

Setup SAML for Single Sign-On

AgileAssets support using SAML protocol to conduct Single Sign-On (SSO). This page shows how to setup SAML with Azure Active Directory as an example Identity Provider (IdP). For other IdPs, the setup is similar.

Note

1. Setting up SAML requires System Admin access on application server, who has write access to Tomcat folder.
2. The following guide uses <https://quappv21.agileassets.com/ams-web> as an example AMS application. Update this URL accordingly when configuring a real-world instance.

Click to jump to a topic:

- 1 [Azure Configuration](#)
- 2 [AMS Configuration](#)
 - 2.1 [Web.xml](#)
 - 2.2 [SAML Security Window Configuration](#)
 - 2.3 [Certificate file](#)
 - 2.4 [User Configuration](#)
- 3 [SSO Login URL in Azure](#)

Azure Configuration

1. Ask client's **Azure Admin** to create a new **Enterprise Applications** within **Azure Active Directory**.
2. Go to **Azure Active Directory** > **Enterprise Application** > <your application> > **Single sign-on**.
3. In the SSO page, ask client to enter these values for these fields:

Field	Value	Example
Identifier (Entity ID)	[Application Base URL]	https://quappv21.agileassets.com/ams-web
Reply URL (Assertion Consumer Service URL)	[Application Base URL]/alias/sp	https://quappv21.agileassets.com/ams-web/alias/sp
Sign on URL	Leave empty	
Relay State	Leave empty	
Logout Url	Leave empty	
All other fields	Leave empty (or default value)	

4. Add some test users to the application under the **Users and groups** page.
5. Download the **Federation Metadata XML** file and **Certificate (Base64)** file (NOT Certificate (RAW)), and send to **AMS Application System Admin**.

AMS Configuration

Web.xml

Make the following changes in AMS's web.xml file under Tomcat application folder.

web.xml

```
<filter>
  <filter-name>SamlFilter</filter-name>
  <filter-class>com.agileassetsinc.core.SsoSAMLFilter</filter-class>
  <init-param>
    <param-name>SIGNATURE_STRATEGY</param-name>
    <param-value>ASSERTION_SIGNATURE</param-value>
  </init-param>
</filter>
<filter-mapping>
  <filter-name>SamlFilter</filter-name>
  <url-pattern>/alias/sp</url-pattern>
</filter-mapping>
```

SAML Security Window Configuration

Insert a new row in the **System > Setup > SAML Security** screen, complete the following values and Save.

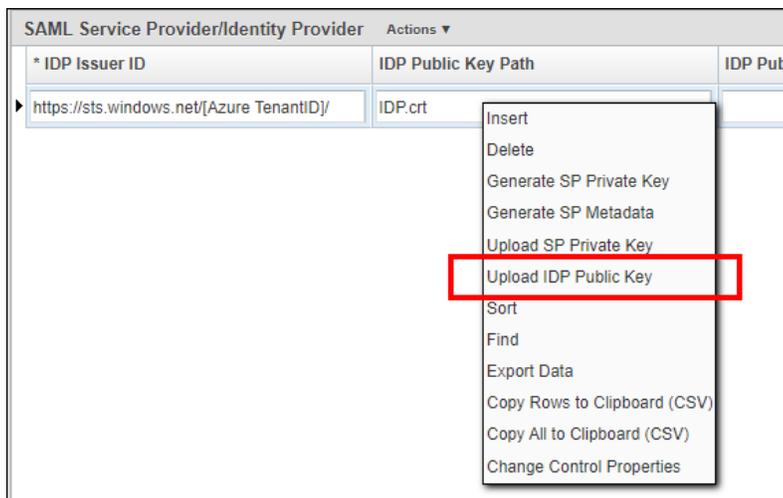
Attribute	Value	Example
IDP Issuer ID	Use the entityID field value retrieved from FederationMetadata.xml	https://sts.windows.net/[Azure TenantID]/
IDP Public Key Path	File name of the Certificate (Base64) file	IDP.cer
IDP Public Key Alias	Can be anything, e.g. "Microsoft Azure Federated SSO Certificate"	Microsoft Azure Federated SSO Certificate
SP Entity ID	Can be anything. e.g. user system name and environment	AMS-DEV
Allowed Skew Time (min)	The column "Allowed Skew Time (min)" enables some difference between the clocks. It's recommended that "Allowed Skew Time (min)" value has to be set between 1 and 3 (in minutes).	3
User ID mapping	NameID	NameID
Error Resource	If the authentication is rejected in AgileAssets (e.g., No corresponding AD_USER_ID or invalid SAML assertion) the URL where the request will be redirected. By default, it will go on the AgileAssets login page.	Blank
Issuer Assertion	Ensure checks are performed.	Checked

Certificate file

Place the **Certificate (Base64)** file from Azure under **[Tomcat Installation Folder]/webapps/[Application Name]/Certificates/** folder.

OR

Right click the record and select **Upload IDP Public Key** option. Select the **Certificate (Base64)** file from Azure and upload it.



User Configuration

On the **System > Security > User Level > User Names and Access** window, add each user's Active Directory user name to the **Active Directory User ID** field. It may be the user's Azure User ID or email - depending on client's Azure configuration. If one does not work, try the other.

* User ID	Administrative Unit	First Name	Middle Name	Last Name	Name	email	Active Directory User ID
TEST_USER						TEST_USER@TRIMBLE	TEST_USER

SSO Login URL in Azure

1. Go to **Azure Active Directory > Enterprise Application > <your application> > Properties**
2. The user login URL is the **User Access URL** value.
3. Clicking this value will ask user to login with their AD user name and password, and login to the AMS application.

The screenshot shows the 'Properties' page for an Enterprise Application in Azure Active Directory. The 'User access URL' field is highlighted with a red box. The page includes a navigation sidebar on the left with categories like 'Manage', 'Security', and 'Activity'. A message at the top states: 'You can't delete this application because you don't have the right permissions. Learn more.'

Enabled for users to sign-in?	Yes No
Name	
Homepage URL	
Logo	PT
User access URL	
Application ID	
Object ID	
Terms of Service URL	Publisher did not provide this information
Privacy Statement URL	Publisher did not provide this information
Reply URL	
Assignment required?	Yes No
Visible to users?	Yes No