Secude

HaloSHARE

Installation and Configuration Manual

Version 1.1

Copyright

© 2025-2026 Secude Solutions AG. All Rights Reserved.

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

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

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

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

Contact

Secude Solutions AG

Murbacherstrasse 19

6003 Luzern, Switzerland

Mail: info@secude.com

Support

Web: https://support.secude.com

Mail: support@secude.com

Table of Contents

1. INTRODUCTION 1

1.1. What distinguishes HaloSHARE GenNXT? 1

1.2. About this Manual 1

1.3. Terminology 2

1.4. Acronyms 3

1.5. Features 4

1.6. Feature Availability and License Requirements 5

1.7. General FAQs 6

2. QUICK START INSTALLATION OVERVIEW 7

3. ARCHITECTURE 8

4. SYSTEM REQUIREMENTS 10

5. PREREQUISITES 12

5.1. MPIP Protection 12

5.1.1. Register an Application in Microsoft Entra ID 12

5.1.2. Create and Configure the Sensitivity Labels 20

5.1.3. Enable TLS 1.2 for Microsoft Entra ID Authentication 21

5.2. Register an application in Autodesk Platform Services 22

5.2.1. Create an APS Account 22

5.2.2. Set up a Developer Hub 22

5.2.3. Create a Developer Hub 23

5.2.4. Create Application Credentials 24

5.2.5. Provide access to Autodesk Forma 25

5.3. Watermarking CAD files 26

5.4. File Signing Task 27

5.5. General 28

6. INSTALLING THE HALOSHARE GENNXT 29

6.1. Interactive Installation 29

6.2. Update from Old to New Version 37

7. CONFIGURING THE HALOSHARE GENNXT 38

7.1. Administration 38

7.1.1. Autodesk Forma Settings 40
7.1.2. Quick Start for Workflows 42
7.2. Configure Workflows 45
7.2.1. Configure Metadata Task Attributes 47
7.2.2. Configure Watermark Task Attributes 49
7.2.3. Configure Compliance Mark Task Attributes 52
7.2.4. Configure Password Protection Task Attributes 53
7.2.5. Configure File Signing Task Attributes 55
7.2.6. Configure MPIP Task Attributes 56
7.2.7. Configure Combined Workflows 59
7.3. Configure the Service by Using the Admin Tool 62
7.4. Registry Settings 67
7.5. Access Protected Files 73
7.5.1. Sample Results 73
8. TROUBLESHOOTING 81
8.1. Installation Interrupted due to Improper Configuration 81
8.2. Installation Interrupted due to Certificate 82
8.3. Installation Interrupted Due to Expired Certificate 83
8.4. HaloSHARE Service fails to Start 84
9. TECHNICAL SUPPORT 85
10. APPENDIX 86
10.1. Third-Party Libraries 86
10.2. Permission Levels and Usage Rights 87
10.2.1. Basic Permissions 87
10.2.2. Custom Permissions 88
10.3. Uninstallation 90

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

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

1.1. What distinguishes HaloSHARE GenNXT?

Digital transformation improves supply chain efficiency but also increases the risk of data exposure. Sharing unprotected files can lead to data breaches, operational disruption, and financial loss. In collaborative environments, unauthorized access and accidental file sharing are common risks. To protect business operations without disrupting workflows, organizations must secure project files by default.

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

HaloSHARE GenNXT also supports watermarking, CUI marking, digital signing, password protection, and metadata tagging. These capabilities help organizations securely share, track, and manage files while maintaining user productivity.

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

1.2. About this Manual

This manual provides step-by-step instructions for installing and configuring HaloSHARE GenNXT. It is intended for system administrators and IT professionals responsible for deploying HaloSHARE GenNXT in enterprise environments.

This manual covers the following tasks:

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

1.3. Terminology

The following table defines the terms used throughout this manual.

Term	Description
HaloSHARE GenNXT radius	A predefined folder monitored by HaloSHARE GenNXT. Files placed in this folder are automatically processed based on the configured workflow.
Workflow	A configured sequence of tasks that processes files, such as applying protection, watermarking, or metadata, before moving them to a destination folder.
Source folder	The folder that HaloSHARE GenNXT monitors to apply the configured workflow tasks.
Destination folder	The folder where processed files are copied or moved after workflow execution.
Sensitivity label	A Microsoft Purview Information Protection label that classifies and protects files based on organizational policies.
Custom permissions	User-defined protection settings that can be applied without using Microsoft Purview sensitivity labels.
Metadata	Additional information embedded in a file to support classification, tracking, or identification.
Watermark	Visible text or graphics added to a document to indicate ownership or classification.
CUI marking	Controlled Unclassified Information markings applied to documents to meet compliance requirements.

Terminology used

1.4. Acronyms

The following table lists the acronyms used throughout this manual.

Acronym	Description
APS	Autodesk Platform Services
CAD	Computer-Aided Design
CA	Certificate Authority
CUI	Controlled Unclassified Information
HTTPS	Hypertext Transfer Protocol Secure
MPIP	Microsoft Purview Information Protection
SDK	Software Development Kit
TLS	Transport Layer Security
URI	Uniform Resource Identifier
URL	Uniform Resource Locator

Acronyms

1.5. Features

HaloSHARE GenNXT provides the following capabilities:

- Protects multiple files in folders in bulk.
- Applies label-based protection by using Microsoft Purview Information Protection or user-defined custom permissions.
- Lets you customize protection settings.
- Enables you to remove protection from files.
- Enables you to relabel files by using existing sensitivity labels.
- Applies bulk watermarks with unique, date-stamped sharing information to improve content security and ownership visibility.
- Adds custom metadata to improve file classification, security, and contextual awareness.

1.6. Feature Availability and License Requirements

Feature	Description	License Requirement
MPIP Protection	Applies Microsoft Purview sensitivity labels and encrypts or decrypts files. Supports relabeling.	Requires a license with the MPIP Protection feature enabled.
Watermarking	Adds user-defined watermarks to PDF, CAD, and Microsoft Office files.	Requires a license with the Watermark feature enabled.
Compliance Marking (CUI)	Applies Controlled Unclassified Information markings to PDF and Microsoft Office files.	Requires a license with the CUI feature enabled.
Password Protection	Protects files by using a user-defined password.	Requires a license with the Password Protection feature enabled.
File Signing	Protects files by using a digital signature.	Requires a license with the File Signing feature enabled.
Metadata Marking	Embeds user-defined metadata for classification and tracking.	Requires a license with the Metadata Marking feature enabled.

Feature set up

License Combinations in HaloSHARE GenNXT

The table lists the base license options available for HaloSHARE GenNXT. Depending on your requirements, you can combine multiple licensed features. For example, you can combine MPIP protection with watermarking for PDF files or watermarking for Microsoft Office files with CUI marking for PDF files.

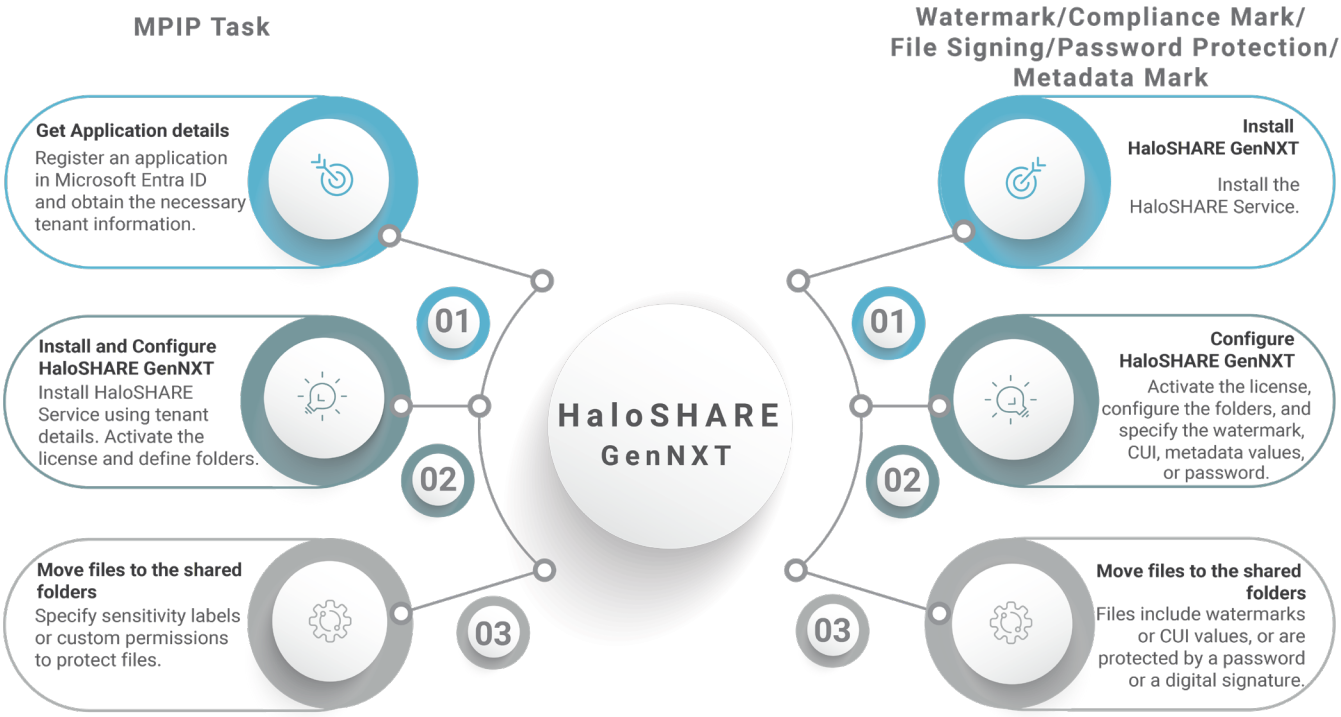
1.7. General FAQs

This section answers frequently asked questions about HaloSHARE GenNXT. If you need additional assistance, contact your Secude sales representative or the Secude Support team.

1. **What does HaloSHARE GenNXT 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 GenNXT supports all CAD native file types.
3. **What happens if an unauthorized person attempts to open a HaloSHARE GenNXT-labeled file?**
   HaloSHARE GenNXT first authenticates the user by verifying their identity. If authentication fails, access to the file is denied, and an error message is displayed.
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 Entra admin center. 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 GenNXT 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 GenNXT allows you to protect files by using user-defined custom permissions without applying MPIP sensitivity labels.
7. **How to open a protected CAD file?**
   You can open protected CAD files by using the HaloCAD Add-on for supported CAD applications.
8. **How to open a protected PDF file?**
   You can open protected PDF files by using Adobe Acrobat Reader DC, Adobe Acrobat DC, Microsoft Edge, or the Microsoft Purview Information Protection Viewer.
9. **How do I view the watermark on a CAD file?**
   To view watermarks in a HaloSHARE GenNXT-protected CAD file, install the HaloCAD Add-on for your supported CAD application.

2. Quick Start Installation Overview

The following figure provides a high-level overview of the HaloSHARE GenNXT installation process.



Quick start implementation steps

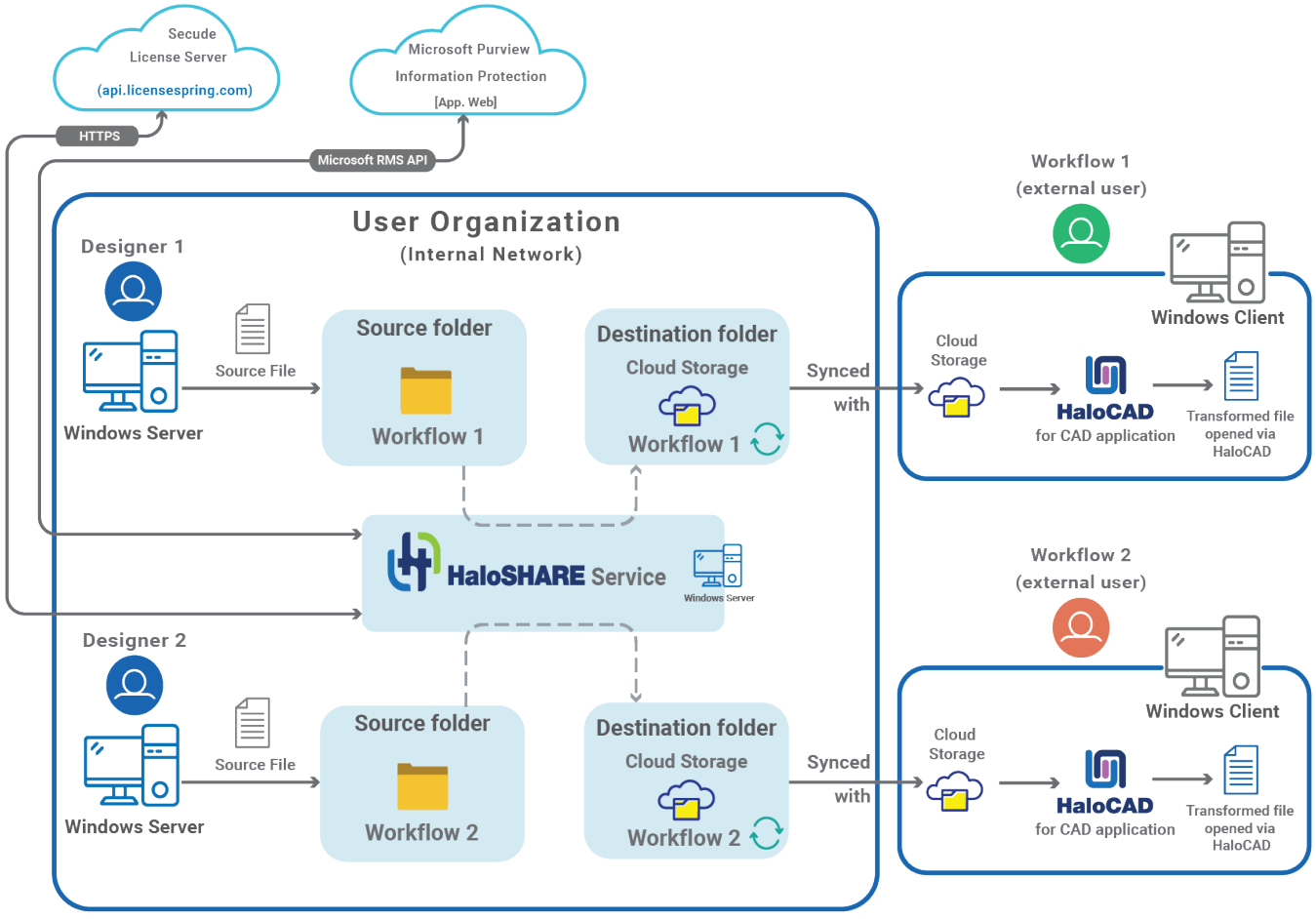
3. Architecture

In a typical deployment, designers share project files with external partners. HaloSHARE GenNXT enables administrators to configure workflows by assigning source and destination folders for each partner. Based on the configured workflow, HaloSHARE GenNXT automatically processes files and moves them from the source folder to the corresponding destination folder, as shown in the following figure.

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

Source and destination Folders

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



Architecture

Shared folder location

- The destination folder for external users can be located on Microsoft OneDrive, Microsoft SharePoint, or Autodesk Forma (formerly Autodesk Construction Cloud Docs), depending on your workflow configuration.
- When sharing files through Microsoft SharePoint or OneDrive, ensure that synchronization occurs through the respective client application (OneDrive sync app).
- If the user selects a source folder from OneDrive or SharePoint, ensure that the folder is synchronized successfully to the local drive and displays a green check mark (✅) before proceeding. This helps ensure that all workflow tasks are completed successfully.

HaloSHARE GenNXT monitors the configured source folder and its subfolders for new files. Depending on the tasks configured in the workflow, it performs one of the following actions:

- **MPIP Task:** Applies the configured MPIP sensitivity label or custom permissions.
- **Watermark Task:** Applies the configured watermark.
- **Compliance Mark Task:** Applies the configured CUI markings.
- **File Signing Task:** Applies the configured digital signature.
- **Password Protection Task:** Applies the configured password protection.
- **Metadata Mark Task:** Embeds the configured metadata.

If **Move to Destination** is configured in the workflow, the processed file is moved to the configured destination folder, where external users, including suppliers, vendors, and consultants, can access HaloSHARE GenNXT-protected and watermarked CAD files only by using the HaloCAD Add-on. For more information, refer to the HaloCAD User Manual.

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	• Microsoft Windows Server 2022 and above. • Latest Windows Server versions may include a .NET Framework version by default. If .NET Framework 4.6.2 or later is not installed, install it before proceeding with the HaloSHARE GenNXT installation. • Latest Windows updates installed.
MPIP task label protection-specific requirements	
Office 365 Subscription	• An Azure subscription is required to use Azure RMS and the MPIP functionality. • A working Microsoft Entra ID service must be available. • Microsoft Purview Information Protection must be fully configured. • HaloSHARE GenNXT creates an outbound network communication with Microsoft Azure Services. • TLS 1.2 or higher must be enabled to ensure the use of cryptographically secure protocols. • Register an application to get the Application (client) ID and Tenant ID in the Microsoft Entra admin center. • Refer to the table below, "**Recommended URLs, Addresses, and Ports for MPIP**" to know about the service endpoints.
Supported file types	• `.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`, `.stl`, `.stp`, `.ste`, `.stpz`, `.tcw`, `.u3d`, `.unv`, `.usdz`, `.vda`, `.pvz`, `.qif`, `.wrl`, `.x_b`, `.x_t`, `.xaml`, `.z3`, `.edrw`, and `.zip`. • Creo file formats with iterations: `.prt`, `.asm`, `.sec`, `.frm`, `.drw`, `.lay`, `.cem`, `.mfg`, `.neu`, `.log`, and `.pvz`.

Components	Details
	• 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 applications	• AutoCAD 2023, 2024, 2025, 2026, 2027 • Revit 2023, 2024, 2025, 2026, 2027
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 • PDF
Compliance Mark (Controlled Unclassified Information) task specific requirements	
Supported file types	• Supported: `.pdf`, `.docx`, and `.pptx` • Not supported: `.xlsx`

Requirements

5. Prerequisites

Complete the following prerequisites before installing HaloSHARE.

5.1. MPIP Protection

This section describes the prerequisites required to configure Microsoft Purview Information Protection.

5.1.1. Register an Application in Microsoft Entra ID

This section describes how to register an application in Microsoft Entra ID, obtain the **Application (client) ID** and **Directory (tenant) ID**, assign the required API permissions, and upload the certificate required for MPIP authentication.

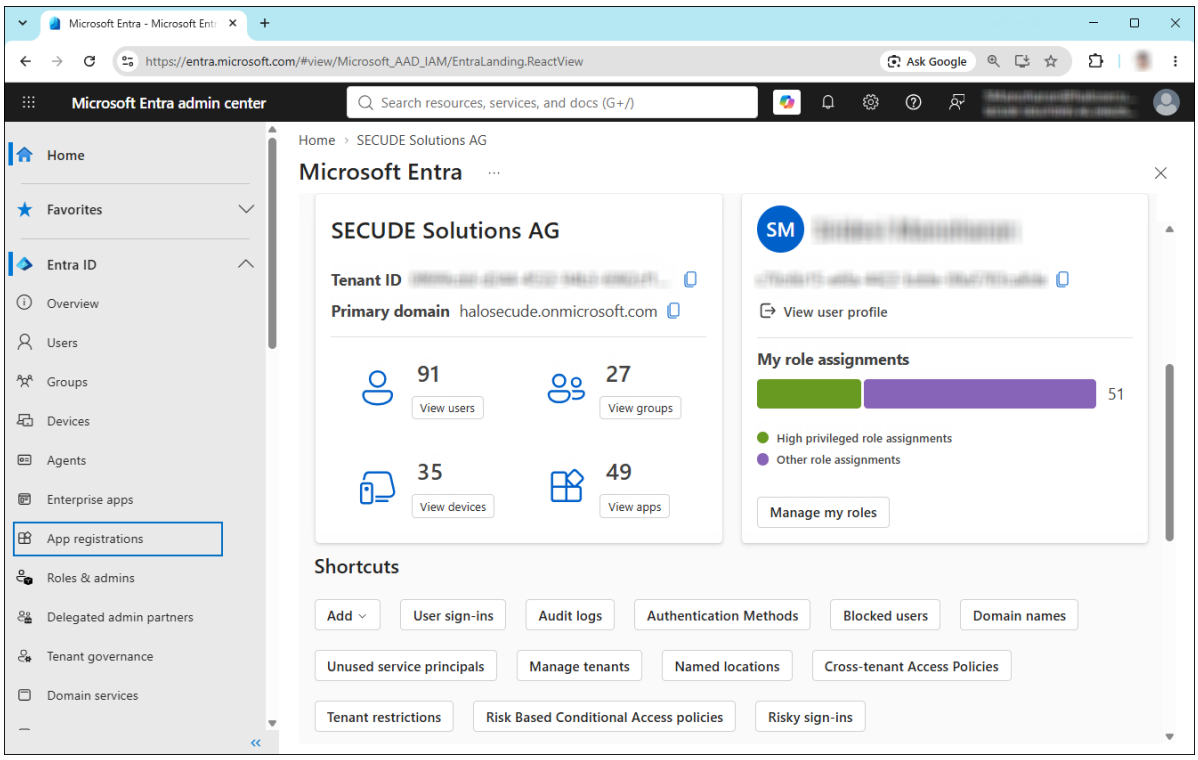
Microsoft documentation
Registering an application in Microsoft Entra ID establishes a trust connection between your application and the identity provider, the Microsoft identity platform. Microsoft documentation takes precedence over this section. Refer to the latest Microsoft documentation for updates.

Prerequisite: You must have sufficient administrative privileges to register an application in your Microsoft Entra ID tenant.

5.1.1.1. Create an Application

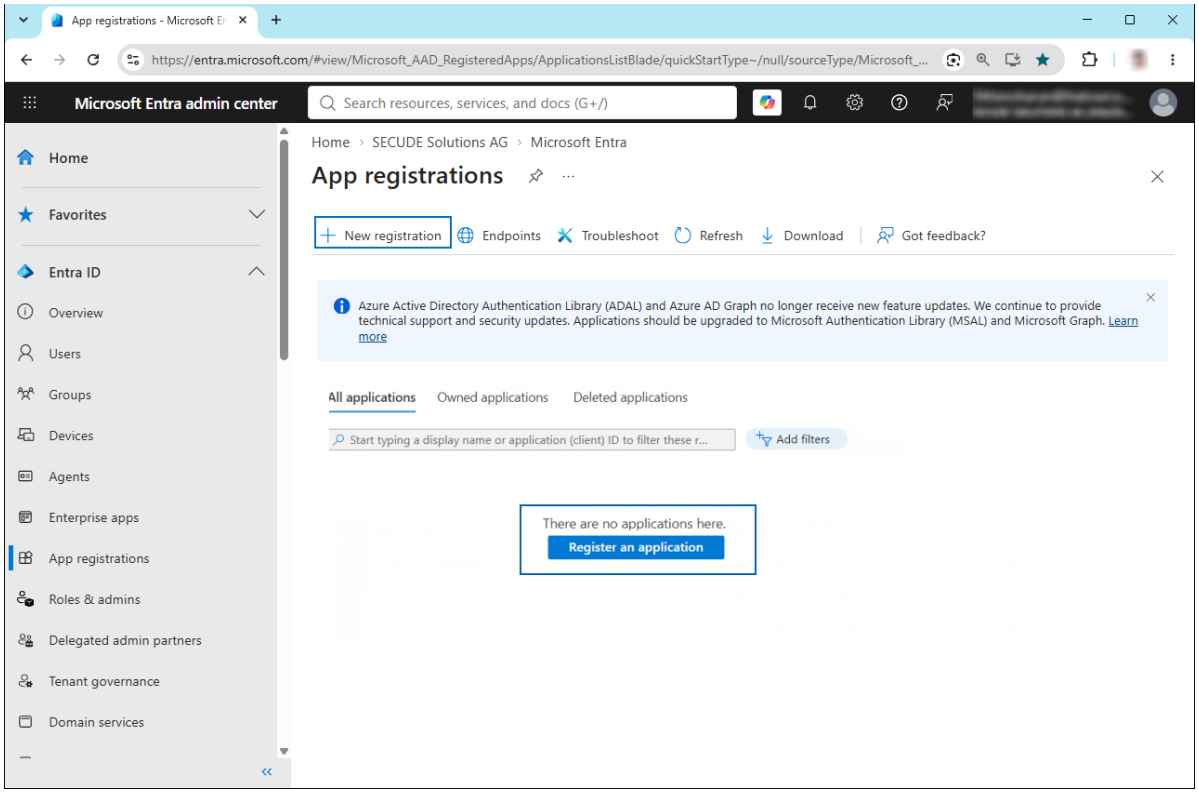
Follow these steps to register an application:

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. From **Directories + subscriptions**, select the tenant in which you want to register the application.
3. The application homepage opens.



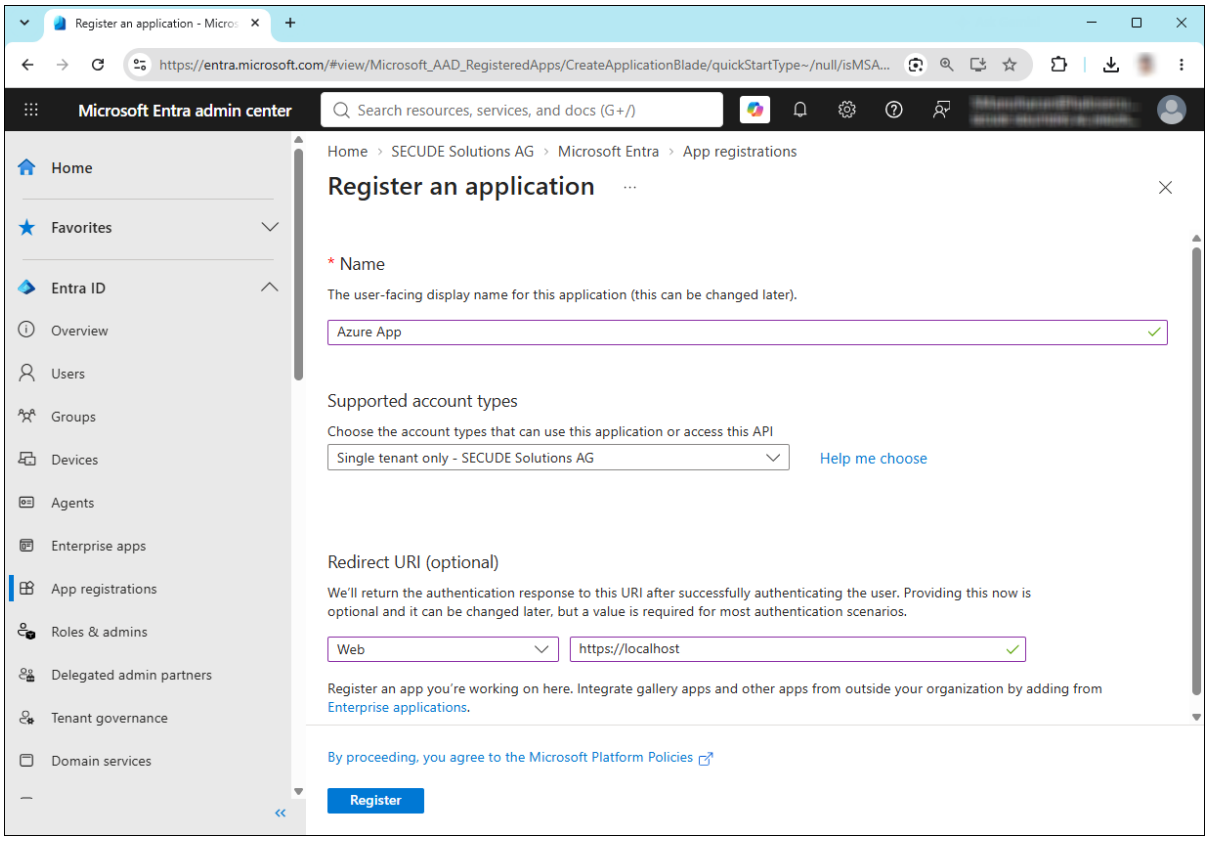
Selecting Microsoft Entra ID

4. In the left navigation pane, select **Entra ID** > **App registrations**.
5. On the **App registrations** page, click **New registration** or **Register an Application.** The **Register an Application** button appears only if no applications have already been created.



New application registration

6. On the **Register an application** page, configure the following:



Application details

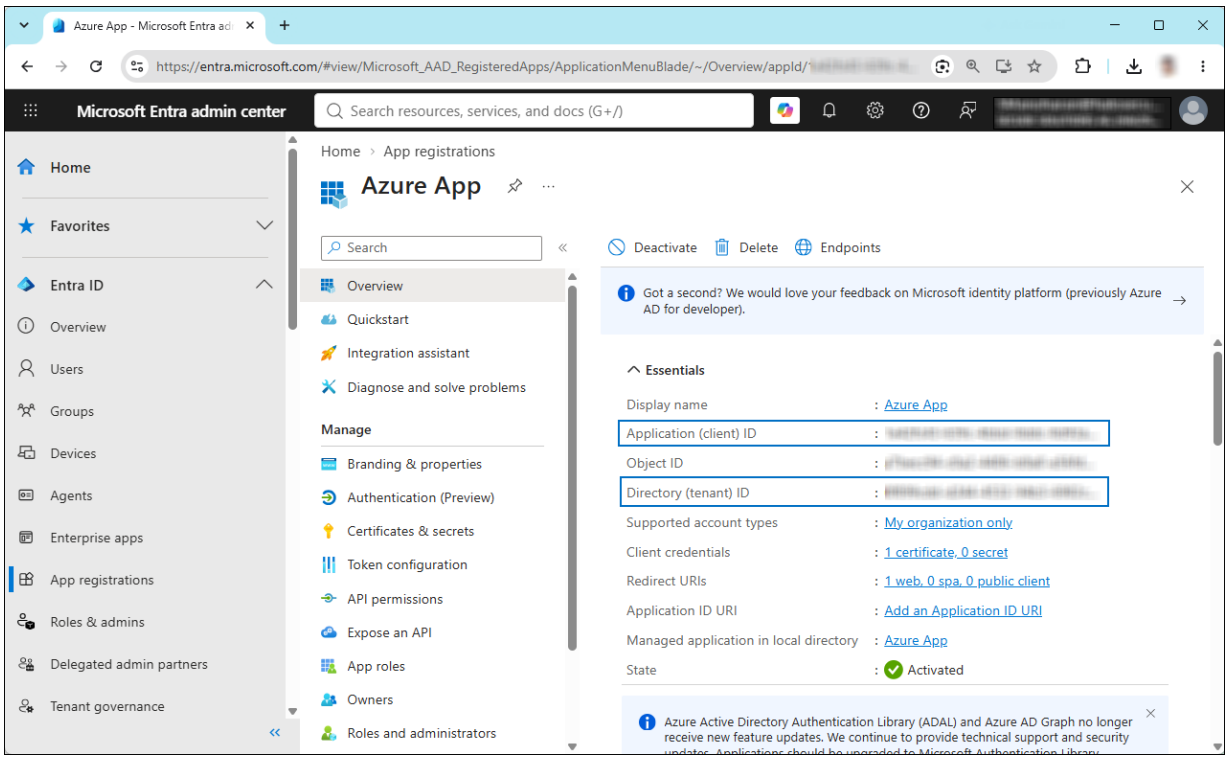
a. **Name:** Enter an appropriate name for the application.

b. **Supported account types:** Select **Single tenant only** from the list. HaloSHARE GenNXT currently supports only single-tenant applications.

c. **Redirect URI:** Select **Web** and enter a valid redirect URI. For example, `https://localhost`.

7. Click **Register**.

8. The Overview page of the newly registered application opens.



Application ID and Tenant ID

9. Once registration is complete, the portal displays the following values. 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

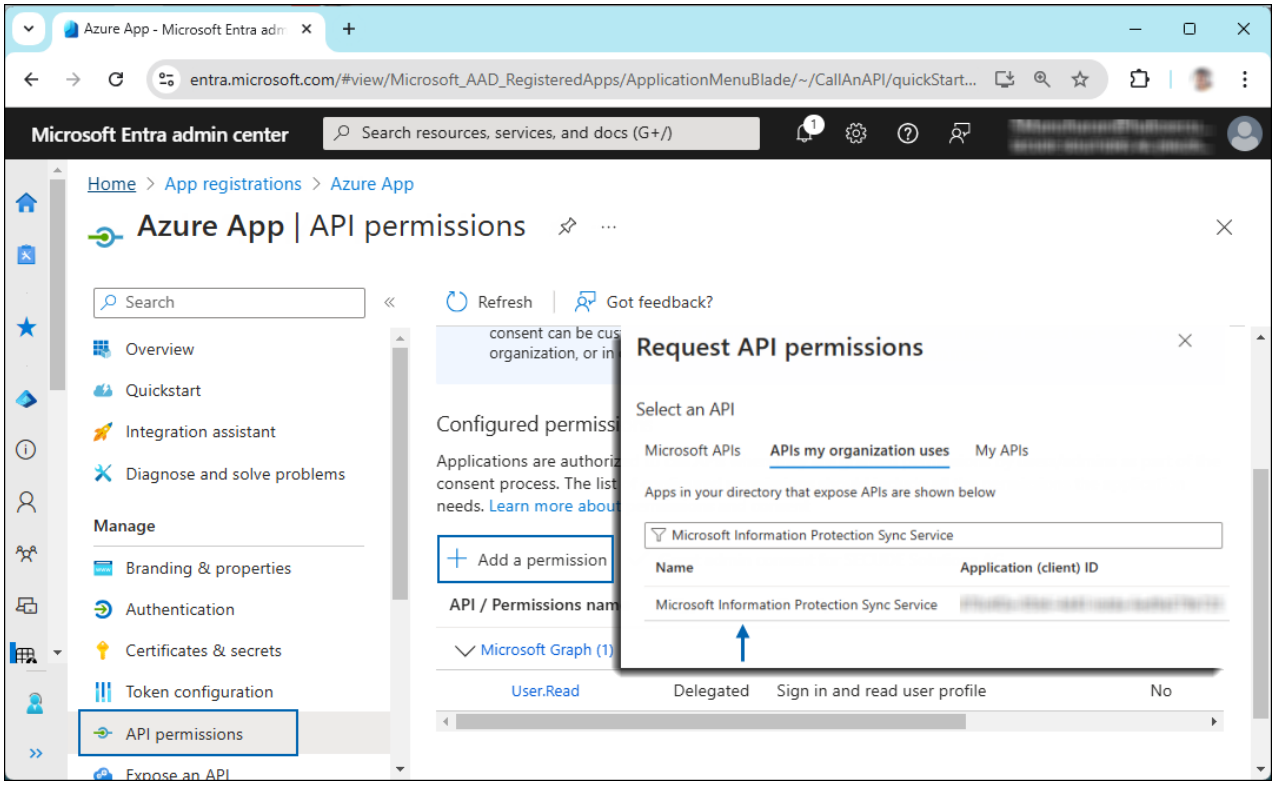
In a text editor (such as Notepad), copy the value of **Application (client) ID** and **Directory (tenant) ID**, and save it for initializing the HaloSHARE.

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.

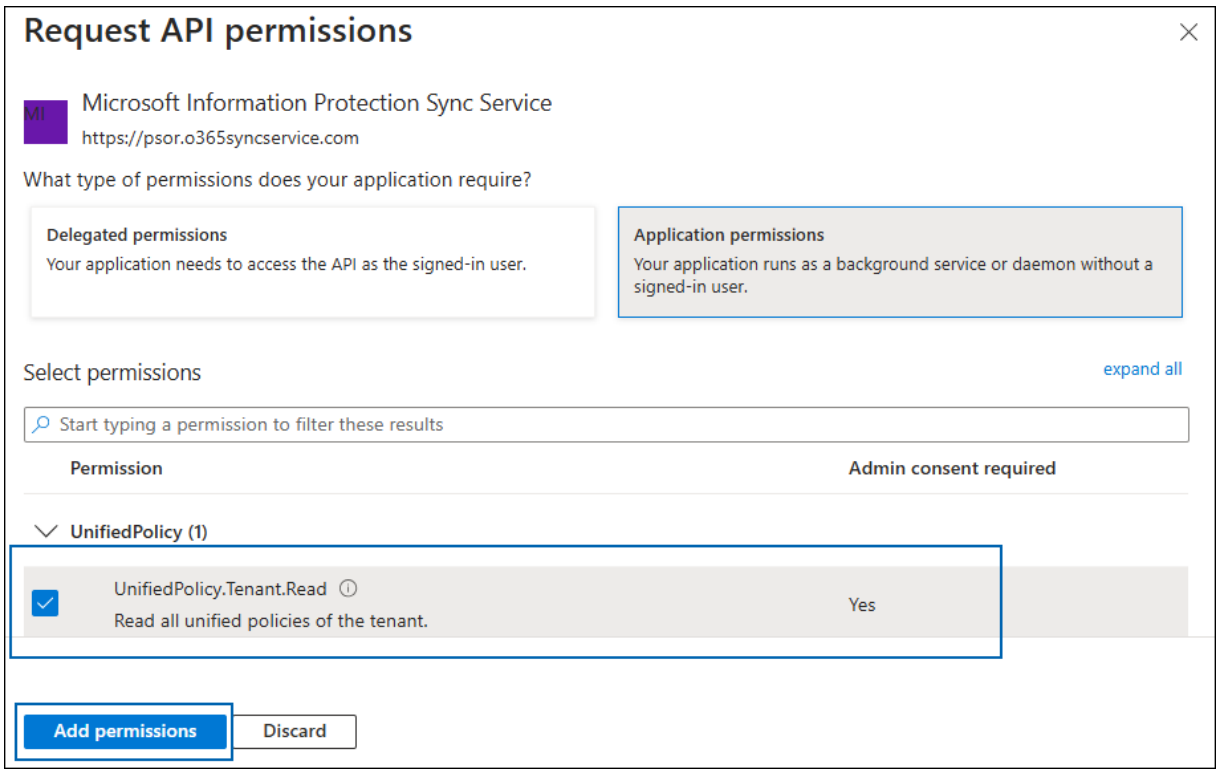
1. In the left navigation pane of the application, select **API permissions**.
2. Click **Add a permission**. The **Request API permissions** page appears.
3. Under the **Select an API** setting, select **APIs my organization uses**. A list appears containing the applications in your directory that expose 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:



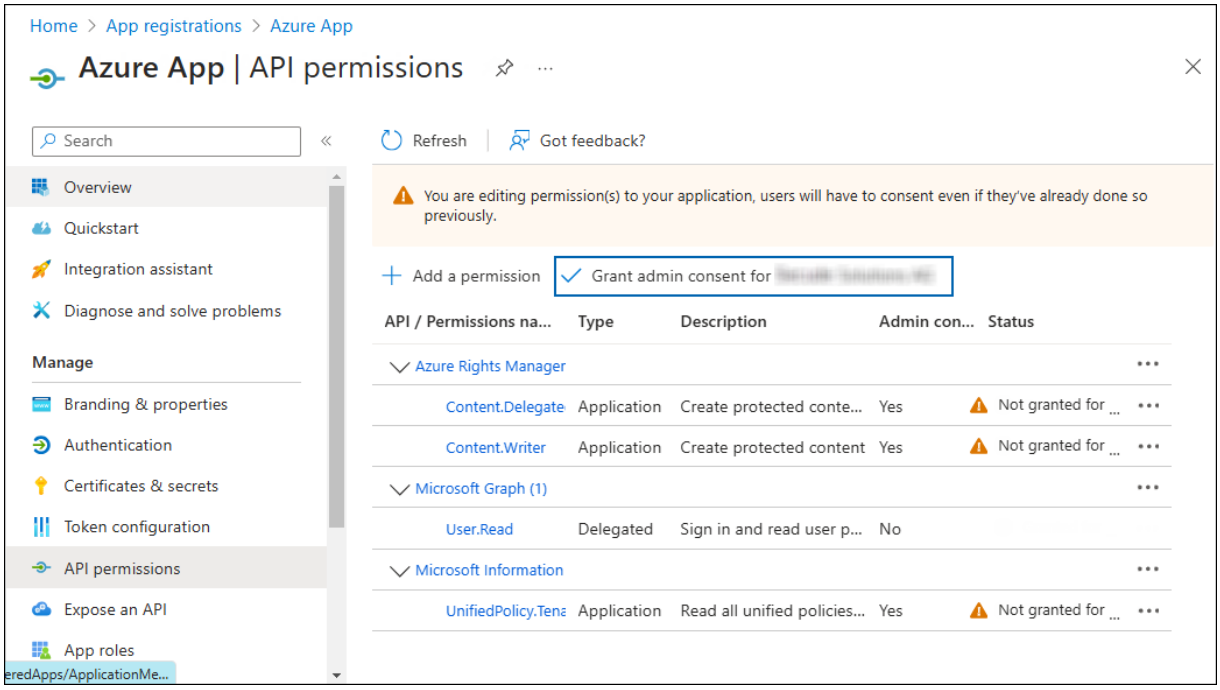
API selection

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** and then, under the **Permission** section, select the checkbox near **Read all unified policies of the tenant**.



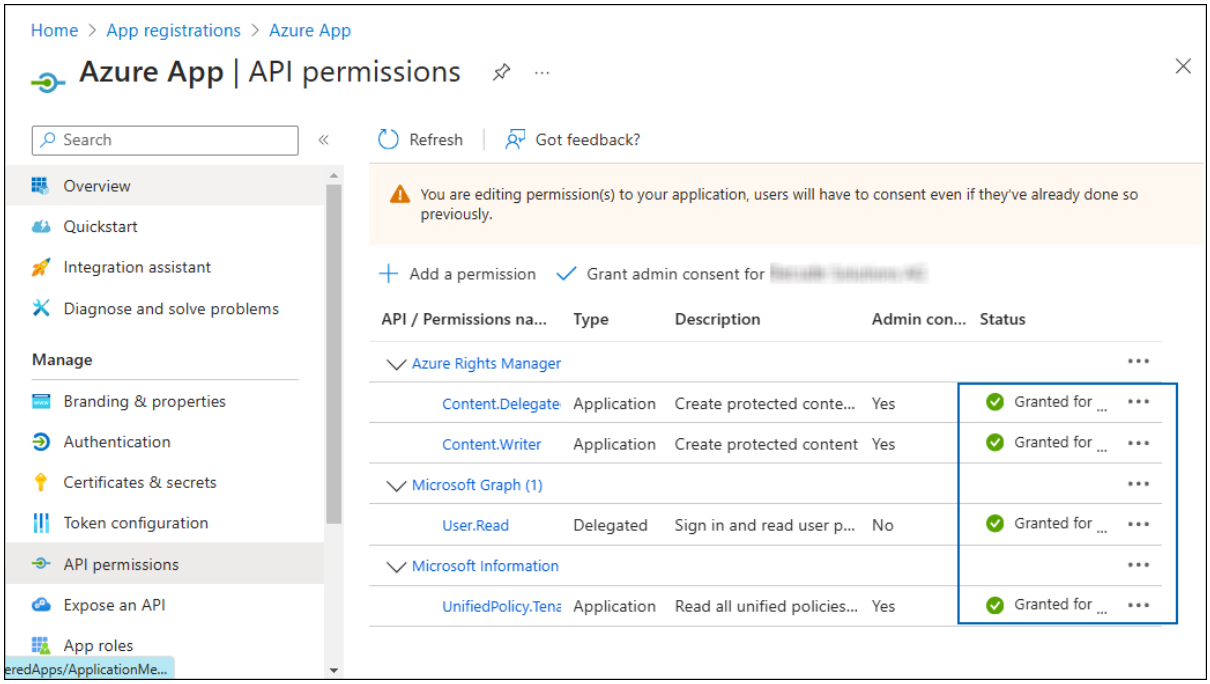
Adding permission

8. Click **Add permissions**.
9. Repeat the steps above to add the other required permissions listed in the “Required permissions” table below.
10. The **API permissions** page opens, and the added permissions appear in the table with the status **Not granted**.



Required API Permissions

11. Click **Grant admin consent for your company**. When prompted to confirm the consent request, click **Yes**.
12. After the admin consent is accepted, the status changes 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 in this tenant.

Required permissions #2

5.1.1.3. Upload the Certificate

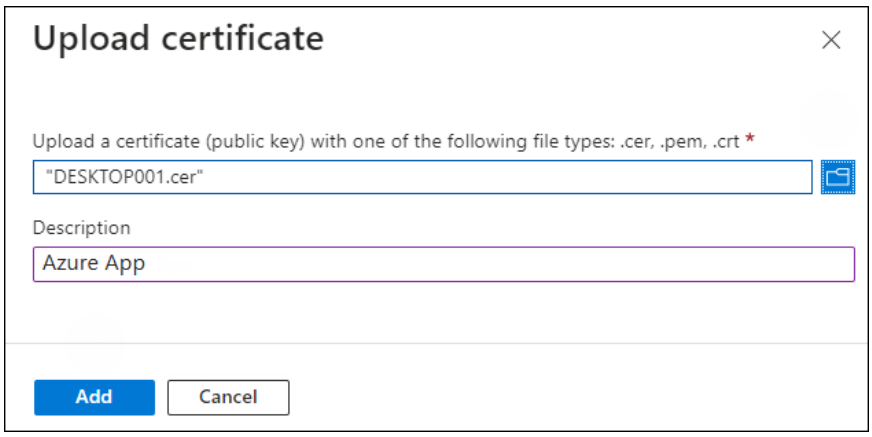
HaloSHARE uses certificate-based authentication, so you must enter your certificate information in the registered application.

Prerequisites:

1. **Certificate**:
   a. Ensure that you have a valid certificate containing the following key properties: `-KeyExportPolicy Exportable` and `-KeySpec Signature`.
   b. The certificate can also be self-signed. As a best practice, use a self-signed certificate only in a test environment.
2. **Install the certificate**:
   a. Ensure that this certificate is installed on the Windows Server machine where HaloSHARE is 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.

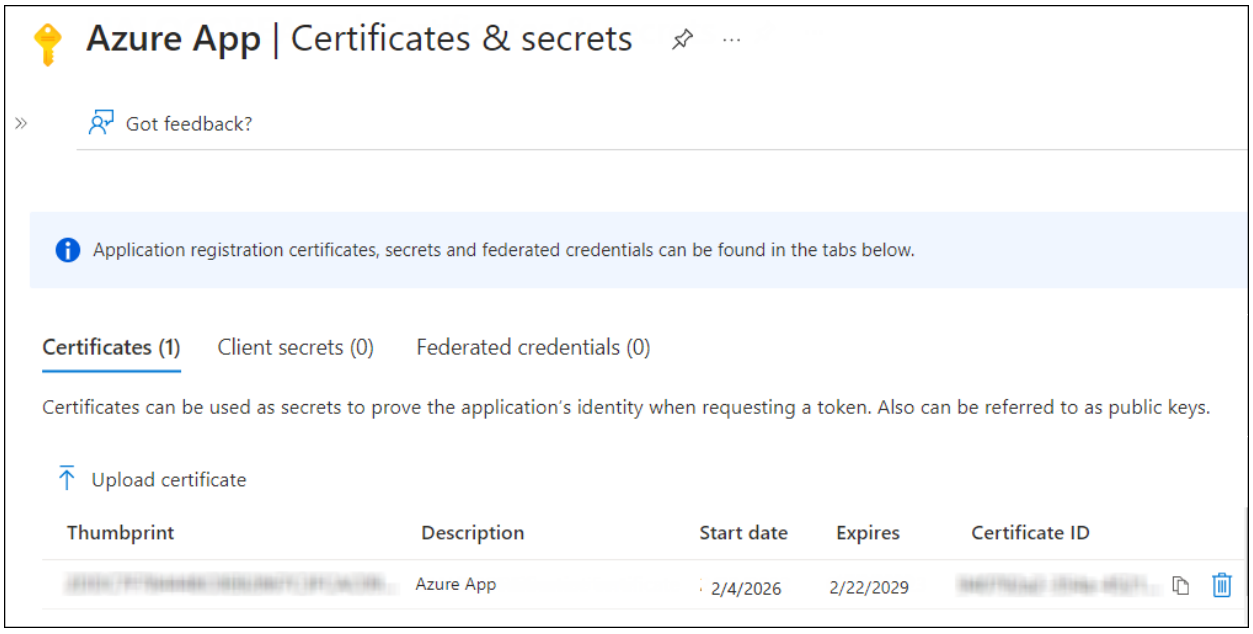
To upload the public key of the certificate, follow the steps below:

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 the folder icon to select the certificate, then click **Open**. For illustration purposes, the file `DESKTOP001.cer` is used.
4. Click **Add**. The certificate is uploaded, and its thumbprint appears on the page, as shown in the following figure:



Upload certificate #2

5. You are now ready to install HaloSHARE.

5.1.2. Create and Configure the Sensitivity Labels

As an administrator, create, configure, and publish sensitivity labels based on your organization's classification taxonomy. Use label names that are familiar to your users. If your organization does not already have a classification taxonomy, consider using labels such as Public, General, Confidential, and Highly Confidential. For more information, refer to the Microsoft documentation on configuring sensitivity labels.

5.1.3. Enable TLS 1.2 for Microsoft Entra ID Authentication

To improve tenant security and comply 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)

To authenticate with Microsoft Entra ID, TLS 1.2 must be enabled on the client workstation. For instructions, refer to the Microsoft documentation on enabling TLS 1.2 in the following link: Microsoft article to enable TLS 1.2.

Microsoft documentation

The Microsoft documentation takes precedence over the information in this section. Because Microsoft may update its guidance, always refer to the latest Microsoft documentation before making configuration changes.

Complete the following steps:

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

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

Registry entries

5.2. Register an application in Autodesk Platform Services

This section describes how to register an application in Autodesk Platform Services (APS), obtain the **Client ID** and **Client Secret**, and configure the required API access.

Prerequisites:

Before you begin, ensure that the following requirements are met:

- Allow the required Autodesk subscription licensing URLs and protocols through the firewall or proxy server.
- 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).
- Allow access to the required Certificate Authority (CA) endpoints (for example, `http://digicert.com`) over port 80 for Certificate Revocation List (CRL) validation.

To complete the configuration, you need:

- An Autodesk Platform Services (APS) account.
- An APS Developer Hub.

If you do not have an APS account, complete 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.

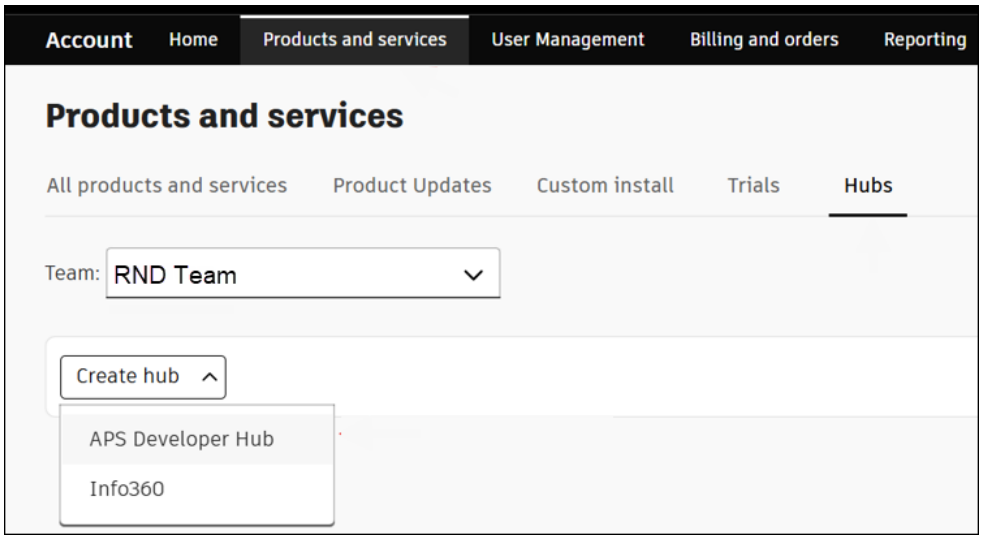
5.2.3. Create a Developer Hub

Prerequisites

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

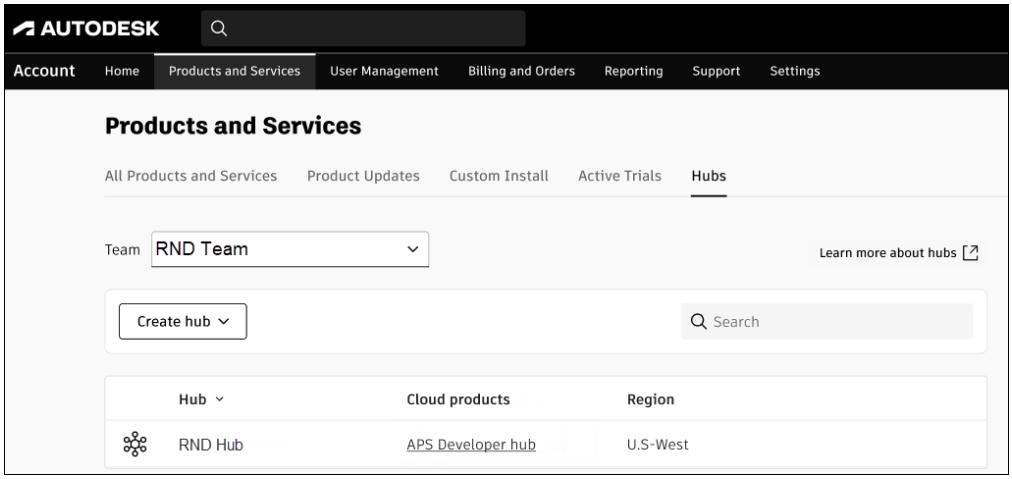
Procedure

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.

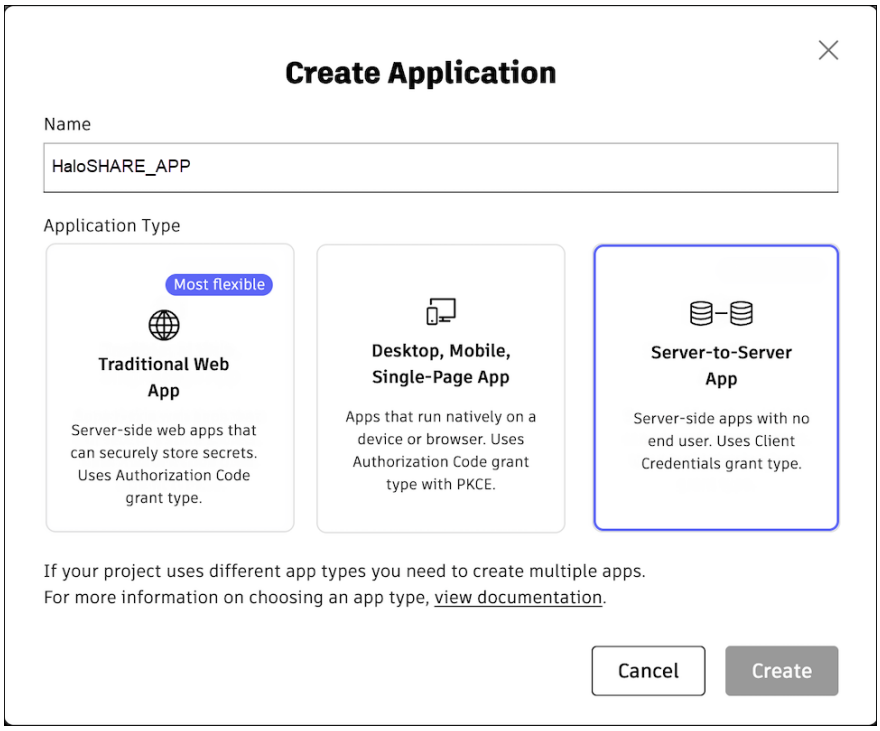


New hub

5.2.4. Create 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

Before configuring watermarking, ensure that the following prerequisites are met:

- Install a supported CAD application, such as **Autodesk Revit** or **AutoCAD**, on the server where HaloSHARE is installed. HaloSHARE installs the required watermarking components only when it detects a supported CAD application during installation.
- Ensure that the SharePoint folder is synchronized with the mapped local drive. Files configured as **Always keep on this device** (green check mark) are downloaded automatically and remain available locally.
- 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 exists, the error message *"Error 1069: The service did not start due to a logon failure*" appears while running HaloSHARE.
- **Revit only**: Install the **RevitLookup** tool to view custom properties (metadata) in Revit. After watermarking is applied, navigate to:
  RevitLookup > **Dashboard** > **Schemas** > **HaloMetadataInfo** > **GetElements** > **GetEntity (Schema)** > **Get()**.

5.4. File Signing Task

When configuring a file signing task, you can select either the **Local Computer** or **Current User** certificate store. Each option has the following requirements:

- 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

Before installing and running HaloSHARE, ensure that the following requirements are met:

- To install the service, you must have local administrator privileges.
- To run the service, you can use a user account with administrative privilege or non-administrative privilege.
- 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 GenNXT

This chapter describes how to install HaloSHARE GenNXT.

6.1. Interactive Installation

Install HaloSHARE GenNXT by using the GUI-based setup program included in the installation package.

Prerequisites

Before installing HaloSHARE GenNXT, ensure that the following prerequisites are met:

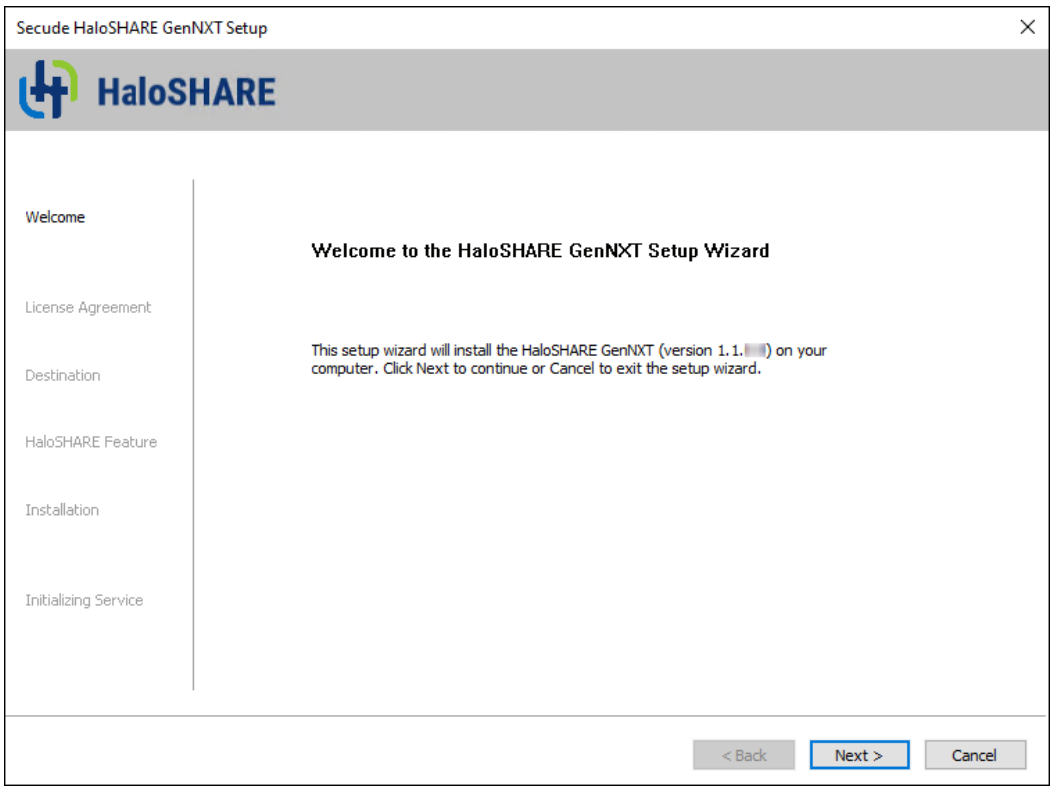
- The user performing the installation has administrator privileges.
- The **Application ID** and **Tenant ID** of the Microsoft Entra ID application are available.
- A certificate required for **MPIP authentication** is available. The certificate can be installed in either the **Current User** or **Local Computer** certificate store during installation. If the **Local Computer** store is used, ensure that the user account running HaloSHARE GenNXT has access to the certificate and its private key.

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 additional selections are required.

1. Double-click `HaloSHAREGenNXT_Setup.exe`. 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**.
2. The **Startup** dialog box appears, followed by the **Welcome** dialog box.

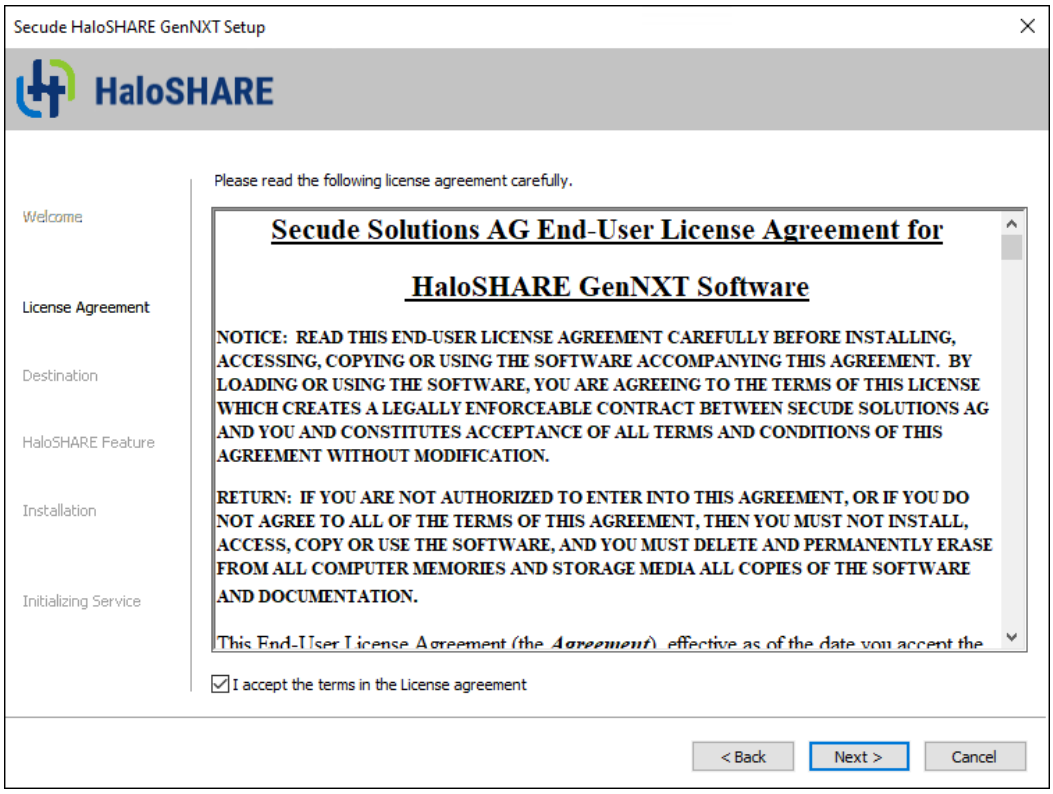


Startup dialog



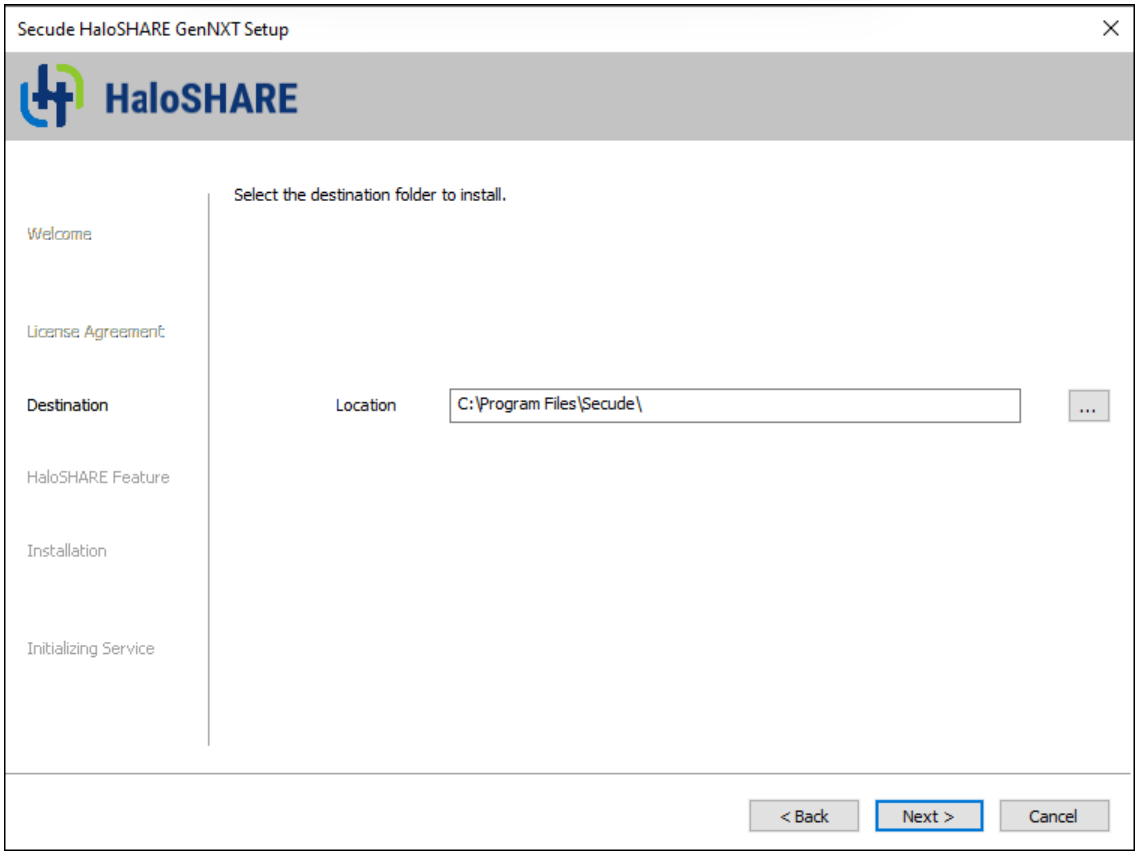
Welcome dialog

3. Click **Next** to continue the installation.
4. The **License Agreement** dialog appears.



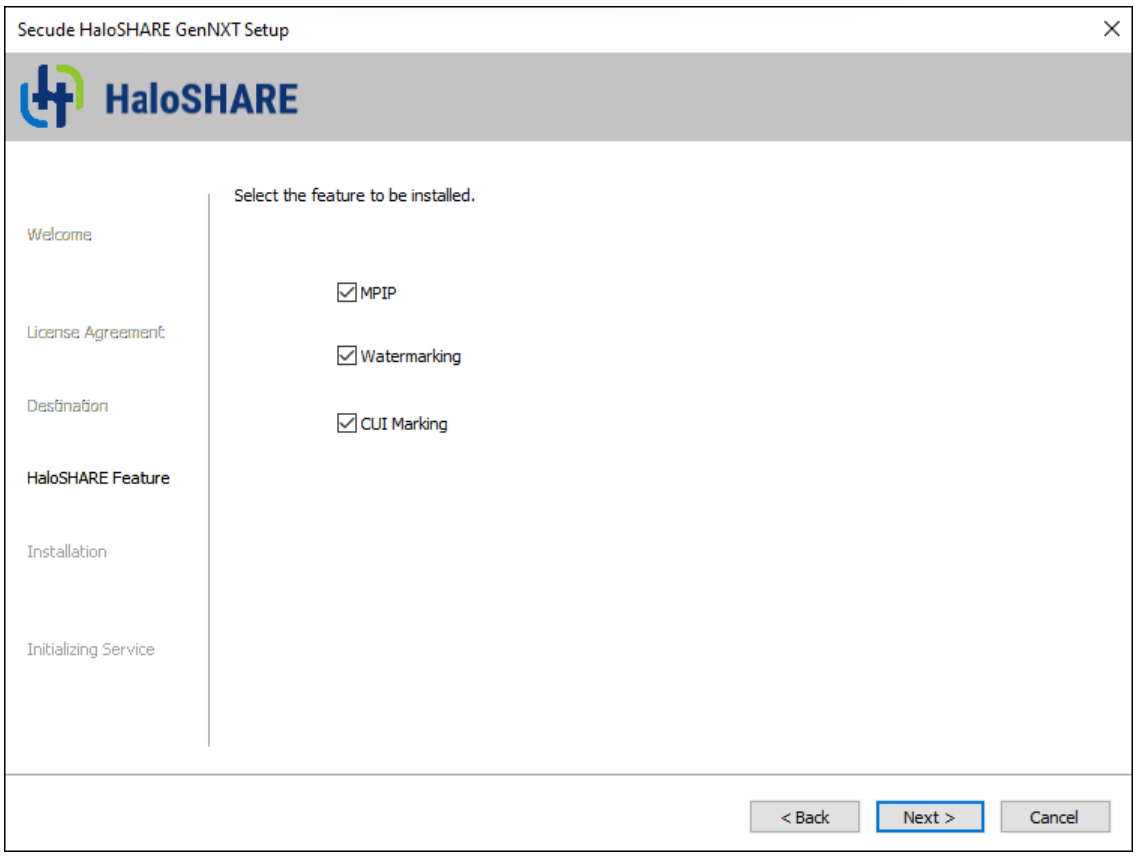
End-user License Agreement dialog

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** dialog appears.



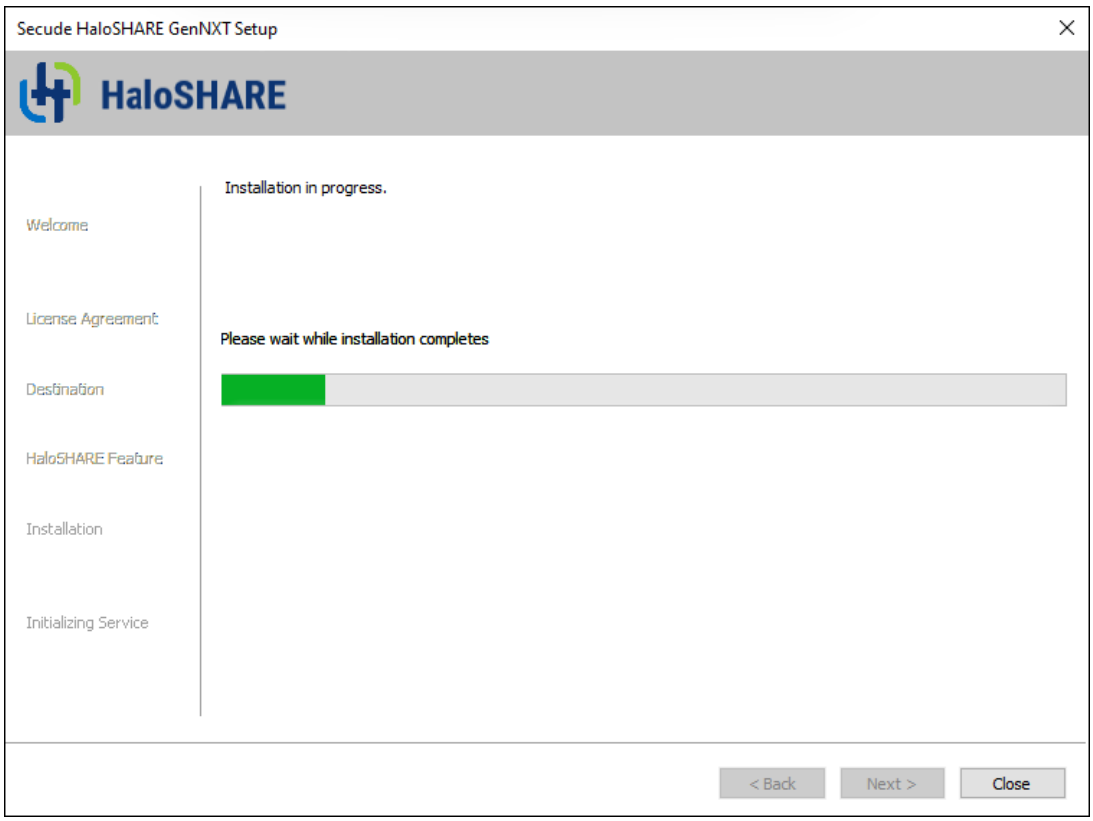
Destination folder selection dialog

7. By default, HaloSHARE GenNXT is installed in: `C:\Program Files\Secude\`. To install HaloSHARE GenNXT in a different location, click **Browse**, select the installation folder, and then click **Next**.
8. The **HaloSHARE Feature** selection dialog appears.



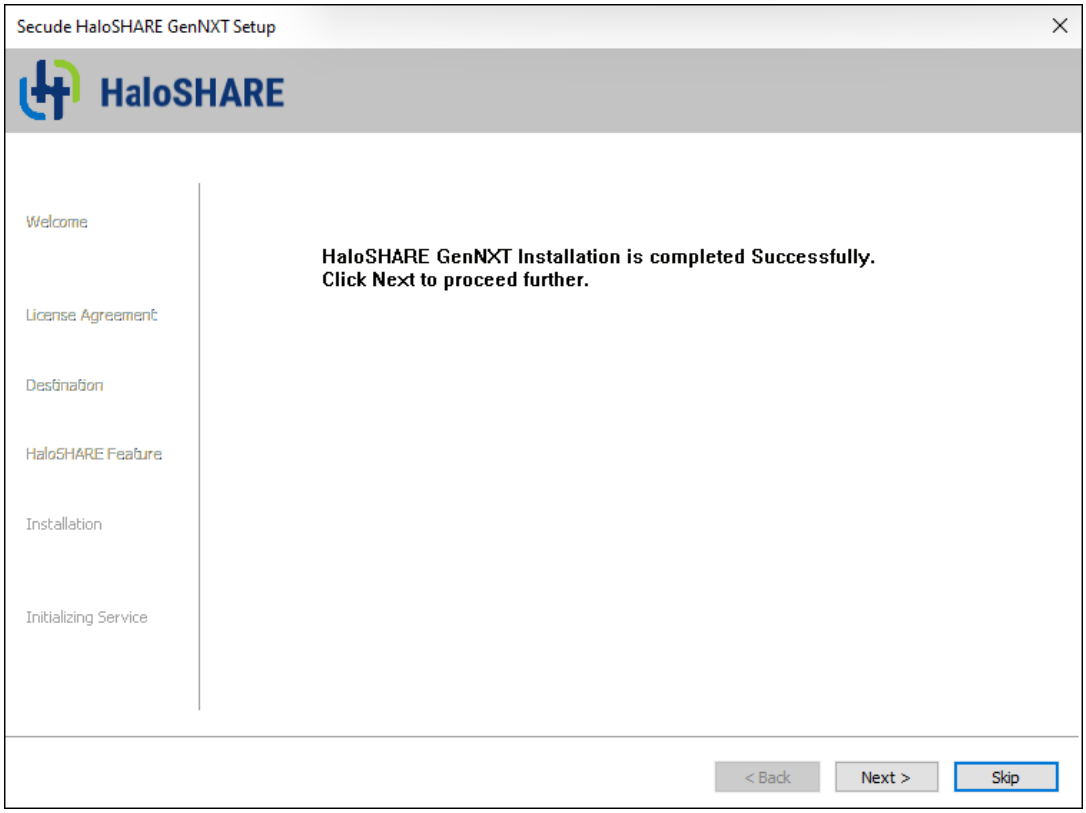
HaloSHARE GenNXT feature selection dialog

9. Select one or more installation features.
    a. **MPIP** – Installs Microsoft Purview Information Protection support.
    b. **Watermarking** – Installs watermarking support.
    c. **CUI Marking** – Installs Controlled Unclassified Information marking support.
    d. To modify the installation settings, click **Back**. Otherwise, click **Next**.
10. The installation begins, and the progress is displayed in the dialog.



Installation progress dialog

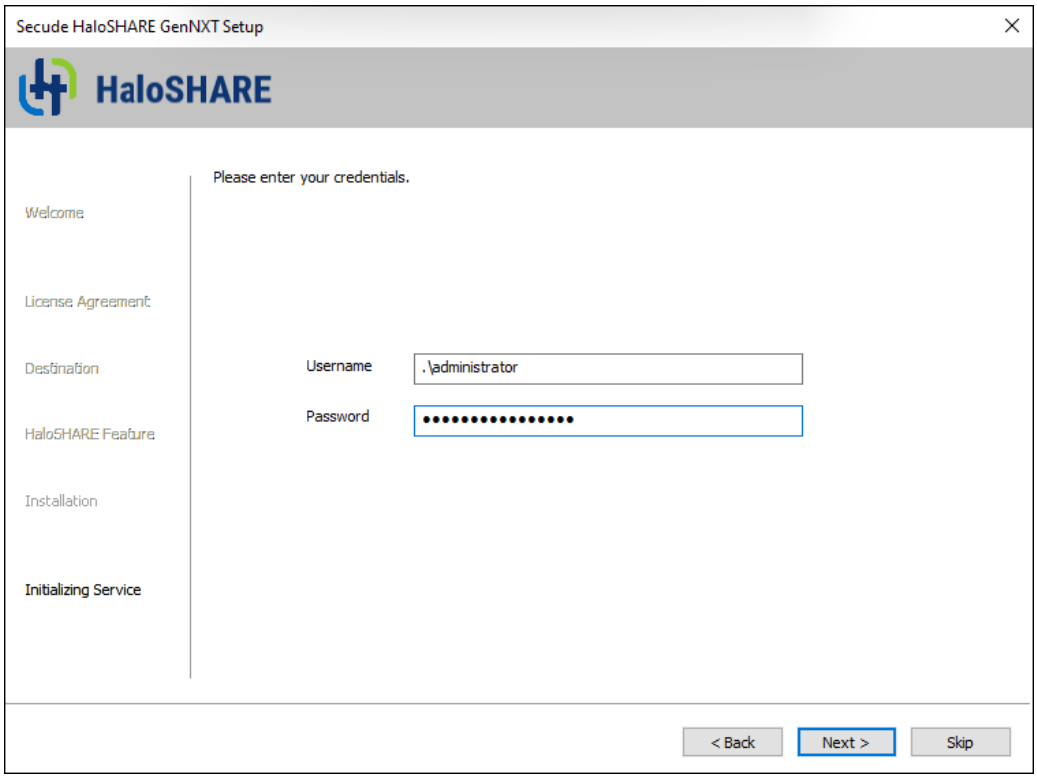
11. When the installation is complete, a confirmation message appears.



Installation completed dialog

12. Click **Next**.

13. The **Initializing Service** dialog appears.



User credential dialog

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

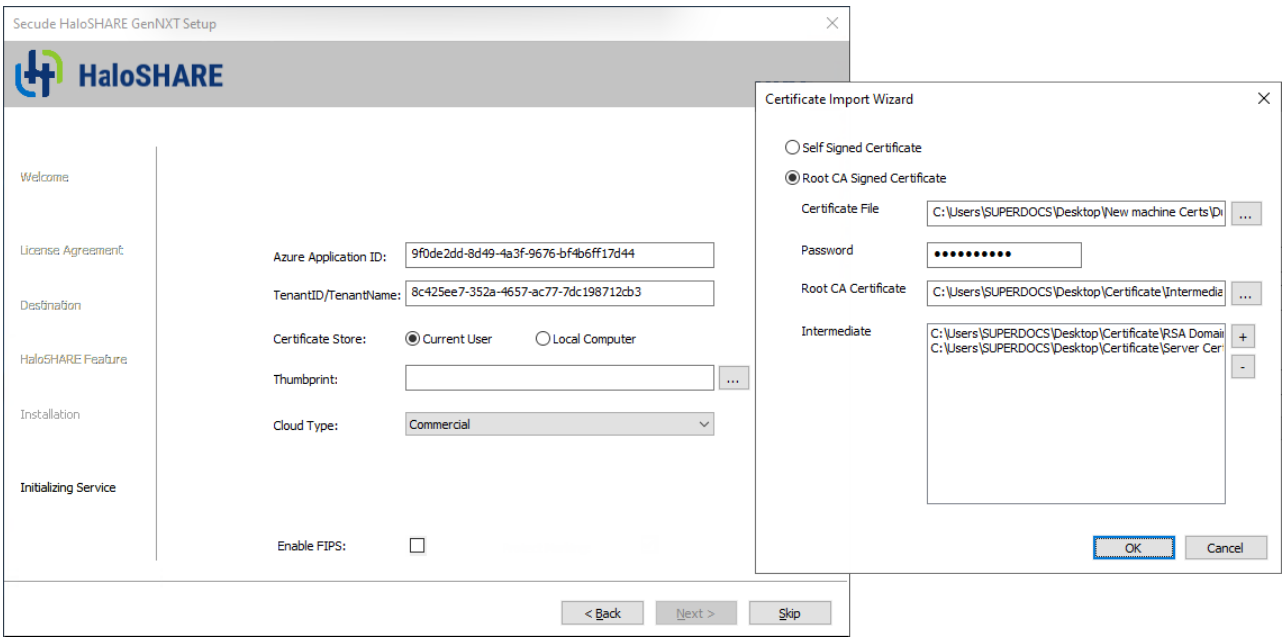
b. On a non-domain-joined computer, you need to enter the username and password of a user. For example, `.\[user]`, `.\john`. This format can also be used when a local user account is created on the computer.

14. Click **Next** to proceed.
15. If you selected **Watermarking**, **CUI Marking**, or both, proceed to Step 17.
16. If you selected **MPIP**, either alone or together with **Watermarking** or **CUI Marking**, the Certificate-based Authentication dialog box appears. To avoid errors, ensure that you enter the correct Azure application registration details in the installation wizard.

a. **Azure Application ID**: Enter the Application ID of the registered application in the Microsoft Entra admin center. 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, 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**.

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



Initialization completed dialog

18. 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 is stored at the following location: `C:\Users\Public\Secude\HaloSHARE`.

6.2. Update from Old to New Version

This section describes how to upgrade HaloSHARE GenNXT while preserving the existing configuration.

Prerequisite:

Before you begin, back up the `haloshare_config.enc` file from the HaloSHARE GenNXT installation directory. This file contains the HaloSHARE GenNXT configuration and is required to preserve your existing settings during the upgrade.

1. Uninstall the current version of HaloSHARE GenNXT.
2. Install the new version of HaloSHARE GenNXT.
3. Replace the `haloshare_config.enc` file in the HaloSHARE GenNXT installation directory. The default path is `C:\Program Files\Secude\HaloSHARE`.
4. Run `HaloSHAREConfiguration.exe` as an administrator.
5. Select the existing workflow.
6. Click **Save**.

This updates the existing configuration so that it is compatible with the current HaloSHARE GenNXT version.

> 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 the continued use of existing configuration files (supplier-based version) with workflow-based versions.

What to do next

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

7. Configuring the HaloSHARE GenNXT

This chapter describes how to configure HaloSHARE GenNXT by using the HaloSHARE GenNXT Configuration tool.

7.1. Administration

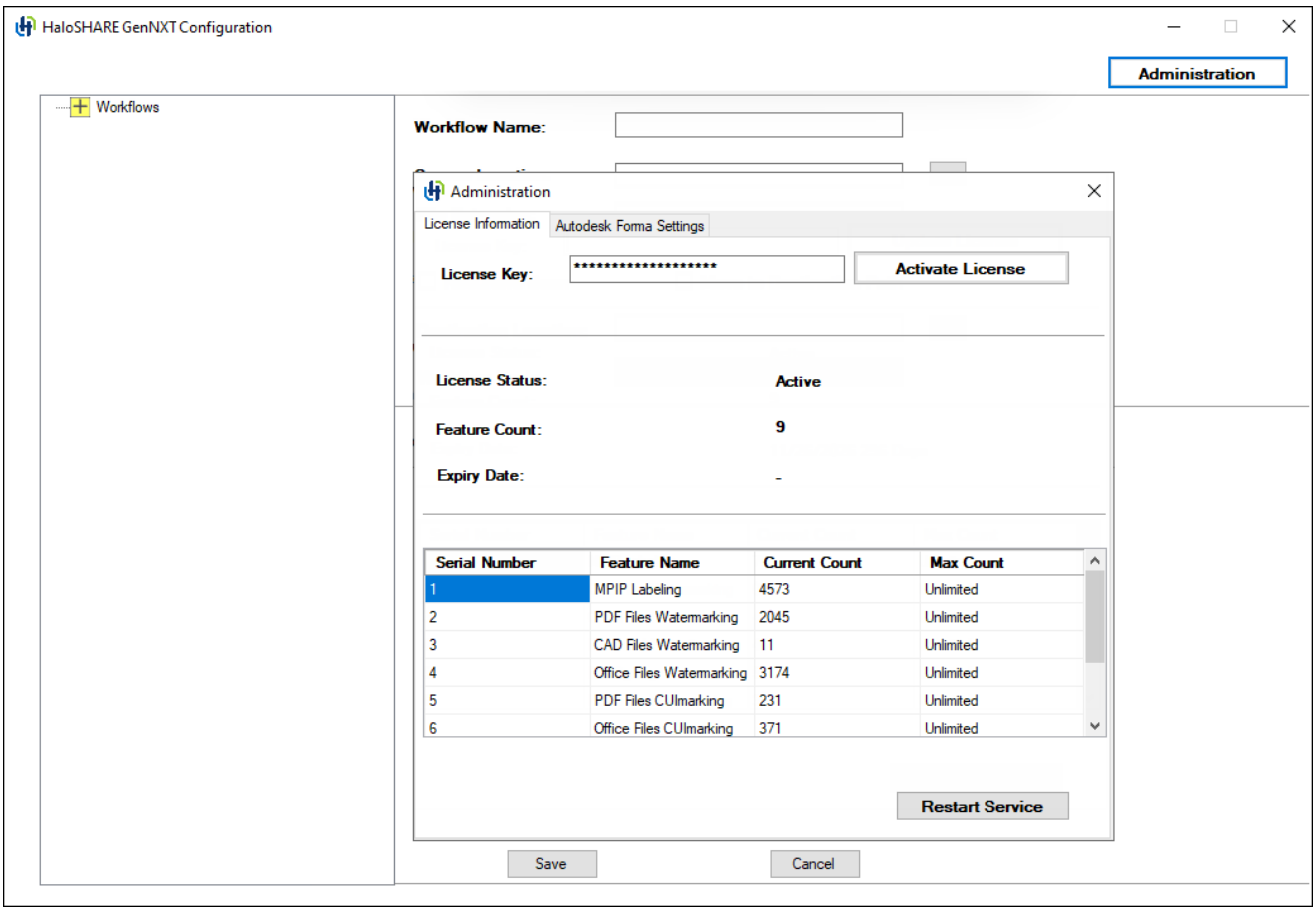
HaloSHARE GenNXT uses a key-based license to control application features. Obtain a license key from Secude Support before installing HaloSHARE GenNXT. After installation, enter the license key in the configuration tool to activate HaloSHARE GenNXT and enable all features.

> This manual does not describe the license purchasing process. To obtain or renew a license, contact your Secude representative.

License Activation

Perform the following steps to activate the HaloSHARE GenNXT license:

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 GenNXT Configuration** screen, click **Administration**.
4. The **Administration** screen appears.



License activation screen

5. Enter the license key.
6. Click **Activate License**.
7. Wait until the activation is complete.

Result:

- After the license is activated successfully, a confirmation message displays the license details, including **License Status**, **Feature Count**, and **Expiry Date**. Additional information is available in the **Feature Name**, **Current Count**, and **Max Count** fields.
- If the license key is invalid, **License Status** displays **LicenseNotFound**.
- If the license key is valid, **License Status** displays **Active**.

Related tasks:

- If your license expires, enter a new license key and click **Activate License**. Alternatively, activate the license by using `hsadm.exe`, and then restart the HaloSHARE service. For more information, refer to "Configure the Service by Using the Admin Tool".
- When HaloSHARE GenNXT is uninstalled, the license is automatically deactivated.
- License and service information is recorded in the log files located at: `C:\Users\UserName\AppData\Local\Secude\HaloSHARE\log`.

7.1.1. Autodesk Forma Settings

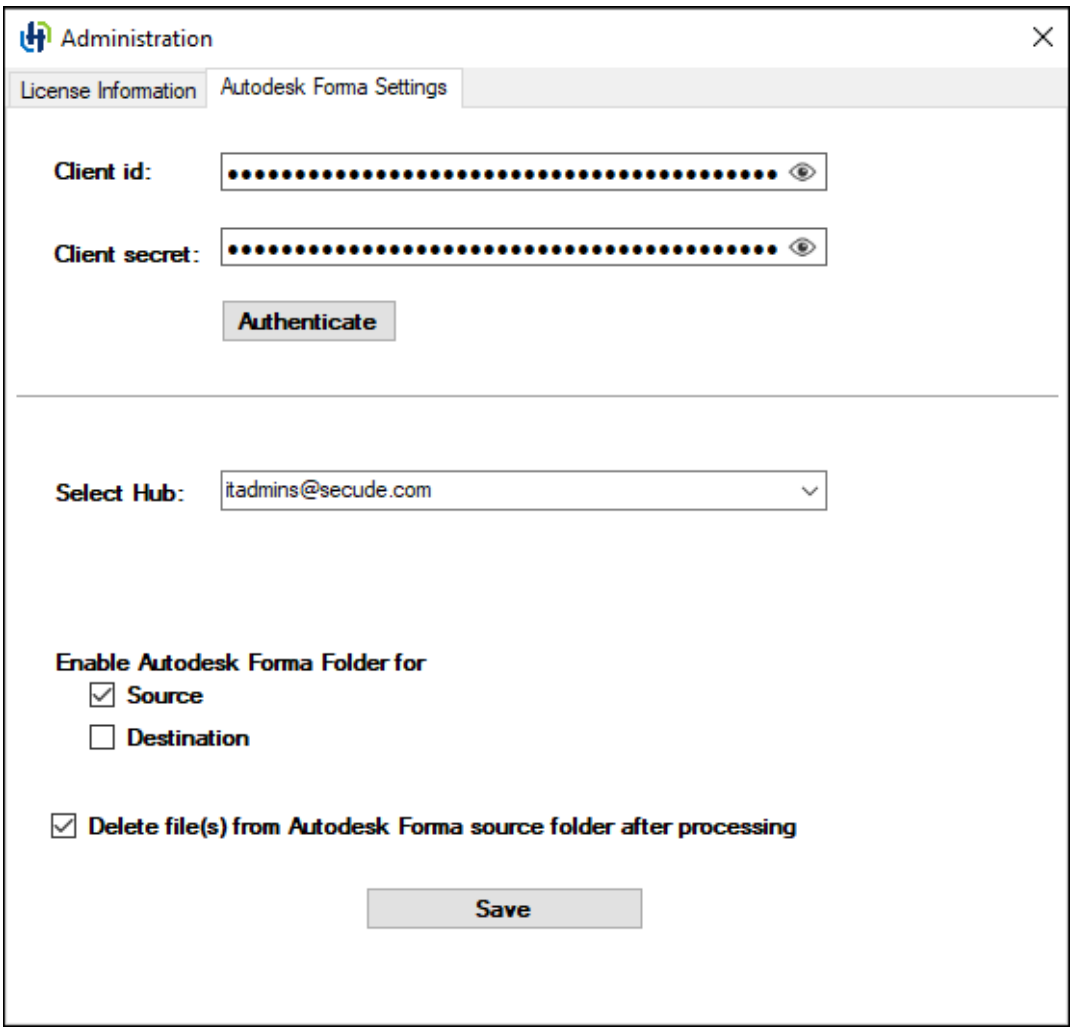
Autodesk Forma integration ensures seamless data flow and collaboration across platforms. HaloSHARE GenNXT enhances this ecosystem with MPIP protection, watermarking, CUI marking, digital signing, password protection, and metadata tagging to enable secure and efficient file sharing.

Before you begin, ensure that the following requirements are met:

- A valid license with the **Autodesk Forma** feature enabled. If the Autodesk Forma feature is not enabled in the license, the **Autodesk Forma** tab is disabled. When you select the tab, the following message appears: *"Autodesk Forma Settings are disabled. Please verify your license for more details."*
- The **Client ID** and **Client Secret** for your Autodesk Platform Services application.

To configure HaloSHARE GenNXT with Autodesk Forma, follow these steps:

1. In the **HaloSHARE GenNXT Configuration** screen, click **Administration**.
2. In the **Administration** window, click the **Autodesk Forma Settings** tab.
3. Enter the following credentials:
   a. Client id
   b. Client secret



Autodesk Forma Settings

4. To display the credentials, click the **Show/Hide** (eye) icon.
5. Click **Authenticate**. A confirmation message is displayed upon successful authentication.
6. From the Hub list, select the Autodesk Forma hub.
7. Configure the **Source** and **Destination** locations. Depending on your workflow, select one or both options.
    - If Autodesk Forma is selected, the folder selection dialog box displays Autodesk Forma folders.
    - Otherwise, the folder selection dialog box displays local or network folders.
8. To delete processed source files from configured source folder, select **Delete file(s) from Autodesk Forma source folder after processing**.
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 GenNXT processes files from a source location and transfers them to a destination location. Each workflow consists of one or more tasks that run sequentially when HaloSHARE GenNXT 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 protection to files.
- **File Signing Task** – Digitally signs files.
- **MPIP Task** – Applies Microsoft Purview Information Protection sensitivity labels to classify and protect files.

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 displays the associated workflow tasks and source locations. 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 external users, they configure a destination location such as `C:\SharePoint\PrestinEng_DestUser1`. The same approach can be used to configure additional workflows.

Workflow Behavior

1. File handling behavior occurs when the same file is repeatedly added or moved to the same source folder.

   Case 1: Move to Destination is not selected

   - **MPIP Task:** Suppose the source location is configured for text files (`.txt`). When you copy a text file, such as `sample.txt`, to the source folder, the file is encrypted and renamed to `sample.ptxt`.

     If the same fresh or unprocessed `sample.txt` file is copied to the source folder again, the existing `sample.ptxt` file is overwritten.

- **Watermark Task:** Suppose the source location is configured for PDF files (`.pdf`). When you copy a PDF file to the source folder, the file is watermarked.

  If the same fresh or unprocessed PDF file is copied to the source folder again, the existing processed file is overwritten.

Case 2: Move to Destination 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 fresh or unprocessed 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 with the same name.

- **Watermark Task:** When a file is placed in the source location, it is watermarked and moved to the destination folder.
  - If an already processed file is added to the source folder again, the existing file in the destination folder is replaced without processing the file again.
  - If a fresh or unprocessed file with the same name is added to the source folder, it is treated as a new file, watermarked, and moved to the destination folder, overwriting the existing file with the same name.

Note: The same behavior applies when a file is digitally signed, password-protected, CUI-marked, or metadata-tagged.
For PDF, Excel, and DOCX files, if processing fails because of a library error, the failed file is cached and is not processed again during subsequent HaloSHARE GenNXT operations.

2. The OneDrive and HaloSHARE services cannot access the same file simultaneously. Similarly, the HaloSHARE GenNXT and SharePoint services cannot access the same file at the same time. Simultaneous access results in an access violation or access denied error.
3. Unconfigured file types: Files that are not configured in the HaloSHARE GenNXT Configuration tool are not moved to the destination folder. HaloSHARE GenNXT identifies such unconfigured file types and leaves them unchanged.
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.

7. The source and destination paths can be swapped only within the same workflow. Configured paths cannot be swapped or used in another workflow.

File Processing in Forma

HaloSHARE GenNXT 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 GenNXT processes and tracks it. If a file (for example, V1) is already processed by HaloSHARE GenNXT and added again without changes, HaloSHARE GenNXT skips processing. Processed files are tagged with **Processed by HaloSHARE** to prevent duplicate processing.
- HaloSHARE GenNXT 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** option is selected in Autodesk Forma, files in the source folder remain unchanged, and the processed files are sent to the destination folder.
- HaloSHARE GenNXT 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 GenNXT 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 GenNXT-protected file is uploaded and relabeling is required, HaloSHARE GenNXT does not process the file if it has already been processed.
  To decrypt or relabel the file and process it again, either delete the tracking version file or 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

This section describes how to create and configure a HaloSHARE GenNXT workflow.

Prerequisite:

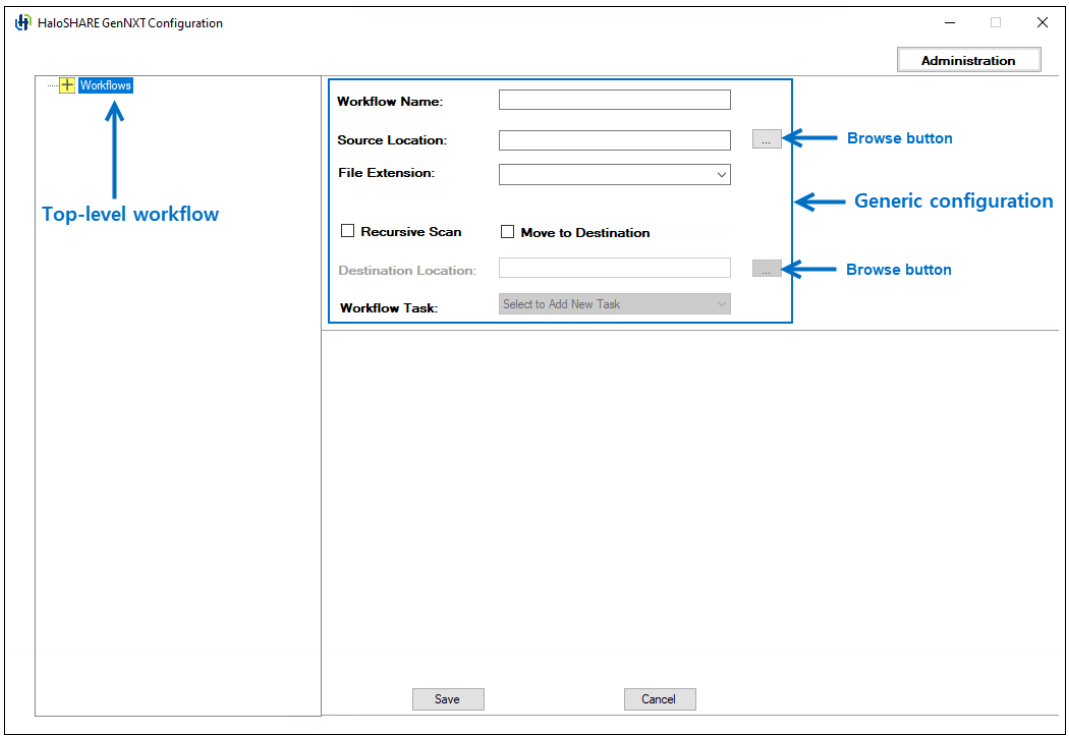
By default, the HaloSHARE GenNXT file extension is available for selection. To add additional extensions, update the `hs_extension_list.json` file. Newly added entries automatically appear in the extension list in the configuration tool.

Shared folder location

- The destination folder for external users can be located on Microsoft OneDrive, Microsoft SharePoint, or Autodesk Forma (formerly Autodesk Construction Cloud Docs), depending on your workflow configuration.
- When sharing files through Microsoft SharePoint or OneDrive, ensure that synchronization occurs through the respective client application (OneDrive sync app).
- If the user selects a source folder from OneDrive or SharePoint, ensure that the folder is synchronized successfully to the local drive and displays a green check mark (✅) before proceeding. This helps ensure that all workflow tasks are completed successfully.

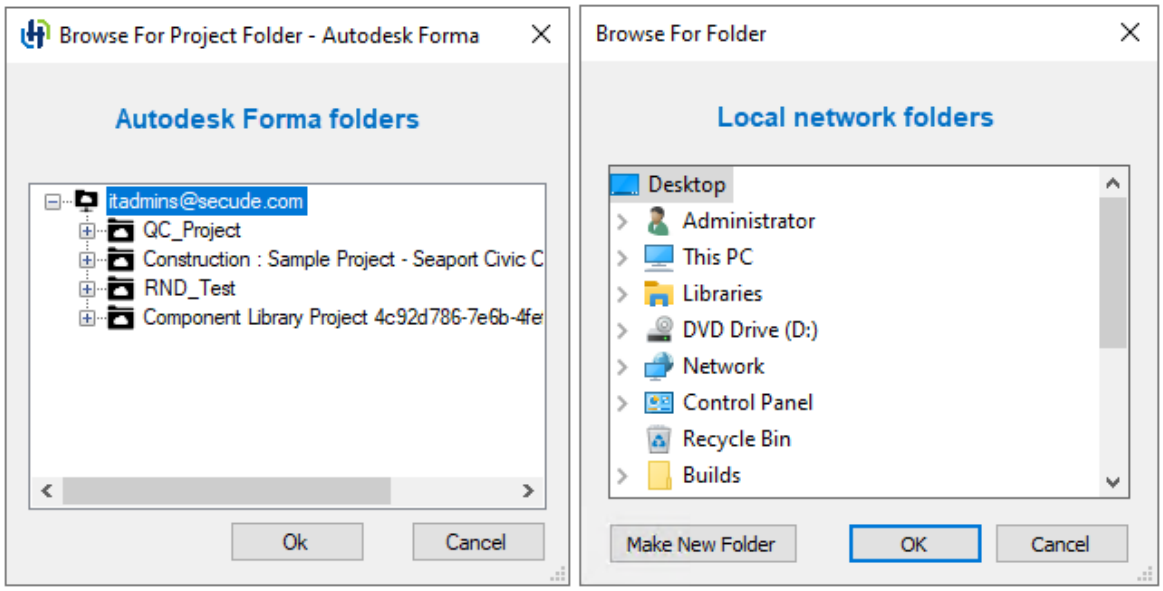
To configure the workflow, follow the steps below:

1. Navigate to the HaloSHARE GenNXT installation directory. The default folder is `C:\Program Files\Secude\HaloSHARE`.
2. Double-click `HaloSHAREConfiguration.exe`.
3. The **HaloSHARE GenNXT Configuration** screen appears.



Generic Workflow configuration fields

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



Folder dialogs

6. Select one or more file extensions from the **File Extensions** list. You can also search for a file type and then select it from the results. Files with extensions that are not configured are ignored.
7. To process files in all subfolders, select **Recursive Scan**. If this option is not selected, HaloSHARE GenNXT processes only files in the source folder.
8. To move processed files to another location, select **Move to Destination**.
9. In **Destination Location**, specify the destination folder where HaloSHARE GenNXT transfers the processed files. The destination folder can be a shared location, such as:
    - Microsoft SharePoint
    - Microsoft OneDrive
    - Autodesk Forma
    - Network folder

    Example: Files from `C:\PrestinEng\Source1` are moved to `C:\SharePoint\PrestinEng_DestUser1`.
10. Click **Save**.

Result:

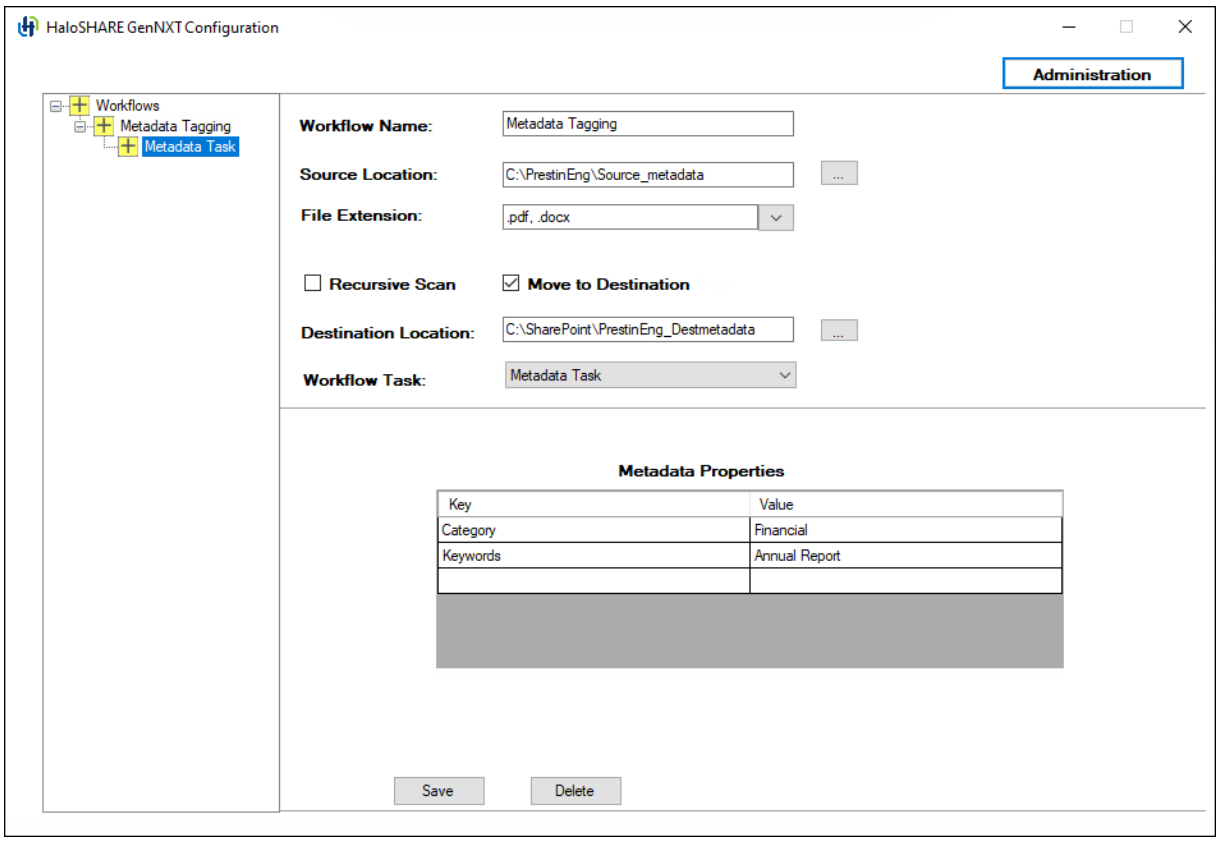
- After you successfully add the workflow, a confirmation message appears. The workflow name appears in the left pane under the top-level workflow. Select the workflow name to view its details in the right pane.
- The **Workflow Task** list is enabled after you save the workflow successfully. Note: To 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 GenNXT to add metadata to files for classification, identification, and ownership.

To configure the **Metadata Task**, perform the following 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 GenNXT Configuration** screen, the metadata task options appear.



Metadata Task configuration

4. Under **Metadata Properties**, enter the metadata values in the designated fields.

   Example:

   a. **Category**: Financial

   b. **Keywords**: Annual Report

5. To remove the metadata 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 configuration output, see the Sample Results section.

7.2.2. Configure Watermark Task Attributes

This task configures HaloSHARE GenNXT to apply watermarks to files to indicate ownership, classification, or usage restrictions.

Prerequisite: Before configuring the watermark workflow task for files in Microsoft Excel and PowerPoint, configure the settings below.

Configure the Watermark Display in Microsoft Office Applications

By default, HaloSHARE GenNXT applies watermarks in the foreground in Microsoft PowerPoint and in the center of worksheets in Microsoft Excel. In Microsoft Excel, users cannot edit cells covered by the watermark, although the watermark can be repositioned within the worksheet. In these display modes, the watermark may interfere with content editing. To allow users to edit content while the watermark is displayed, manually configure the appropriate registry value.

Application	Name	Type	Value
Microsoft PowerPoint	`enable_legacy`	`REG_SZ`	`true`
Microsoft Excel	`xl_wm_mode`	`REG_SZ`	`header` or `bkground`

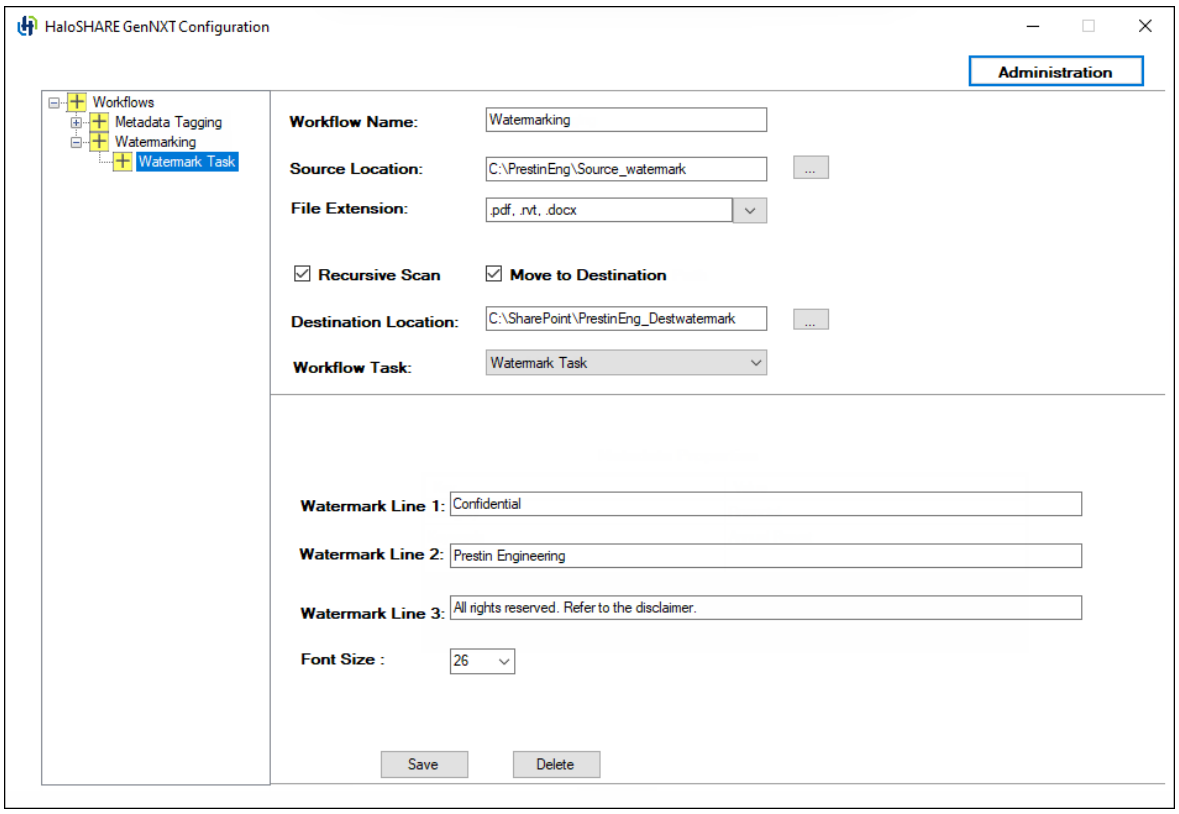
Registry keys

Registry Value Descriptions

- `true` (Microsoft PowerPoint) – Displays the watermark in the background, allowing users to add and edit content in the presentation.
- `header` (Microsoft Excel) – Displays the watermark in the worksheet header. The watermark is visible only in **Page Layout** view and on printed pages, while allowing users to edit worksheet content.
- `bkground` (Microsoft Excel) – Displays the watermark as the worksheet background. The watermark is visible throughout the worksheet while allowing users to edit worksheet content.

To configure the Watermark Task, perform the following 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 GenNXT Configuration** screen, the watermark-related UI field appears.



Watermark Task configuration

4. Enter the text to be embedded in the files. Enter text that matches 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**. HaloSHARE GenNXT uses the Times New Roman font for watermarking across all supported file types.
5. Click **Save.**
6. Restart the HaloSHARE service from 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. By default, the watermark is applied diagonally.
- For examples of configuration output, see the Sample Results section.
- 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 GenNXT

This feature enables HaloSHARE GenNXT to apply watermarks to Revit files without requiring the HaloCAD Add-on for Revit.

Prerequisites

Before you begin, ensure that the following requirements are met:

- AutoCAD and Revit are not running during the installation or uninstallation of HaloSHARE GenNXT.
- The **HaloCAD Add-on for Revit** and **HaloCAD Add-on for AutoCAD** are not installed on the watermarking server.
- HaloSHARE GenNXT is installed and running.
- Restart the HaloSHARE service before proceeding.
- Ensure that `hsmetadataMessageProcessor.exe` is running in the background. After a fresh installation, log off and log on again to start the process automatically, or start the process manually.
- Ensure that **Revit** and **AutoCAD** do not display any pop-ups or errors when started manually. Watermarking automation must not be interrupted by pop-ups or errors; otherwise, the application may become unresponsive.

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

1. Open **Task Manager**, and then select the **Details** tab.
2. Verify that `hsmetadataMessageProcessor.exe` is running.
3. If the process is not running, navigate to the HaloSHARE GenNXT installation path (`C:\Program Files\Secude\common\<version>`) and double-click `hsmetadataMessageProcessor.exe` to start it.
4. Configure a workflow to process Revit (`.rvt`) files by specifying the source and destination folders.

5. Copy the Revit file to the configured source folder.

Result

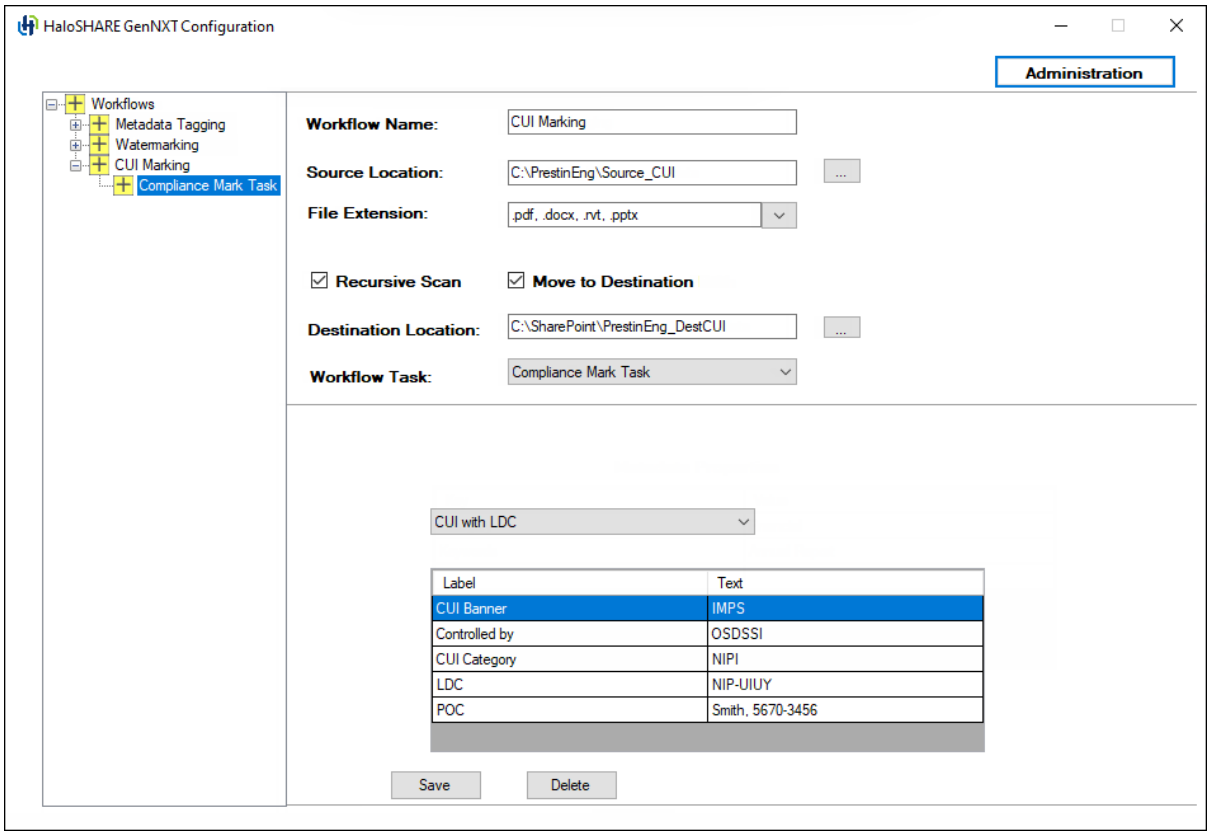
- HaloSHARE applies the configured watermark to the Revit file.
- The processed file is moved to the configured destination folder.
- To view the watermark text in Revit, refer to the section "Watermark in RevitLookup".

7.2.3. Configure Compliance Mark Task Attributes

This task configures HaloSHARE GenNXT to apply Controlled Unclassified Information markings to files.

To configure the CUI marking, follow these steps:

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 GenNXT Configuration** screen, the compliance marking options appear.



CUI with LDC configuration

4. Select one of the following compliance marking options:
   - **CUI with LDC** (Limited Dissemination Control)
   - **CUI with DS** (Distribution Statement)

5. Specify 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
6. To remove custom properties, select the row, right-click, and choose **Delete**.
7. Click **Save**.
8. Restart the HaloSHARE service from the **Administration** UI. Repeat these steps to add additional workflows.

Result:

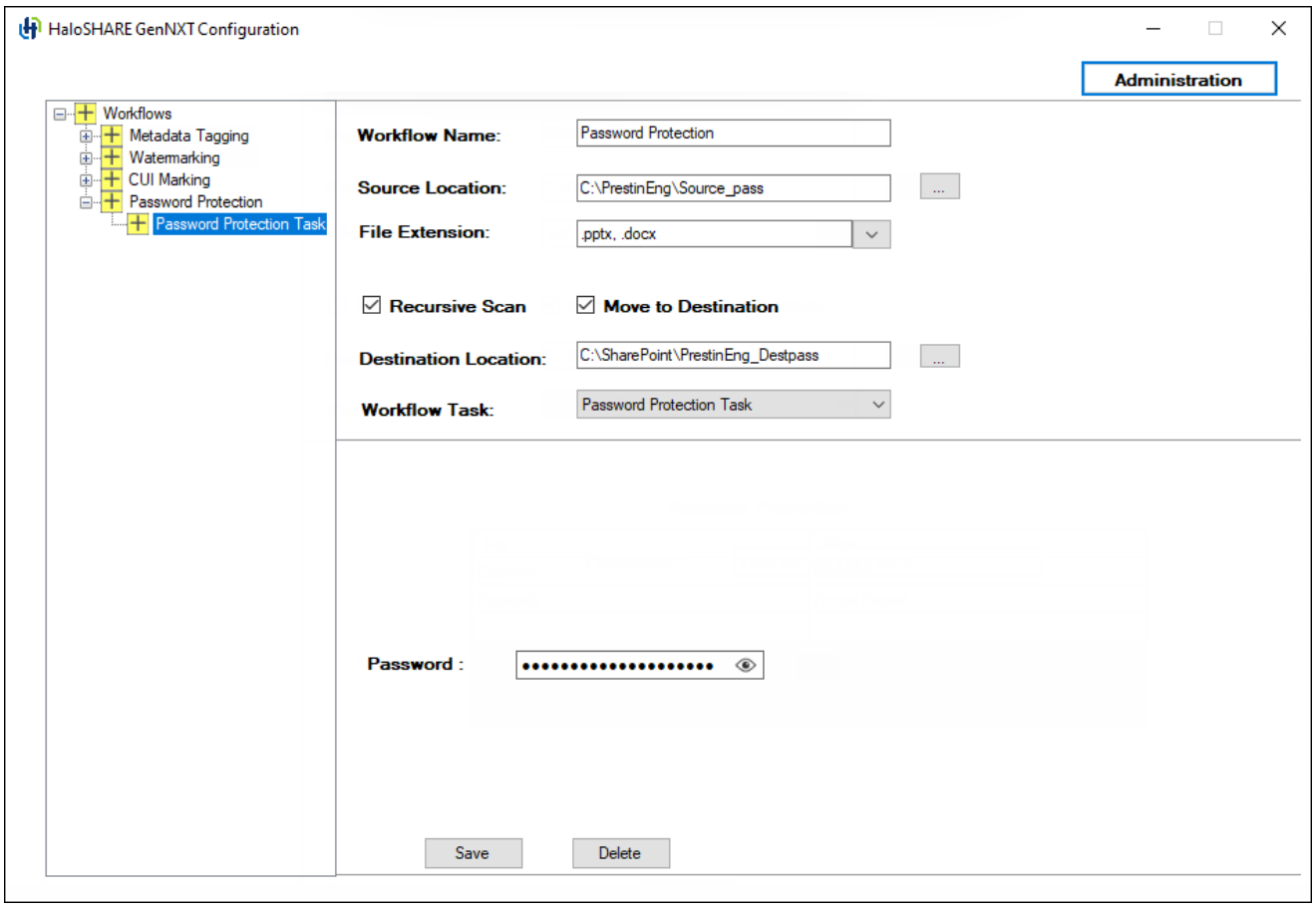
- After you successfully add the workflow, a confirmation message appears. The workflow name appears in the left pane under the top-level workflow. Select the workflow name to view its details in the right pane at any time.
- The first page of the document displays the CUI values as defined in the configuration.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

7.2.4. Configure Password Protection Task Attributes

This task configures HaloSHARE GenNXT to protect files using a user-defined password. HaloSHARE GenNXT applies only the password; all other behavior is determined by the native functionality of Microsoft Office and PDF 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 GenNXT Configuration** screen, the password protection field appears.



Password Protection Task configuration

4. Enter a password and keep a record of it, as it is required to edit the file later. 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.
5. To view the password, click the eye icon next to it.
6. Click **Save**.
7. Restart the HaloSHARE service from 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 configuration output, see the Sample Results section.
- 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

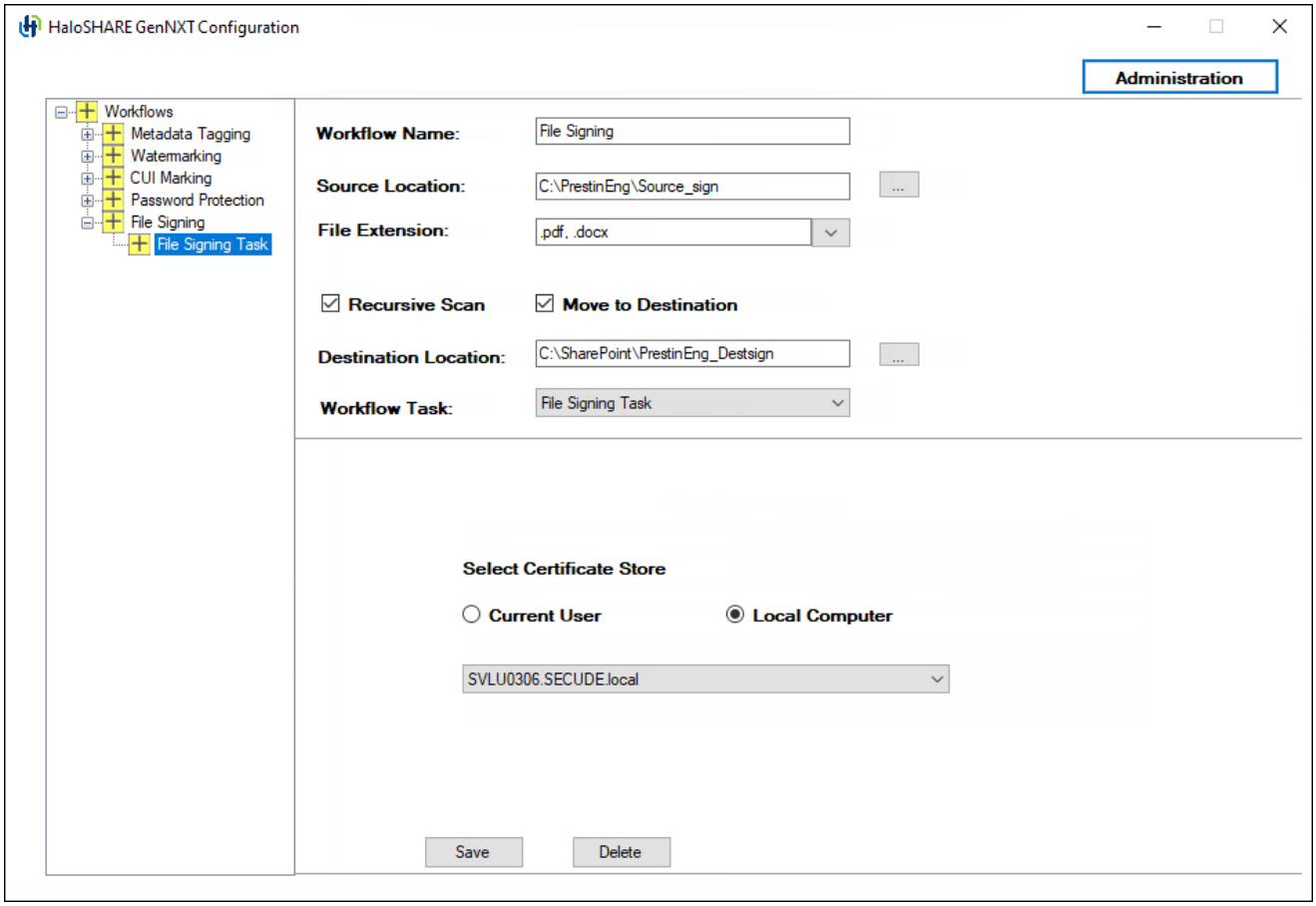
This task configures HaloSHARE GenNXT to automatically apply a digital signature to files in the background to help ensure file integrity and authenticity.

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 GenNXT 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**.
7. Restart the HaloSHARE service from 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 configuration output, see the Sample Results section.
- To delete a workflow, click **Delete**, and then confirm the action when prompted. The workflow is removed.

7.2.6. Configure MPIP Task Attributes

This task configures HaloSHARE GenNXT to protect files by applying **Microsoft Purview Information Protection** sensitivity labels or **custom permissions**. Files protected with sensitivity labels can be relabeled by using custom permissions. Likewise, files protected 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

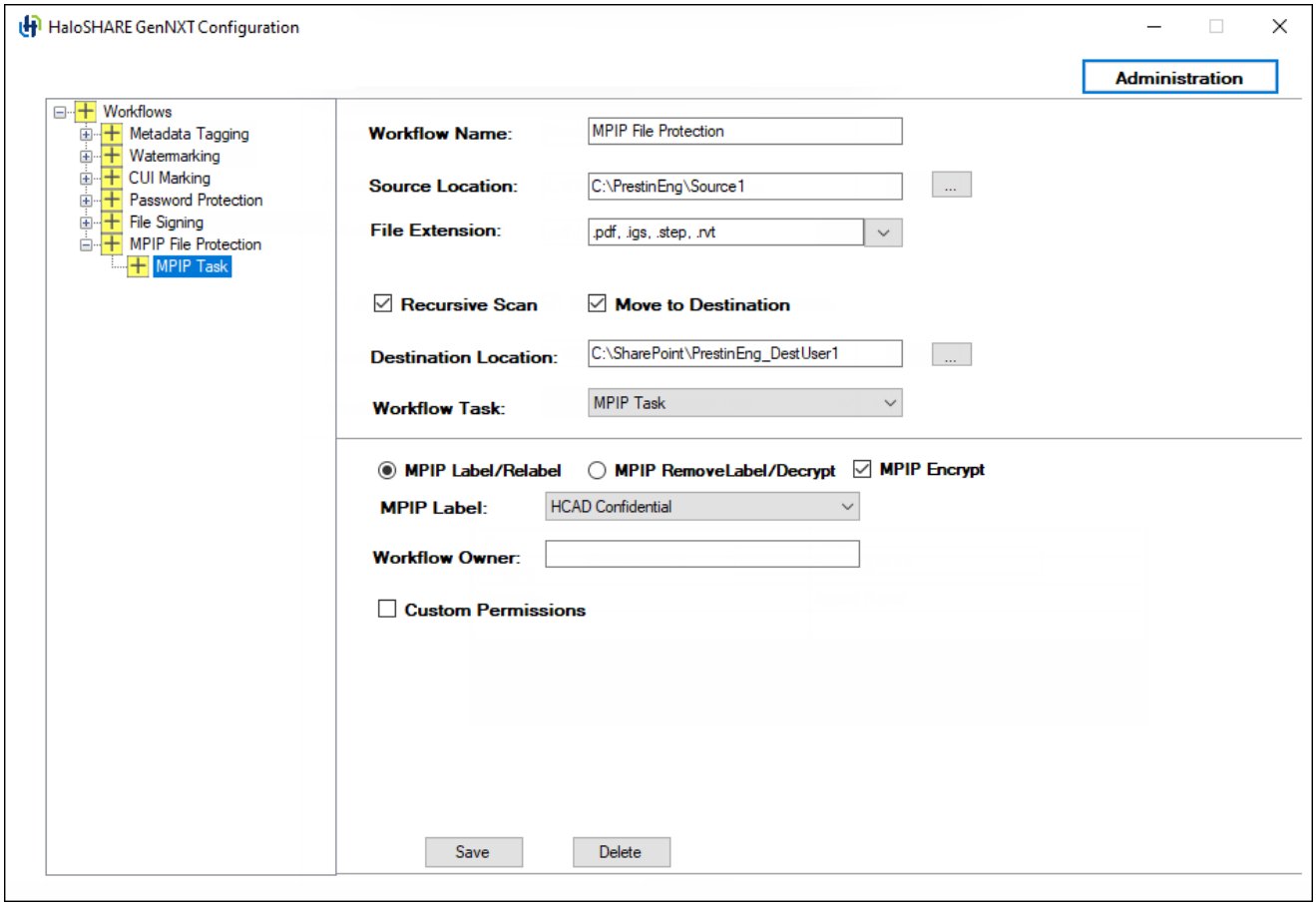
Sensitivity labels are defined and managed by administrators in the Microsoft Entra admin center. Each sensitivity label includes a predefined set of permissions and is referred to as an **administrator-defined permission**.

Custom Permissions

Custom permissions allow users to define permission settings when applying protection to a file. These permissions are referred to as **user-defined permissions**.

To apply file protection, follow these steps:

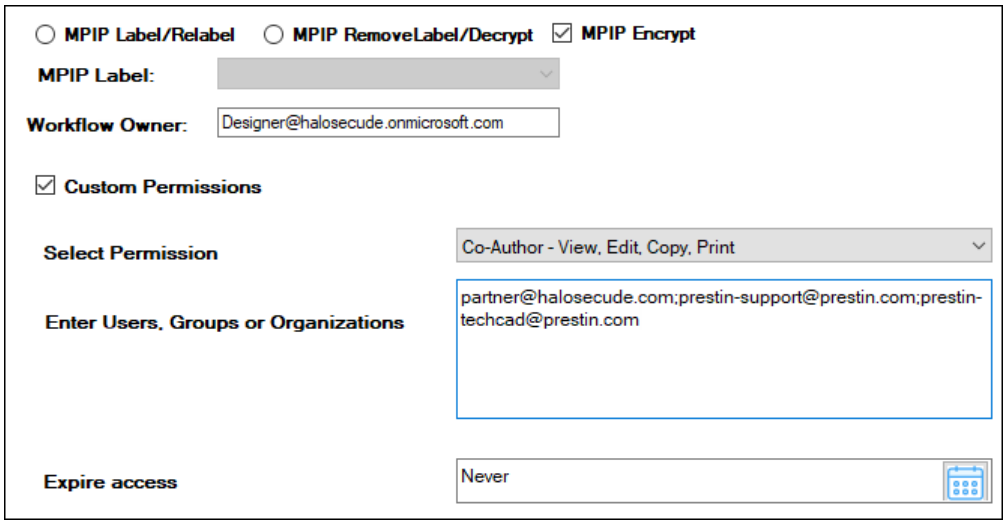
1. As described in the Configure Workflows section, configure your workflow task.
2. From the **Workflow Task** list, select **MPIP Task**.
3. On the **HaloSHARE GenNXT Configuration** screen, the following MPIP task options appear:



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.



Custom permissions

7. From the **Select Permission** list, choose the required permission level:
   a. **Viewer** – View only
   b. **Reviewer** – View and Edit
   c. **Co-Author** – View, Edit, Copy, and Print
   d. **Co-Owner** – Full permissions
   e. **Only for me** – Grants access only to the file author. To know the usage rights of the permissions, please refer to the section "Permissions Level and Usage Rights".
   f. In **Enter Users, Groups, or Organizations**, specify the users, groups, or organization domains that can access the file. Separate multiple entries with commas, spaces, or semicolons. For example `partner@halosecude.com;prestin-support@prestin.com;prestin-techcad@prestin.com`
   g. In **Expire Access**, specify how long users can access the protected file.
      i. Select **Never** to allow unlimited access.

ii. Specify an expiration date to restrict access after the selected date.

h. To remove the selected expiration date, click **Clear date selection**.

8. To decrypt a file, select **MPIP RemoveLabel/Decrypt**.
9. To make a user the file owner and grant full access, enter the user's email ID in the **Workflow Owner** field. For example, `Designer@halosecude.onmicrosoft.com`.
10. Click **Save**.
11. Restart the HaloSHARE service from 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 configuration output, see the Sample Results section.
- To delete a workflow, click **Delete**, and then confirm the action when prompted. The workflow is removed.

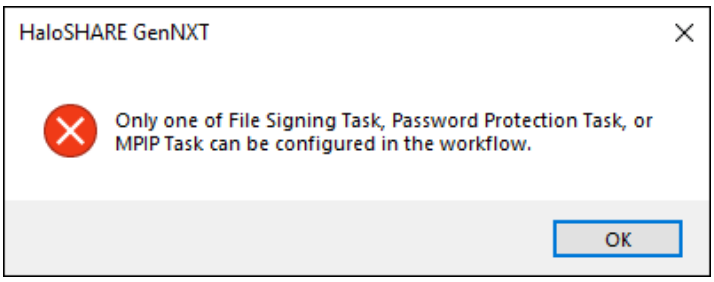
7.2.7. Configure Combined Workflows

A combined workflow enables HaloSHARE GenNXT to execute multiple workflow tasks sequentially on the same file.

Workflow Task Execution Order (Combined Configuration):

- Metadata task
- Watermark task
- File Signing task

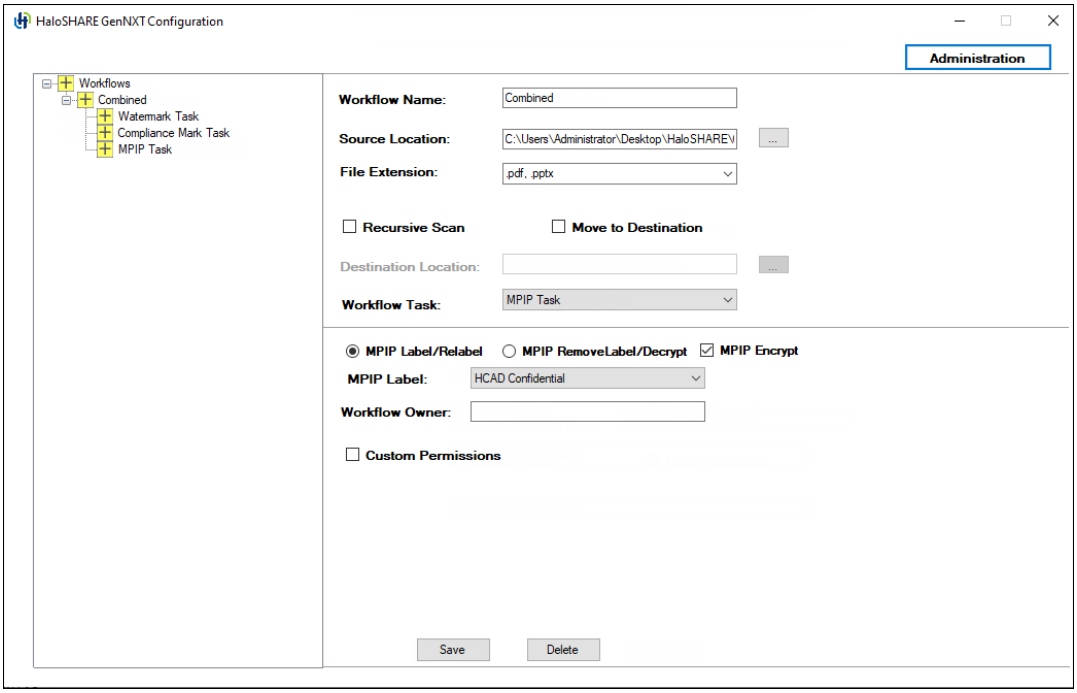
In a workflow, you cannot combine the **Password Protection** or **File Signing** subtasks with the **MPIP** task because they are mutually exclusive. The MIP SDK does not support digitally signed or password-protected files. Attempting to combine them results in the following error message.



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. Restart the HaloSHARE service from the **Administration** UI.

Result

- A confirmation message appears after the workflow is saved successfully.
- HaloSHARE GenNXT processes each file by executing the configured tasks in sequence.
- The processed file is then moved to the configured destination folder if **Move to Destination** is enabled.
- For examples of configuration output, see the Sample Results section.

7.3. Configure the Service by Using the Admin Tool

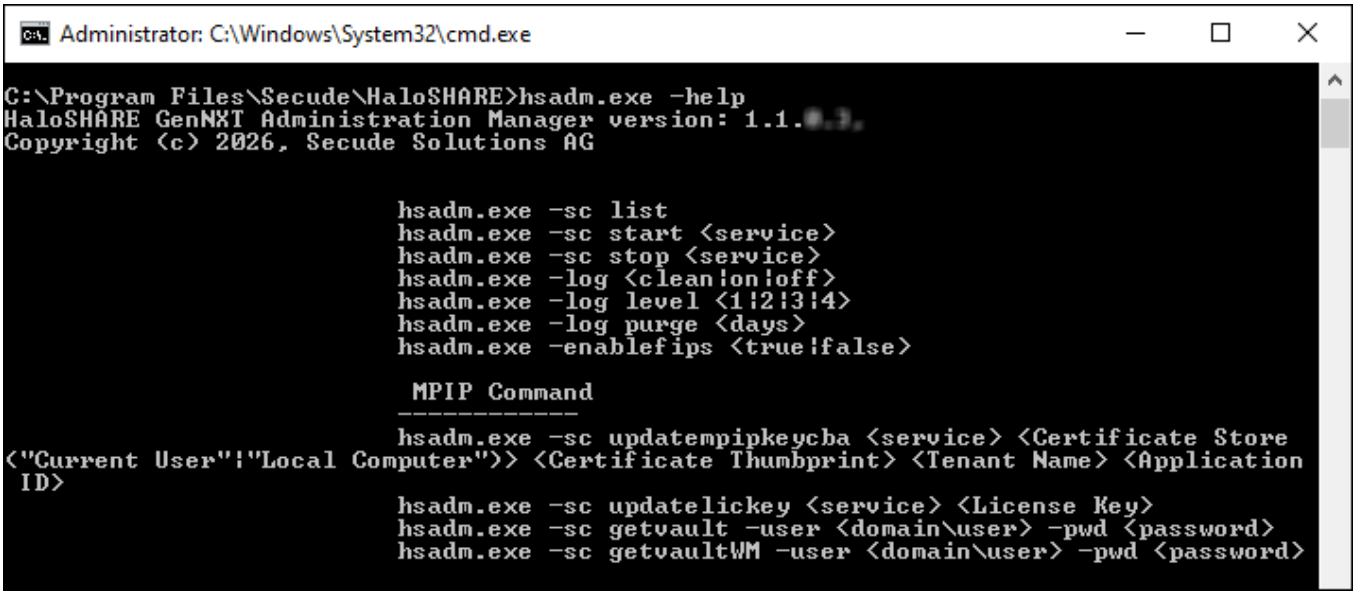
After installing HaloSHARE GenNXT, you may want to change the configuration. To do so, run the tool `...\Secude\HaloSHARE\hsadm.exe` to view the commands. Please note that the admin tool does not support uppercase.

How to update MPIP labels in HaloSHARE GenNXT?

If an MPIP label is added, removed, or updated in the Microsoft Entra admin center, the administrator should restart the HaloSHARE Service for the changes to take effect.

When is it necessary to restart the HaloSHARE service?

Whenever you modify the HaloSHARE GenNXT 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 GenNXT. Note: This can be used only after setting user credentials to run HaloSHARE GenNXT.
 	
For example,
 	
`hsadm.exe -sc start HaloSHARE`
 	
Output
 	
`Service Started successfully.`

`hsadm.exe -sc stop <service>`
 	
Use this command to stop HaloSHARE GenNXT.
 	
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 configure the log purge duration, which defines the number of days after which log files are 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

```
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 require a restart of HaloSHARE GenNXT 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 GenNXT.
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 components are 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.

Name	Default value	Type	Description
			• On = A log file is generated in the default location. • Off = No log file is generated. • Clean = Log files are deleted. This parameter deletes only the logs and does not change the `log_enable` value from "On/Off" to "Clean".
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 the removal of files older than a defined time frame. By default, log files older than 7 days are 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 is visible in clear text in the MIP SDK logs. • true — PII is masked with asterisks in the MIP SDK logs, helping to protect the confidentiality of the PII.
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: The End User License (EUL) is not stored in the MPIP cache storage. • 1 — true (default): The End User License (EUL) is stored in the MPIP cache storage.
cloudtype		REG_SZ	User's Azure Cloud Type. For example: Commercial.

Name	Default value	Type	Description
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.
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.
enablefiletracking	0	REG_SZ	Obtain the protected file's content ID to track the file. • 0 (default value) — The content ID is not extracted for use in File Tracking. • 1 — The content ID is extracted for use in File Tracking.
enableMIP	false	REG_SZ	1. true — When set to `true`, the CUI Marking feature is enabled. 2. false — When set to `false`, 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.

Name	Default value	Type	Description
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 GenNXT 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 GenNXT.
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 GenNXT 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.

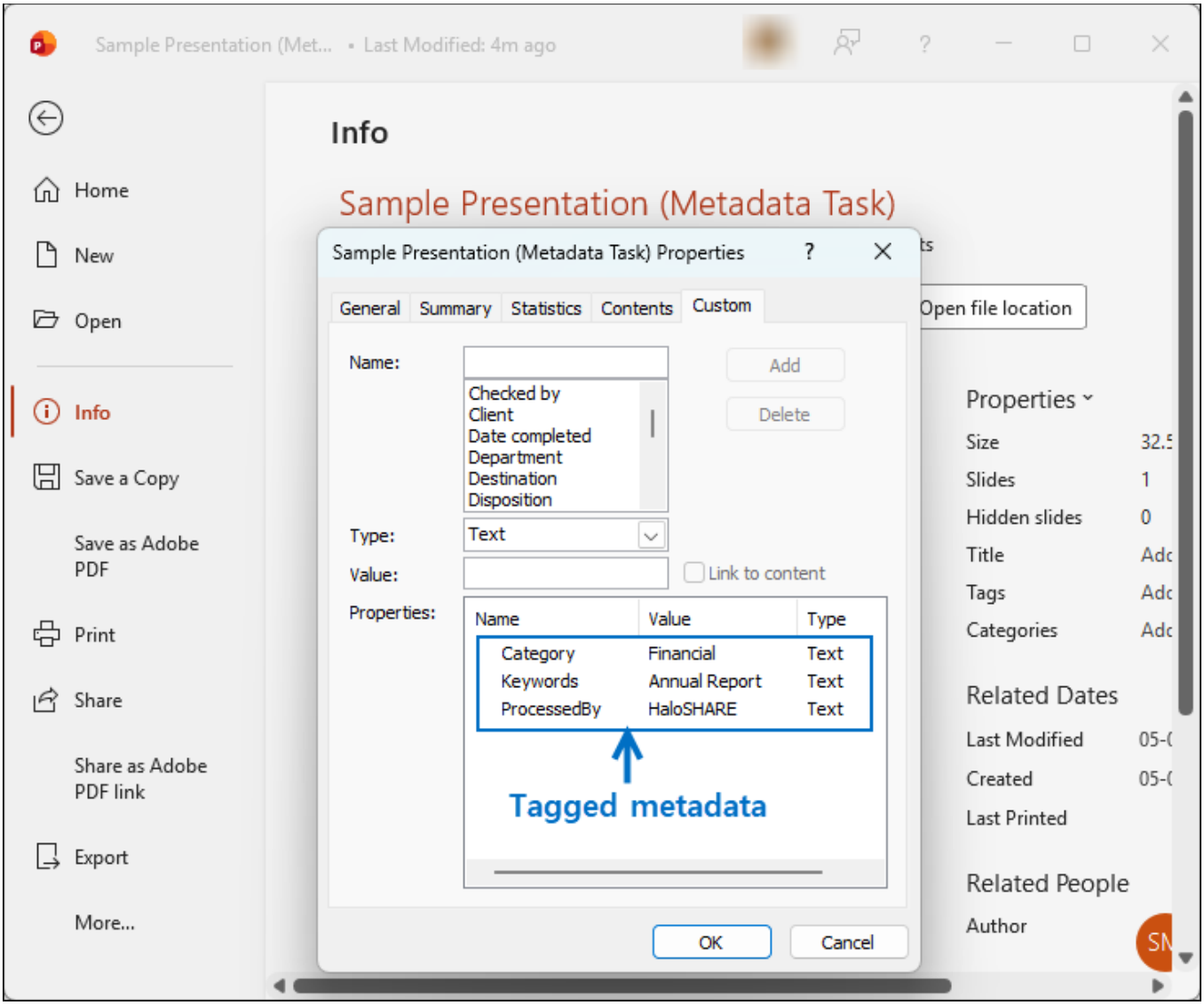
7.5.1. Sample Results

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

Viewing Watermark metadata in CAD files:

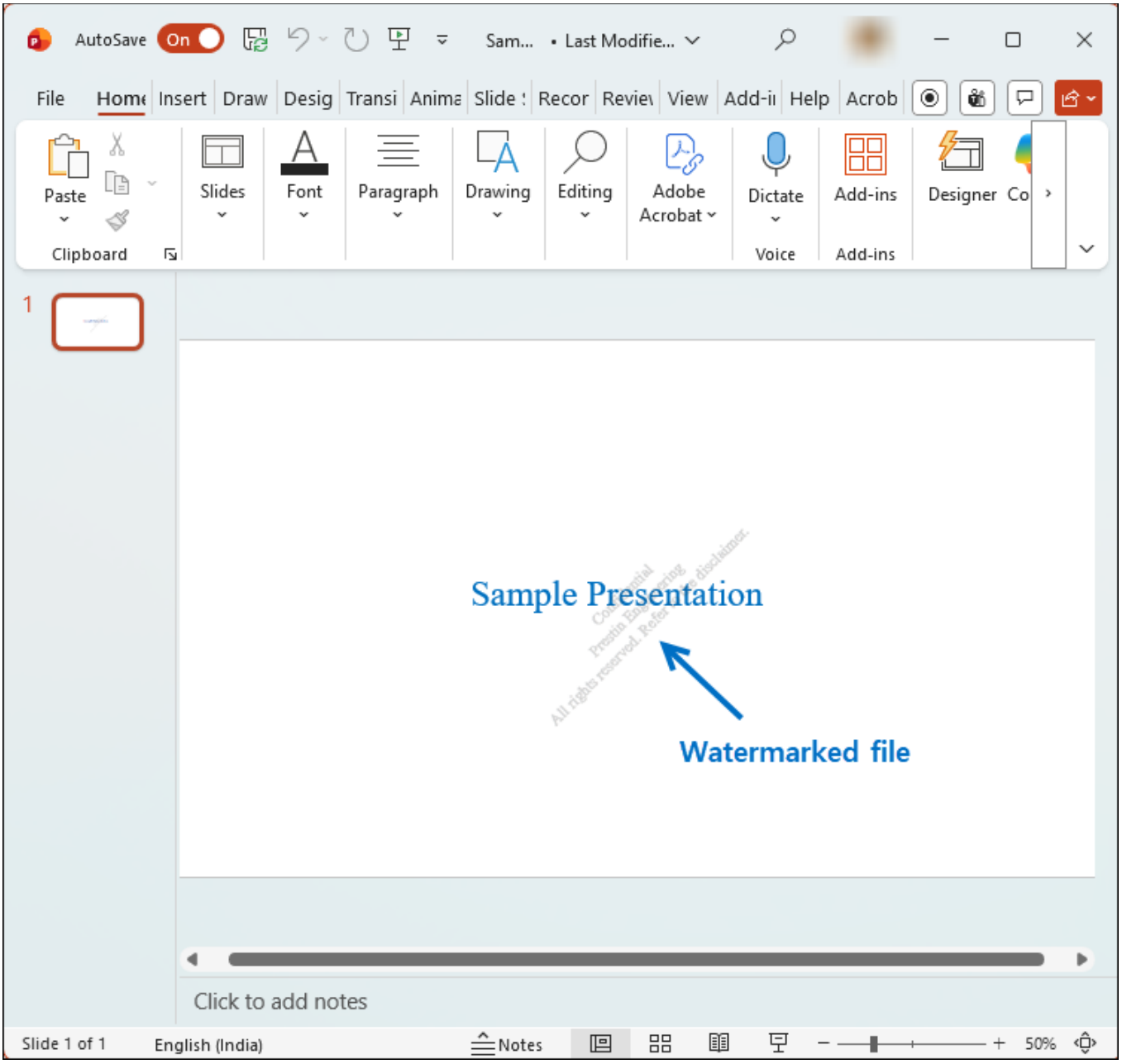
1. **RVT:** Install the **RevitLookup** tool to view the metadata. For more details, please refer to "Watermark in RevitLookup".
2. **DWG:** Go to the file's Custom Properties to view the metadata.
3. **IFC:** Open the file in any text editor and scroll to the end to view the metadata.

7.5.1.1. Metadata Task



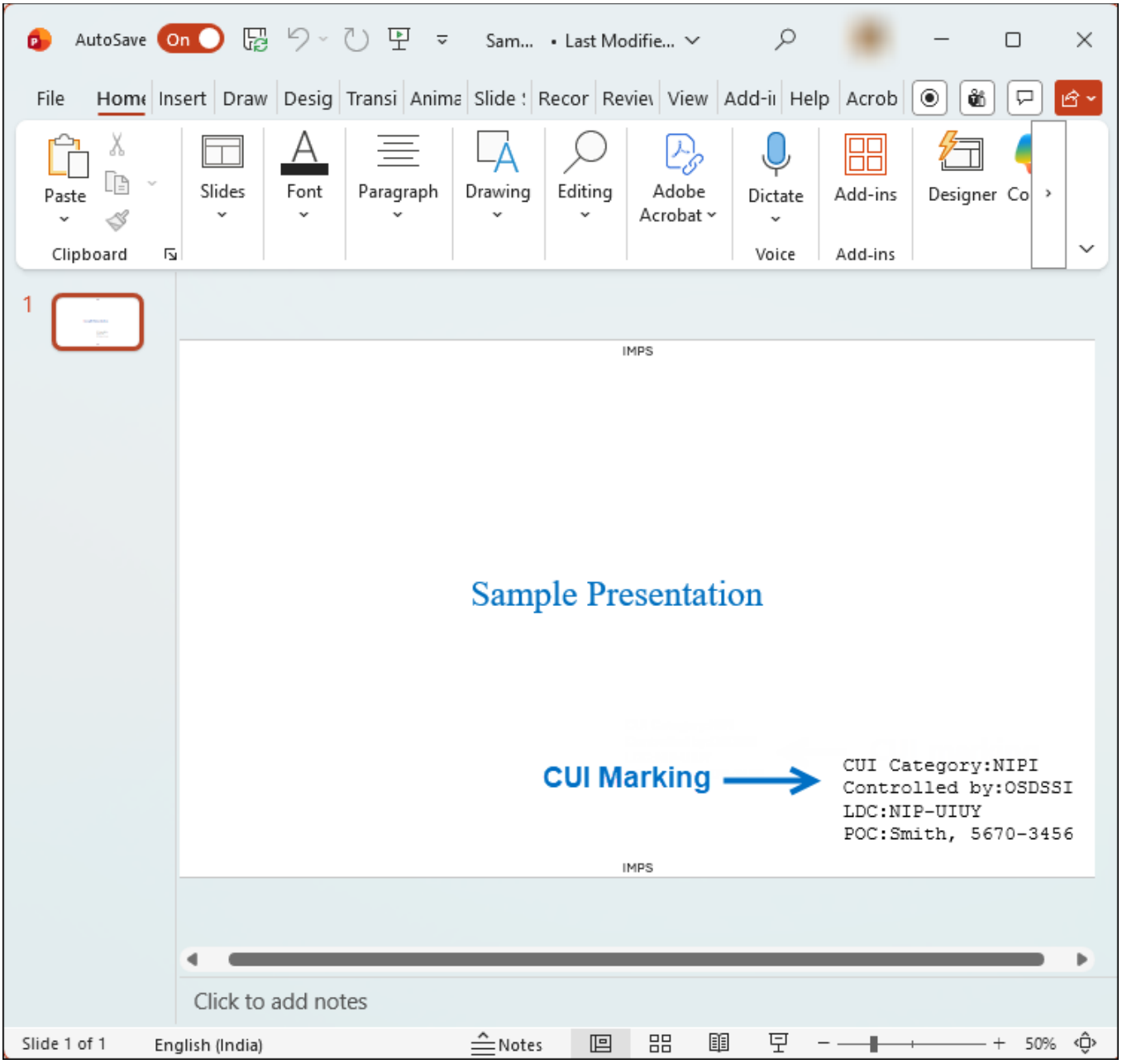
Sample - Metadata Task

7.5.1.2. Watermark Task



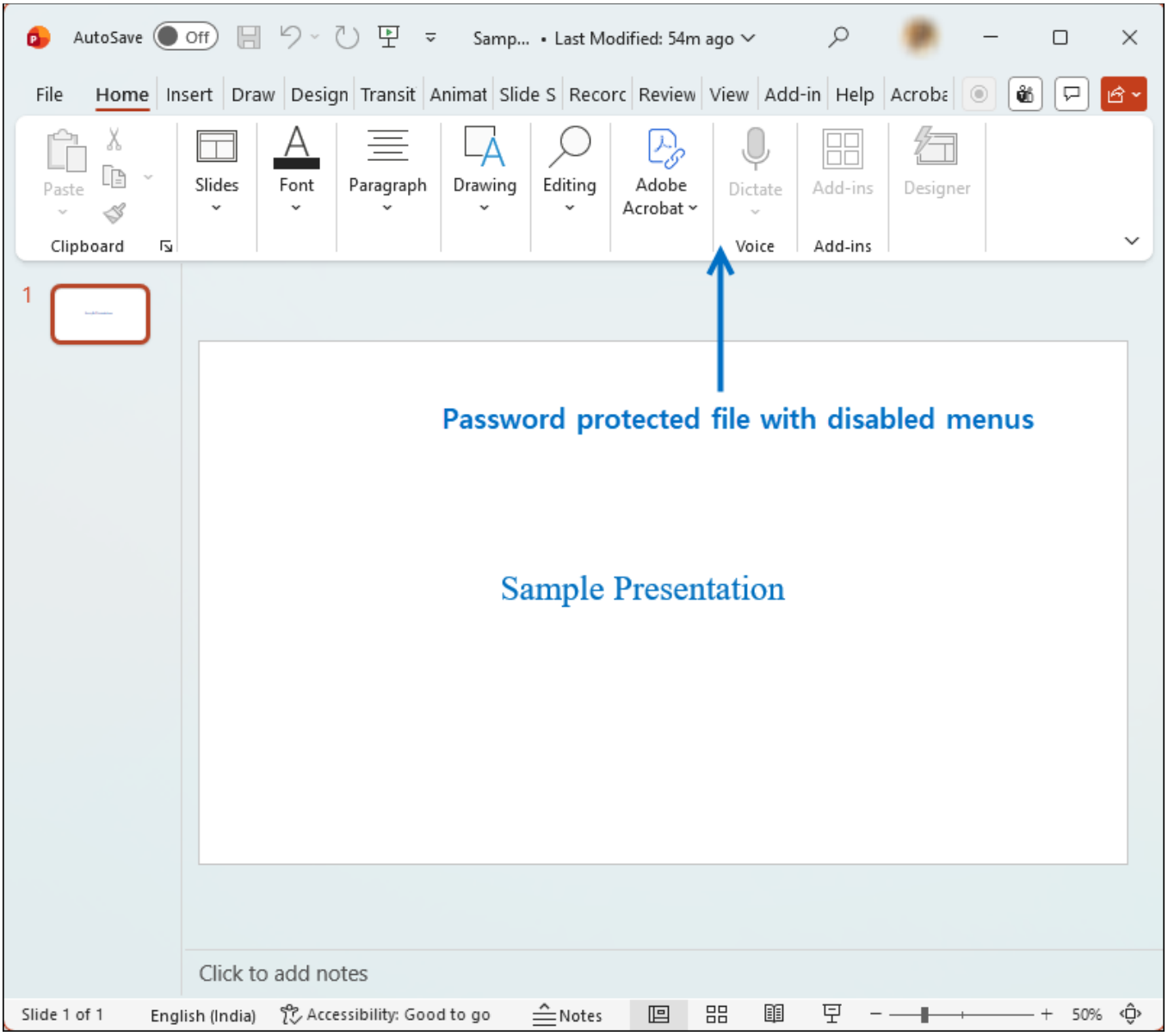
Sample - Watermark Task

7.5.1.3. Compliance Task



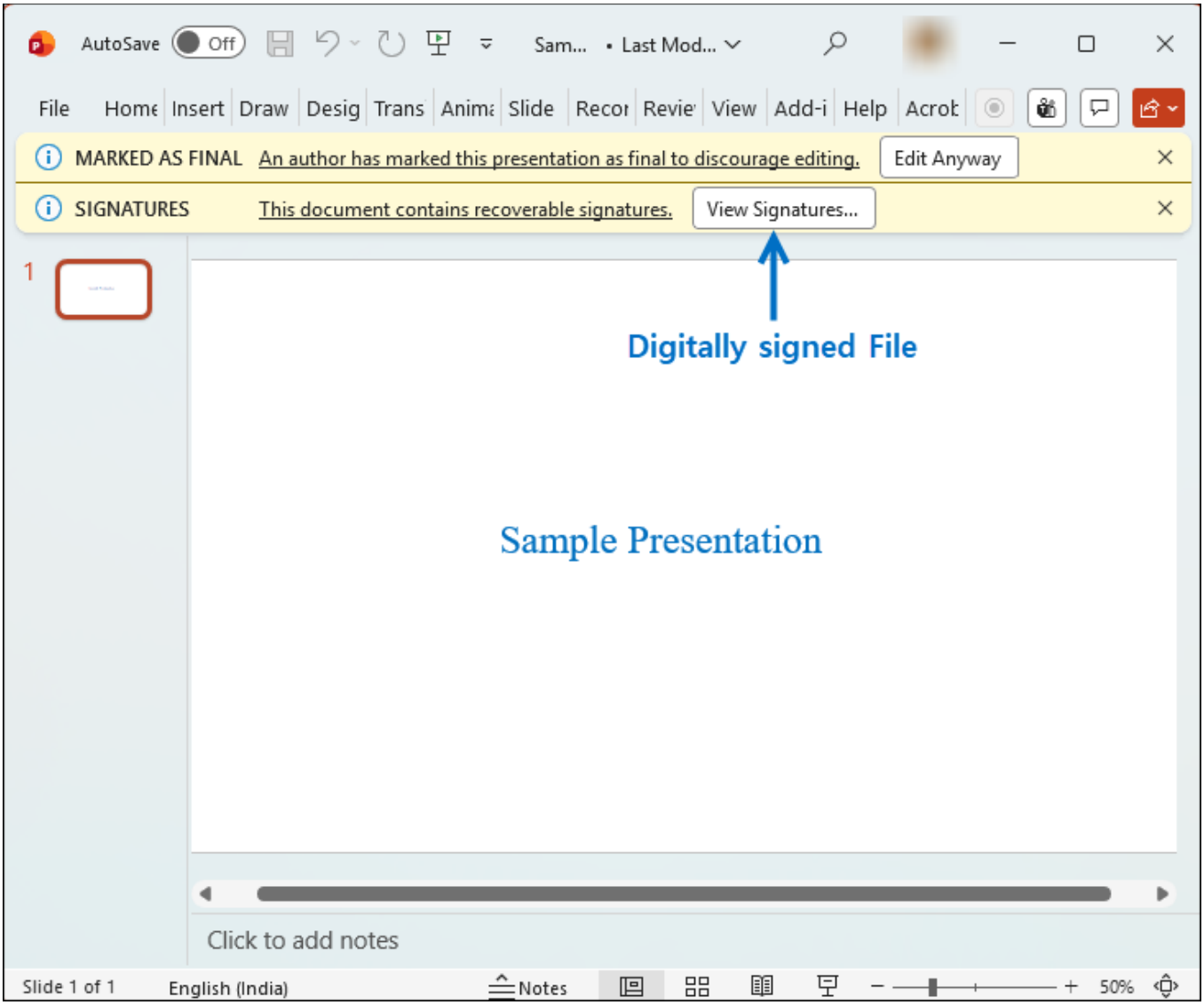
Sample - Compliance Task

7.5.1.4. Password Protection Task



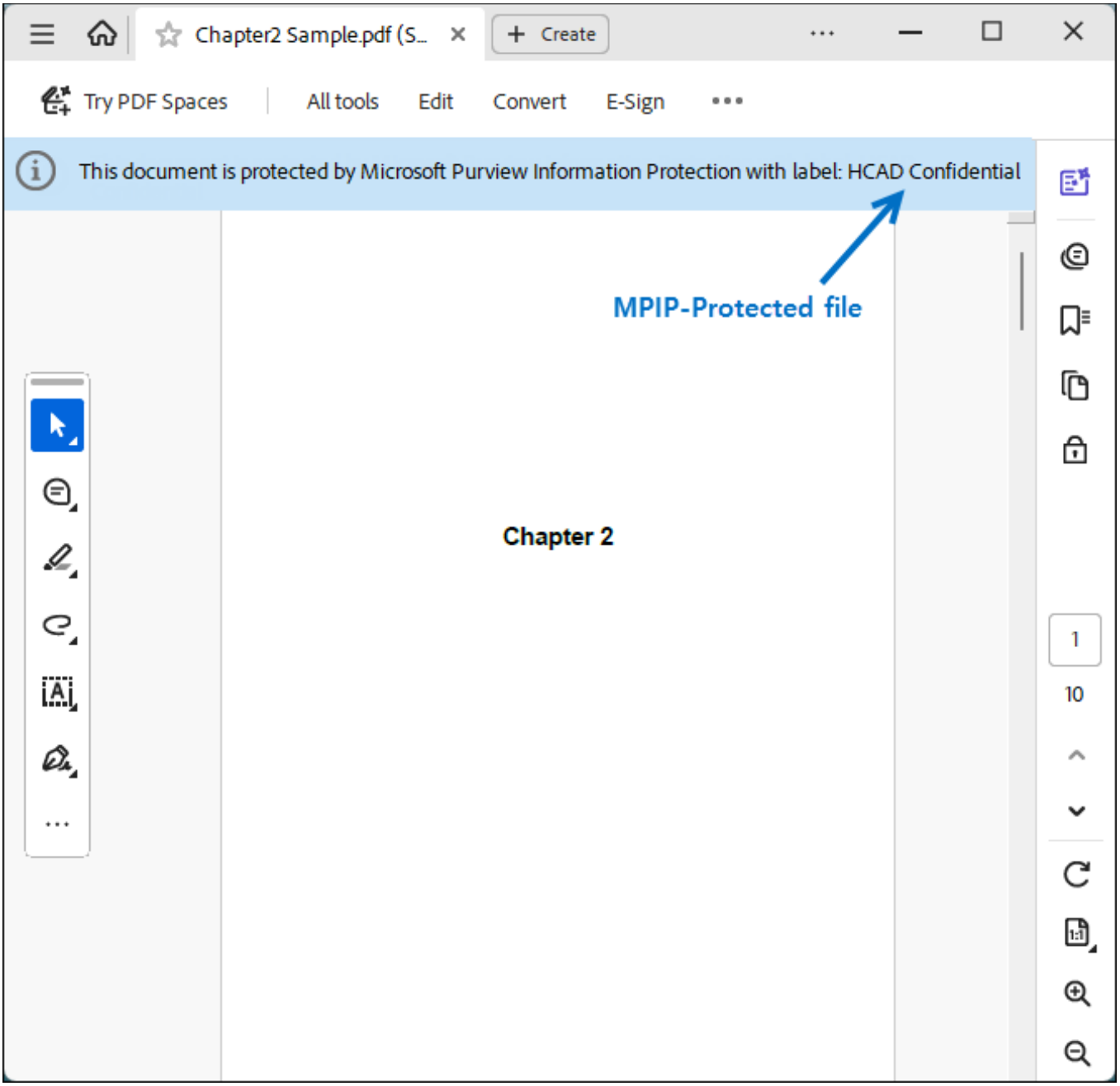
Sample - Password Protection Task

7.5.1.5. File Signing Task



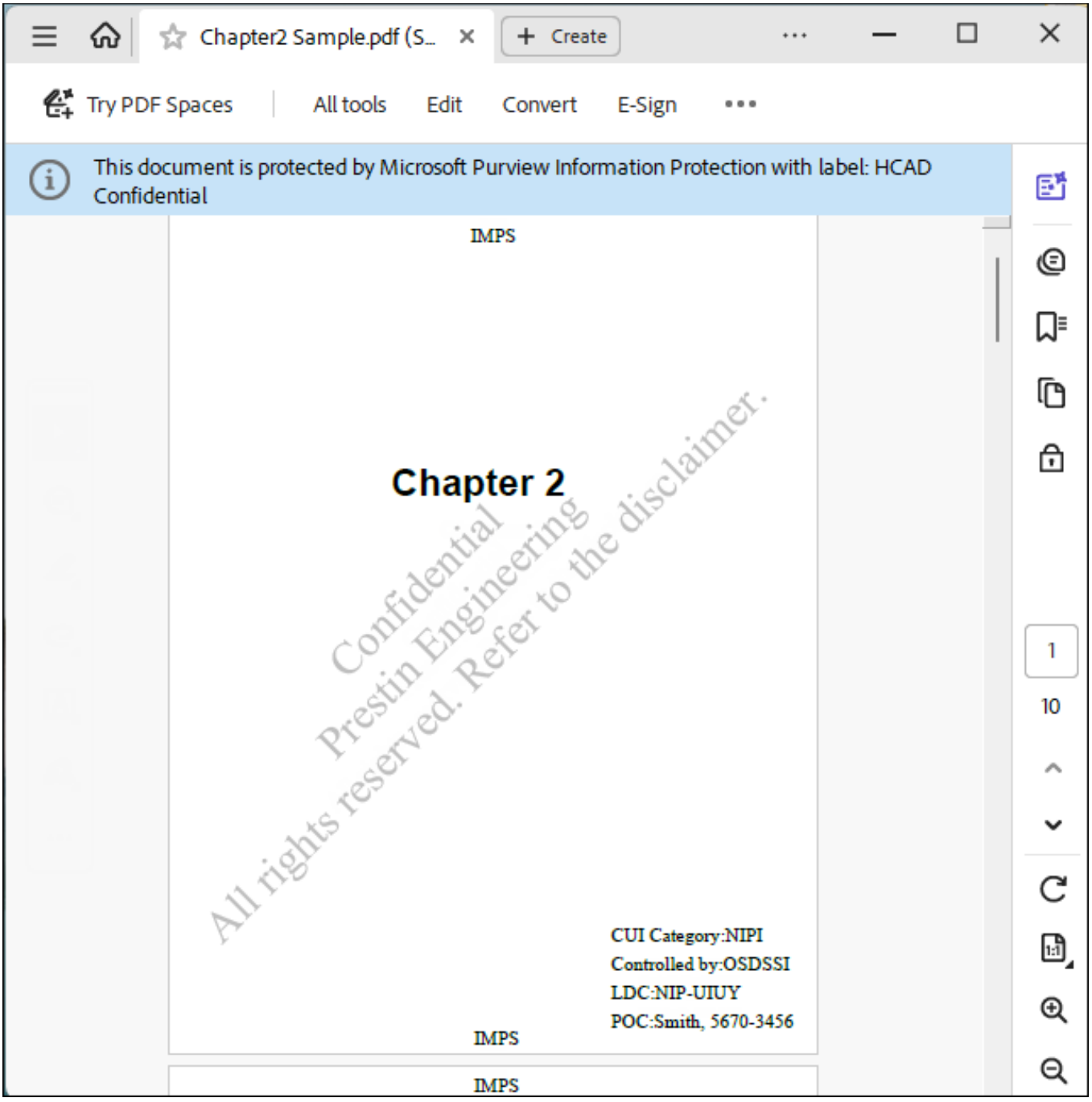
Sample - File Signing Task

7.5.1.6. MPIP Task



Sample - MPIP Task

7.5.1.7. Combined Workflow



Sample - Combined Workflow

8. Troubleshooting

This page helps you resolve common issues that may occur during the installation and configuration of HaloSHARE GenNXT, as listed below.

8.1. Installation Interrupted due to Improper Configuration

Symptoms

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 HaloSHARE GenNXT.

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

Symptoms

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 with installing HaloSHARE GenNXT at this point, the following message appears: "*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

Symptoms

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

Symptoms

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 GenNXT` and reinitialize the service.

Name	Type	Data
ipc_enable_file	REG_SZ	on

Configuring registry entry

9. Technical Support

Before Contacting 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 GenNXT 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	1.18.124	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	6.2.5	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	3.3.0.0, 3.5.1.0	https://github.com/dotnet/Open-XML-SDK	https://github.com/dotnet/Open-XML-SDK?tab=MIT-1-ov-file#readme
ShapeCrawler	0.80.0 all MIT license	https://github.com/ShapeCrawler/ShapeCrawler	https://github.com/ShapeCrawler/ShapeCrawler?tab=MIT-1-ov-file#readme
Autodesk.SDKManager	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.DataManagement	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 describes the basic permissions and the actions allowed for each permission level.

S.No	Permission Level	Usage Rights (Allowed Recipient Actions)
1	View	Open and read the data (read-only access). It includes zooming and viewing from different angles (for CAD file types).
2	Edit	Edit the file and save it

S.No	Permission Level	Usage Rights (Allowed Recipient Actions)
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 under a different file name (Save As). Also includes **Export to PDF**.
6	Change Rights	Change the label applied to a file, remove protection, or save the file in an unprotected format.
7	Owner (Full Control rights)	Grants full access to the file and allows all available actions. This permission also includes the following rights: • Remove protection • 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 describes the available custom permission levels.

S.No	Permission Level	Usage Rights (Allowed Recipient Actions)
1	Viewer	Open and read the data (read-only access). It includes zooming and viewing from different angles.
2	Reviewer	Viewer's allowed permissions plus: 1. Edit 2. Save the file
3	Co-Author	Reviewer's allowed permissions plus: 1. Print

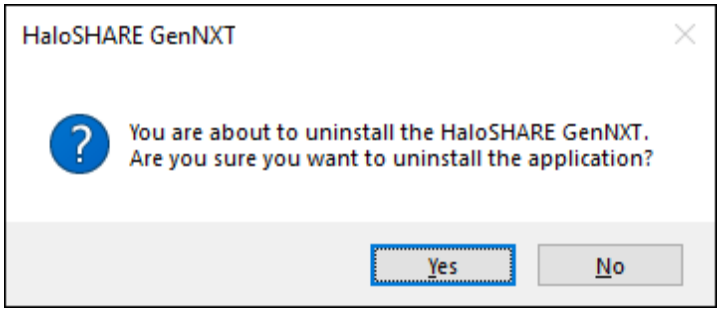
S.No	Permission Level	Usage Rights (Allowed Recipient Actions)
		2. Extract data (including screen captures) from the file into the same or another file.
4	Co-Owner	Co-Author’s allowed permissions plus: 1. Export 2. Change Rights
5	Only for me	Grants all rights to the file and allows all available actions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

Custom Permissions

10.3. Uninstallation

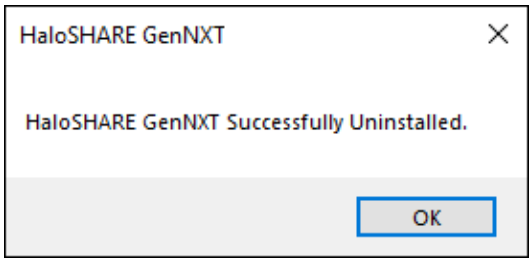
When you no longer use the service, you may uninstall the application. Uninstalling removes all files and registry settings that were added to your computer during the initial installation.

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

A

Acc 1
Api 12
Application-id 29
Aps 12
Autodesk-forma 38

C

Cad 1
Client-id 1, 12
Client-secret 1, 12
Cui 1, 29, 38
Current-user 29

E

Entra-id 12

H

Hub 12

L

Local-computer 29

R

Redirect-uri 12

T

Tenant-id 12, 29
Tls 1

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.