Secude

HaloCAD

HaloCAD Prerequisites

1. Prerequisites

The prerequisites and dependencies for installing and configuring the HaloCAD add-ons are summarized in this section.

1.1. Register an Application in Microsoft Entra ID

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

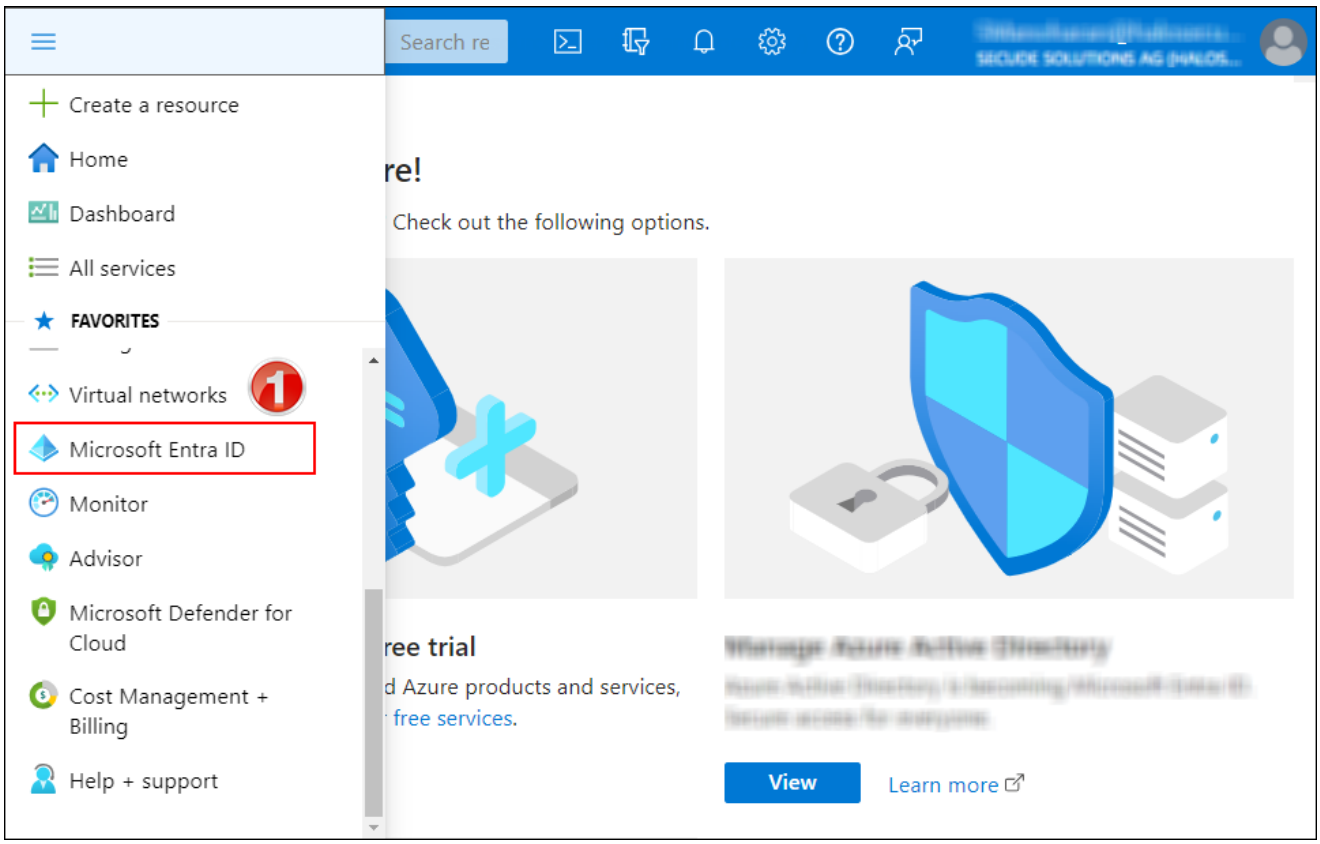
Microsoft documentation

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.

1.1.1. Create an Application

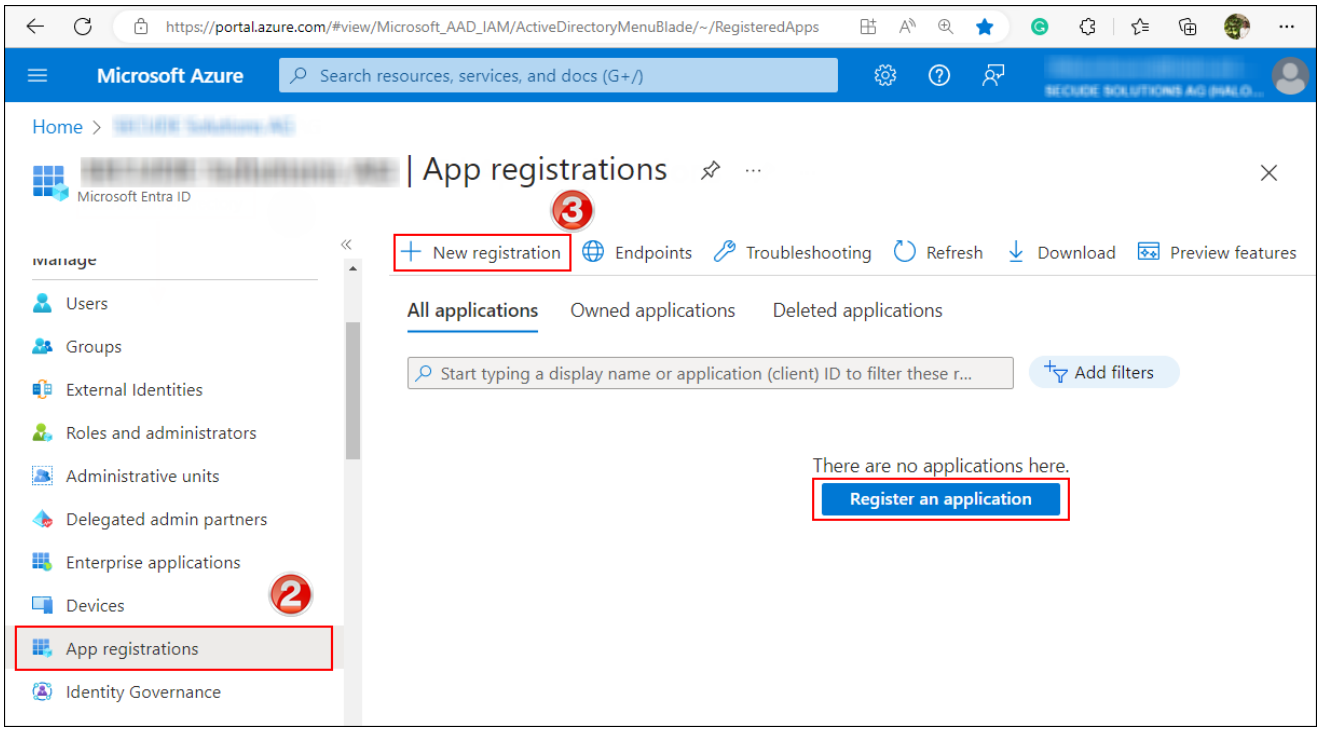
Follow the instructions below to register an application:

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**.



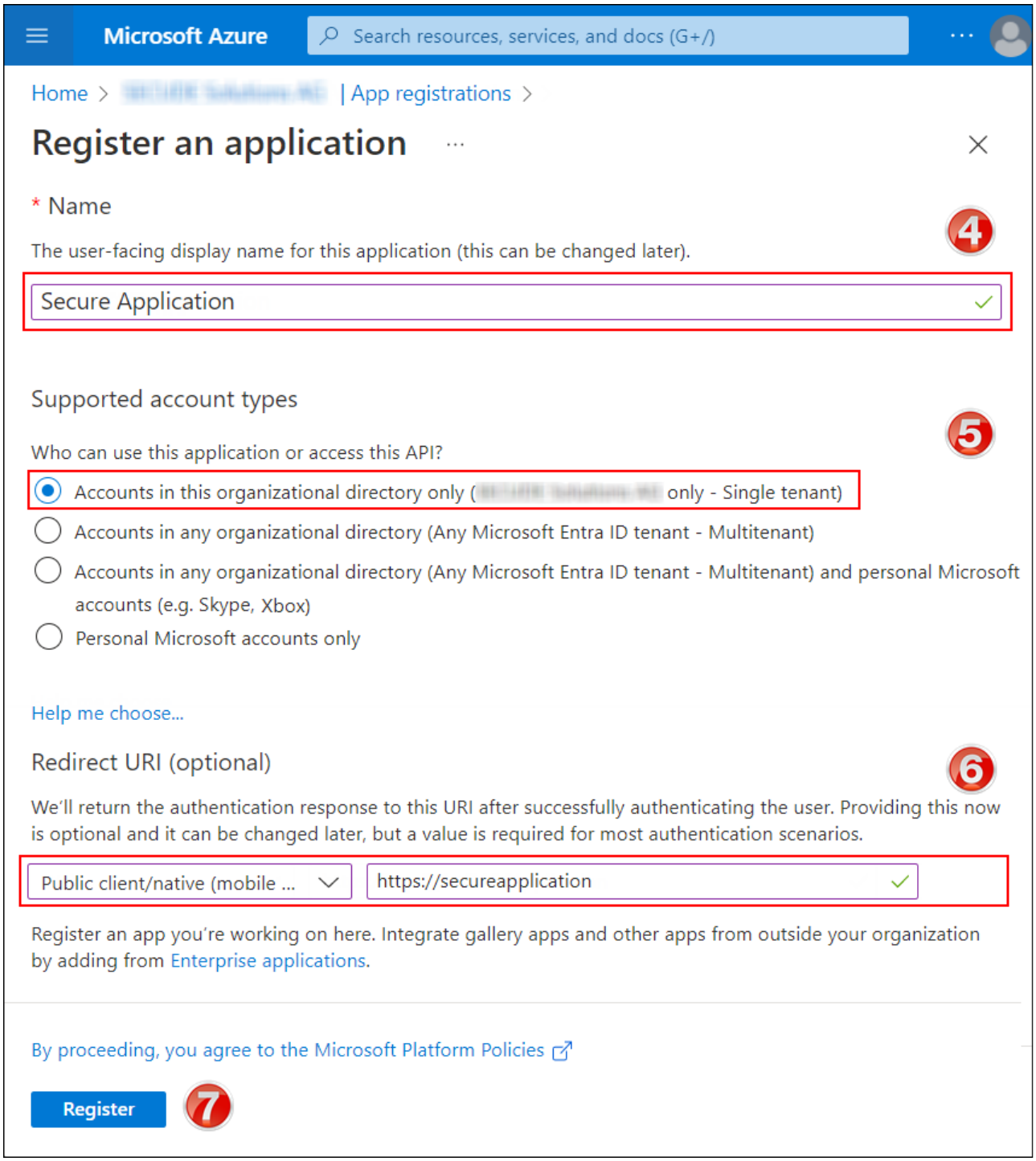
Selecting Microsoft Entra ID

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.



Public client application details

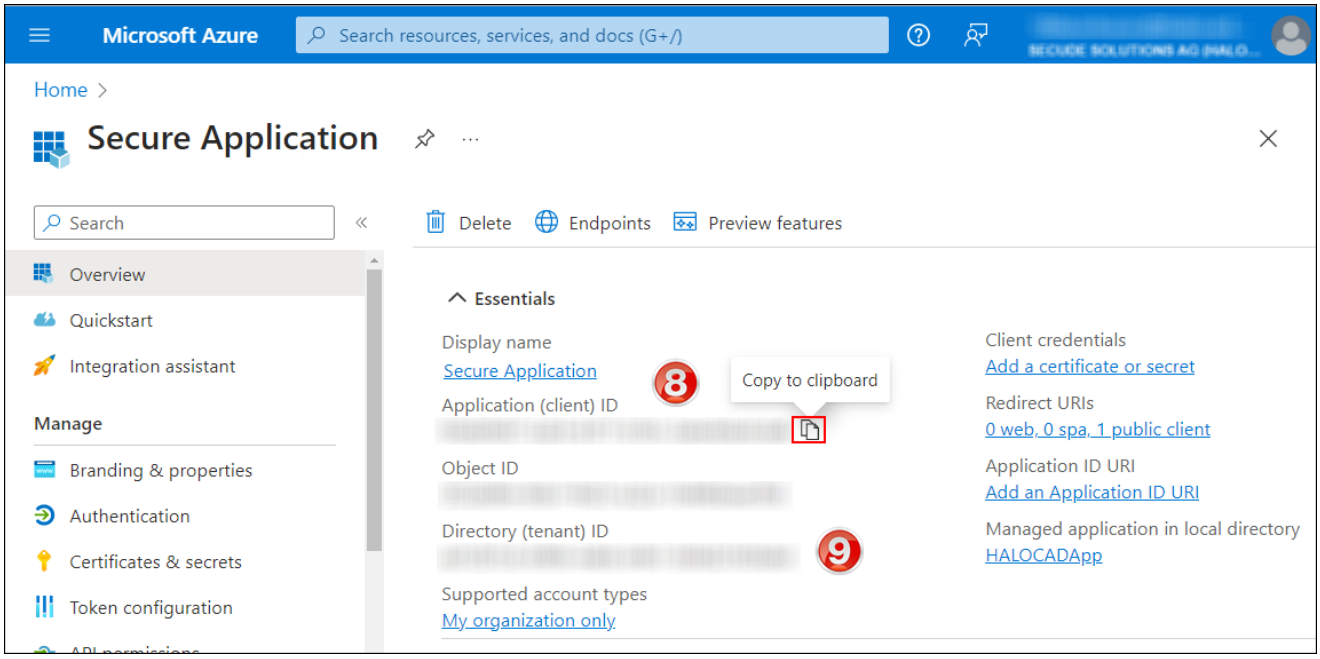
6. In the **Name** section, enter a meaningful application name.
7. Under **Supported account types**, select which account you would like your application to support. For detailed information on these types, please see Microsoft documentation.
    a. To target only accounts that are internal to your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

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

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

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

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



Application ID and Tenant ID

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

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

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

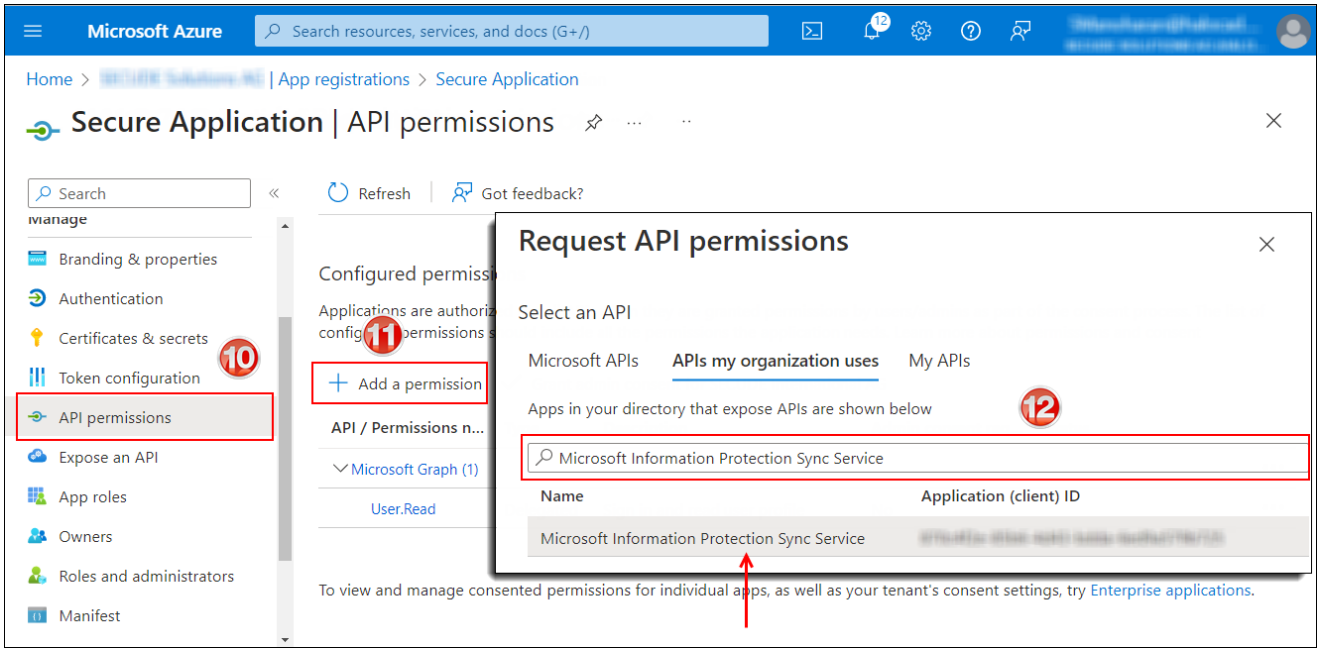
Save the authentication parameters

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

1.1.2. Add Required Permissions

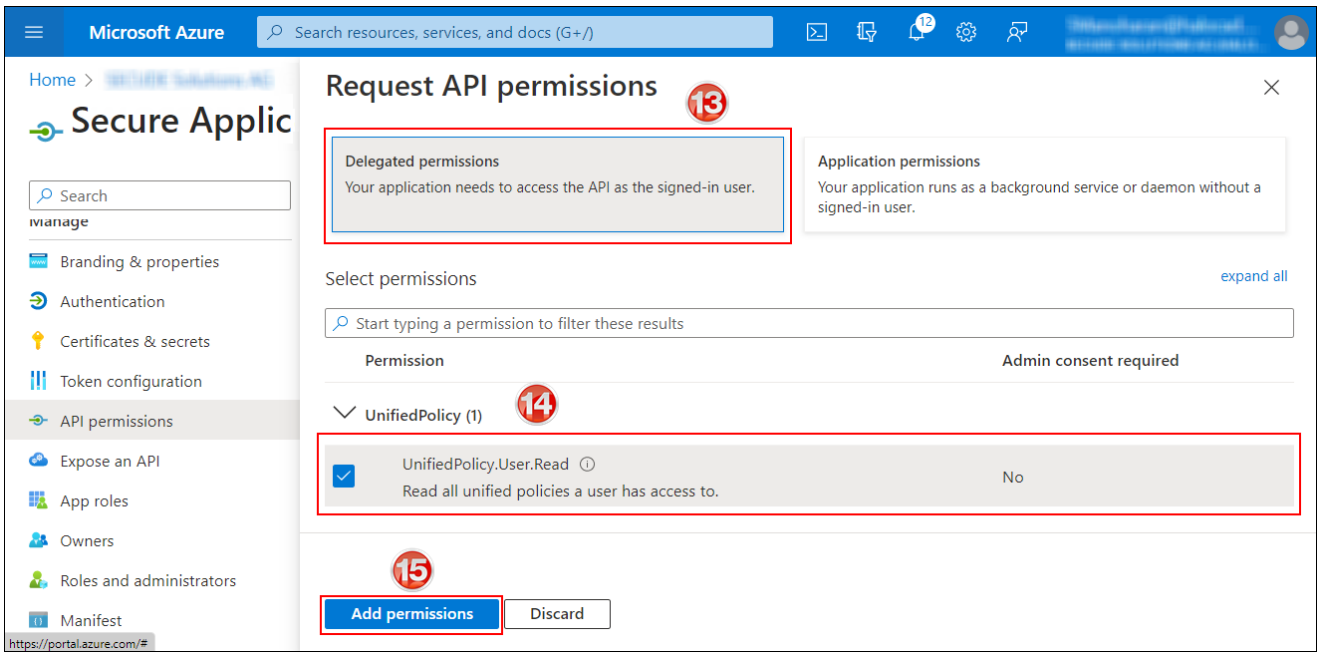
To protect content using MIP SDK, you need to provide the following API permission(s) for the created application ID.

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



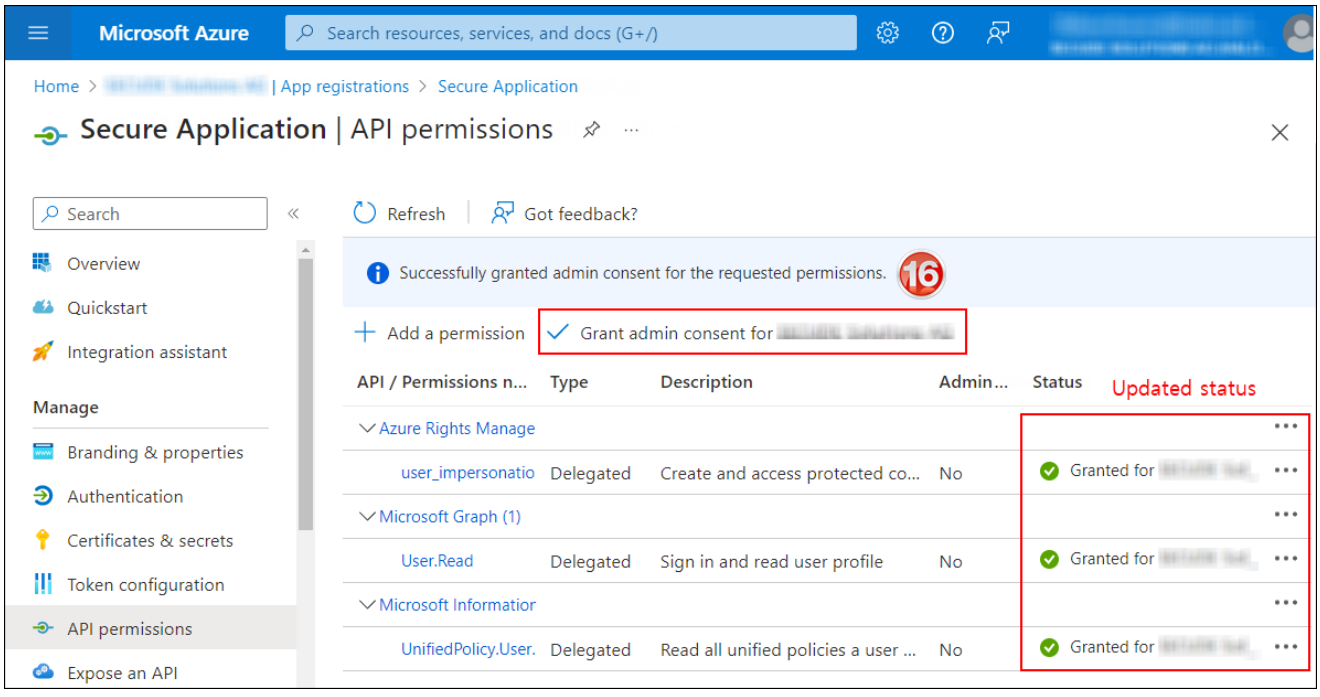
Searching permissions

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



Adding permission

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



API Required permissions

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

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

Required permissions

1.2. Create and Configure the Sensitivity Labels

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

1.3. Office 365 Subscription Details

1. Fully configured Azure Information Protection.
2. An Azure subscription is required to use Azure RMS and the MPIP functionality.
3. A working Microsoft Entra ID service must be available.
4. Transport Layer Security (TLS) 1.2 or higher must be enabled to ensure the use of cryptographically secure protocols at all client workstations. Please refer to the section "Enable Support for TLS 1.2 at the Client Workstation for Microsoft Entra ID".
5. To avail revoke access feature, the user should be assigned to Azure Information Protection Premium P1/P2 license. (Not required for reader add-on)
6. Audit logging: Your Azure subscription must include Log Analytics on the same tenant as Azure Information Protection.

1.4. Recommended URLs, Addresses, and Ports for MPIP

MIP SDK doesn't support the use of authenticated proxies. So, make sure you set the Azure Information Protection 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 US Government	`https://login.microsoftonline.us`
Microsoft Entra ID (global service) For details on Microsoft Entra ID endpoints, please refer to "Microsoft Online Documentation".	`https://login.microsoftonline.com`

Recommended endpoints

Secude License Manager for HaloCAD

To communicate with Secude License Manager for HaloCAD, 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

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

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

- TLS 1.1
- TLS 1.0
- 3DES cipher suite (TLS_RSA_WITH_3DES_EDE_CBC_SHA)

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

Microsoft documentation

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

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

In summary, the following steps must be performed:

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

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

Registry entries