



**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**.

#### Secude Ŗ ন্দ ≡ Search re >\_ Û ្មើរ ? SECURE SOLUTIONS AS (HA + Create a resource 合 Home re! 📶 Dashboard Check out the following options. 📃 All services ★ FAVORITES J Virtual networks 🔶 Microsoft Entra ID 🕑 Monitor 🗛 Advisor Microsoft Defender for Cloud ree trial Whereaster Weissen Weiligen Characterity d Azure products and services, a Welling (Hing Here, A Her contring / Microsoff (1964a) (H) 💿 Cost Management + free services. er second für mennete Billing Relp + support View Learn more 🗹

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 h	nave already been	created).

$\leftarrow$ C $\bigcirc$ https://portal.azure.com/#view	v/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/~/RegisteredApps	표 A @ ★ 🞯 🤃 🖆 🍘 …
■ Microsoft Azure	h resources, services, and docs (G+/)	🕸 🕐 🕅 SECLICE SOLUTIONS AG (SALO., 🎱
Home > The second secon		
Microsoft Entra ID	App registrations 🛷 … 3	×
іліанауе «	+ New registration 🕀 Endpoints 🤌 Troubleshow	oting 💍 Refresh 🞍 Download 💀 Preview features
🚨 Users	All applications Owned applications Deleted	applications
🍰 Groups		
龏 External Identities	Start typing a display name or application (client) II	D to filter these r 'Y Add filters
👃 Roles and administrators		
Administrative units	Th	ere are no applications here.
🚸 Delegated admin partners		Register an application
Enterprise applications		
Devices		
App registrations		
Identity Governance		

New application registration

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

	$\mathcal P$ Search resources, services, and docs (G+/)	🙆
Home >	App registrations >	
Register an app	lication	×
* Name		
The user-facing display name	for this application (this can be changed later).	•
Secure Application		~
Supported account type	S	0
Who can use this application of	or access this API?	6
• Accounts in this organiza	tional directory only ( only - Single tenant)	
<ul> <li>Accounts in any organiza</li> </ul>	itional directory (Any Microsoft Entra ID tenant - Multitenant)	
Accounts in any organiza	itional directory (Any Microsoft Entra ID tenant - Multitenant) and perso	onal Microsoft
Accounts (e.g. Skype, Xbo	XX)	
Help me choose		
Redirect URI (optional)		6
We'll return the authentication is optional and it can be chang	n response to this URI after successfully authenticating the user. Providi ged later, but a value is required for most authentication scenarios.	ing this now
Public client/native (mobile	V https://secureapplication	_
Register an app you're workin by adding from Enterprise app	g on here. Integrate gallery apps and other apps from outside your orgolications.	ganization
By proceeding, you agree to t	he Microsoft Platform Policies 🗗	_
Register 🕜		

#### 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.

$\equiv$ Microsoft Azure $\rho$ s	earch resources, services, and docs (G+/)	?	প্ন	SECURE BOLUTIONS AG (MALO	
Home >					
Secure Applicatio	on ☆ …				$\times$
✓ Search	« 前 Delete 🕀 Endpoints 💀 Preview features				
Overview					
📣 Quickstart			C	iont cradentials	
🚀 Integration assistant	Secure Application Copy to dinboard		Ac	Id a certificate or secret	
Manage	Application (client) ID		Re <u>0 v</u>	direct URIs <u>web, 0 spa, 1 public client</u>	
🚍 Branding & properties	Object ID		Ap	plication ID URI	
Authentication	Directory (tenant) ID		M	anaged application in local di	rectory
📍 Certificates & secrets			<u>H/</u>	ALOCADApp	,
Token configuration	Supported account types My organization only				
ADI permissions					

#### 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:

$\equiv$ Microsoft Azure	▷ Search resources, services, and docs (G+/)	9
Home > 11 11 Adda a	App registrations > Secure Application ation   API permissions ☆ ×	
Search	« 🕐 Refresh   🖗 Got feedback?	_
<ul> <li>Branding &amp; properties</li> <li>Authentication</li> <li>Certificates &amp; secrets</li> <li>Token configuration</li> <li>API permissions</li> <li>Expose an API</li> </ul>	Configured permission   Applications are authoriz configured permissions   Applications are authoriz configured permissions   + Add a permission   API / Permissions n   VMicrosoft Graph (1)	
App roles	User.Read Application (client) ID	
Owners     Roles and administrators     Manifest	Microsoft Information Protection Sync Service To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try Enterprise applications.	_

#### 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".

E Microsoft Azure 🔎 Se	earch resources, services, and docs (G+/)	D 🕼 🤔 🎯 R 🛛 🥌
Home > Secure Applic	Request API permissions 🔞	×
₽ Search Ivianage	Delegated permissions Your application needs to access the API as the signed-in user.	Application permissions Your application runs as a background service or daemon without a signed-in user.
<ul> <li>Branding &amp; properties</li> <li>Authentication</li> </ul>	Select permissions	expand all
Certificates & secrets	$ \mathcal{P} $ Start typing a permission to filter these results	
Token configuration	Permission	Admin consent required
<ul> <li>API permissions</li> </ul>	✓ UnifiedPolicy (1)	
<ul> <li>Expose an API</li> <li>App roles</li> </ul>	UnifiedPolicy.User.Read ① Read all unified policies a user has access to.	No
<ul> <li>Owners</li> <li>Roles and administrators</li> </ul>	Ð	
❶ Manifest https://portal.azure.com/≠	Add permissions Discard	

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.

	Microsoft Azure	𝒫 Search resource	s, services,	and docs (G+	<i>٨</i>	<u>ې</u> و	) R			0
Ног	me > 11 III III IIII IIII IIII IIII IIII	op registrations > Se	ecure Applic	ation						
P	Secure Applicat	on   API perr	mission	S 🖈						$\times$
2	Search	Refresh	🕂 G	ot feedback?						
	Overview	Succes	sfully grante	d admin conse	nt for the requested permissions.	16				
<b>a</b> a <b>X</b>	Quickstart Integration assistant	+ Add a p	ermission	🗸 Grant ad	Imin consent for	iline Wi				
Ma	220	API / Permi	ssions n	Туре	Description	Α	dmin	Status	Updated status	
		∽ Azure Rig	hts Manage							•••
•	Branding & properties	user_in	npersonatio	Delegated	Create and access protected	co N	0	🕑 Gra	nted for	
7	Authentication	✓ Microsoft	Graph (1)							•••
	Certificates & secrets	User.Re	ead	Delegated	Sign in and read user profile	N	0	🕑 Gra	nted for	•••
- 111	Token configuration	✓ Microsoft	Informatior							
<del>.</del>	API permissions	Unified	Policy.User.	Delegated	Read all unified policies a us	er N	0	🥑 Gra	nted for	
2	Expose an API			J				_		



- 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	Туре	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.R ead	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.
- 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 "<u>Enable Support for TLS 1.2 at</u> <u>the Client Workstation for Microsoft Entra ID</u>".
- 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 "<u>Microsoft Online</u> <u>Documentation</u>". However, Microsoft recommends the following:

Ports
TCP 443
TCP 443
TCP 443
Microsoft Entra ID authentication
endpoint
https://login.microsoftonline.us
https://login.microsoftonline.com
P T T

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 <u>Microsoft article to enable TLS 1.2</u>.

#### 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\WOW6432No	"SystemDefaultTlsVersions"=dword:0000001
	<pre>de\Microsoft\.NETFramework\v4.0.30319]</pre>	"SchUseStrongCrypto"=dword:0000001
2	[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft	"SystemDefaultTlsVersions"=dword:0000001
	\.NETFramework\v4.0.30319]	"SchUseStrongCrypto"=dword:0000001

Registry entries