

# Tutorial: Azure Active Directory Integration with Qualys Cloud Platform using SAML SSO

In this tutorial we'll show you how to integrate Microsoft Azure Active Directory (Azure AD) with Qualys Cloud Platform using SAML 2.0 SP-initiated SSO.

Integrating Qualys Cloud Platform with Azure AD provides you with these benefits:

- Control who has access to Qualys Cloud Platform from Azure AD
- Enable users to automatically log in to Qualys with their Azure AD credentials
- Manage your accounts from the Azure portal

## Prerequisites

- Qualys Cloud Platform subscription
- SAML SSO must be enabled for your subscription. Follow the steps below to get this feature.
- The New Data Security Model must be accepted for the subscription. A Manager can opt in by going to Users > Setup > Security in the Qualys UI.

## How do I request SAML SSO

To initiate SAML onboarding complete these steps:

1) Download and complete sections 1 and 2 of the [SAML 2.0 Integration Request Form](#)

You'll provide these details:

- Entity ID string from IdP (SAML Identity Provider)
- Public key certificate for the IdP (your organization's IdP base64 cert in .txt format)
- Organization's SAML IdP SSO URL (SP initiated authentication requests)
- Qualys Subscription Login (for Manager POC)
- Custom exit URL for a subscription (optional)

2) Submit the form to [Qualys Support](#)

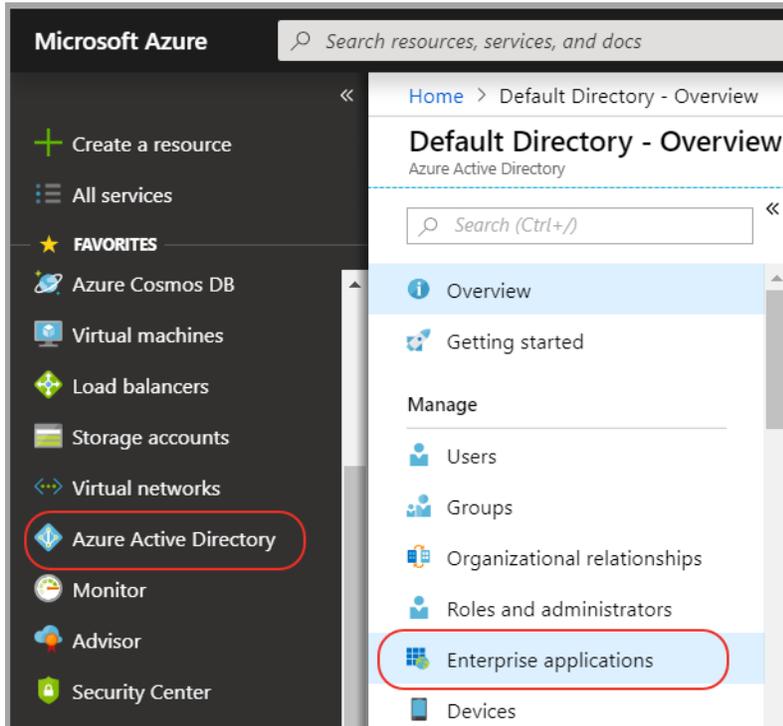
3) Qualys Support will work with you to configure the trust relationship between your Identity Provider (IdP) and the Qualys SAML 2.0 Service Provider (SP). Qualys will provide you with 2 URLs: Identifier and Reply URL. You'll need these URLs to configure Azure AD in Azure portal.

# Configure Azure Active Directory

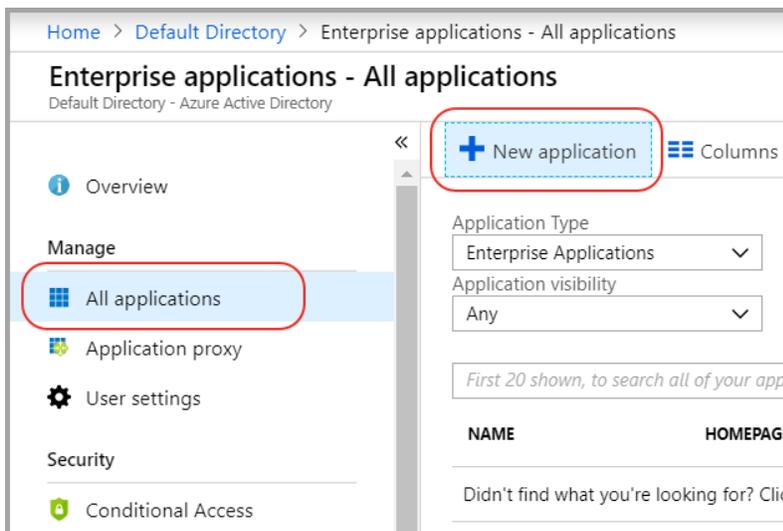
Complete these steps in Azure portal.

## Add new application (non-gallery application)

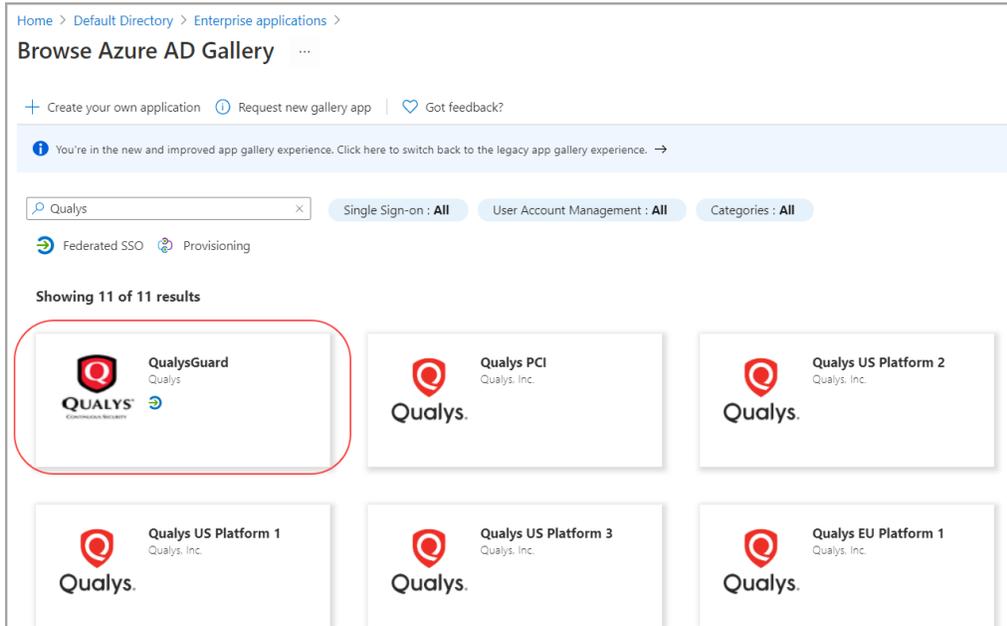
Select Azure Active Directory on the left navigation pane. Then choose Enterprise applications.



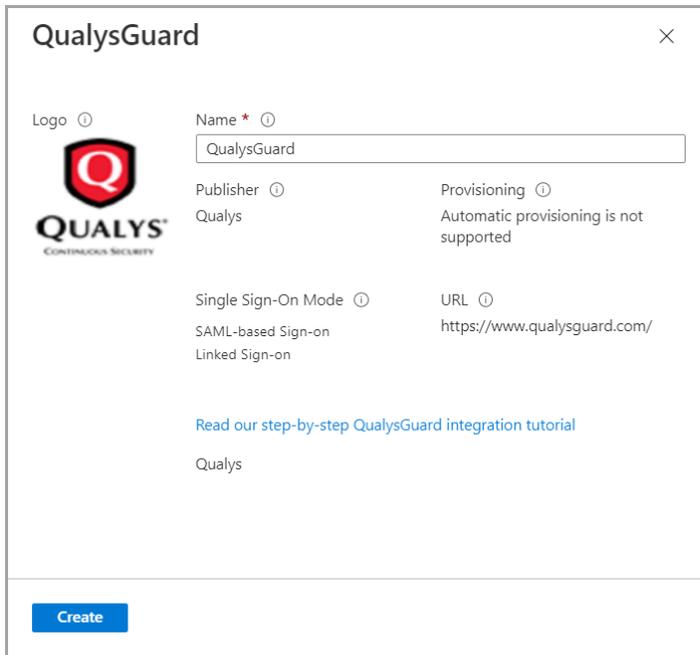
Choose All applications and click New application.



Perform a search for “Qualys”. You’ll see various Qualys applications available. Choose the first application, which has the  Federated SSO tag.



After you click on the application with the Federated SSO tag, the application appears in the right pane. Click Create.



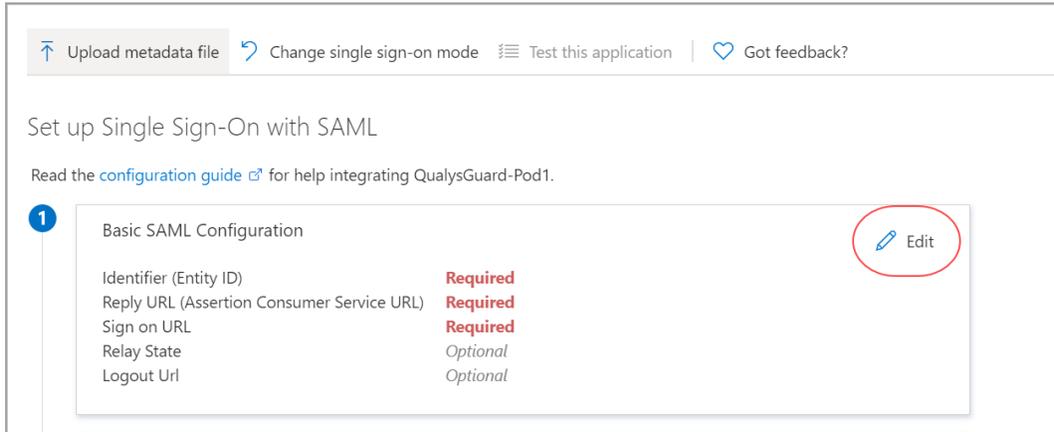
The new application is added and you can now configure it to use SAML single sign-on.

## Configure the application to use SAML single sign-on

From the Qualys application page, select Single sign-on and choose SAML for the sign-on method.

Provide SAML configuration details in these sections:

1) Basic SAML Configuration. Click the Edit icon to provide required SAML configuration settings.



Enter the Identifier ID, Reply URL and Sign on URL provided to you by Qualys. Other values are not required. Follow the Patterns shown on the screen for each of the fields.

Identifier (Entity ID) \* ⓘ  
*The default identifier will be the audience of the SAML response for IDP-initiated SSO*

Default

ⓘ 🗑️

**Patterns:** QualysGuard\_SharedPlatform-SAML20-SP

Reply URL (Assertion Consumer Service URL) \* ⓘ  
*The default reply URL will be the destination in the SAML response for IDP-initiated SSO*

Default

ⓘ 🗑️

**Patterns:** https://qualysguard.qg1.apps.qualys.in/IdM/saml2/

Sign on URL \* ⓘ

**Patterns:** https://qualysguard.qg1.apps.qualys.in/

Samples:

Identifier: [https://QualysGuard\\_SharedPlatform-SAML20-SP](https://QualysGuard_SharedPlatform-SAML20-SP)

Reply URL (based on the Qualys Cloud Platform for your subscription):

<https://qualysguard.qualys.com/IdM/saml2/>

<https://qualysguard.qg2.apps.qualys.com/IdM/saml2/>

<https://qualysguard.qg3.apps.qualys.com/IdM/saml2/>

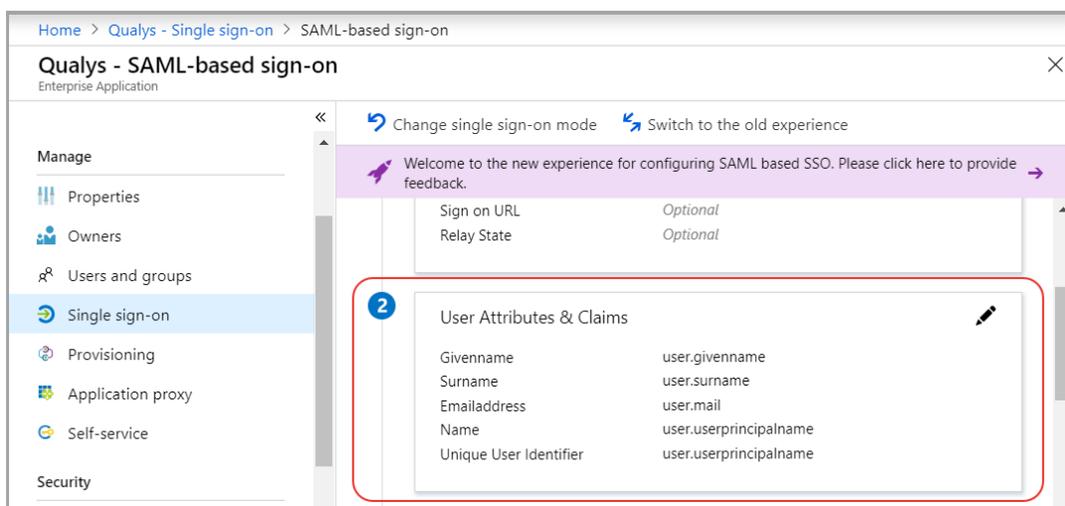
<https://qualysguard.qualys.eu/IdM/saml2/>

<https://qualysguard.qg2.apps.qualys.eu/IdM/saml2/>

<https://qualysguard.qg1.apps.qualys.in/IdM/saml2/>

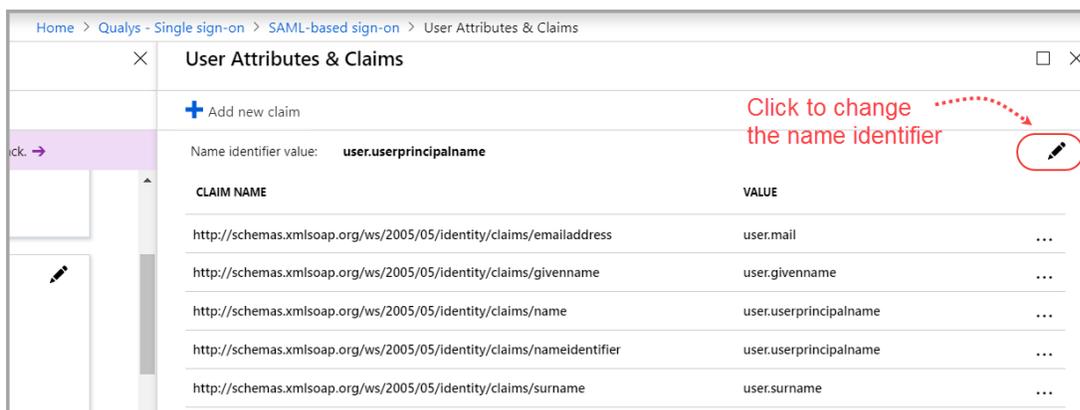
[https://qualysguard.BASE\\_URL/IdM/saml2/](https://qualysguard.BASE_URL/IdM/saml2/) (for Private Cloud Platform)

2) User Attributes & Claims. When a user authenticates to an application through Azure AD using the SAML 2.0 protocol, Azure AD sends a token to the application as a part of SAML Auth Response (via an HTTP POST). And then, the application validates and uses the token to log the user in instead of prompting for a username and password. These SAML tokens contain pieces of information about the user known as "claims".



### Change the name identifier (optional)

You'll notice that the Unique User Identifier is mapped to the value of the Azure user's username (user.userprincipalname). Click the Edit icon to change the name identifier to a different source attribute like user.employeeid.



### Add claim for Qualys external ID (required)

By default, Qualys Cloud Platform is configured to parse the value of `qualysguard_external_id` that is issued with the SAML token. You'll need to add this claim to the list.

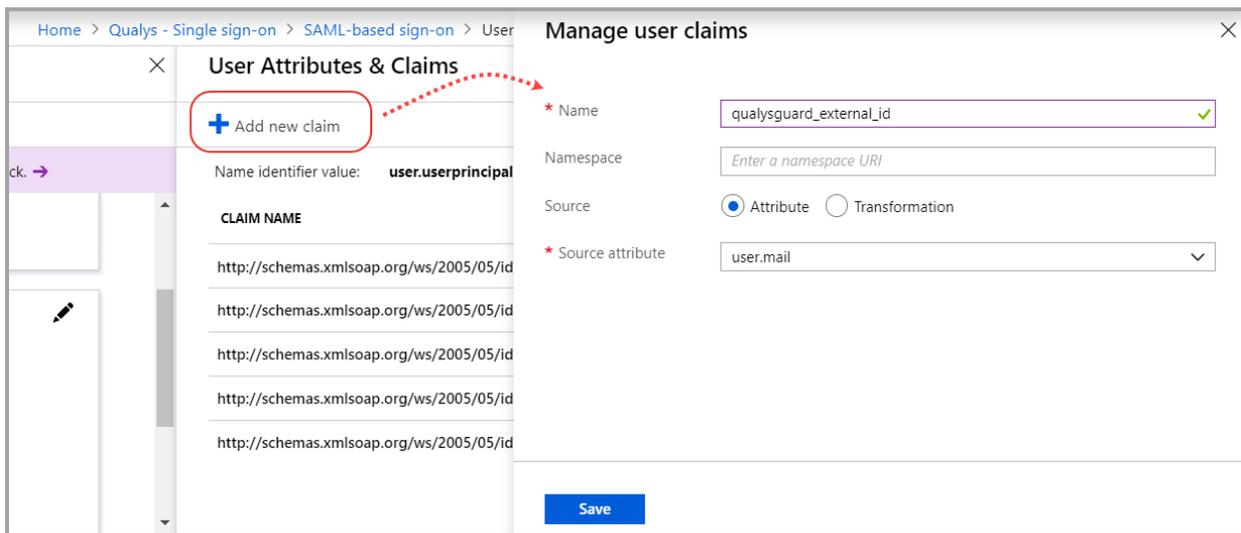
Click Add new claim, and provide these settings:

Name: `qualysguard_external_id`

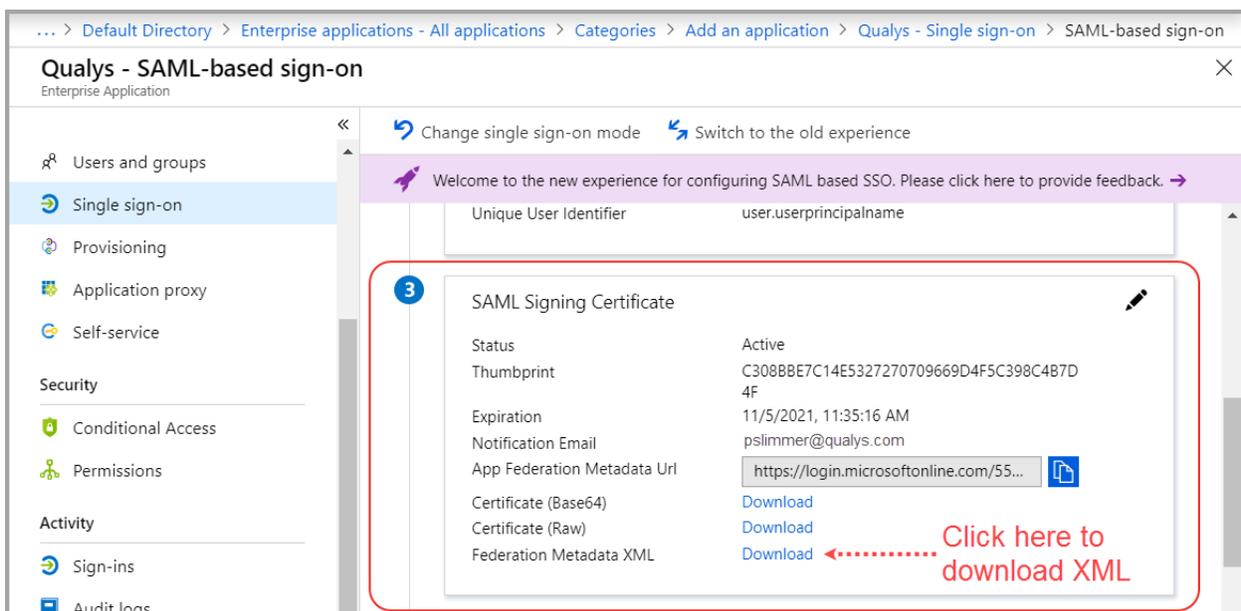
Namespace: leave blank

Source attribute: `user.mail` (recommended)

When the source attribute is set to `user.mail` you'll enter the user's email address in the External ID field in the user's Qualys account to validate the claim. You can choose to set the source attribute to another value. If you do, be sure to set the External ID value to match.



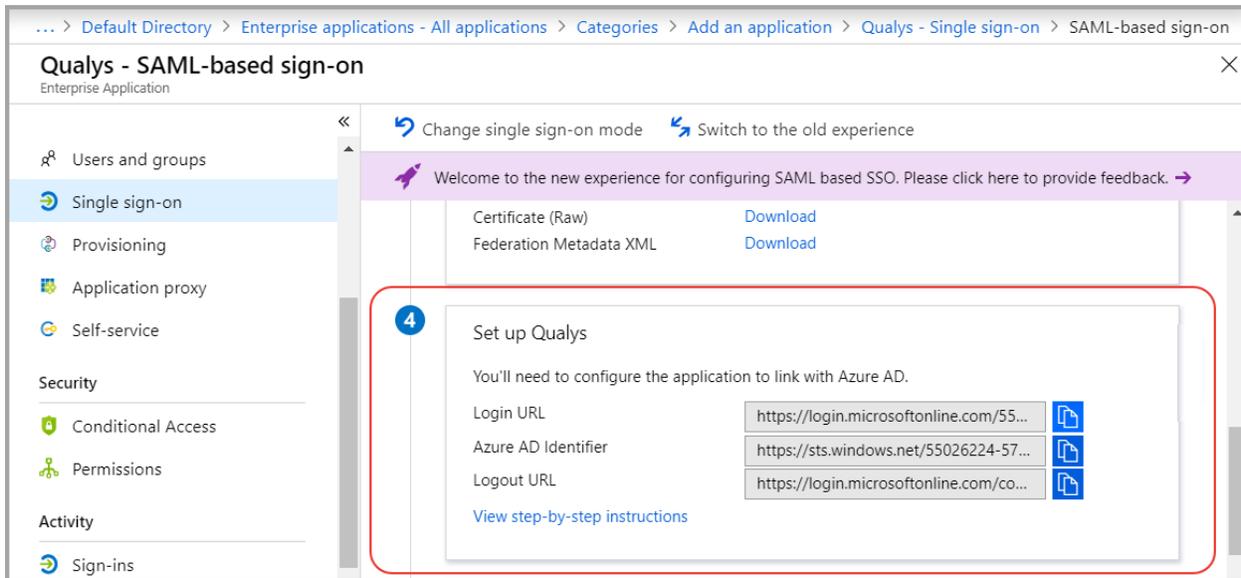
3) SAML Signing Certificate. Click Download next to Federation Metadata XML to save the metadata file to your computer. Send this file to Qualys.



The Federation Metadata XML file is used by Qualys to create the IDP and IDM profile for your subscription. It contains useful information like IDP Entity ID, SSO Re-Direct URL and the Base64 encoded Token Signing certificate.

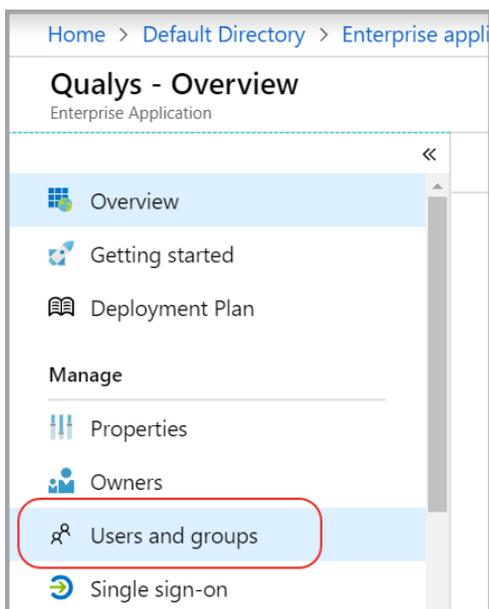
4) Set up Qualys. The Federation Metadata XML file downloaded in the previous step has the info that Qualys needs. You can skip this step unless you want to customize the logout URL.

By default, the logout URL is set to <https://www.qualys.com>. You can add a custom logout URL to section 2 of the [SAML 2.0 Integration Request Form](#).



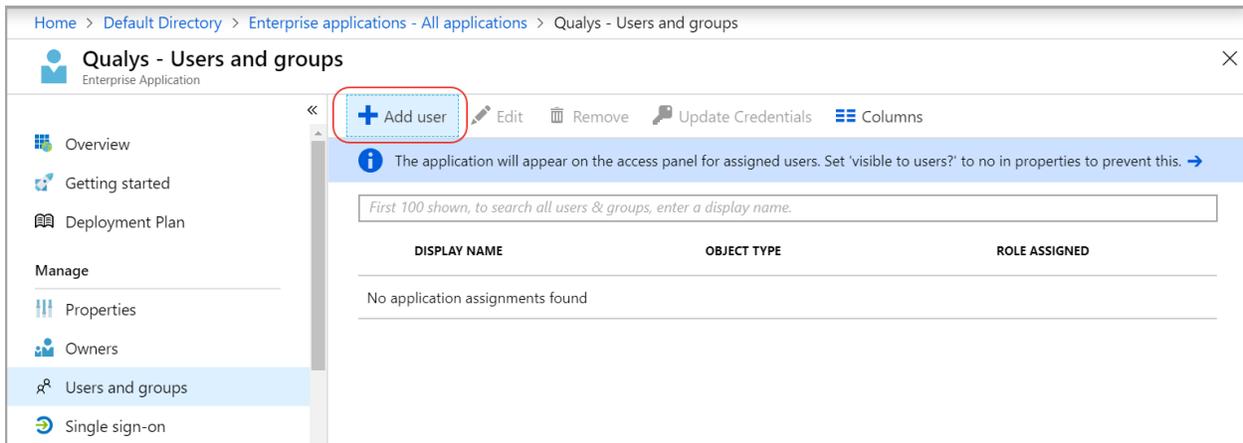
## Assign the Azure AD user to Qualys application

You'll need to assign users or groups to the application. Azure AD will not allow a user to sign into the Qualys application unless Azure AD has granted access to the user.

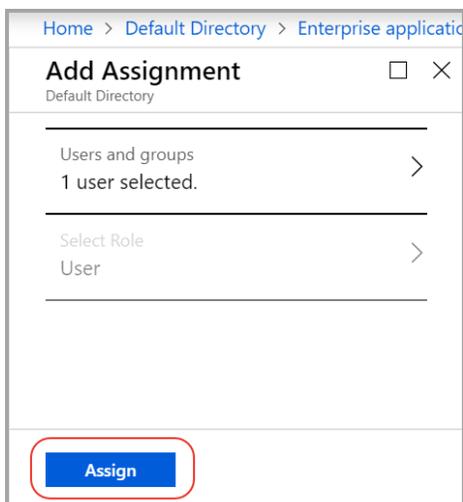
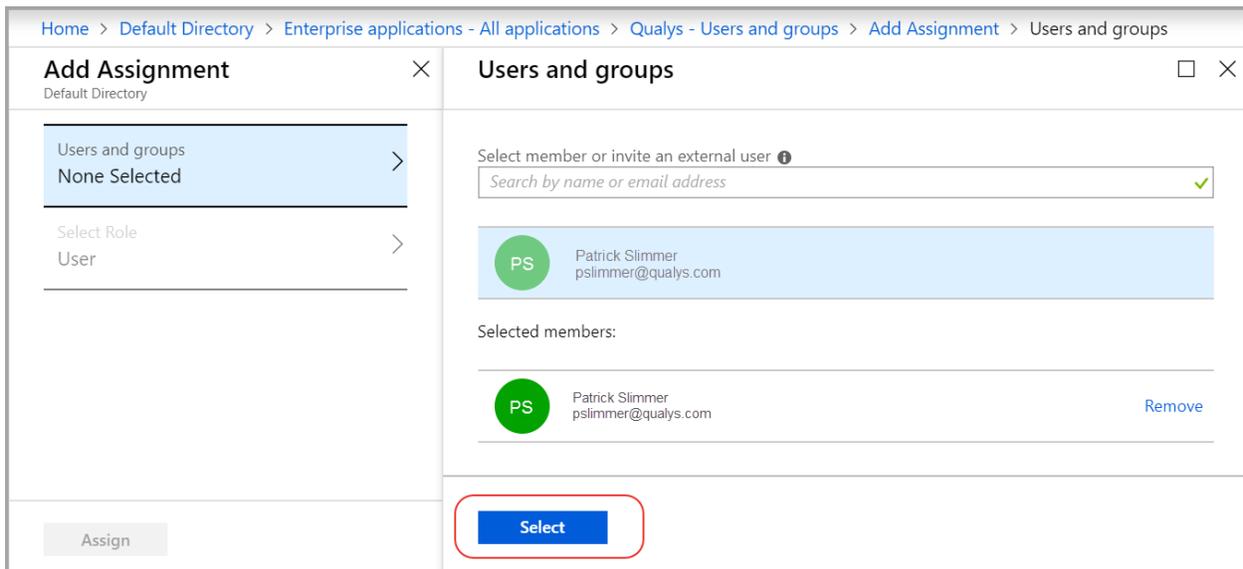


Pick the Qualys application from your list of applications. Then choose Users and groups.

Click the Add user button.



Select Users and groups under Add Assignment. Click on one or more users in the list to select them, then click the Select button.



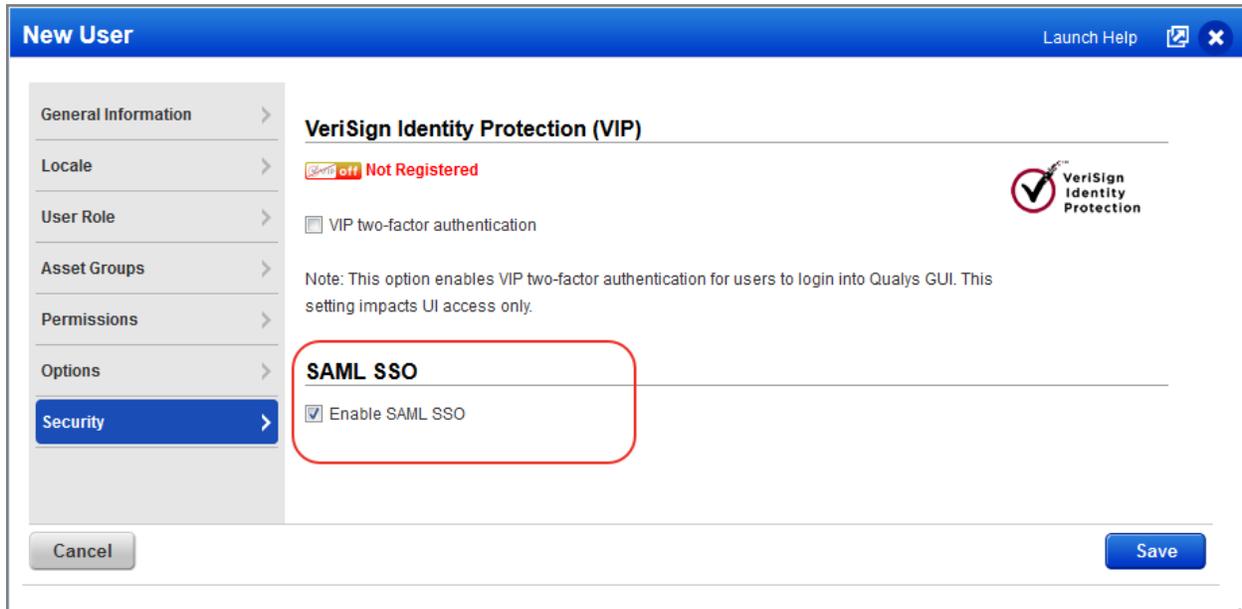
Finally, click the Assign button. The selected user is now assigned the Qualys application.

# Enable SAML SSO for Qualys User

Complete these steps using Qualys Cloud Platform.

## Enable SAML SSO in user account

Go to the Users section in the Qualys UI. Create a new user or edit an existing one. In the user account settings, select Enable SAML SSO in the Security section.



## Set the external ID

You'll need to set the external ID for the user. The external ID value corresponds to the `qualysguard_external_id` claim that you've defined in your Azure SAML configuration. We've recommended that the external ID is set to the user's email address. You may have changed this to another attribute present in the SAML Auth Response.

You can set the external ID from the UI (as shown below) or via the Add/Edit User API (`/msp/user.php`). See the [Qualys API \(VM,PC\) User Guide](#) to learn more.

## Good to Know

- The external ID can be set to any string but the string must be unique for each user in the subscription and the same value should be passed in the claim.
- By default the external ID validation is case sensitive. If you need this to be case insensitive then we can configure it that way. Please reach out to Qualys Support to customize your IDM settings.
- Initially, only the Manager Primary Contact has permission to edit the external ID for a user. Other managers may be granted this permission. [Click here](#) to learn more.

## Test Qualys login using SAML SSO

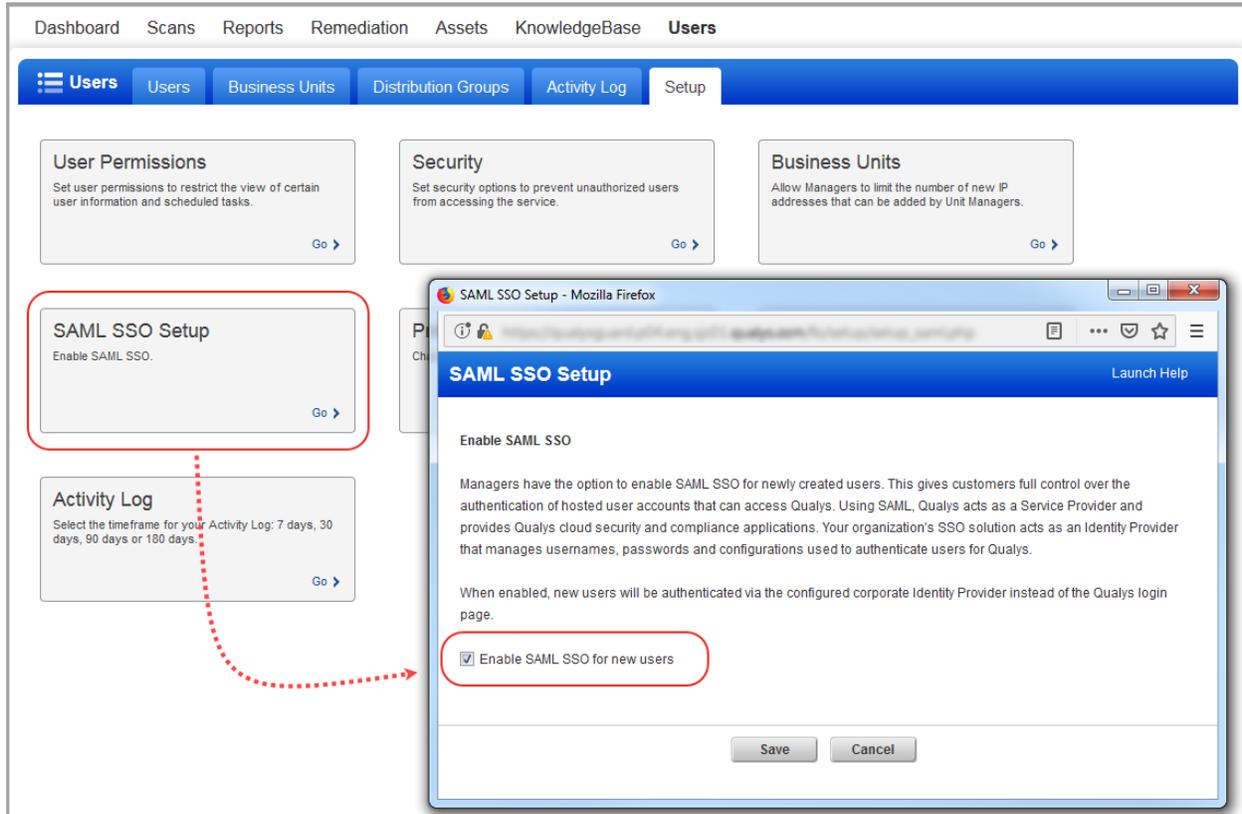
- 1) Use a web browser and open the unique Login URL
- 2) The web browser should redirect you to the SAML SSO page where you'll enter your Azure Active Directory login and password.
- 3) Upon successful authentication, the web browser should be redirected to Qualys and a valid session should be opened with the expected user identity.
- 4) When logging out of Qualys, the web browser should be redirected to <https://www.qualys.com> or a custom logout URL provided by the customer.

# Roll out SAML SSO for more Qualys users

You can enable SAML SSO for all new users or select users.

## Enable SAML SSO for all new users

Go to Users > Setup > SAML SSO Setup. Select the option “Enable SAML SSO for new users”.



## Bulk Enable SAML SSO for multiple users

The Users list will show you whether users have SAML SSO enabled.

The screenshot shows the Qualys Users list. The 'SAML SSO' column is highlighted with a red box. The table contains the following data:

Name	Login	Role	Business Unit	Status	Last Login	Modified	SAML SSO
Brendan Skulan	quays_bs1	Auditor	Unassigned	Active	08/04/2017	07/31/2018	Enabled
Jason Kim	quays_ak4	Manager	Unassigned	Active	05/01/2017	05/01/2017	Enabled
Patrick Slimmer *	quays_ps	Manager	Unassigned	Active	07/26/2018	05/23/2018	Disabled
Suzy Van Pelt	quays_sx22	Reader	Unassigned	Active	07/31/2018	06/11/2018	Enabled
Hana Fedasz	quays_hf	Scanner	Unassigned	Active	11/05/2018	07/26/2018	Disabled
Jake Anthony	quays_aa9	Scanner	Unassigned	Active	07/12/2018	07/12/2018	Enabled
Susan Schlemmer	quays_ts9	Scanner	Unassigned	Active	07/09/2018	07/09/2018	Disabled
UM Created Scanner	quays_us2	Scanner	BU1	Active	08/04/2017	01/03/2018	Disabled
James Adrian	quays_aa32	Unit Manager	BU1	Active	07/31/2018	07/31/2018	Enabled

Click the Search button (above the list) to quickly find accounts with SAML SSO disabled.

**Search**

Name:

Title:

Business Unit:

External ID:

User Login:

Role:  Manager  Unit Manager  Auditor  Scanner  
 Reader  Remediation User  Contact  User Administrator

Status:  Active  Inactive  Pending Activation

Not Logged In Since:  31

Modified Since:  31

SAML SSO:  Disabled  Enabled

**Search**

Select all the rows in your search results and pick Enable SAML from the Actions menu. Note that you can disable SAML in this same way by choosing Disable SAML.

Dashboard Scans Reports Remediation Assets KnowledgeBase **Users**

**Users** Users Business Units Distribution Groups Activity Log Setup

Actions (5) New Search Filters 1 - 5 of 5

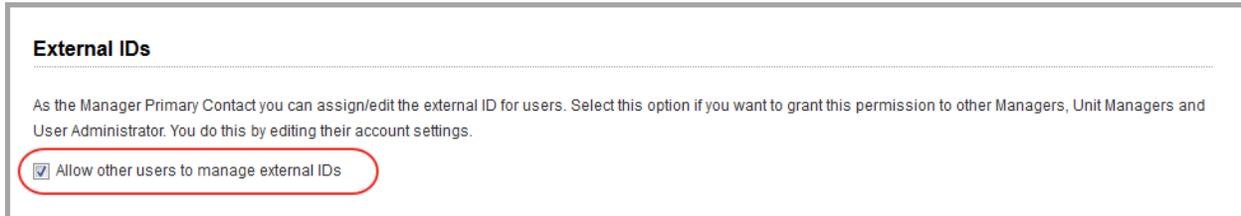
	Login	Role	Business Unit	Status	Last Login	Modified	SAML SSO	
<input type="checkbox"/>	quays_ps	Manager	Unassigned	Active	07/26/2018	05/23/2018	Disabled	
<input type="checkbox"/>	quays_tr2	Manager	Unassigned	Active	11/05/2018	07/26/2018	Disabled	
<input checked="" type="checkbox"/>	Hana Fedasz	quays_hf	Scanner	Unassigned	Active	07/09/2018	07/09/2018	Disabled
<input checked="" type="checkbox"/>	UM Created Scanner	quays_us2	Scanner	BU1	Active	08/04/2017	01/03/2018	Disabled
<input checked="" type="checkbox"/>	Susan Schlemmer	quays_ts9	Scanner	Unassigned	Active	08/09/2017	01/03/2018	Disabled

## Granting Managers permission to add external IDs

External IDs can be added by the Manager Primary Contact (for the subscription).

The Manager Primary Contact has the option to allow other Managers, Unit Managers and User Administrators to edit external IDs for users by following these steps:

- 1) Go to Users > Setup > Security and select “Allow other users to manage external IDs”

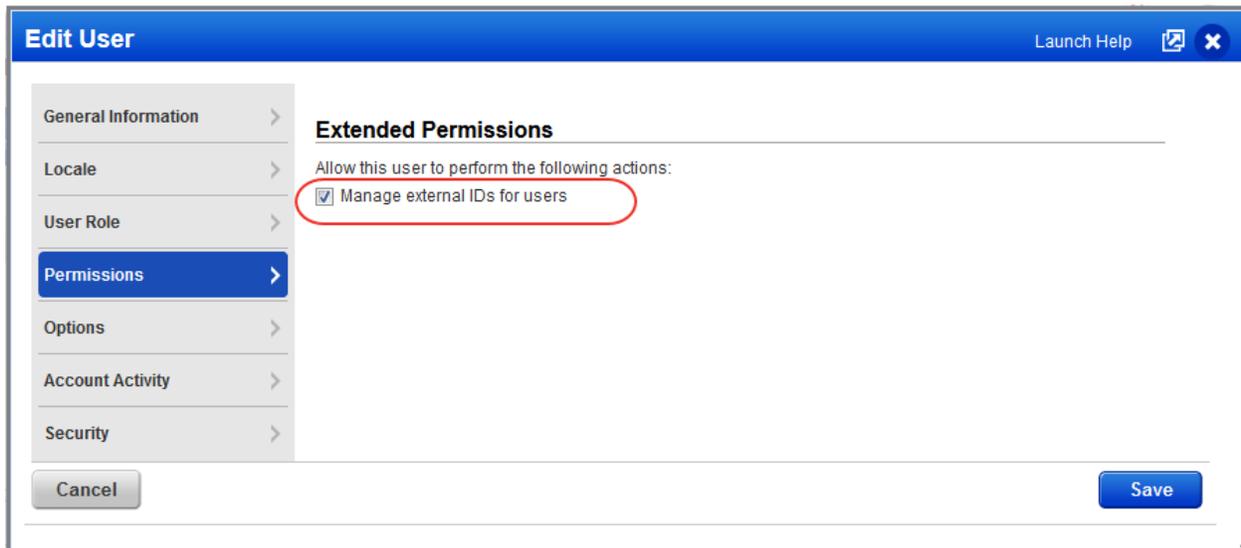


**External IDs**

As the Manager Primary Contact you can assign/edit the external ID for users. Select this option if you want to grant this permission to other Managers, Unit Managers and User Administrator. You do this by editing their account settings.

Allow other users to manage external IDs

- 2) Edit a manager’s account to grant this extended permission. Once granted, the manager can assign external IDs to other users.



**Edit User** Launch Help

General Information > **Extended Permissions**

Locale > Allow this user to perform the following actions:

User Role >  Manage external IDs for users

Permissions >

Options >

Account Activity >

Security >

Cancel Save

Last updated: April 7, 2021