

User administration

- Azure

- [Register Entra application](#)
- [Update global settings](#)
- [Limit access to groups / UPN](#)

Register Entra application

Basic application setup

<div><div>Register an application</div><div><div><div>Name</div><div>The user-facing display name for this application (this can be changed later).</div><div>ABit Software SSO</div></div><div><div>Supported account types</div><div>Who can use this application or access this API?</div><div><div>Accounts in this organizational directory only (ABIT HOLDINGS PTY LTD only - Single tenant)</div><div>Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)</div><div>Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)</div><div>Personal Microsoft accounts only</div></div><div><div>Redirect URI (optional)</div><div>We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.</div><div>Webhttp://localhost</div></div><div>Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from Enterprise applications.</div></div></div></div>	<div>Create a new application and allow Web URL of http://localhost</div>
<div><div><div>Essentials</div><div><div>Display name</div><div>ABit Software SSO</div></div><div><div>Application (client) ID</div><div></div></div><div><div>Object ID</div><div></div></div><div><div>Directory (tenant) ID</div><div></div></div><div><div>Supported account types</div><div>My organization only</div></div></div><div><div><div>Client credentials</div><div>Add a certificate or secret</div></div><div><div>Redirect URIs</div><div>1 web, 0 spa, 0 public client</div></div><div><div>Application ID URI</div><div></div></div></div><div><div>Record Application (client) ID and Directory (tenant) ID for future use.</div><div>Click Add a certificate or secret</div></div></div>	<div>Record Application (client) ID and Directory (tenant) ID for future use.</div> <div>Click Add a certificate or secret</div>

Certificates

Got feedback?

Credentials enable c
at a web addressabl
certificate (instead o

Application re

Certificates (0)

A secret string that
application passwo

+ New client se

DescripNew client secret

No client secrets hi

DescriptionNovember 2024 - 2026

Expires730 days (24 months)

Click new secret, and create an entry with required duration and name

+ New client secret

Copy the value., NOTE: you cannot view this value again.

Description	Expires	Value	Secret ID
November 2024 - 2026	11/14/2026		

Click new secret, and create an entry with required duration and name

Copy the value.

NOTE: you cannot view this value again.

Allow groups for authentication restrictions

Manage

Branding & properties

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Owners

Roles and administrators

Manifest

Support + Troubleshooting

New support request

The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your organization, or in organizations where this app will be used. [Learn more](#)

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission

Grant admin consent for ABIT HOLDINGS PTY LTD

API / Permissions name

Type

Description

Admin consent required

Microsoft Graph (1)

User Read

Delegated

Sign in and read user profile

No

To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try [Enterprise applications](#).

To access group details the API needs Group.Read.All application permission

Select an API

Microsoft APIs

APIs my organization uses

My APIs

Commonly used Microsoft APIs

Microsoft Graph

Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Microsoft Entra ID, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.

Select Microsoft Graph

Microsoft Graph

<https://graph.microsoft.com/> [Docs](#)

What type of permissions does your application require?

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 with signed-in user.

Select permissions

group

The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your organization, or in organizations where this app will be used. [Learn more](#)

Permission

Admin consent required

> Group-Conversation

< Group (1)

☒

Group.Read.All

Read all groups

Yes

☐

Group.ReadWrite.All

Read and write all groups

Yes

< GroupMembers

Select delegated permissions and search for group to add Group.Read.All

Refresh

Got feedback?

Grant admin consent confirmation.

Do you want to grant consent for the requested permissions for all accounts in ABIT HOLDINGS PTY LTD? This will update any existing admin consent records this application already has to match what is listed below.

Yes

No

The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your organization, or in organizations where this app will be used. [Learn more](#)

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission

Grant admin consent for ABIT HOLDINGS PTY LTD

API / Permissions name

Type

Description

Admin consent required

Status

Microsoft Graph (2)

Group.Read.All

Delegated

Read all groups

Yes

Not granted for ABIT H...

User Read

Delegated

Sign in and read user profile

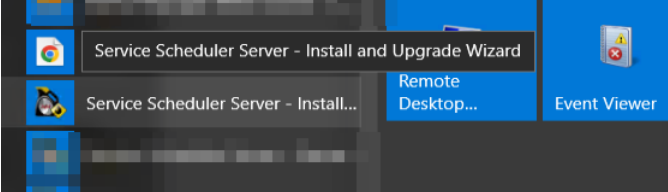
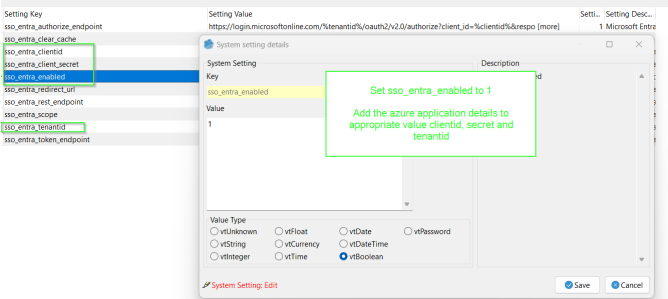
No

To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try [Enterprise applications](#).

Confirm admin consent

Update global settings

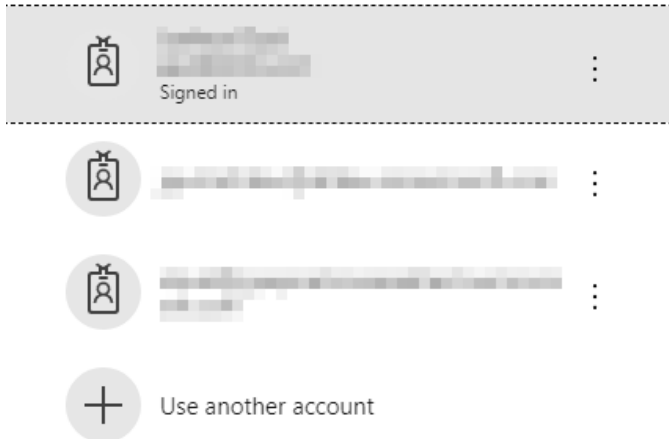
You will need the Azure clientid, applicationid and secret from the [Azure Application](#)

	<p>Start the Service Scheduler Install / Upgrade wizard on the server</p>
<p>Account Settings Modify account settings and system settings</p> <p>Settings Global</p> <p>Account Name <input checked="" type="checkbox"/> ABit - Dev</p>	<p>Click next until the Account Settings page and select "Global"</p>
	<p>Set sso_entra_enabled to 1</p> <p>Add the azure application details to appropriate value clientid, secret and tenantid</p>

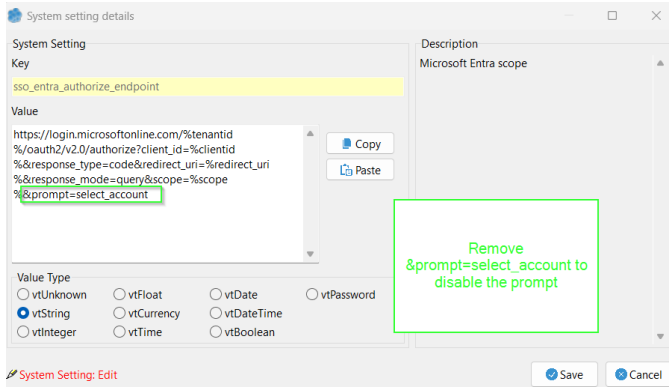
Stop service scheduler for prompting for account on login



Pick an account



To stop the prompt adjust global setting
sso_entra_authorize_endpoint

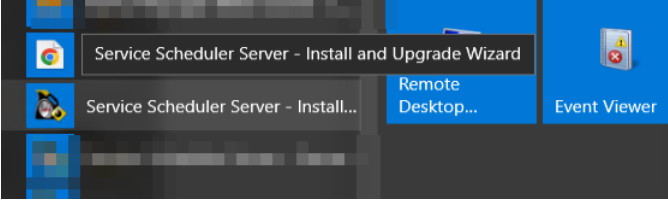
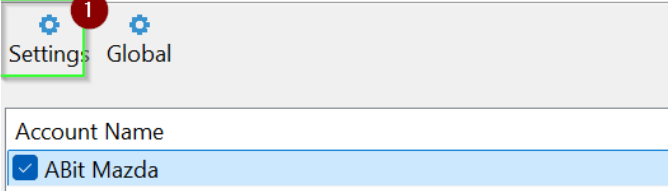

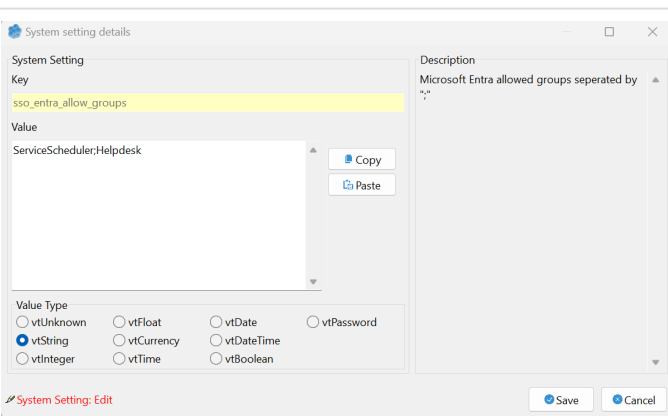
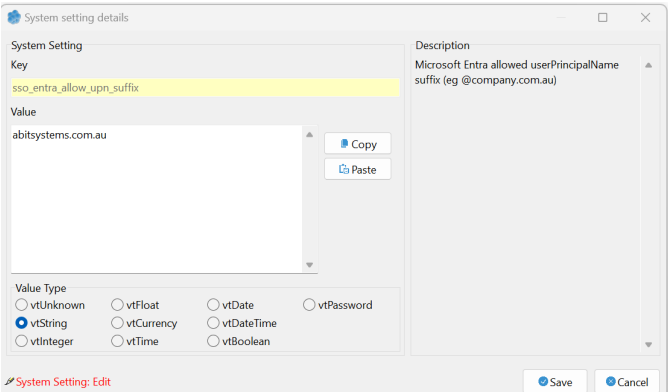


https://login.microsoftonline.com/%tenantid%/oauth2/v2.0/authorize?client_id=%clientid%&response_type=code&redirect_uri=%redirect_uri%&response_mode=query&scope=%scope%&prompt=select_account

Remove the &prompt=select_account to disable.

Limit access to groups / UPN

For groups to work the Microsoft Entra application will need [Group.Read.All](#) permission

	<p>Start the Service Scheduler install and upgrade wizard</p>
<p>Account Settings Modify account settings and system settings</p> 	<p>Select settings</p>
	<p>Locate the settings <code>sso_entra_allow_groups</code> and <code>sso_allow_upn_suffix</code></p>
	<p>To limit access to certain group, add the group names separated by the ";" character.</p>
	<p>To limit to user UPN suffix enter the userPrincipalName suffix</p>