasing a license. Please contact Secude's representative for additional details.

License Activation

To complete the license activation, perform the following steps:

1. Navigate to the installation directory. The default location is `C:\Program Files\Secude\HaloSHARE`.
2. Right-click `HaloSHAREConfiguration.exe` and select **Run as administrator**.
3. In the **HaloSHARE Configuration** window, click **Administration** in the top-right corner.
4. The **Administration** screen appears.



License activation screen

5. Enter the license key and click **Activate License**.
6. Please be patient while the license key is activated.

Result:

- After successful license activation, a confirmation message appears displaying the license details, including **License Status**, **Feature Count**, and **Expiry Date**. Additional information is shown in the **Feature Name**, **Current Count**, and **Max Count** fields.
- If you enter an invalid license key, **License Status** displays **LicenseNotFound**.
- If you enter a valid license key, **License Status** displays **Active**.

Related tasks:

- If your license expires, enter a new license key and click **Activate License**, or activate the license using the `hsadm.exe` tool, then restart the service. For more details, refer to the section "Configure the Service by Using the Admin Tool".
- The license is automatically deactivated when HaloSHARE is uninstalled.
- You can find license and service information in the log file located at: `C:\Users\UserName\AppData\Local\Secude\HaloSHARE\log`.

7.1.1. Autodesk Forma Settings

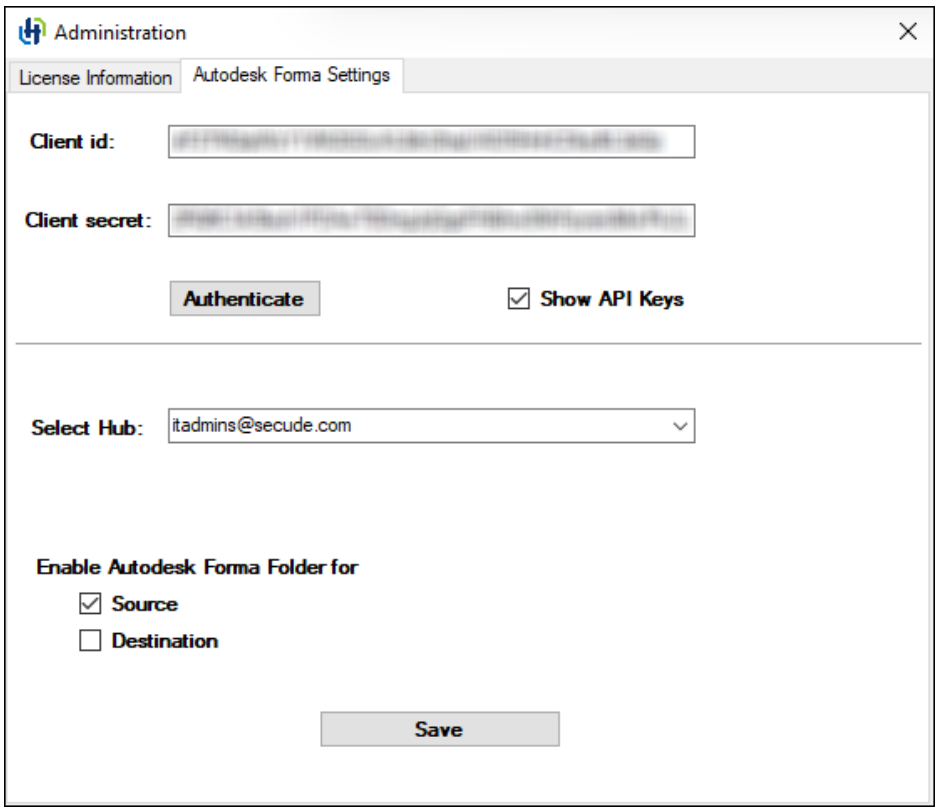
Autodesk Forma integration ensures seamless data flow and collaboration across platforms. HaloSHARE enhances this ecosystem with MPIP protection, watermarking, CUI marking, digital signing, password protection, and metadata tagging to enable secure and efficient file sharing.

Prerequisites:

- A valid license with the Autodesk Forma feature enabled.
- Ensure that you have the Client ID and Client Secret.

To configure HaloSHARE with Autodesk Forma, follow these steps:

1. In the **HaloSHARE Configuration** window, click **Administration** in the top-right corner.
2. The **Administration** screen appears.
3. Click **Autodesk Forma Settings**.
4. Enter the required credentials:
   a. Client id
   b. Client secret



Autodesk Forma Settings

5. To view the entered keys, click **Show API Keys**.
6. Click **Authenticate**. A confirmation message is displayed upon successful authentication.
7. From the drop-down list, select the required **Hub**.
8. Configure the **Source** and **Destination** by selecting one or both of the options below. If an option is selected, the corresponding Autodesk Forma folders will be displayed in the folder selection dialog; otherwise, the local network folder will appear.
9. Click **Save**.

Result

A confirmation message appears after the settings are successfully saved.

7.1.2. Quick Start for Workflows

A workflow defines how HaloSHARE automatically processes files from a source location to a destination location. A workflow consists of an ordered set of tasks that run sequentially when HaloSHARE detects a new file in the source folder.

Each workflow can include one or more of the following tasks. The execution order is shown below.

- **Metadata Task** – Embeds metadata into files.
- **Watermark Task** – Adds watermarks to files.

- **Compliance Mark Task** – Applies compliance markings to files.
- **Password Protection Task** – Applies password-based protection to files.
- **File Signing Task** – Digitally signs files to ensure authenticity and integrity.
- **MPIP Task** – Applies Microsoft Purview Information Protection (MPIP) labels for classification and protection.

Workflow Task Execution Order (Combined Configuration)

- Metadata task
- Watermark task
- File Signing task

In a workflow, you cannot combine the **Password Protection** or **File Signing** subtasks with the **MPIP** task because they are mutually exclusive. The MIP SDK does not support digitally signed or password-protected files.

In the **Workflow** pane, expanding a top-level workflow item displays the associated workflow tasks, along with each workflow and the corresponding source location. For example, designers at Prestin Engineering may store sensitive files in the source folder location `C:\PrestinEng\Source1` within the organization. To securely share these files with the external users, they configure a destination location such as `C:\SharePoint\PrestinEng_DestUser1`. The same approach can be used to configure folders for other workflows.

Points to Remember While Working with HaloSHARE Workflow

1. File overwriting occurs when the same file is moved repeatedly to the same source folder.
    a. Case 1: When the **Move to Destination Path** option is not selected.

    MPIP Task: Suppose the source location is configured for the text file (`.txt`) type. When you copy a text file, for example, `sample.txt`, into the source folder, it is encrypted and renamed to `sample.ptxt`. If you copy the same file `sample.txt` into the source folder again, the existing `sample.ptxt` file is overwritten.

    Watermark Task: Suppose the source location is configured for the PDF file (`.pdf`) type. When you copy a PDF file into the source folder, it is watermarked. If you copy the same PDF file again, the existing file is overwritten.

    Note: The same behavior applies when a file is digitally signed, password-protected, CUI-marked, or metadata-tagged.

    b. Case 2: When the **Move to Destination Path** option is selected.

MPIP Task: When a file is placed in the source location, it is encrypted and moved to the destination folder. If the same file is added to the source folder again, it is treated as a new file, encrypted, and moved to the destination folder, overwriting the existing file.

Watermark Task: When a file is placed in the source location, it is watermarked and moved to the destination folder. If the same file is added to the source folder again, it is treated as a new file, watermarked, and moved to the destination folder, overwriting the existing file. For files of type **PDF**, **Excel**, and **DOCX**, if processing fails due to a library error, the failed file is cached and is not processed again in subsequent HaloSHARE operations.

Note: The same behavior applies when a file is digitally signed, password-protected, CUI-marked, or metadata-tagged.

2. The OneDrive and HaloSHARE services cannot access the same file simultaneously. Similarly, the HaloSHARE and SharePoint services cannot access the same file at the same time. Attempting to access simultaneously will result in an access violation or an access denied error.
3. Unconfigured file types: Files that are not specified in the HaloSHARE configuration tool will not be moved to the destination folder. HaloSHARE identifies these unconfigured file types and leaves them untouched.
4. A top-level workflow cannot be deleted if it contains configured tasks. Delete all tasks before deleting the top-level workflow.
5. The same location cannot be configured more than once, and existing workflow names cannot be reused.
6. The workflow name cannot be changed after it is created. To rename a workflow, delete the existing workflow and create a new workflow with the desired name.

File Processing in Forma

HaloSHARE identifies each file in Forma using the **Item ID** and **Version ID**, ensuring that the source folder is not processed repeatedly.

- When a new file is added to the source folder, HaloSHARE processes and tracks it. If a file (for example, V1) is already processed by HaloSHARE and added again without changes, HaloSHARE skips processing. Processed files are tagged with **Processed by HaloSHARE** to prevent duplicate processing.
- HaloSHARE creates a new version when a file with the same name exists in the destination folder.
- Unlike local folder configuration, when the **Move to Destination Path** option is selected in Autodesk Forma, files in the source folder remain unchanged, and the processed files are sent to the destination folder.

- HaloSHARE tracks the version of each file in the source (Autodesk Forma) folder and the destination folder. This ensures that if a user configures a folder in Autodesk Forma that already contains processed files, HaloSHARE identifies them and does not process them again. File tracking details are stored in `TrackVersions.json` under `C:\Users\Public\Secude\HaloSHARE\adfcache`.
- If a HaloSHARE-protected file is uploaded and relabeling is required, HaloSHARE does not process the file if it has already been processed.
  To decrypt/relabel and process the file again, do one of the following:
  - Delete the tracking version file.
  - Download the file and place it in a different folder.

  This approach prevents repeated processing of the same file when Autodesk Forma folders are configured by tracking item versions.

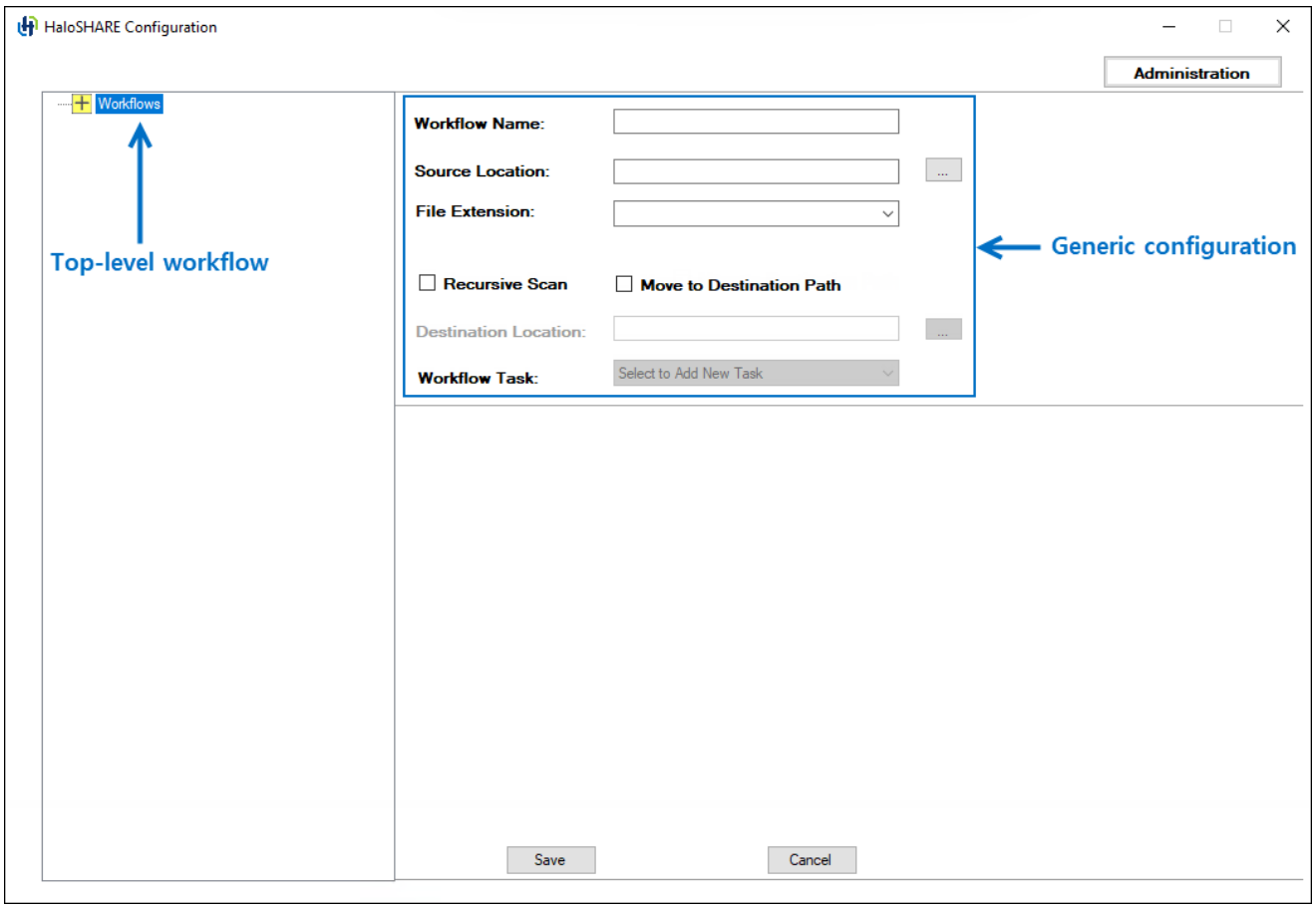
7.2. Configure Workflows

To configure the workflow, navigate to the destination folder that you specified during installation. The default folder is `C:\Program Files\Secude\HaloSHARE`.

Prerequisite:

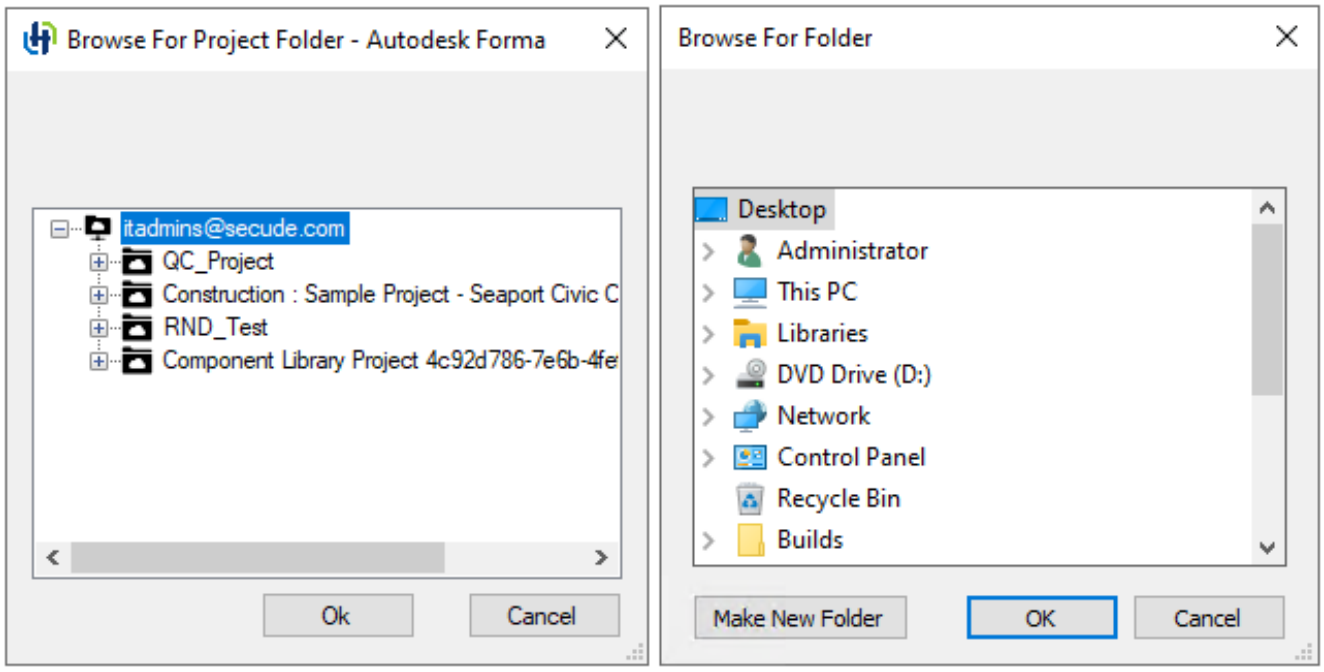
By default, the HaloSHARE file extension is available for selection. To add additional extensions, update the `hs_extension_list.json` file. Newly added entries automatically appear in the extension list in the configuration tool.

1. Double-click on the `HaloSHAREConfiguration.exe` file, and the **HaloSHARE Configuration** screen appears as shown below.



Generic Workflow configuration fields

2. In **Workflow Name**, enter a name for the workflow. Example: Prestin Engineering
3. In **Source Location**, enter the path to the source folder that HaloSHARE monitors, or click **Browse** to select the folder. The folders available in the dialog box depend on your configuration.
   - If Autodesk Forma is integrated, Autodesk Forma folders appear when the Source and Destination options are enabled. Example: `RND_Test:\Project Files\Lib\Assembly`.
   - If Autodesk Forma is not integrated, local network folders are available. Example: `C:\PrestinEng\Source1`.



Folder dialogs

4. From the drop-down list, select the file extensions. You can also search for a file type and then select it from the results. Files with extensions that are not configured are ignored. However, if **Move to Destination Path** is selected, both processed and unconfigured files are moved to the destination folder.
5. Select **Recursive Scan** to scan all subfolders in the source folder. If you don't select this option, HaloSHARE processes only files in the source folder.
6. Select **Move to Destination Path** to transfer files from the source location to a destination path. The destination folder can be a shared location for external access, such as a supplier, vendor, or consultant folder. Example: a SharePoint or OneDrive folder.
7. In **Destination Location**, enter the path to the destination folder where HaloSHARE copies the processed files, or click **Browse** to select the folder. Ensure that the specified workflow can access this folder. Example: Files from `C:\PrestinEng\Source1` are moved to `C:\SharePoint\PrestinEng_DestUser1`.
8. Click **Save**.

Result:

- After you successfully add the workflow, a confirmation message appears. The workflow name appears in the left pane under the top-level workflow. Select the workflow name to view its details in the right pane.
- The **Workflow Task** list is enabled after you save the workflow successfully. Note: To add a workflow task, the user must have a valid license and a proper installation.

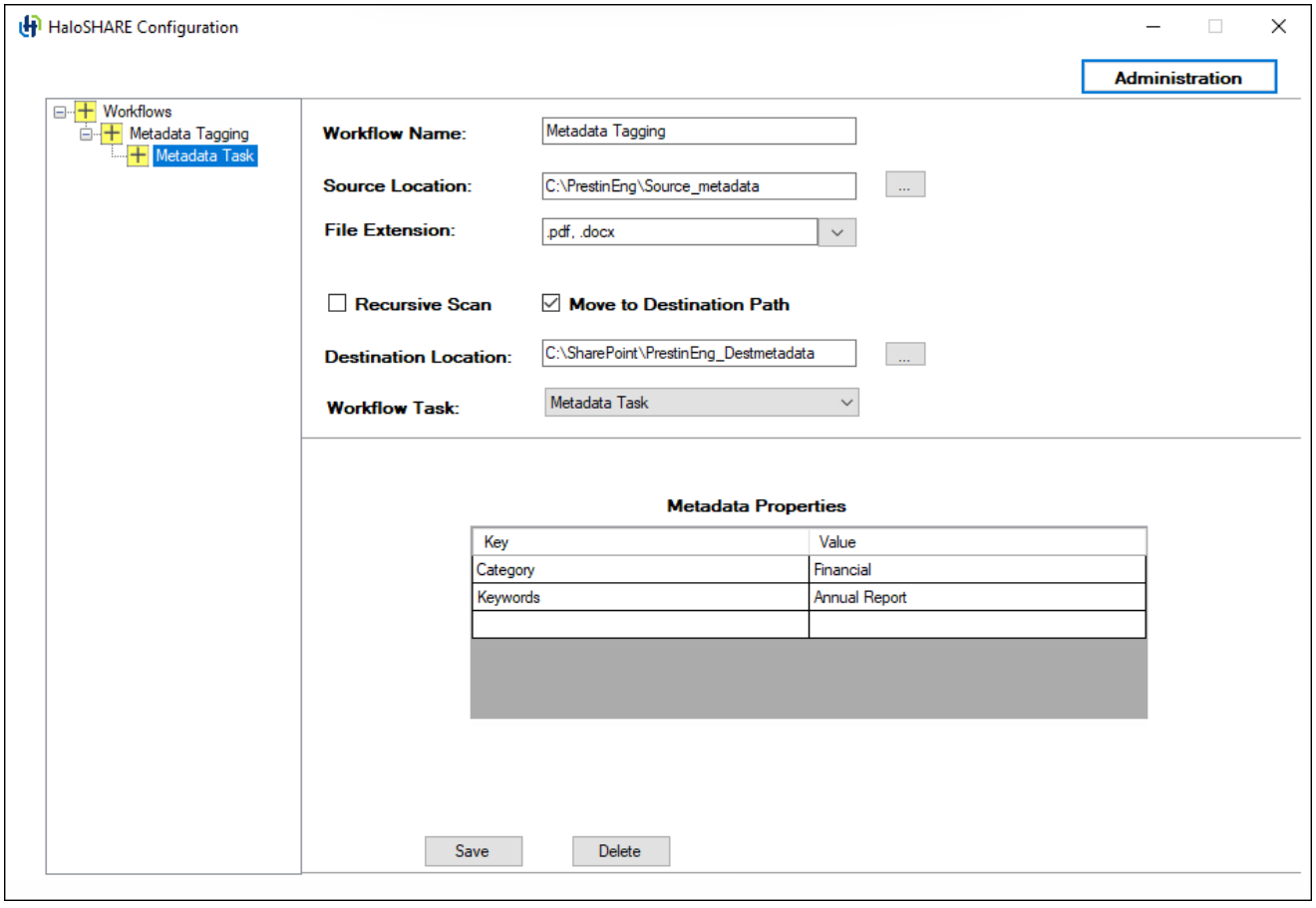
- To create a new workflow, select top-level **Workflow** in the left pane. The empty fields appear. Enter the required details to create a new sub-level workflow.

7.2.1. Configure Metadata Task Attributes

This task configures HaloSHARE to add metadata tags to files to help protect sensitive content and provide ownership context.

To tag metadata to files, follow these steps:

1. As described in the Configure Workflows section, configure your workflow task.
2. From the **Workflow Task** list, select the **Metadata Task**.
3. On the **HaloSHARE configuration** screen, the metadata task options appear.



Metadata Task configuration

4. Under **Metadata Properties**, enter the required metadata values in the designated fields.
   Example:
   a. Category: Financial
   b. Keywords: Annual Report
5. To remove added custom properties, select the row, right-click, and choose **Delete**.

6. Click **Save**, and then click **Restart Service** in the **Administration** UI. Repeat these steps to add additional workflows.

Result:

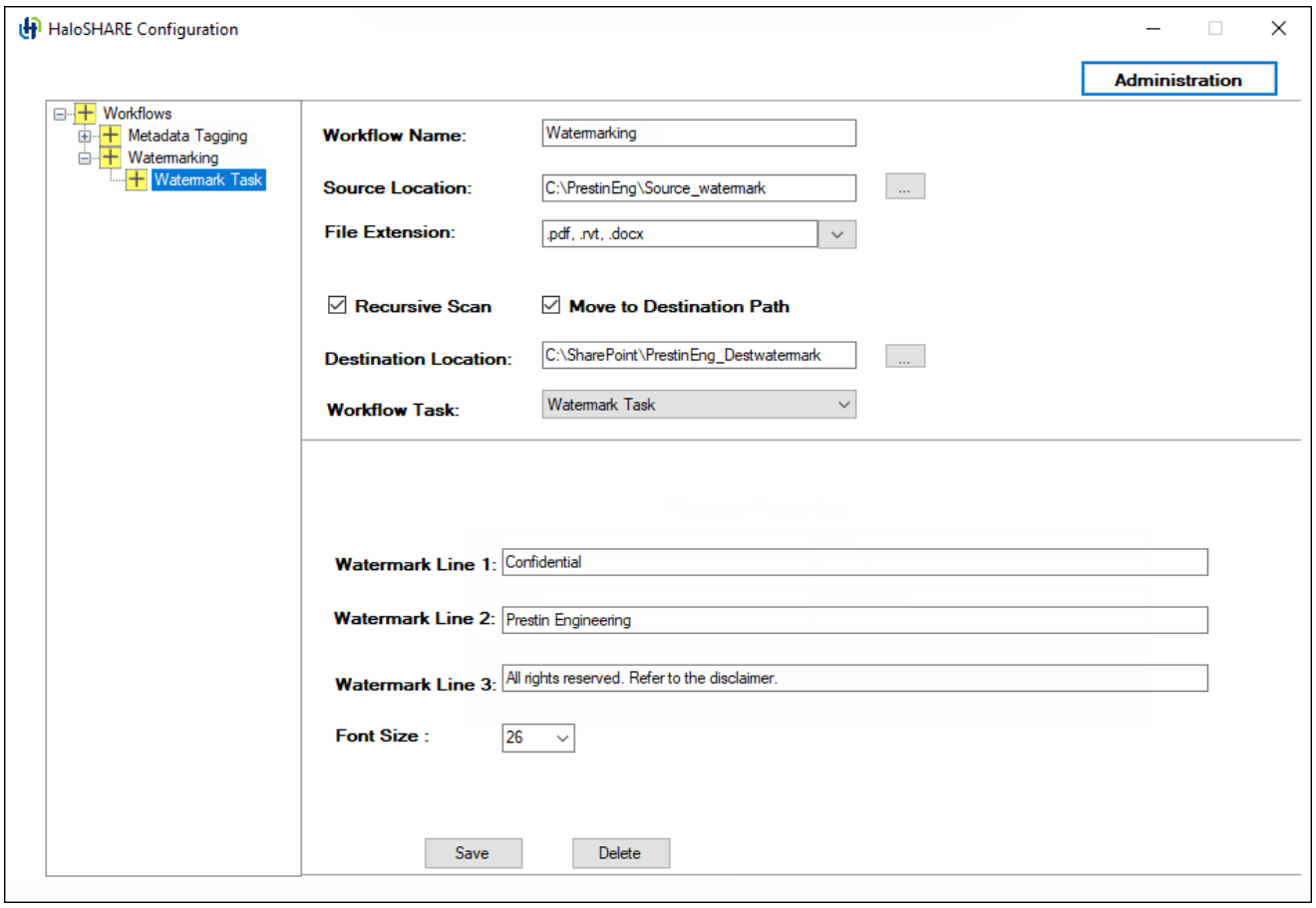
- After you successfully add the workflow, a confirmation message appears. The workflow name appears in the left pane under the top-level workflow. Select the workflow name to view its details in the right pane at any time.
- The files are tagged with the specified metadata values.
- To delete a workflow, click **Delete**, and then confirm the action when prompted. The workflow is removed.
- For examples of the configuration output, see Sample Results section to view the configuration output.

7.2.2. Configure Watermark Task Attributes

This task configures HaloSHARE to apply watermarks to files to help protect sensitive content and indicate file ownership.

To add a watermark to files, follow these steps:

1. As described in the Configure Workflows section, configure your workflow task.
2. From the **Workflow Task** list, select the **Watermark Task**.
3. On the **HaloSHARE configuration** screen, the watermark-related UI field appears.



Watermark Task configuration

4. Enter the text to be embedded in the files. By default, the watermark will be applied diagonally. You can type any text suited for the sensitivity level of the document on watermark lines 1, 2, and 3. Example:
   a. **Watermark Line 1**: Confidential
   b. **Watermark Line 2**: Prestin Engineering
   c. **Watermark Line 3**: All rights reserved. Refer to the disclaimer.
   d. **Font Size**: Select a font size between **8** and **72**. Times New Roman is currently used for watermarking across all file types.
5. Click **Save**, and then click **Restart Service** in the **Administration** UI. Repeat these steps to add additional workflows.

Result:

- After you successfully add the workflow, a confirmation message appears. The workflow name appears in the left pane under the top-level workflow. Select the workflow name to view its details in the right pane at any time.
- The files are watermarked with the specified text.

- For examples of the configuration output, see Sample Results section to view the configuration output.
- To delete a workflow, click **Delete**, and then confirm the action when prompted. The workflow is removed.

7.2.2.1. Watermarking Revit Files Using HaloSHARE

This feature enables watermarking of Revit files without using the HaloCAD add-on for Revit.

Prerequisites

- Ensure that CAD applications such as AutoCAD or Revit are not running during the installation or uninstallation of HaloSHARE.
- Ensure that Secude add-ons (HaloCAD add-on for Revit or HaloCAD add-on for AutoCAD) are not installed on the watermarking machine.
- Ensure that HaloSHARE is installed and running.
- Restart HaloSHARE before proceeding.

To add a watermark to Revit files, follow these steps:

1. Open **Task Manager** → **Details** tab and verify whether `hsmetadataMessageProcessor.exe` is running.
2. If the process is not running, navigate to the HaloSHARE installation path (`C:\Program Files\Secude\common\<version>`) and double-click `hsmetadataMessageProcessor.exe` to start it.
3. Configure a new supplier with source and destination paths specific to Revit file types (for example, `.RVT`).
4. Place the Revit file (for example, `sample.rvt`) in the source folder.

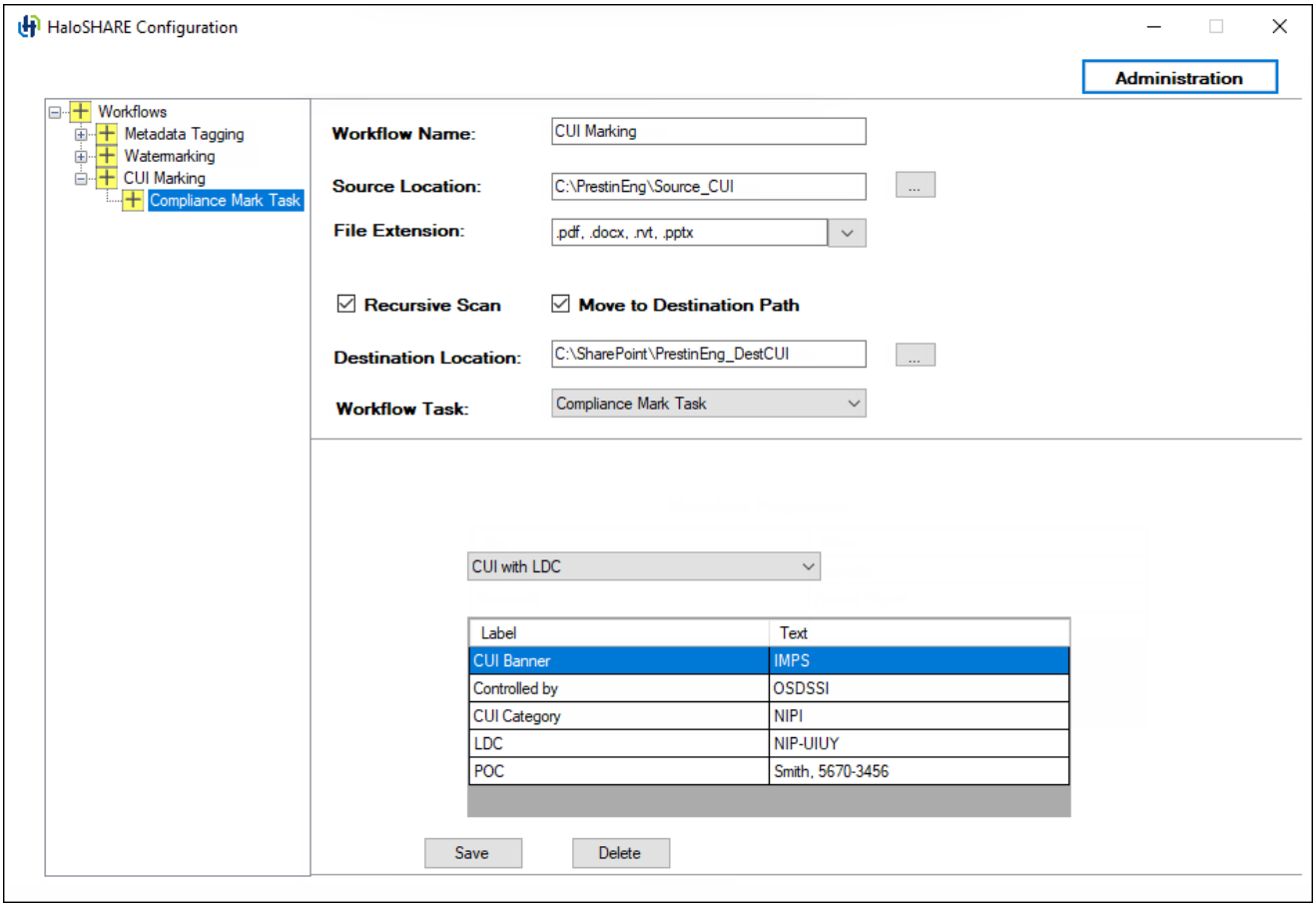
Result

- The file is watermarked with the specified text and moved to the destination folder.
- To view the watermark text in Revit, refer to the section "Watermark in RevitLookup".

7.2.3. Configure Compliance Mark Task Attributes

This task configures HaloSHARE to apply CUI marking to files.

1. As described in the Configure Workflows section, configure your workflow task.
2. From the **Workflow Task** list, select **Compliance Mark Task**.
3. On the **HaloSHARE configuration** screen, the compliance marking options appear.



CUI with LDC configuration

4. Select **CUI with LDC** or **CUI with DS**, and then enter the required CUI values in the corresponding fields.

   Example:

   a. CUI Banner: IMPS

   b. Controlled by: OSDSSI

   c. CUI Category: NIPI

   d. LDC: NIP-UIUY

   e. POC: Smith, 5670-3456

5. To remove added custom properties, select the row, right-click, and choose **Delete**.
6. Click **Save**, and then click **Restart Service** in the **Administration** UI. Repeat these steps to add additional workflows.

Result:

- After you successfully add the workflow, a confirmation message appears. The workflow name appears in the left pane under the top-level workflow. Select the workflow name to view its details in the right pane at any time.

- The first page of the document displays the CUI values as defined in the configuration.
- To delete a workflow, click **Delete**, and then confirm the action when prompted. The workflow is removed.
- For examples of the configuration output, see Sample Results section to view the configuration output.

Adjusting the watermark display to the background

To display the watermark in the background instead of the foreground in Excel and PowerPoint, manually add the following registry key, `enable_legacy`, with the value `true`. This makes it possible to add or edit content, just like in Microsoft Word, by enabling the watermark to appear in the background.

Name	Type	Data
enable_legacy	REG_SZ	true

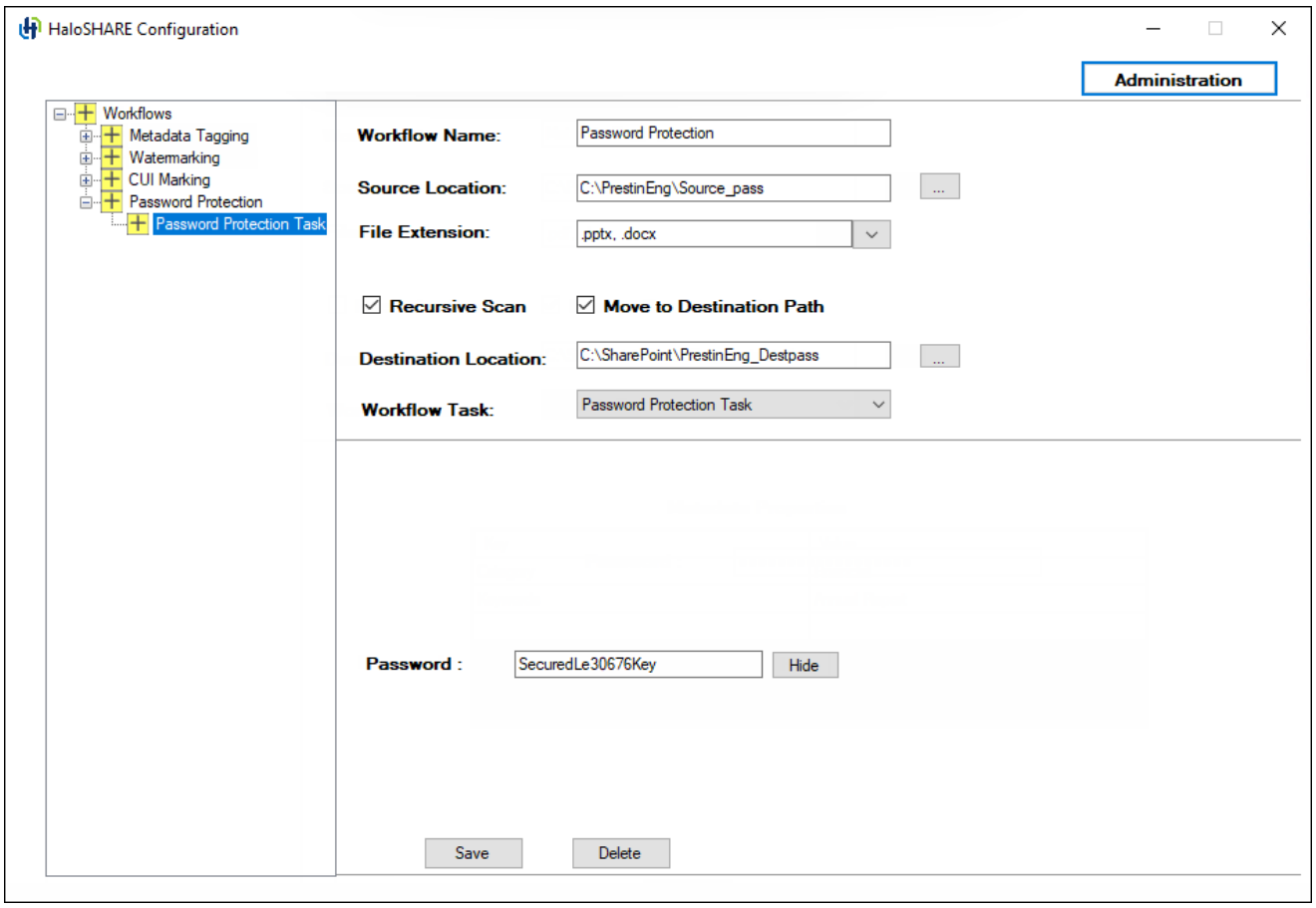
Manual addition of the key

7.2.4. Configure Password Protection Task Attributes

This task configures HaloSHARE to protect files using a user-defined password. The password must be 8–15 characters long and can contain letters, numbers, or a combination of both. Spaces and special characters are not allowed. HaloSHARE applies only the password; all other behavior is determined by the native functionality of Microsoft Office applications.

To protect files using a password, follow these steps:

1. As described in the Configure Workflows section, configure your workflow task.
2. From the **Workflow Task** list, select the **Password Protection Task**.
3. On the **HaloSHARE configuration** screen, the password protection field appears.



Password Protection Task configuration

4. Enter a password, and ensure that you remember it, as you will need it to edit the file later. You can use the **Show**/**Hide** button to view or hide the password.
5. Click **Save**, and then click **Restart Service** in the **Administration** UI. Repeat these steps to add additional workflows.

Result:

- After you successfully add the workflow, a confirmation message appears. The workflow name appears in the left pane under the top-level workflow. Select the workflow name to view its details in the right pane at any time.
- Files in the source folder are protected by a user-defined password and moved to the destination folder.
- For examples of the configuration output, see Sample Results section to view the configuration output.
- To delete a workflow, click **Delete**, and then confirm the action when prompted. The workflow is removed.

7.2.5. Configure File Signing Task Attributes

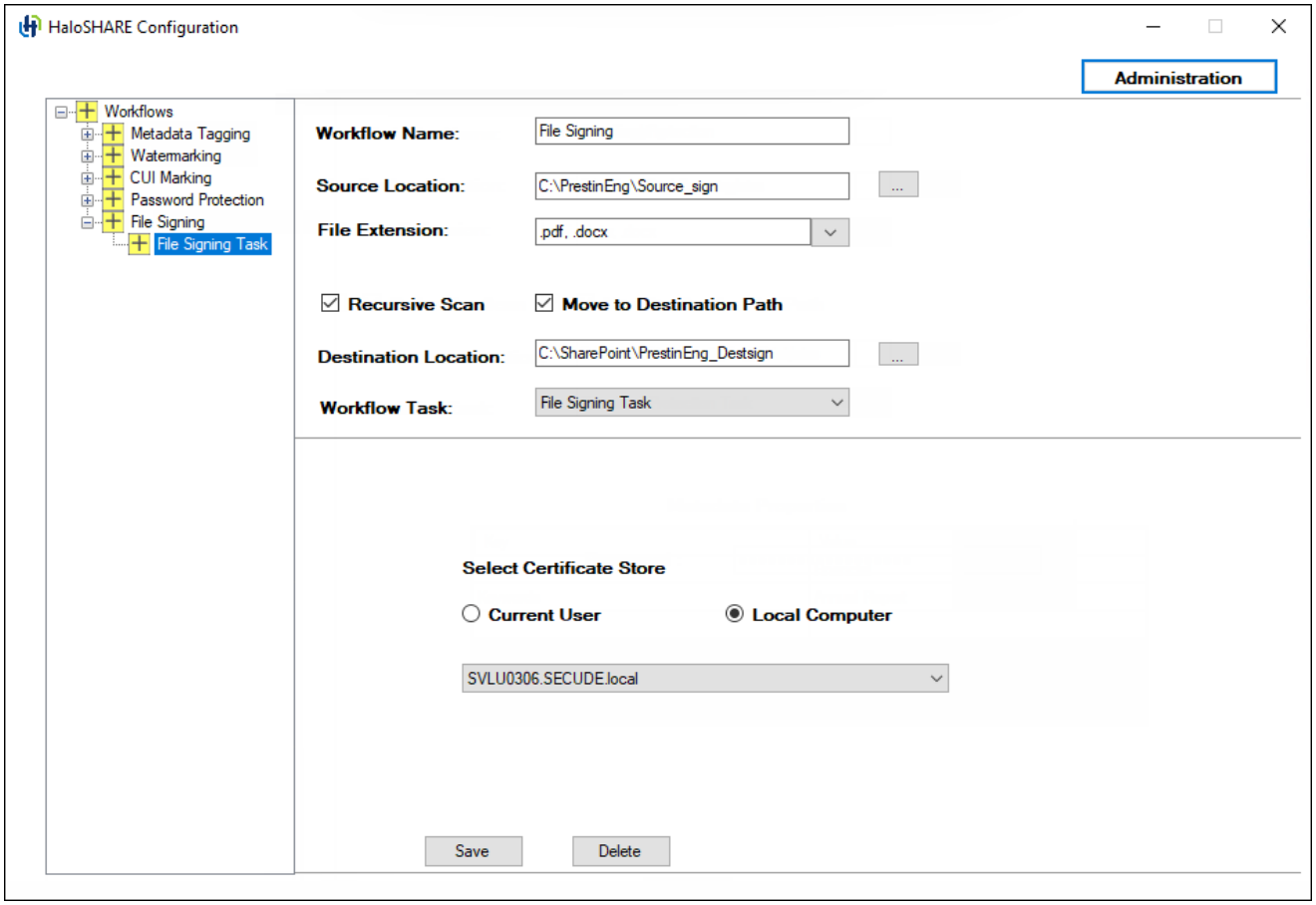
This task configures HaloSHARE to automatically apply a digital signature to files in the background to help ensure file integrity and authenticity.

You can select either **Local Computer** or **Current User**. However, both options have certain restrictions.

- If you select **Local Computer**, the service running user must have access to the Local Computer certificates or to the specific certificate in the Local Computer store. If the service running user is a local non-admin user, promote the service running user to a local admin user or grant the service running user access to the private key.
- If you select **Current User**, the selected certificate must be installed in the certificate store of the service running user.

To sign files, follow these steps:

1. As described in the Configure Workflows section, configure your workflow task.
2. From the **Workflow Task** list, select **File Signing Task**.
3. On the **HaloSHARE configuration** screen, the file signing options appear.



File Signing Task configuration

4. Under **Select Certificate Store**, select **Current User** or **Local Computer**.

5. From the list, select the appropriate certificate.
6. Click **Save**, and then click **Restart Service** in the Administration UI. Repeat these steps to add additional workflows.

Result:

- After you successfully add the workflow, a confirmation message appears. The workflow name appears in the left pane under the top-level workflow. Select the workflow name to view its details in the right pane at any time.
- Files in the source folder are digitally signed and moved to the destination folder.
- For examples of the configuration output, see Sample Results section to view the configuration output.
- To delete a workflow, click **Delete**, and then confirm the action when prompted. The workflow is removed.

7.2.6. Configure MPIP Task Attributes

In the MPIP task, HaloSHARE encrypts files by using either sensitivity labels or custom permissions. Files encrypted with sensitivity labels can be relabeled by using custom permissions, and files encrypted with custom permissions can be relabeled by using sensitivity labels. Note: You cannot configure File Signing, Metadata, or Password Protection tasks together with the MPIP task. Compliance Mark and Watermark tasks can be configured if your license supports these features.

Relabeling prerequisites

Before relabeling files, ensure that one of the following conditions is met:

- The user is the document owner.
- The user has superuser privileges.
- The user has export permissions assigned to the applied label.
- The API permission for relabeling is configured in the application. Refer to section "Additional Permission (Only for Relabeling)".

Difference Between Sensitivity Labels and Custom Permissions

Sensitivity Labels

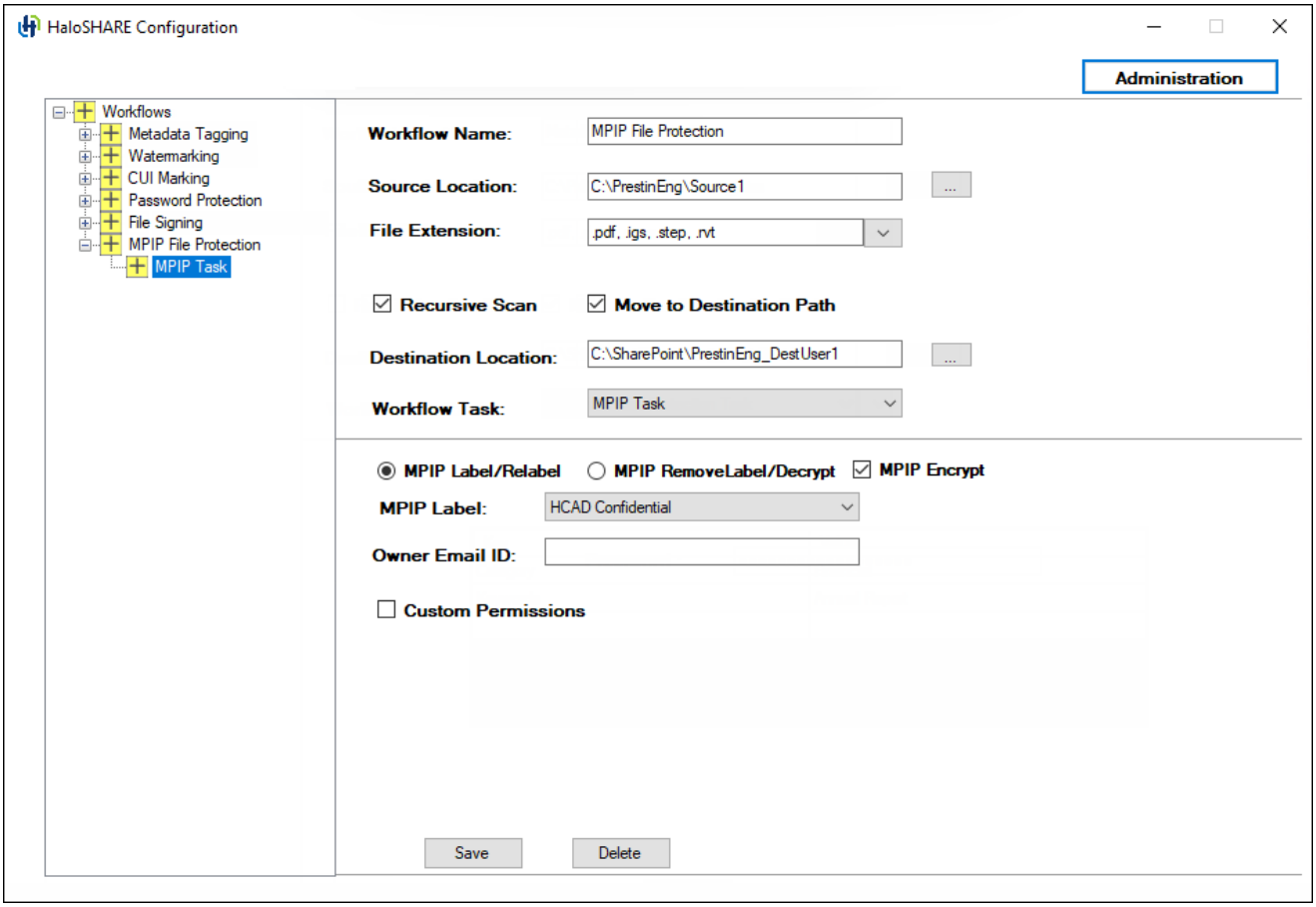
Sensitivity Labels are defined and managed by an organization's administrator in the Microsoft Purview portal. Each label includes a predefined set of permissions and is also referred to as administrator-defined permissions.

Custom Permissions

Custom Permissions are user-selectable permission sets available in the HaloSHARE application UI. These permissions are defined by users and are also referred to as user-defined permissions.

To apply file protection, follow these steps:

1. As described in the Configure Workflows section, configure your workflow task.
2. From the **Workflow Task** list, select **MPIP Task**.
3. On the **HaloSHARE configuration** screen, the following MPIP task options appear:



MPIP Task configuration

4. **MPIP Encrypt** is selected by default, but you can clear it. When selected, the **MPIP Label** list shows both protection and non-protection labels. When cleared, the **MPIP Label** list shows only non-protection labels.
5. To apply MPIP labels to files, select **MPIP Label/Relabel**. This option acts as a toggle between labeling and relabeling.
   a. Select a sensitivity label from the **MPIP Label** list.

b. You may also choose a label without encryption settings. In that case, the following message appears *"The selected MPIP label has no encryption settings and can only be applied to MIP SDK–supported file types."* To apply such a label, specify the supported file types, for example, `.txt`, `.docx`, and `.pdf`.

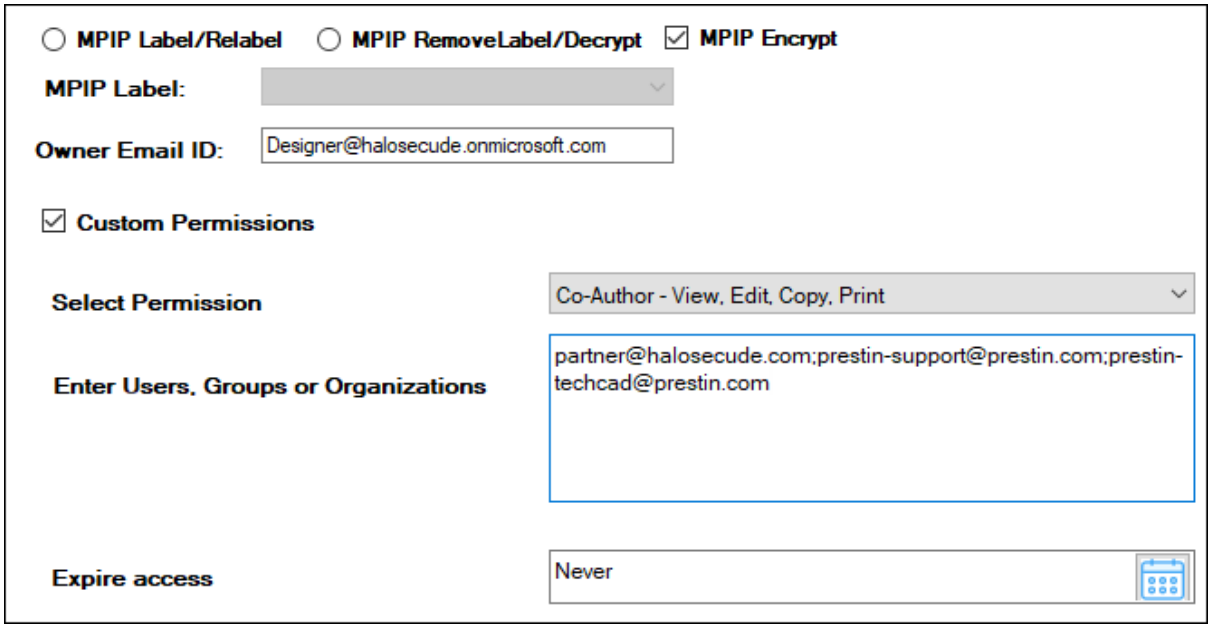
c. Skip to step 8.

6. To apply user-defined permissions, select **Custom Permissions**. The author can then assign permissions to users, groups, or organizations based on the selected permission level.

   a. From the **Select Permissions** list, choose the access level for users when protecting the file: (Viewer - View Only / Reviewer - View, Edit / Co-Author - View, Edit, Copy, Print / Co-Owner - All Permissions / Only for me). To know the usage rights of the permissions, please refer to the section "Permissions Level and Usage Rights".

   b. In the **Enter Users, Groups, or Organizations** field, specify who should have access to your file. Type individual email addresses, group email addresses, or a domain name for all users in that organization, separated by commas, spaces, or semicolons. For example `partner@halosecude.com;prestin-support@prestin.com;prestin-techcad@prestin.com`

   c. In the **Expire Access** field, specify how long the labeled file can be accessed. Use **Never** for unlimited access, suitable for less sensitive content. For highly sensitive content, select an expiry date so that recipients (other than the owner) cannot access the file after that date.



Custom permissions

7. To decrypt a file, select **MPIP RemoveLabel/Decrypt**.

8. To make a user the file owner and grant full access, enter the user's email ID in the **Owner Email ID** field. For example, `Designer@halosecude.onmicrosoft.com`.
9. Click **Save**, and then click **Restart Service** in the **Administration** UI. Repeat these steps to add additional workflows.

Result:

- After you successfully add the workflow, a confirmation message appears. The workflow name appears in the left pane under the top-level workflow. Select the workflow name to view its details in the right pane at any time.
- **MPIP protection**: Files are protected based on the selected label.
- **Relabeling**: Files in the workflow folder are updated with the new label.
- **Remove protection**: Files in the workflow folder are decrypted successfully.
- For examples of the configuration output, see Sample Results section to view the configuration output.
- To delete a workflow, click **Delete**, and then confirm the action when prompted. The workflow is removed.

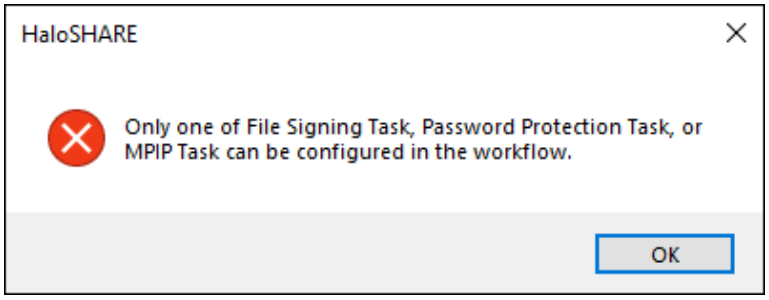
7.2.7. Configure Combined Workflows

In the previous sections, independent workflows were explained. This section describes how to configure a combined workflow with multiple tasks.

Workflow Task Execution Order (Combined Configuration):

- Metadata task
- Watermark task
- File Signing task

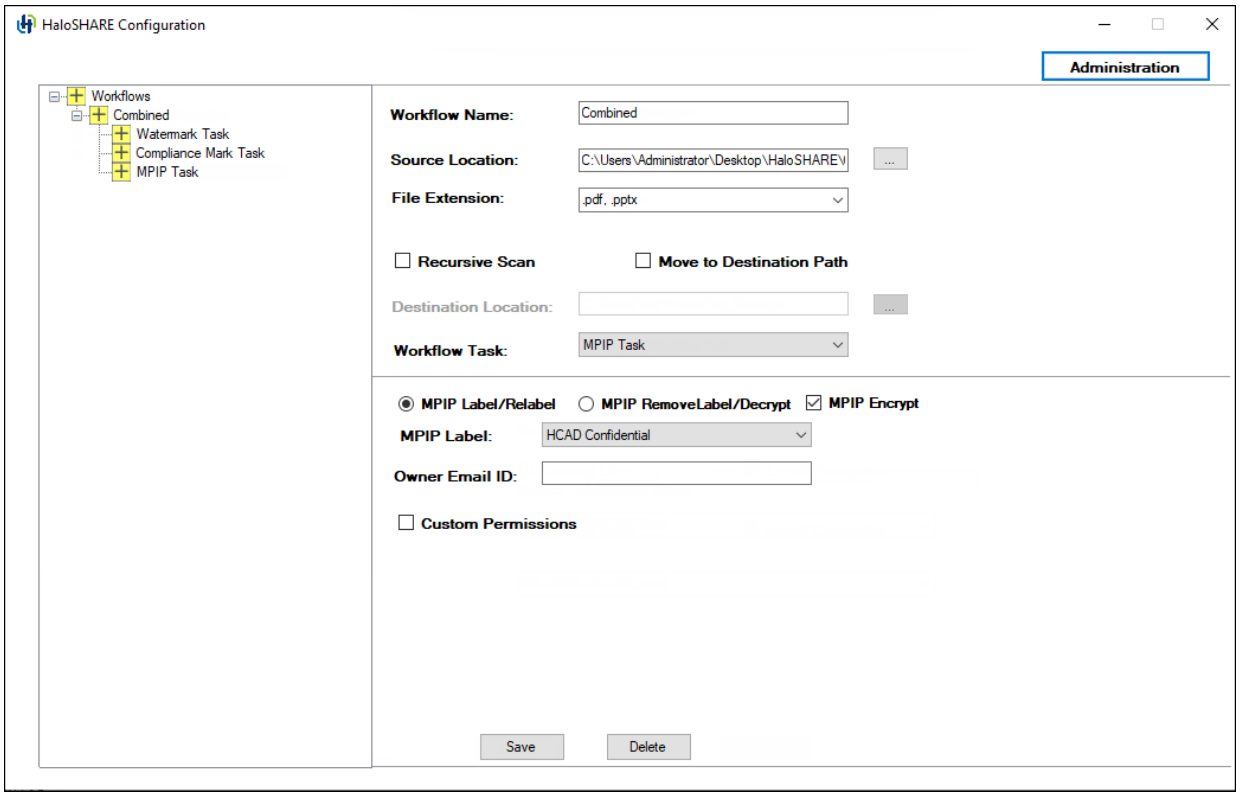
In a workflow, you cannot combine the **Password Protection** or **File Signing** subtasks with the **MPIP** task because they are mutually exclusive. The MIP SDK does not support digitally signed or password-protected files. Attempting to combine them results in the following error message.



Mutually exclusive error message

Follow the procedure for a combined Workflow:

1. Select an existing workflow. Example: Combined.
2. Under the selected workflow, add the required subworkflow tasks.
3. From the **Workflow Task** list, select a task. Example: Select the **Watermark Task**.
    a. Enter the required details.
    b. Click **Save**.
4. From the **Workflow Task** list, select another task. Example: Select the **Compliance Mark Task**.
    a. Enter the required details.
    b. Click **Save**.
5. From the **Workflow Task** list, select another task. Example: Select the **MPIP Task**.
    a. Enter the required details,
    b. Click **Save**.



Combined workflow

6. Click **Restart Service** in the **Administration** UI.

Result

- The selected workflow contains multiple appended workflow tasks, which are executed as part of the combined workflow.

- For examples of the configuration output, see Sample Results section to view the configuration output.

7.3. Configure the Service by Using the Admin Tool

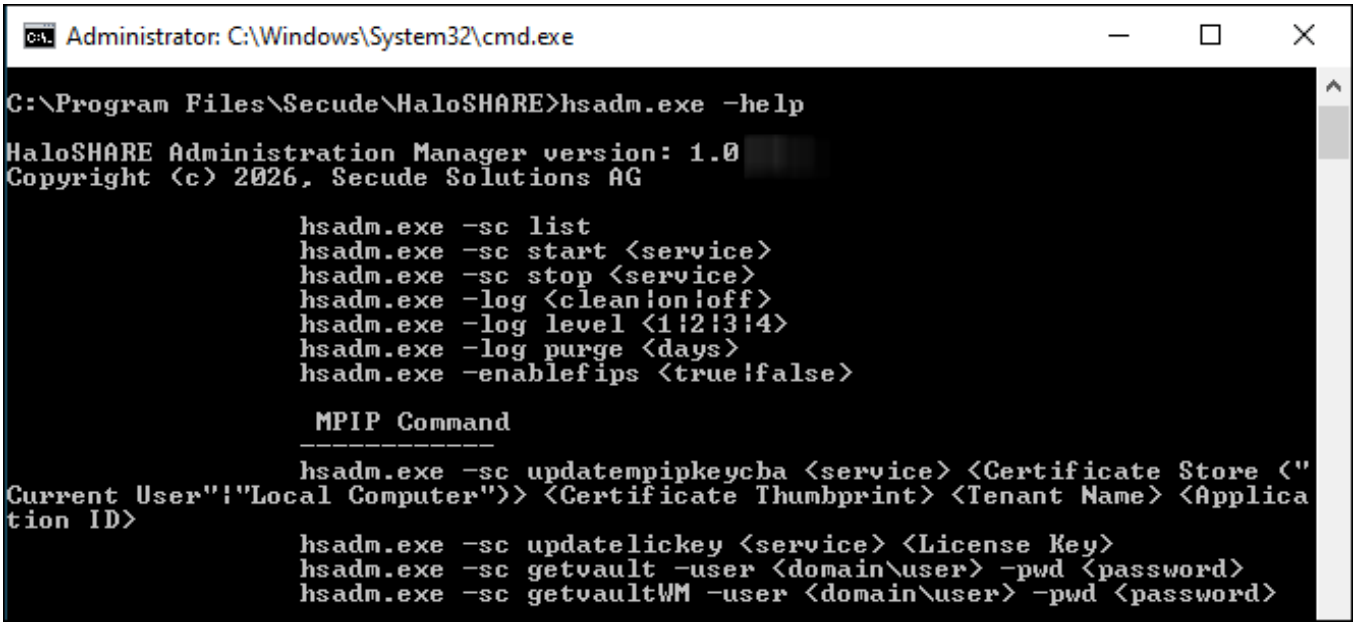
After installing HaloSHARE, you may want to change the configuration. To do so, run the tool `...\Secude\HaloSHARE\hsadm.exe` to view the commands. Please note that the admin tool does not support uppercase.

How to update MPIP labels in HaloSHARE?

If an MPIP label is added, removed, or updated in the Microsoft Purview portal, the administrator should restart the HaloSHARE Service so that the changes will take effect.

When is it necessary to restart the HaloSHARE service?

Whenever you modify the HaloSHARE registry settings, you need to restart the HaloSHARE Service.



hsadm.exe commands

Service Control Commands
`hsadm.exe -sc list` Use this command to view the service. **Output** **For a Domain User**

```
Display Name: Secude HaloSHARE
Service Name: HaloSHARE
Domain: HC.test
User Name: HC.test\administrator
Service Mode: MPIP
```

For a Non-Domain local user:

```
Display Name: Secude HaloSHARE
Service Name: HaloSHARE
Domain: .
User Name: .\superdocs
Service Mode: MPIP
```

```
hsadm.exe -sc start <service>
```

Use this command to start HaloSHARE. Note: This can be used only after setting user credentials to run HaloSHARE.

For example,

```
hsadm.exe -sc start HaloSHARE
```

Output

```
Service Started successfully.
```

```
hsadm.exe -sc stop <service>
```

Use this command to stop the HaloSHARE.

For example,

```
hsadm.exe -sc stop HaloSHARE
```

Output

```
Service Stopped successfully.
```

Log Command

```
hsadm.exe -log <clean|on|off>
```

1. clean: removes all files from the logging directory.
2. on: enables the service logging.
3. off: disables the service logging.

For example,

`hsadm.exe -log on`

Output

```
Current log enabled, level = 3.

INFO,Log already on.
C:\Users\Administrator\AppData\Local\Secude\HaloSHARE\log\
```

`hsadm.exe -log level <1|2|3|4>`

1. Log level: 1: Error and Info
2. Log level: 2: Error, Warning, and Info
3. Log level: 3: Error, Warning, and Info
4. Log level: 4: Error, Warning, Info, and Debug

For example,

`hsadm.exe -log level 4`

Output

```
Current log enabled, level = 3.

INFO,Logging enabled, level = 4.
```

`hsadm.exe -log purge <days>`

Use this command to set a time for log purging, i.e., the number of days by which the logs will be deleted.

For example,

`hsadm.exe -log purge 2`

Output

```
Current log enabled, level = 4.

INFO,Log files purge set to 2 day(s).
```

FIPS

`hsadm.exe -enablefips <true|false>`

Use this command to enable/disable the FIPS mode.

For example,

`hsadm.exe -enablefips true`

Output

```
Enabling FIPS module started.

Service Stopped successfully.

Extracting fips module files done.

Trying to Install fips modules for this pc.

fips modules configuration generated for this pc successfully.

Service Started successfully.
```

MPIP Commands

Update MPIP Certificate

```
hsadm.exe -sc updatempipkeycba <service> <Certificate Store ("Current User"|"Local Computer")> <Certificate Thumbprint> <Tenant Name> <Application ID>
```

Use this command to update the new MPIP CBA (Certificate-Based Authentication) Keys.

For example,

```
hsadm.exe -sc updatempipkeycba HaloSHARE "Current User" 6e9685132e2e86d1b0af75a848fcc7c0ec29839b halosecude.onmicrosoft.com u8352197-65e0-4fd2-9efb-b90027b801fb
```

Output

```
Policy XML file fetched successfully.

MPIP key updated successfully.
```

Update MPIP License Key

```
hsadm.exe -sc updatelickey <service> <License Key>
```

Use this command to update the License Key

For example,

```
hsadm.exe -sc updatelickey HaloSHARE B27N-CMTO-LWGH-AKEQ
```

Output

Spring License Key updated successfully

Display MPIP key

```
hsadm.exe -sc getvault -user <domain\user> -pwd <password>
```

Use this command to know your MPIP key information.

For example,

```
hsadm.exe -sc getvault -user .\administrator -pwd #9y->\"raQ8<
```

Output

```
Application ID: u8352197-65e0-4fd2-9efb-b90027b801fb

Tenant ID/Name: halosecude.onmicrosoft.com

Certificate Store: LocalComputer

Certificate Thumbprint: 6e9685132e2e86d1b0af75a848fcc7c0ec29839b

License Spring Key: B27N-CMTO-LWGH-AKEQ
```

Watermark details

Display Watermark key

```
hsadm.exe -sc getvaultWM -user <domain\user> -pwd <password>
```

Use this command to get your watermark licensing key information.

For example,

```
hsadm.exe -sc getvaultWM -user .\administrator -pwd #9y->\"raQ8<
```

Output

```
Certificate Store: LocalComputer

Certificate Thumbprint: 6e9685132e2e86d1b0af75a848fcc7c0ec29839b

License Spring Key: B37N-CSUO-LWIJ-AKBS
```

Help Commands

7.4. Registry Settings

The following section explains how the registry is used to store service settings. To modify the registry value, open Registry Editor, navigate to this path `Registry Root Directory = HKEY_LOCAL_MACHINE\SOFTWARE\Secude\HaloSHARE`, and modify the Reg Key as you want. Any changes to the registry will require a restart of HaloSHARE to take effect.

Name	Default value	Type	Description
dir_common	common	REG_SZ	The path to the directory where all the dependent DLL files are stored for the execution of HaloSHARE.
dir_log	log	REG_SZ	Log files are generated in the service running user's local profile, i.e., in the following location `%LOCALAPPDATA%\Secude\HaloSHARE\log`.
dir_tmp	tmp	REG_SZ	It stores the temporary files located at `%LOCALAPPDATA%\Secude\HaloSHARE\tmp`.
dir_vendor	C:\Program Files\Secude\	REG_SZ	This is Secude's vendor directory under which Secude's components will get installed. For example, `HaloSHARE`.
enable_fips	false	REG_SZ	1. true: By selecting this option, MPIP only uses FIPS-compliant encryption algorithms. 2. false: MPIP uses standard encryption algorithms.
enable_relabeling	on	REG_SZ	Defines the status of the relabeling. • on = Relabel feature is enabled to change the applied label or remove the label to decrypt the file. • off = Relabel feature is disabled.
haloshare_config_file	haloshare_config.enc	REG_SZ	Name of the configuration file that includes information about the folders and other essential parameters.
log_enable	on	REG_SZ	Defines the status of the log. • On = A Log file will be generated in the default location • Off = Log file will not be generated • Clean = Log files will be deleted. This parameter deletes only the logs and does

Name	Default value	Type	Description
			not modify the log_enable to "Clean" from "on/off".
log_level	3	REG_SZ	• Log level: 1: Error and Info • Log level: 2: Error, Warning, and Info • Log level: 3: Error, Warning, and Info • Log level: 4: Error, Warning, Info, and Debug
log_purge	7	REG_SZ	It indicates removing files older than a defined time frame. By default, the log files older than 7 days will be deleted.
ls_proxy		REG_SZ	Allows you to use a proxy server to access Secude's License Manager. This is an optional feature that should only be used if your firewall is blocking License Manager. Enter proxy server settings in the format `<URL>:<PORT>`. For example, `http://10.41.0.130:808`. Please make sure to restart the service.
scan_wait_time	5	REG_SZ	Specifies the service wait time. For any modification in the local source folder, the service scans every 5 seconds. For the Autodesk Forma folder, the service scans for changes every 30 seconds. If a rate limiter issue is expected, then you can increase the scan time. Example, 2 minutes (120 seconds).
version		REG_SZ	The version number of the installed service.

Configuration in the Registry

Endpoint Description

```
Registry path of endpoint = HKEY_LOCAL_MACHINE\SOFTWARE\Secude\HaloSHARE\ep\HaloSHARE
```

Name	Default value	Type	Description
block_pii	`false`	REG_SZ	Enable or disable the visibility of Personally Identifiable Information (PII) in the MIP SDK logs. The MIP SDK logs are located at`%LOCALAPPDATA%\Secude\HaloSHARE Service\log\mip_cache_storage\mip\logs\mip_sdk.miplog`. • false—PII will be visible in clear text in the MIP SDK logs. • true—PII will be masked with asterisks in the MIP SDK logs. This helps to protect the PII's confidentiality.
cachetype	`1`	REG_SZ	MPIP cache storage type used by the service. • In Memory—0, maintains the storage cache in memory in the application. • On Disk—1 (default storage type), stores the database (SQLite3) on disk in the directory provided in the settings object. The database is stored in plaintext. • On Disk Encrypted—2, stores the database (SQLite3) on disk in the directory provided in the settings object. The database is encrypted using OS-specific APIs.
cacheuserlicense	`1`	REG_SZ	• 0—false, End User License (EUL) will NOT be stored in the MPIP cache storage. • 1—true (default value), End User License (EUL) will be stored in the MPIP cache storage.

Name	Default value	Type	Description
cloudtype		REG_SZ	User's Azure Cloud Type. For example: Commercial.
credential		REG_SZ	Domain or computer name, name of the user under which the HaloSHARE service runs
databoundary	Default	REG_SZ	Audit and telemetry events are sent to the nearest collector, where these events are stored and processed. Other options: 1. Asia 2. Europe_MiddleEast_Africa 3. European_Union 4. North_America For example, if your AIP administrator sets North_America, the HaloSHARE service forces all telemetry and audit data to go directly to North America.
domain		REG_SZ	Name of the domain.
enableCUI	false	REG_SZ	1. true – CUI Marking feature is installed. 2. false – CUI Marking feature is not installed.
enabledke	0	REG_SZ	Double Key Encryption • 0—(default value) - disables the DKE functionality in the HaloSHARE service. • 1—(On) - Enables the DKE functionality in the HaloSHARE service. Please be aware that DKE labels are only visible when DKE functionality is enabled.

Name	Default value	Type	Description
enablefiletracking	0	REG_SZ	Obtain the protected file's content ID to track the file. • 0 (default value)—the content ID does not get extracted for the use of File Tracking. • 1—the content ID will be extracted for the use of File Tracking.
enableMIP	false	REG_SZ	1. true: When this option is selected, the CUI Marking feature is enabled. 2. false: When this option is not selected, the CUI Marking feature is disabled.
enableWM	false	REG_SZ	1. true: When this option is selected, the Watermarking feature is enabled. 2. false: When this option is not selected, the Watermarking feature is disabled.
IterationLimit	10	REG_SZ	Iteration limit for Creo file types. The default value is 10, however, you can modify and set your limit. Example: `test.prt.1`, `test.asm.2`
MIPAuthType		REG_SZ	Type of authentication method. MSALCBA for MPIP mode.
mode		REG_SZ	Type of HaloSHARE features. MPIP, Watermarking, or Combined.
policycloudurl		REG_SZ	Policy Cloud URL. For example: `https://dataservice.protection.outlook.com`
protectioncloudurl		REG_SZ	Protection Cloud URL. For example: `https://api.aadrm.com`
service	`HaloSHARE`	REG_SZ	Name of the service. By default, it is HaloSHARE.

Name	Default value	Type	Description
streambuffersize	10	REG_SZ	It is a buffer size used for memory-based encryption with the MIP SDK. When the allotted buffer size is exceeded, an additional memory of stream buffer size is allocated, and this process is repeated until the encryption/decryption operation is completed. The default setting is 10 MB.

Configuring Endpoint

Proxy Configuration

Many enterprises enforce a **Group Policy Objects** (GPO) that requires all outbound internet traffic routed through a proxy server. These proxy settings must be used by both the MIP SDK and the MSAL library for MPIP authentication and functionality. To use proxy settings for the MSAL library, we need to set the `msal_proxy_address` in `HKEY_LOCAL_MACHINE\SOFTWARE\Secude\HaloSHARE`.

Name	Type	Data
msal_proxy_address	REG_SZ	`<http://IP Address>`

Configuring MSAL proxy

If the above steps do not work for the service running user, set the **ProxyServer** and **ProxyEnable** registry keys under `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings` for the service running user.

Name	Type	Data
ProxyServer	REG_SZ	`<http://IP Address>`
ProxyEnable	REG_SZ	• 1 to enable. • 0 to disable.

Configuring proxy

To allow MIP SDK to use the proxy settings set up in your environment, follow the steps below:

Determine whether the proxy server has been properly set up by running the following command.

```
C:\Windows\system32>netsh winhttp show proxy
Current WinHTTP proxy settings:
Direct access (no proxy server).
```

If the response to the command is as shown above, it indicates that the proxy server has not been configured in the registry for WinHTTP.

To configure the proxy server for WinHTTP, use the following command:

Syntax: `C:\Windows\system32>netsh winhttp set proxy <proxyservername>:<portnumber>`

Example: `C:\Windows\system32>netsh winhttp set proxy 190.160.166.191:8080`

In this case, the proxy server has been set up with `190.160.166.191:8080`. Once this command is executed successfully, the registry is updated with the proxy server URL, and the HaloENGINE Tomcat Service ensures that the configured proxy settings are applied.

7.5. Access Protected Files

After setting HaloSHARE in your environment, you may start sharing business files in folders. Once the files have been protected, you should know how to open MPIP-protected files with HaloCAD Add-ons. For information on how to open a protected file, refer to the corresponding HaloCAD Add-on documentation.

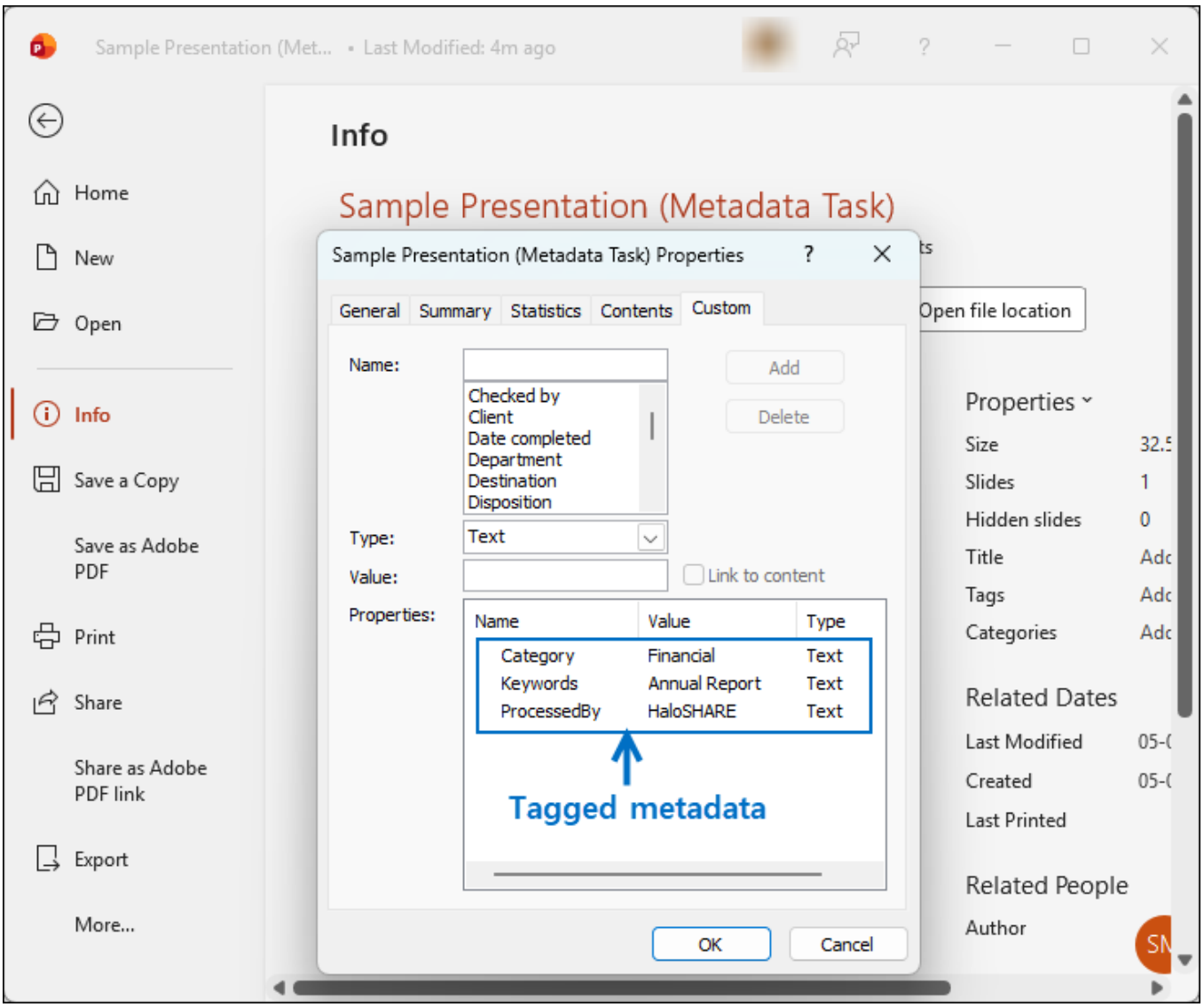
7.5.1. Sample Results

To view the HaloSHARE watermarked CAD files, the HaloCAD Add-on is required for the CAD application. For information on how to view a HaloSHARE watermarked CAD file, refer to the HaloCAD Add-on documentation.

Viewing Watermark metadata in CAD files:

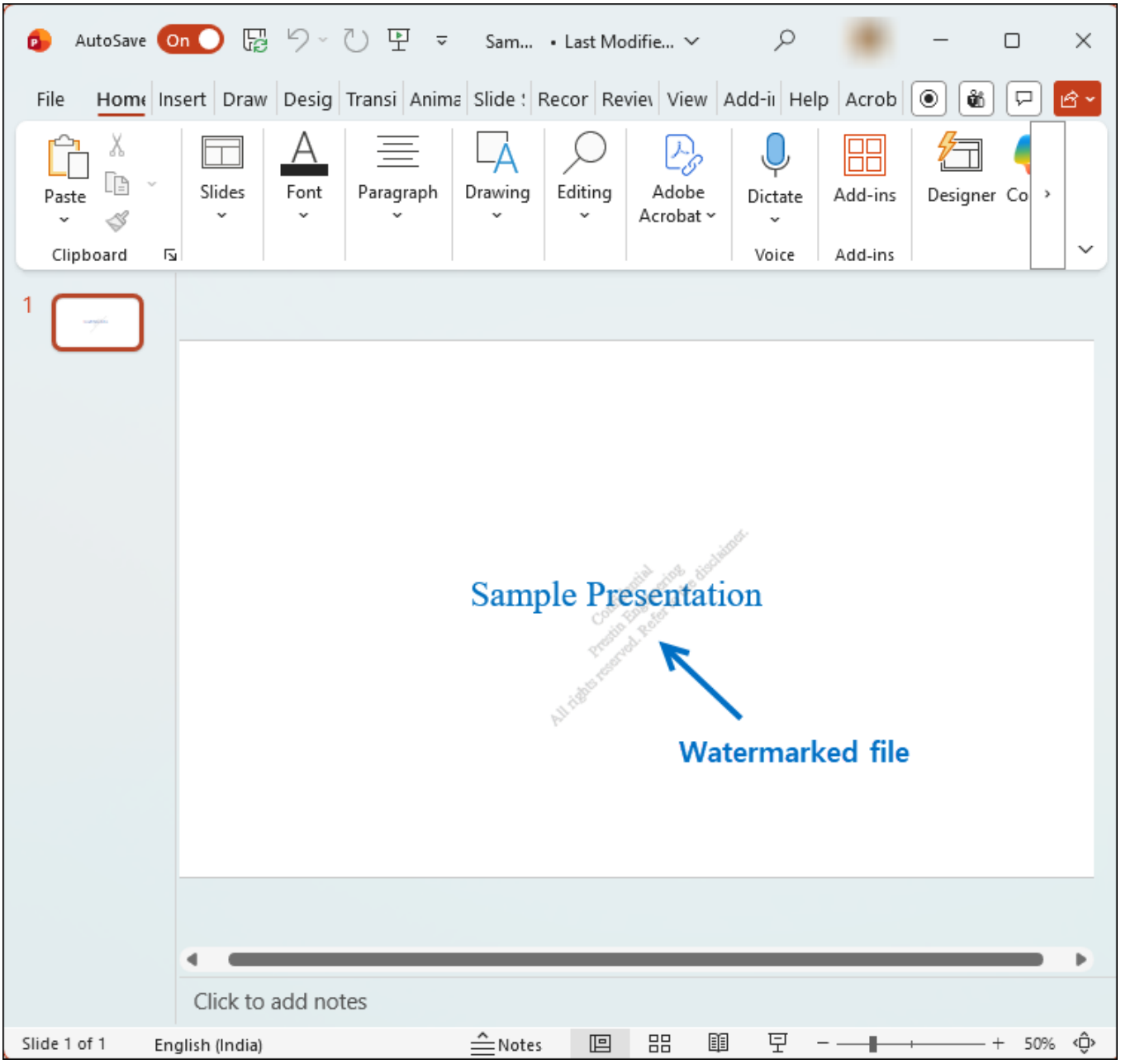
1. **RVT:** Install the **RevitLookup** tool to view the metadata. For more details, please refer to "Watermark in RevitLookup".
2. **DWG:** Go to the file's Custom Properties to view the metadata.
3. **IFC:** Open the file in any text editor, and scroll to the end to view the metadata.

7.5.1.1. Metadata Task



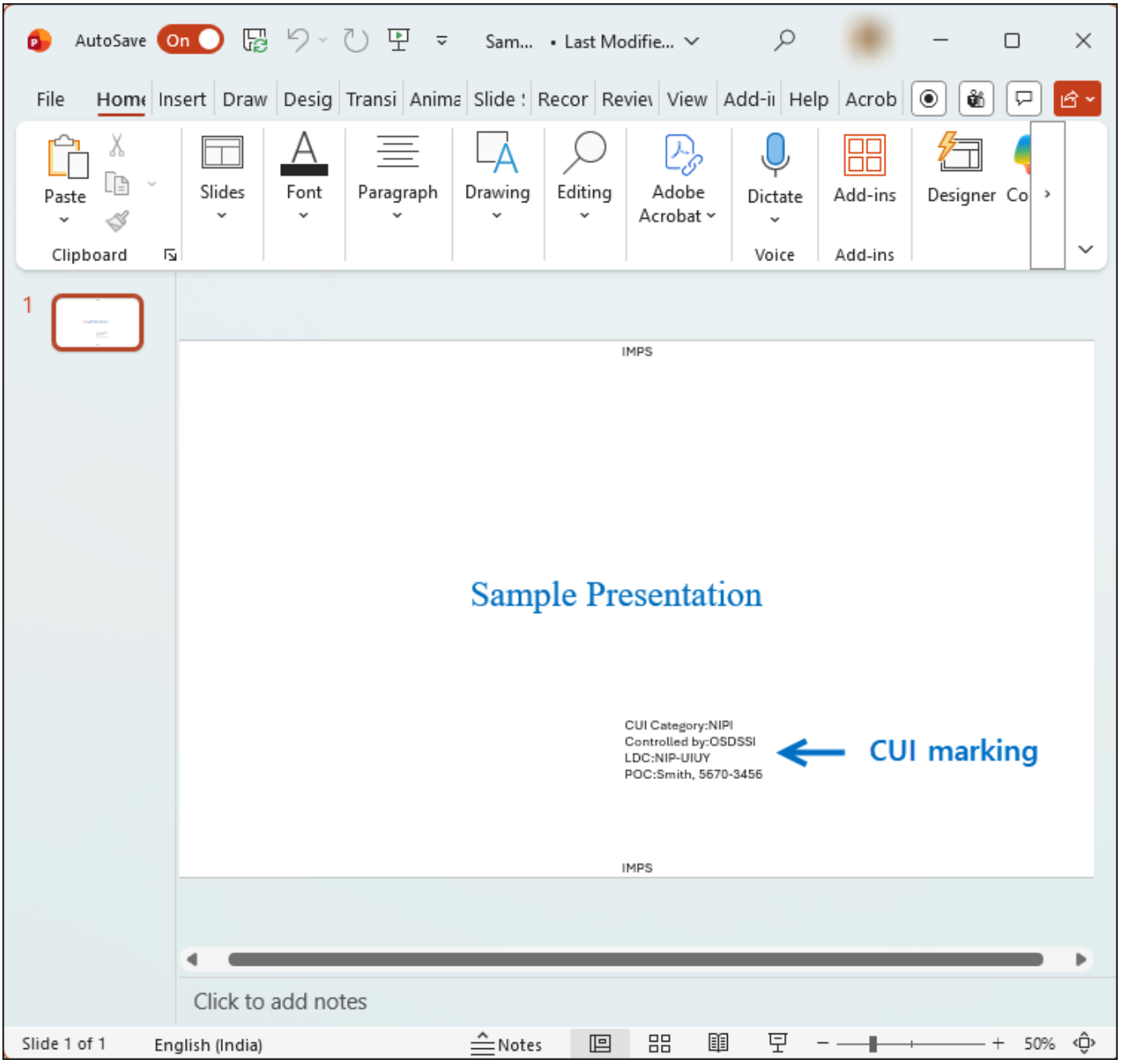
Sample - Metadata Task

7.5.1.2. Watermark Task



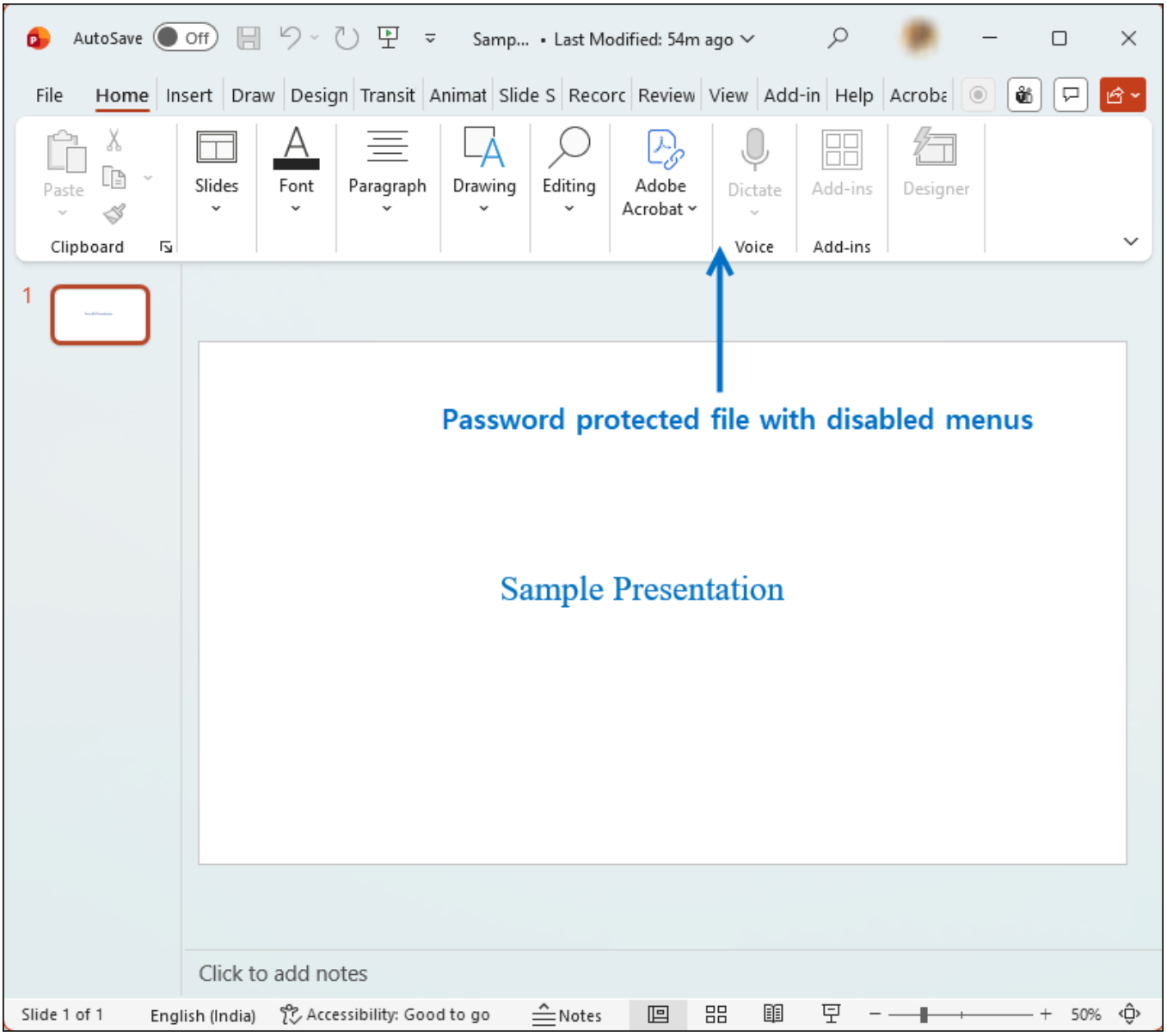
Sample - Watermark Task

7.5.1.3. Compliance Task



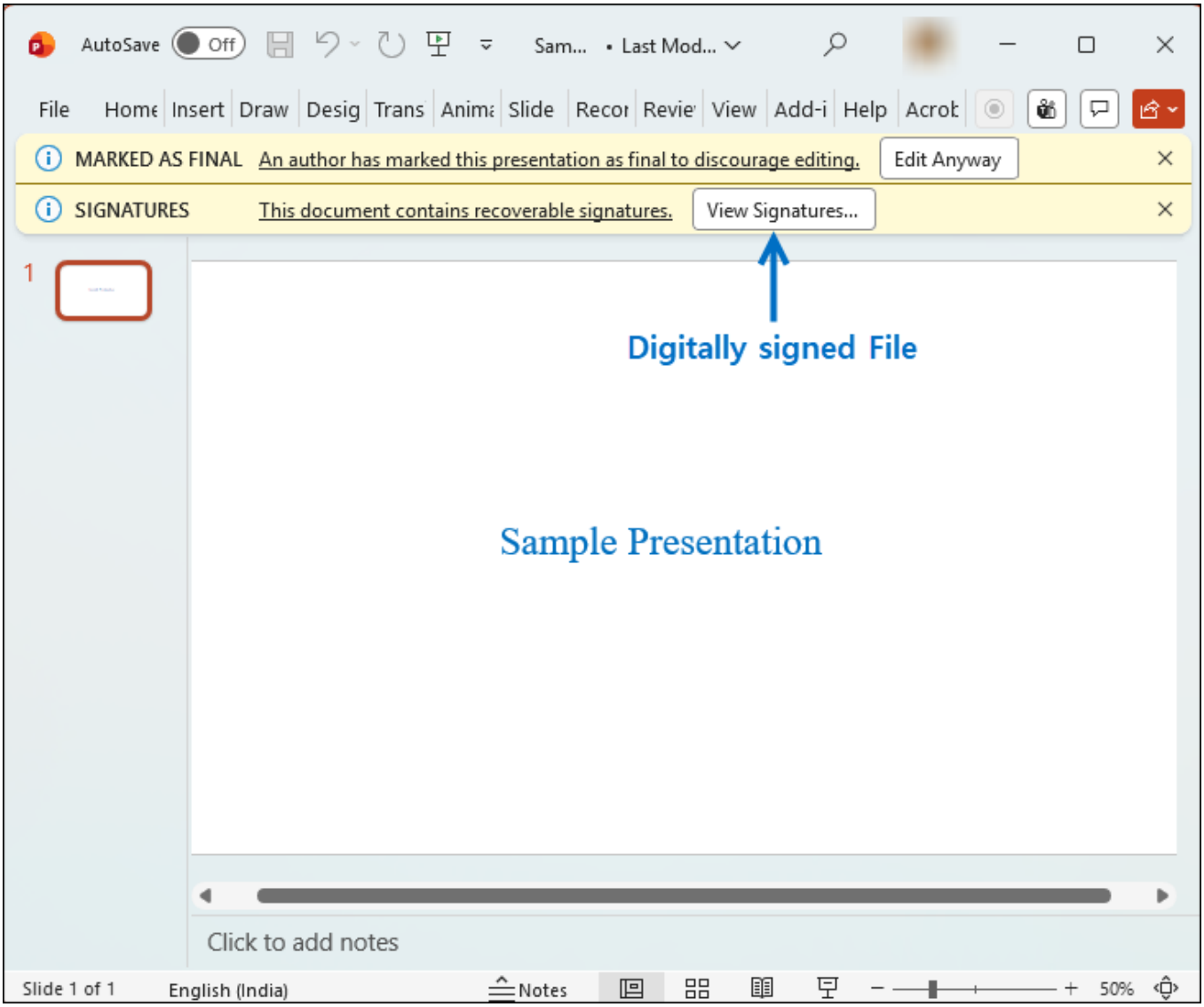
Sample - Compliance Task

7.5.1.4. Password Protection Task



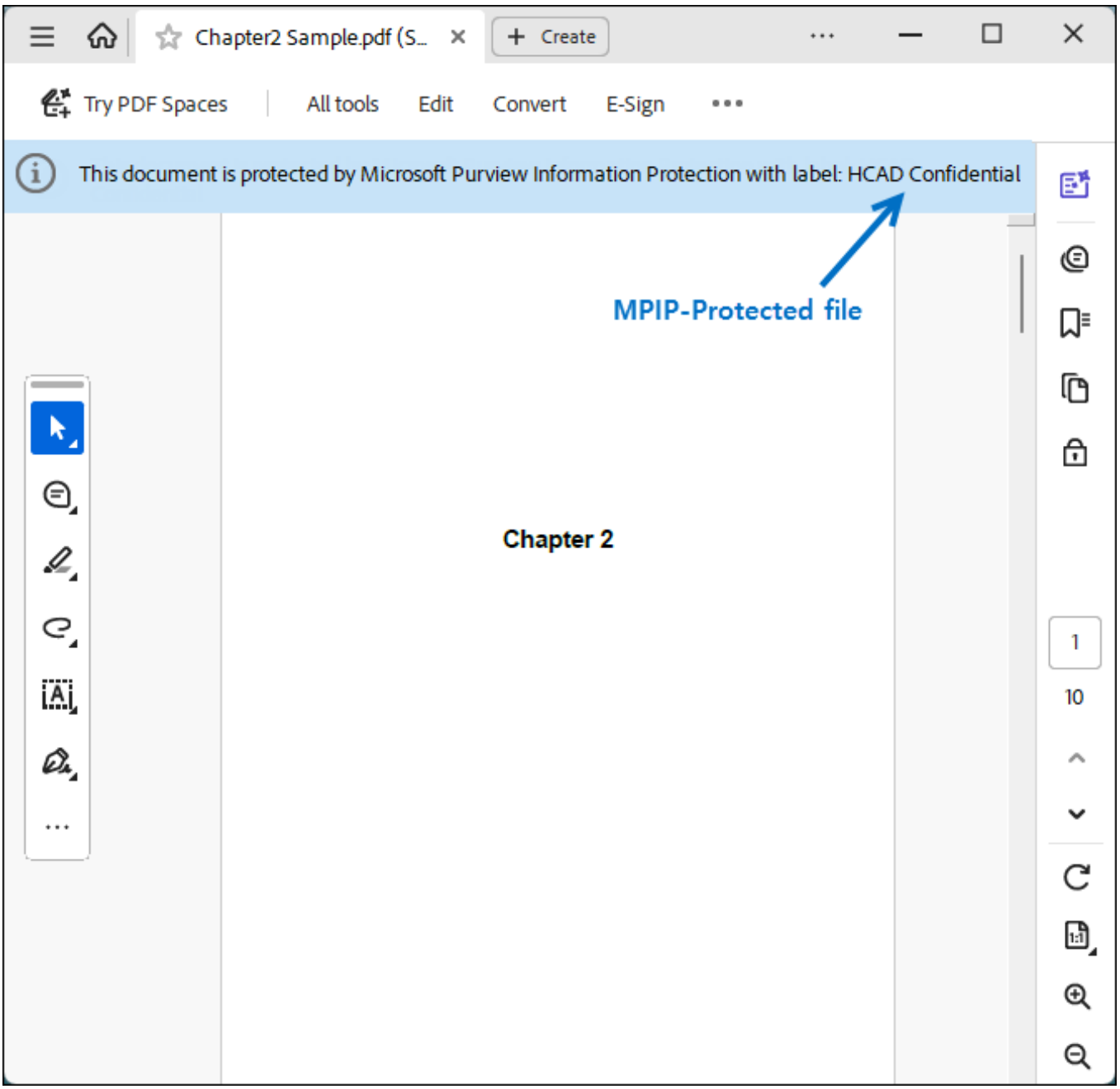
Sample - Password Protection Task

7.5.1.5. File Signing Task



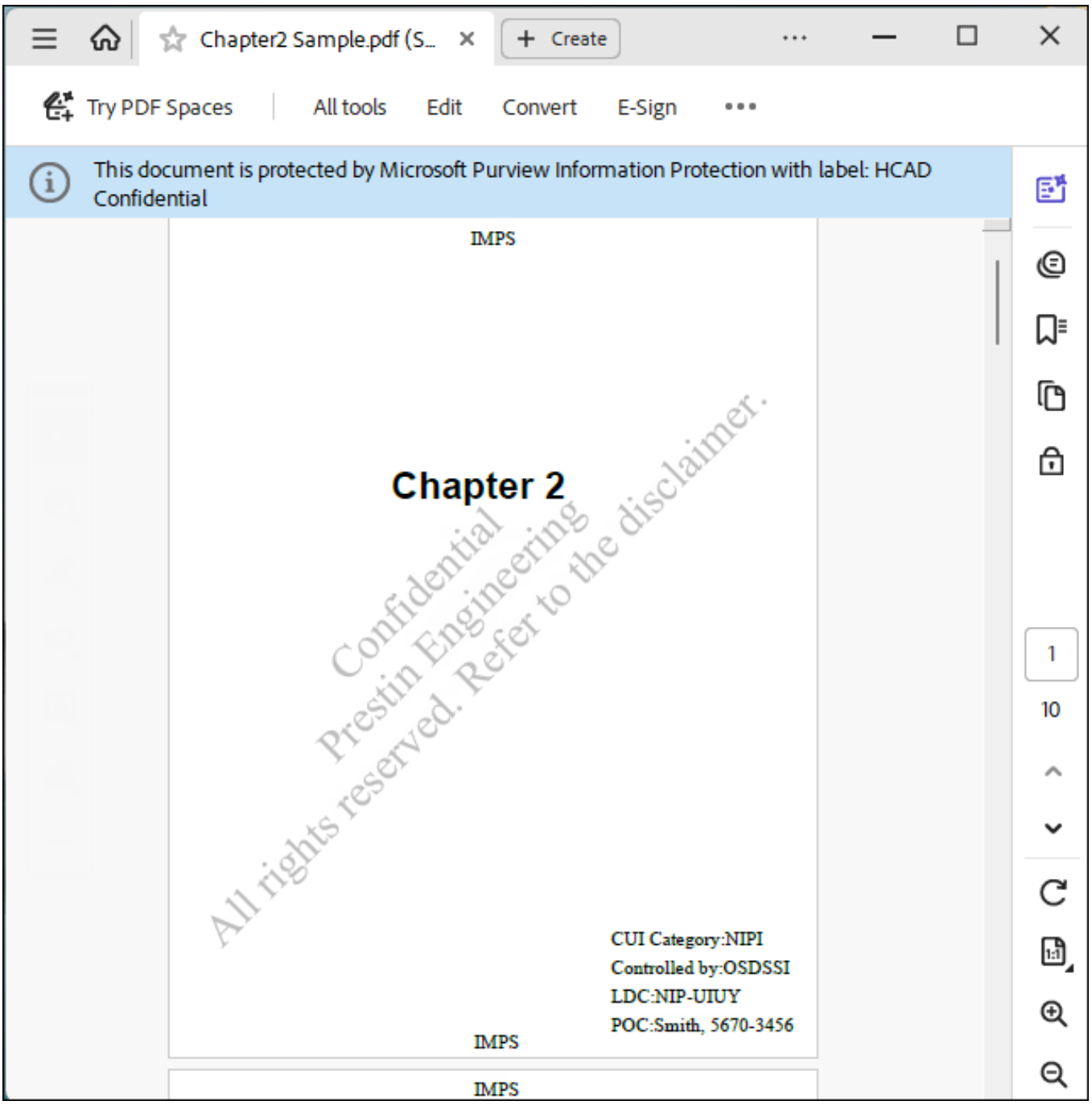
Sample - File Signing Task

7.5.1.6. MPIP Task



Sample - MPIP Task

7.5.1.7. Combined Workflow



Sample - Combined Workflow

8. Troubleshooting

This page will help you overcome the most common problems that may occur during the installation and configuration of the HaloSHARE, as listed below.

8.1. Installation Interrupted due to Improper Configuration

Symptom

Error message: "*Failed to get thumbprint. Please check whether correct certificate file or correct password is given.*"

Background

The error message given above appears while installing the HaloSHARE.

Cause

The Root CA Signed Certificate password that you are attempting to import into the Certificate Store is incorrect.

Recommended Action

Verify and enter the correct certificate password.

8.2. Installation Interrupted due to Certificate

Symptom

Error message: "*Please check the certificate details and verify the certificate is installed properly.*"

Background

HaloSHARE installation in MPIP results in the error message shown above.

Cause

The certificate that you installed in the Certificate Store (Current User or Local Computer) has expired.

Recommended Action

1. Verify the certificate using the Microsoft Management Console (MMC) snap-in.
    a. If the certificate is invalid, add a new certificate.
    b. If you proceed to install HaloSHARE at this point, you will receive the following message "*Please check the certificate validity and details, Verify the certificate is installed properly and configured in the Azure portal.*"

2. Make sure that the same certificate is updated on the Azure portal (under the **Certificate** section > click **Upload certificate**).
3. Continue with the installation now.

8.3. Installation Interrupted Due to Expired Certificate

Symptom

The following error message is displayed:
"*Client assertion contains an invalid signature. [Reason - The key was not found, Thumbprint of the key used by client.]*"

Background

HaloSHARE installation in MPIP displays the error message shown above.

Cause

The certificate has expired. Although it was updated in the Certificate Store (Current User or Local Computer), it was not updated in the Azure portal.

Recommended Action

1. Log in to the Azure portal.
2. Go to your registered application.
3. Under **Manage** > **Certificates & secrets**, click **Upload certificate** and install the new certificate.
4. Continue the installation.

8.4. HaloSHARE Service fails to Start

Symptom

The error appears as "*Process finished with error. Please check logs for more details*."

The HaloSHARE Service log shows the following error.

```
Cannot establish access to the shared memory [Global\0150B81D-A6E6-4EFD-B1FA-
97172AD05C44HCS].

(hr = 0x80070005)

Access is denied.
```

Background

The error messages mentioned above appear while initializing the HaloSHARE Service.

Recommended Action

Add the following registry key `ipc_enable_file` in `HKEY_LOCAL_MACHINE\SOFTWARE\Secude\HaloSHARE` and reinitialize the service.

Name	Type	Data
ipc_enable_file	REG_SZ	on

Configuring registry entry

9. Technical Support

Before contacting Technical Support, ensure that you have the following information available.
Providing this information helps the support team investigate and resolve your issue more efficiently.

- Full contact details
- Product build version
- Date, time, and description of the error (include screenshots, if possible)
- Details of any third-party software used with the product
- Any additional information required to reproduce the issue

Contact Technical Support

Secude provides technical support through email support@secude.com. When contacting Technical Support by email, include your company details, a detailed description of the issue, and the relevant log files (if available). A support representative will respond to your inquiry.

Additional Resources

Visit the Secude website https://secude.com to learn about upcoming events, press releases, and to download white papers.

Documentation Feedback

Secude values your feedback and continuously strives to improve product documentation. To provide feedback, send an email to: documentation@secude.com
Include the following details in your feedback:

- Product name and version
- Documentation topic
- Description of the suggestion or error

The technical documentation team reviews all feedback and incorporates relevant updates in future documentation releases.

10. Appendix

This section provides supplemental information.

10.1. 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 HaloSHARE are shown in the table below.

Library	Version	Source Code	License Link
Boost Library	1.85.0	https://archives.boost.io/release/1.85.0/source/	https://www.boost.org/LICENSE_1_0.txt
Protobuf Library	5.26.1	https://github.com/protocolbuffers/protobuf/releases/tag/v21.2	https://github.com/protocolbuffers/protobuf/blob/master/LICENSE
WTL	9.0	https://github.com/wxWidgets/wxWidgets	https://en.wikipedia.org/wiki/Common_Public_License
Rapidxml	1.13	https://sourceforge.net/projects/rapidxml/files/latest/download	http://rapidxml.sourceforge.net/license.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/
Licensespring	7.49.0	-	-
OpenSSL	3.2	https://github.com/openssl	https://github.com/openssl/openssl/blob/master/LICENSE.txt
MSAL	4.82.1	https://github.com/AzureAD/microsoft-authentication-library-for-dotnet	https://github.com/AzureAD/microsoft-authentication-library-for-dotnet/blob/master/LICENSE

Library	Version	Source Code	License Link
PDFSharp	6.2.2	https://github.com/empira/PDFsharp	https://github.com/empira/PDFsharp?tab=License-1-ov-file#readme
Closed XML	0.105.0	https://github.com/ClosedXML/ClosedXML	https://github.com/ClosedXML/ClosedXML?tab=MIT-1-ov-file#readme
Open XML SDK	3.2.0, 3.1.1	https://github.com/dotnet/Open-XML-SDK	https://github.com/dotnet/Open-XML-SDK?tab=MIT-1-ov-file#readme
ShapeCrawler	0.78.5 all MIT license	https://github.com/ShapeCrawler/ShapeCrawler	https://github.com/ShapeCrawler/ShapeCrawler?tab=MIT-1-ov-file#readme
Autodesk.SDK Manager	1.1.2	https://www.nuget.org/packages/Autodesk.SDKManager	https://www.nuget.org/packages/Autodesk.SDKManager/1.1.2/License
Autodesk.Authentication	2.0.1	https://www.nuget.org/packages/Autodesk.Authentication	https://www.nuget.org/packages/Autodesk.Authentication/2.0.1/License
Autodesk.Oss	2.3.3	https://www.nuget.org/packages/Autodesk.Oss	https://www.nuget.org/packages/Autodesk.Oss/2.3.3/License
Autodesk.Data Management	2.1.3	https://www.nuget.org/packages/Autodesk.DataManagement	https://www.nuget.org/packages/Autodesk.DataManagement/2.1.3/License

Third-party libraries

10.2. Permission Levels and Usage Rights

10.2.1. Basic Permissions

The following table lists the basic permissions and the usage rights that they contain:

S.No	Permission Level	Usage Rights (Allowed Recipient Actions)
1	View	Open and read the data (also known as “Read-only”). It includes Zoom and view from different angles (for CAD file types).

S.No	Permission Level	Usage Rights (Allowed Recipient Actions)
2	Edit	Edit the file and save it
3	Copy	Extract data (including screen captures) from the file into the same or another file.
4	Print	Print the content
5	Export	Save the content to a different filename (Save As). Also includes “Export to PDF”.
6	Change Rights	Changing the label that is applied to a file includes removing protection and saving it as an unprotected file.
7	Owner (Full Control rights)	Grants all rights to the file and all available actions can be performed. Also includes the following permissions: 1. Remove protection 2. Relabel a file

Basic Permissions

Author (creator) of a file

The author of a file has all the rights and actions mentioned in the above table. Also includes the following permissions:

1. Open file after the expiry date
2. Revoke access

10.2.2. Custom Permissions

The following table lists the custom permissions and the usage rights that they contain:

S.No	Permission Level	Usage Rights (Allowed Recipient Actions)
1	Viewer	Open and read the data (also known as “Read-only”). It includes Zoom and view from different angles.
2	Reviewer	Viewer’s allowed permissions plus: 1. Edit 2. Save the file
3	Co-Author	Reviewer’s allowed permissions plus:

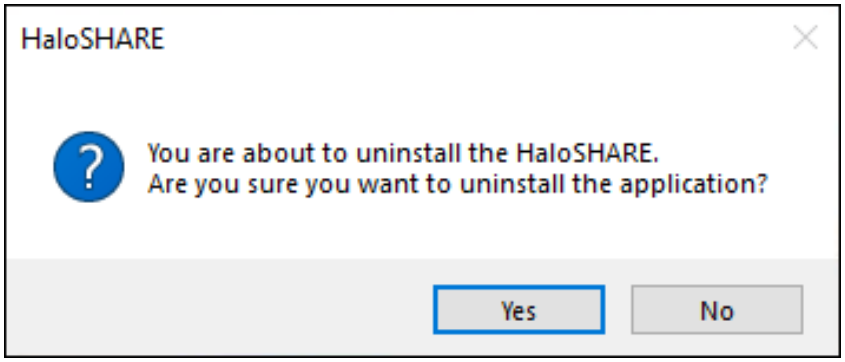
S.No	Permission Level	Usage Rights (Allowed Recipient Actions)
		1. Print 2. Extract data (including screen captures) from the file into the same or another file.
4	Co-Owner	Co-Author's allowed permissions plus: 1. Export 2. Change Rights
5	Only for me	Grants all rights to the file and all available actions can be performed only by the author of the file.

Custom Permissions

10.3. Uninstallation

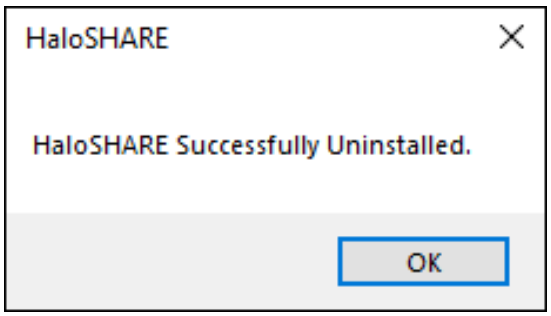
When you no longer use the service, you may uninstall the application. Uninstalling removes all files and registry settings that were added to your computer during the initial installation.

1. Click **Start** menu > go to **Control Panel** > **Programs** > **Programs and Features** > **Uninstall a Program** > select **HaloSHARE** from the list > right-click and select **Uninstall** option.
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 application.
3. The following confirmation message appears.



Uninstall message #1

4. Click **Yes** to confirm that you want to remove it from the computer.
5. The service is uninstalled successfully. Click **OK** to close the dialog.



Uninstall message #2

Index

Secude

www.secude.com

About Secude

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

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