HaloSHARE 1.1

Installation and Configuration Manual

Copyright

Contact

Secude Solutions AG

Landenbergstrasse 34

6005 Luzern

Switzerland

Tel: +41 41 510 70 70

Mail: info@secude.com

Support

Web: https://support.secude.com

Mail: support@secude.com

Table of Contents

Typographic Conventions

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

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

1. Introduction

Secude's HaloSHARE is a best-of-breed solution that monitors the configured local or network folders within the organization. HaloSHARE monitors only the folder that the user defines within it. When a file is placed in the configured folder, HaloSHARE encrypts it by effortlessly applying Microsoft Purview Information Protection (MPIP) labels, providing persistent access controls regardless of where it is moved.

1.1. What distinguishes HaloSHARE?

In a multiuser environment, where multiple users share access to a system or network, there are several potential file access and security issues. Here are a few common issues:

1. Users may maliciously or unintentionally access other users' files.
2. There is a risk in a shared environment that one user will overwrite or modify files belonging to another user.
3. Inadequate access control systems might let users access files for which they don't have the right authorization.
4. Unauthorized users gain access to sensitive files.

HaloSHARE, a labeling solution, can easily overcome the challenge by encrypting the files without user intervention with a simple drag-and-drop into a specific local folder on a HaloSHARE-installed machine. This means that any file moved within the HaloSHARE's radius (configured folder) is encrypted and protected from accidental file sharing and unauthorized access. As a result, this labeling solution protects your data as it travels within and outside of your organization.

Implementing this solution in your environment reduces the risk of a data breach and guarantees data protection regulations are always followed without the need for security personnel to perform any additional manual procedures.

1.2. About this Manual

This guide will walk you through the installation, configuration, and workflow of HaloSHARE.

1.3. Features

1. Supports folder-based bulk file protection.
2. Supports both MPIP-based label protection and user-defined custom permissions.
3. Support for easily removing protection as needed and relabeling an already-existing label on a protected file.
4. It supports a variety of CAD file types, as well as PDF and Office files.

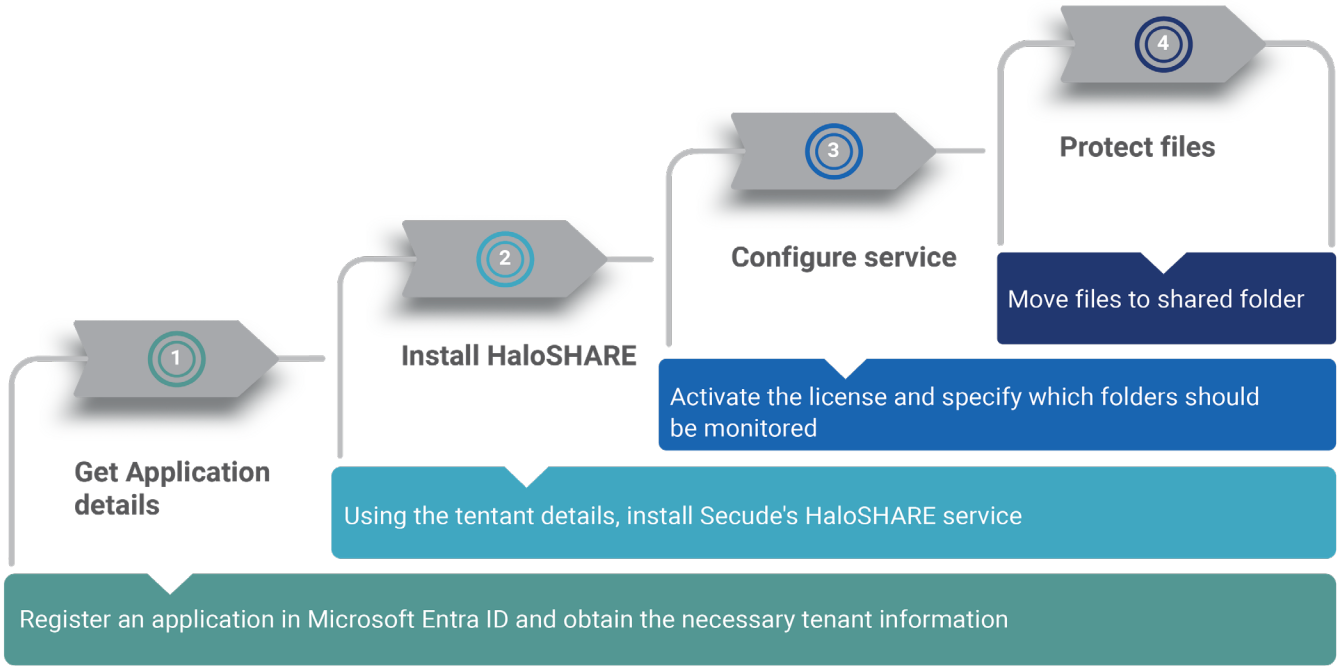
1.4. General FAQs

This section provides answers to the most frequently asked questions (FAQ). If you have any further inquiries, please get in touch with our sales representative or our support team.

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

2. Quick Start Installation Summary

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

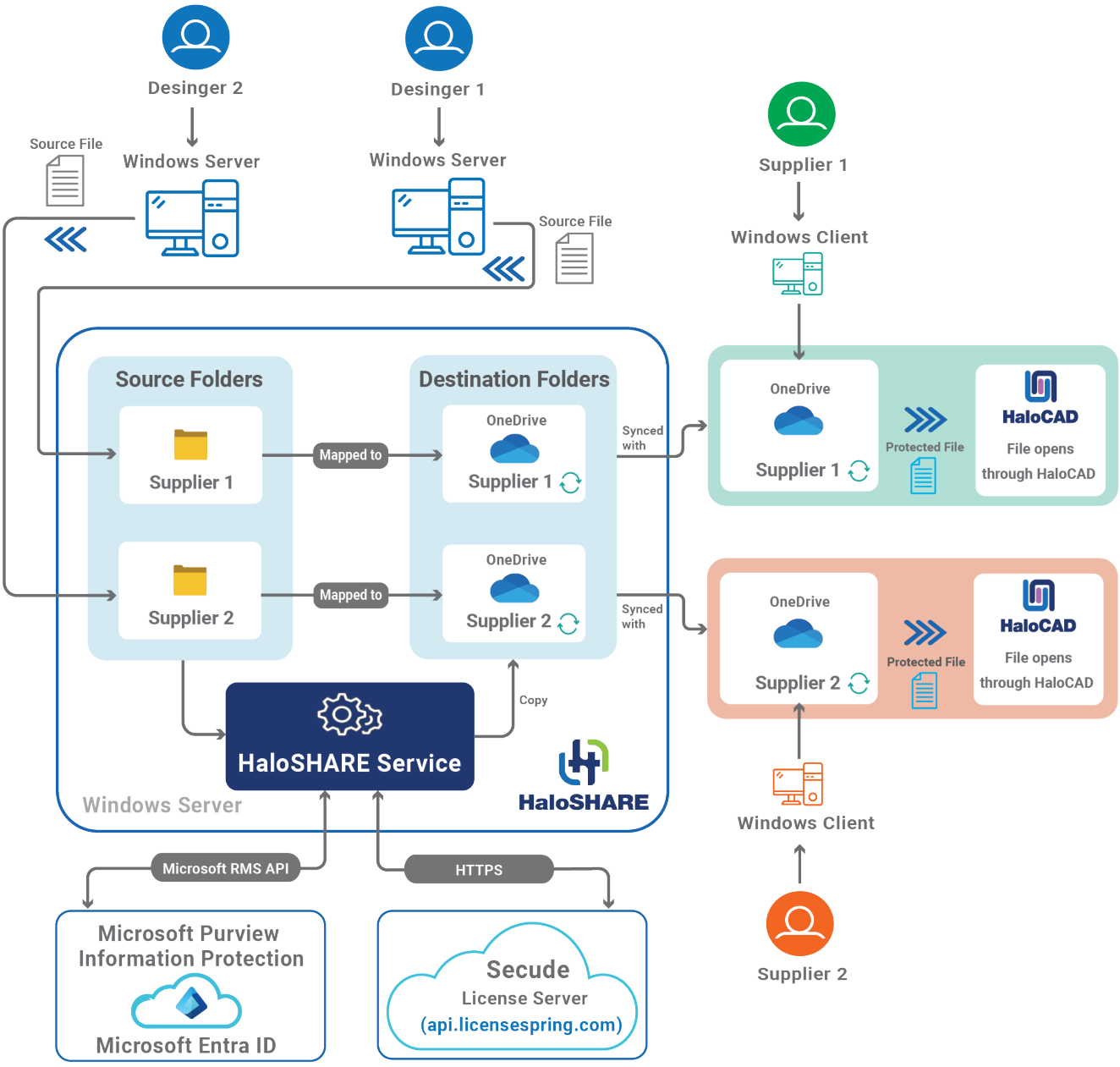


Quick start implementation steps

3. Architecture

HaloSHARE is a service that runs on a Windows Server that communicates with the Microsoft Rights Management Service (RMS) to encrypt files in a specific folder using predefined MPIP labels or user-defined custom permissions. When any unprotected design files are placed inside the shared folder that HaloSHARE constantly monitors, the files are screened and automatically protected without user intervention based on how the configuration is defined in the service.

Note: When a CAD file is protected by HaloSHARE and shared with partners/suppliers, they can view the file by installing the HaloCAD Add-on for CAD applications on their machines.



Architecture

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

1. In an enterprise landscape, different teams create and share files with specific names such as "supplier 1-Prestin Engineering" and "supplier 1-United Engineering" in a locally shared folder on a HaloSHARE-installed machine.
2. HaloSHARE scans the folder and subfolders for new file arrivals determines whether to encrypt or not, and then applies the appropriate MPIP label or custom permission.
3. If HaloSHARE is configured to move a file to a destination folder, the labeled file is copied to the destination location, which is typically a shared folder for your specific supplier, after applying the encryption. The destination folder can be a OneDrive directory. As a result, each supplier gets its own destination folder for sharing business information. In contrast, if moving the file to the destination folder is not enabled, the protected files remain in the source folder.
4. Third parties, such as suppliers, vendors, or external consultants, can only access their folders and consume MPIP-labeled files through HaloCAD Add-ons. Please refer to HaloCAD manuals for more information.

Microsoft documentation

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

4. System Requirements

The following system requirements table specifies the minimum and recommended technical specifications, such as software and network resources, necessary to run the product.

Components	Details
Operating System	1. Supported in Microsoft Windows Server: 2016 and above. Note: HaloSHARE can also run on a Windows client machine, but it is recommended to run it on a server system. 2. Requires **.NET** Framework 4.6.2 and above. 3. Latest Windows system updates installed.
Office 365 Subscription	1. An Azure subscription is required to use Azure RMS and the MPIP functionality. 2. A working Microsoft Entra ID service must be available. 3. Microsoft Purview Information Protection must be fully configured. 4. HaloSHARE creates an outbound network communication with Microsoft Azure Services. 5. TLS 1.2 or higher must be enabled to ensure the use of cryptographically secure protocols. 6. Register an application to get the Application (client) ID and Tenant ID in the Azure portal.

Requirements

Recommended URLs, Addresses, and Ports for MPIP

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

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

Recommended endpoints

Secude License Manager

To communicate with Secude License Manager, the following URL and port must be whitelisted in the customer's proxy:

Address	Port
License API - api.licensespring.com	TCP 443

Recommended license manager endpoint

5. Prerequisites

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

5.1. Registering an Application in Microsoft Entra ID

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

Microsoft documentation

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

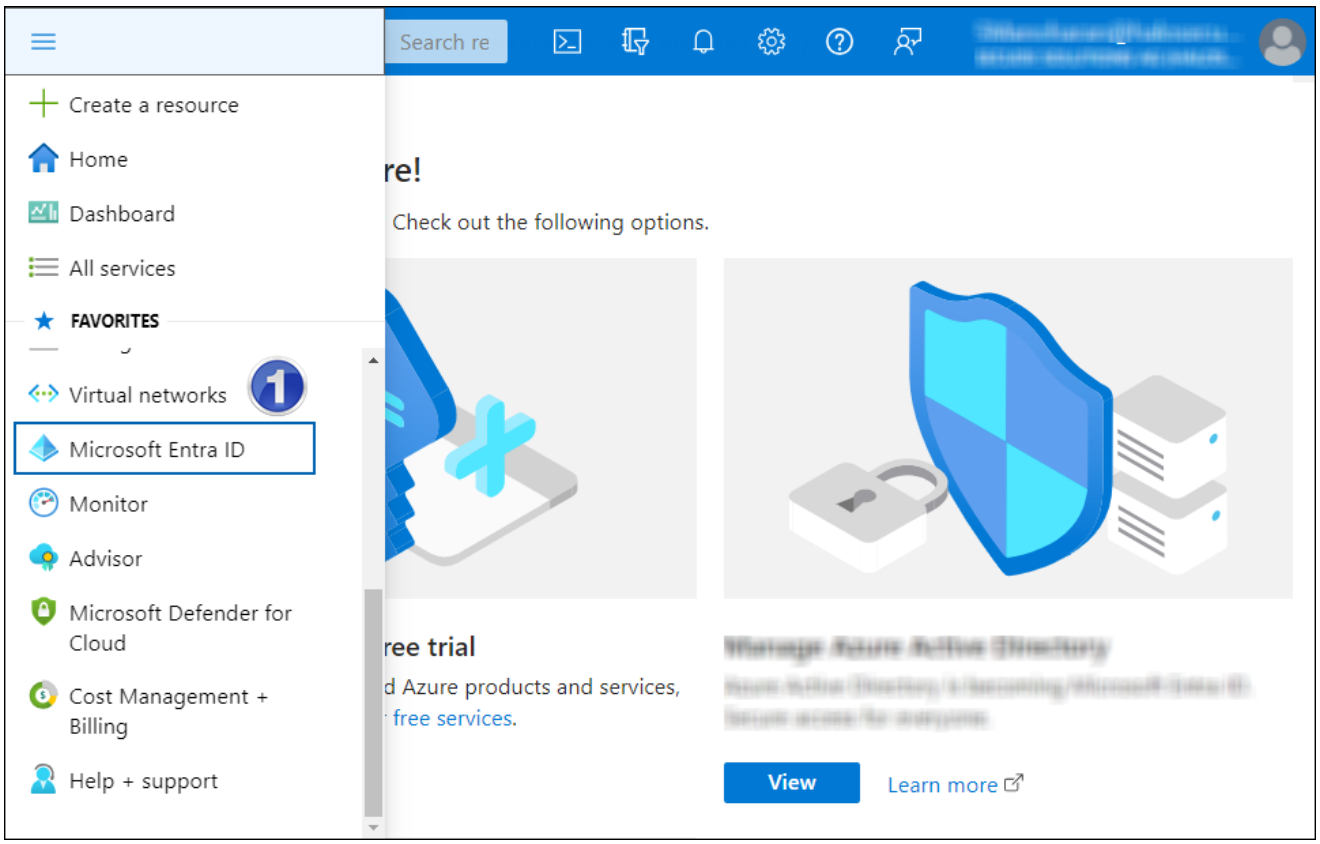
For demonstration purposes, an application is created in the Azure portal; alternatively, you may create an application using https://entra.microsoft.com.

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

5.1.1. Create an Application

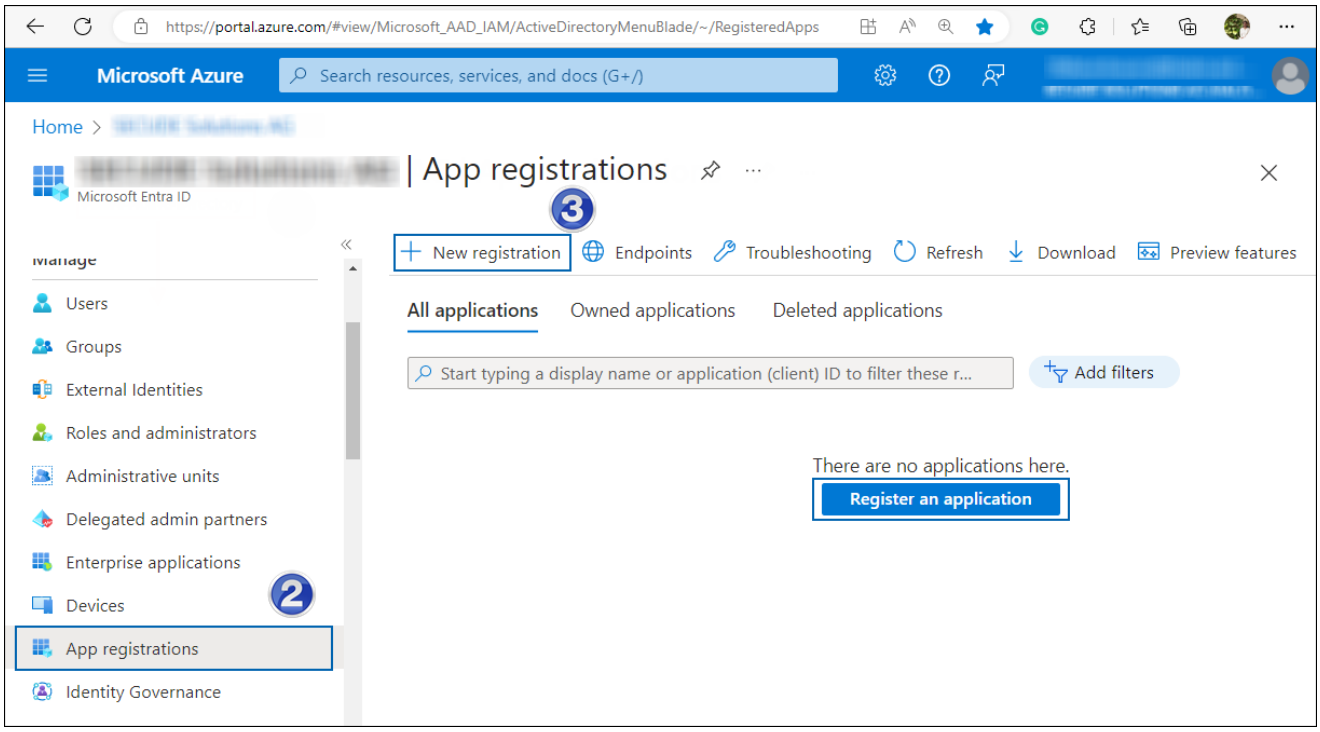
Follow the instructions below to register an application:

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



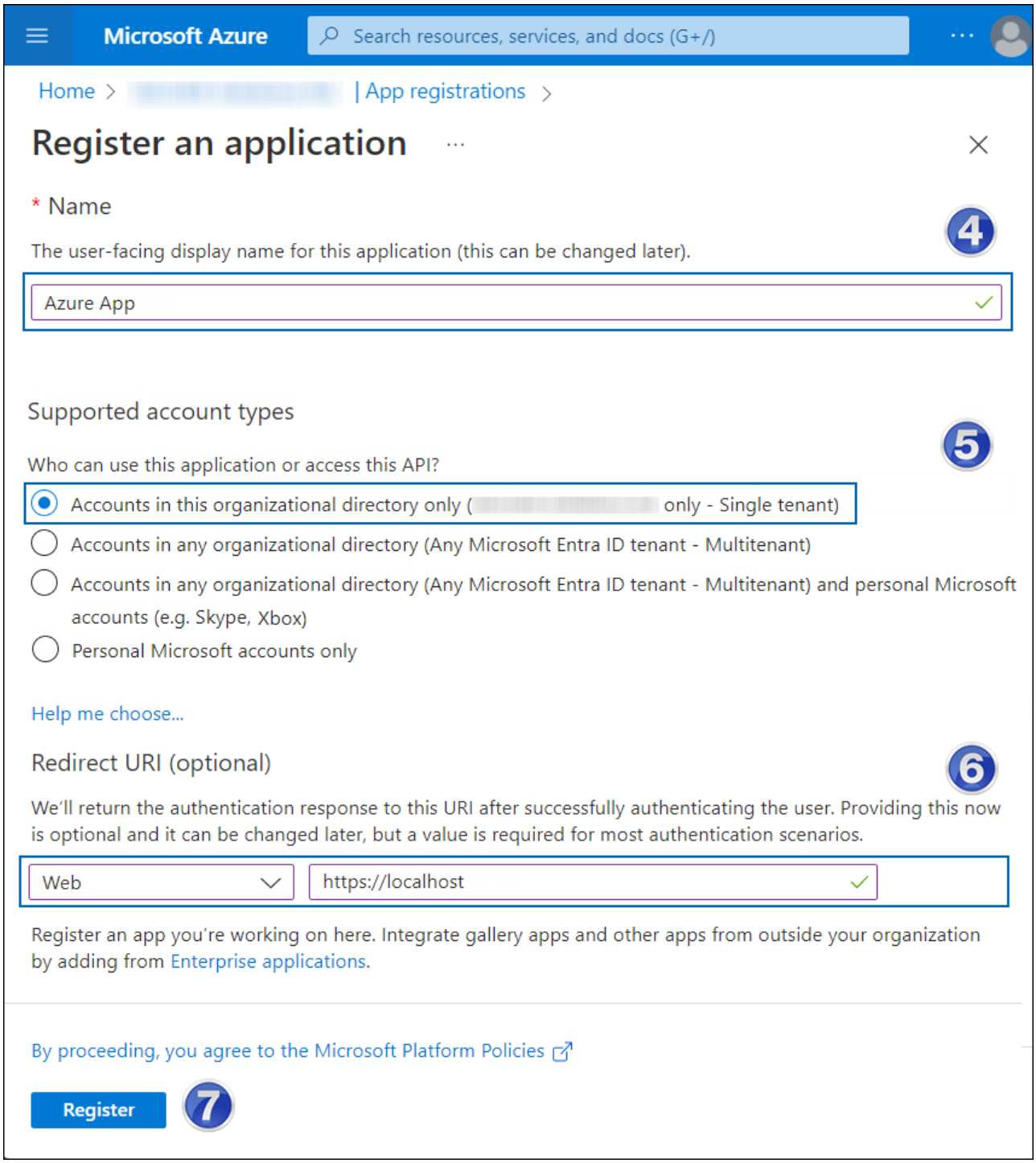
Selecting Microsoft Entra ID

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



New application registration

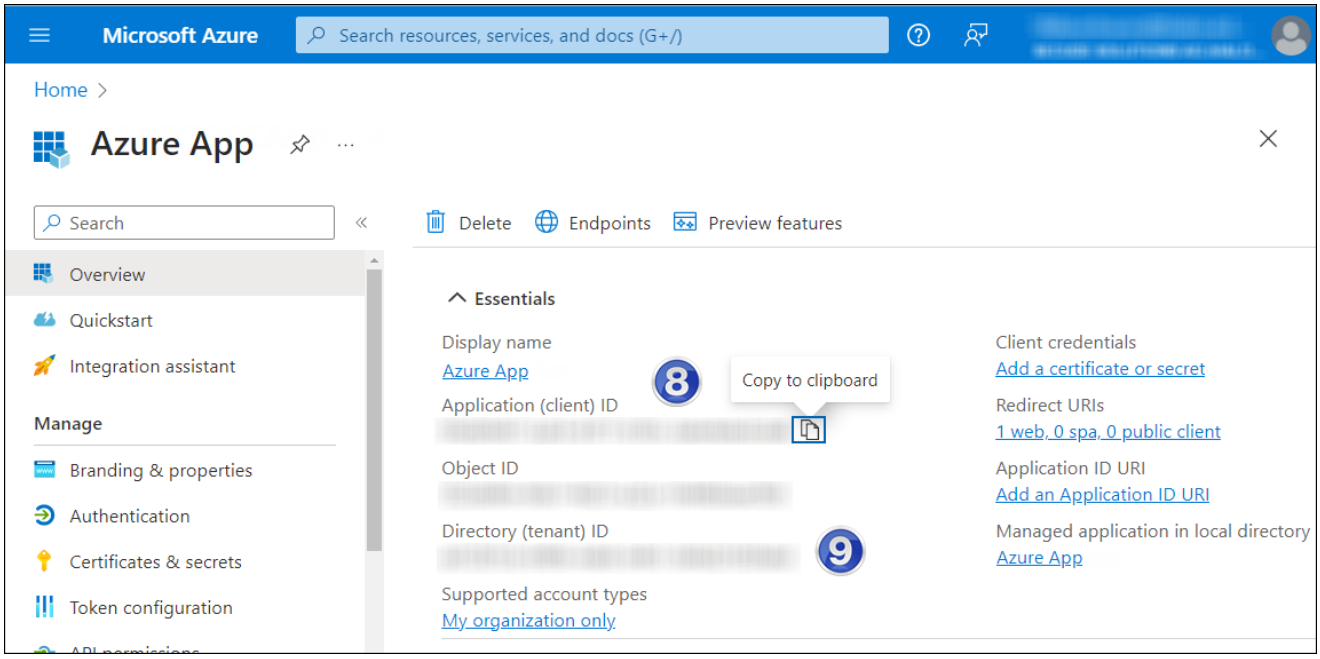
5. On the **Register an application** page, enter your application's registration information.



Webapp client details

6. In the **Name** section, enter a meaningful application name.
7. Under **Supported account types**, select the option **Accounts in this organizational directory only (single tenant)**. As of now, HaloSHARE Service only supports a single tenant.
8. Under **Redirect URI**: Select **Web**, and then type a valid redirect URI for your application. For example, `https://localhost`.

9. When finished, click **Register**.
10. An overview page for the new application registration is created and displayed.



Application ID and Tenant ID

11. The following values are shown on the portal once registration is complete. To copy and save the ID value in a text editor, hover your cursor over it and click the **Copy to clipboard** icon.
    a. **Application ID** – It is also referred to as **Client ID**.
    b. **Directory ID** – It is also referred to as **Tenant ID**.

Save the authentication parameters

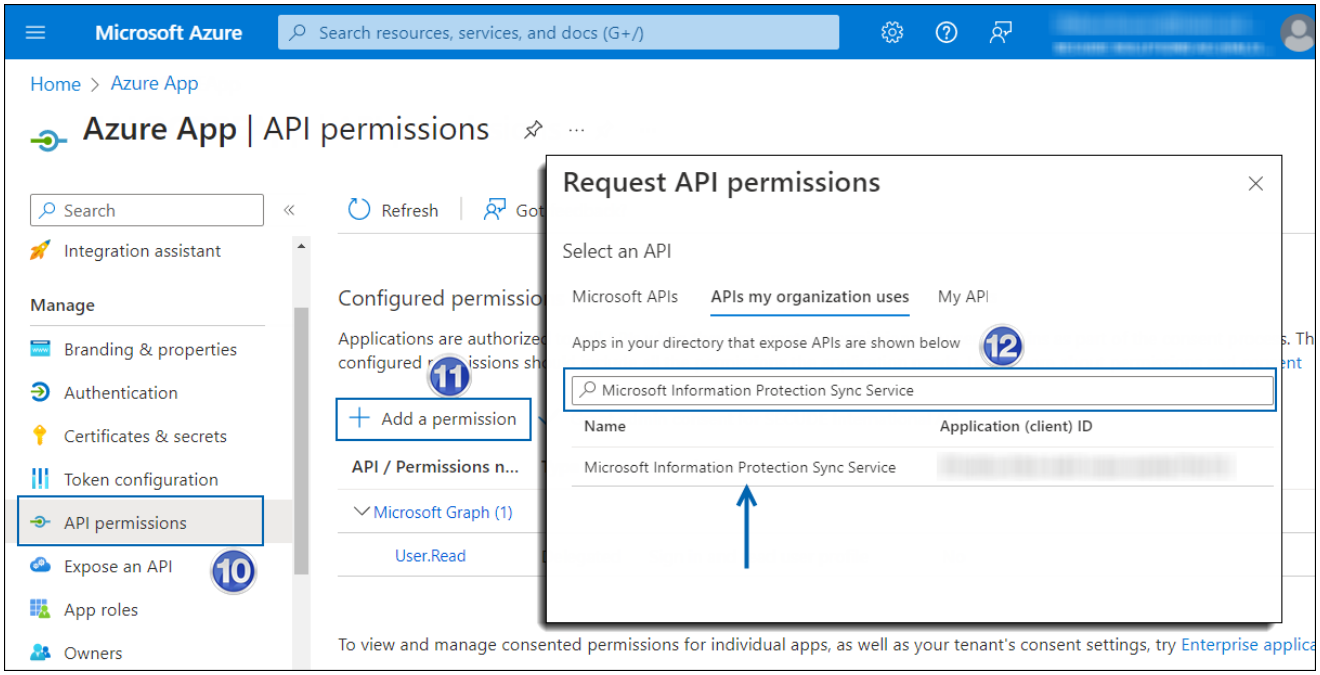
In a text editor (such as Notepad), copy the value of **Application (client) ID** and **Directory (tenant) ID**, and save it for initializing the HaloSHARE.

5.1.2. Add Required Permissions

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

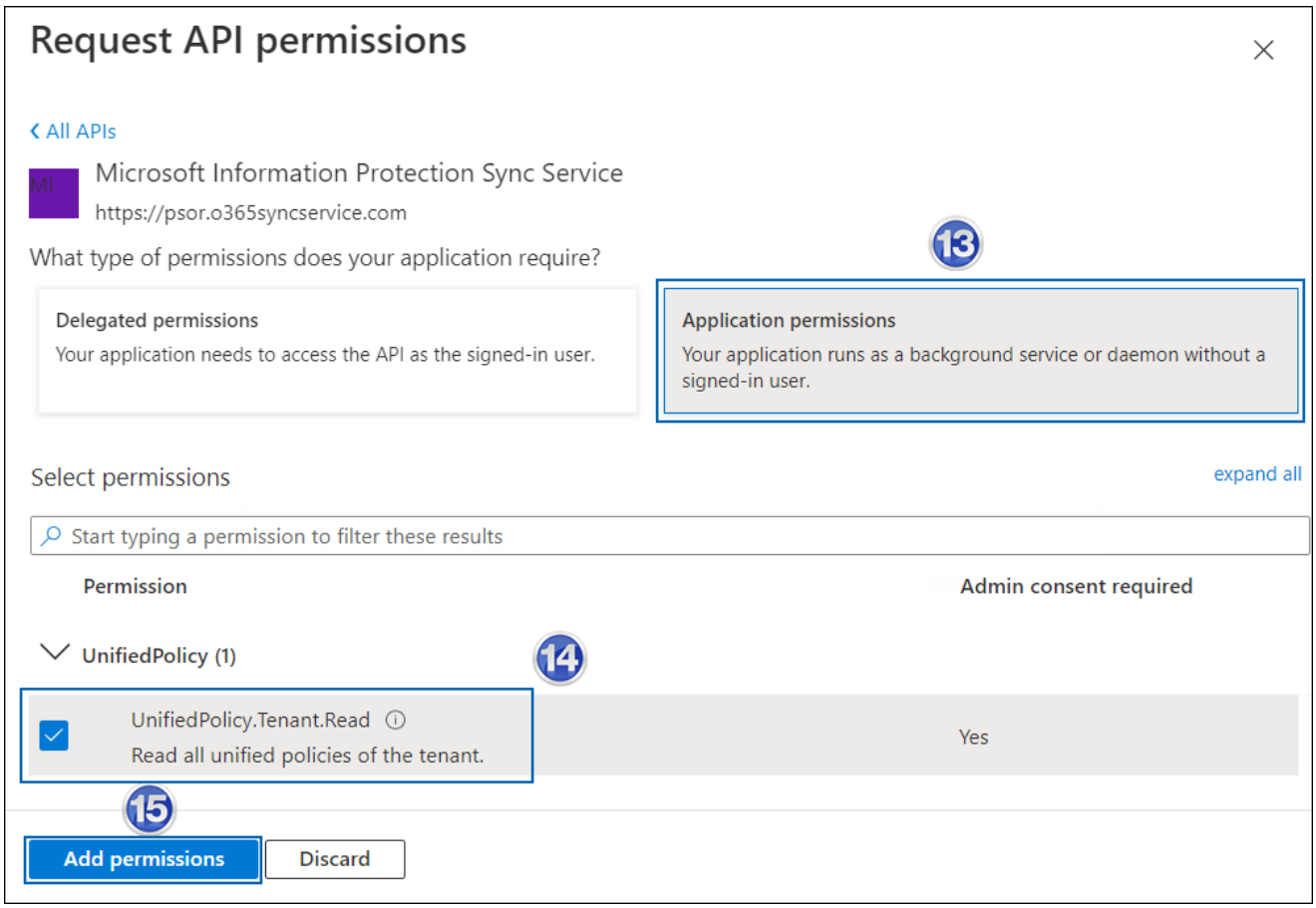
1. In the sidebar of the application page, select **API permissions**. The **API permissions** page for the new application registration page appears.
2. Click **Add a permission** button. The **Request API permissions** page appears.
3. Under the **Select an API** setting, select **APIs my organization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

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



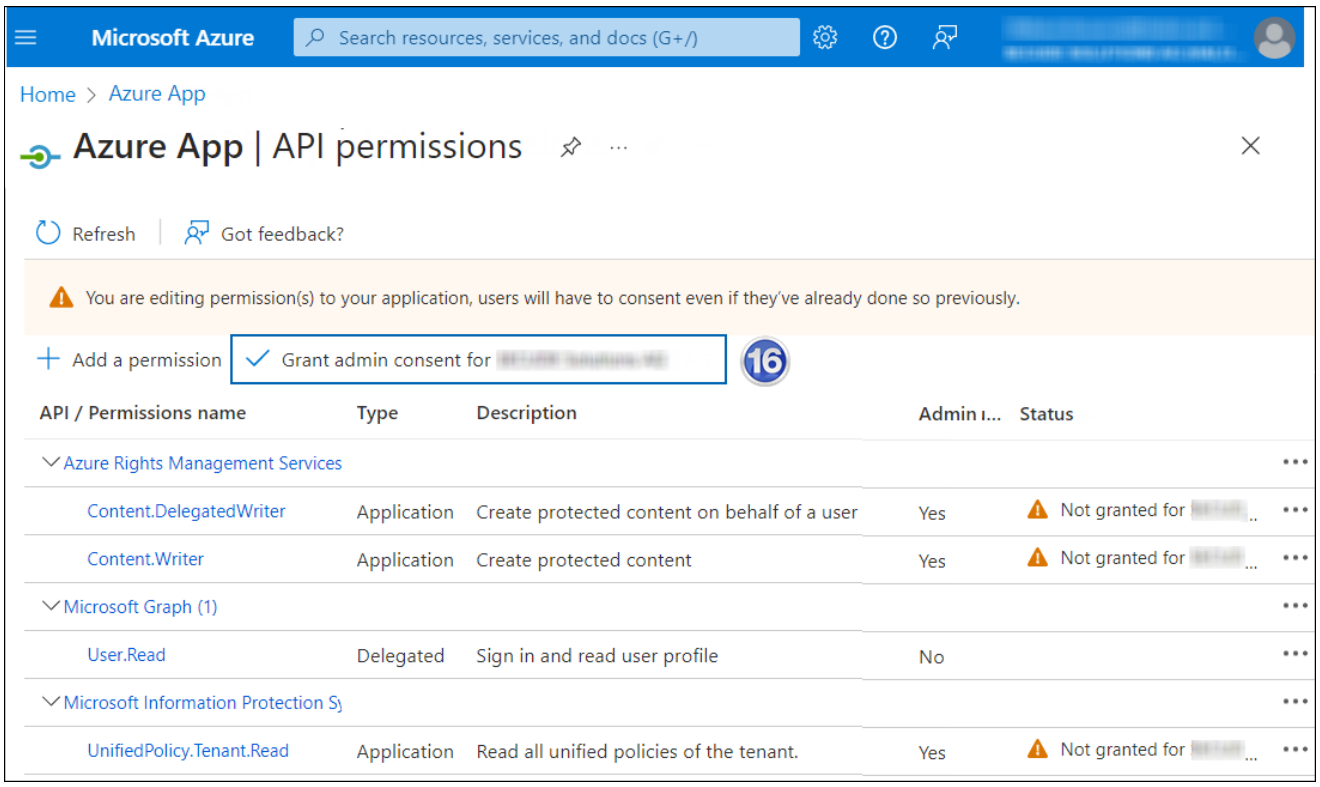
API selection

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



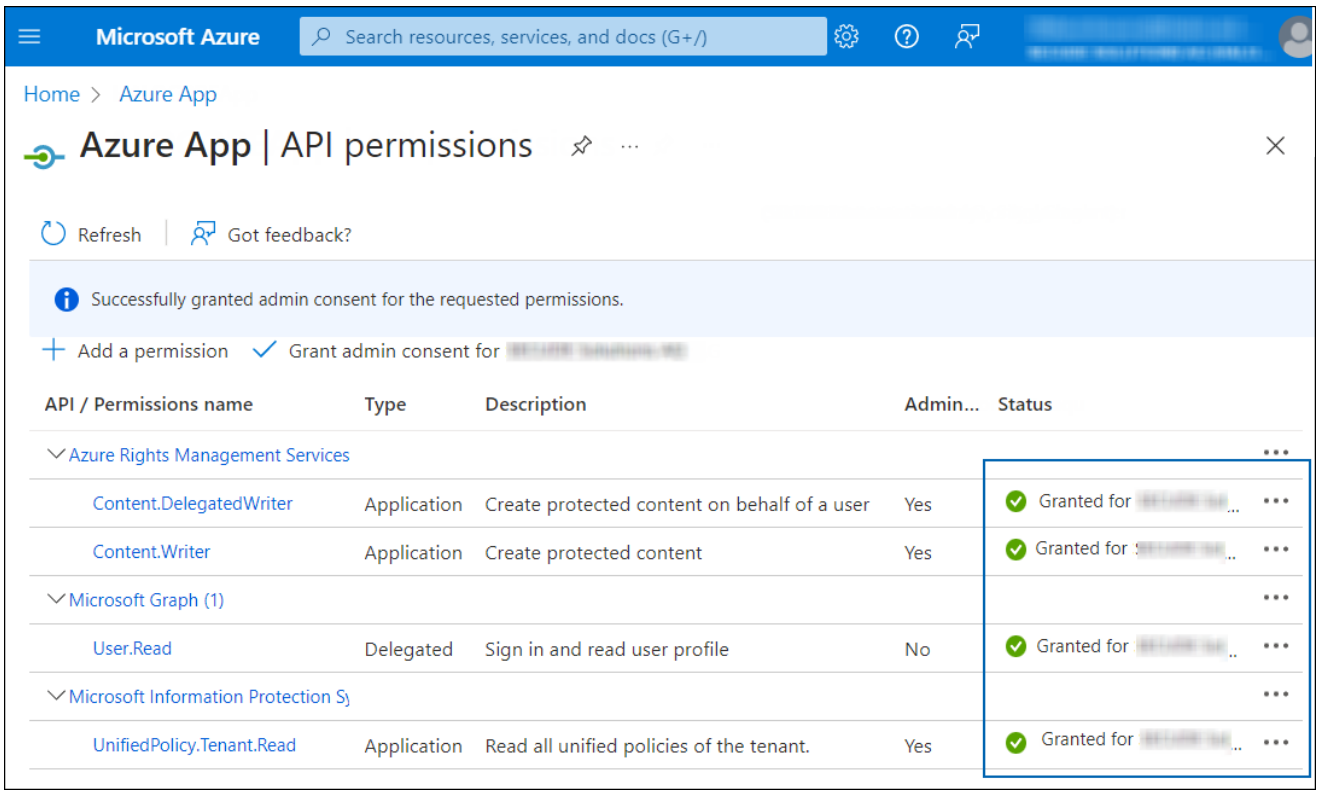
Adding permission

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



Required API Permissions

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



API Permissions with admin consent

13. The following table lists the required permissions.

API / Permission Name	Display Name	Type	Description
Microsoft Graph	`User.Read`	Delegated	Sign in and read the user profile. This API permission is added by default, but HaloSHARE does not use it.
Azure Rights Management Services	`Content.DelegatedWriter`	Application	Create protected content on behalf of a user
(Microsoft Rights Management Services)	`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-mentioned permissions are adequate for applying the MPIP label to a file. In addition, HaloSHARE requires the following superuser privilege to relabel a file.

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

Required permissions #2

5.1.3. Upload the Certificate in Azure Portal

HaloSHARE is based on certificate authentication, so you must enter your certificate information into the registered application.

Prerequisites:

1. **Certificate**:
    a. Make sure to have a valid certificate that contains keys such as `-KeyExportPolicy Exportable` and `-KeySpec Signature`.

b. And that can also be a self-signed certificate. Note: As a best practice and for security reasons, we recommend using a self-signed certificate in a test environment and NOT recommended for a production environment.

2. **Install the certificate**:

   a. Make sure to install this certificate on a Windows Server machine where the HaloSHARE is going to be installed.

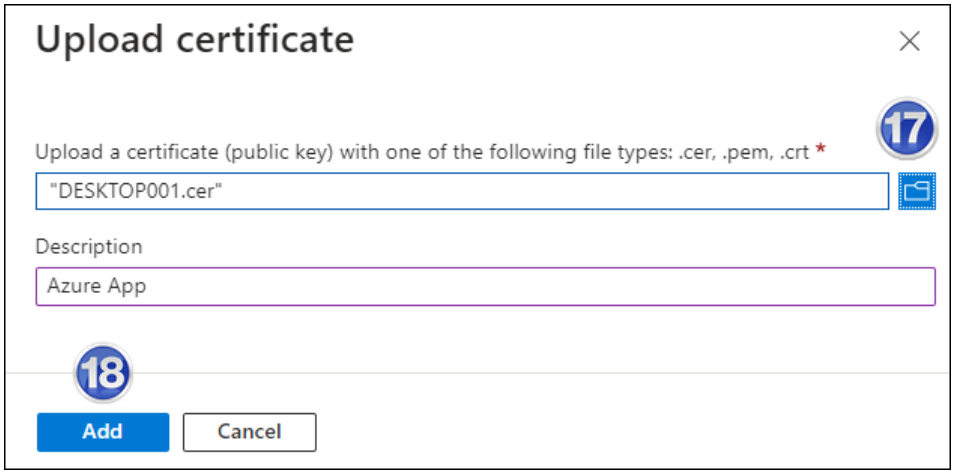
   b. Certificate Store can either be **Current User** or **Local Computer**.

   c. If it is a self-signed certificate, then it should also be installed in **Trusted Root Certification Authorities**.

   d. If the certificate is signed, then the root CA authority and intermediate CA authority (if any) should also be installed in the respective trusted store.

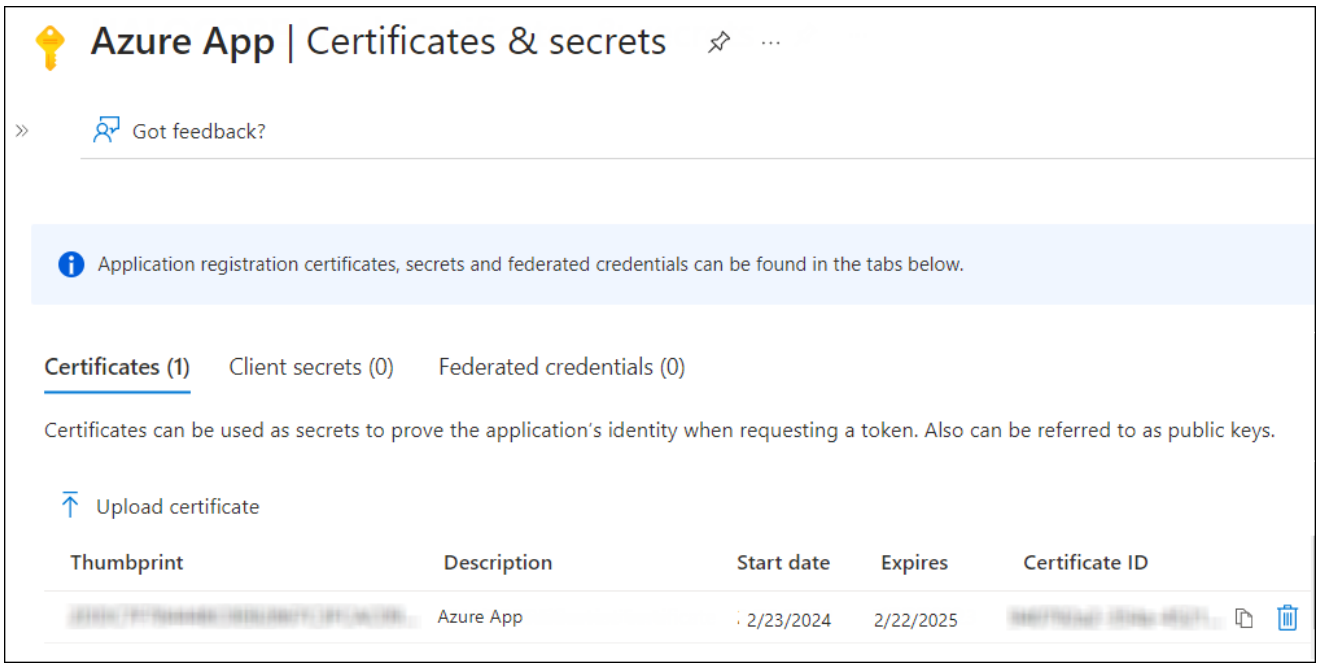
To upload the public key of certificate, follow the below steps:

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 below figure:



Upload certificate #1

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



Upload certificate #2

5. You are now ready to install the HaloSHARE.

5.2. Create and Configure the Sensitivity Labels

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

5.3. Others

1. To install the service, you must have local administrator privileges.
2. To run the service, you can use a user account with administrative privilege or non-administrative privilege.
3. The user who initializes the service should have appropriate permissions on the source and destination folders. In addition, the user who is running the service should have access to that network location in the format of an IP address. For example, `\\10.0.0.138\foldername`
4. Before you begin, make sure that the user who is running the service or a specific group that the user belongs to is not to the **Deny log on as a service** policy (**Local Security Policy** > **Security Settings** > **Local Policies** > **User Rights Assignment**). If the user(s) exist, the **Error 1069: The Service did not start due to a logon failure** message will appear while running the HaloSHARE.

6. Installing the HaloSHARE

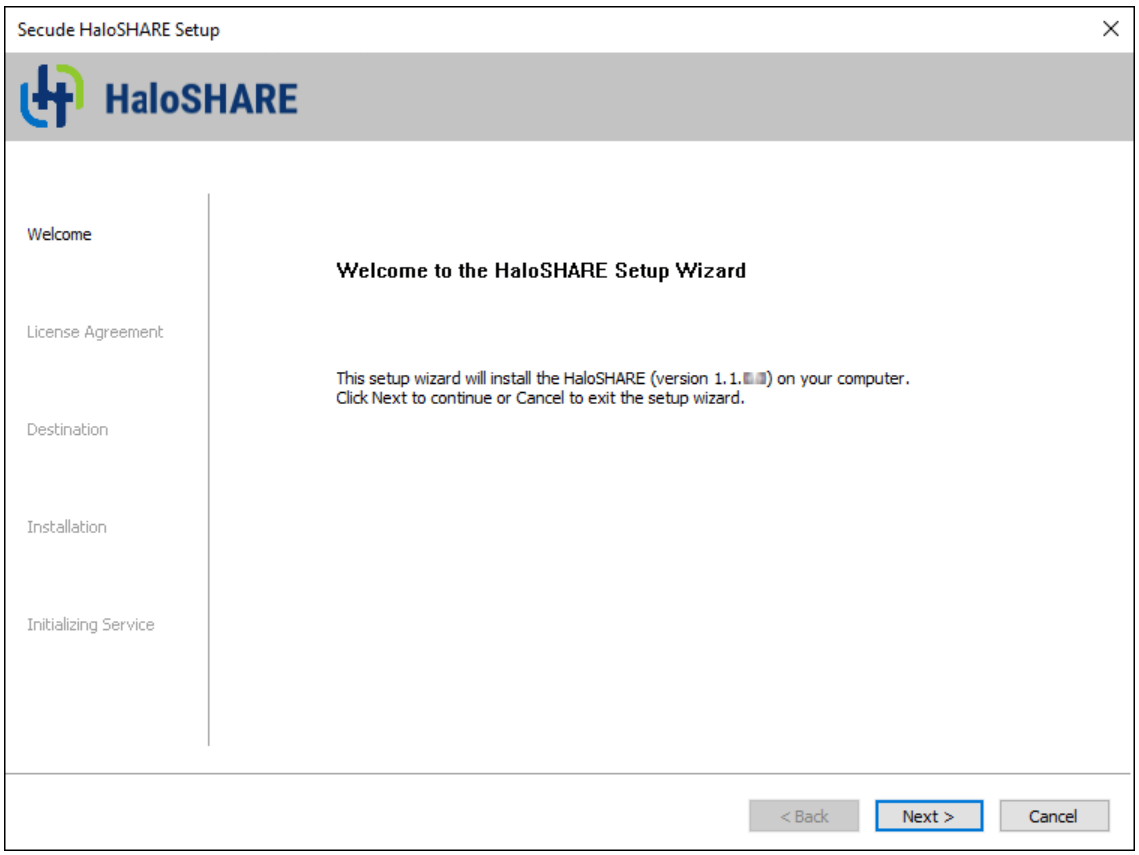
This chapter walks through the process of installing and configuring the HaloSHARE.

6.1. Interactive Installation

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

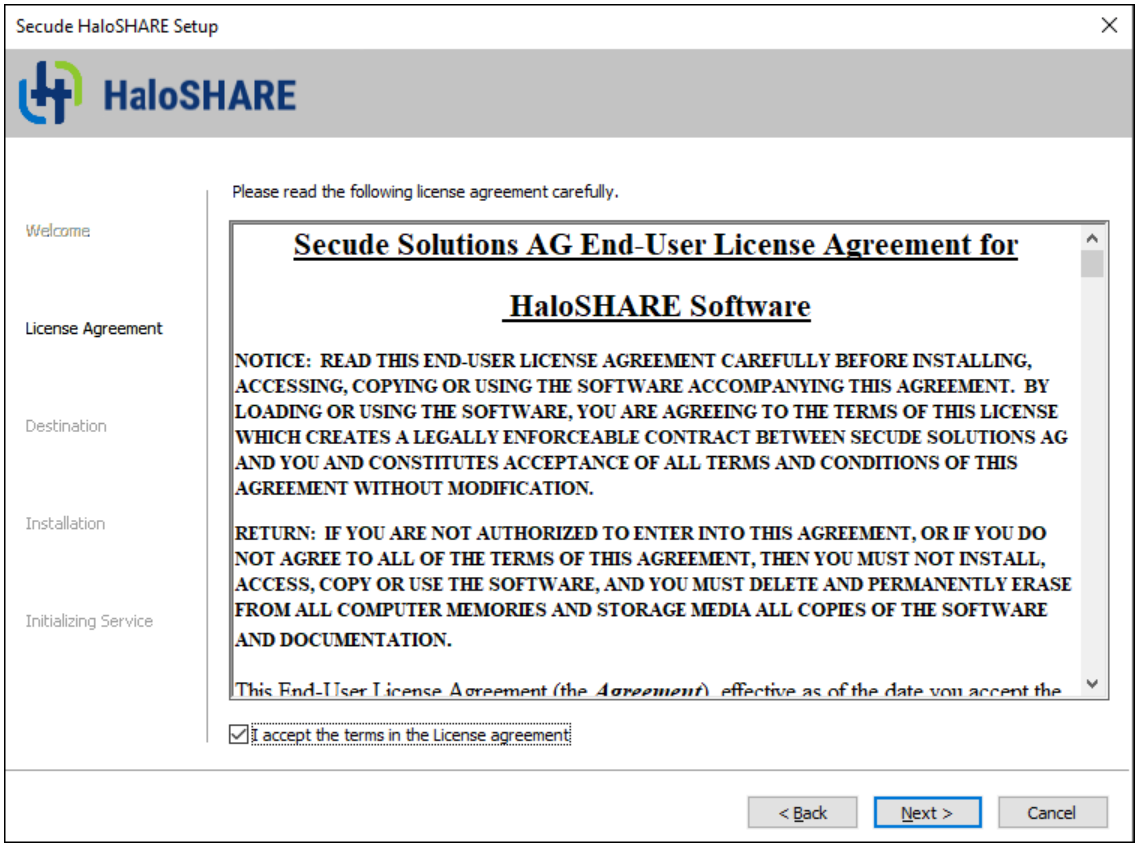
1. To begin the interactive installation, double-click the installer `HaloSHARE_Setup.exe` file. Depending on your Windows security settings, you may get a warning such as "*Do you want to allow the following program to make changes to this computer?*". If you get this security warning, click the **Yes**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

Startup dialog



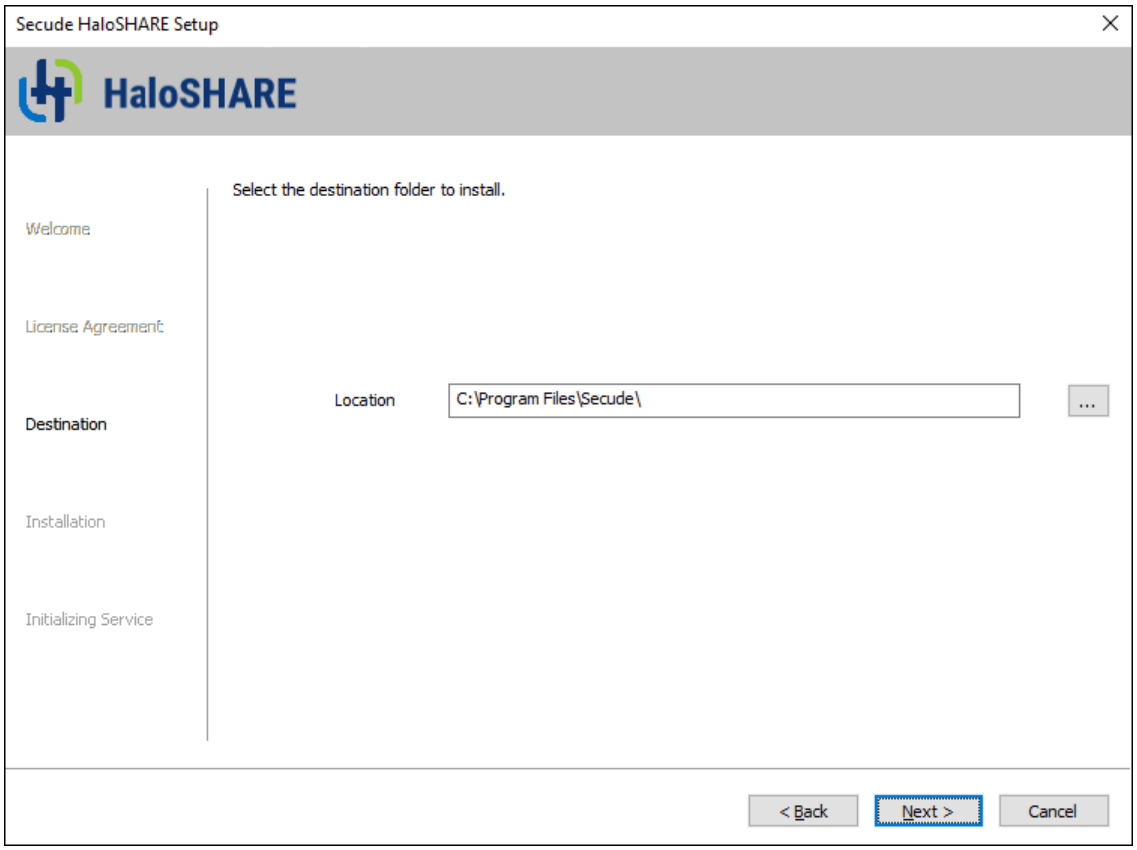
Welcome dialog

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



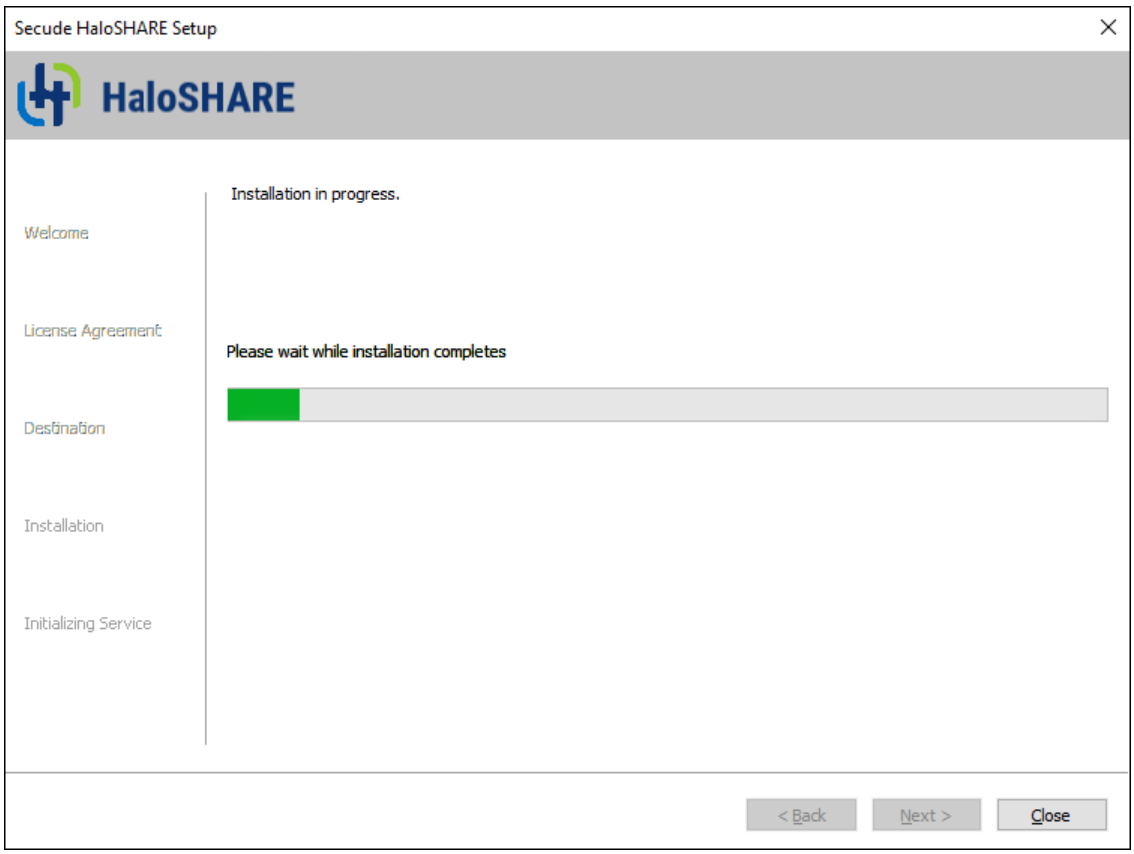
End-user License Agreement dialog

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



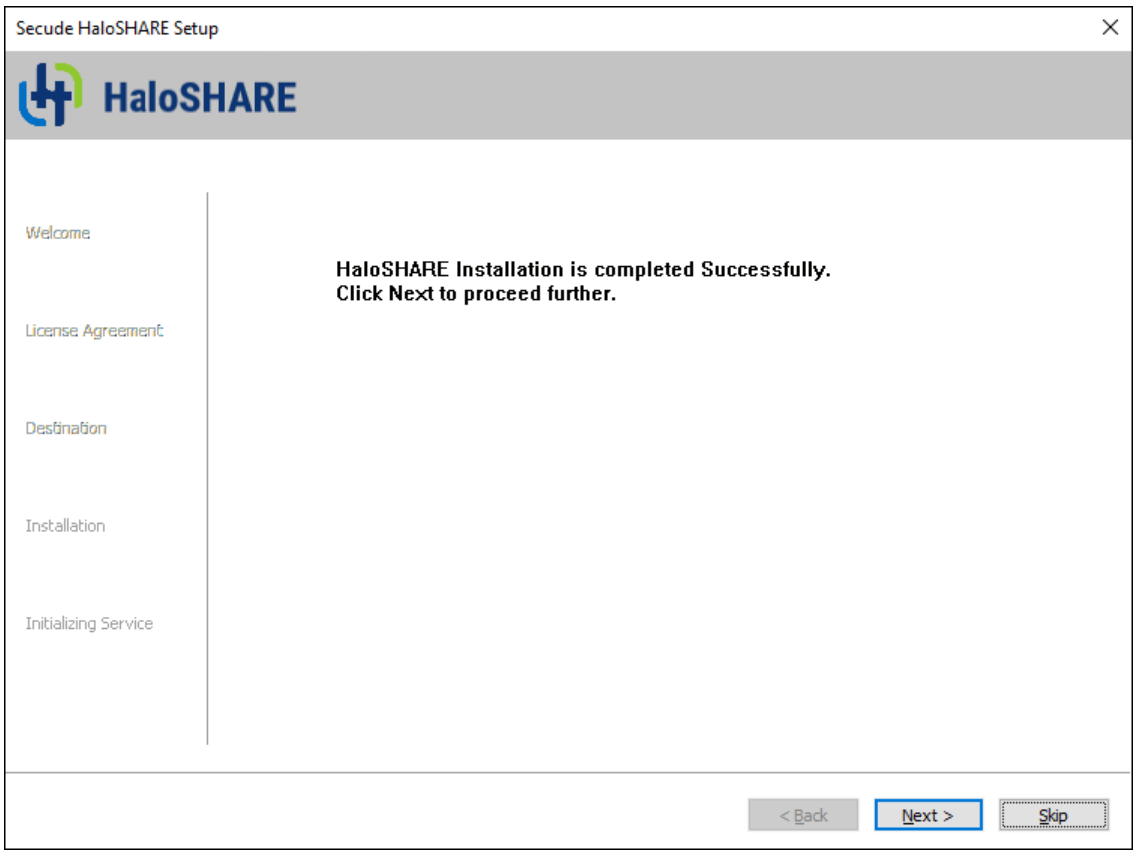
Destination folder selection dialog

6. By default, application files are stored in the program files directory (`C:\Program Files\Secude\`). If you would like to choose an alternate location, click the **Browse** button and select your location preference. When you are finished, click **Next**.
7. The installation starts with a progress bar that displays the status of the process.



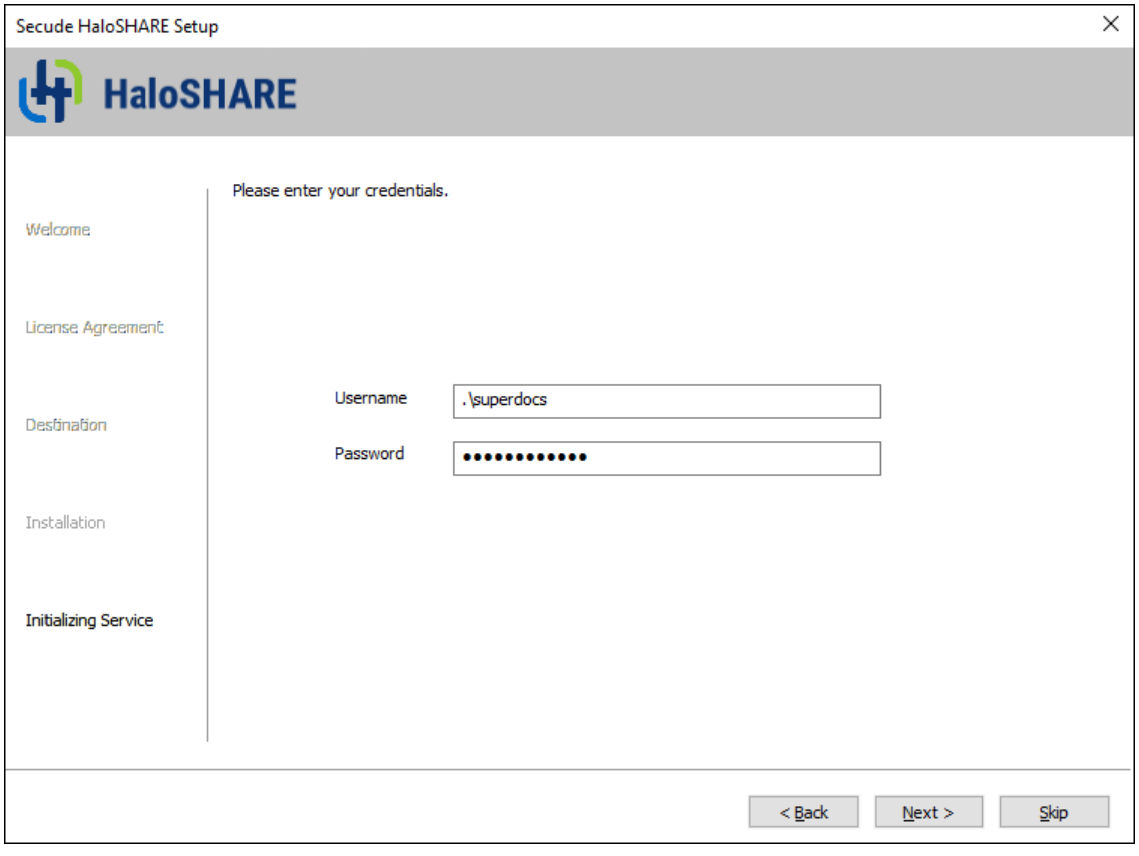
Installation progress dialog

8. When the installation is completed, you will see a message confirming that the HaloSHARE has been successfully installed.



Installation completed dialog

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



User credential dialog

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

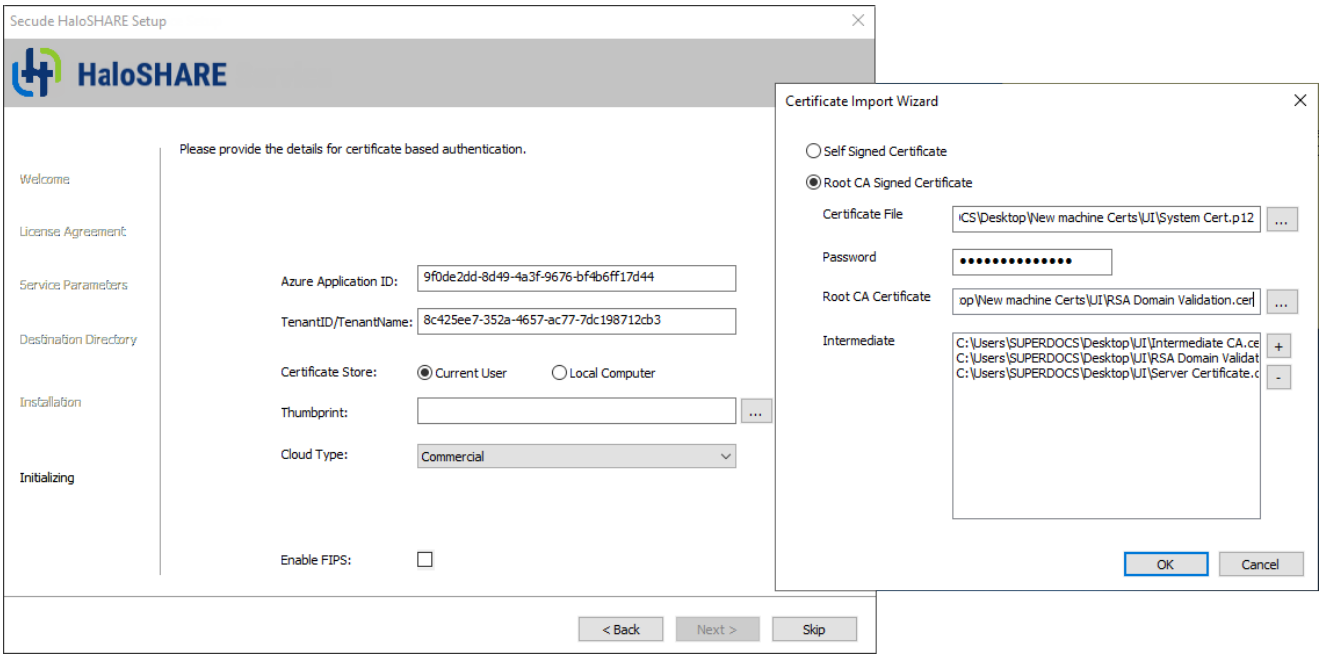
b. On a non-domain joined computer, you need to enter the username and password of a user. For example, `.\[user]`, `.\john`.

10. Click **Next**. The certificate based authentication dialog will appear. To avoid errors, please ensure that you enter the correct Azure application registration details in the installation wizard.

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

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

c. **Certificate Store Location**: 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, you need to enter the thumbprint manually. If the certificate is not installed, click the **Browse** button to select the necessary certificates as explained below:

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

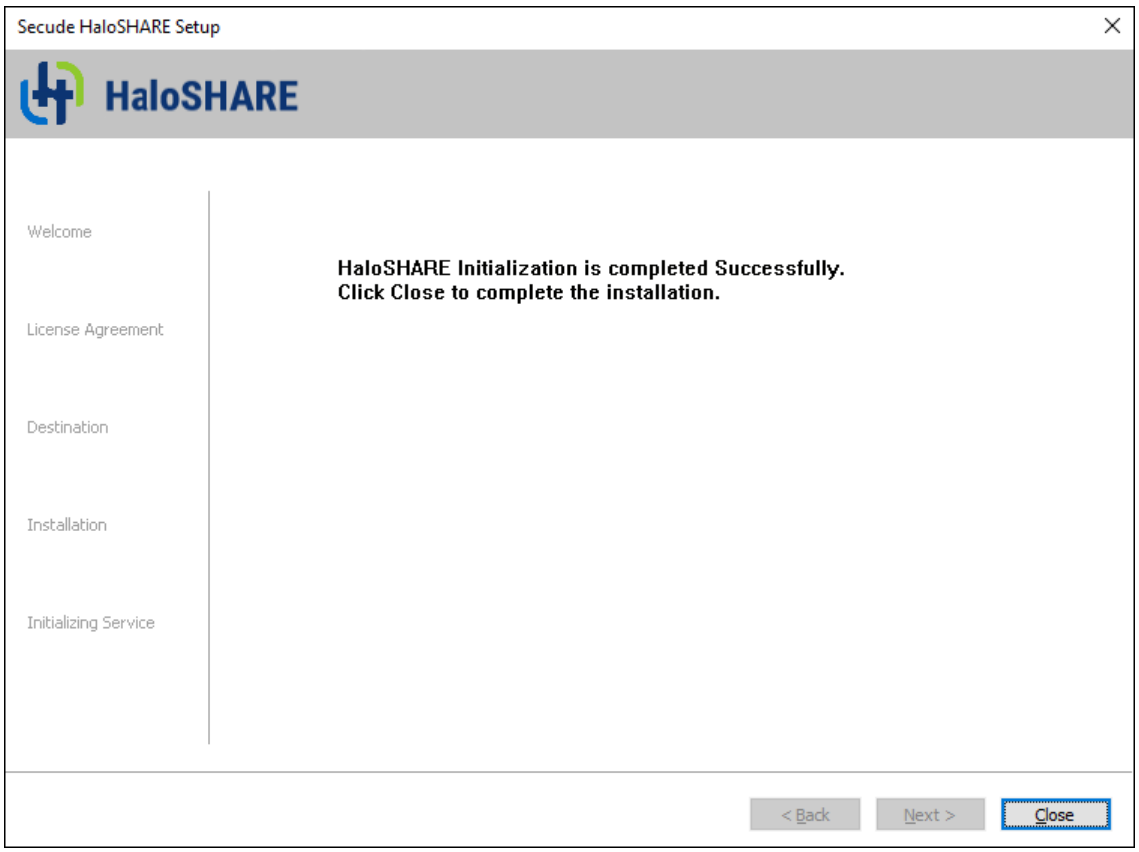
f. **Option 2: Root CA Signed Certificate**—select this option if you have a certificate that is signed by a CA. Click **Browse** button to select the signed certificate. The certificate path will appear in **Certificate File** field. Type its password in **Password** field. To select the Root CA (`.cer` / `.crt`), click **Browse** button in **Root CA Certificate** field. To select the intermediate CA certificates, click **Add** button in **Intermediate CA** field. In case, you want to remove a certificate from the "*Certificate Import Wizard*", click **Delete** button. Click **OK**, the thumbprint will be populated automatically.

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

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 MIP SDK Documentation "MIP SDK FIPS Compliance Statement".

i. Click **Next**.

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



Initialization completed dialog

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

Post-installation checks:

1. You can view the log files at `C:\Users\Username(user running service)\AppData\Local\Secude\HaloSHARE\log`.
2. You can see the configuration information of the HaloSHARE add-on in the registry—`HKEY_LOCAL_MACHINE\SOFTWARE\Secude\HaloSHARE`.
3. A protected policy XML file will be located at `C:\Users\Public\Secude\HaloSHARE`.

6.2. Update from Old to New Version

Prerequisite:

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

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

6.3. What to do next

After installing the HaloSHARE, you must configure it to meet your company's requirements. To learn how to configure it, please refer to the following chapter.

7. Configuring the HaloSHARE

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

7.1. License Activation

A license for a product is necessary for access to features and support, legal compliance, security, and reliability. The primary Secude licensing method uses a Key-based license that regulates and allows access to the application's features. Therefore, to enable features, we suggest obtaining the license key from Secude support before installing the HaloSHARE.

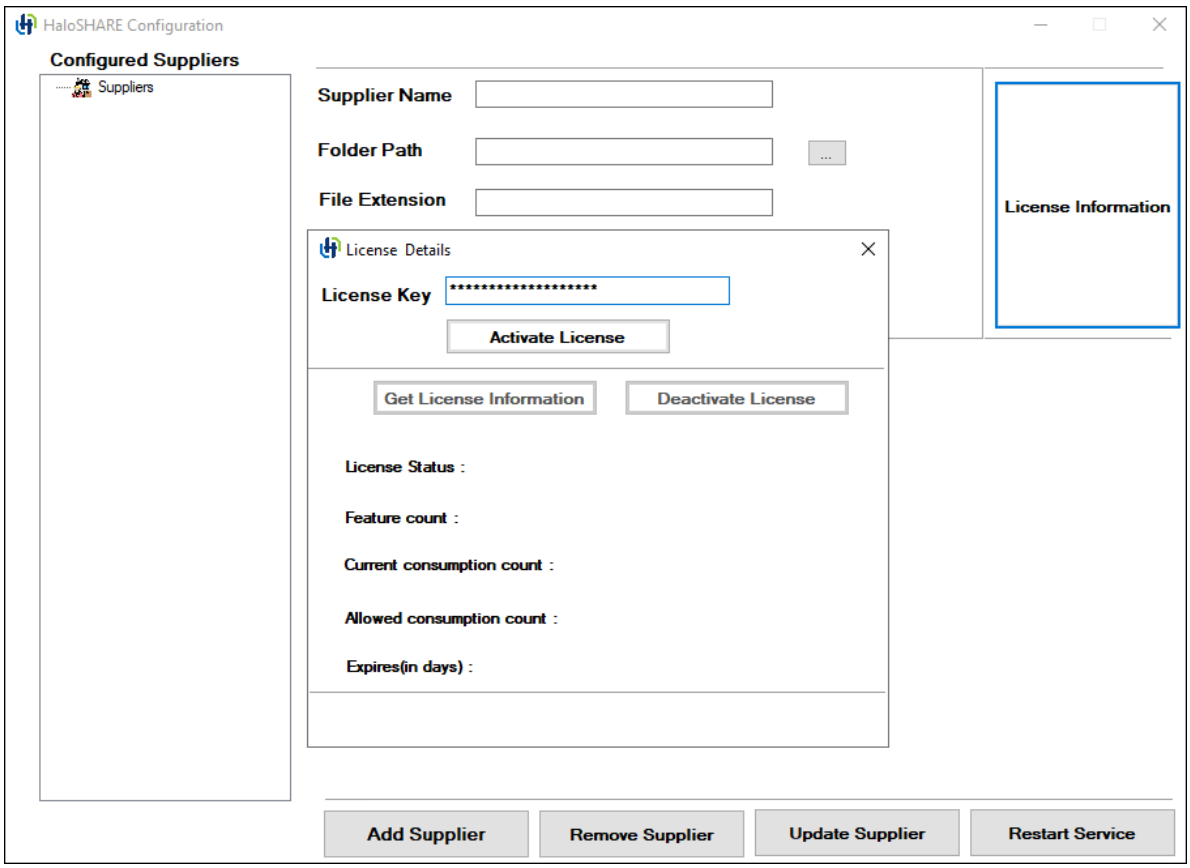
Key-based License

Upon purchase or registration with Secude, a special "license key" is provided to the user to control the use of the application. After installing the service, the administrator must enter the license key, which is an alphanumeric code, in the configuration tool to activate the license. By entering this key, the entire functionality of HaloSHARE is unlocked, and the user's authorization to use it is validated.

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

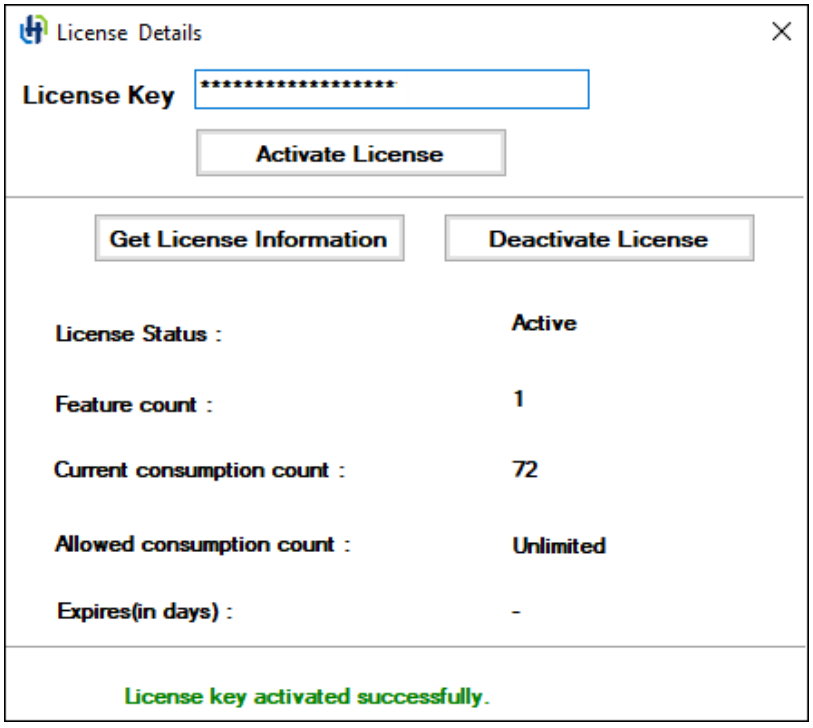
To complete the license activation, carry out the following steps:

1. Navigate to the destination folder you specified during installation. The default folder is `C:\Program Files\Secude\HaloSHARE`.
2. Run the program `HaloSHAREConfiguration.exe` with **Run as Administrator** permission.
3. The *HaloSHARE Configuration* screen will appear, and on the configuration screen, click **License Information**.
4. The **License Details** screen will appear as shown below:



HaloSHARE Configuration screen

5. Enter the license key provided to you by Secude and click **Activate License**.
6. Please be patient while the license key activation is completed.



License Information

7. You will receive a confirmation message after successfully activating the license.
    a. You will automatically receive detailed license information only the first time you activate the license. However, you can get the details at any time by clicking **Get License Information**.
    b. If the **License Status** is **Active**, it means you entered a valid license key, whereas a **license error** means you entered an incorrect license key.

Related tasks:

a. **License Deactivation:** Administrators may deactivate a HaloSHARE license for a variety of reasons, based on your organization's standards and specific scenarios. To do so, click on **Deactivate License**.
b. Please note that a license is deactivated automatically if HaloSHARE is uninstalled.
c. If your license expires, enter a new license and click **Update License**, or activate it using the tool `hsadm.exe`. For more details, refer to the section "Service Configuration using Admin Tool".

7.2. Supplier Configuration

HaloSHARE can encrypt files with either a Static Permission label or a Custom Permission.

Difference between Basic/Static Permission Labels and Custom Permissions

Static Permission Labels - These are sensitivity labels in which the administrator defines the permission set while defining the labels in the Microsoft Purview portal.

Custom Permissions - This is a list of permissions available for user selection in the HaloSHARE application UI. They are also known as user-defined permissions.

7.2.1. Quick Start on Configured Suppliers

The Configured Suppliers pane on the right side of the screen on the configuration tool displays a supplier and the folder path with whom you have shared sensitive business data. For example, if “Prestin Engineering” is a supplier and `C:\Prestin Engineering` is the source path where you store Prestin-related business data internally. Additionally, to share it with Prestin representatives in a shared folder, you would have a destination folder where files are copied from the source. You can configure similarly with different source and destination folders for other suppliers, such as "Manifold Dynamics" and "Oriental Construction".

1. File overwriting occurs when the same file is moved repeatedly to the same source folder.
    a. Case 1: Without the **Move to Destination Path** option.

       For example, suppose the source folder is configured with the text file extension and **Move to Destination Path** is not selected. Copy a text file (`sample.txt`) into the source folder. The file is encrypted and named `sample.ptxt`. If you place the same (`sample.txt`) file back into the source folder, the existing `sample.ptxt` is overwritten.

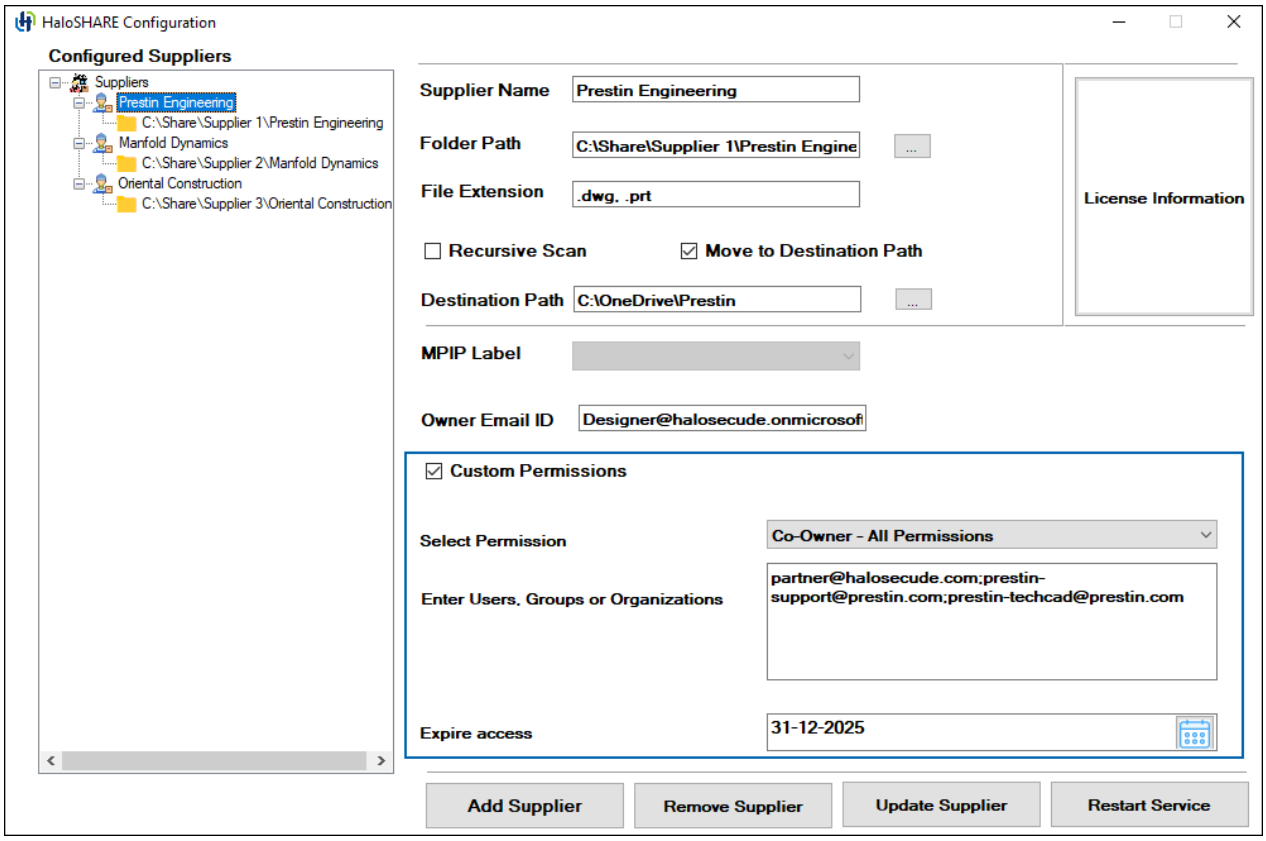
    b. Case 2: With the **Move to Destination Path** option.

       In this case, when a file is moved to the source folder, it is encrypted and sent to the destination folder. When you place the same file in the source folder, it is considered a new file, encrypted, overwritten, and moved to the destination folder.
2. It is not allowed to set the same folder or subfolder path for more than one supplier.
3. Both the OneDrive service and our HaloSHARE service cannot access the same file at the same time. There will be an access violation or access denied error.

7.2.2. How to Configure HaloSHARE

Follow the steps below to configure HaloSHARE:

1. Navigate to the destination folder you specified during installation. The default folder is `C:\Program Files\Secude\HaloSHARE`.
2. Double-click on the `HaloSHAREConfiguration.exe` file.
3. The *HaloSHARE Configuration* screen will appear as shown below:



HaloSHARE screen

4. Enter the supplier's name in the **Supplier Name** box, whose files must be protected. For example, `Prestin Engineering`
5. Click the **Browse** button next to the **Folder Path** to select the source folder that HaloSHARE should monitor. For example, `C:\Supplier 1\Prestin Engineering`
6. Enter the file extension in the **File Extension** box. By defining the extensions, protection will only apply to the specified file extension, leaving other files in the source folder unencrypted. For example, `.dwg`, `.prt`. Note: If you mention asterisk symbol (*) the following files will be included by default for protection `.prt`, `.asm`, `.sec`, `.frm`, `.drw`, `.lay`, `.cem`, `.mfg`, `.neu`, and `.log`. You may also add Creo file formats along with iteration. For example, `.prt.1`.
7. Select the **Recursive Scan** option to scan all subfolders within the source folder and encrypt the files within them. If this option is not selected, encryption is only performed on the source folder.

8. Select the **Move to Destination Path** option to move the encrypted files from the source folder to the destination folder. The destination folder can be another shared folder where you store files for external access, such as those associated with a supplier, vendor, or external consultant. For example, the destination folder could be a OneDrive folder.
9. Click the **Browse** button next to the **Destination Path** to select the destination folder. HaloSHARE will copy the encrypted files to this destination folder, which is accessible to the specified supplier. For example, `C:\OneDrive\Prestin`. As a result, the files from **Folder Path** (`C:\Supplier 1\Prestin Engineering`) will be moved to **Destination Path** (`C:\OneDrive\Prestin`).
10. Select a suitable label.
    a. Select a label from the **MPIP Label** list based on the level of authorization you want to provide the supplier. For example, `HCAD Confidential`. Alternatively, you can select a label with no encryption settings. In this case, you will receive a message "*The selected MPIP label has no encryption settings and can only be applied to MIP SDK-supported file types.*". If you want to apply such a label, enter the file types that are supported, such as `.txt`, `.docx`, and `.pdf`.
    b. Alternatively, you can use a custom permission label. Please skip to point 12.
11. If you want to give a user full access to the file, i.e. make a user the owner of the file, enter a user email ID in the **Owner Email ID**. For example, `Designer@halosecude.onmicrosoft.com`
12. Select **Custom Permissions** if you want to set the permission now or if the MPIP label has not yet been defined. The author can assign permission to users, groups, or organizations based on the permission level.
    a. From the **Select Permissions** list, select the level of access you want the users to have when you protect the file (Viewer - View Only / Reviewer - View, Edit / Co-Author - View, Edit, Copy, Print / Co-Owner - All Permissions / Only for me). To know the usage rights of the permissions, please refer to the section "Permissions Level and Usage Rights".
    b. Specify the users who should have permission to access your file in **Enter Users, Groups or Organizations**. Type their full email address, a group email address, or a domain name from the organization for all users in that organization separated by comma or space or semicolon. For example `partner@halosecude.com;prestin-support@prestin.com;prestin-techcad@prestin.com`
    c. You can specify how long the labeled file can be accessed in the **Expire access** field. Use the **Never** option if you want the label to never expire and to have unlimited access to the file. It can be used for less sensitive content. Alternatively, for highly sensitive content, select a date on the calendar so that recipients other than the owner cannot access the file after the expiry date.
13. Click **Add Supplier** and then click **Restart Service**. Repeat the previous steps to add more suppliers.

Results:

a. You will see a confirmation message after the supplier has been successfully added.

b. The name of the supplier will be added to the list on the left pane.

c. The supplier detail can be viewed on the right pane by clicking the supplier name node.

d. You will see a confirmation message after successfully restarting the service.

Related tasks:

a. To remove a supplier from the list, click **Remove Supplier**.

b. If you make changes to the configuration, click **Update Supplier** to make the changes take effect.

c. Remember to restart the HaloSHARE after making changes.

d. You can find license and service information in the log `C:\Users\UserName\AppData\Local\Secude\HaloSHARE\log`.

What happens to unconfigured file types?
Any files that are not specified in the HaloSHARE settings should be shared with caution. If you have configured **Move to Destination Path**, these files will be moved to the destination folder unprotected. Users must therefore be aware of this type of file sharing.

7.2.3. How to Relabel a File or Modify the Applied Label

A designer may need to relabel files in the supplier folder for a variety of reasons, and in some cases, they may decide to remove protection. To accomplish this purpose, HaloSHARE provides the option to remove protection and relabel features by setting the registry key `enable_relabeling=on`.

1. Files encrypted with MPIP label can be relabeled with Custom Permissions, and vice versa for files encrypted with Custom Permissions.
1. Files encrypted with Custom Permissions can be decrypted using the Remove Protection label.

Prerequisites:

1. Make sure you are the owner of the document, a user with superuser privileges, or a user with export permissions assigned to an already applied label.
2. Make sure that the API permission for relabeling has been configured in the application. For more information, refer to the section “Additional Permission (Only for Relabeling)”.
3. Enable the relabel feature by changing the registry key `enable_relabeling` from `off` to `on`. For more information, please refer to the section "Registry Settings".

Follow the procedure to relabel.

1. Double-click on the `HaloSHAREConfiguration.exe` file.
2. On the *HaloSHARE Configuration* screen, change the label as needed. Please note that applying the **Remove Protection** label will remove protection.
3. Click **Update Supplier** and then click **Restart Service**.

   Results:

   a. Relabeling: The files in the supplier folder will be updated with the new label.

   b. Removing protection: The files in the supplier folder will be successfully decrypted.

7.3. Service Configuration using Admin Tool

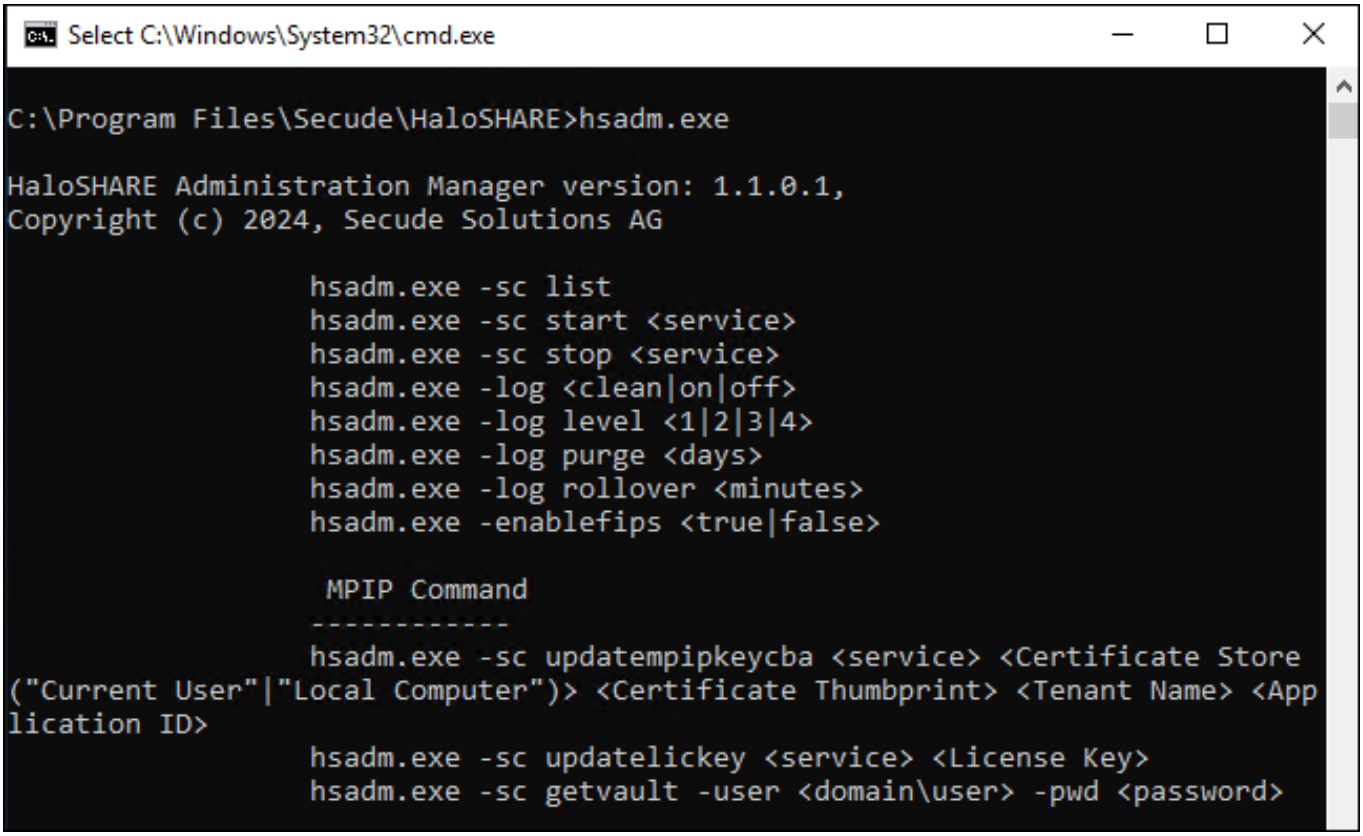
After installing the HaloSHARE, you may want to change the configuration. To do so, run the tool `...\Secude\HaloSHARE\hsadm.exe` to view the commands. Please note that the admin tool does not support uppercase.

How to update MPIP labels in HaloSHARE?

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

When is it necessary to restart the HaloSHARE service?

Whenever you modify the HaloSHARE registry settings, then 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 the HaloSHARE. Note: This can be used only after setting user credentials to run HaloSHARE.

For example,

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

Output

```
Service Started successfully.
```

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

Use this command to stop the HaloSHARE.

For example,

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

Output

```
Service Stopped successfully.
```

Log Command

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

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

For example,

```
hsadm.exe -log on
```

Output

```
Current log enabled, level = 3.

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

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

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

For example,

```
hsadm.exe -log level 4
```

Output

```
Current log enabled, level = 3.

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

```
hsadm.exe -log purge <days>
```

Use this command to set a time for log purging, i.e., the no. of day(s) by which the logs will be deleted.

For example,

```
hsadm.exe -log purge 2
```

Output

```
Current log enabled, level = 4.

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

```
hsadm.exe -log rollover <minutes>
```

Use this command to set a log rollover time, i.e., the minute(s) by which a new log file will be generated.

For example,

```
hsadm.exe -log rollover 60
```

Output

```
Current log enabled, level = 4.

INFO,Log files rollover set to 60 minute(s).
```

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
```

```
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.
```

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 wanted. Any changes to the registry will require a restart of the HaloSHARE to take effect.

Name	Default value	Type	Description
dir_common	`common`	REG_SZ	The path to the directory where all the dependent DLL files are stored for the execution of HaloSHARE.
dir_log	`log`	REG_SZ	Log files are generated in the service running user's local profile i.e., in the following location `%LOCALAPPDATA%\Secude\HaloSHARE\log`.
dir_tmp	`tmp`	REG_SZ	It stores the temporary files located at `%LOCALAPPDATA%\Secude\HaloSHARE\tmp`.
dir_vendor	`C:\Program Files\Secude\`	REG_SZ	This is the Secude's vendor directory under which Secude's components will get installed. For example, `HaloSHARE`.
enable_fips	`false`	REG_SZ	1. true: By selecting this option, MPIP only uses FIPS-compliant encryption algorithms. 2. false: MPIP uses standard encryption algorithms.
enable_relabeling	`off`	REG_SZ	Defines the status of the relabeling. • On = Relabel feature is enabled to change the applied label • 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 = Log file will be generated in the default location • Off = Log file will not be generated • Clean = Log files will be deleted. This parameter deletes only the logs and does not modify the log_enable to "Clean" from "on/off".
log_level	3	REG_SZ	• Log level: 1: Error and Info • Log level: 2: Error, Warning, and Info • Log level: 3: Error, Warning, and Info • Log level: 4: Error, Warning, Info, and Debug
log_purge	7	REG_SZ	It indicates removing files older than a defined time frame. By default, the log files older than 7 days will be deleted.
log_rollover	100	REG_SZ	Defines the log rollover time, i.e., a new log file will be generated based on the specified minute(s). By default, a new log file will be generated every 100 minutes.
ls_proxy		REG_SZ	Allows you to use a proxy server to access Secude's License Manager. This is an optional feature that must be utilized only 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	It indicates the service's waiting time and begins scanning after 5 seconds if the folder has not been modified.

Name	Default value	Type	Description
templatefile_purge	1	REG_SZ	Defines the purge time of template files that are generated for every CAD assembly file (compound file) download. The default value set is one hour. For example, when a file is downloaded at 15:25 hours, the HaloSHARE service creates a template file in the tmp\GUID folder (which can be located in the HaloSHARE service user's profile folder). In the background, it examines and deletes the files which had reached the configured time i.e., after 16:25 hours. Note: This is only applicable in the event of CAD assembly file labeling.
version		REG_SZ	The version number of the installed service.

Configuration in the Registry

7.5. Configuring Endpoint

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

Name	Default value	Type	Description
block_pii	`false`	REG_SZ	Enable or disable the visibility of Personally Identifiable Information (PII) in the MIP SDK logs. The MIP SDK logs are located at`%LOCALAPPDATA%\Secude\HaloSHARE Service\log\mip_cache_storage\mip\logs\mip_sdk.miplog`. • false—PII will be visible in clear text in the MIP SDK logs. • true—PII will be masked with asterisks in the MIP SDK logs. This helps to protect the PII's confidentiality.
cachetype	1	REG_SZ	MPIP cache storage type used by the service. • In Memory—0, maintains the storage cache in memory in the application. • On Disk—1 (default storage type), stores the database (SQLite3) on disk in the directory provided in the settings object. The database is stored in plaintext. • On Disk Encrypted—2, stores the database (SQLite3) on disk in the directory provided in the settings object. The database is encrypted using OS-specific APIs.
cacheuserlicense	1	REG_SZ	• 0—false, End User License (EUL) will NOT be stored in the MPIP cache storage. • 1—true (default value), End User License (EUL) will be stored in the MPIP cache storage.
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 HaloSHARE service runs
databoundary	Default	REG_SZ	Audit and telemetry events are sent to the nearest collector, where these events are stored and processed. Other options: 1. Asia 2. Europe_MiddleEast_Africa 3. European_Union 4. North_America For example, if your AIP administrator sets North_America, the HaloSHARE service forces all telemetry and audit data to go directly to North America.
domain		REG_SZ	Name of the domain.
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 in order to track the file. • 0 (default value)—the content ID does not get extracted for the use of File Tracking. • 1—the content ID will be extracted for the use of File Tracking.

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	MSALCBA	REG_SZ	Type of authentication method (MSALCBA).
mode	MPIP	REG_SZ	MPIP
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.
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 10MB.

Configuring Endpoint

7.6. How to Access Protected Files

After setting HaloSHARE in your environment, you may start sharing business files in folders. Once the files have been protected, you should know how to open MPIP-protected files with HaloCAD Add-ons. Please look in the respective manuals to learn more about how HaloCAD add-ons work.

8. Troubleshooting

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

8.1. Installation Interrupted due to Improper Configuration

Symptom

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

Background

The error message given above appears while installing the HaloSHARE.

Probable Cause

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

Recommended Action

Verify and enter the correct certificate password.

8.2. Installation Interrupted due to Certificate

Symptom

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

Background

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

Probable Cause

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

Recommended Action

1. Verify the certificate using the Microsoft Management Console (MMC) snap-in.
    a. If the certificate is invalid, add a new certificate.
    b. If you proceed to install HaloSHARE at this point, you will receive the following message "*Please check the certificate validity and details, Verify the certificate is installed properly and configured in the Azure portal.*"
2. Make sure that the same certificate is updated on the Azure portal (under the **Certificate** section > click **Upload certificate**).
3. Continue with the installation now.

9. Appendix

This section provides supplemental information.

9.1. Open-source Software

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

The third-party libraries and dependencies used by HaloSHARE are shown in the table below.

Library	Version	Source Code	License Link
Boost Library	1.85.0	https://boostorg.jfrog.io/artifactory/main/release/1.79.0/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	1.15.94	https://learn.microsoft.com/en-us/information-protection/develop/version-release-history	https://docs.microsoft.com/en-us/information-protection/develop/
Licensespring	7.32	-	-
OpenSSL	3.2	https://github.com/openssl	https://github.com/openssl/openssl/blob/master/LICENSE.txt
MSAL	4.61.3	https://github.com/AzureAD/microsoft-authentication-library-for-dotnet	https://github.com/AzureAD/microsoft-authentication-library-for-dotnet/blob/master/LICENSE

Open-source software

9.2. Permissions Level and Usage Rights

9.2.1. Basic Permissions

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

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

Basic Permissions

Author (creator) of a file

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

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

9.2.2. Custom Permissions

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

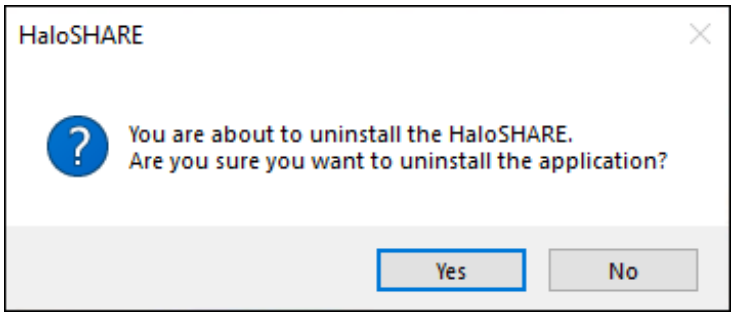
S.No	Permission Level	Usage Rights (Allowed Recipient Actions)
1	Viewer	Open and read the data (also known as “Read-only”). It includes Zoom and view from different angles.
2	Reviewer	Viewer’s allowed permissions plus: 1. Edit 2. Save the file
3	Co-Author	Reviewer’s allowed permissions plus: 1. Print 2. Extract data (including screen captures) from the file into the same or another file.
4	Co-Owner	Co-Author’s allowed permissions plus: 1. Export 2. Change Rights
5	Only for me	Grants all rights to the file and all available actions can be performed only by the author of the file.

Custom Permissions

9.3. Uninstallation

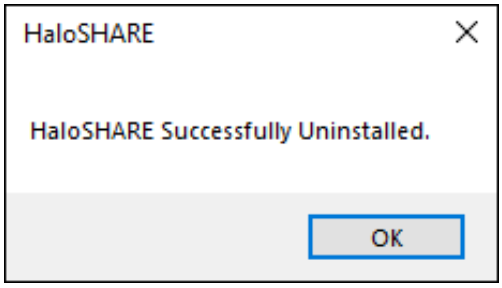
When you no longer use the service, you may uninstall the application. Uninstalling removes all files and registry settings that were added to your computer during the initial installation.

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 will appear.



Uninstall message #1

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



Uninstall message #2

Index

Secude

www.secude.com

About Secude

Secude, a Microsoft and SAP Partner, is a global leader for Zero Trust Data-centric security and Enterprise Digital Rights Management (EDRM) solutions.

For more than 25 years Secude has been trusted by many Fortune 500 and DAX-listed companies for architecting, implementing, and protecting their data. Our data-centric security professionals apply their passion and deep domain expertise to provide a holistic approach to protect priceless Intellectual Property (IP) in CAD & SAP based collaborations and supply chains.

With branches in Europe, North America and Asia, Secude supports customers with the implementation of IT security strategies through a global network.