Tenable Product SAML Quick Reference Guide

Last Revised: October 21, 2025

Table of Contents

Welcome to the Tenable SAML Quick Reference Guide

This guide exists to provide complete configuration steps to use SAML with Tenable products. If you are a Tenable One customer, you can configure a single SAML setup for all of your applications. Otherwise, some applications support individual SAML configuration at the application level.

Tip: For more information about Tenable One, see the *Tenable One Deployment Guide*.

What is SAML?

Security Assertion Markup Language (SAML) is an open standard that allows identity providers (IdP) to pass authorization credentials to service providers (SP). This means you can use one set of credentials to log into multiple websites. SAML is the link between the authentication of a user and that user's authorization to access an application.

SAML in Tenable Products

This guide includes the following information:

Product	Tenable One SAML Instructions?	Individual Application SAML Instructions?
Tenable Vulnerability Management	Yes	Same setup as Tenable One
Tenable Web App Scanning	Yes	Same setup as Tenable One
Tenable Cloud Security	Yes	Same setup as Tenable One
Tenable Identity Exposure	Yes	Yes
Tenable Exposure Management	Yes	N/A **Note:** Tenable Exposure Management is only available as part of the Tenable One package.

Tenable Attack Surface Management	Yes	Same setup as Tenable One
Tenable Security Center	N/A	Yes
Tenable FedRAMP Moderate Environments	Yes	Same setup as Tenable One

SAML for Tenable One

You can configure Tenable One products to accept credentials from your SAML identity provider. This allows for an additional layer of security, where the SAML credentials are certified for use within Tenable One. Once you enable SAML for a user, they can log in to Tenable One directly through their identity provider, which automatically signs them in and redirects them to the Tenable One Workspace landing page.

These instructions apply to the Tenable One product suite as well as the following products purchased individually. For more information, see the table on the Welcome page.

- Tenable Vulnerability Management
- Tenable Web App Scanning
- Tenable Cloud Security
- Tenable Attack Surface Management

While several configuration steps occur directly in the Tenable user interface, the entire SAML configuration process includes several processes across multiple applications. This guide describes three of the most commonly used Identity Providers (IdPs) and how to configure them for use with Tenable One SAML from start to finish.

> **Important:** Because Tenable One cannot accept private keys to decrypt SAML assertions, Tenable One does not support SAML assertion encryption. If you want to configure SAML authentication in Tenable One, choose an identity provider that does not require assertion encryption and confirm that assertion encryption is not enabled.

To get started, see the following topics:

- Tenable One: Okta IdP
- Tenable One: Ping Identity IdP
- Tenable One: Google Workspace IdP
- Tenable One: Microsoft Entra ID IdP
- Troubleshooting and Common Errors

Tenable One: Okta IdP

One of the most common IdPs used to configure SAML with Tenable One is Okta. The following steps guide you through the configuration process from start to finish.

Manual configuration requires the following:

- Login URL: A custom URL provided by Tenable in the following format:

  ```
  https://cloud.tenable.com/saml/login/PLACEHOLDER
  ```

  > **Tip:** FedRAMP environments use the following custom URL format: `https://fedcloud.tenable.com/saml/login/PLACEHOLDER`

- Audience URI (SP Entity ID): A custom ID provided by Tenable during SAML configuration in the following format:

  ```
  TENABLE_IO_PLACEHOLDER
  ```

- A certificate within the SAML metadata object that matches the data originally sent to Tenable.

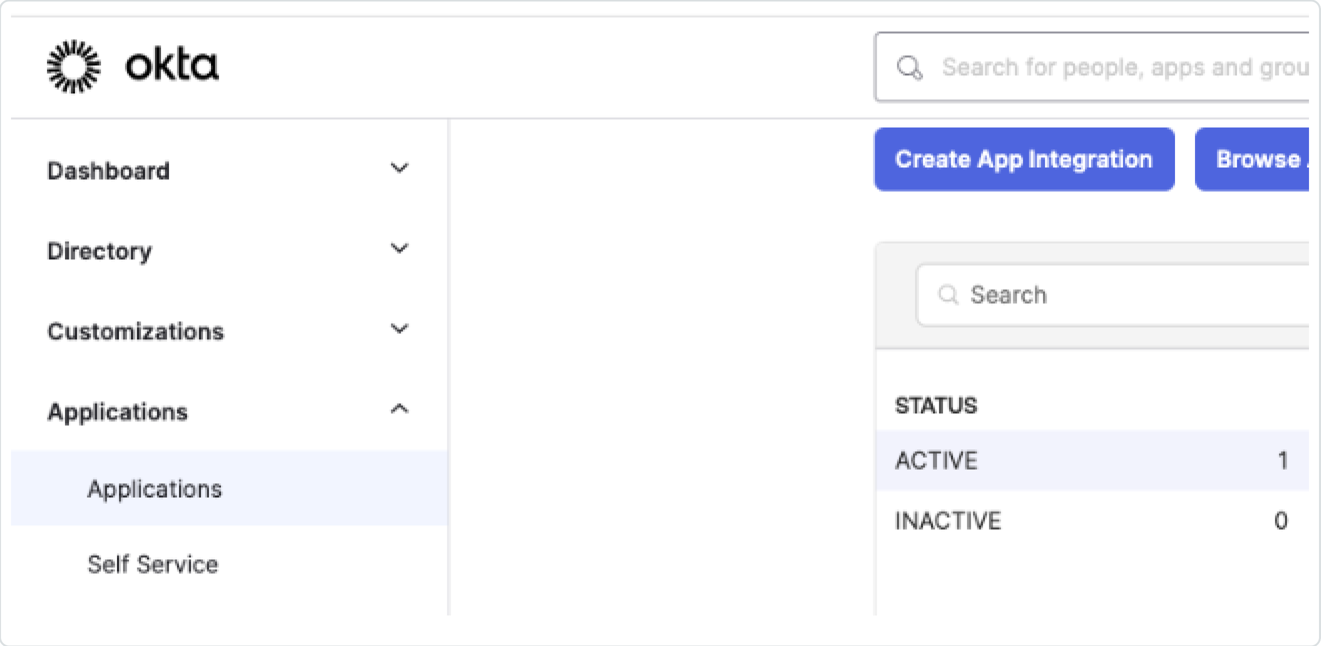
  > **Note:** Tenable does not support the use of multiple certificates and only extracts the first certificate from the metadata object. If the object includes multiple certificates, you must specify which certificate to use if it is not the first one listed.

Okta: Create Initial Application Integration

To create an application integration in Okta:

1. In your browser, navigate to the Okta Admin portal.
2. In the left navigation menu, click **Applications** > **Applications**.

   The application window appears.

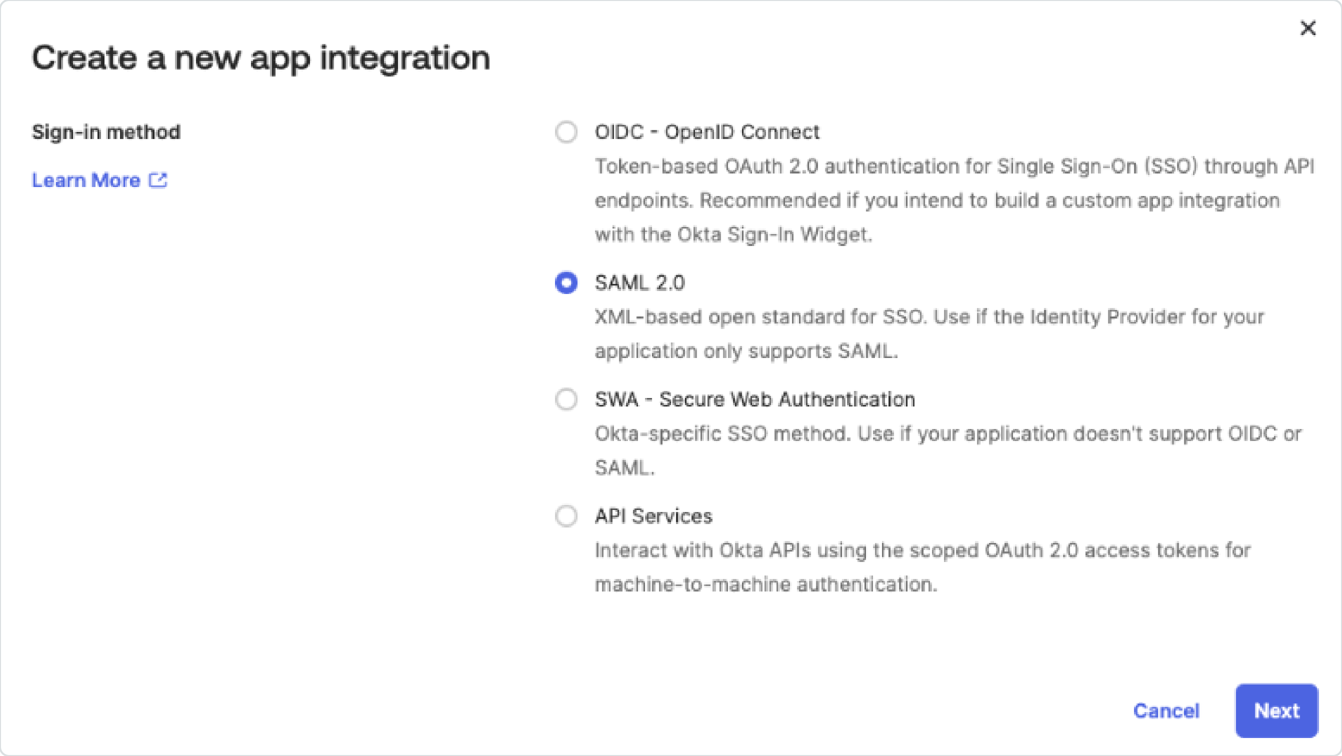


STATUS	
ACTIVE	1
INACTIVE	0

3. Click **Create App Integration**.

   The **Create a new app integration** window appears.

4. Select the **SAML 2.0** radio button.



Create a new app integration

Sign-in method

Learn More

○ OIDC - OpenID Connect
Token-based OAuth 2.0 authentication for Single Sign-On (SSO) through API endpoints. Recommended if you intend to build a custom app integration with the Okta Sign-In Widget.

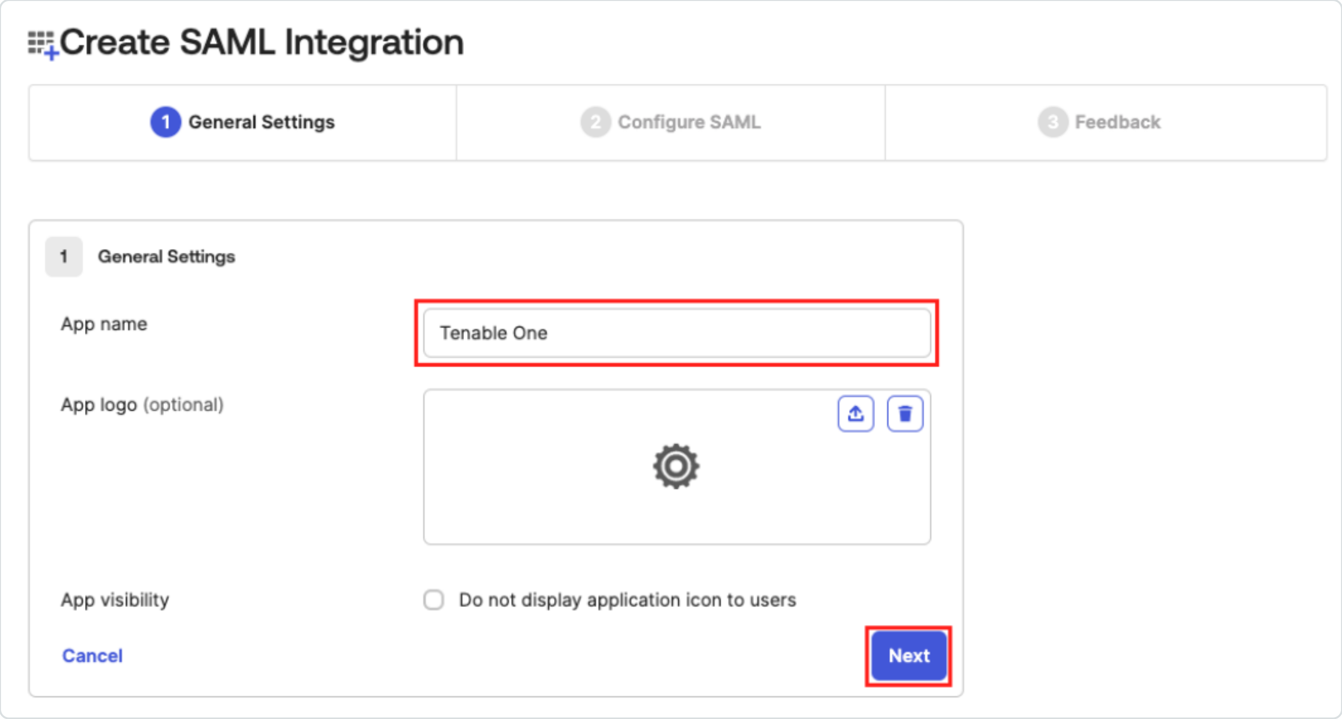
● SAML 2.0
XML-based open standard for SSO. Use if the Identity Provider for your application only supports SAML.

○ SWA - Secure Web Authentication
Okta-specific SSO method. Use if your application doesn't support OIDC or SAML.

○ API Services
Interact with Okta APIs using the scoped OAuth 2.0 access tokens for machine-to-machine authentication.

5. Click **Next**.

   The **General Settings** options appear.



Create SAML Integration

1 General Settings

App name: Tenable One

App logo (optional)

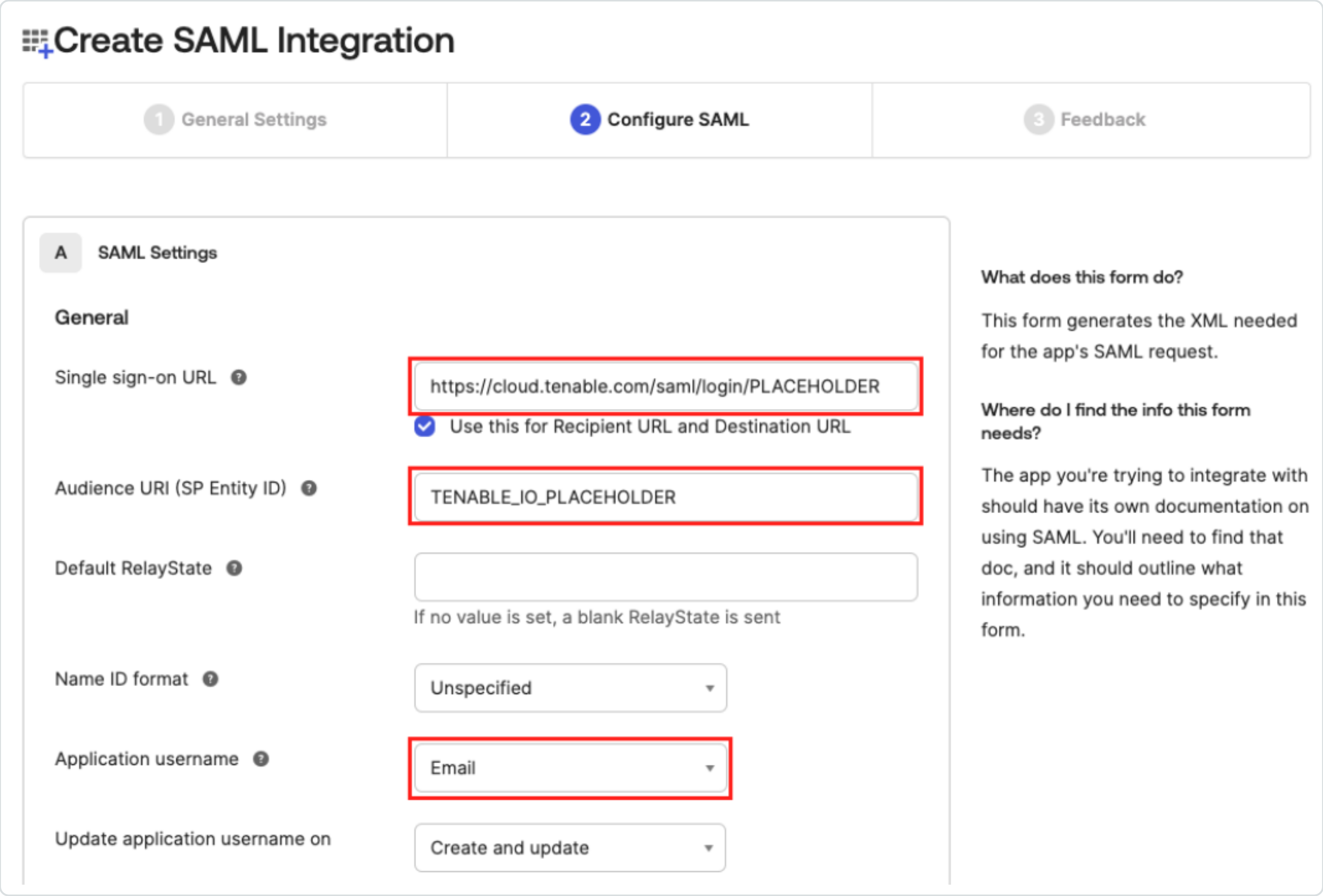
App visibility: □ Do not display application icon to users

6. In the **App name** text box, type a name for your application.

7. (Optional) To add a custom logo for the application, in the **App logo** section, upload a .png, .jpeg, or .gif file.

8. Click **Next**.

   The **Configure SAML** options appear.



Create SAML Integration

A SAML Settings

General

Single sign-on URL: https://cloud.tenable.com/saml/login/PLACEHOLDER

☑ Use this for Recipient URL and Destination URL

Audience URI (SP Entity ID): TENABLE_IO_PLACEHOLDER

Default RelayState:

If no value is set, a blank RelayState is sent

Name ID format: Unspecified

Application username: Email

Update application username on: Create and update

What does this form do?

This form generates the XML needed for the app's SAML request.

Where do I find the info this form needs?

The app you're trying to integrate with should have its own documentation on using SAML. You'll need to find that doc, and it should outline what information you need to specify in this form.

9. In the **Single sign-on URL** text box, type the following placeholder URL:

```
https://cloud.tenable.com/saml/login/PLACEHOLDER
```

> **Note:** You will later replace *PLACEHOLDER* with a unique UUID for the SAML configuration. This link is case-sensitive.

10. In the **Audience URI (SP Identity ID)** text box, type the following placeholder text:

```
TENABLE_IO_PLACEHOLDER
```

> **Note:** You will later replace *PLACEHOLDER* with a unique UUID for the SAML configuration.

11. In the **Application username** drop-down, select **Email**.

12. Leave all other default settings. For reference:

a. The **Use this for Recipient URL and Destination URL** check box is selected.

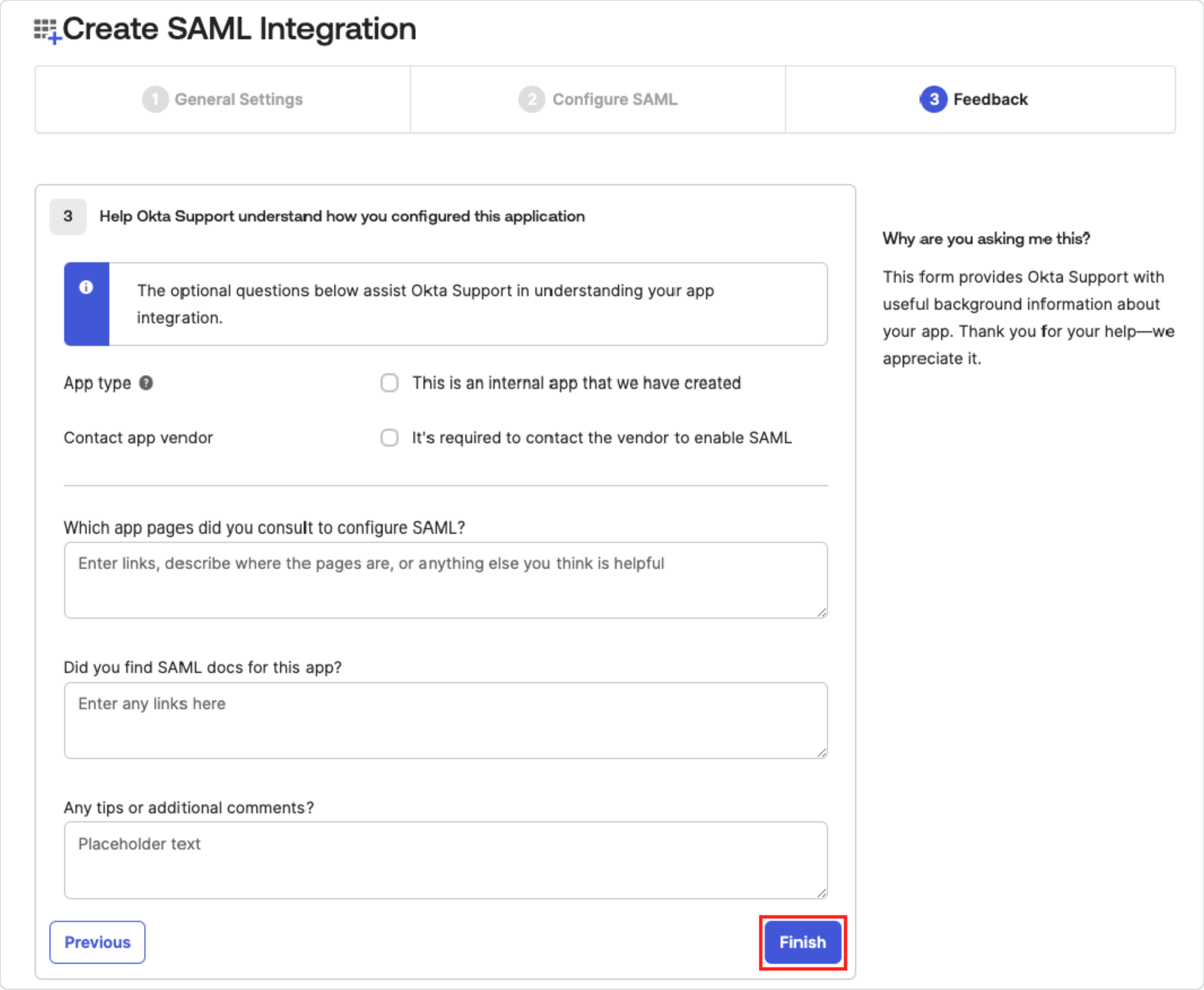
b. The **Default RelayState** text box is blank.

c. The **Name ID format** drop-down is set to **Unspecified**.

d. The **Update application username on** drop-down is set to **Create and update**.

13. Click **Next**.

The **Feedback** options appear.



Create SAML Integration

3 Help Okta Support understand how you configured this application

The optional questions below assist Okta Support in understanding your app integration.

App type: □ This is an internal app that we have created

Contact app vendor: □ It's required to contact the vendor to enable SAML

Which app pages did you consult to configure SAML?

Enter links, describe where the pages are, or anything else you think is helpful

Did you find SAML docs for this app?

Enter any links here

Any tips or additional comments?

Placeholder text

Why are you asking me this?

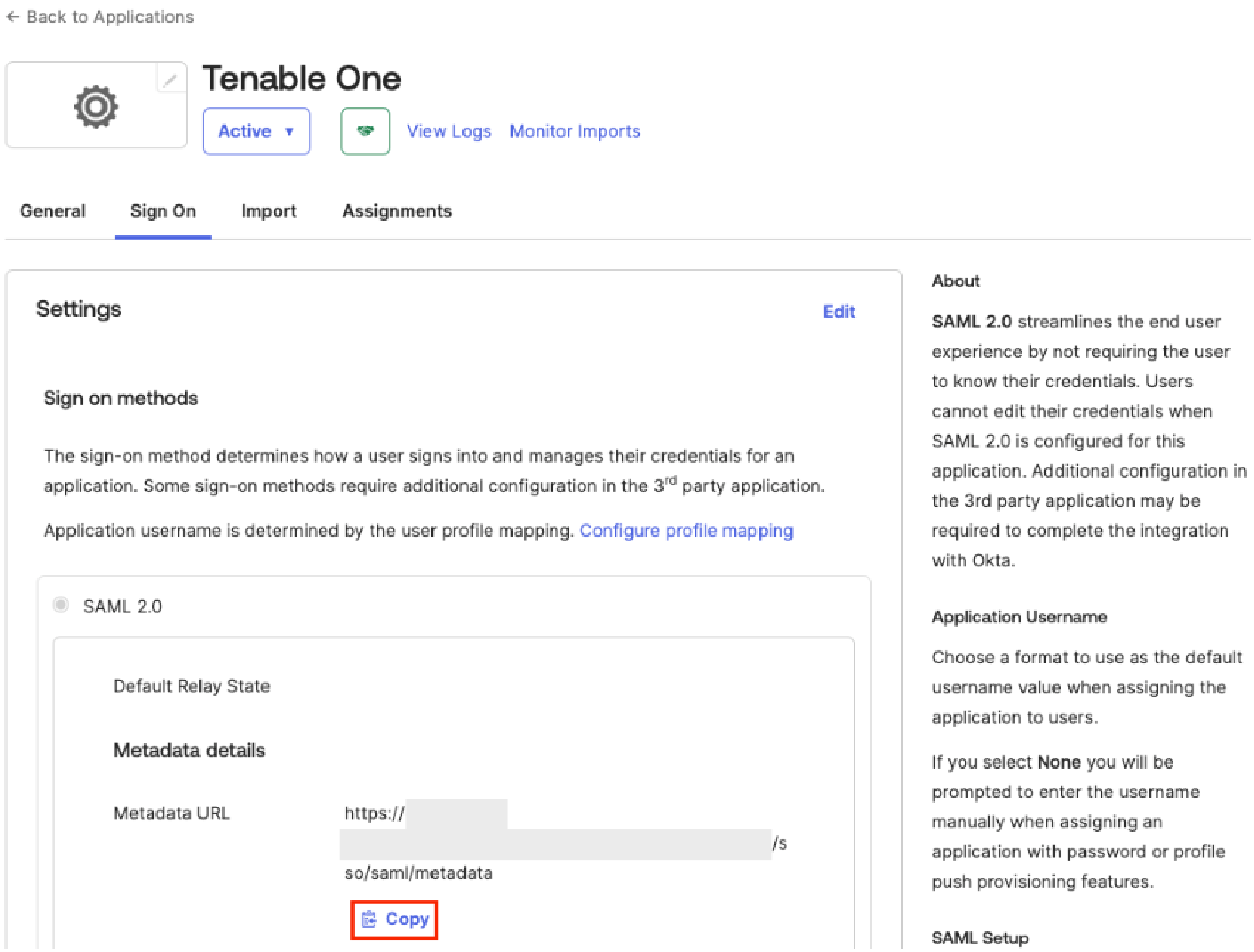
This form provides Okta Support with useful background information about your app. Thank you for your help—we appreciate it.

14. (Optional) Provide any feedback you want to include.

15. Click **Finish**.

Okta saves your application configuration and the new application's **Sign On** settings page appears.

16. Under **SAML 2.0** > **Metadata details** > **Metadata URL**, click **Copy**.



← Back to Applications

Tenable One

Active ▾ View Logs Monitor Imports

General Sign On Import Assignments

Settings Edit

Sign on methods

The sign-on method determines how a user signs into and manages their credentials for an application. Some sign-on methods require additional configuration in the 3rd party application.

Application username is determined by the user profile mapping. Configure profile mapping

○ SAML 2.0

Default Relay State

Metadata details

Metadata URL https://[redacted]/sso/saml/metadata

Copy

About

SAML 2.0 streamlines the end user experience by not requiring the user to know their credentials. Users cannot edit their credentials when SAML 2.0 is configured for this application. Additional configuration in the 3rd party application may be required to complete the integration with Okta.

Application Username

Choose a format to use as the default username value when assigning the application to users.

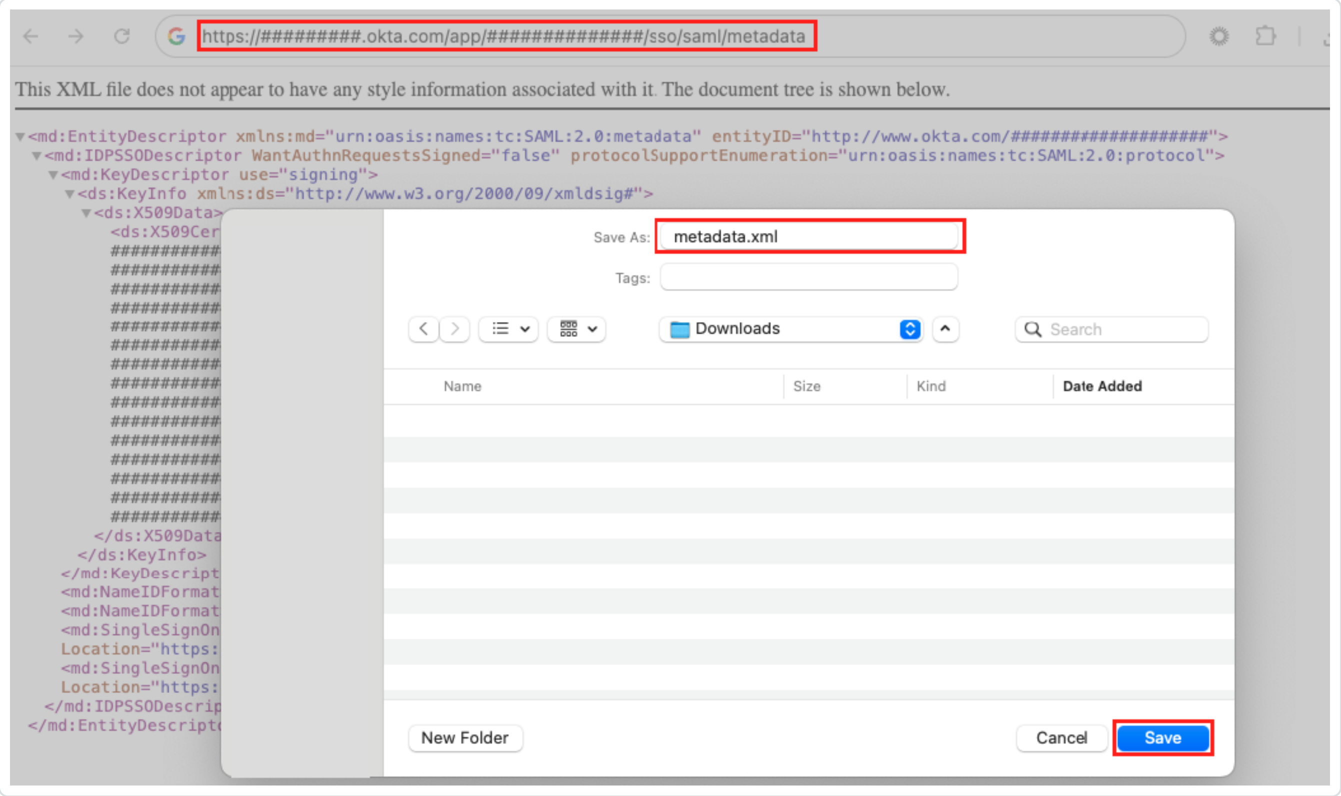
If you select **None** you will be prompted to enter the username manually when assigning an application with password or profile push provisioning features.

SAML Setup

17. In a new browser tab, navigate to the copied URL.

    The application's metadata appears in XML format.

18. In your browser, using the **Save Page As** option, save the resulting file as *metadata.xml*.



https://#########.okta.com/app/##############/sso/saml/metadata

This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
▼<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" entityID="http://www.okta.com/###################">
  ▼<md:IDPSSODescriptor WantAuthnRequestsSigned="false" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    ▼<md:KeyDescriptor use="signing">
      ▼<ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        ▼<ds:X509Data>
            <ds:X509Cer
            ###########
            ###########
            ###########
            ###########
            ###########
            ###########
            ###########
            ###########
            ###########
            ###########
            ###########
            ###########
            ###########
            ###########
            ###########
          </ds:X509Data
        </ds:KeyInfo>
      </md:KeyDescript
      <md:NameIDFormat
      <md:NameIDFormat
      <md:SingleSignOn
      Location="https:
      <md:SingleSignOn
      Location="https:
    </md:IDPSSODescrip
  </md:EntityDescript
```

Save As: metadata.xml

Tags:

Your browser downloads the metadata.xml file.

Tenable One SAML Configuration

Once you have downloaded your medata.xml file, you can use it to configure SAML in Tenable One. You can configure this directly in the Tenable Vulnerability Management application.

To set up the Tenable One SAML configuration:

1. In your browser, navigate to Tenable One.
2. On the **Workspace** page, click Tenable Vulnerability Management.

   The Tenable Vulnerability Management user interface appears.
3. In the upper-left corner, click the ☰ button.

   The left navigation plane appears.
4. In the left navigation plane, click **Settings**.

   The **Settings** page appears.

5. Click the **SAML** tile.

   The **SAML** page appears.

6. In the action bar, click ⊕ **Create**.

   The **SAML Settings** page appears.

7. Do one of the following:

To provide configuration details by uploading the metadata.xml file from your IdP:

a. In the first drop-down box, select **Import XML**.

> **Note**: **Import XML** is selected by default.

b. The **Type** drop-down box specifies the type of identity provider you are using. Tenable One supports SAML 2.0 (for example, Okta, OneLogin, etc.).
This option is read-only.

c. Under **Import**, click **Add File**.

   A file manager window appears.

d. Select the metadata.xml file.

   The metadata.xml file is uploaded.

To manually create your SAML configuration using data from the metadata.xml file from your IdP:

a. In the first drop-down box, select **Manual Entry**.

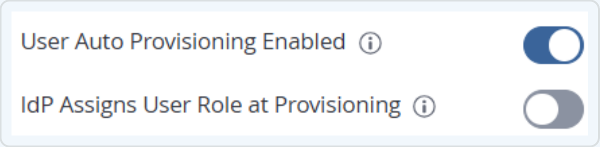
   A **SAML** configuration form appears.

b. Configure the settings described in the following table:

Settings	Description
Enabled toggle	A toggle in the upper-right corner that indicates whether the SAML configuration is enabled or disabled.

	By default, the **Enable** setting is set to **Enabled**. Click the toggle to disable SAML configuration.
Type	Specifies the type of identity provider you are using. Tenable One supports SAML 2.0 (for example, Okta, OneLogin, etc.). This option is read-only.
Description	A description for the SAML configuration.
IdP Entity ID	The unique entity ID that your IdP provides. **Note**: If you want to configure multiple IdPs for a user account, create a new configuration for each identity provider with separate identity provider URLs, entity IDs, and signing certificates.
IdP URL	The SAML URL for your IdP.
Certificate	Your IdP security certificate or certificates. **Note**: Security certificates are found in a metadata.xml file that your identity provider provides. You can copy the content of the file and paste it in the **Certificate** box.
Authentication Request Signing Enabled	A toggle that indicates whether authentication request signing is enabled. When this toggle is enabled, if: • a user is logged in via SAML and their session expires • a user logs out and tries to log back in directly via the Tenable One interface rather than their IdP Tenable One automatically signs the SAML authentication request that is sent to the IdP to log the user back in. **Note:** The authentication request can only be validated if the IdP

	is also configured to accept this setting. For more information, see the following resources: - Manage Signing Certificates in Okta - Enforce Signed SAML Authentication Requests in Microsoft Entra ID - Edit a SAML Application in Ping Identity (**Enforce Signed AuthnRequest** option)
User Auto Provisioning Enabled	A toggle that indicates whether automatic user account creation is enabled or disabled. Automatic account provisioning allows users with an account for the IdP named in the SAML configuration to create a Tenable Vulnerability Management account the first time they log in via the IdP. **Note:** This option only appears during intial configuration if the setup is manual. Otherwise, you must edit the configuration after initial setup to enable this option.
IdP Assigns User Role at Provisioning	To assign a user role during provisioning, enable this toggle. In your SAML identity provider, add an attribute statement with **userRoleUuid** as the attribute name and the user role UUID as the attribute value. To obtain the UUID for a user role, go to **Settings** > **Access Control** > **Roles**. **Note:** This option only appears during intial configuration if the setup is manual. Otherwise, you must edit the configuration after initial setup to enable this option. **Note:** To access this option, you must first enable the **User Autoprovisioning Enabled** option.

	 User Auto Provisioning Enabled ⓘ ● IdP Assigns User Role at Provisioning ⓘ ○
IdP Resets User Role at Each Login	To assign a role each time a user logs in, overwriting the current role with the one chosen in your IdP, enable this toggle. In your SAML identity provider, add an attribute statement with **userRoleUuid** as the attribute name and the user role UUID as the attribute value. To obtain the UUID for a user role, go to **Settings** > **Access Control** > **Roles**. **Note:** This option only appears during intial configuration if the setup is manual. Otherwise, you must edit the configuration after initial setup to enable this option.
Group Management Enabled	Enable this toggle to allow the Tenable One SAML configuration to manage user groups. You must enable this toggle for the Managed by SAML option to function successfully.

8. Click **Save**.

   Tenable Vulnerability Management saves your SAML configuration and you return to the **SAML** page.

9. In the row for the SAML configuration you just created, click the ⋮ button.

   An actions menu appears.

10. Click **Download SAML SP metadata**.

    Your browser downloads the metadata.xml file. You can now use this file for final configuration in your IdP.

Optional: Configure One or More User Groups to Automatically Add a User upon SAML Login

User groups allow you to manage user permissions for various resources in Tenable One. When you assign users to a group, the users inherit the permissions assigned to the group. When you enable the **Managed by SAML** option for a user group, Tenable One allows you to automatically add any user that logs in via SAML to that group.

> **Important:** For this option to work successfully, you must also configure the related group claim within your IdP. View the final IdP configuration steps for more information.

Before you begin:

Ensure you've enabled the Group Management Enabled toggle when configuring the SAML settings within Tenable One.

To enable the Managed by SAML option:

1. In Tenable Vulnerability Management, in the upper-left corner, click the ☰ button.

   The left navigation plane appears.

2. In the left navigation plane, click **Settings**.

   The **Settings** page appears.

3. Click the **Access Control** tile.

   The **Access Control** page appears.

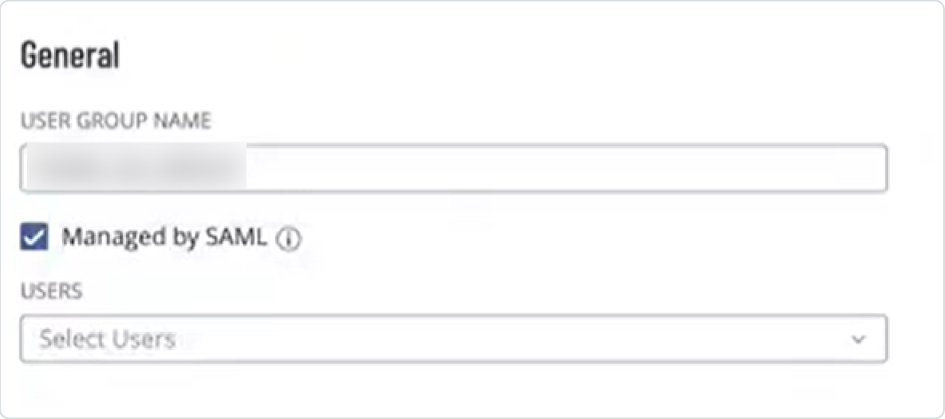
4. Click the **Groups** tab.

   The **Groups** page appears.

5. In the user groups table, click the user group to which you want to automatically add your SAML users.

   The **Edit User Group** page appears.

6. In the **General** section, select the **Managed by SAML** check-box.



General

USER GROUP NAME

☑ Managed by SAML

USERS

Select Users

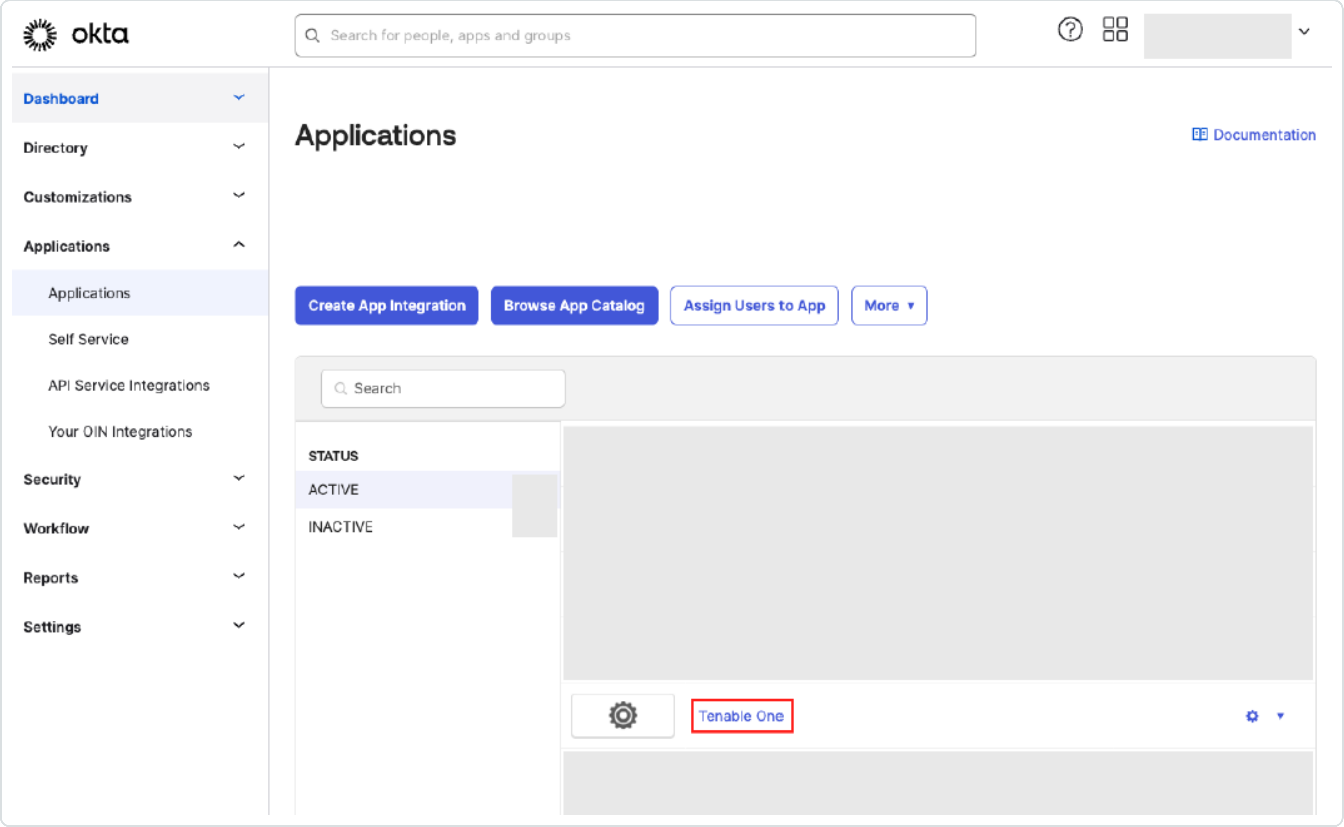
7. Click **Save**. Tenable Vulnerability Management saves your changes. Once you configure the related claim within your IdP, any time a user logs in via your SAML configuration, Tenable One automatically adds them to the specified user group.

Okta: Configure Final Application Integration and Upload Metadata

Now that you have downloaded the completed metadata file, you can use that file to finalize the Tenable application configurations in Okta.

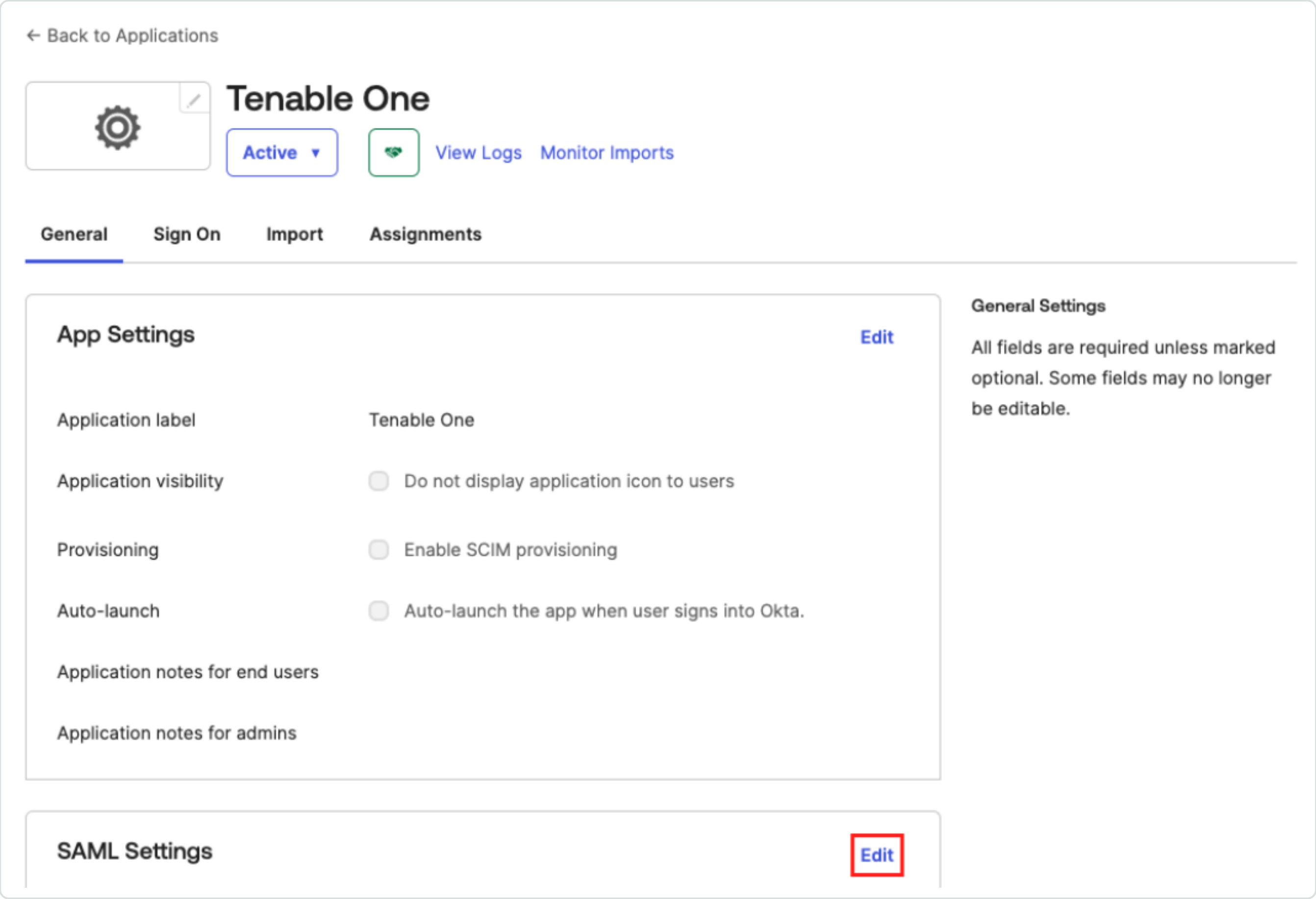
1. In your browser, navigate to the Okta Admin portal.
2. In the left navigation menu, click **Applications** > **Applications**.

   The **Applications** page appears.



3. Select the application you previously created.

   The **General** page appears.



Tenable One

App Settings

Application label	Tenable One
Application visibility	□ Do not display application icon to users
Provisioning	□ Enable SCIM provisioning
Auto-launch	□ Auto-launch the app when user signs into Okta.
Application notes for end users	
Application notes for admins	

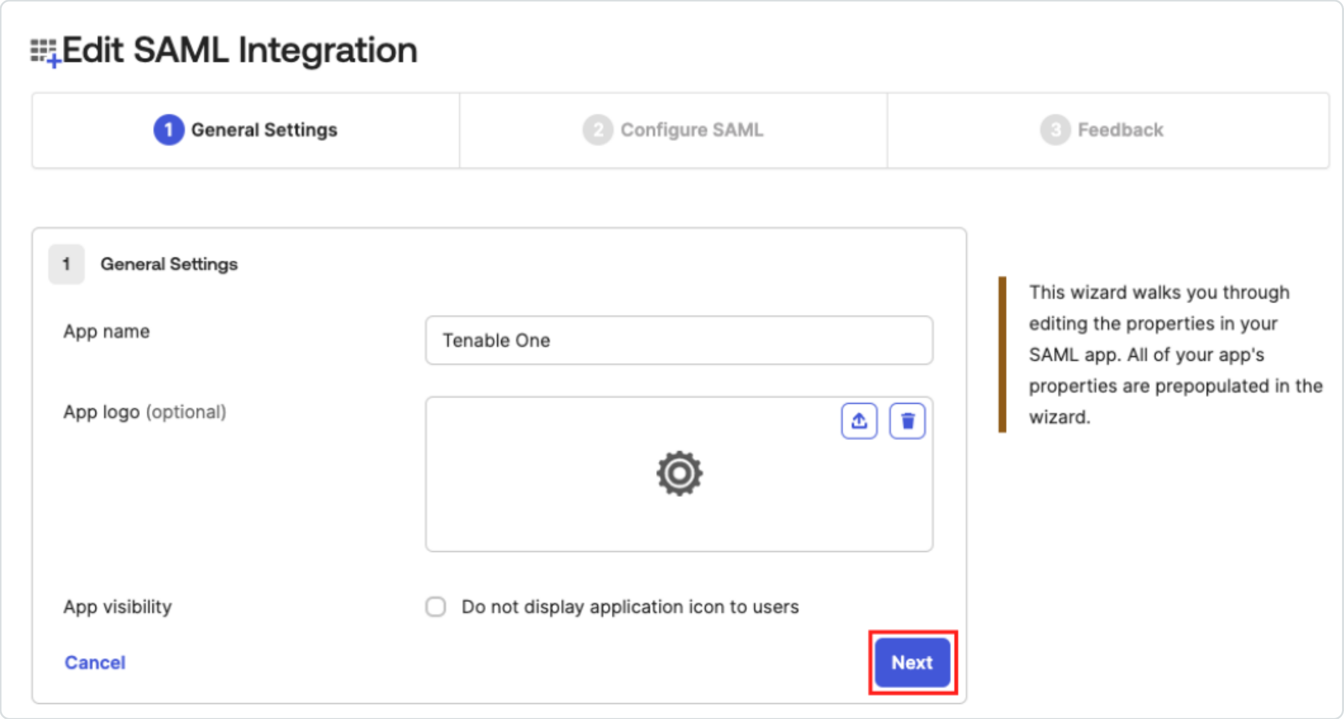
General Settings

All fields are required unless marked optional. Some fields may no longer be editable.

SAML Settings

4. In the **SAML Settings** section, click **Edit**.

   The **General Settings** page appears.



Edit SAML Integration

1 General Settings | 2 Configure SAML | 3 Feedback

1 General Settings

App name: Tenable One

App logo (optional)

App visibility: ☐ Do not display application icon to users

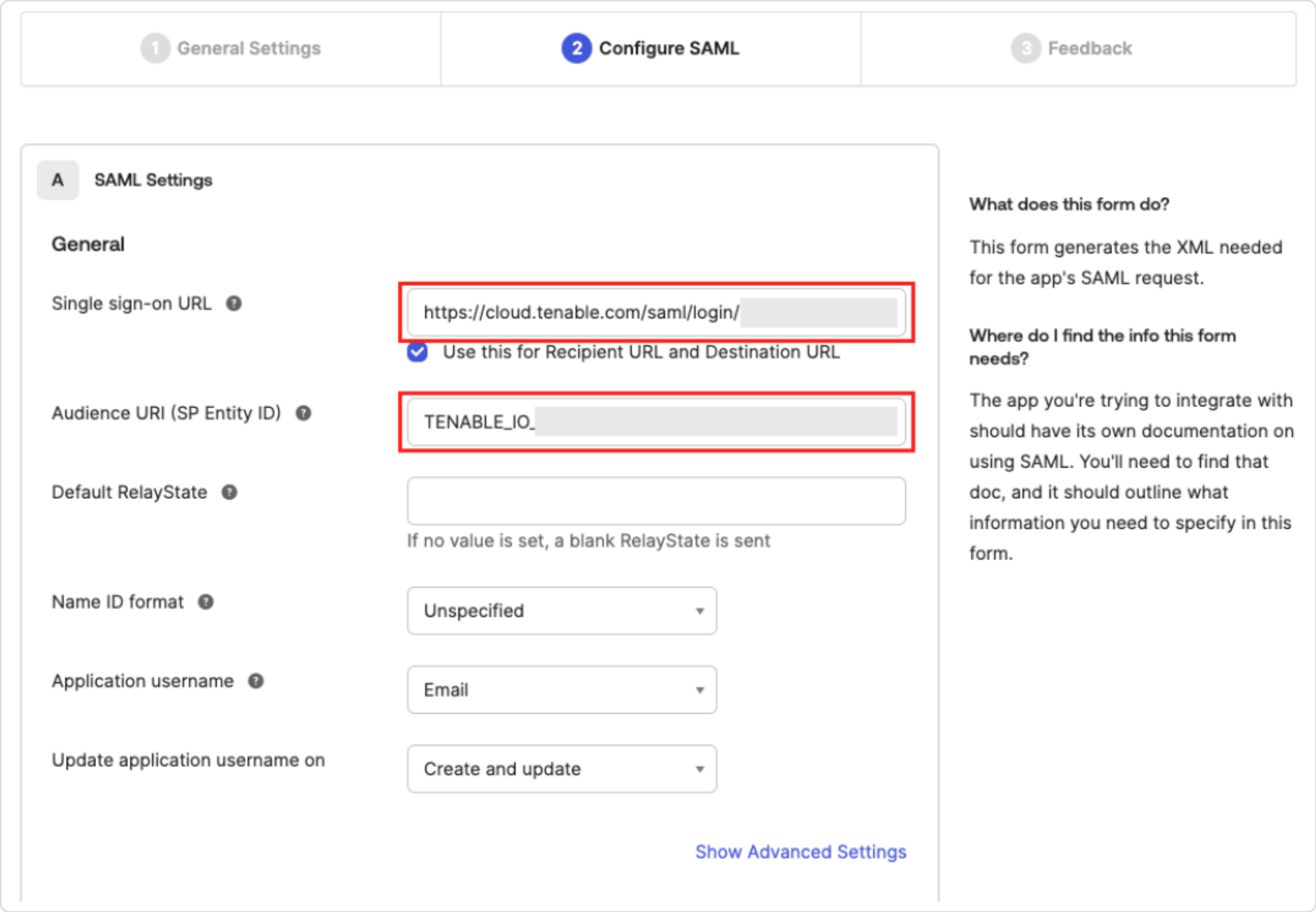
Cancel

Next

This wizard walks you through editing the properties in your SAML app. All of your app's properties are prepopulated in the wizard.

5. Click **Next**.

   The **Configure SAML** options appear.



1 General Settings | 2 Configure SAML | 3 Feedback

A SAML Settings

General

Single sign-on URL: https://cloud.tenable.com/saml/login/

☑ Use this for Recipient URL and Destination URL

Audience URI (SP Entity ID): TENABLE_IO_

Default RelayState:

If no value is set, a blank RelayState is sent

Name ID format: Unspecified

Application username: Email

Update application username on: Create and update

Show Advanced Settings

What does this form do?

This form generates the XML needed for the app's SAML request.

Where do I find the info this form needs?

The app you're trying to integrate with should have its own documentation on using SAML. You'll need to find that doc, and it should outline what information you need to specify in this form.

6. In the **Single sign-on URL** text box, replace the previously submitted placeholder with the URL listed in the metadata.xml file that you downloaded from Tenable One.

   Tip: This URL is in the following format: https://cloud.tenable.com/saml/login/*PLACEHOLDER*.

7. In the **Audience URI (SP Identity ID)** text box, replace the previously submitted placeholder with the ID listed in the metadata.xml file that you downloaded from Tenable One.

   Tip: This ID is in the following format: TENABLE_IO_*PLACEHOLDER*.

8. Click **Next**.

   The **Feedback** options appear.

9. Click **Finish**.

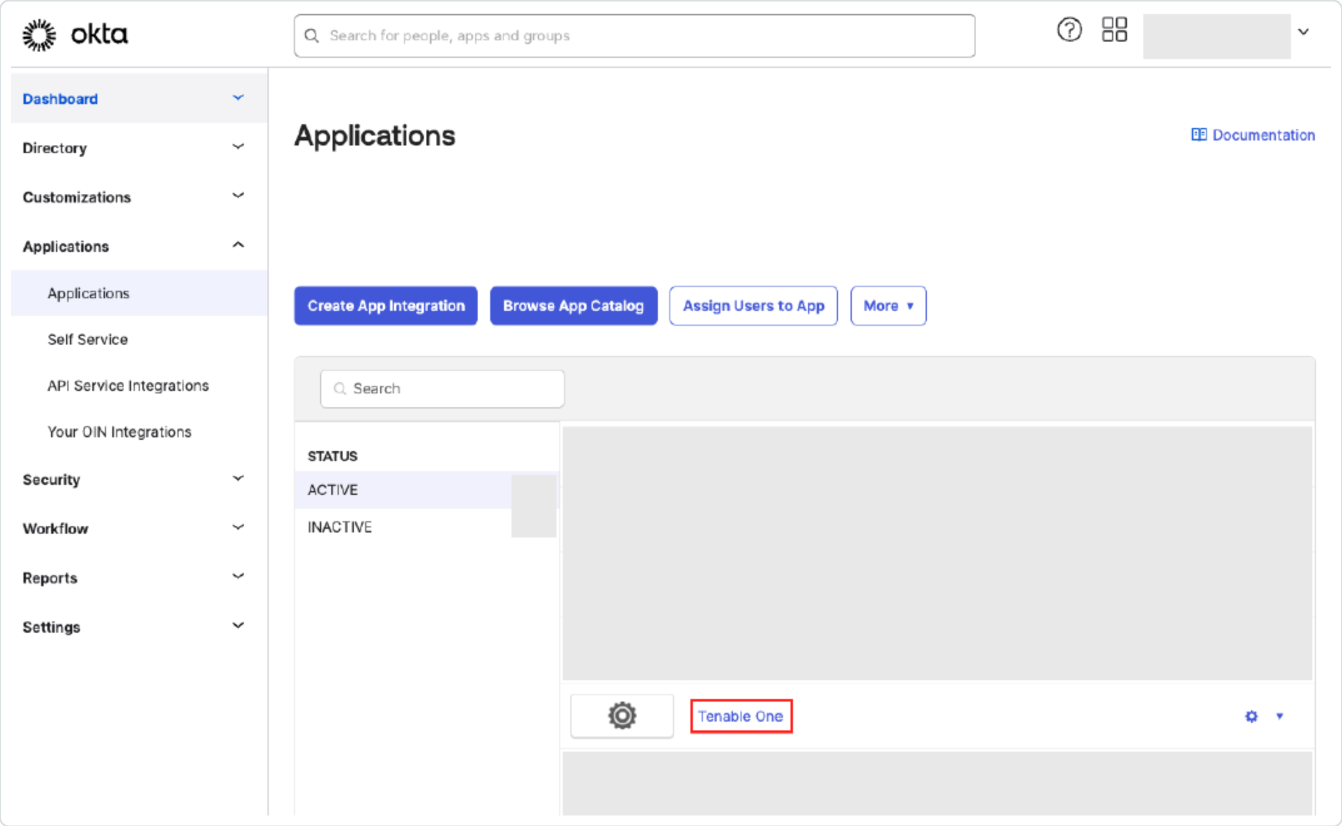
   Okta saves your changes to the application.

Assign Users and/or Groups to the Okta Application

To assign the application to your users or groups:

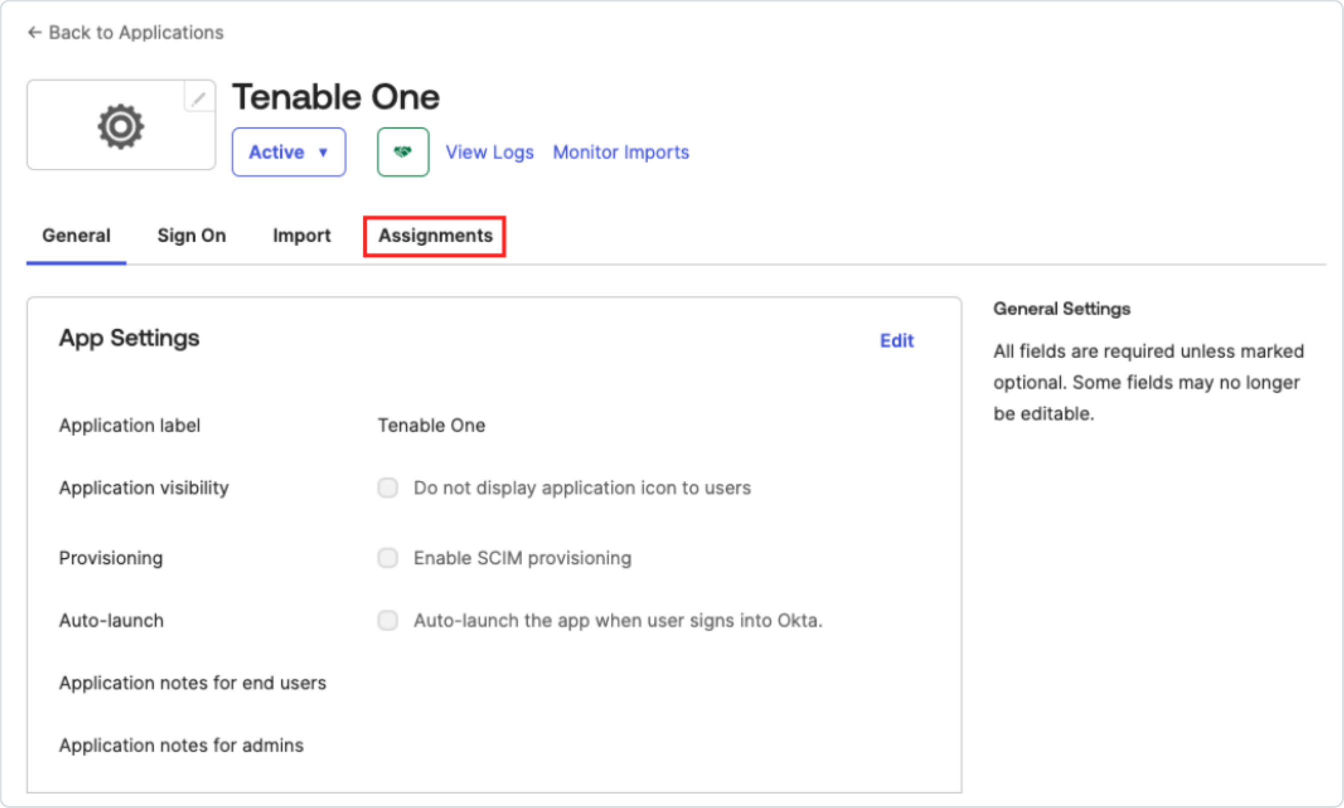
1. In your browser, navigate to the Okta Admin portal.
2. In the left navigation menu, click **Applications** > **Applications**.

   The **Applications** page appears.



3. Select the application you previously created.

   The **General** page appears.
4. Click the **Assignments** tab.



Tenable One

App Settings

Application label Tenable One

Application visibility □ Do not display application icon to users

Provisioning □ Enable SCIM provisioning

Auto-launch □ Auto-launch the app when user signs into Okta.

Application notes for end users

Application notes for admins

General Settings

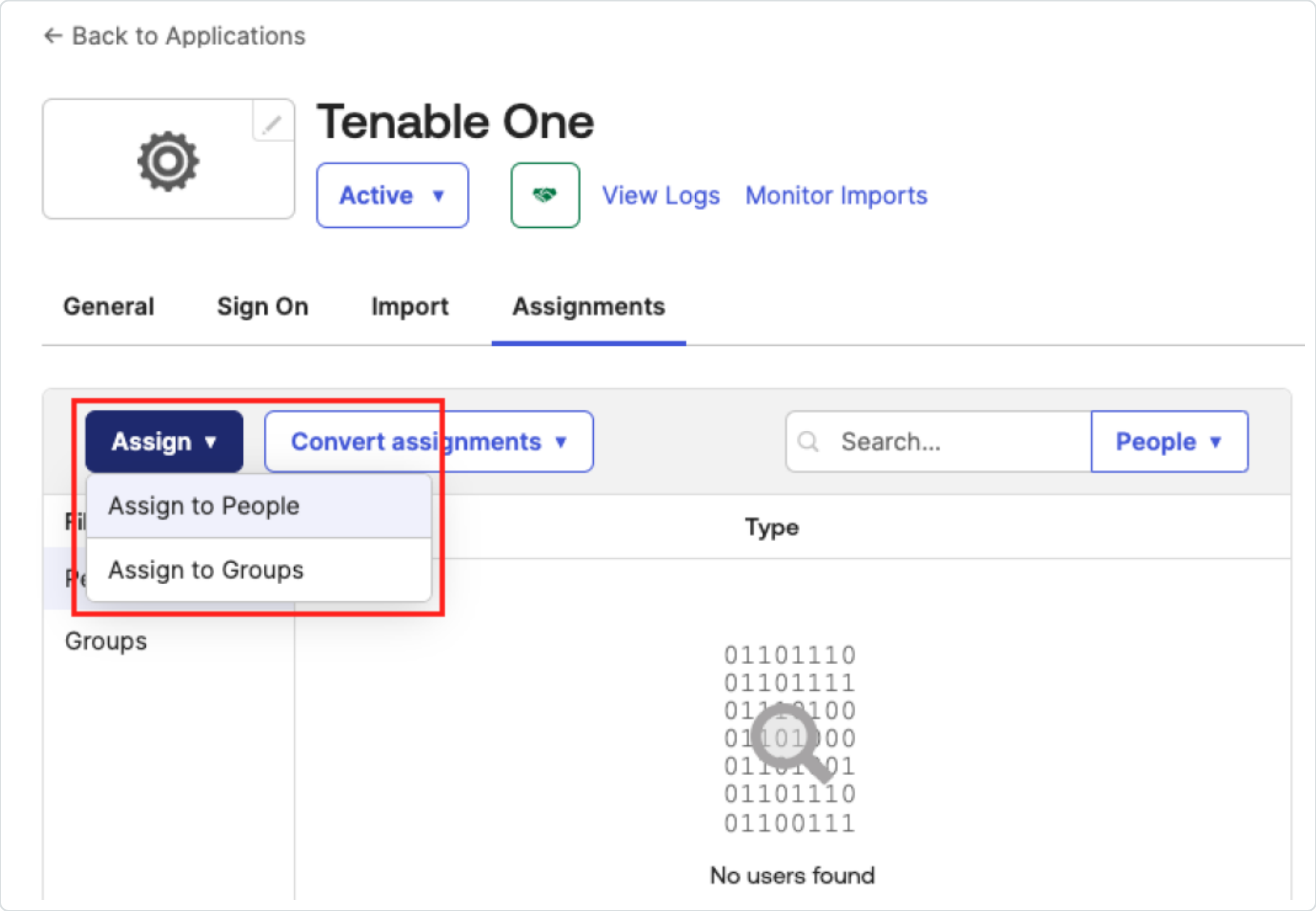
All fields are required unless marked optional. Some fields may no longer be editable.

The **Assignments** page appears.

5. Click the **Assign** button and, in the drop-down, select one or both of the following:

   - **Assign to People** — Any assigned users will have access to this application within their Okta My Apps dashboard, and will be able to login to Tenable One.

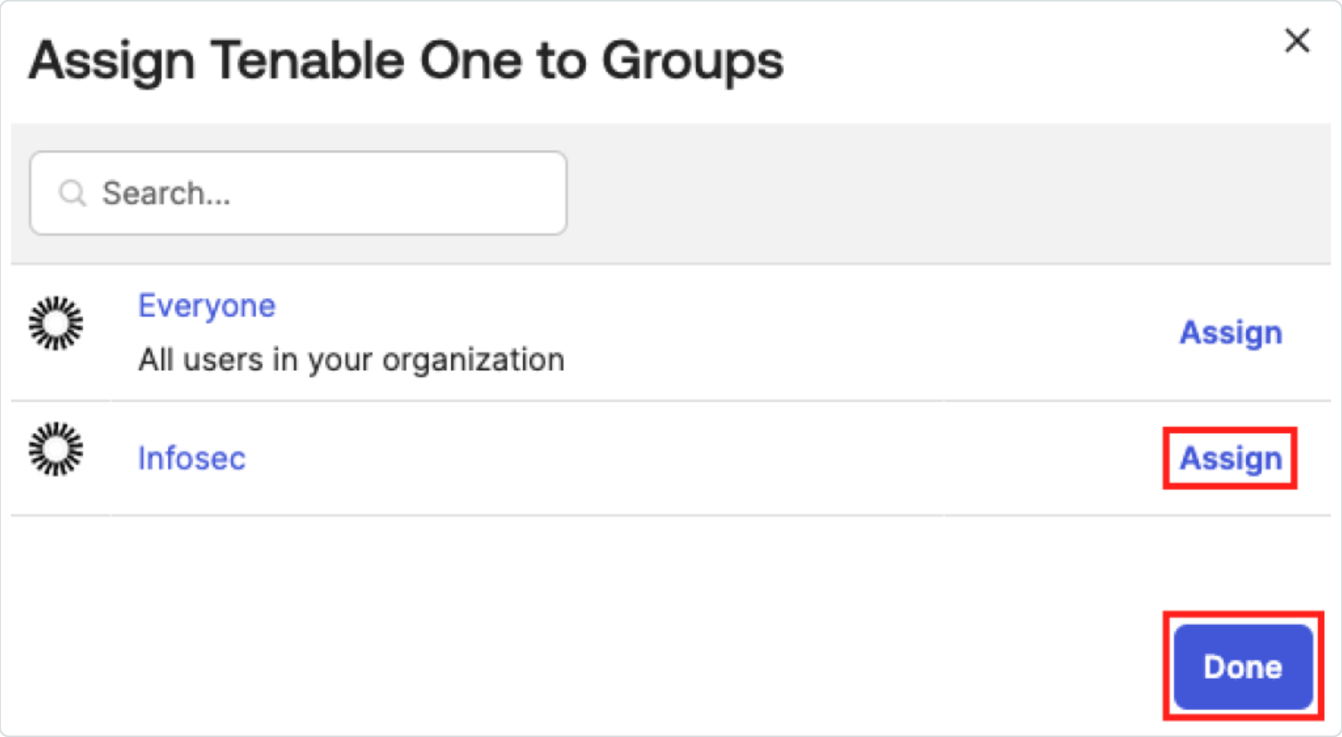
   - **Assign to Groups** — Any users within assigned groups will have access to this application within their Okta My Apps dashboard, and will be able to login to Tenable One.



> **Important:** If you've opted to optionally **Configure One or More User Groups to Automatically Add a User upon SAML Login**, ensure any assigned group name in Okta matches the user group name within Tenable One. If the names do not match, the user and/or user group link will fail.

An **Assign** window appears.

6. Next to the user or group to which you want to assign the application, click **Assign**.



Assign Tenable One to Groups

Everyone
All users in your organization

Infosec

7. Repeat for each user or group to which you want to assign the application.

8. Click **Done**.

   Okta saves your changes, and your configuration is ready for use.

Optional: Finalize Configuration for Managed by SAML Group Option

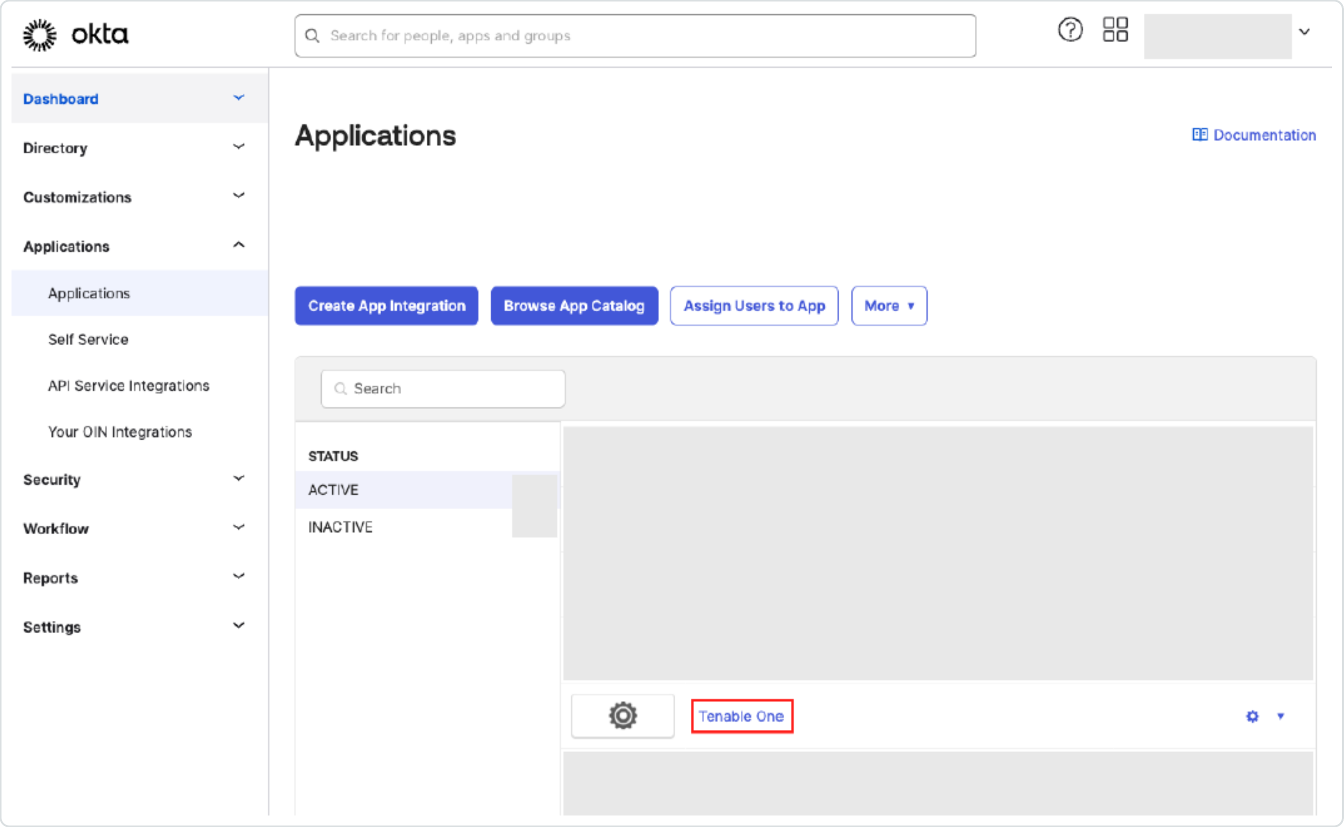
If you enabled the **Managed by SAML** option to automatically add any user that logs in via SAML to a user group, then you must configure a related group claim within the Okta IdP.

To configure the IdP group claim:

1. In your browser, navigate to the Okta Admin portal.

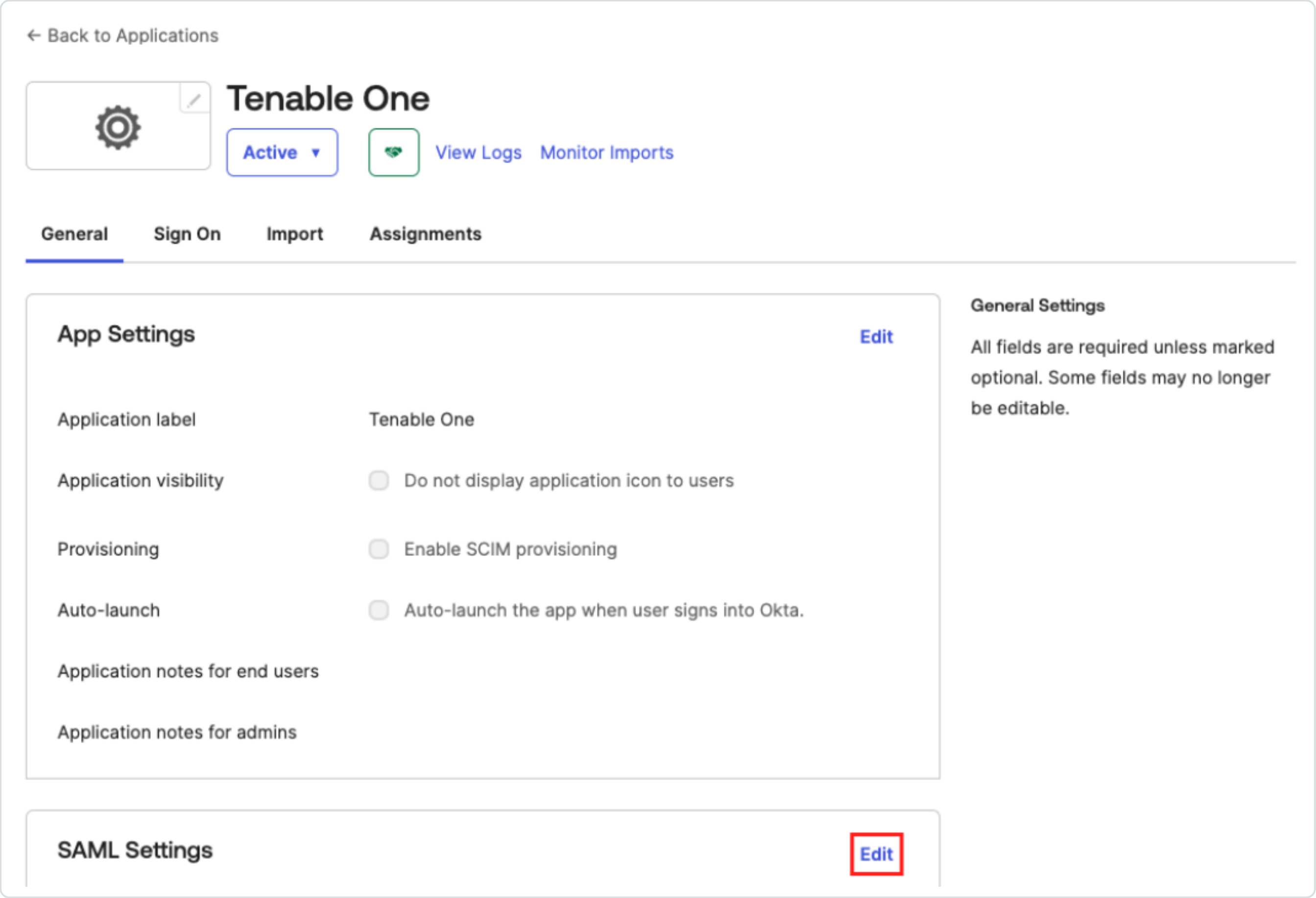
2. In the left navigation menu, click **Applications** > **Applications**.

   The **Applications** page appears.



3. Select the application you previously created.

   The **General** page appears.



← Back to Applications

Tenable One

Active ▾ | View Logs | Monitor Imports

General | Sign On | Import | Assignments

App Settings — Edit

Application label: Tenable One

Application visibility: □ Do not display application icon to users

Provisioning: □ Enable SCIM provisioning

Auto-launch: □ Auto-launch the app when user signs into Okta.

Application notes for end users

Application notes for admins

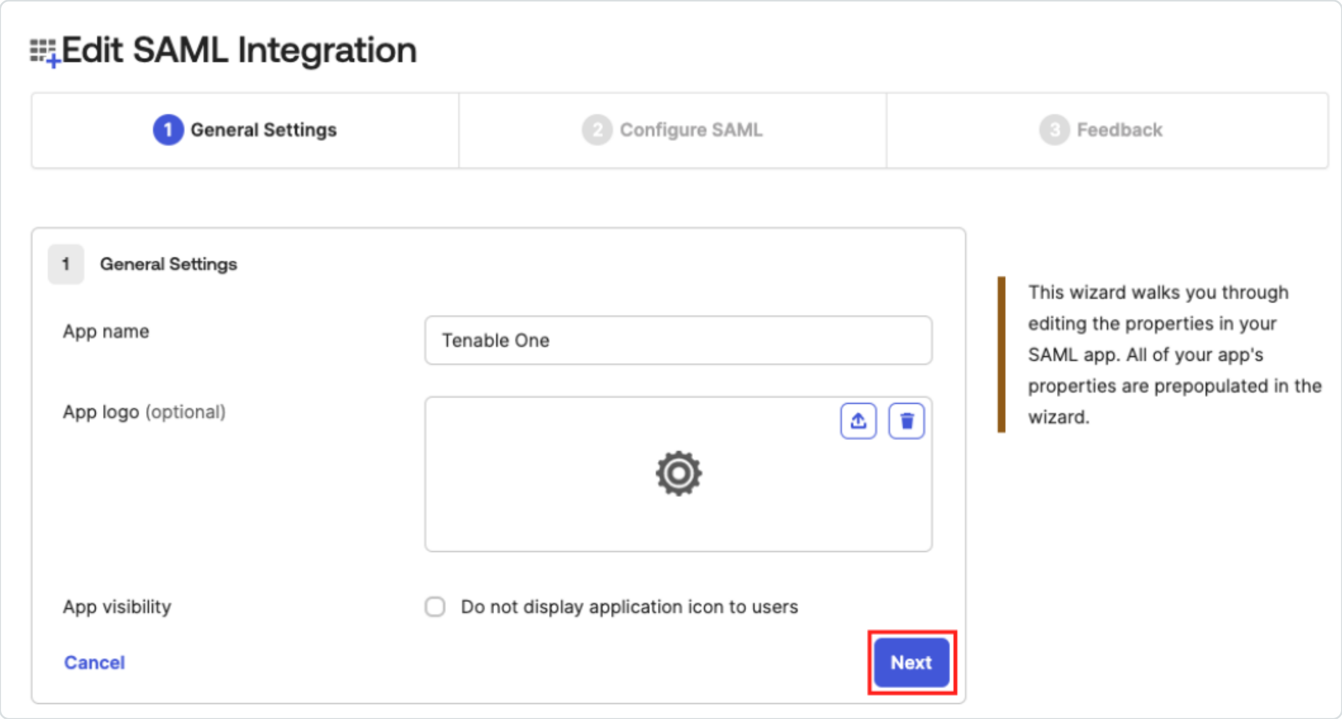
General Settings

All fields are required unless marked optional. Some fields may no longer be editable.

SAML Settings — Edit

4. In the **SAML Settings** section, click **Edit**.

   The **General Settings** page appears.



Edit SAML Integration

1 General Settings

App name: Tenable One

App logo (optional)

App visibility: □ Do not display application icon to users

This wizard walks you through editing the properties in your SAML app. All of your app's properties are prepopulated in the wizard.

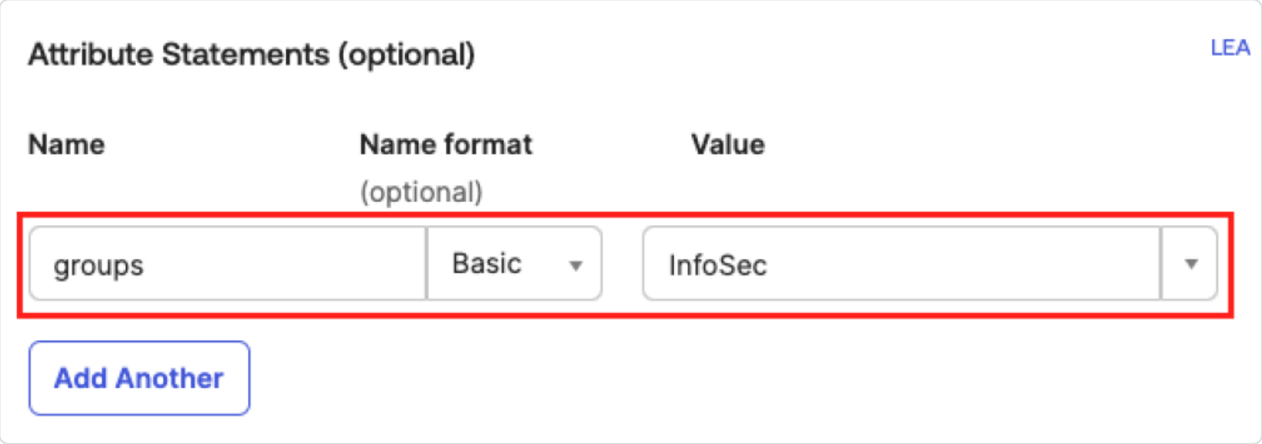
5. Click **Next**.

   The **Configure SAML** options appear.

6. Do one of the following:

   - To map all users to the same group:

     In the **Attribute Statements** section, insert the following values:



Attribute Statements (optional)

Name	Name format (optional)	Value
groups	Basic	InfoSec

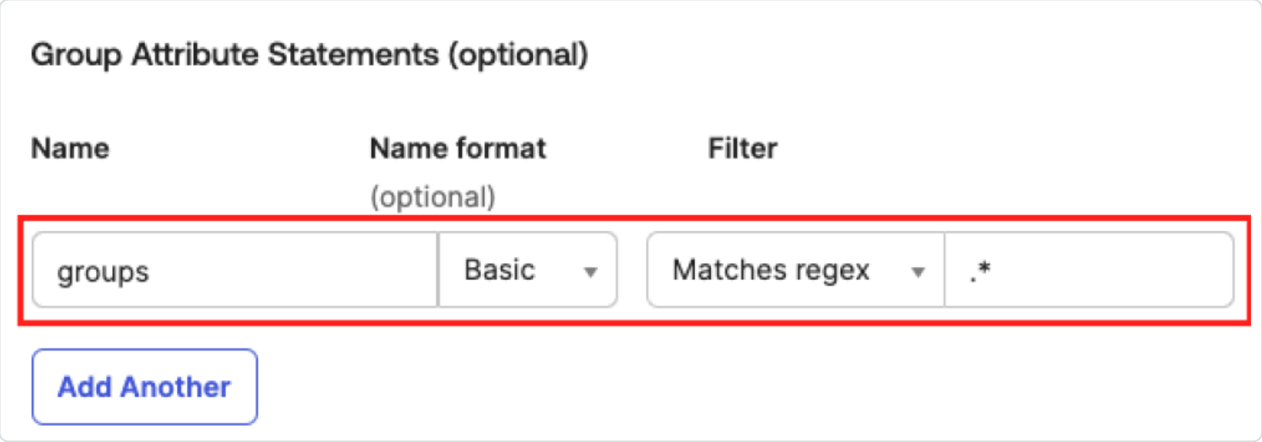
a. In the **Name** text box, type **groups**.

b. In the **Name format** drop-down, select **Basic**.

c. In the **Value** text box, type the group name that corresponds to the existing Tenable One group (for example, **InfoSec**).

- To map all users to groups based on their individual group membership within Okta:

  In the **Group Attribute Statements** section, insert the following values:



Group Attribute Statements (optional)

Name	Name format (optional)	Filter	
groups	Basic	Matches regex	.*

a. In the **Name** text box, type **groups**.

b. In the **Name format** drop-down, select **Basic**.

c. In the **Filter** boxes, select **Matches regex** and then type **.***.

7. Click **Next**.

   The **Feedback** options appear.

8. Click **Finish**.

   Any time a user assigned to this Okta group name logs in via your SAML configuration, Tenable One automatically adds them to the specified matching user group within Tenable One.

Optional: Finalize Configuration for Managed by SAML Role Option

Roles allow you to manage privileges for major functions in Tenable One and control which Tenable One resources users can access.

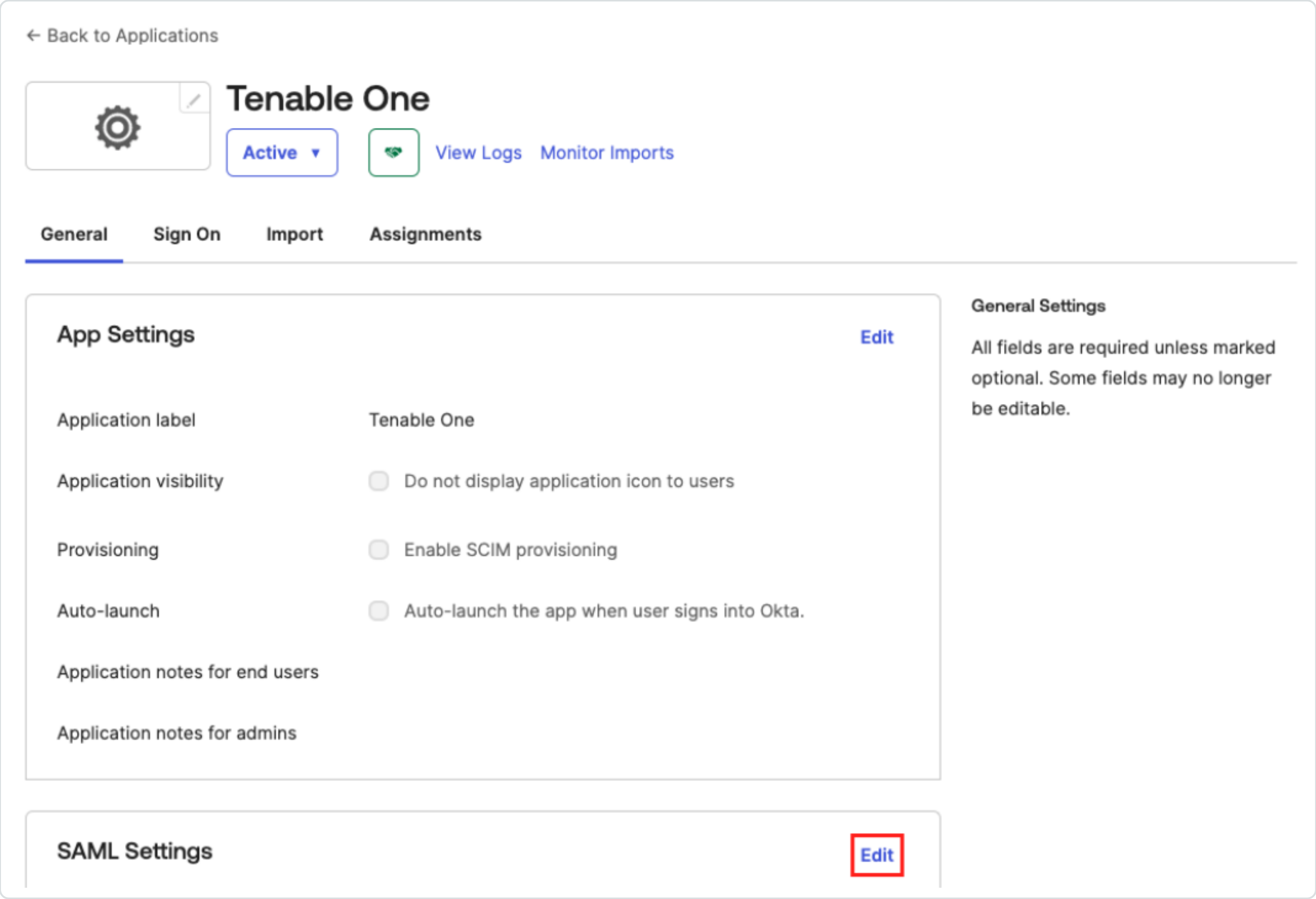
If you enabled the **IdP Assigns User Role at Provisioning** and/or **IdP Resets User Role at Each Login** (to automatically add and/or assign any user that logs in via SAML to a user role) settings, then you must complete the following steps within Okta:

To configure the managed by SAML role option:

1. In your browser, navigate to the Okta Admin portal.
2. In the left navigation menu, click **Applications** > **Applications**.

   The **Applications** page appears.
3. Select the application you previously created.

   The **General** page appears.

   Tenable One

   App Settings

Application label	Tenable One
Application visibility	□ Do not display application icon to users
Provisioning	□ Enable SCIM provisioning
Auto-launch	□ Auto-launch the app when user signs into Okta.
Application notes for end users	
Application notes for admins	

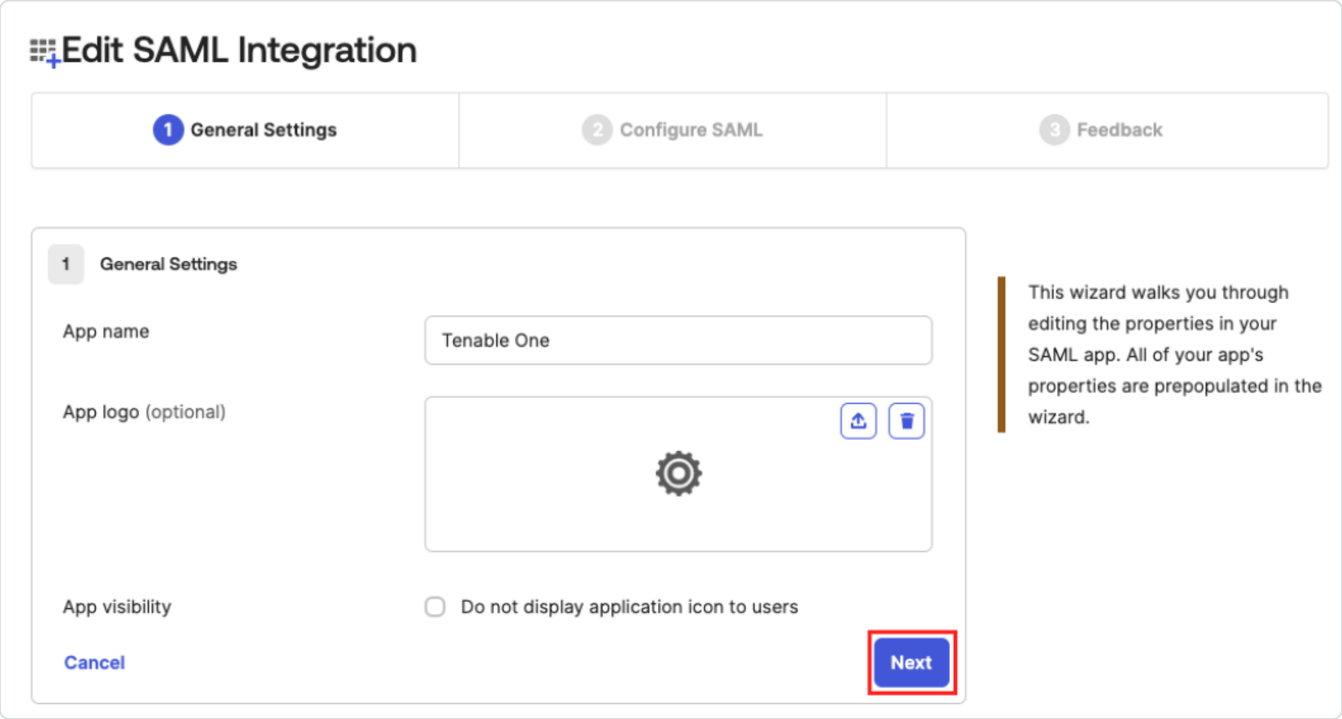
   General Settings

   All fields are required unless marked optional. Some fields may no longer be editable.

   SAML Settings

4. In the **SAML Settings** section, click **Edit**.

   The **General Settings** page appears.



Edit SAML Integration

1 General Settings

App name: Tenable One

App logo (optional)

App visibility: □ Do not display application icon to users

This wizard walks you through editing the properties in your SAML app. All of your app's properties are prepopulated in the wizard.

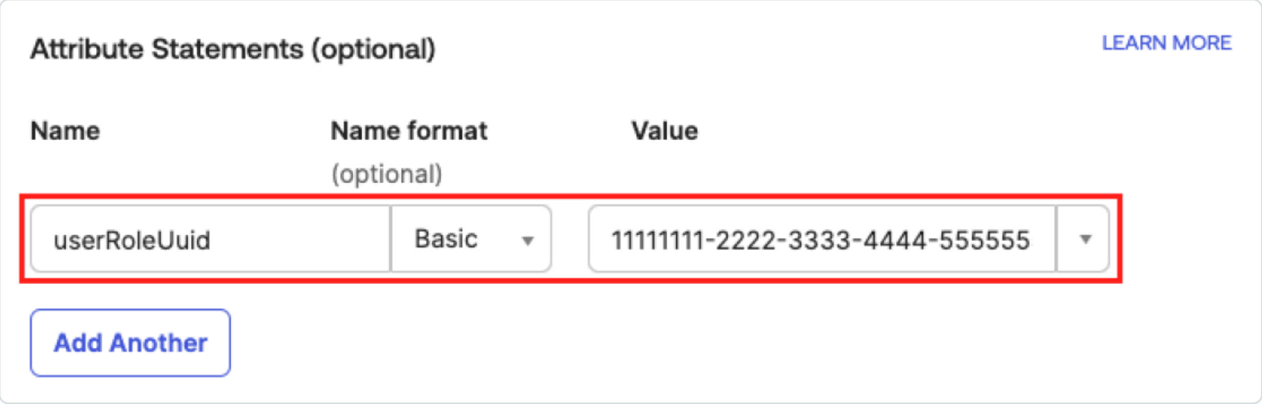
5. Click **Next**.

   The **Configure SAML** options appear.

6. Do one of the following:

   - To map all users assigned to the application to the same role:

     In the **Attribute Statements** section, insert the following values:



Attribute Statements (optional)

Name	Name format (optional)	Value
userRoleUuid	Basic	11111111-2222-3333-4444-555555

a. In the **Name** text box, type **userRoleUuid**.

b. In the **Name format** drop-down, select **Basic**.

c. In the **Value** text box, type the UUID of the Tenable user role.

> **Tip:** Tenable user role UUIDs can be found in Tenable Vulnerability Management, in the **Settings** > **Access Control** > **Roles** table.

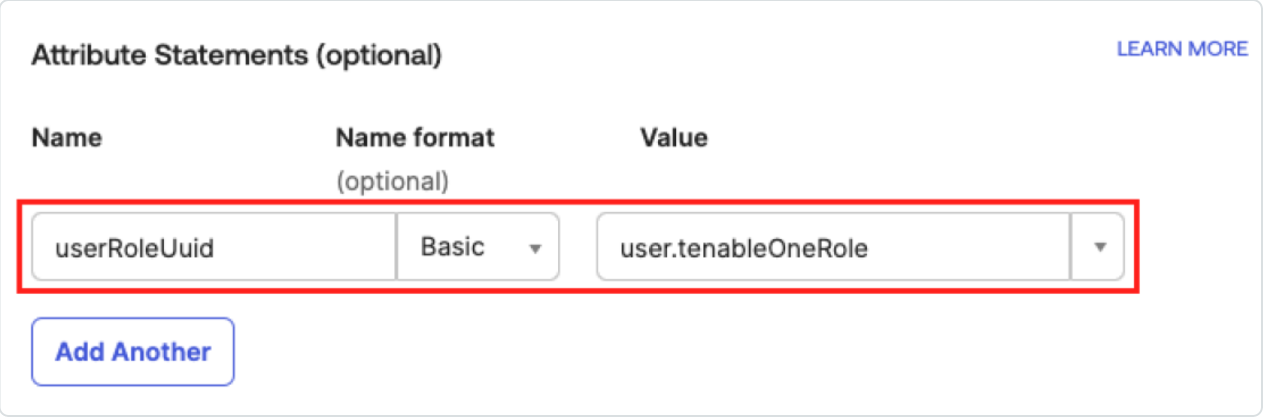
d. Click **Next**.

The **Feedback** options appear.

e. Click **Finish**.

- To map individual users assigned to the application to different roles:

In the **Attribute Statements** section, insert the following values:



Attribute Statements (optional)

Name	Name format (optional)	Value
userRoleUuid	Basic	user.tenableOneRole

a. In the **Name** text box, type **userRoleUuid**.

b. In the **Name format** drop-down, select **Basic**.

c. In the **Value** text box, type **user.tenableOneRole**.

d. Click **Next**.

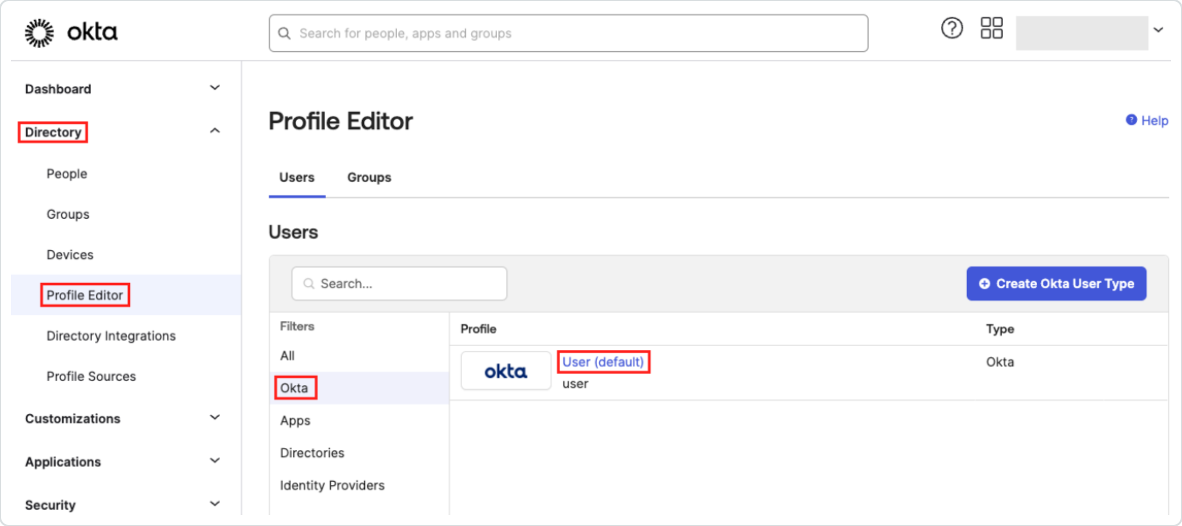
The **Feedback** options appear.

e. Click **Finish**.

f. In the left navigation menu, click **Directory** > **Profile Editor**.

The **Profile Editor** page appears.

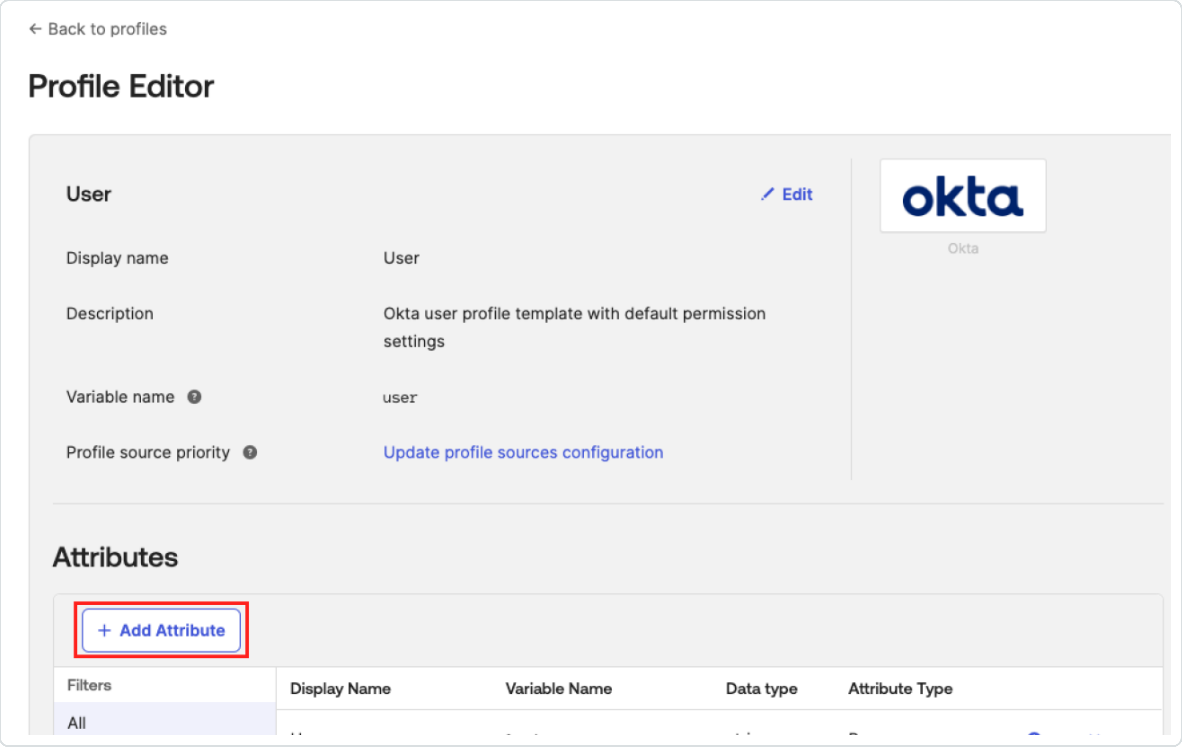
g. In the **Filters** section, click **Okta**.



h. Click the User (default) profile to edit it.

The **Profile Editor** appears.

i. In the **Attributes** section, click **Add Attribute**.



← Back to profiles

Profile Editor

User

Edit

Display name: User

Description: Okta user profile template with default permission settings

Variable name: user

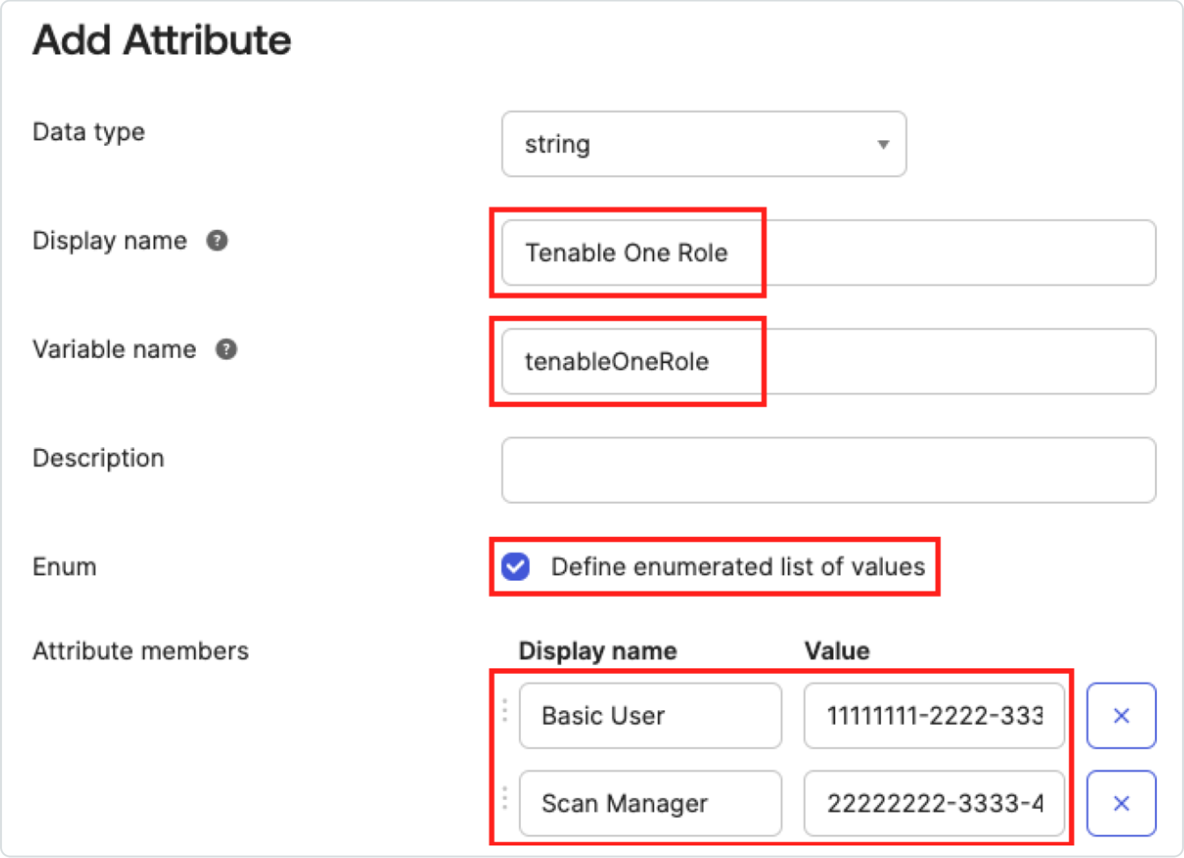
Profile source priority: Update profile sources configuration

Attributes

Display Name	Variable Name	Data type	Attribute Type

The **Add Attribute** page appears.

j. Modify the following fields:



Add Attribute

Data type: string

Display name: Tenable One Role

Variable name: tenableOneRole

Description:

Enum: ☑ Define enumerated list of values

Attribute members:

Display name	Value
Basic User	11111111-2222-333
Scan Manager	22222222-3333-4

i. In the **Display name** text box, type a descriptive name to display for the attribute in the Admin Console (for example, **Tenable One Role**).

ii. In the **Variable name** text box, type an attribute name for the attribute that can be referenced in mappings (for example, **tenableOneRole**).

> **Tip:** Variable names should only contain alphanumeric characters and underscores, and should not start with a digit. Once created, Okta prepends "*user.*" to the chosen variable name. If you configure a variable name other than **user.tenableOneRole**, refer back to step **c** in this section and ensure the variable name matches.
>
> For more information on custom user attributes, see Add custom attributes to an Okta user profile.

iii. Select the **Enum** check box.

iv. In the **Attribute Members** section:

A. In the **Display name** text box, type the user role you're interested in mapping (for example, **Basic User**).

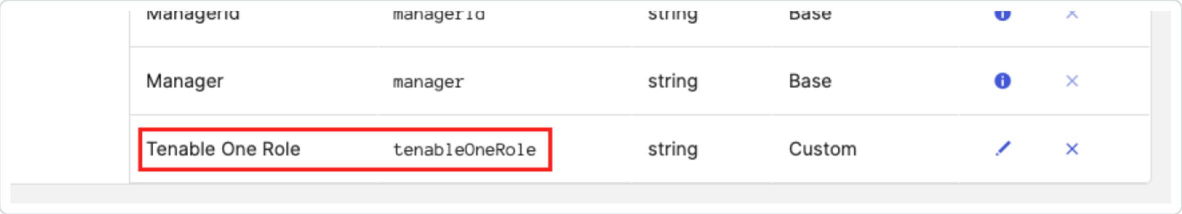
B. In the the **Value** text box, type the UUID of the corresponding Tenable user role.

> **Tip:** Tenable user role UUIDs can be found in Tenable Vulnerability Management, in the **Settings** > **Access Control** > Roles table.

C. To map more roles, select **Add Another** and repeat the process.

k. Click **Save**.

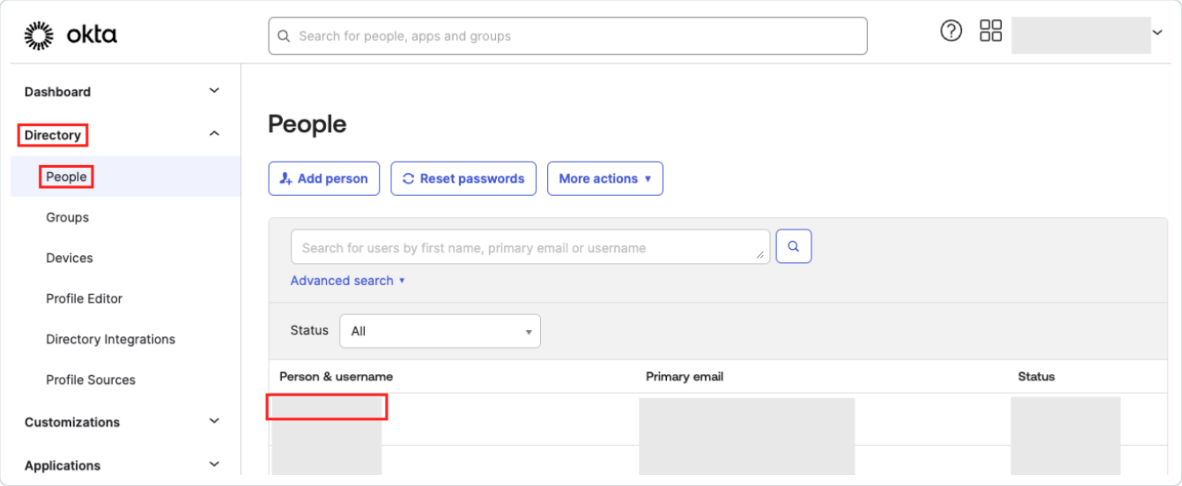
The default user **Profile Editor** page appears, and Okta adds the newly added custom attribute to the bottom of the list of attributes.



managerId	managerId	string	Base
Manager	manager	string	Base
Tenable One Role	tenableOneRole	string	Custom

l. In the left navigation menu, click **Directory** > **People**.

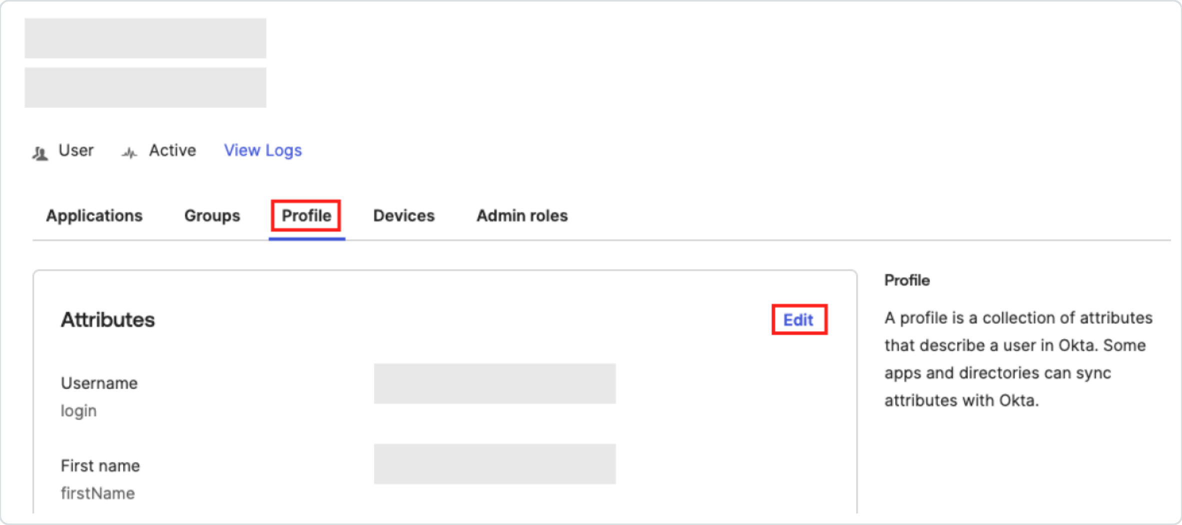
The **People** page appears.



m. Click the name of the user to which you want to map a Tenable One role.

   The user's **Application** page appears.

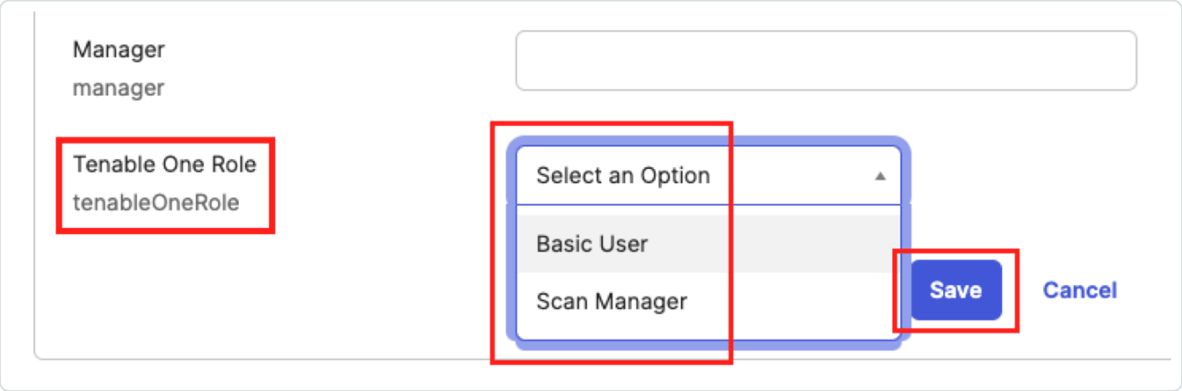
n. Click **Profile** > **Edit**.



A profile is a collection of attributes that describe a user in Okta. Some apps and directories can sync attributes with Okta.

o. Locate the newly added custom attribute.

p. In the **Select an Option** drop-down, select the appropriate Tenable role for the selected user (for example, **Basic User**).



q. Click **Save**.

Any time a user assigned to the application logs in via your SAML configuration, Tenable One automatically adds them to the user role mapped to the Okta application, or, depending on your configuration, mapped to their Okta user profile.

Additional Resources

For more information on Okta IdP configuration, see the following resources:

- Create SAML App Integrations
- Application Integration Wizard SAML field reference
- Define Group Attribute Statements
- Define Attribute Statements
- Add Custom Attributes to an Okta User Profile

Tenable One: Ping Identity IdP

One of the most common IdPs used to configure SAML with Tenable One is Ping Identity. The following steps guide you through the configuration process from start to finish.

Manual configuration requires the following:

- ACS URL: A custom URL provided by Tenable in the following format:

  ```
  https://cloud.tenable.com/saml/login/PLACEHOLDER
  ```

  Tip: FedRAMP environments use the following custom URL format: `https://fedcloud.tenable.com/saml/login/PLACEHOLDER`

- Entity ID: A custom ID provided by Tenable during SAML configuration in the following format:

  ```
  TENABLE_IO_PLACEHOLDER
  ```

- A certificate within the SAML metadata object that matches the data originally sent to Tenable.

  Note: Tenable does not support the use of multiple certificates and only extracts the first certificate from the metadata object. If the object includes multiple certificates, you must specify which certificate to use if it is not the first one listed.

- A user in Tenable One that also matches a user created within Ping Identity. For more information on creating users, see:

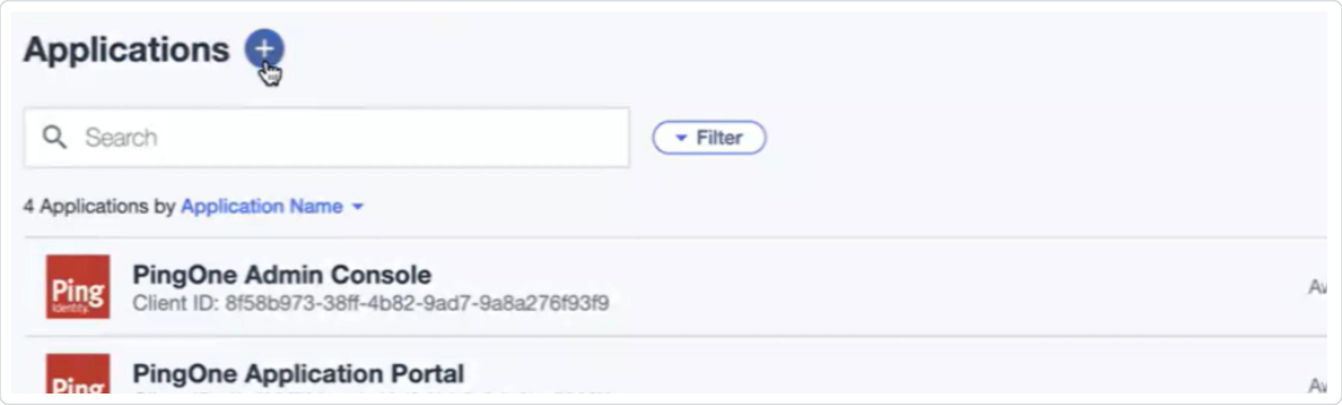
  - Create a User Account in the *Tenable Vulnerability Management User Guide*
  - Creating Users in the *Ping Identity User Guide*

Ping Identity: Create Temporary Application

To create a temporary application in Ping Identity:

1. In your browser, navigate to the Ping Identity admin portal.
2. In the left navigation menu, navigate to **Connections** > **Applications**.

   The **Applications** page appears.

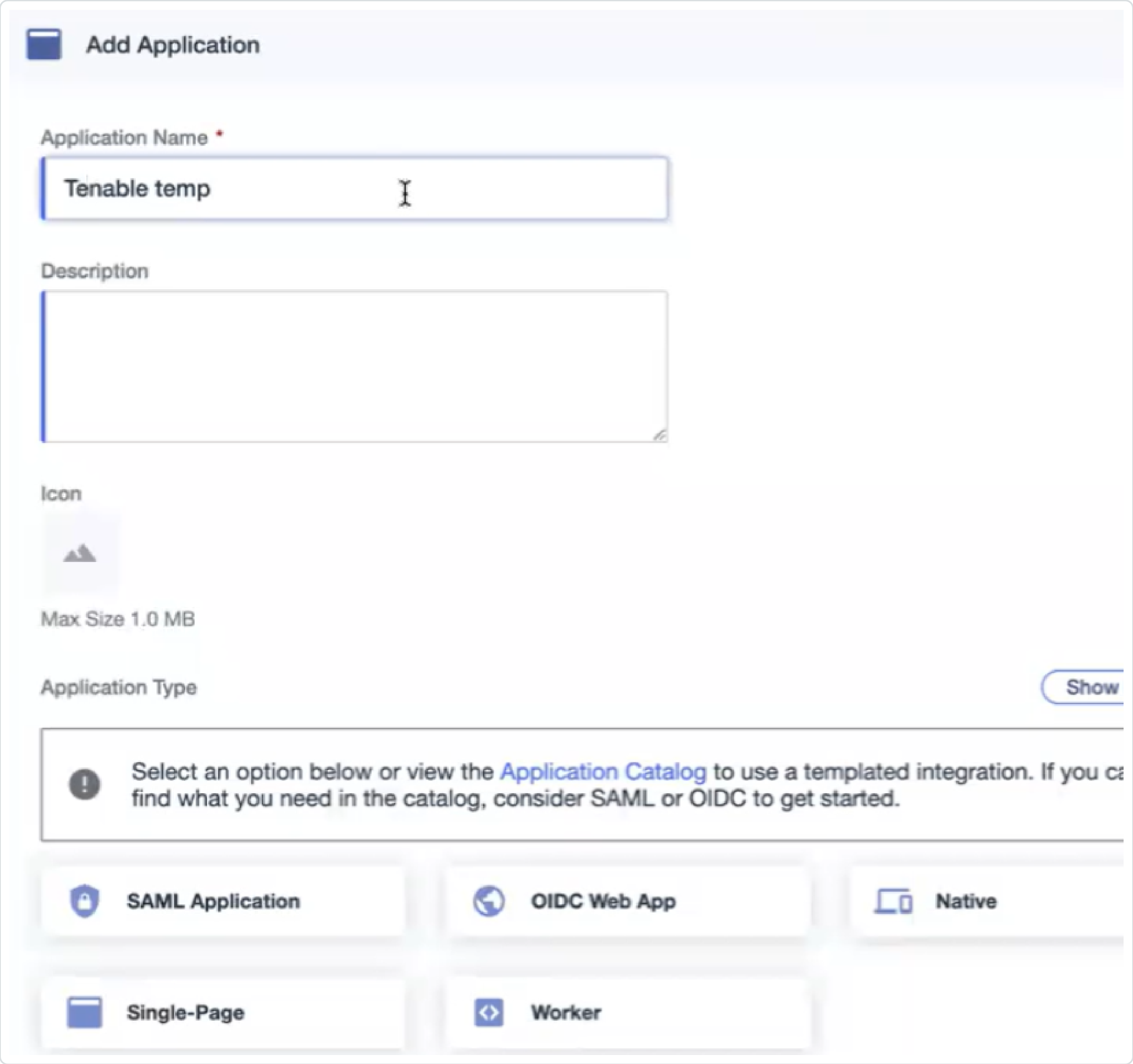
   4 Applications by Application Name

   PingOne Admin Console
   Client ID: 8f58b973-38ff-4b82-9ad7-9a8a276f93f9

   PingOne Application Portal

3. At the top of the page, click the ⊕ button.

   The **Add Application** page appears.



Add Application

Application Name *

Tenable temp

Description

Icon

Max Size 1.0 MB

Application Type

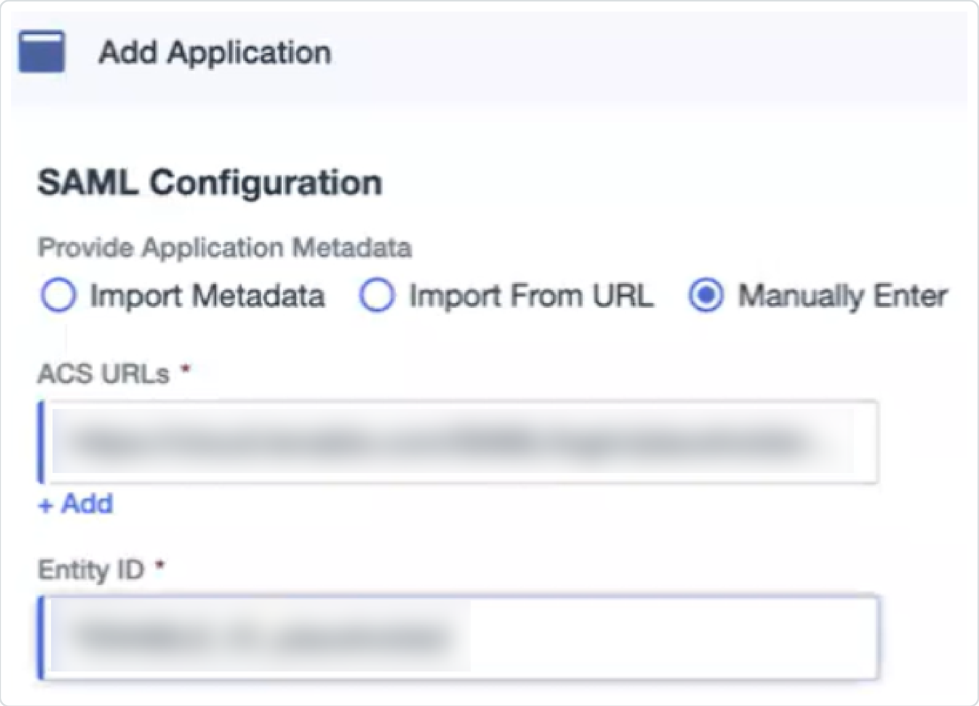
Select an option below or view the Application Catalog to use a templated integration. If you ca find what you need in the catalog, consider SAML or OIDC to get started.

4. In the **Application Name** box, type a name for your temporary application.

5. Click the **SAML Application** tile.

6. Click **Configure**.

   The **SAML Configuration** page appears.



Add Application

SAML Configuration

Provide Application Metadata

○ Import Metadata ○ Import From URL ● Manually Enter

ACS URLs *

+ Add

Entity ID *

7. In the **Provide Application Metadata** section, select the **Manually Enter** radio button.

8. In the **ACS URLs** text box, type the following placeholder text:

    ```
    https://cloud.tenable.com/saml/login/PLACEHOLDER
    ```

    > **Note:** You will later replace *PLACEHOLDER* with a unique UUID for the SAML configuration. This link is case-sensitive.

9. In the **Entity ID** text box, type the following placeholder text:

    ```
    TENABLE_IO_PLACEHOLDER
    ```

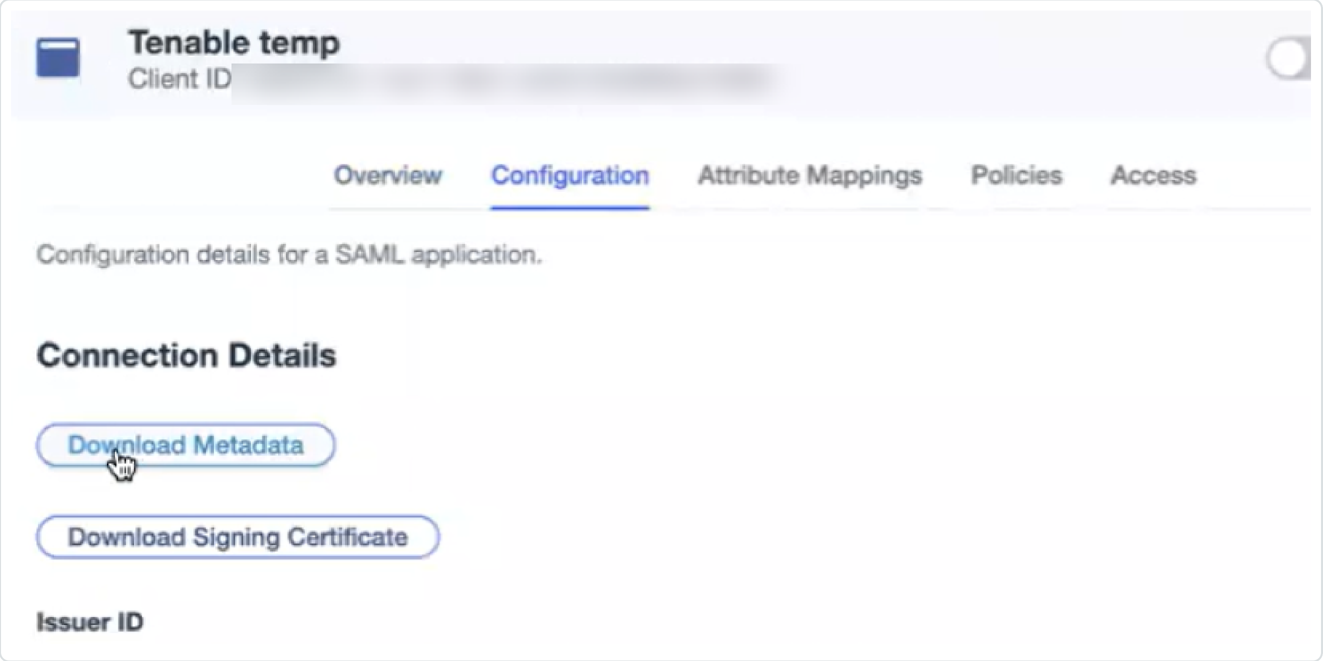
    > **Note:** You will later replace *PLACEHOLDER* with a unique UUID for the SAML configuration.

10. Click **Save**.

    A success message appears and Ping Identity directs you to an overview page for the application.

11. At the top of the page, click **Configuration**.

The **Connection Details** appear.



Tenable temp

Client ID [redacted]

Configuration details for a SAML application.

Connection Details

Issuer ID

12. Click **Download Metadata**.

    Your browser downloads the metadata.xml file.

Tenable One SAML Configuration

Once you have downloaded your medata.xml file, you can use it to configure SAML in Tenable One. You can configure this directly in the Tenable Vulnerability Management application.

To set up the Tenable One SAML configuration:

1. In your browser, navigate to Tenable One.
2. On the **Workspace** page, click Tenable Vulnerability Management.

   The Tenable Vulnerability Management user interface appears.
3. In the upper-left corner, click the ≡ button.

   The left navigation plane appears.
4. In the left navigation plane, click **Settings**.

The **Settings** page appears.

5. Click the **SAML** tile.

   The **SAML** page appears.

6. In the action bar, click ⊕ **Create**.

   The **SAML Settings** page appears.

7. Do one of the following:

   ### To provide configuration details by uploading the metadata.xml file from your IdP:

   a. In the first drop-down box, select **Import XML**.

   > **Note**: **Import XML** is selected by default.

   b. The **Type** drop-down box specifies the type of identity provider you are using. Tenable One supports SAML 2.0 (for example, Okta, OneLogin, etc.).
   This option is read-only.

   c. Under **Import**, click **Add File**.

   A file manager window appears.

   d. Select the metadata.xml file.

   The metadata.xml file is uploaded.

   ### To manually create your SAML configuration using data from the metadata.xml file from your IdP:

   a. In the first drop-down box, select **Manual Entry**.

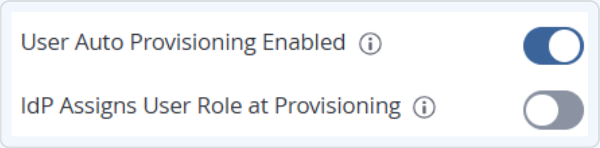
   A **SAML** configuration form appears.

   b. Configure the settings described in the following table:

Settings	Description
Enabled toggle	A toggle in the upper-right corner that indicates whether the

	SAML configuration is enabled or disabled. By default, the **Enable** setting is set to **Enabled**. Click the toggle to disable SAML configuration.
Type	Specifies the type of identity provider you are using. Tenable One supports SAML 2.0 (for example, Okta, OneLogin, etc.). This option is read-only.
Description	A description for the SAML configuration.
IdP Entity ID	The unique entity ID that your IdP provides. **Note**: If you want to configure multiple IdPs for a user account, create a new configuration for each identity provider with separate identity provider URLs, entity IDs, and signing certificates.
IdP URL	The SAML URL for your IdP.
Certificate	Your IdP security certificate or certificates. **Note**: Security certificates are found in a metadata.xml file that your identity provider provides. You can copy the content of the file and paste it in the **Certificate** box.
Authentication Request Signing Enabled	A toggle that indicates whether authentication request signing is enabled. When this toggle is enabled, if: • a user is logged in via SAML and their session expires • a user logs out and tries to log back in directly via the Tenable One interface rather than their IdP Tenable One automatically signs the SAML authentication request that is sent to the IdP to log the user back in.

	Note: The authentication request can only be validated if the IdP is also configured to accept this setting. For more information, see the following resources: - Manage Signing Certificates in Okta - Enforce Signed SAML Authentication Requests in Microsoft Entra ID - Edit a SAML Application in Ping Identity (**Enforce Signed AuthnRequest** option)
User Auto Provisioning Enabled	A toggle that indicates whether automatic user account creation is enabled or disabled. Automatic account provisioning allows users with an account for the IdP named in the SAML configuration to create a Tenable Vulnerability Management account the first time they log in via the IdP. **Note:** This option only appears during intial configuration if the setup is manual. Otherwise, you must edit the configuration after initial setup to enable this option.
IdP Assigns User Role at Provisioning	To assign a user role during provisioning, enable this toggle. In your SAML identity provider, add an attribute statement with **userRoleUuid** as the attribute name and the user role UUID as the attribute value. To obtain the UUID for a user role, go to **Settings** > **Access Control** > **Roles**. **Note:** This option only appears during intial configuration if the setup is manual. Otherwise, you must edit the configuration after initial setup to enable this option. **Note:** To access this option, you must first enable the **User Autoprovisioning Enabled** option.

	 User Auto Provisioning Enabled IdP Assigns User Role at Provisioning
IdP Resets User Role at Each Login	To assign a role each time a user logs in, overwriting the current role with the one chosen in your IdP, enable this toggle. In your SAML identity provider, add an attribute statement with **userRoleUuid** as the attribute name and the user role UUID as the attribute value. To obtain the UUID for a user role, go to **Settings** > **Access Control** > **Roles**. **Note:** This option only appears during intial configuration if the setup is manual. Otherwise, you must edit the configuration after initial setup to enable this option.
Group Management Enabled	Enable this toggle to allow the Tenable One SAML configuration to manage user groups. You must enable this toggle for the Managed by SAML option to function successfully.

8. Click **Save**.

   Tenable Vulnerability Management saves your SAML configuration and you return to the **SAML** page.

9. In the row for the SAML configuration you just created, click the ⋮ button.

   An actions menu appears.

10. Click **Download SAML SP metadata**.

    Your browser downloads the metadata.xml file. You can now use this file for final configuration in your IdP.

Optional: Configure One or More User Groups to Automatically Add a User upon SAML Login

User groups allow you to manage user permissions for various resources in Tenable One. When you assign users to a group, the users inherit the permissions assigned to the group. When you enable the **Managed by SAML** option for a user group, Tenable One allows you to automatically add any user that logs in via SAML to that group.

> **Important:** For this option to work successfully, you must also configure the related group claim within your IdP. View the final IdP configuration steps for more information.

Before you begin:

Ensure you've enabled the Group Management Enabled toggle when configuring the SAML settings within Tenable One.

To enable the Managed by SAML option:

1. In Tenable Vulnerability Management, in the upper-left corner, click the ☰ button.

   The left navigation plane appears.

2. In the left navigation plane, click **Settings**.

   The **Settings** page appears.

3. Click the **Access Control** tile.

   The **Access Control** page appears.

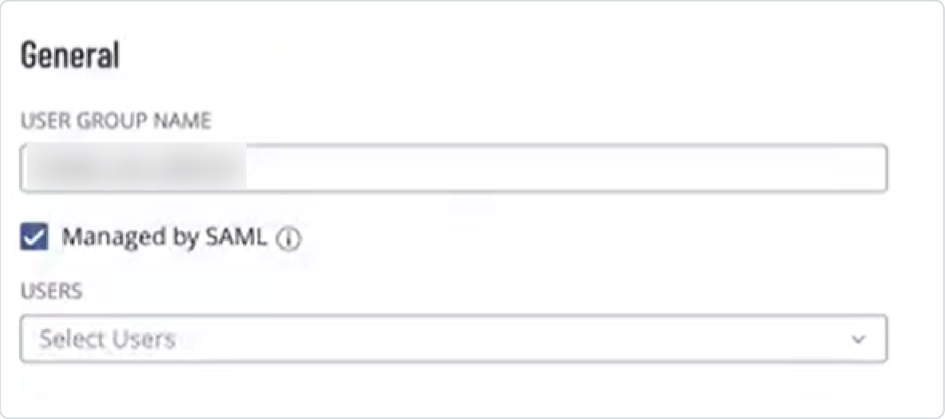
4. Click the **Groups** tab.

   The **Groups** page appears.

5. In the user groups table, click the user group to which you want to automatically add your SAML users.

   The **Edit User Group** page appears.

6. In the **General** section, select the **Managed by SAML** check-box.



General

USER GROUP NAME

[redacted]

☑ Managed by SAML ⓘ

USERS

Select Users

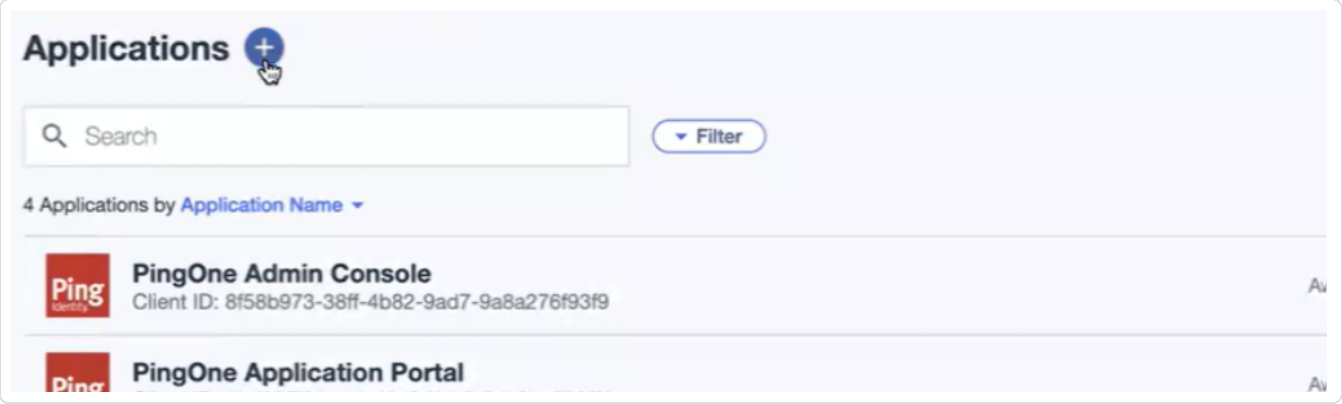
7. Click **Save**. Tenable Vulnerability Management saves your changes. Once you configure the related claim within your IdP, any time a user logs in via your SAML configuration, Tenable One automatically adds them to the specified user group.

Ping Identity: Create Permanent Application and Import Metadata

Now that you have downloaded the completed metadata file, you can use that file to create a permanent Tenable application in Ping Identity.

1. In your browser, navigate to the Ping Identity admin portal.
2. In the left navigation menu, navigate to **Connections** > **Applications**.

   The **Applications** page appears.



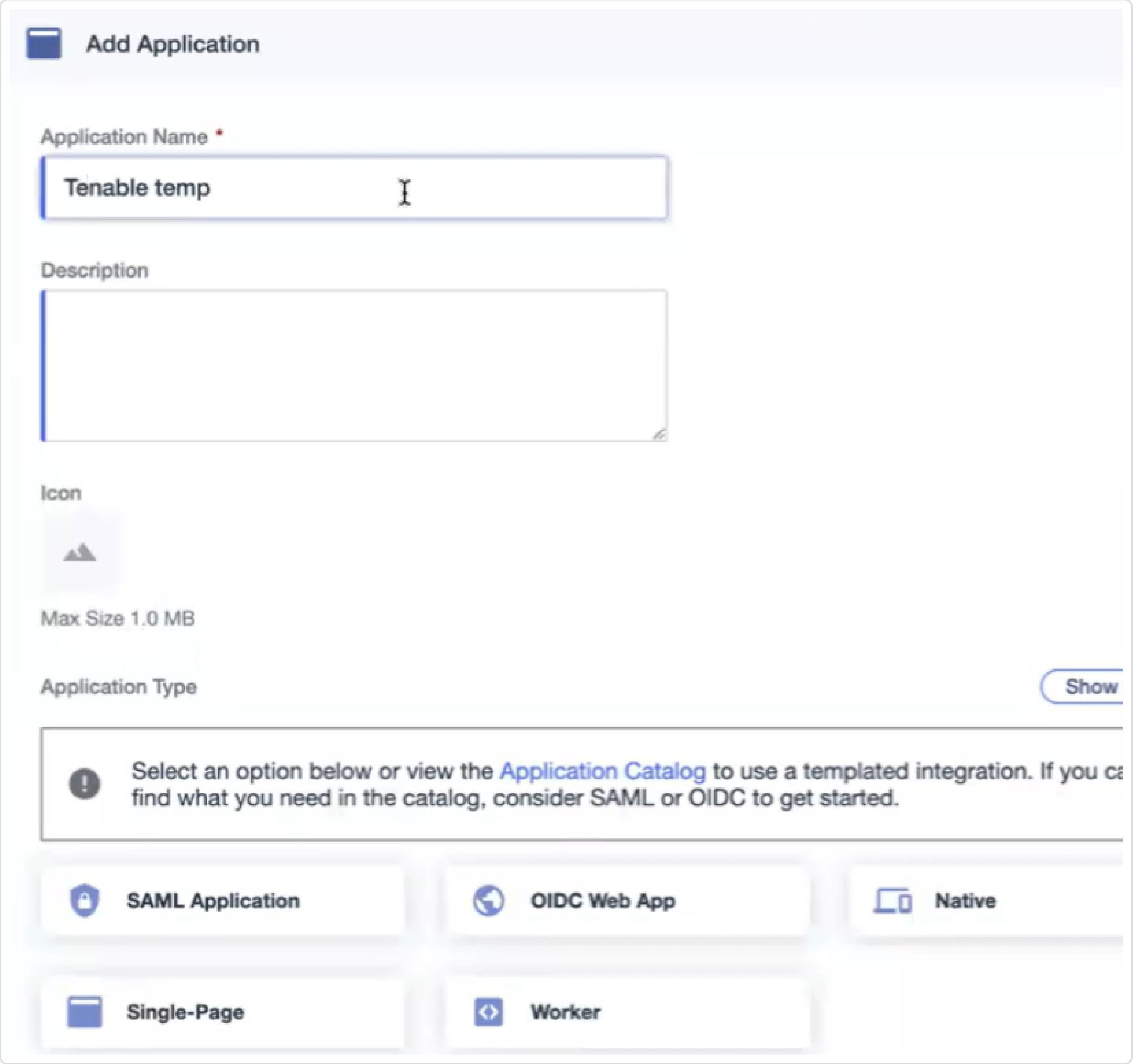
4 Applications by Application Name

PingOne Admin Console
Client ID: 8f58b973-38ff-4b82-9ad7-9a8a276f93f9

PingOne Application Portal

3. Delete the temporary application you previously created.
4. At the top of the page, click the ⊕ button.

The **Add Application** page appears.



Add Application

Application Name *

Tenable temp

Description

Icon

Max Size 1.0 MB

Application Type

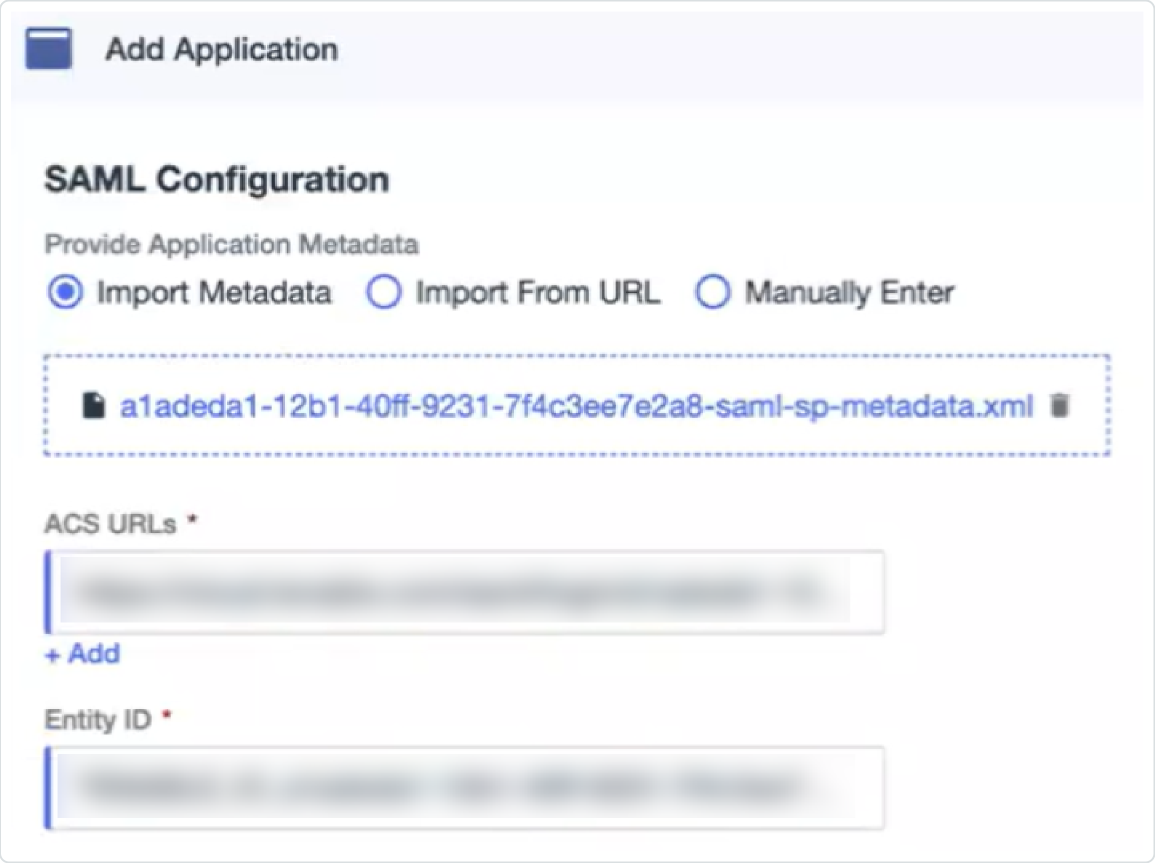
Select an option below or view the Application Catalog to use a templated integration. If you ca find what you need in the catalog, consider SAML or OIDC to get started.

5. In the **Application Name** box, type a name for your permanent application.

6. Click the **SAML Application** tile.

7. Click **Configure**.

   The **SAML Configuration** page appears.



Add Application

SAML Configuration

Provide Application Metadata

● Import Metadata ○ Import From URL ○ Manually Enter

a1adeda1-12b1-40ff-9231-7f4c3ee7e2a8-saml-sp-metadata.xml

ACS URLs *

+ Add

Entity ID *

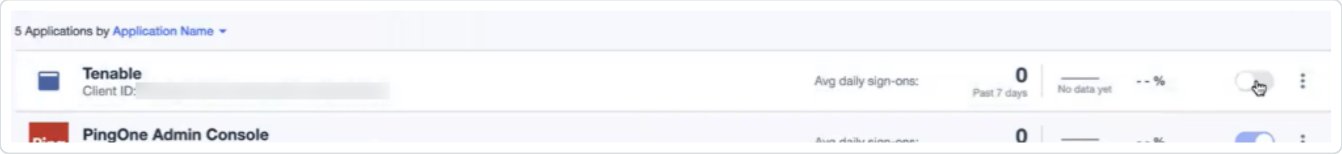
8. In the **Provide Application Metadata** section, select the **Import Metadata** radio button.

9. In your file manager, select the Service Provider metadata.xml file that you downloaded from Tenable Vulnerability Management.

   Ping Identity imports the metadata from the file, including the ACS URL and Entity ID specific to the SAML configuration.

10. Click **Save**.

11. On the **Applications** page, enable the toggle for the permanent Tenable application you created.



5 Applications by Application Name ▾

Tenable
Client ID:
Avg daily sign-ons: 0 Past 7 days
No data yet -- %

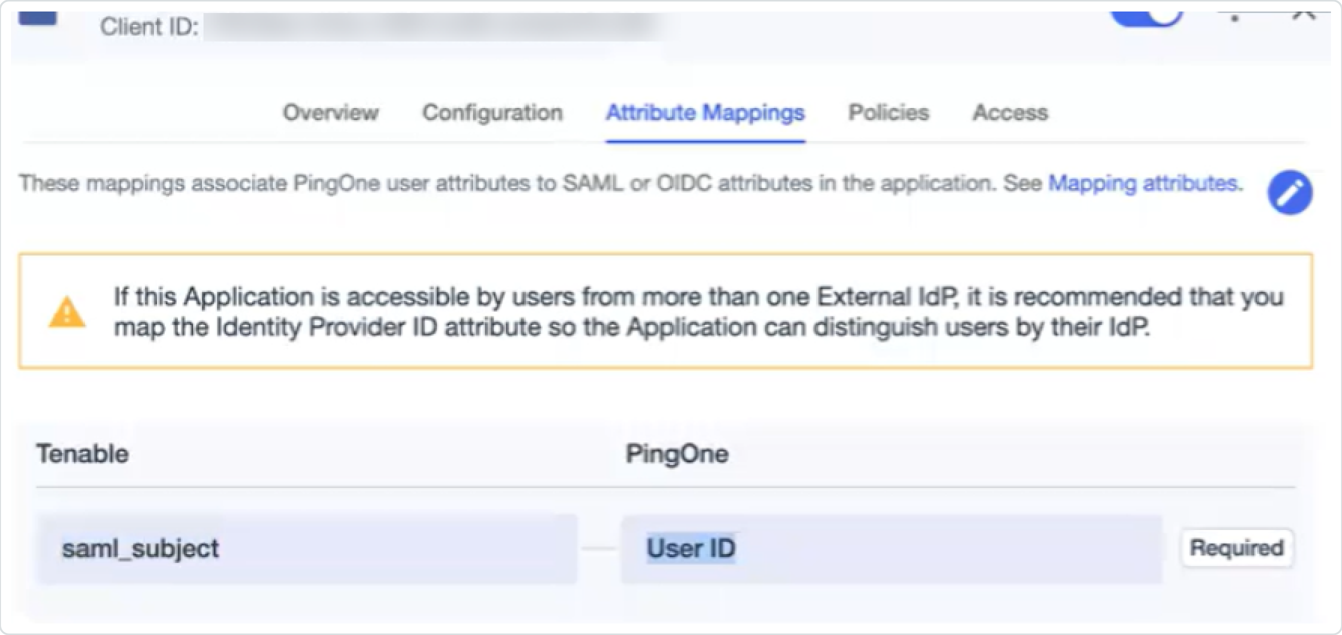
PingOne Admin Console
Avg daily sign-ons: 0 -- %

12. Click the name of the application you created.

The overview page for the application appears.

13. At the top of the page, click the **Attribute Mappings** tab.

    Attribute mapping options appear.

    Client ID: [redacted]

    These mappings associate PingOne user attributes to SAML or OIDC attributes in the application. See Mapping attributes.

    If this Application is accessible by users from more than one External IdP, it is recommended that you map the Identity Provider ID attribute so the Application can distinguish users by their IdP.

Tenable	PingOne	
saml_subject	User ID	Required

14. In the upper-right corner, click the ✎ button.

    The **PingOne Mappings** item becomes editable.

15. In the drop-down menu, select **Email Address**.

16. Click **Save**.

    Ping Identity saves your changes to the permanent application, and your SAML configuration is ready for use.

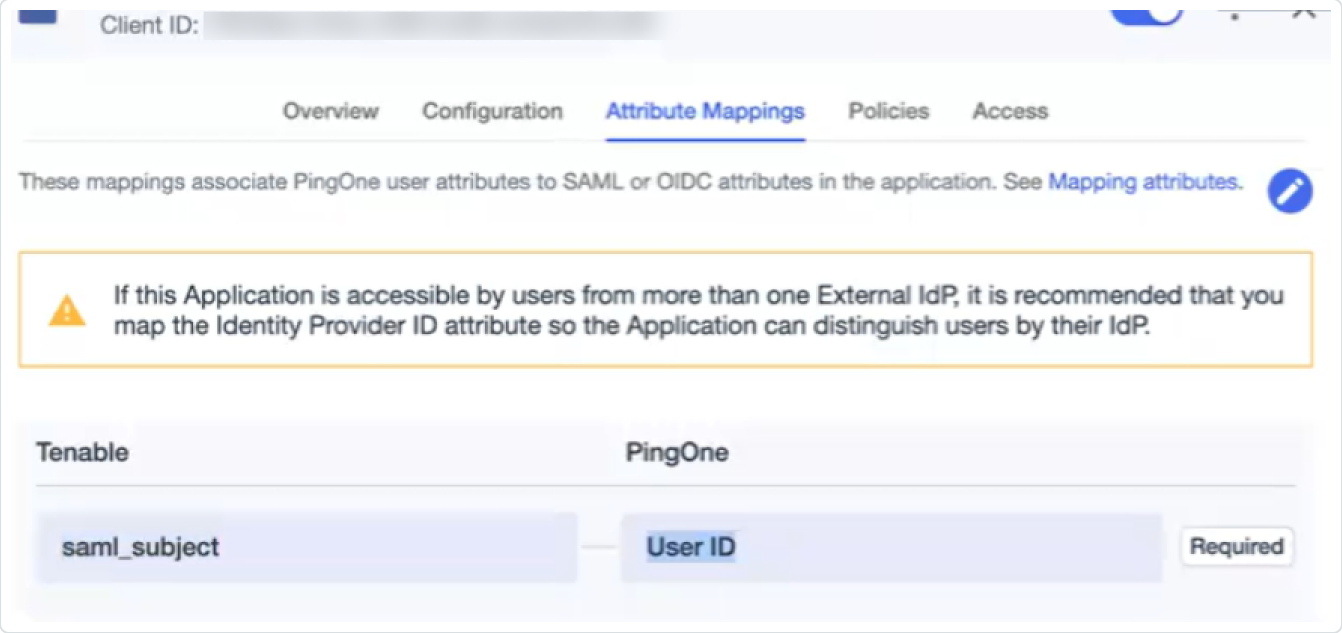
Optional: Finalize Configuration for Managed by SAML Group Option

If you configured the **Managed by SAML** option to automatically add any user that logs in via SAML to a user group, then you must configure a related group claim within the Microsoft Entra ID IdP.

To configure the IdP group claim:

1. In Ping Identity, on the overview page for your application, click the **Attribute Mappings** tab.

   Attribute mapping options appear.

   Client ID: [redacted]

   These mappings associate PingOne user attributes to SAML or OIDC attributes in the application. See Mapping attributes.

   If this Application is accessible by users from more than one External IdP, it is recommended that you map the Identity Provider ID attribute so the Application can distinguish users by their IdP.

Tenable	PingOne	
saml_subject	User ID	Required

2. In the upper-right corner, click the ✎ button.

3. Add a new attribute mapping:

   a. In the **Tenable** column, type **groups**.

   b. In the **PingOne** column, select **Group Names**.

4. Click **Save**. Any time a user logs in via your SAML configuration, Tenable One automatically adds them to the specified user group in Tenable One.

Additional Resources

For more information on Ping Identity IdP configuration, see the following resources:

- Ping Identity Developer Portal
- Creating a Manual SAML Connection
- Add a SAML Application in Ping Identity

Tenable One: Google Workspace IdP

One of the most common IdPs used to configure SAML with Tenable One is Google Workspace. The following steps guide you through the configuration process from start to finish, including optional configurations associated with user role and group mapping.

> **Tip:** Most service status changes in Google Workspace take effect within in a few minutes. Keep this in mind as you start using your SAML configurations. To learn more, see *How Changes Propagate to Google Services*.

Manual configuration requires the following:

- ACS URL: A custom URL provided by Tenable in the following format:

  ```
  https://cloud.tenable.com/saml/login/PLACEHOLDER
  ```

  > **Tip:** FedRAMP environments use the following custom URL format: `https://fedcloud.tenable.com/saml/login/PLACEHOLDER`

- Entity ID: A custom ID provided by Tenable during SAML configuration in the following format:

  ```
  TENABLE_IO_PLACEHOLDER
  ```

- A certificate within the SAML metadata object that matches the data originally sent to Tenable.

  > **Note:** Tenable does not support the use of multiple certificates and only extracts the first certificate from the metadata object. If the object includes multiple certificates, you must specify which certificate to use if it is not the first one listed.

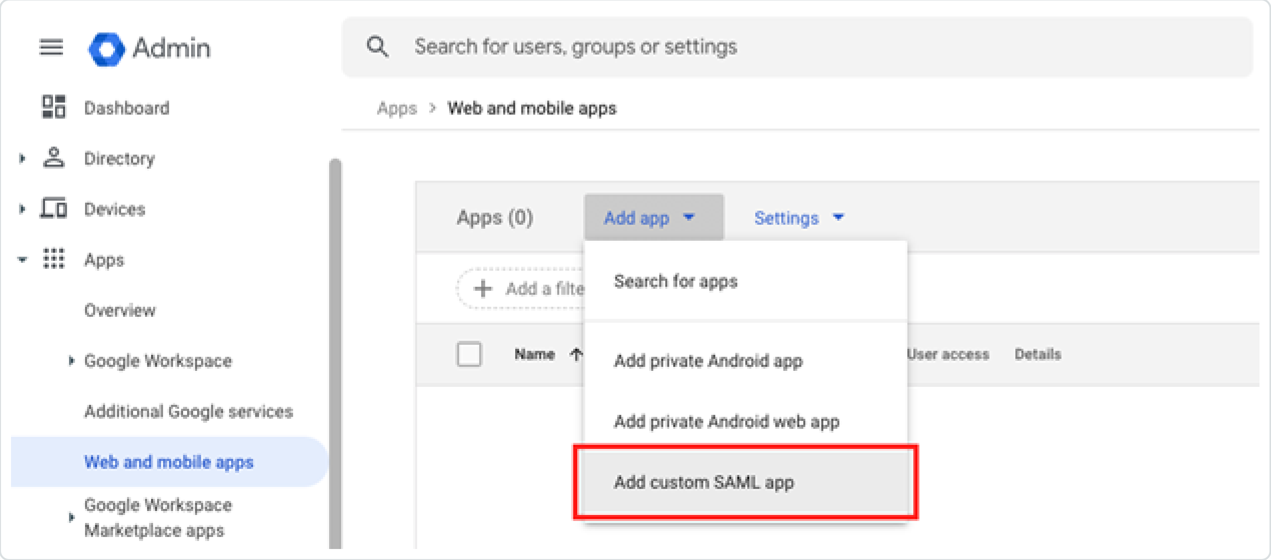
Google Workspace: Create Initial Application Integration

To create an application in Google Workspace:

1. In your browser, sign in to the Google Admin console.
2. In the navigation menu, navigate to **Apps** > **Web and mobile apps**.

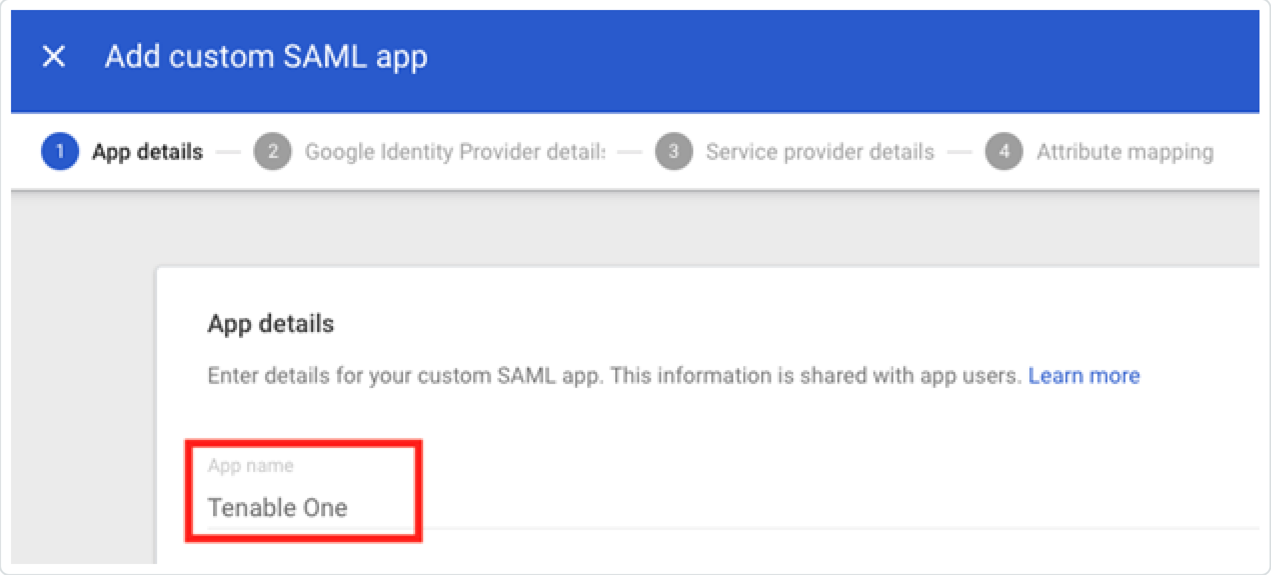
   The **Web and mobile apps** page appears.

3. Click **Add App** > **Add custom SAML app**.



The **App details** pane appears.

4. In the **App name** text box, type a name for your application (for example, Tenable One).



Enter details for your custom SAML app. This information is shared with app users. Learn more

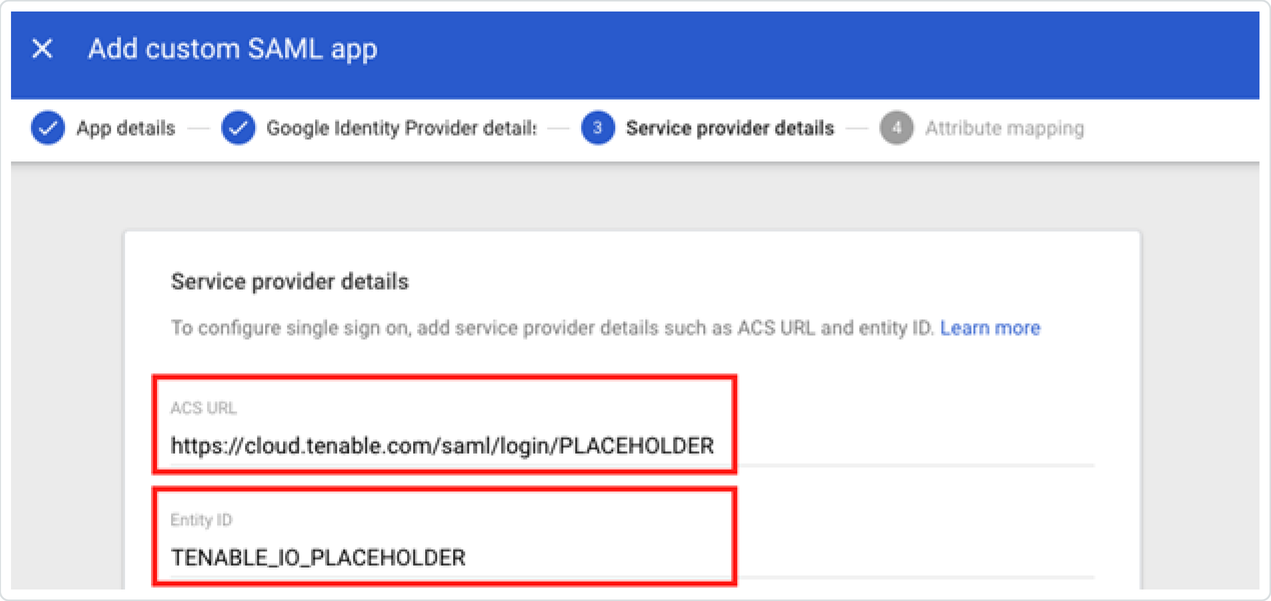
App name: Tenable One

5. Click **Continue.**

The **Google Identity Provider details** pane appears.

6. Skip **Option 1** and **Option 2** and click **Continue**.

The **Service provider details** pane appears.



Service provider details

To configure single sign on, add service provider details such as ACS URL and entity ID. Learn more

ACS URL

https://cloud.tenable.com/saml/login/PLACEHOLDER

Entity ID

TENABLE_IO_PLACEHOLDER

7. In the **ACS URL** text box, type the following placeholder URL:

   ```
   https://cloud.tenable.com/saml/login/PLACEHOLDER
   ```

   Note: You will later replace *PLACEHOLDER* with a unique UUID for the SAML configuration. This link is case-sensitive.

8. In the **Entity ID** text box, type the following placeholder text:

   ```
   TENABLE_IO_PLACEHOLDER
   ```

   Note: You will later replace *PLACEHOLDER* with a unique UUID for the SAML configuration.

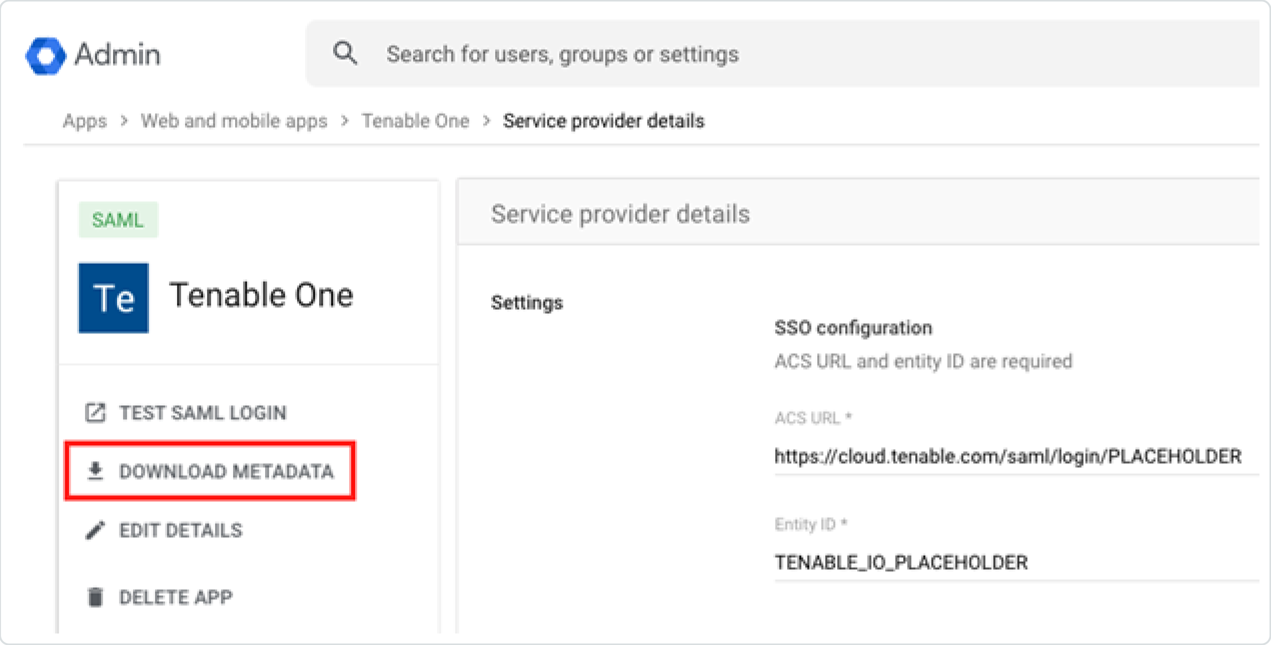
9. Click **Continue**.

   The **Attribute mapping** pane appears.

10. Click **Finish**.

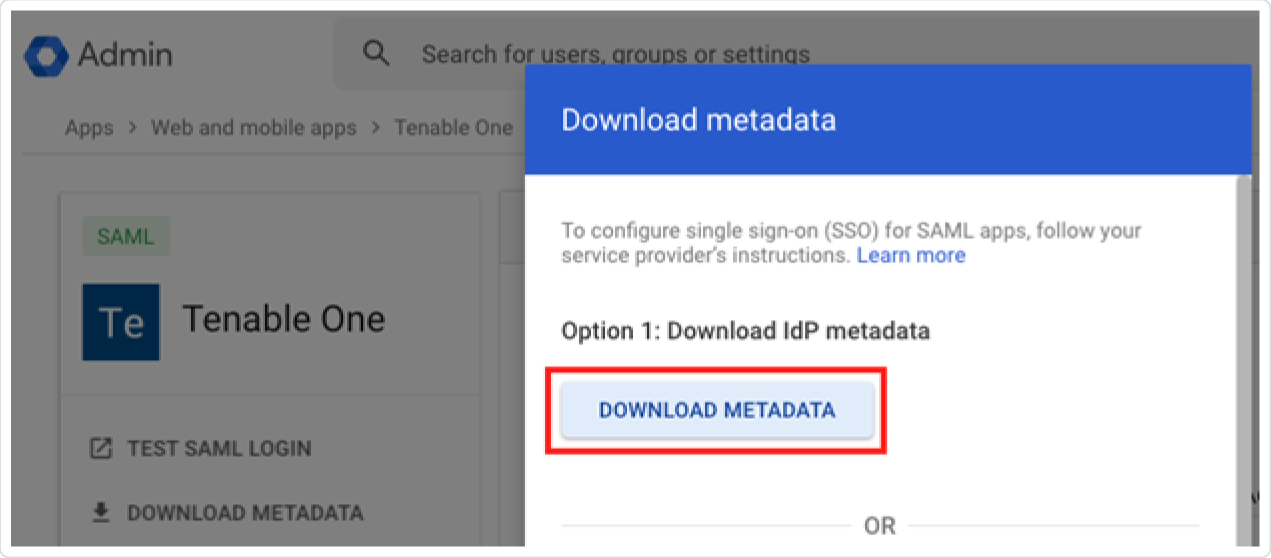
    The application details appear.

11. Click **Download Metadata**.


Admin
Search for users, groups or settings
Apps > Web and mobile apps > Tenable One > Service provider details
SAML
Te
Tenable One
TEST SAML LOGIN
DOWNLOAD METADATA
EDIT DETAILS
DELETE APP
Service provider details
Settings
SSO configuration
ACS URL and entity ID are required
ACS URL *
https://cloud.tenable.com/saml/login/PLACEHOLDER
Entity ID *
TENABLE_IO_PLACEHOLDER

The **Download metadata** page appears.

12. Under **Option 1: Download IdP metadata**, click **Download Metadata**.


Admin
Search for users, groups or settings
Apps > Web and mobile apps > Tenable One
SAML
Te
Tenable One
TEST SAML LOGIN
DOWNLOAD METADATA
Download metadata
Option 1: Download IdP metadata
DOWNLOAD METADATA
OR

To configure single sign-on (SSO) for SAML apps, follow your service provider's instructions. Learn more

Your browser downloads the metadata.xml file.

13. Click **Close**.

Tenable One SAML Configuration

Once you have downloaded your medata.xml file, you can use it to configure SAML in Tenable One. You can configure this directly in the Tenable Vulnerability Management application.

To set up the Tenable One SAML configuration:

1. In your browser, navigate to Tenable One.
2. On the **Workspace** page, click Tenable Vulnerability Management.

   The Tenable Vulnerability Management user interface appears.
3. In the upper-left corner, click the ≡ button.

   The left navigation plane appears.
4. In the left navigation plane, click **Settings**.

   The **Settings** page appears.
5. Click the **SAML** tile.

   The **SAML** page appears.
6. In the action bar, click ⊕ **Create**.

   The **SAML Settings** page appears.
7. Do one of the following:

   #### To provide configuration details by uploading the metadata.xml file from your IdP:

   a. In the first drop-down box, select **Import XML**.

   > **Note**: **Import XML** is selected by default.

   b. The **Type** drop-down box specifies the type of identity provider you are using. Tenable One supports SAML 2.0 (for example, Okta, OneLogin, etc.).
   This option is read-only.

   c. Under **Import**, click **Add File**.

   A file manager window appears.

d. Select the metadata.xml file.

   The metadata.xml file is uploaded.

To manually create your SAML configuration using data from the metadata.xml file from your IdP:

a. In the first drop-down box, select **Manual Entry**.

   A **SAML** configuration form appears.

b. Configure the settings described in the following table:

Settings	Description
Enabled toggle	A toggle in the upper-right corner that indicates whether the SAML configuration is enabled or disabled. By default, the **Enable** setting is set to **Enabled**. Click the toggle to disable SAML configuration.
Type	Specifies the type of identity provider you are using. Tenable One supports SAML 2.0 (for example, Okta, OneLogin, etc.). This option is read-only.
Description	A description for the SAML configuration.
IdP Entity ID	The unique entity ID that your IdP provides. **Note**: If you want to configure multiple IdPs for a user account, create a new configuration for each identity provider with separate identity provider URLs, entity IDs, and signing certificates.
IdP URL	The SAML URL for your IdP.
Certificate	Your IdP security certificate or certificates. **Note**: Security certificates are found in a metadata.xml file that your identity provider provides. You can copy the content of the file and paste it in the **Certificate** box.

User Auto Provisioning Enabled	A toggle that indicates whether automatic user account creation is enabled or disabled. Automatic account provisioning allows users with an account for the IdP named in the SAML configuration to create a Tenable Vulnerability Management account the first time they log in via the IdP. **Note:** This option only appears during intial configuration if the setup is manual. Otherwise, you must edit the configuration after initial setup to enable this option.
IdP Assigns User Role at Provisioning	To assign a user role during provisioning, enable this toggle. In your SAML identity provider, add an attribute statement with **userRoleUuid** as the attribute name and the user role UUID as the attribute value. To obtain the UUID for a user role, go to **Settings** > **Access Control** > **Roles**. **Note:** This option only appears during intial configuration if the setup is manual. Otherwise, you must edit the configuration after initial setup to enable this option.
IdP Resets User Role at Each Login	To assign a role each time a user logs in, overwriting the current role with the one chosen in your IdP, enable this toggle. In your SAML identity provider, add an attribute statement with **userRoleUuid** as the attribute name and the user role UUID as the attribute value. To obtain the UUID for a user role, go to **Settings** > **Access Control** > **Roles**. **Note:** This option only appears during intial configuration if the setup is manual. Otherwise, you must edit the configuration after initial setup to enable this option.

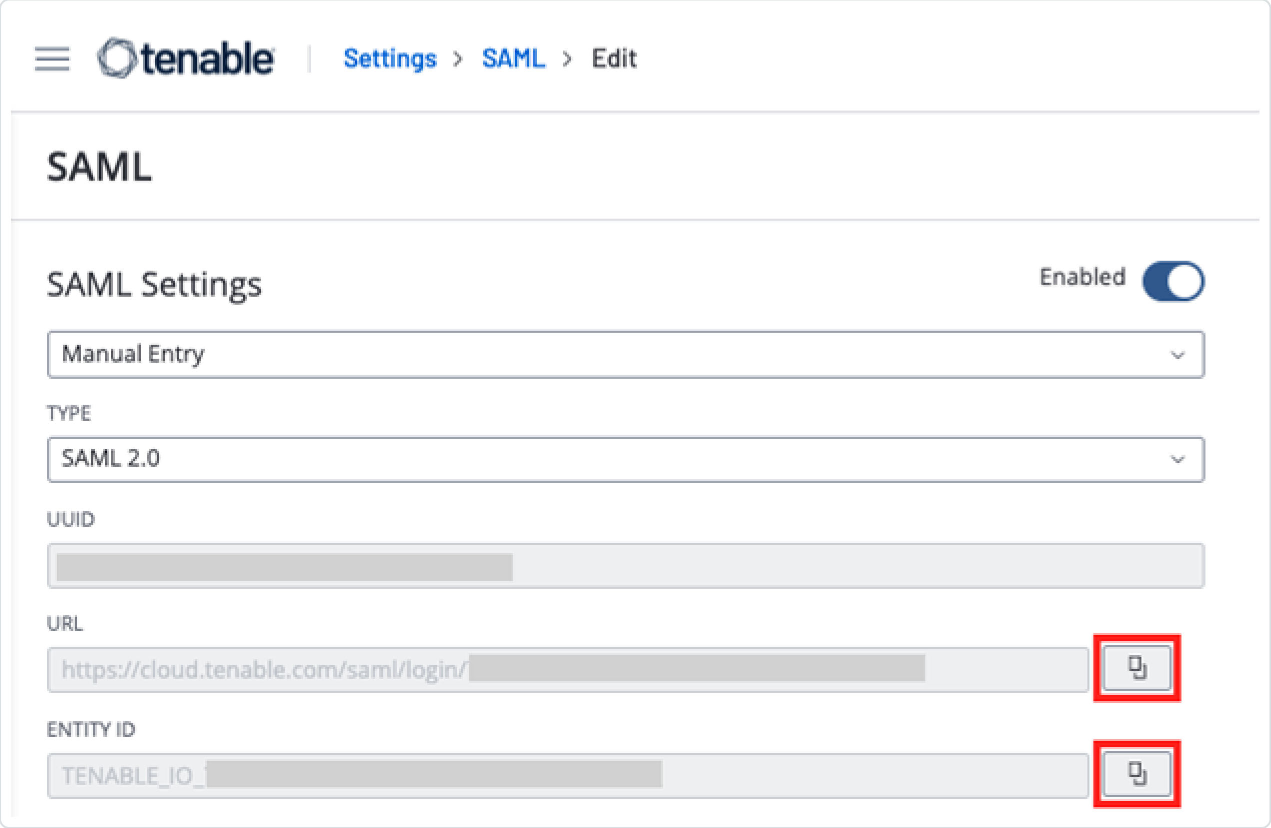
Group Management Enabled	Enable this toggle to allow the Tenable One SAML configuration to manage user groups. You must enable this toggle for the Managed by SAML option to function successfully.

8. Click **Save**.

   Tenable Vulnerability Management saves your SAML configuration and you return to the **SAML** page.

9. Click on the SAML configuration you just created.

   The **SAML Settings** page appears.

   Settings > SAML > Edit

   SAML

   SAML Settings

   Enabled

   Manual Entry

   TYPE

   SAML 2.0

   UUID

   [redacted]

   URL

   https://cloud.tenable.com/saml/login/[redacted]

   ENTITY ID

   TENABLE_IO_[redacted]

10. Copy both the **URL** and **Entity ID** values. You will need both of these values for the final configuration in your IdP.

Optional: Configure One or More User Groups to Automatically Add a User upon SAML Login

User groups allow you to manage user permissions for various resources in Tenable One. When you assign users to a group, the users inherit the permissions assigned to the group. When you enable the **Managed by SAML** option for a user group, Tenable One allows you to automatically add any user that logs in via SAML to that group.

> **Important:** For this option to work successfully, you must also configure the related group claim within your IdP. View the final IdP configuration steps for more information.

Before you begin:

Ensure you've enabled the Group Management Enabled toggle when configuring the SAML settings within Tenable One.

To enable the Managed by SAML option:

1. In Tenable Vulnerability Management, in the upper-left corner, click the ☰ button.

   The left navigation plane appears.

2. In the left navigation plane, click **Settings**.

   The **Settings** page appears.

3. Click the **Access Control** tile.

   The **Access Control** page appears.

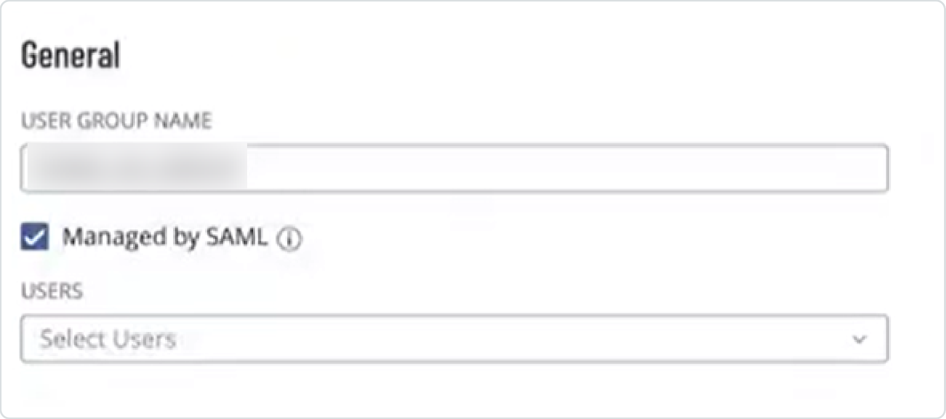
4. Click the **Groups** tab.

   The **Groups** page appears.

5. In the user groups table, click the user group to which you want to automatically add your SAML users.

   The **Edit User Group** page appears.

6. In the **General** section, select the **Managed by SAML** check-box.



General

USER GROUP NAME

[redacted]

☑ Managed by SAML ⓘ

USERS

Select Users

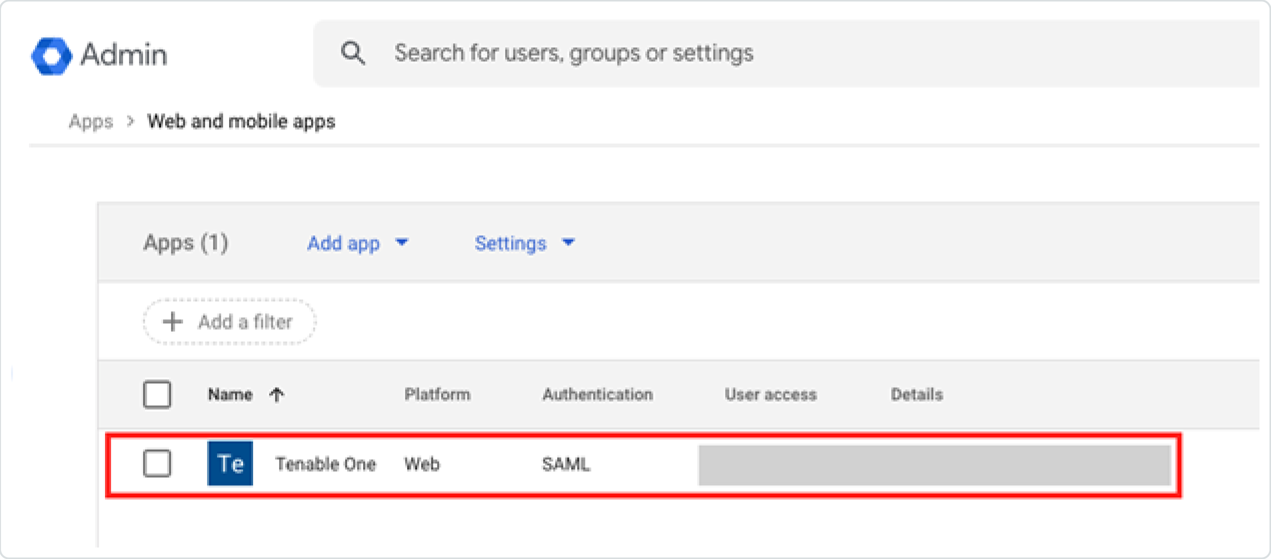
7. Click **Save**. Tenable Vulnerability Management saves your changes. Once you configure the related claim within your IdP, any time a user logs in via your SAML configuration, Tenable One automatically adds them to the specified user group.

Google Workspace: Configure Final Application Integration and Upload Metadata

Now that you have completed your Tenable One SAML configurations and copied the associated **URL** and **Entity ID** values, you can update your Tenable application in Google Workspace.

1. In your browser, navigate to the Google Admin console.
2. In the navigation menu, navigate to **Apps** > **Web and mobile apps**.

   The **Web and mobile apps** page appears.
3. Select the newly created application.

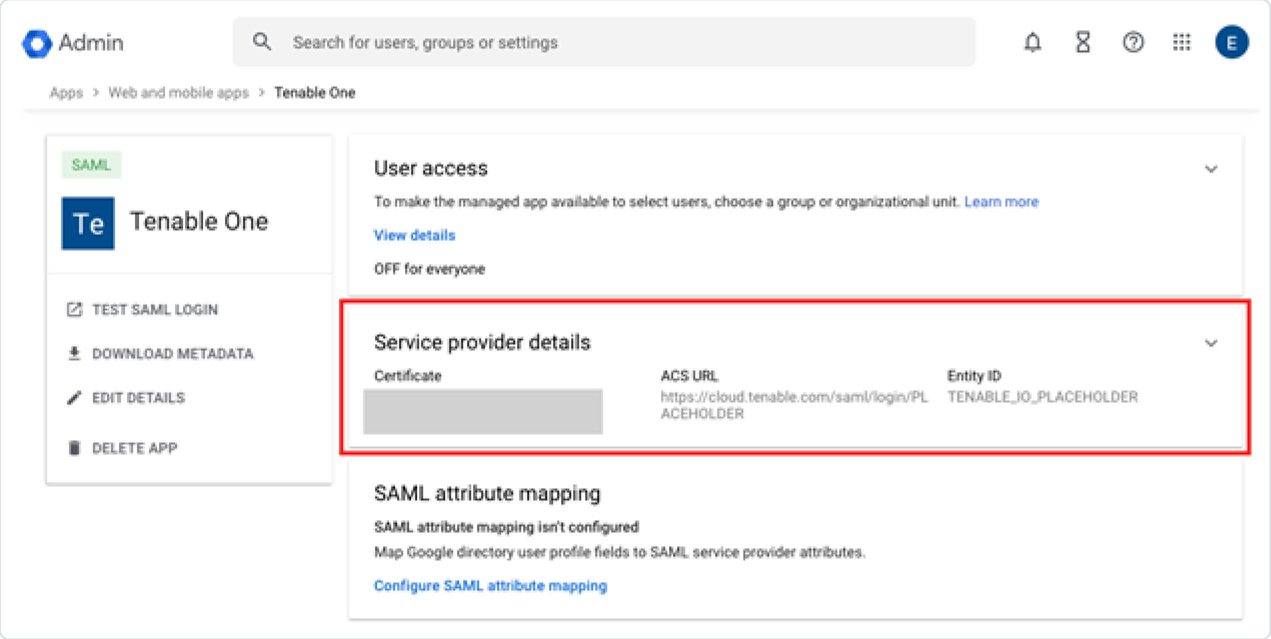


Admin
Search for users, groups or settings
Apps > Web and mobile apps
Apps (1)
Add app
Settings
Add a filter

	Name	Platform	Authentication	User access	Details
□	Te Tenable One	Web	SAML	[redacted]	

The application details appear.

4. Click on the **Service provider details** section.



User access

To make the managed app available to select users, choose a group or organizational unit. Learn more

View details

OFF for everyone

Service provider details

Certificate	ACS URL	Entity ID
[redacted]	https://cloud.tenable.com/saml/login/PLACEHOLDER	TENABLE_IO_PLACEHOLDER

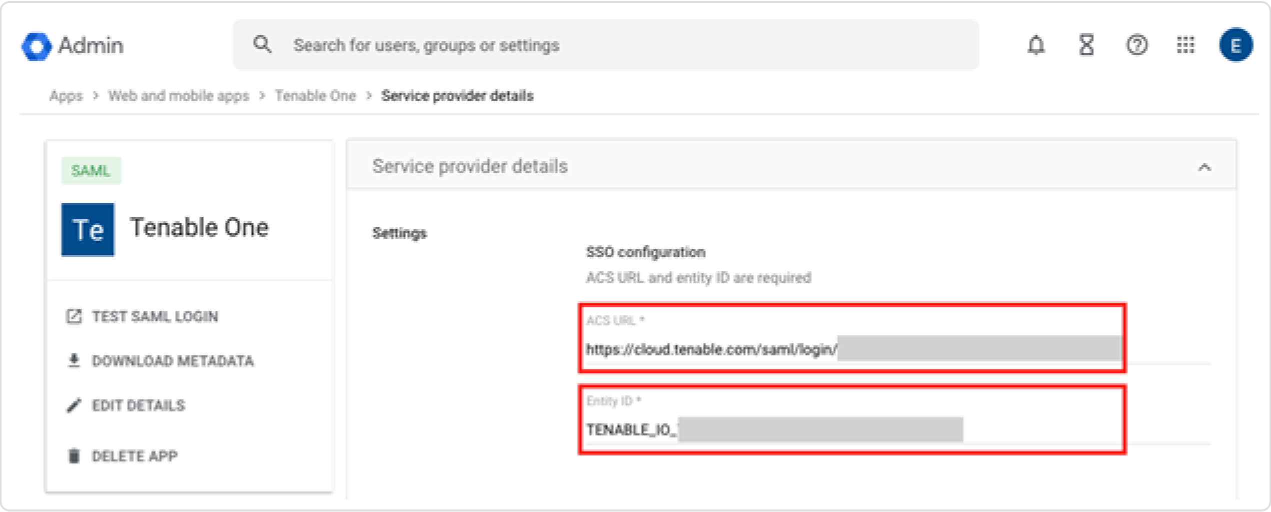
SAML attribute mapping

SAML attribute mapping isn't configured

Map Google directory user profile fields to SAML service provider attributes.

Configure SAML attribute mapping

The **Settings** page appears.


Admin
Search for users, groups or settings
E
Apps > Web and mobile apps > Tenable One > Service provider details
SAML
Te
Tenable One
TEST SAML LOGIN
DOWNLOAD METADATA
EDIT DETAILS
DELETE APP
Service provider details

Settings

SSO configuration

ACS URL and entity ID are required

ACS URL *

https://cloud.tenable.com/saml/login/[redacted]

Entity ID *

TENABLE_IO_[redacted]

5. In the **ACS URL** text box, replace the placeholder value with the previously saved URL value.

   > **Tip:** This URL is in the following format: https://cloud.tenable.com/saml/login/*PLACEHOLDER*.

6. In the **Entity ID** text box, replace the placeholder value with the previously saved Entity ID value.

   > **Tip:** This ID is in the following format: TENABLE_IO_*PLACEHOLDER*.

7. Click **Save**.

   Google Workspace saves your changes to the permanent application, and your SAML configuration is ready for use.

Optional: Finalize Configuration for Managed by SAML Group Option

If you configured the **Managed by SAML** option to automatically add any user that logs in via SAML to a user group, then you must configure a related group claim within Google Workspace.

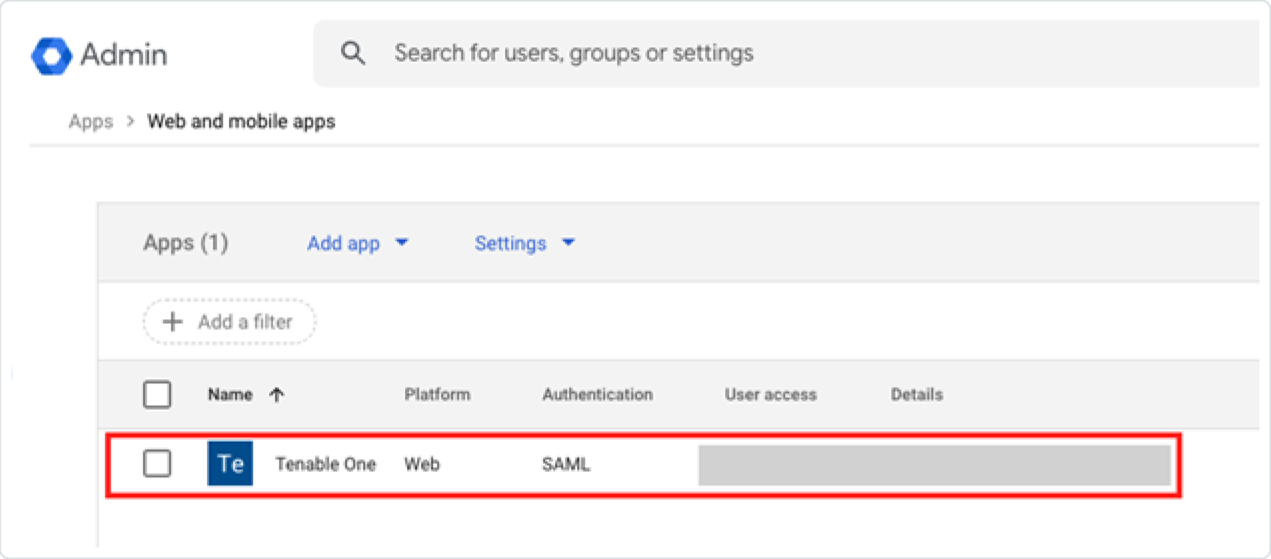
To configure the IdP group claim:

1. In your browser, navigate to the Google Admin console.

2. In the navigation menu, navigate to **Apps** > **Web and mobile apps**.

   The **Web and mobile apps** page appears.

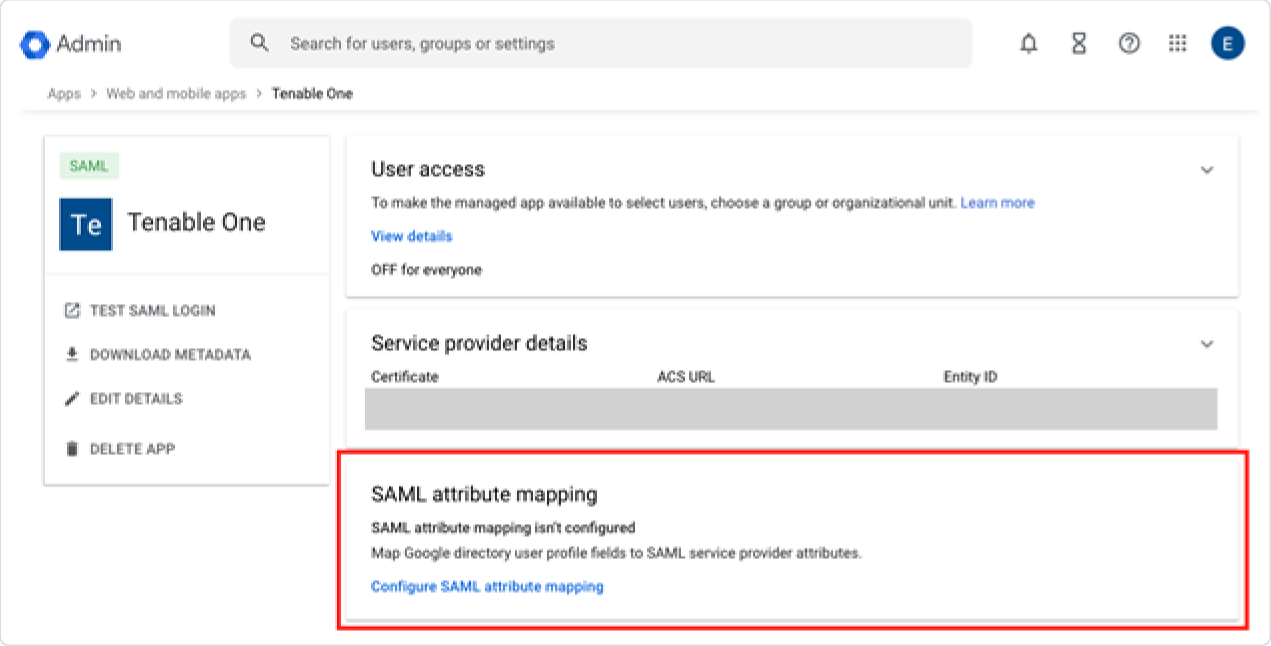
3. Select the newly created application.


Admin
Search for users, groups or settings
Apps > Web and mobile apps
Apps (1)
Add app
Settings
Add a filter

☐	Name	Platform	Authentication	User access	Details
☐	Te Tenable One	Web	SAML	[redacted]	

The application details appear.

4. Click **SAML attribute mapping**.



User access

To make the managed app available to select users, choose a group or organizational unit. Learn more

View details

OFF for everyone

Service provider details

Certificate	ACS URL	Entity ID
[redacted]		

SAML attribute mapping

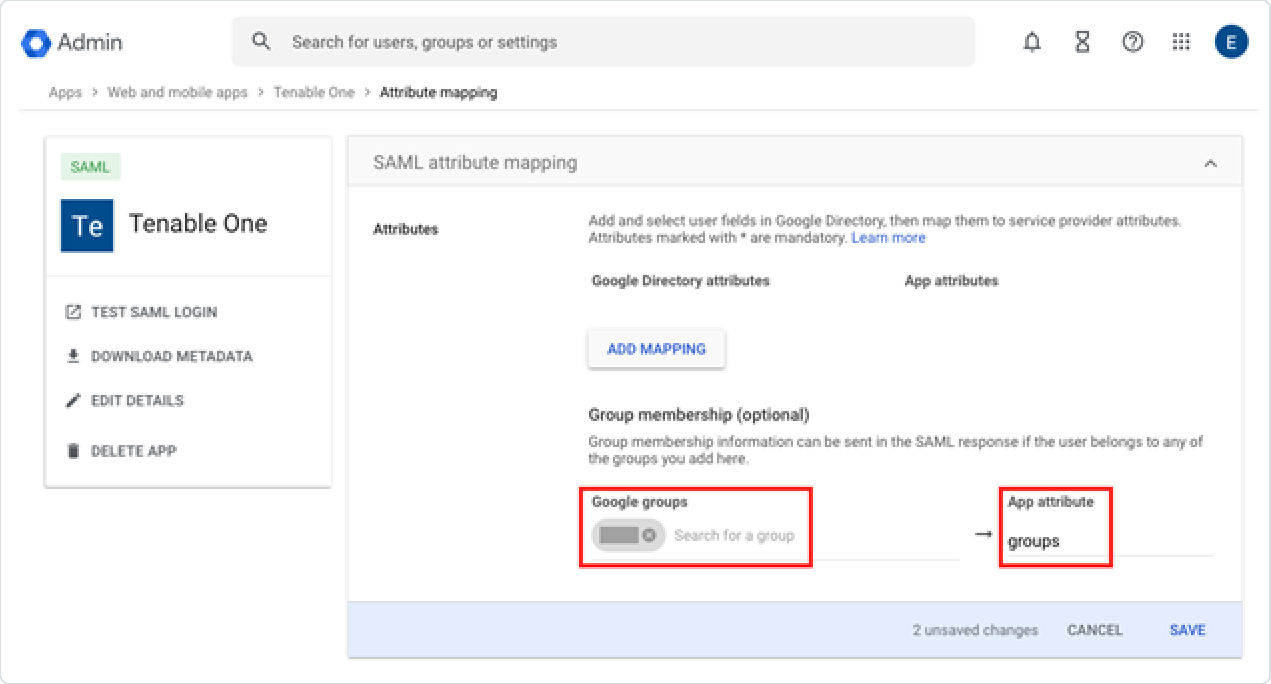
SAML attribute mapping isn't configured

Map Google directory user profile fields to SAML service provider attributes.

Configure SAML attribute mapping

The **Attributes** page appears.

5. In the **Group membership** section:



Add and select user fields in Google Directory, then map them to service provider attributes. Attributes marked with * are mandatory. Learn more

Group membership (optional)

Group membership information can be sent in the SAML response if the user belongs to any of the groups you add here.

App attribute: groups

   a. In the **Google groups** search box, search for (and select) the appropriate Google Workspace group.

   b. In the **App attribute** text box, type **groups**.

6. Click **Save**. Any time a user logs in via your SAML configuration, Tenable One automatically adds them to the specified user group in Tenable One.

Optional: Configure Managed by SAML Role Option

Roles allow you to manage privileges for major functions in Tenable One and control which Tenable One resources users can access. If you toggled on the SAML configuration options IdP Assigns User Role at Provisioning and/or IdP Resets User Role at Each Login (to automatically add and/or assign any user that logs in via SAML to a user role), then you must complete the following three steps in Google Workspace:

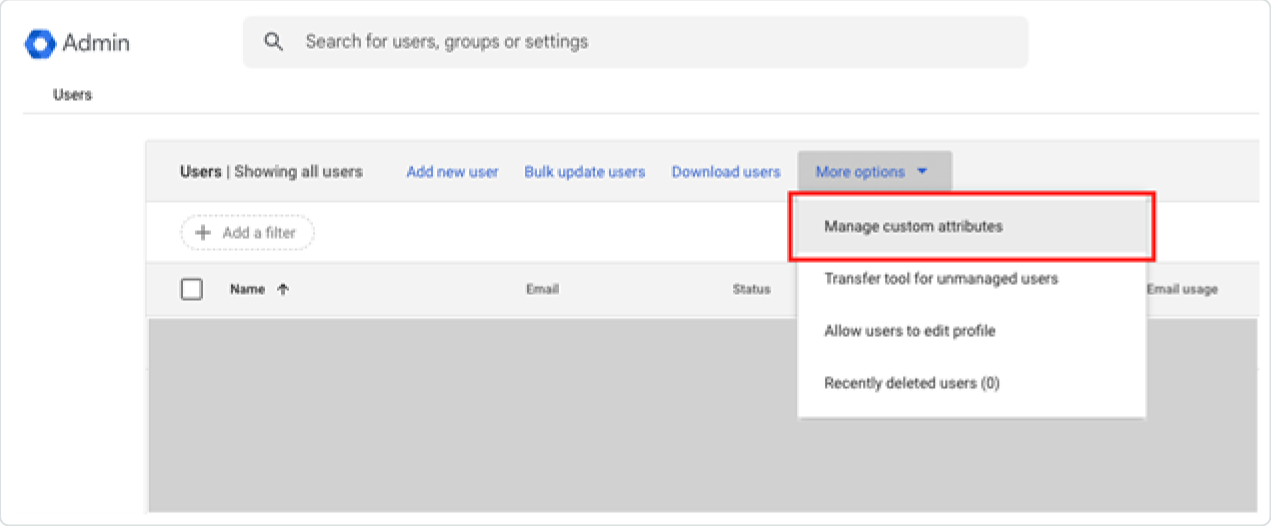
Add a Custom Attribute for Roles

To add a custom attribute for roles:

1. In the navigation menu, navigate to **Directory** > **Users**.

   The **Users** page appears.

2. Click **More options** > **Manage custom attributes**.

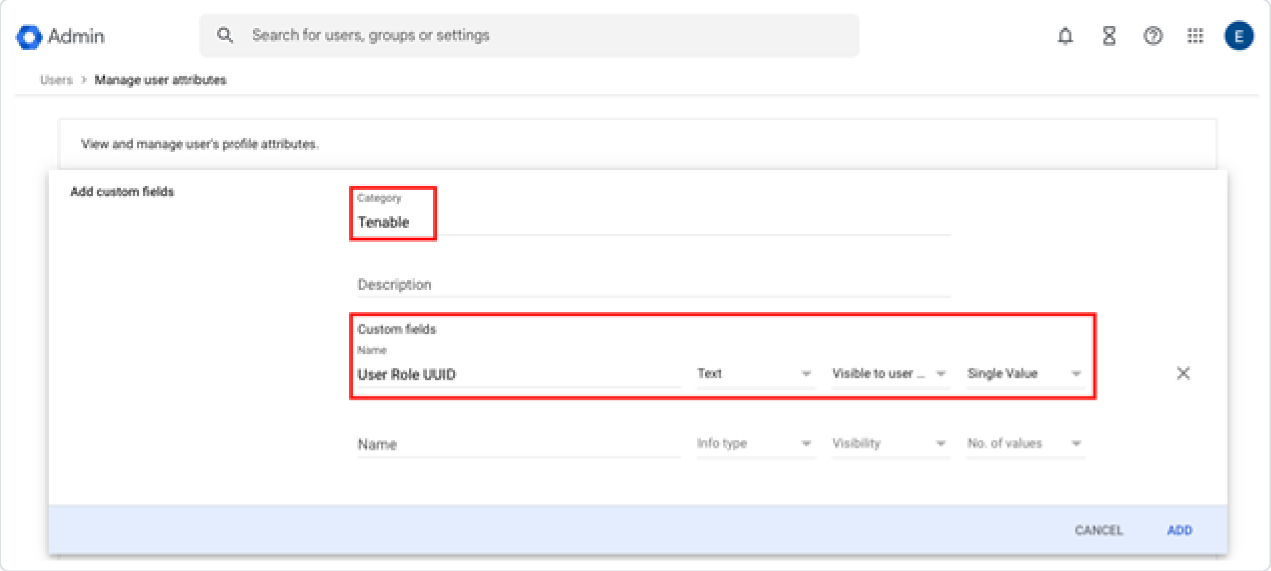

Admin
Search for users, groups or settings
Users
Users | Showing all users
Add new user
Bulk update users
Download users
More options
Add a filter
Name
Email
Status
Email usage
Manage custom attributes
Transfer tool for unmanaged users
Allow users to edit profile
Recently deleted users (0)

   The **Manage user attributes** page appears.

3. Click **Add Custom Attribute**.

   The **Add custom fields** page appears.

4. In the **Category** text box, type a category name (e.g. Tenable).


Admin
Search for users, groups or settings
Users > Manage user attributes
View and manage user's profile attributes.
Add custom fields
Description
Name
Info type
Visibility
No. of values
CANCEL
ADD

Category: Tenable

Custom fields

Name: User Role UUID | Text | Visible to user ... | Single Value

5. In the **Custom fields** section:

    a. In the **Name** text box, type a name for this attribute (e.g. User Role UUID).

    b. In the **Info type** drop-down, select **Text**.

    c. In the **Visibility** drop-down, select your preferred visibility.

    d. In the **No. of values** drop-down, select **Single Value**.

6. Click **Add**.

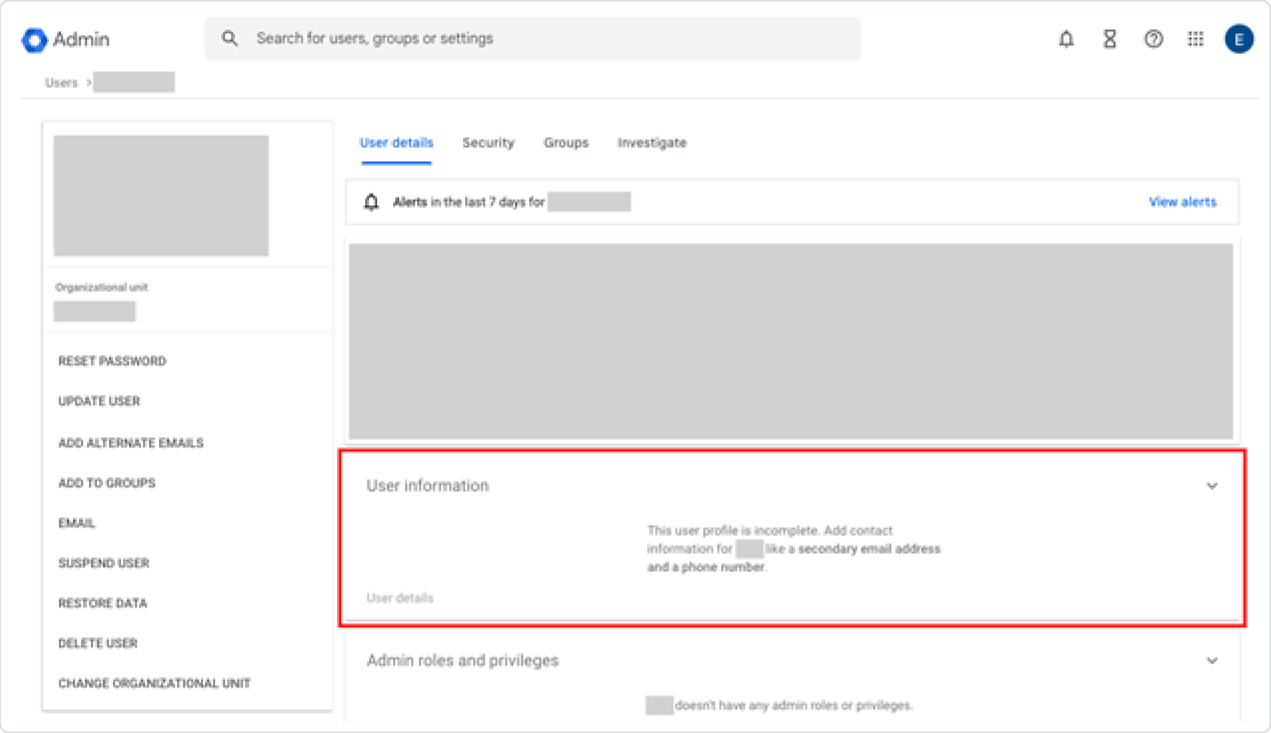
Configure the Attribute for a User

To configure the attribute for a user (with a user role UUID):

1. On the **Users** page, click the name of the user for which you want to configure the attribute.

    The user configuration page appears.

2. In the **User Details** section, click **User information**.



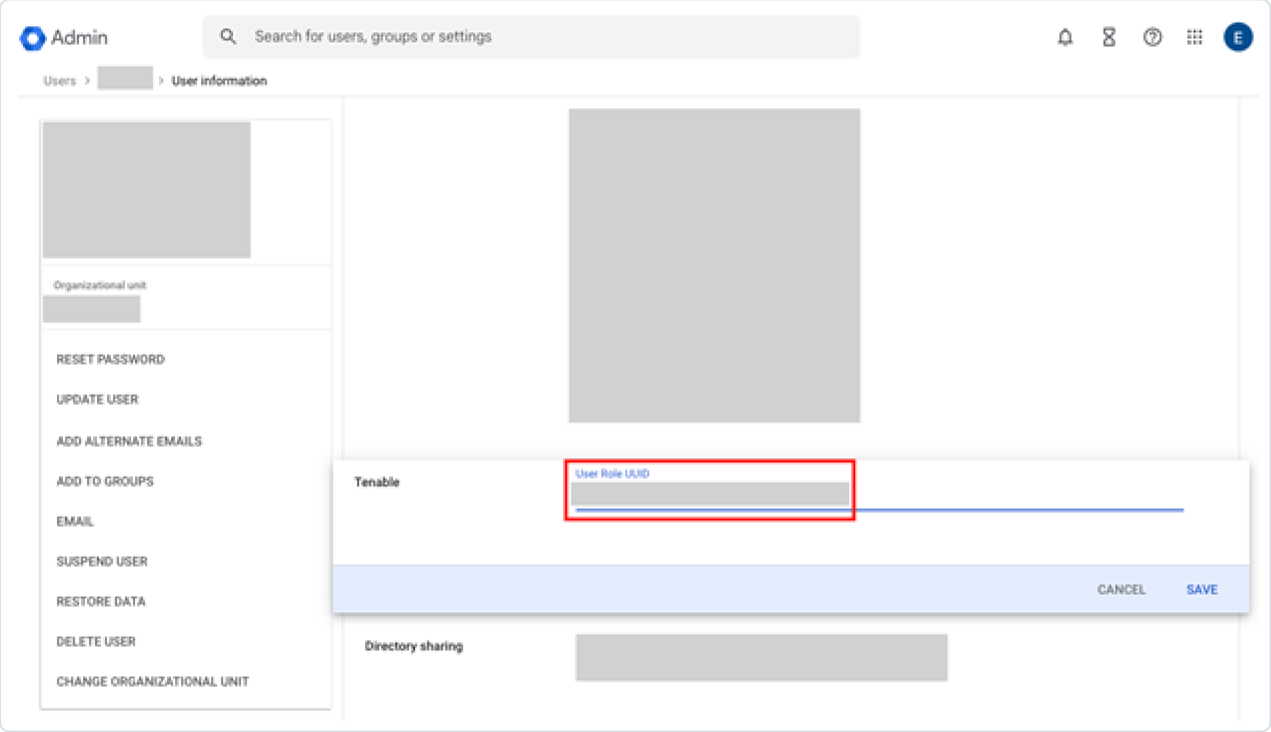
This user profile is incomplete. Add contact information for [redacted] like a secondary email address and a phone number.

[redacted] doesn't have any admin roles or privileges.

    The **User Details** page appears.

3. Click on the recently created custom attribute.

4. In the text box, type the UUID of the Tenable user role.



> **Tip:** Tenable user role UUIDs can be found in Tenable Vulnerability Management, in the **Settings** > **Access Control** > **Roles** table.

5. Click **Save**.

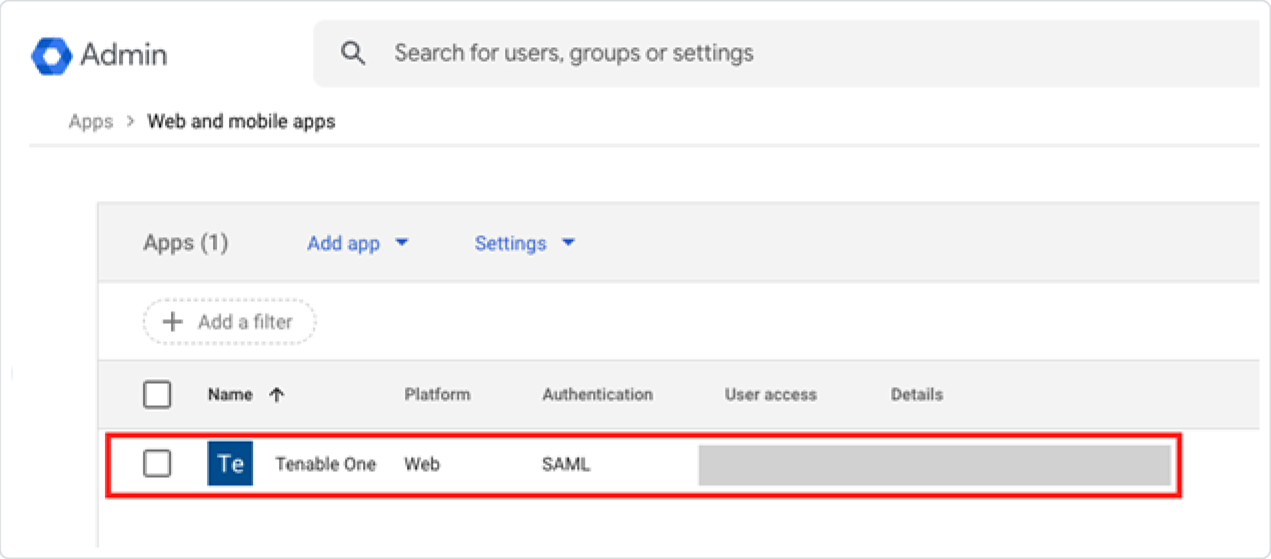
Configure the Role Claim

To configure the role claim:

1. In the navigation menu, navigate to **Apps** > **Web and mobile apps**.

   The **Web and mobile apps** page appears.

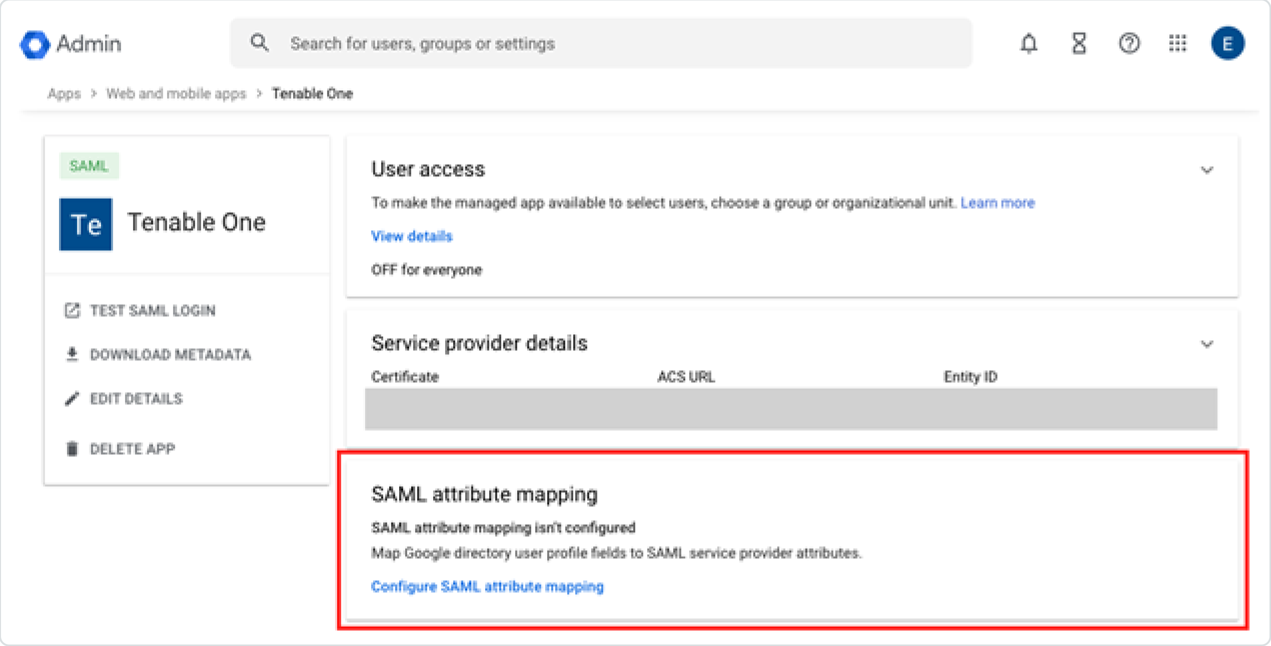
2. Select the newly created application.


Admin
Search for users, groups or settings
Apps > Web and mobile apps
Apps (1)
Add app
Settings
Add a filter

☐	Name ↑		Platform	Authentication	User access	Details
☐	Te	Tenable One	Web	SAML	[redacted]	

The application details appear.

3. Click **SAML attribute mapping**.



User access

To make the managed app available to select users, choose a group or organizational unit. Learn more

View details

OFF for everyone

Service provider details

Certificate	ACS URL	Entity ID
[redacted]		

SAML attribute mapping

SAML attribute mapping isn't configured

Map Google directory user profile fields to SAML service provider attributes.

Configure SAML attribute mapping

The **Attributes** page appears.

4. In the **Google Directory attributes** drop-down, select the appropriate Google Workspace custom attribute for the user role.

5. In the **App attributes** text box, type **userRoleUuid**.

6. Click **Save**.

   Any time a user logs in via your SAML configuration, Tenable One automatically adds them to the specified user role.

Additional Resources

For more information on Google Workspace IdP configuration, see the following resources:

- Set up Your Own Custom SAML App
- Access Apps via Google Workspace

Tenable One: Microsoft Entra ID IdP

One of the most common IdPs used to configure SAML with Tenable One is Microsoft Entra ID. The following steps guide you through the configuration process from start to finish.

Manual configuration requires the following:

- Reply URL: A custom URL provided by Tenable in the following format:

  ```
  https://cloud.tenable.com/saml/login/PLACEHOLDER
  ```

  > **Tip:** FedRAMP environments use the following custom URL format: `https://fedcloud.tenable.com/saml/login/PLACEHOLDER`

- Identifier (Entity ID): A custom ID provided by Tenable during SAML configuration in the following format:

  ```
  TENABLE_IO_PLACEHOLDER
  ```

- A certificate within the SAML metadata object that matches the data originally sent to Tenable.

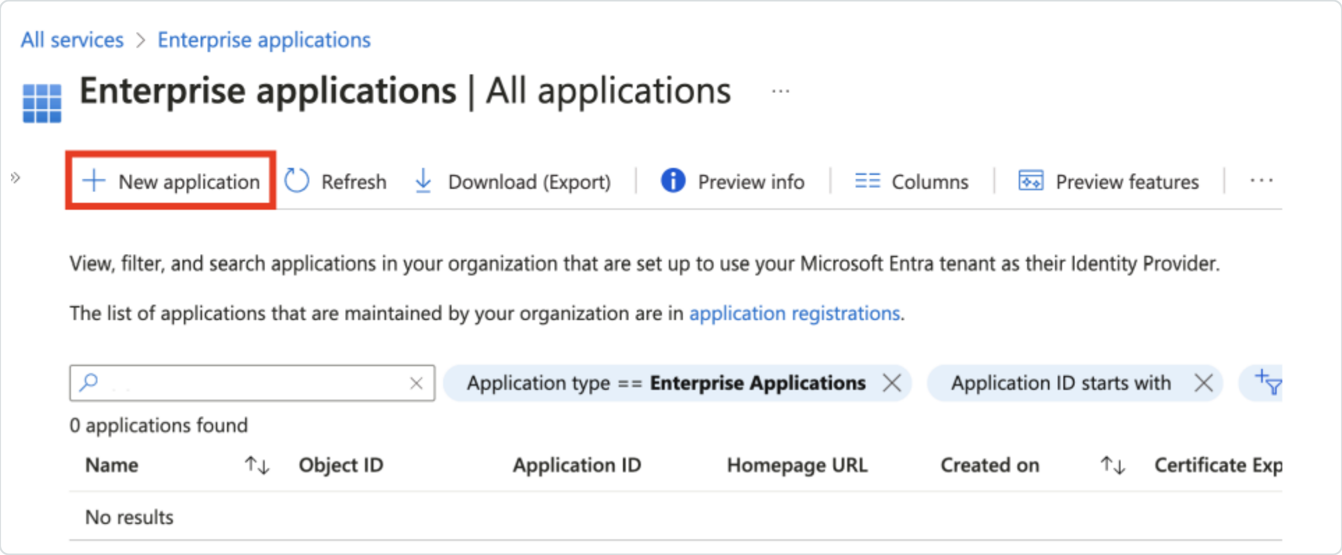
  > **Note:** Tenable does not support the use of multiple certificates and only extracts the first certificate from the metadata object. If the object includes multiple certificates, you must specify which certificate to use if it is not the first one listed.

Microsoft Entra ID: Create Initial Application

To create an application in Microsoft Entra ID:

1. In your browser, navigate to the Azure Admin portal.
2. In the navigation menu, navigate to **All services** > **Enterprise Applications**.

   The application gallery appears.



All services > Enterprise applications
Enterprise applications | All applications
+ New application
Refresh
Download (Export)
Preview info
Columns
Preview features
Application type == Enterprise Applications
Application ID starts with

View, filter, and search applications in your organization that are set up to use your Microsoft Entra tenant as their Identity Provider.

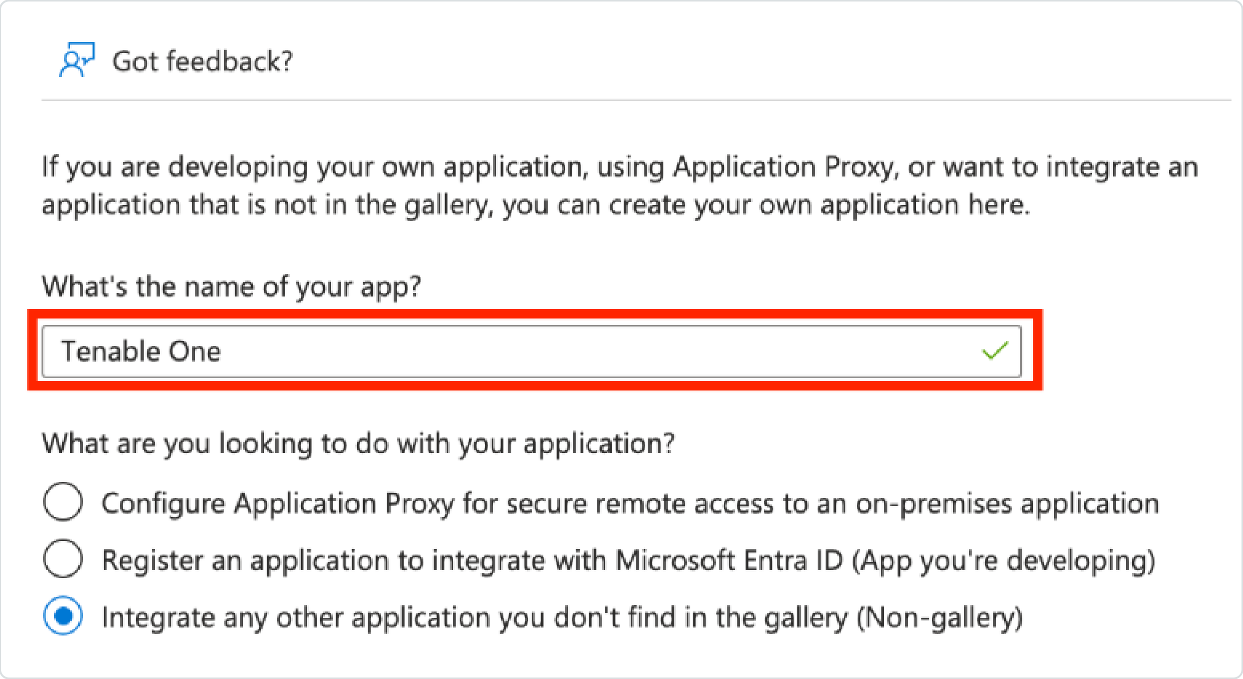
The list of applications that are maintained by your organization are in application registrations.

0 applications found

Name ↑↓	Object ID	Application ID	Homepage URL	Created on ↑↓	Certificate Exp
No results					

3. Click **New Application** > **Create your own application**.

   The **Create your own application** window appears.



Got feedback?

If you are developing your own application, using Application Proxy, or want to integrate an application that is not in the gallery, you can create your own application here.

What's the name of your app?

Tenable One ✓

What are you looking to do with your application?

○ Configure Application Proxy for secure remote access to an on-premises application

○ Register an application to integrate with Microsoft Entra ID (App you're developing)

● Integrate any other application you don't find in the gallery (Non-gallery)

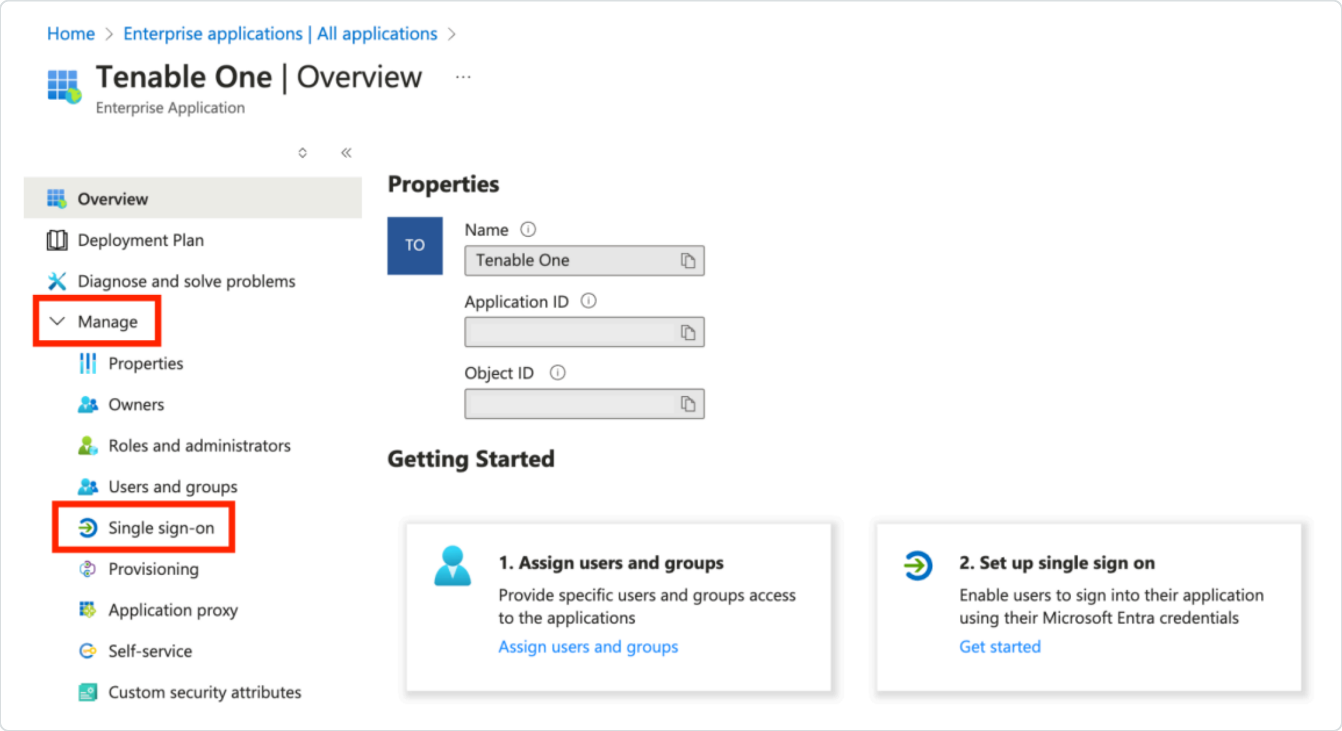
4. In the **What's the name of your app?** text box, type a name for your application, for example, **Tenable One**.

5. In the **What are you looking to do with your application** section, select the **Integrate any other application you don't find in the gallery** radio button.

6. Click **Create**.

   Microsoft Entra ID redirects you to the application overview page.

7. In the left navigation menu, click **Manage** > **Single sign-on**.



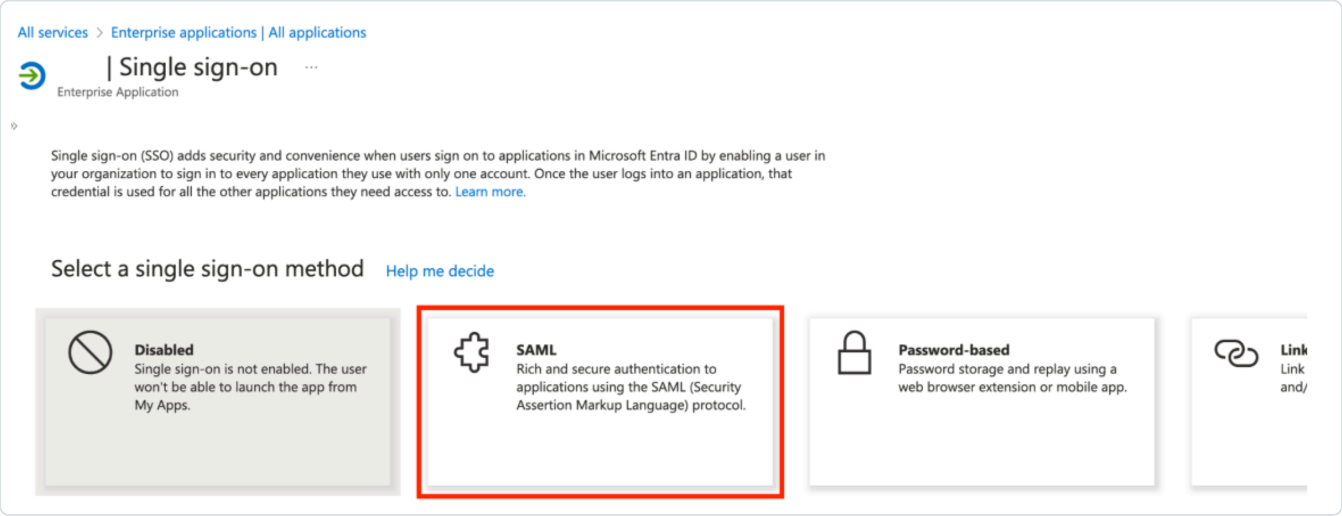
Name: Tenable One

Provide specific users and groups access to the applications

Enable users to sign into their application using their Microsoft Entra credentials

The **Single Sign-on** options appear.

8. Click the **SAML** tile.


All services > Enterprise applications | All applications
| Single sign-on ...
Enterprise Application
Select a single sign-on method
Help me decide
Disabled
SAML
Password-based
Link

Single sign-on (SSO) adds security and convenience when users sign on to applications in Microsoft Entra ID by enabling a user in your organization to sign in to every application they use with only one account. Once the user logs into an application, that credential is used for all the other applications they need access to. Learn more.

Single sign-on is not enabled. The user won't be able to launch the app from My Apps.

Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.

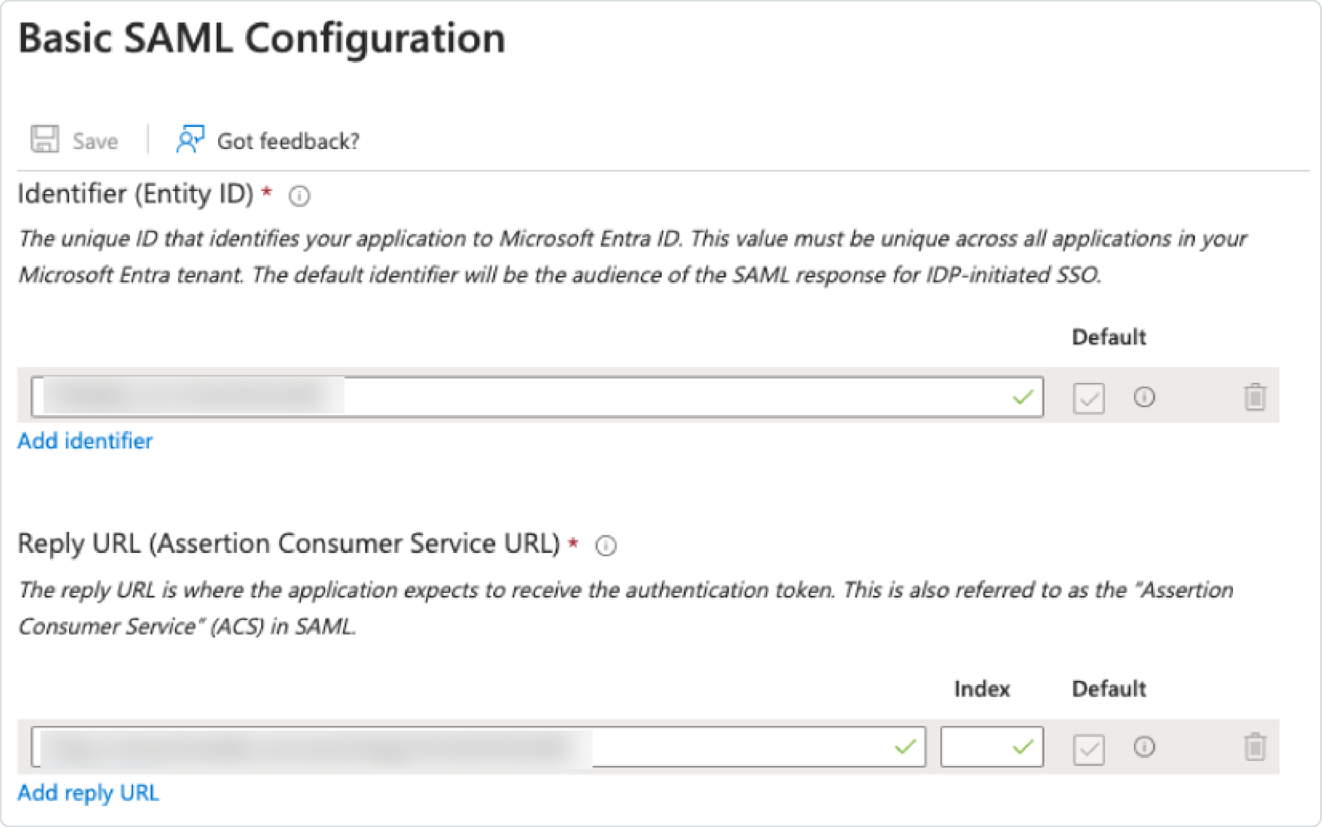
Password storage and replay using a web browser extension or mobile app.

Link and/

The **SAML-based Sign-on** page appears.

9. On the **Basic SAML Configuration** tile, click the ✎ **Edit** button.

The **Basic SAML Configuration** page appears.



Basic SAML Configuration

Identifier (Entity ID) *

The unique ID that identifies your application to Microsoft Entra ID. This value must be unique across all applications in your Microsoft Entra tenant. The default identifier will be the audience of the SAML response for IDP-initiated SSO.

Reply URL (Assertion Consumer Service URL) *

The reply URL is where the application expects to receive the authentication token. This is also referred to as the "Assertion Consumer Service" (ACS) in SAML.

10. In the **Identifier (Entity ID)** text box, type the following placeholder text:

    ```
    TENABLE_IO_PLACEHOLDER
    ```

    Note: You will later replace PLACEHOLDER with a unique UUID for the SAML configuration.

11. In the **Reply URL** text box, type the following placeholder text:

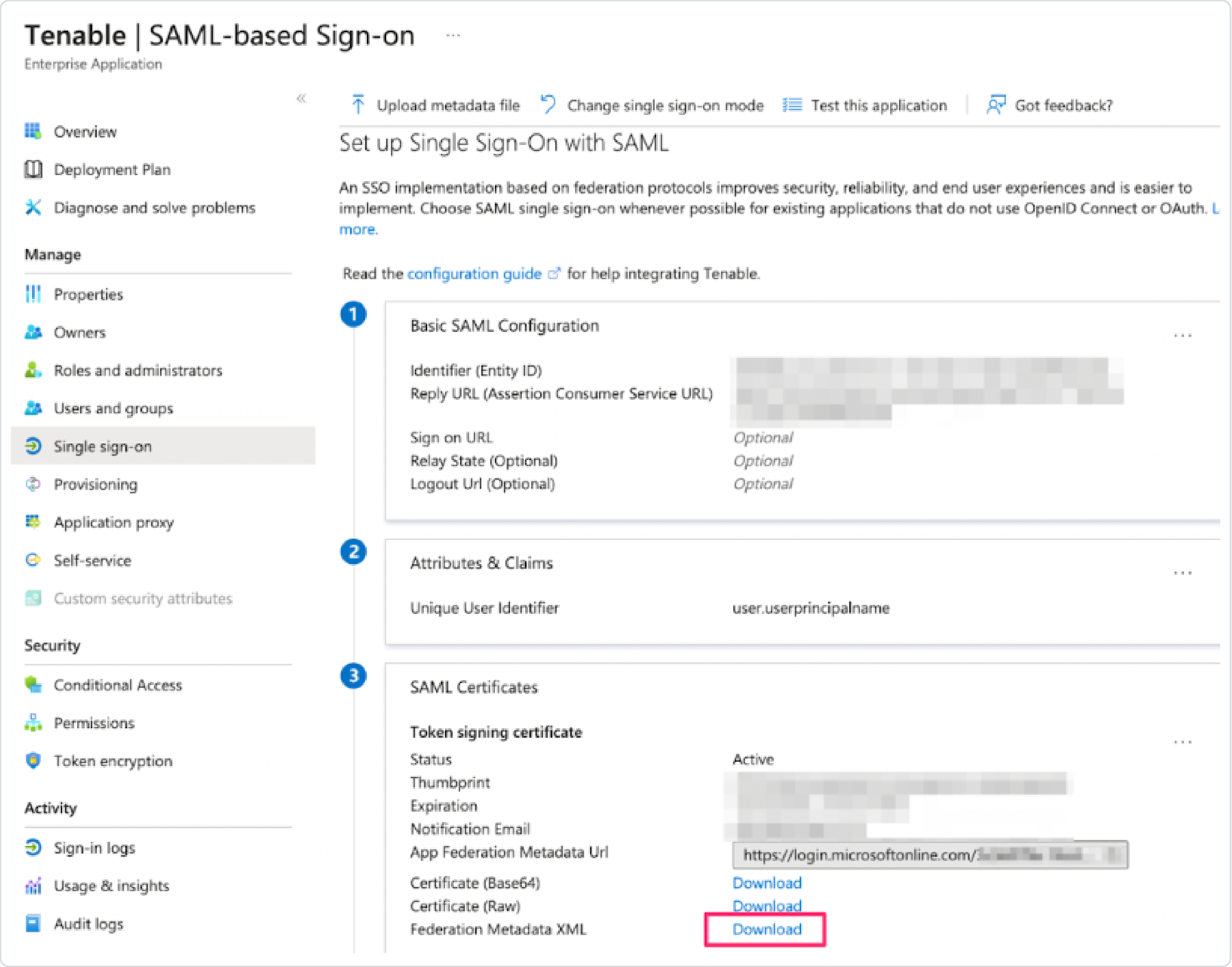
    ```
    https://cloud.tenable.com/saml/login/PLACEHOLDER
    ```

    Note: You will later replace *PLACEHOLDER* with a unique UUID for the SAML configuration. This link is case-sensitive.

12. Click **Save**.

    You return to the **SAML-based Sign-on** page.

13. On the **SAML Certificates** tile, in the **Federation Metadata XML** section, click **Download**.



Set up Single Sign-On with SAML

An SSO implementation based on federation protocols improves security, reliability, and end user experiences and is easier to implement. Choose SAML single sign-on whenever possible for existing applications that do not use OpenID Connect or OAuth. L more.

Read the configuration guide for help integrating Tenable.

1 Basic SAML Configuration

Identifier (Entity ID) [redacted]
Reply URL (Assertion Consumer Service URL)
Sign on URL *Optional*
Relay State (Optional) *Optional*
Logout Url (Optional) *Optional*

2 Attributes & Claims

Unique User Identifier user.userprincipalname

3 SAML Certificates

Token signing certificate
Status Active
Thumbprint [redacted]
Expiration
Notification Email
App Federation Metadata Url https://login.microsoftonline.com/[redacted]
Certificate (Base64) Download
Certificate (Raw) Download
Federation Metadata XML Download

Your browser downloads the metadata.xml file.

Tenable One SAML Configuration

Once you have downloaded your medata.xml file, you can use it to configure SAML in Tenable One. You can configure this directly in the Tenable Vulnerability Management application.

To set up the Tenable One SAML configuration:

1. In your browser, navigate to Tenable One.
2. On the **Workspace** page, click Tenable Vulnerability Management.

   The Tenable Vulnerability Management user interface appears.

3. In the upper-left corner, click the ☰ button.

   The left navigation plane appears.

4. In the left navigation plane, click **Settings**.

   The **Settings** page appears.

5. Click the **SAML** tile.

   The **SAML** page appears.

6. In the action bar, click ⊕ **Create**.

   The **SAML Settings** page appears.

7. Do one of the following:

   ### To provide configuration details by uploading the metadata.xml file from your IdP:

   a. In the first drop-down box, select **Import XML**.

      > **Note**: **Import XML** is selected by default.

   b. The **Type** drop-down box specifies the type of identity provider you are using. Tenable One supports SAML 2.0 (for example, Okta, OneLogin, etc.).
      This option is read-only.

   c. Under **Import**, click **Add File**.

      A file manager window appears.

   d. Select the metadata.xml file.

      The metadata.xml file is uploaded.

   ### To manually create your SAML configuration using data from the metadata.xml file from your IdP:

   a. In the first drop-down box, select **Manual Entry**.

      A **SAML** configuration form appears.

b. Configure the settings described in the following table:

Settings	Description
Enabled toggle	A toggle in the upper-right corner that indicates whether the SAML configuration is enabled or disabled. By default, the **Enable** setting is set to **Enabled**. Click the toggle to disable SAML configuration.
Type	Specifies the type of identity provider you are using. Tenable One supports SAML 2.0 (for example, Okta, OneLogin, etc.). This option is read-only.
Description	A description for the SAML configuration.
IdP Entity ID	The unique entity ID that your IdP provides. **Note**: If you want to configure multiple IdPs for a user account, create a new configuration for each identity provider with separate identity provider URLs, entity IDs, and signing certificates.
IdP URL	The SAML URL for your IdP.
Certificate	Your IdP security certificate or certificates. **Note**: Security certificates are found in a metadata.xml file that your identity provider provides. You can copy the content of the file and paste it in the **Certificate** box.
Authentication Request Signing Enabled	A toggle that indicates whether authentication request signing is enabled. When this toggle is enabled, if: • a user is logged in via SAML and their session expires • a user logs out and tries to log back in directly via the

	Tenable One interface rather than their IdP Tenable One automatically signs the SAML authentication request that is sent to the IdP to log the user back in. **Note:** The authentication request can only be validated if the IdP is also configured to accept this setting. For more information, see the following resources: • Manage Signing Certificates in Okta • Enforce Signed SAML Authentication Requests in Microsoft Entra ID • Edit a SAML Application in Ping Identity (**Enforce Signed AuthnRequest** option)
User Auto Provisioning Enabled	A toggle that indicates whether automatic user account creation is enabled or disabled. Automatic account provisioning allows users with an account for the IdP named in the SAML configuration to create a Tenable Vulnerability Management account the first time they log in via the IdP. **Note:** This option only appears during intial configuration if the setup is manual. Otherwise, you must edit the configuration after initial setup to enable this option.
IdP Assigns User Role at Provisioning	To assign a user role during provisioning, enable this toggle. In your SAML identity provider, add an attribute statement with **userRoleUuid** as the attribute name and the user role UUID as the attribute value. To obtain the UUID for a user role, go to **Settings** > **Access Control** > **Roles**. **Note:** This option only appears during intial configuration if the setup is manual. Otherwise, you must edit the configuration after initial setup to enable this option.

IdP Resets User Role at Each Login	To assign a role each time a user logs in, overwriting the current role with the one chosen in your IdP, enable this toggle. In your SAML identity provider, add an attribute statement with **userRoleUuid** as the attribute name and the user role UUID as the attribute value. To obtain the UUID for a user role, go to **Settings** > **Access Control** > **Roles**. **Note:** This option only appears during intial configuration if the setup is manual. Otherwise, you must edit the configuration after initial setup to enable this option.
Group Management Enabled	Enable this toggle to allow the Tenable One SAML configuration to manage user groups. You must enable this toggle for the Managed by SAML option to function successfully.

8. Click **Save**.

   Tenable Vulnerability Management saves your SAML configuration and you return to the **SAML** page.

9. In the row for the SAML configuration you just created, click the ⋮ button.

   An actions menu appears.

10. Click **Download SAML SP metadata**.

    Your browser downloads the metadata.xml file. You can now use this file for final configuration in your IdP.

Optional: Configure One or More User Groups to Automatically Add a User upon SAML Login

User groups allow you to manage user permissions for various resources in Tenable One. When you assign users to a group, the users inherit the permissions assigned to the group. When you enable the **Managed by SAML** option for a user group, Tenable One allows you to automatically add any user that logs in via SAML to that group.

Important: For this option to work successfully, you must also configure the related group claim within your IdP. View the final IdP configuration steps for more information.

Before you begin:

Ensure you've enabled the Group Management Enabled toggle when configuring the SAML settings within Tenable One.

To enable the Managed by SAML option:

1. In Tenable Vulnerability Management, in the upper-left corner, click the ≡ button.

   The left navigation plane appears.

2. In the left navigation plane, click **Settings**.

   The **Settings** page appears.

3. Click the **Access Control** tile.

   The **Access Control** page appears.

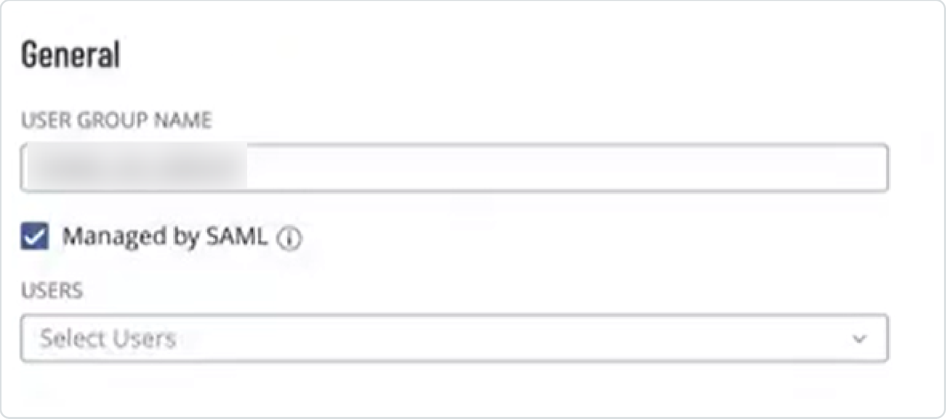
4. Click the **Groups** tab.

   The **Groups** page appears.

5. In the user groups table, click the user group to which you want to automatically add your SAML users.

   The **Edit User Group** page appears.

6. In the **General** section, select the **Managed by SAML** check-box.



USER GROUP NAME: [redacted]

☑ Managed by SAML

7. Click **Save**. Tenable Vulnerability Management saves your changes. Once you configure the related claim within your IdP, any time a user logs in via your SAML configuration, Tenable One automatically adds them to the specified user group.

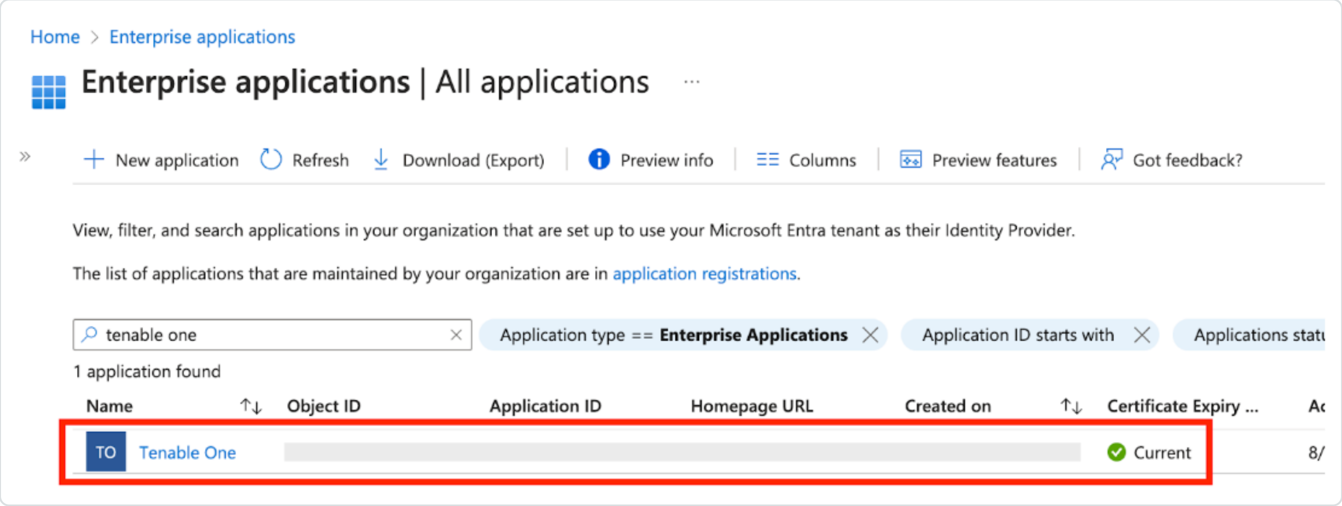
Microsoft Entra ID: Configure Final Application and Upload Metadata

Now that you have downloaded the completed metadata file, you can upload that file to your Tenable application in Microsoft Entra ID.

1. In your browser, navigate to the Azure Admin portal.
2. In the navigation menu, navigate to **All services** > **Enterprise Applications**.

   The application gallery appears.

3. Select the newly created application.



Home > Enterprise applications
Enterprise applications | All applications ···
»
+ New application
Refresh
Download (Export)
Preview info
Columns
Preview features
Got feedback?
tenable one
Application type == Enterprise Applications
Application ID starts with
Applications statu

View, filter, and search applications in your organization that are set up to use your Microsoft Entra tenant as their Identity Provider.

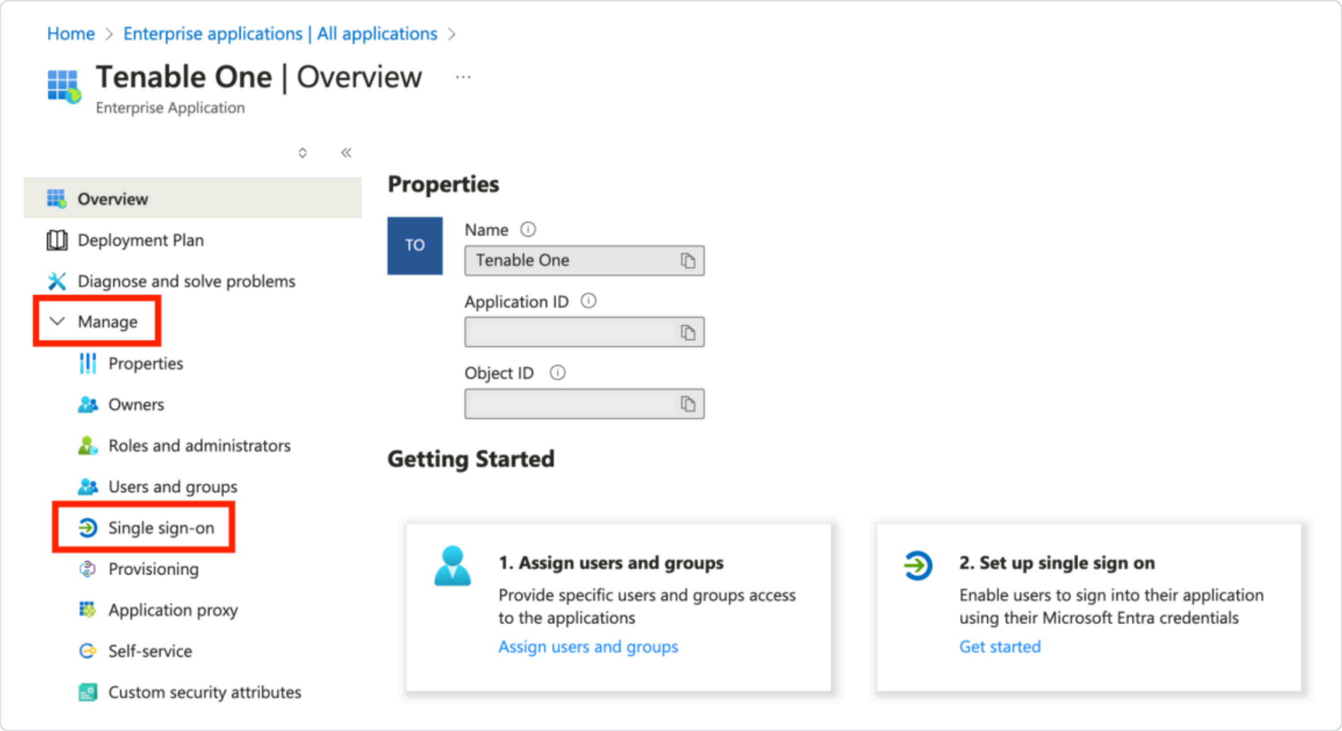
The list of applications that are maintained by your organization are in application registrations.

1 application found

Name	Object ID	Application ID	Homepage URL	Created on	Certificate Expiry ...	Ac
TO Tenable One	[redacted]	[redacted]	[redacted]	[redacted]	Current	8/

   The application overview appears.

4. In the left navigation menu, click **Manage** > **Single sign-on**.



Properties

Name: Tenable One

Application ID

Object ID

Getting Started

1. Assign users and groups

Provide specific users and groups access to the applications

Assign users and groups

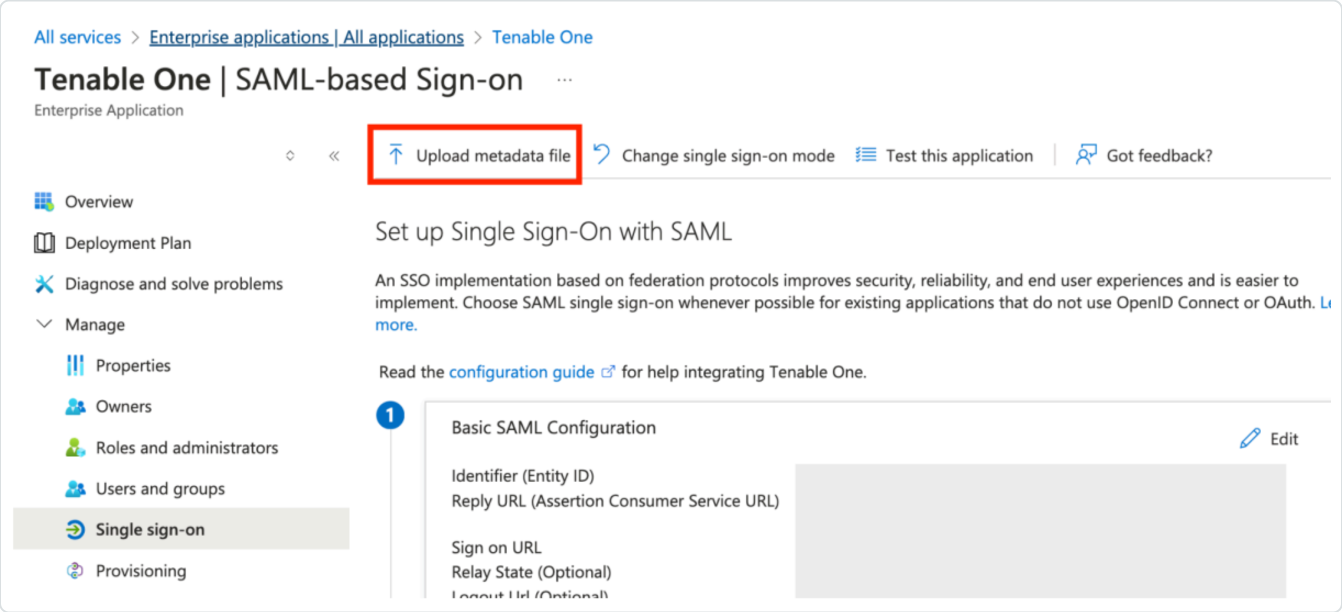
2. Set up single sign on

Enable users to sign into their application using their Microsoft Entra credentials

Get started

The **SAML-based Sign-on** options appear.

5. Click **Upload Metadata file**.



Set up Single Sign-On with SAML

An SSO implementation based on federation protocols improves security, reliability, and end user experiences and is easier to implement. Choose SAML single sign-on whenever possible for existing applications that do not use OpenID Connect or OAuth. Le more.

Read the configuration guide for help integrating Tenable One.

Basic SAML Configuration

Identifier (Entity ID)
Reply URL (Assertion Consumer Service URL)

Sign on URL
Relay State (Optional)
Logout Url (Optional)

6. In your file manager, select the Service Provider metadata.xml file that you downloaded from Tenable Vulnerability Management.

Microsoft Entra ID imports the metadata from the file, including the Reply URL and Identifier specific to the SAML configuration.

7. Click **Save**.

   Microsoft Entra ID saves your changes to the permanent application, and your SAML configuration is ready for use.

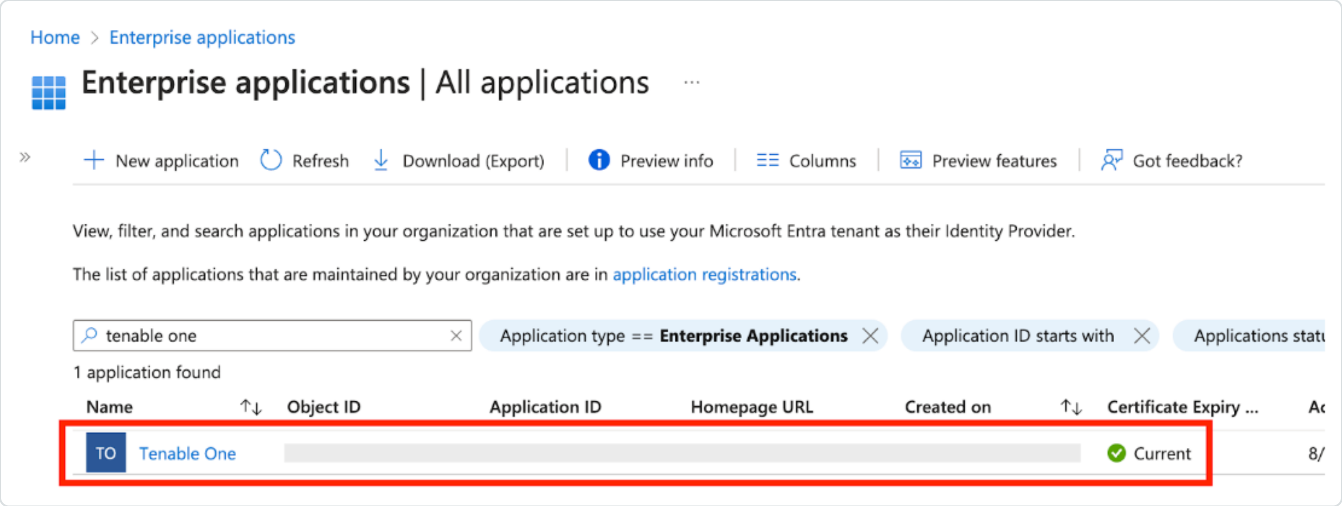
Optional: Finalize Configuration for Managed by SAML Group Option

If you configured the **Managed by SAML** option to automatically add any user that logs in via SAML to a user group, then you must configure a related group claim within the Microsoft Entra ID IdP.

To configure the IdP group claim:

1. In your browser, navigate to the Azure Admin portal.
2. In the navigation menu, navigate to **All services** > **Enterprise Applications**.

   The application gallery appears.
3. Select the newly created application.



Home > Enterprise applications

Enterprise applications | All applications ···

View, filter, and search applications in your organization that are set up to use your Microsoft Entra tenant as their Identity Provider.

The list of applications that are maintained by your organization are in application registrations.

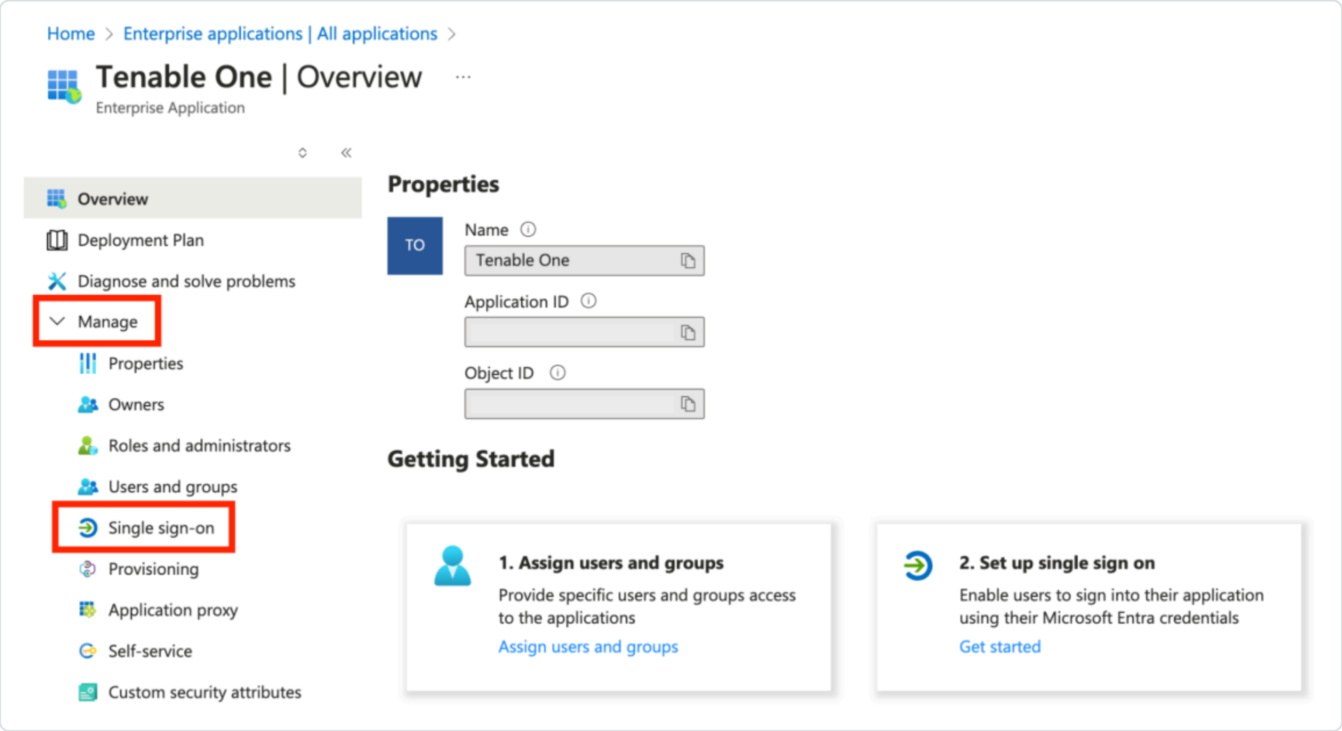
tenable one

Application type == **Enterprise Applications** ✕ | Application ID starts with ✕ | Applications statu

1 application found

Name ↑↓	Object ID	Application ID	Homepage URL	Created on ↑↓	Certificate Expiry ...	Ac
TO Tenable One	[redacted]				✓ Current	8/

   The application overview appears.
4. In the left navigation menu, click **Manage** > **Single sign-on**.



Name: Tenable One

1. Assign users and groups

Provide specific users and groups access to the applications

2. Set up single sign on

Enable users to sign into their application using their Microsoft Entra credentials

The **SAML-based Sign-on** options appear.

5. On the **Attributes & Claims** tile, click the ✎ **Edit** button.

   The **Attributes & Claims** page appears.

6. Click **Add a group claim**.

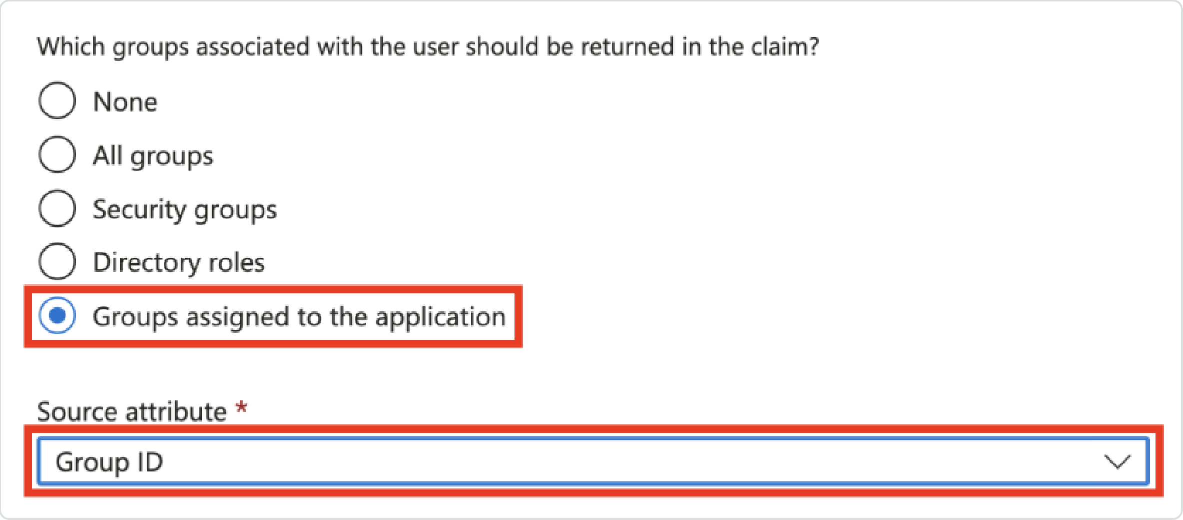
   The **Group Claims** pane appears.

7. Do one of the following:

   - To map all users to the same group:

     a. Select the **Groups assigned to the application** radio button.

     b. In the **Source attribute** drop-down, select the best option based on your environment, such as **Group ID**.



Which groups associated with the user should be returned in the claim?

○ None

○ All groups

○ Security groups

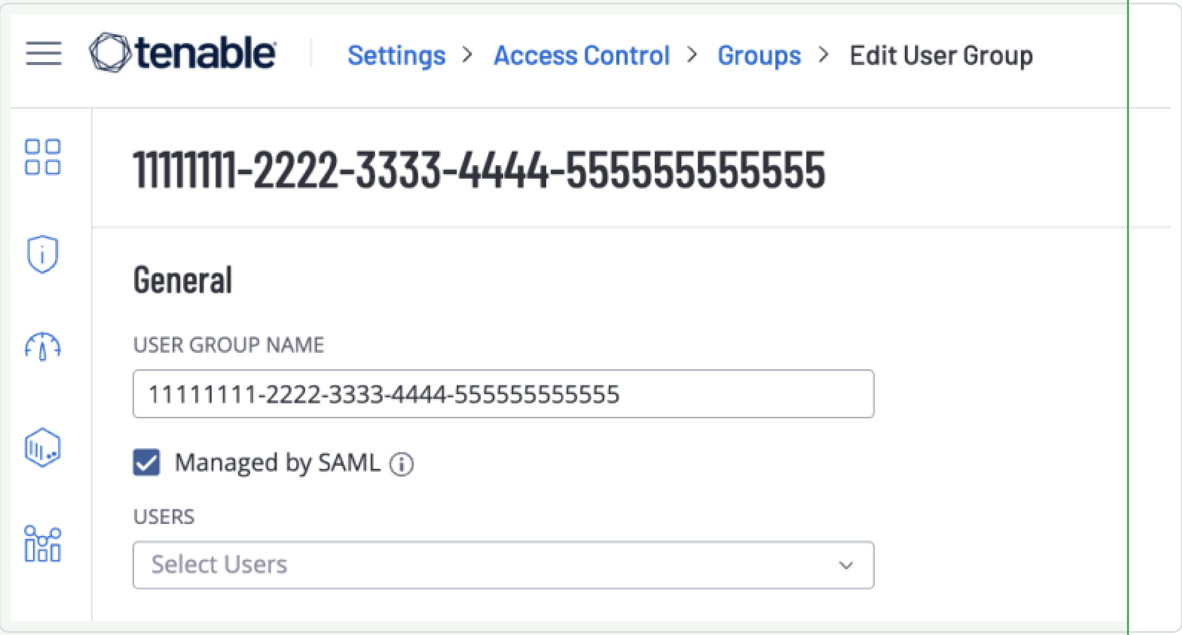
○ Directory roles

● Groups assigned to the application

Source attribute *

Group ID

Tip: The source attribute options available vary based on the selected groups. For example, the **Group ID** source attribute does not divulge a group's Display Name (for example, Developers), but rather its Object ID (for example, 11111111-2222-3333-4444-555555555555). As such, if you select Group ID, you must ensure that the name of the associated group configured within Tenable One matches the ID of the group listed within the Microsoft Entra ID portal (**Home** > **Groups** > **All Groups**).



11111111-2222-3333-4444-555555555555

General

USER GROUP NAME

11111111-2222-3333-4444-555555555555

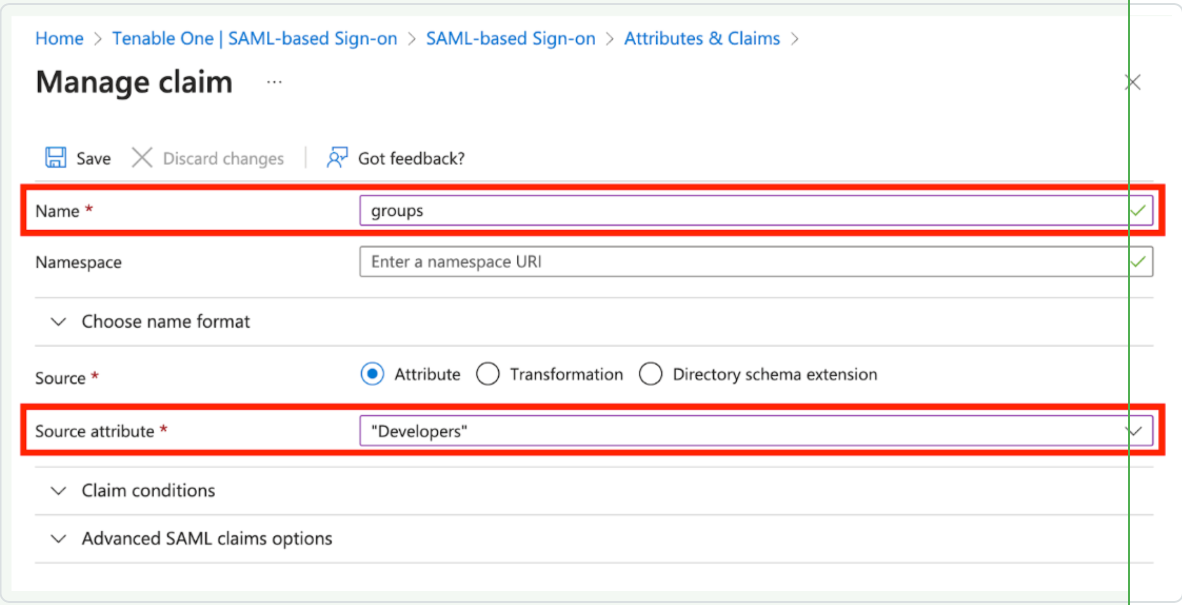
☑ Managed by SAML

USERS

Select Users

Where available, you may instead choose to select **Cloud-only group display names**. If you sync with Active Directory, there are other available options within the **Source Attribute** drop-down.

Alternatively, you could create a custom claim using **groups** as the claim name and setting the group's readable name (for example, Developers) as the source attribute.



Home > Tenable One | SAML-based Sign-on > SAML-based Sign-on > Attributes & Claims >

Manage claim

Name *	groups
Namespace	Enter a namespace URI

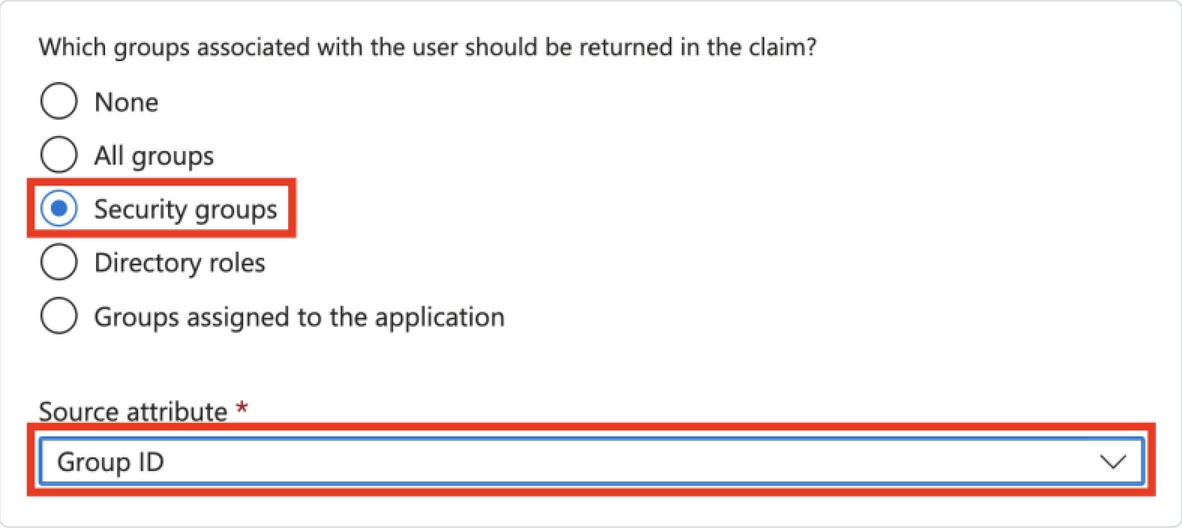
Source *	● Attribute ○ Transformation ○ Directory schema extension
Source attribute *	"Developers"

This allows mapping to readable names within Tenable One, instead of IDs, while not accounting for groups assigned to an application within Microsoft Entra ID. To maximize your configurations and make sure that you're familiar with all caveats, see [Configure group claims for applications by using Microsoft Entra ID](#).

- To map users to different groups:

    a. Select the radio button for the option that best suits your environment, for example, **Security Groups**.

    b. In the **Source attribute** drop-down, select the best option based on your environment, such as **Group ID**.



Which groups associated with the user should be returned in the claim?

○ None

○ All groups

● Security groups

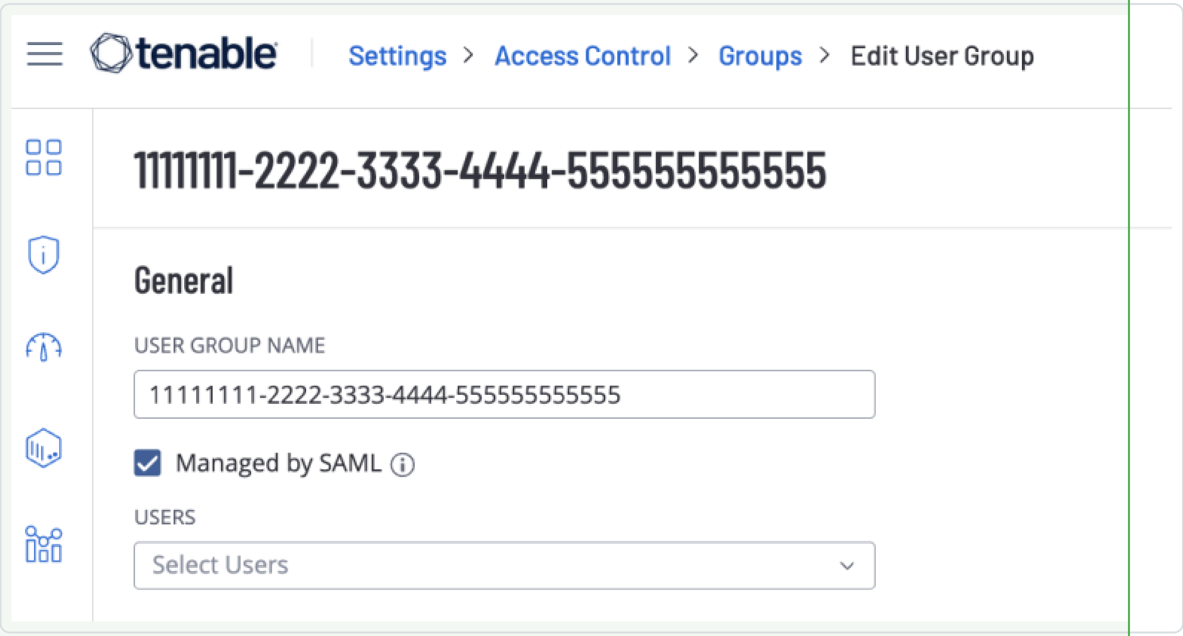
○ Directory roles

○ Groups assigned to the application

Source attribute *

Group ID

Tip: The source attribute options available vary based on the selected groups. For example, the **Group ID** source attribute does not divulge a group's Display Name (for example, Developers), but rather its Object ID (for example, 11111111-2222-3333-4444-555555555555). As such, if you select Group ID, you must ensure that the name of the associated group configured within Tenable One matches the ID of the group listed within the Microsoft Entra ID portal (**Home** > **Groups** > **All Groups**).



11111111-2222-3333-4444-555555555555

General

USER GROUP NAME

11111111-2222-3333-4444-555555555555

☑ Managed by SAML

USERS

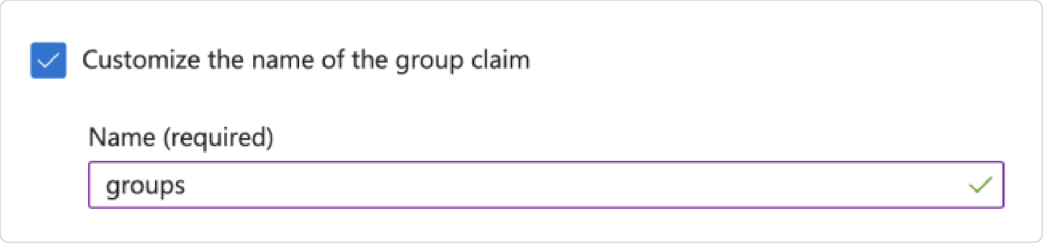
Select Users

Where available, you may instead choose to select **Cloud-only group display names**. If

> you sync with Active Directory, there are other available options within the **Source Attribute** drop-down.
>
> To maximize your configurations and make sure that you're familiar with all caveats, see Configure group claims for applications by using Microsoft Entra ID.

8. Select **Advanced** > **Customize the name of the group claim** check box.

9. In the **Name** text box, type **groups**.



☑ Customize the name of the group claim

Name (required)

groups

10. Click **Save**. Any time a user logs in via your SAML configuration, Tenable One automatically adds them to the specified user group in Tenable One.

Optional: Configure Managed by SAML Role Option

Roles allow you to manage privileges for major functions in Tenable One and control which Tenable One resources users can access. If you toggled on the SAML configuration options **IdP Assigns User Role at Provisioning** and/or **IdP Resets User Role at Each Login** (to automatically add and/or assign any user that logs in via SAML to a user role), then you must complete the following steps in Microsoft Entra ID:

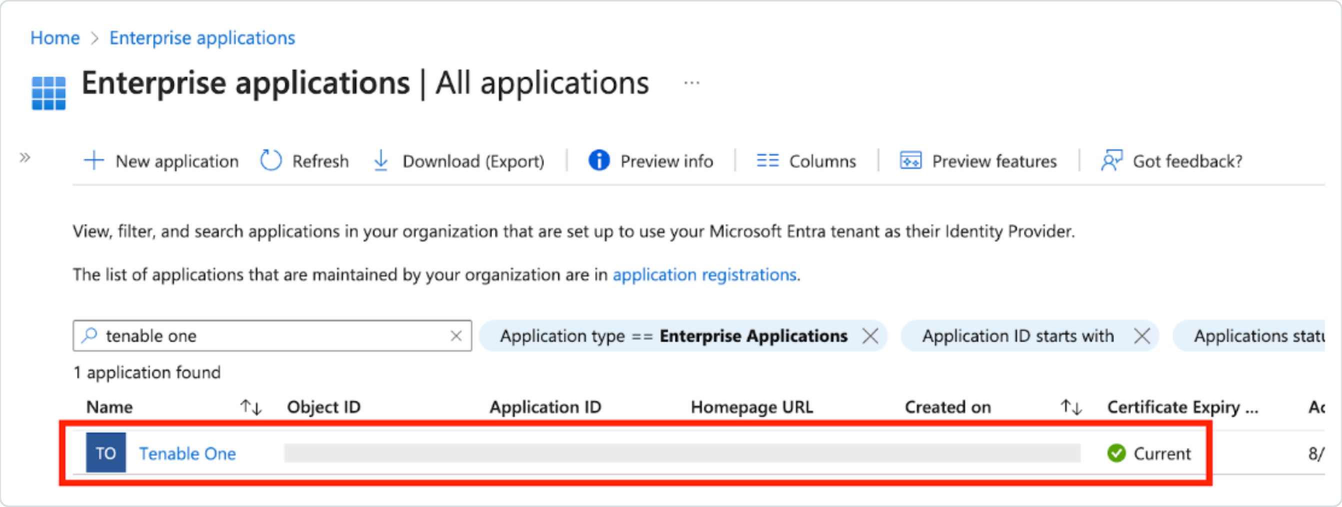
To configure Managed by SAML role option:

1. In your browser, navigate to the Azure Admin portal.

2. In the navigation menu, navigate to **All services** > **Enterprise Applications**.

   The application gallery appears.

3. Select the newly created application.


Home > Enterprise applications
Enterprise applications | All applications
+ New application
Refresh
Download (Export)
Preview info
Columns
Preview features
Got feedback?

View, filter, and search applications in your organization that are set up to use your Microsoft Entra tenant as their Identity Provider.

The list of applications that are maintained by your organization are in application registrations.

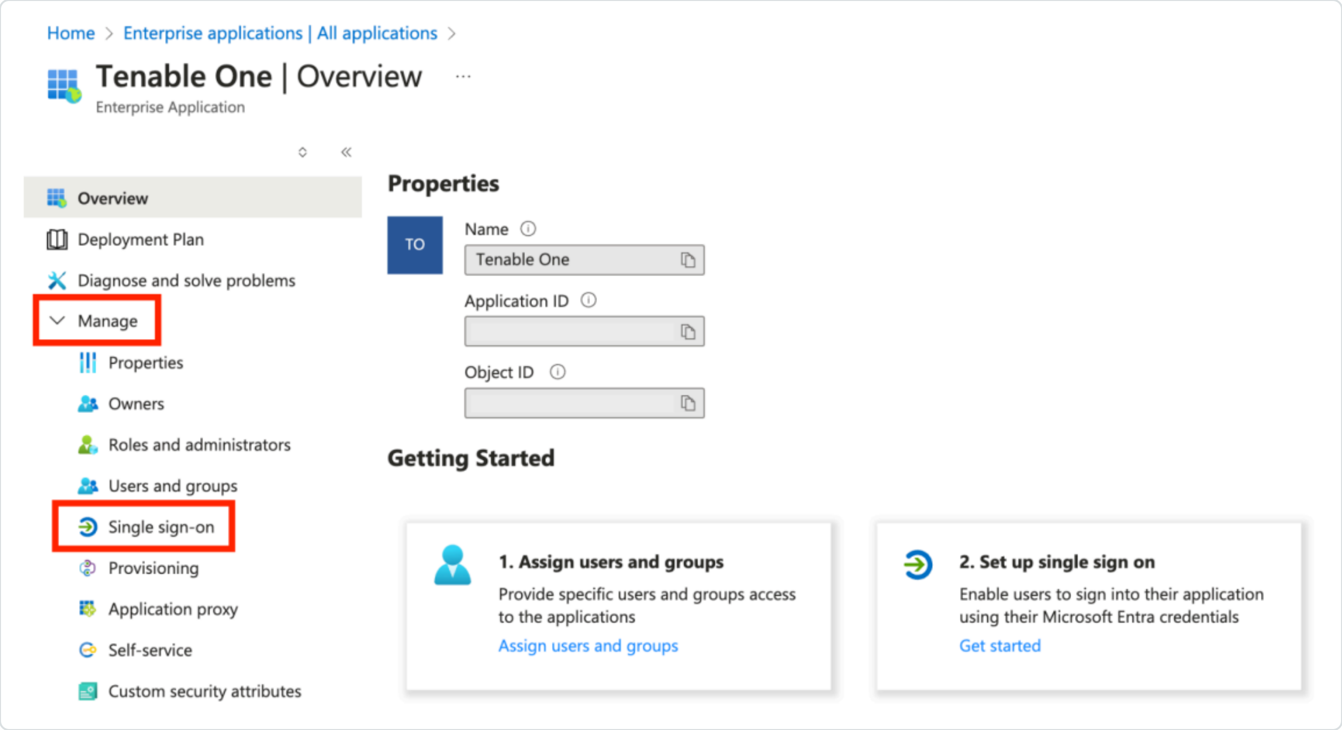
tenable one
Application type == Enterprise Applications
Application ID starts with
Applications statu

1 application found

Name	Object ID	Application ID	Homepage URL	Created on	Certificate Expiry ...	Ac
TO Tenable One	[redacted]				✓ Current	8/

The application overview appears.

4. In the left navigation menu, click **Manage** > **Single sign-on**.



Name: Tenable One

Application ID:

Object ID:

1. Assign users and groups

Provide specific users and groups access to the applications

Assign users and groups

2. Set up single sign on

Enable users to sign into their application using their Microsoft Entra credentials

Get started

The **SAML-based Sign-on** options appear.

5. On the **Attributes & Claims** tile, click the ✎ **Edit** button.

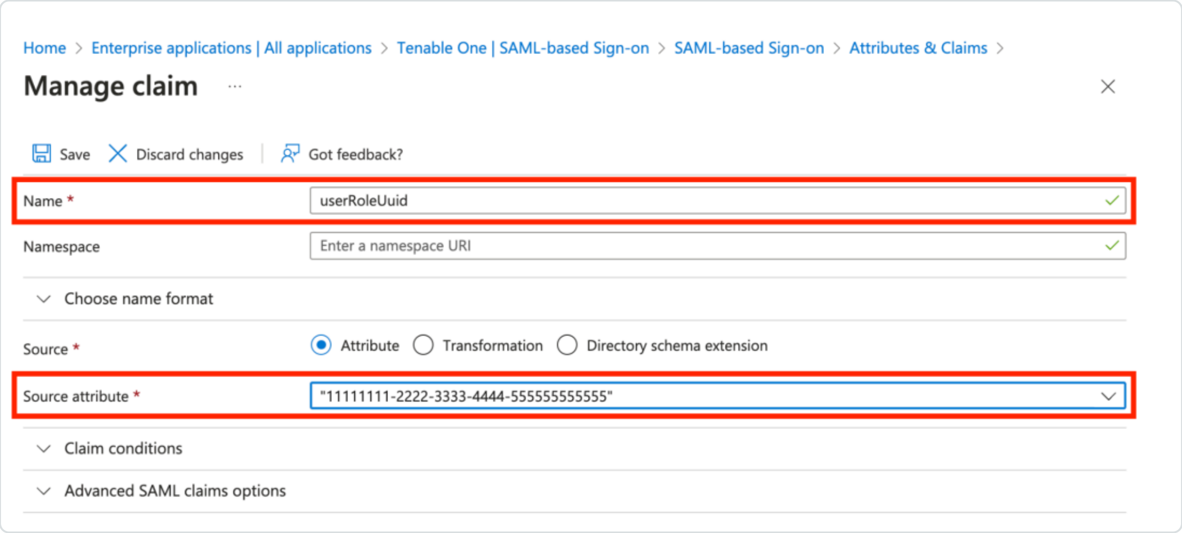
The **Attributes & Claims** page appears.

6. Do one of the following:

- To map all users to the same role:

    a. Click **Add new claim**.

    The **Manage claim** pane appears.



Home > Enterprise applications | All applications > Tenable One | SAML-based Sign-on > SAML-based Sign-on > Attributes & Claims >

Manage claim

Name * userRoleUuid

Namespace Enter a namespace URI

Source * ● Attribute ○ Transformation ○ Directory schema extension

Source attribute * "11111111-2222-3333-4444-555555555555"

    b. In the **Name** text box, type **userRoleUuid**.

    c. In the **Source attribute** text box, type the UUID of the Tenable user role.

    > **Tip:** Tenable user role UUIDs can be found in Tenable Vulnerability Management, in the **Settings** > **Access Control** > **Roles** table.

- To map individual users to different roles:

    If each user should be assigned their own unique role, you can define their role with user attributes. Based on your level of experience with Microsoft Entra ID and Microsoft Graph, you may be most comfortable with one option or another. Some examples include:

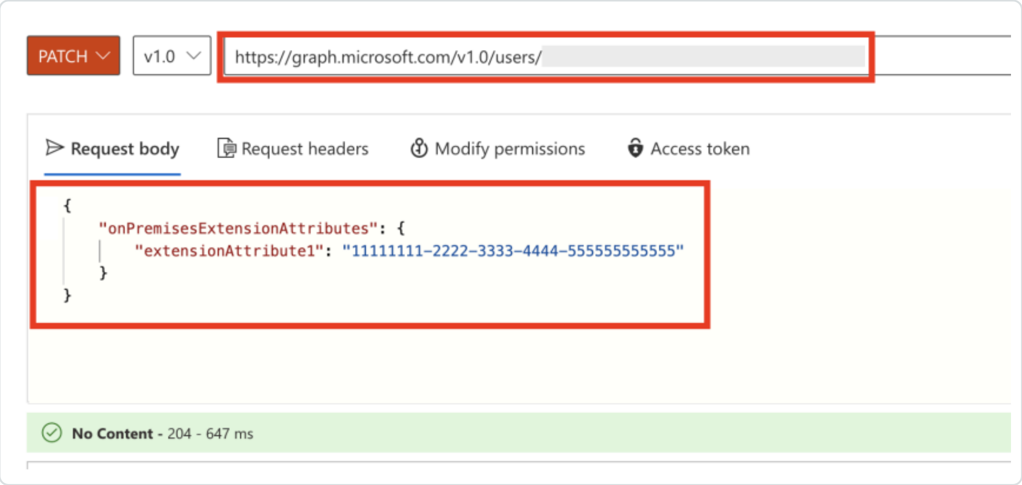
    - Leverage extension attribute: Microsoft Entra ID offers a set of 15 extension attributes with predefined names, which can be edited with Microsoft Graph. You can learn to add and read these extension attributes by visiting Add Custom data to Resources Using Extensions.

a. Using Microsoft Graph, identify an available (unused) extension attribute.

b. For each user within the organization, update the selected extension attribute with the UUID of the Tenable user role.

> **Tip:** Tenable user role UUIDs can be found in Tenable Vulnerability Management, in the **Settings** > **Access Control** > **Roles** table.

a. For example, you can modify the attribute using the PATCH method:

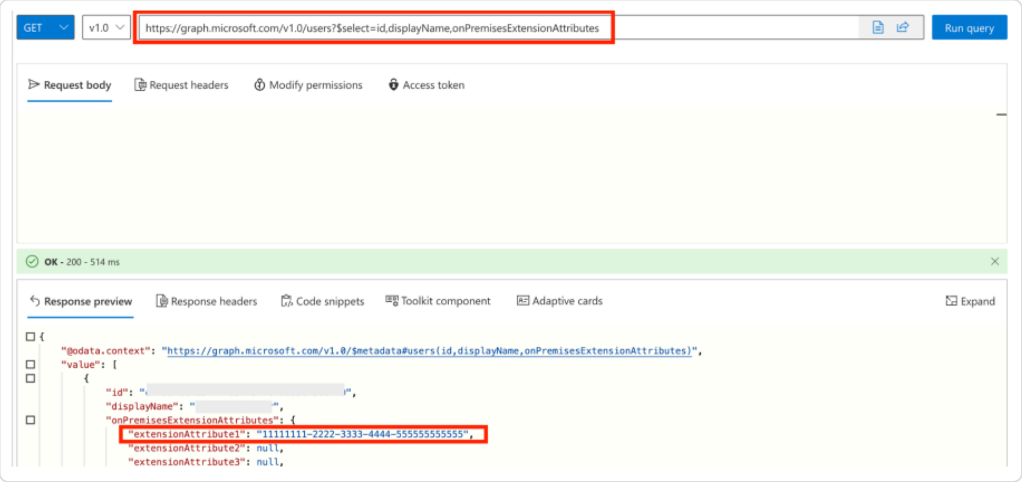


```
https://graph.microsoft.com/v1.0/users/[redacted]
```

```
{
    "onPremisesExtensionAttributes": {
        "extensionAttribute1": "11111111-2222-3333-4444-555555555555"
    }
}
```

No Content - 204 - 647 ms

b. Then confirm the change using the GET method:



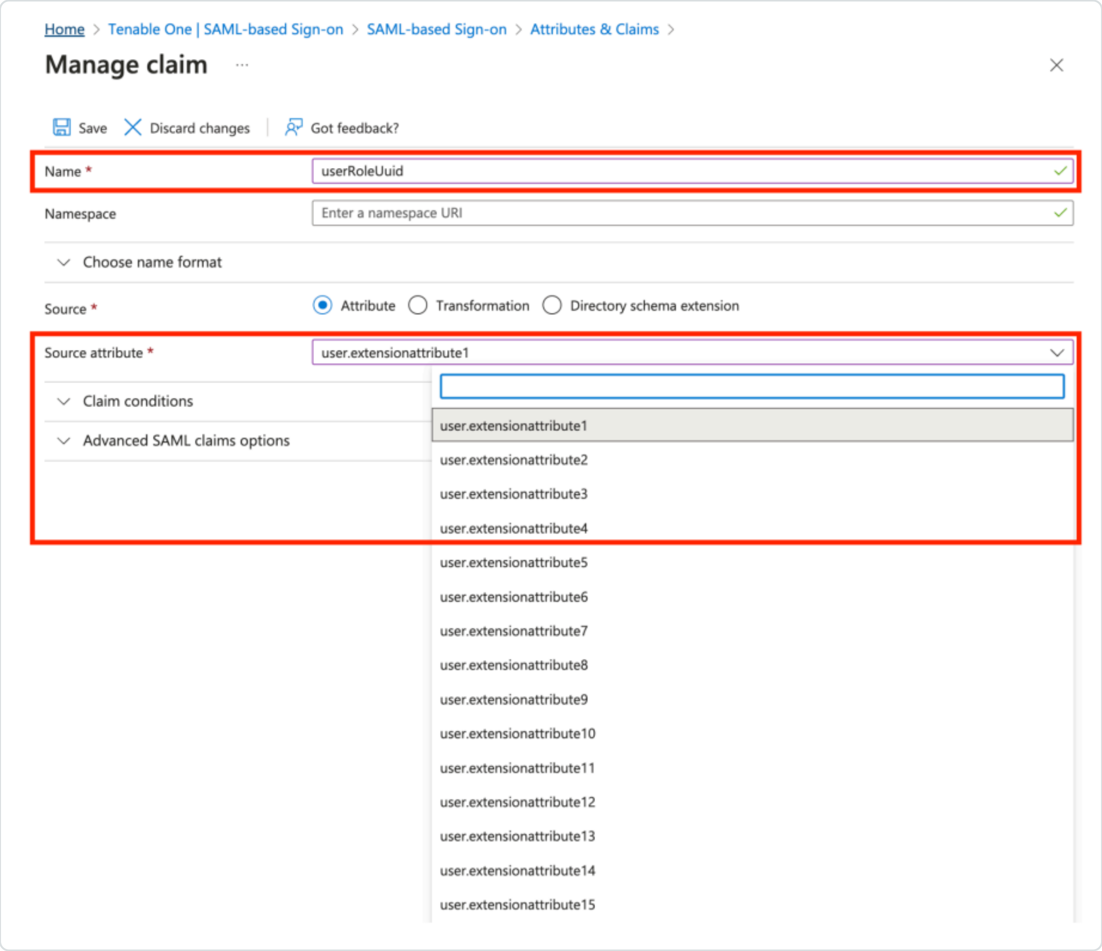
https://graph.microsoft.com/v1.0/users?$select=id,displayName,onPremisesExtensionAttributes

OK - 200 - 514 ms

```
{
    "@odata.context": "https://graph.microsoft.com/v1.0/$metadata#users(id,displayName,onPremisesExtensionAttributes)",
    "value": [
        {
            "id": "[redacted]",
            "displayName": "[redacted]",
            "onPremisesExtensionAttributes": {
                "extensionAttribute1": "11111111-2222-3333-4444-555555555555",
                "extensionAttribute2": null,
                "extensionAttribute3": null,
```

c. Within the **Attributes & Claims** page of the newly created app, click **Add new claim**.

The **Manage claim** pane appears.


Home > Tenable One | SAML-based Sign-on > SAML-based Sign-on > Attributes & Claims >
Manage claim ···
Save
Discard changes
Got feedback?
Choose name format
Claim conditions
Advanced SAML claims options

Name * userRoleUuid

Namespace Enter a namespace URI

Source * ● Attribute ○ Transformation ○ Directory schema extension

Source attribute * user.extensionattribute1

user.extensionattribute1
user.extensionattribute2
user.extensionattribute3
user.extensionattribute4
user.extensionattribute5
user.extensionattribute6
user.extensionattribute7
user.extensionattribute8
user.extensionattribute9
user.extensionattribute10
user.extensionattribute11
user.extensionattribute12
user.extensionattribute13
user.extensionattribute14
user.extensionattribute15

d. In the **Name** text box, type **userRoleUuid**.

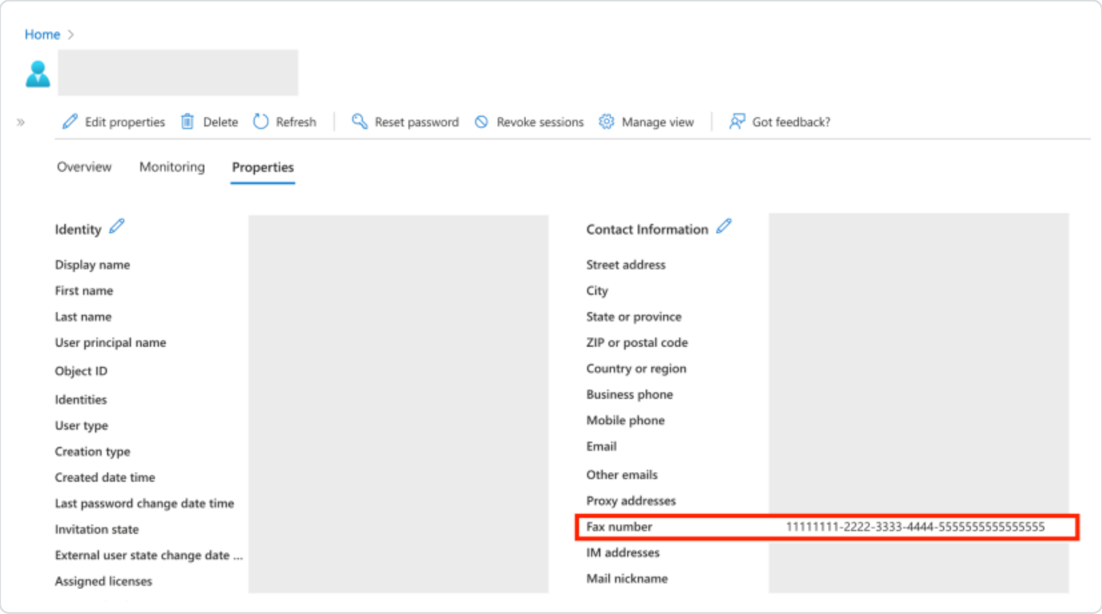
e. In the **Source attribute** text box, find and select the appropriate extension attribute (for example, **user.extensionattribute1**).

- Leverage existing attributes: You may opt to modify an existing and available (unused) attribute (for example, **Fax Number**). This can be useful for testing, small scale deployments, or until extension attributes can be leveraged.

  a. Navigate to **Home** > **Users**.

  b. For each user in scope, select **Properties**.

  The **Properties** pane appears.



Home >

Identity

Display name
First name
Last name
User principal name
Object ID
Identities
User type
Creation type
Created date time
Last password change date time
Invitation state
External user state change date ...
Assigned licenses

Contact Information

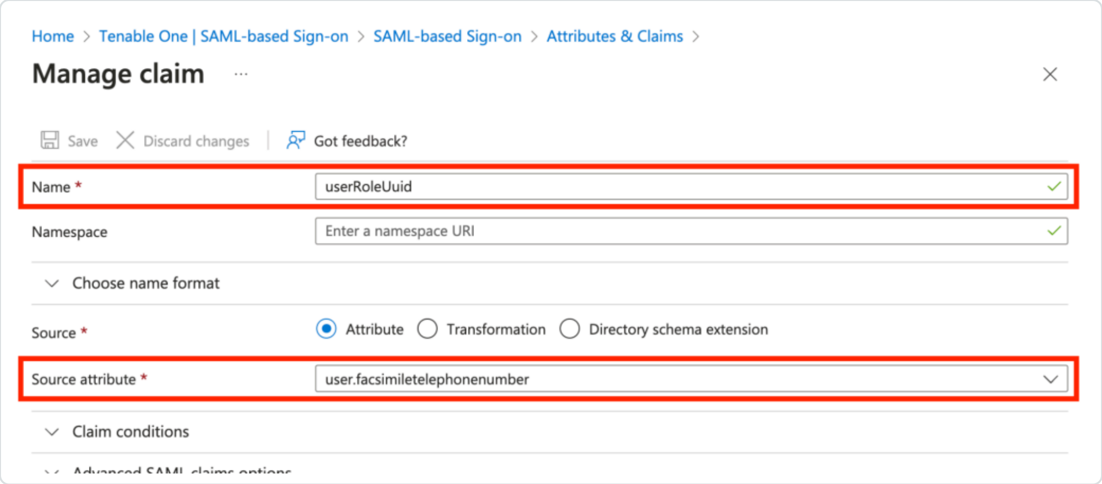
Street address
City
State or province
ZIP or postal code
Country or region
Business phone
Mobile phone
Email
Other emails
Proxy addresses
Fax number 11111111-2222-3333-4444-555555555555555
IM addresses
Mail nickname

c. Select an available existing attribute and edit the value with the UUID of the Tenable user role.

> **Tip:** Tenable user role UUIDs can be found in Tenable Vulnerability Management, in the **Settings** > **Access Control** > **Roles** table.

d. Within the **Attributes & Claims** page of the newly created app, click **Add new claim**.

The **Manage claim** pane appears.



Home > Tenable One | SAML-based Sign-on > SAML-based Sign-on > Attributes & Claims >

Manage claim

Name *	userRoleUuid
Namespace	Enter a namespace URI

Choose name format

Source *	● Attribute ○ Transformation ○ Directory schema extension
Source attribute *	user.facsimiletelephonenumber

Claim conditions

Advanced SAML claims options

e. In the **Name** text box, type **userRoleUuid**.

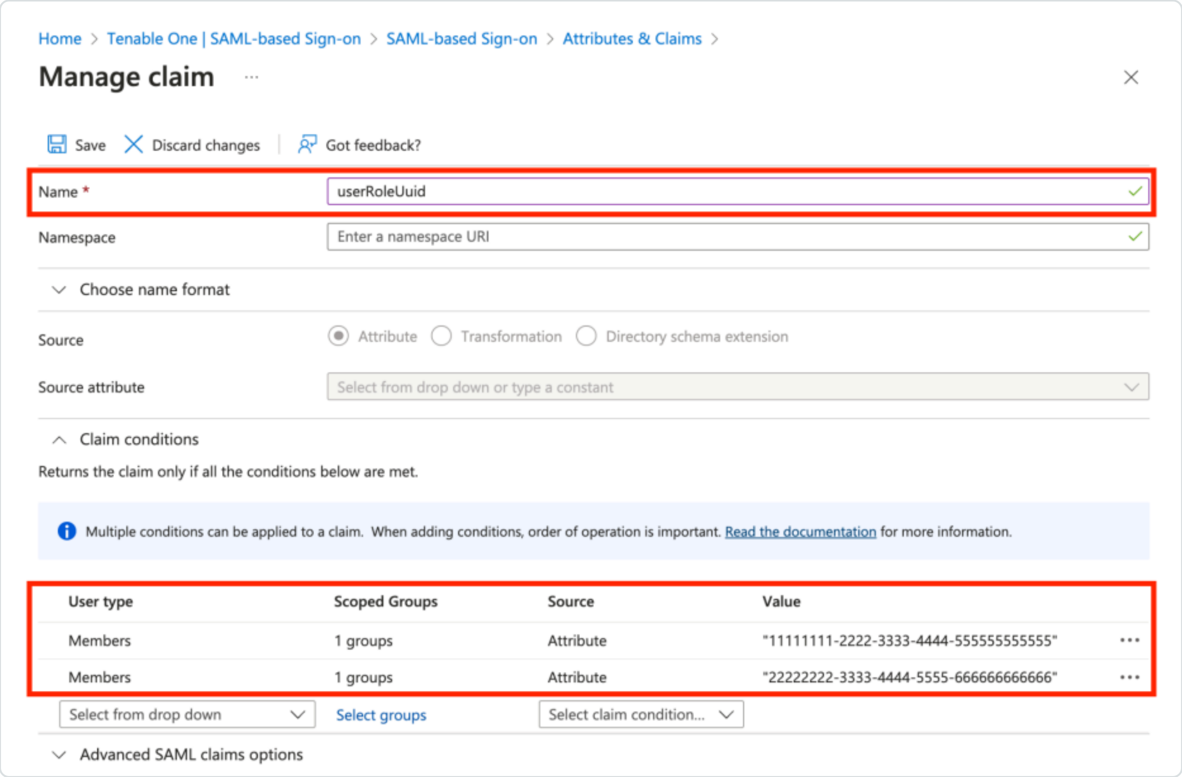
f. In the **Source attribute** text box, and and select the appropriate extension attribute (for example, **user.facsimiletelephonenumber**).

- To map user groups to different roles:

  If users of a specific user group within Microsoft Entra ID should all be assigned the same role within Tenable One, (for example, **Administrators**), then you can leverage their existing group membership:

  a. Click **Add new claim**.

  The **Manage claim** pane appears.



Home > Tenable One | SAML-based Sign-on > SAML-based Sign-on > Attributes & Claims >

Manage claim ···

Name * userRoleUuid

Namespace Enter a namespace URI

Choose name format

Source ● Attribute ○ Transformation ○ Directory schema extension

Source attribute Select from drop down or type a constant

Claim conditions

Returns the claim only if all the conditions below are met.

Multiple conditions can be applied to a claim. When adding conditions, order of operation is important. Read the documentation for more information.

User type	Scoped Groups	Source	Value
Members	1 groups	Attribute	"11111111-2222-3333-4444-555555555555"
Members	1 groups	Attribute	"22222222-3333-4444-5555-666666666666"
Select from drop down	Select groups	Select claim condition...	

Advanced SAML claims options

  b. In the **Name** text box, type **userRoleUuid**.

  c. For each required role:

i. Under **Claim conditions**, in the **User type** drop-down, select the best option based on your environment, such as **Members**.

ii. Click **Select groups** and then select the relevant user group.

iii. In the **Source** drop-down, select **Attribute**.

d. In the **Value** text box, type the UUID of the Tenable user role.

> **Tip:** Tenable user role UUIDs can be found in Tenable Vulnerability Management, in the **Settings** > **Access Control** > **Roles** table.

7. Click **Save**. Any time a user logs in via your SAML configuration, Tenable One automatically adds them the specified user role in Tenable One.

> **Tip:** Alternatively, you can create separate applications in Microsoft Entra ID: one for each role and/or each user group (along with separate SAML integrations within Tenable One), where each user is assigned to an application based on their expected role/group mapping.

Additional Resources

For more information on Microsoft Entra ID IdP configuration, see the following resources:

- Microsoft Entra ID Developer Portal
- SAML Authentication with Microsoft Entra ID
- Use a SAML 2.0 IdP for Single Sign On

SAML for Individual Tenable Applications

Several Tenable applications support configuring an individual SAML configuration for the app. You may require these configuration steps if you are not a Tenable One customer, or you want to configure a SAML configuration for an application individually or outside of the Tenable One product suite.

The information in this section aims to provide complete configuration steps to use SAML with the following Tenable products:

> **Tip:** Looking for individual configuration instructions for Tenable Vulnerability Management, Tenable Web App Scanning, Tenable Cloud Security, or Tenable Attack Surface Management? These apps follow the SAML for Tenable One configuration workflow. For more information, see the table on the Welcome page.

Tenable Identity Exposure SAML Configuration

You can configure Tenable Identity Exposure to accept credentials from your SAML identity provider. This allows for an additional layer of security, where the SAML credentials are certified for use within Tenable Identity Exposure. Once you enable SAML for a user, they can log in to Tenable Identity Exposure directly through their identity provider, which automatically signs them in and redirects them to the Tenable Identity Exposure landing page.

While several configuration steps occur directly in the Tenable Identity Exposure user interface, the entire SAML configuration process includes several processes across multiple applications. This guide describes three of the most commonly used Identity Providers (IdPs) and how to configure them for use with Tenable Identity Exposure SAML from start to finish.

To get started, see the following topics:

- Tenable Identity Exposure: Okta IdP
- Tenable Identity Exposure: Microsoft Entra ID IdP
- Troubleshooting and Common Errors

Tenable Identity Exposure: Okta IdP

One of the most common IdPs used to configure SAML with Tenable Identity Exposure is Okta. The following steps guide you through the configuration process from start to finish.

Manual configuration requires the following:

- **URL of the SAML server**: A value that corresponds to the **IdP provider SSO URL** within Okta.
- **Assert endpoint of the Tenable.ad service provider**: A value that corresponds to the **Audience URI (SP Identity ID)** within Okta.
- **Trusted Certificate Authorities**: The SAML server certificate in PEM-encoded format, beginning with `-----BEGIN CERTIFICATE -----` and ending with `-----END CERTIFICATE -----`, provided by Okta in the **X.509 certificate** section.

Enable Tenable Identity Exposure SAML

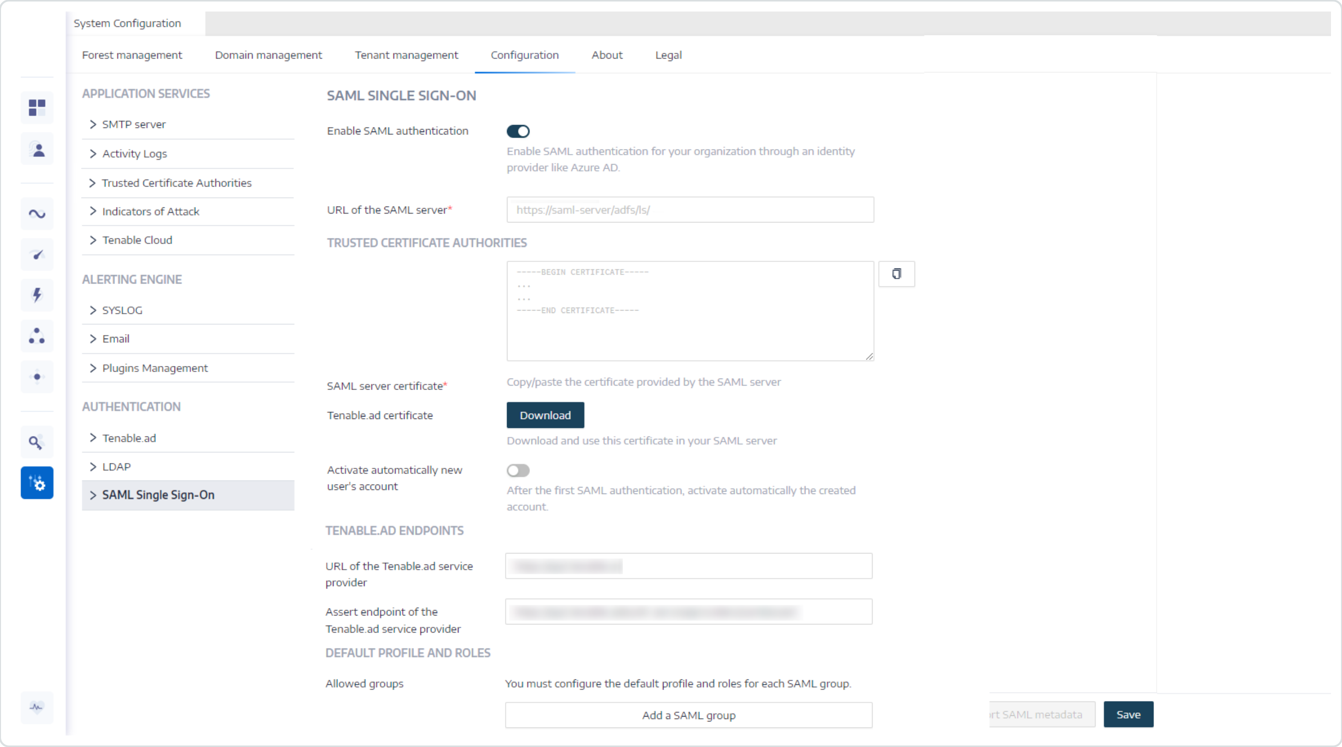
The first step in configuring SAML for use with Tenable Identity Exposure is to enable the configuration in the Tenable Identity Exposure application. Then, you can download your certificate file to use in your IdP.

To enable the Tenable Identity Exposure SAML configuration:

1. In your browser, navigate to Tenable Identity Exposure.
2. Navigate to **Systems** > **Configuration**.

   The configuration pane appears.
3. Under the **Authentication** section, click **SAML Single Sign-on**.
4. Click the **Enable SAML authentication** toggle.

   A SAML information form appears.



SAML SINGLE SIGN-ON

Enable SAML authentication: on

Enable SAML authentication for your organization through an identity provider like Azure AD.

URL of the SAML server*: https://saml-server/adfs/ls/

TRUSTED CERTIFICATE AUTHORITIES

```
-----BEGIN CERTIFICATE-----
...
...
-----END CERTIFICATE-----
```

SAML server certificate*: Copy/paste the certificate provided by the SAML server

Tenable.ad certificate: Download

Download and use this certificate in your SAML server

Activate automatically new user's account: off

After the first SAML authentication, activate automatically the created account.

TENABLE.AD ENDPOINTS

URL of the Tenable.ad service provider: [redacted]

Assert endpoint of the Tenable.ad service provider: [redacted]

DEFAULT PROFILE AND ROLES

Allowed groups: You must configure the default profile and roles for each SAML group.

5. In the **Tenable.ad Certificate** section, click **Download**.

   Your browser downloads the certificate needed to connect with your IdP.

6. In the **Tenable.ad Endpoints** section, copy the following values for use within your IdP:

   - **URL of the Tenable.ad service provider**
   - **Assert endpoint of the Tenable.ad service provider**

You can now use the downloaded certificate and copied values to set up the connection with your IdP.

Okta: Configure Application Integration and Upload Certificate

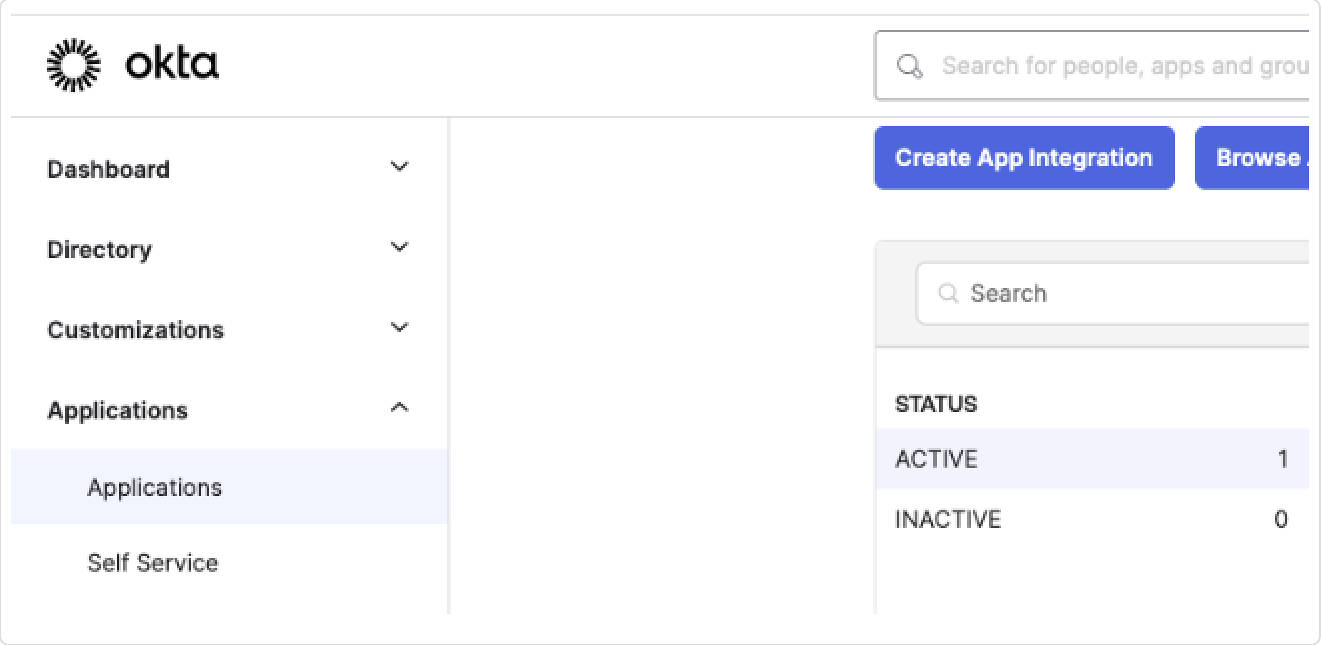
Now that you have enabled the Tenable Identity Exposure SAML configuration, you can create a Tenable application in Okta.

1. In your browser, navigate to the Okta Admin portal.
2. In the left navigation menu, click **Applications** > **Applications**.

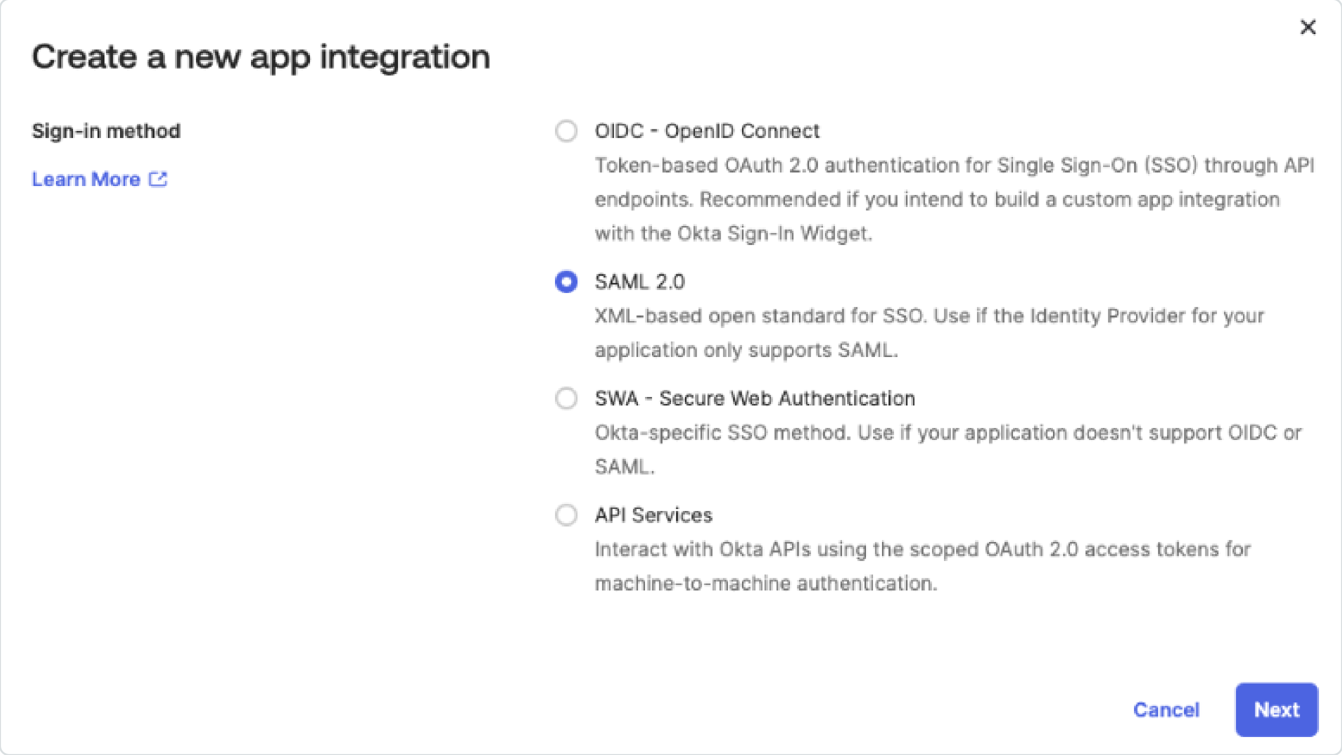
   The **Applications** page appears.

3. Click **Create App Integration**.

   The **Create a new app integration** window appears.



4. Select the **SAML 2.0** radio button.



Create a new app integration

Sign-in method

Learn More

○ OIDC - OpenID Connect
Token-based OAuth 2.0 authentication for Single Sign-On (SSO) through API endpoints. Recommended if you intend to build a custom app integration with the Okta Sign-In Widget.

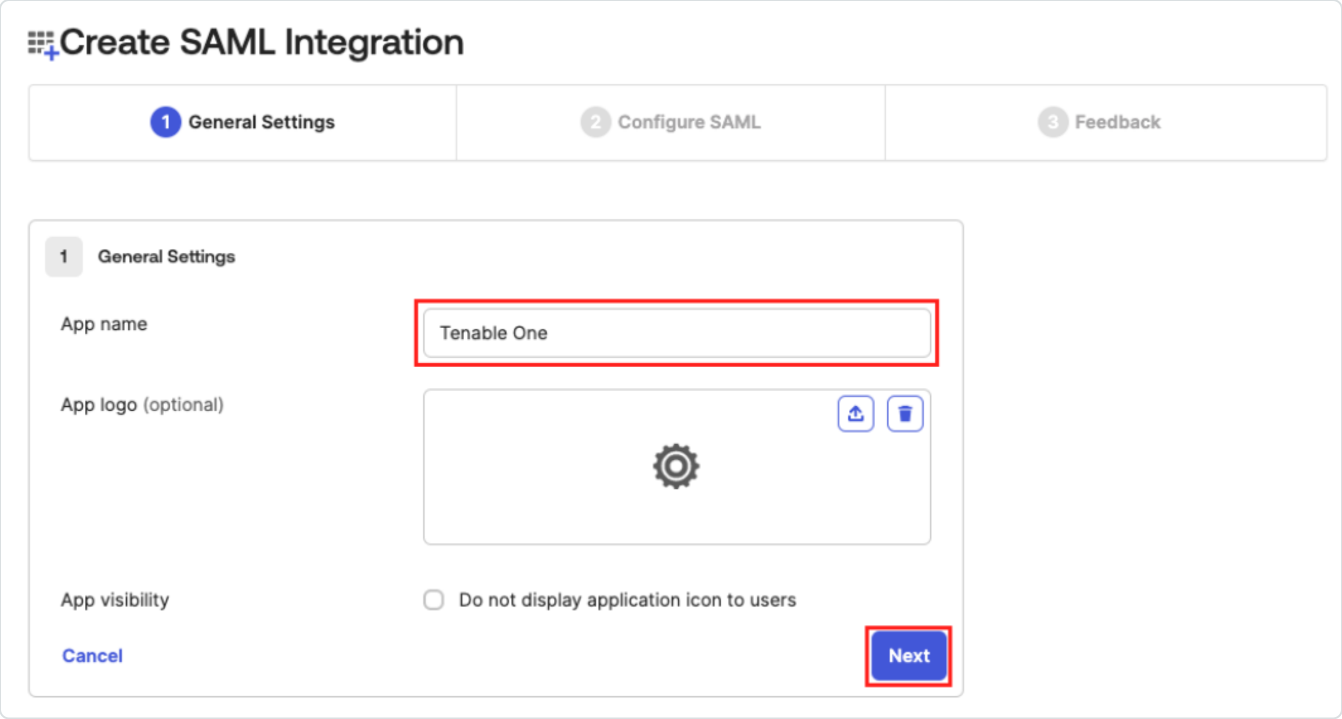
● SAML 2.0
XML-based open standard for SSO. Use if the Identity Provider for your application only supports SAML.

○ SWA - Secure Web Authentication
Okta-specific SSO method. Use if your application doesn't support OIDC or SAML.

○ API Services
Interact with Okta APIs using the scoped OAuth 2.0 access tokens for machine-to-machine authentication.

5. Click **Next**.

   The **General Settings** options appear.



Create SAML Integration

1 General Settings

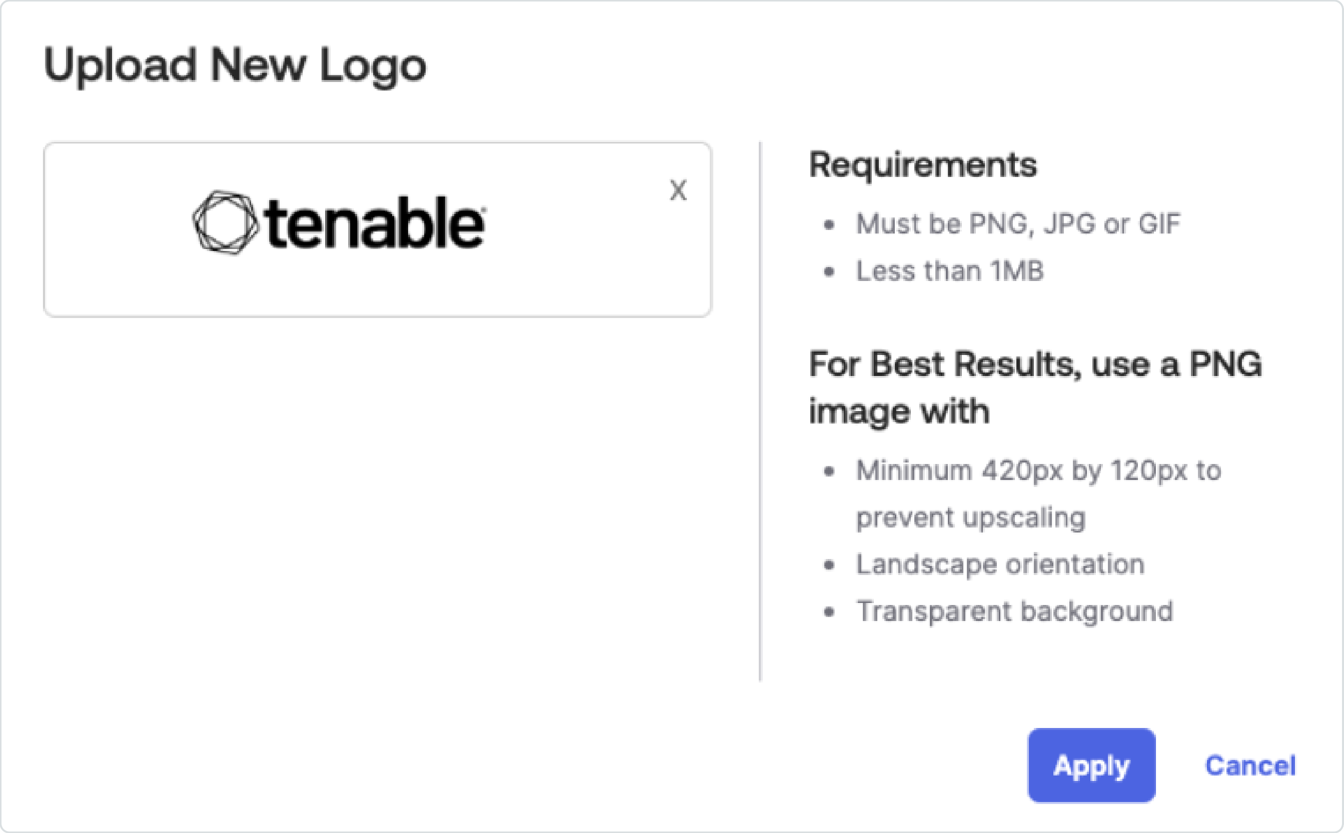
App name: Tenable One

App logo (optional)

App visibility: □ Do not display application icon to users

6. In the **App name** text box, type a name for your application.

7. (Optional) To add a custom logo for the application, in the **App logo** section, upload a .png, .jpeg, or .gif file and click **Apply**.



Upload New Logo

Requirements

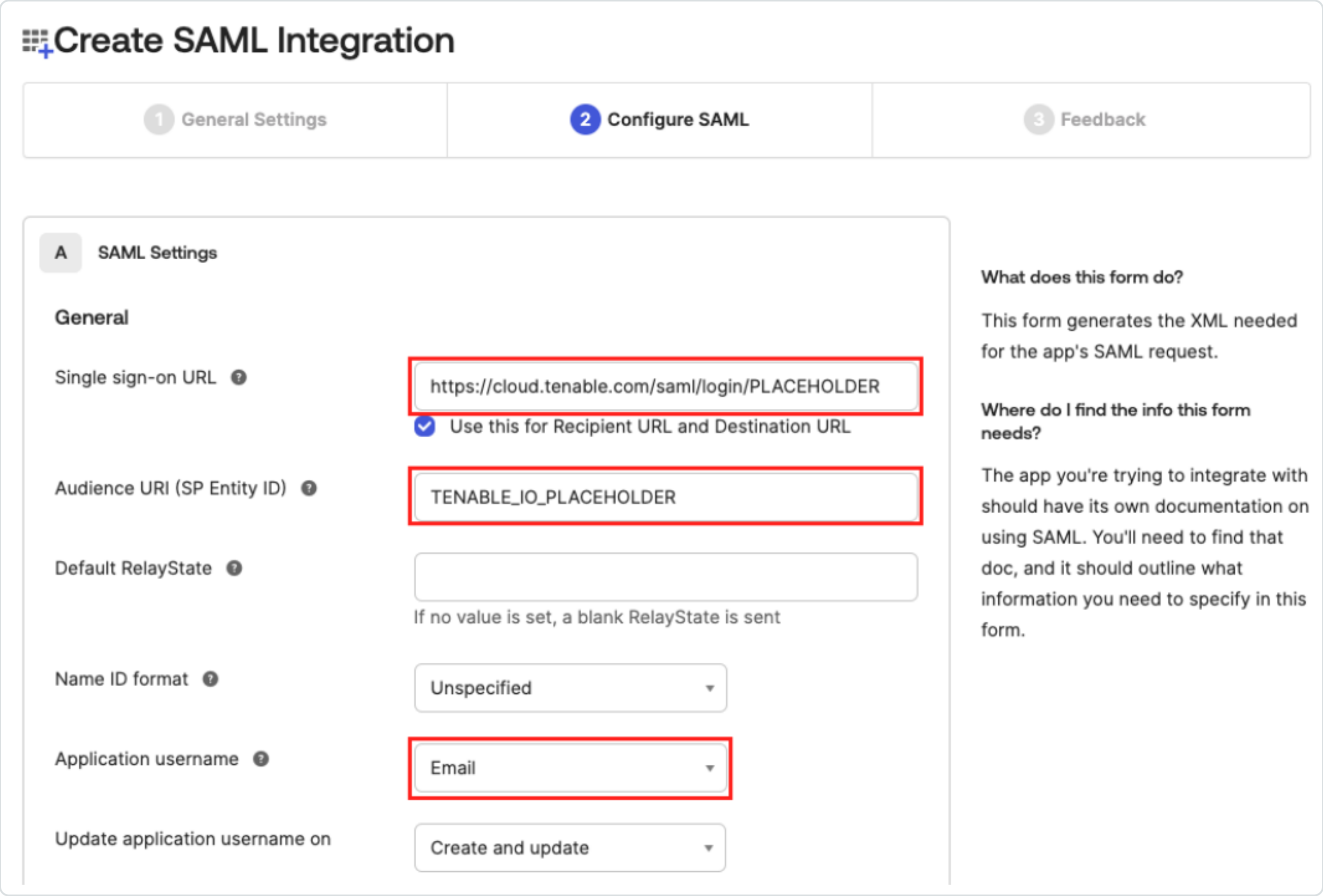
- Must be PNG, JPG or GIF
- Less than 1MB

For Best Results, use a PNG image with

- Minimum 420px by 120px to prevent upscaling
- Landscape orientation
- Transparent background

8. Click **Next**.

   The **Configure SAML** options appear.



Create SAML Integration

A SAML Settings

General

Single sign-on URL: https://cloud.tenable.com/saml/login/PLACEHOLDER

☑ Use this for Recipient URL and Destination URL

Audience URI (SP Entity ID): TENABLE_IO_PLACEHOLDER

Default RelayState:

If no value is set, a blank RelayState is sent

Name ID format: Unspecified

Application username: Email

Update application username on: Create and update

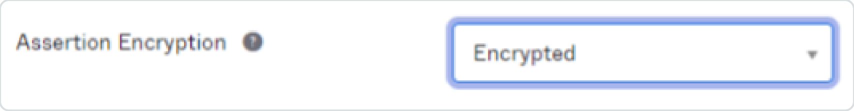
What does this form do?

This form generates the XML needed for the app's SAML request.

Where do I find the info this form needs?

The app you're trying to integrate with should have its own documentation on using SAML. You'll need to find that doc, and it should outline what information you need to specify in this form.

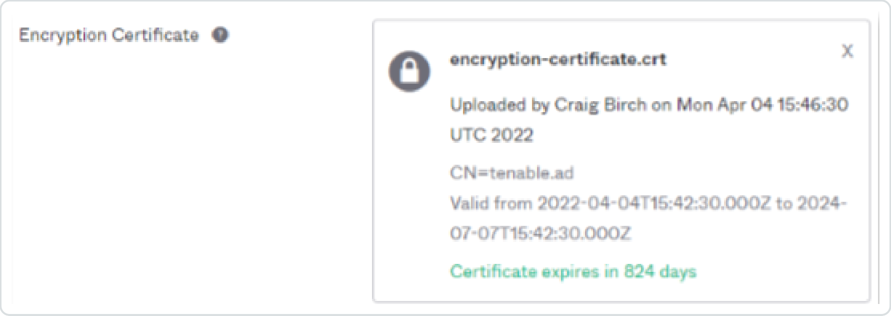
9. In the **Single sign-on URL** text box, paste the **URL of the Tenable.ad service provider** value you copied from Tenable Identity Exposure.
10. In the **Audience URI (SP Identity ID)** text box, paste the **Assert endpoint of the Tenable.ad service provider** value you copied from Tenable Identity Exposure.
11. Click **Show Advanced Settings**.
12. In the **Assertion Encryption** drop-down, select **Encrypted**.



Assertion Encryption: Encrypted

13. Click the **Encryption Certificate** field, and, in your browser, select the certificate you downloaded from Tenable Identity Exposure.

    Okta saves the certificate.



Encryption Certificate

encryption-certificate.crt

Uploaded by Craig Birch on Mon Apr 04 15:46:30 UTC 2022

CN=tenable.ad
Valid from 2022-04-04T15:42:30.000Z to 2024-07-07T15:42:30.000Z

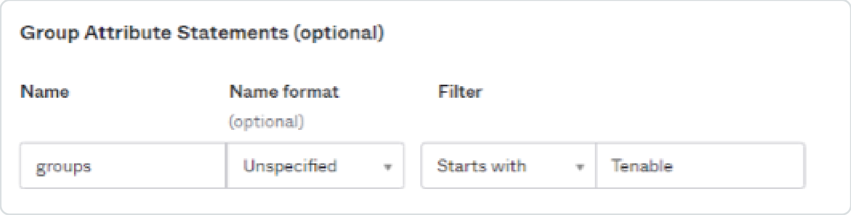
Certificate expires in 824 days

14. In the **Group Attribute Statements** section, insert the following values:

    a. In the **Name** text box, type **groups**.

    b. In the **Name format** drop-down, select **Unspecified**.

    c. In the **Filter** boxes, select **Starts with** and then type **Tenable**.



Group Attribute Statements (optional)

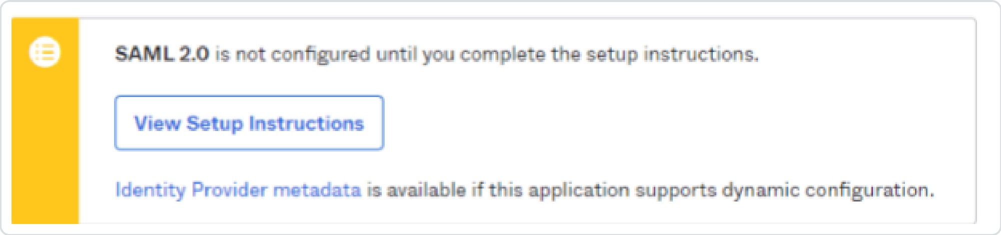
Name	Name format (optional)	Filter	
groups	Unspecified	Starts with	Tenable

15. Click **Next**.

16. Select **I'm an Okta customer and adding an internal app**.

17. Click **Finish**.

18. On the **Sign-On** tab, click the **View Setup Instructions** button.



SAML 2.0 is not configured until you complete the setup instructions.

Identity Provider metadata is available if this application supports dynamic configuration.

19. Save the following for use with Tenable Identity Exposure:

    - **IdP provider SSO URL**

      Tip: You'll later paste this as the **URL of the SAML server** within Tenable Identity Exposure.

- **X.509 certificate**

> **Tip:** You'll later paste the contents of this certificate in the **Trusted Certificate Authorities** section of Tenable Identity Exposure.

Create Okta Groups and Assign Users

To create groups and assign users:

1. In Okta, navigate to **Directory Groups** > **Add Group**.
2. Create the following groups for use with Tenable Identity Exposure:
   - Create a Tenable_users group. Add any users with Standard User Access to this group.
   - Create a Tenable_admins group. Add any Administrators to this group.

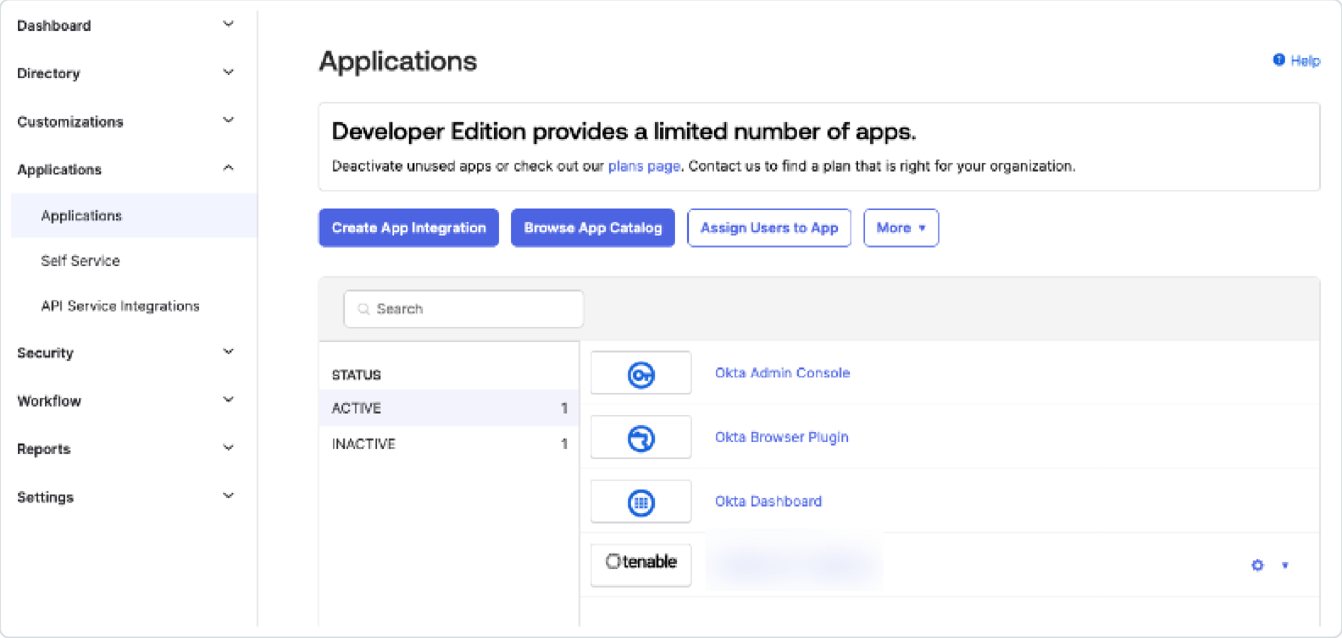
> **Tip:** You'll later paste these as the **SAML group name** within Tenable Identity Exposure.

You can now finish your SAML configuration within the Tenable Identity Exposure application.

Assign the Okta Application to your Users

To assign the application to your users or groups:

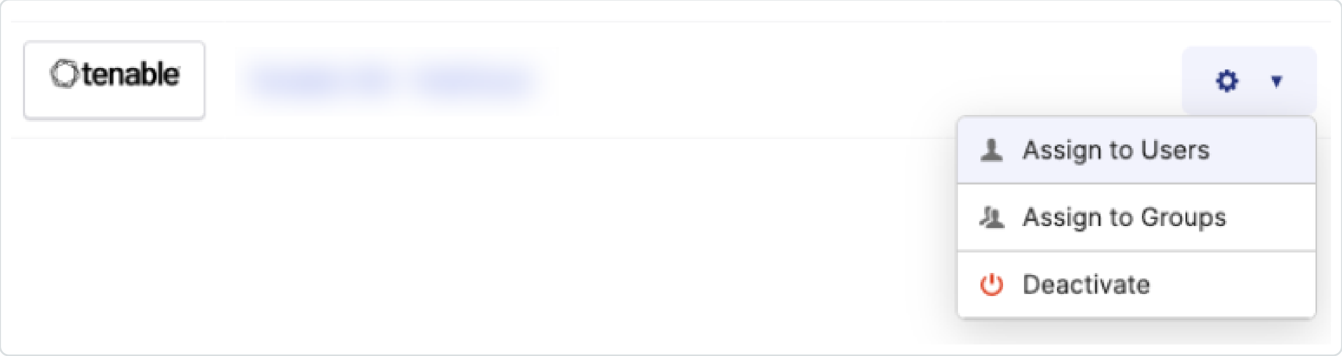
1. In the left navigation menu, click **Applications** > **Applications**.



Developer Edition provides a limited number of apps.

Deactivate unused apps or check out our plans page. Contact us to find a plan that is right for your organization.

2. Next to your newly created application configuration, click the ⚙ button.



3. Assign the application to one or more users or groups:

   - Click **Assign to Users**.
   - Click **Assign to Groups**.

   An **Assign** window appears.

4. Next to the user or group to which you want to assign the application, click **Assign**.

   A confirmation window appears.

5. Click **Save and Go Back**.

6. Repeat for each user or group to which you want to assign the application.

7. Click **Done**.

   Okta saves your changes, and you can now configure the final piece of the SAML configuration within Tenable Identity Exposure.

Finalize the Tenable Identity Exposure SAML Configuration

Once you've set up your application within your IdP, you can finalize your SAML configuration via the Tenable Identity Exposure interface.

To finalize the Tenable Identity Exposure SAML configuration:

1. In your browser, navigate to Tenable Identity Exposure.

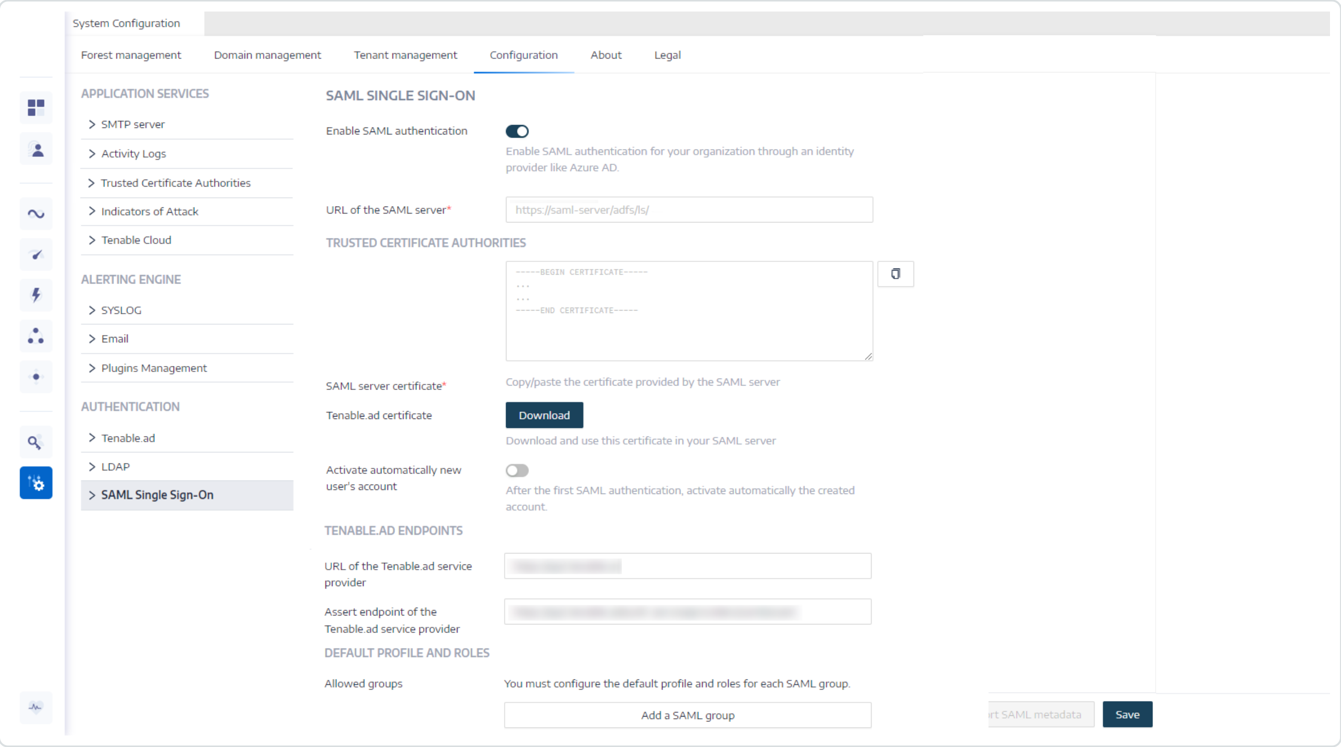
2. Navigate to **Systems** > **Configuration**.

   The configuration pane appears.

3. Under the **Authentication** section, click **SAML Single Sign-on**.

4. Click the **Enable SAML authentication** toggle.

   A SAML information form appears.



SAML SINGLE SIGN-ON

Enable SAML authentication

Enable SAML authentication for your organization through an identity provider like Azure AD.

URL of the SAML server* https://saml-server/adfs/ls/

TRUSTED CERTIFICATE AUTHORITIES

```
-----BEGIN CERTIFICATE-----
...
...
-----END CERTIFICATE-----
```

SAML server certificate* Copy/paste the certificate provided by the SAML server

Tenable.ad certificate

Download and use this certificate in your SAML server

Activate automatically new user's account

After the first SAML authentication, activate automatically the created account.

TENABLE.AD ENDPOINTS

URL of the Tenable.ad service provider

Assert endpoint of the Tenable.ad service provider

DEFAULT PROFILE AND ROLES

Allowed groups You must configure the default profile and roles for each SAML group.

5. In the **URL of the SAML server** box, paste the value you copied from your IdP. This value identifies the SAML server where Tenable Identity Exposure must connect.

6. In the **Trusted Certificate Authorities** box, paste certificate values that you copied from your IdP, beginning with `-----BEGIN CERTIFICATE -----` and ending with `-----END CERTIFICATE -----`.

7. Enable the **Activate automatically new user's account** toggle.

8. In the **Default Profiles and Roles** section, configure at least one **Allowed Group**. This group name should match the name and description of the group you created in your IdP.

   - **A group for your administrators that matches the group you created in your IdP:**

     a. In the **SAML group name** text box, type the name of the group you created in your IdP.

     b. In the **Default profile** text box, select the default profile you want to use for the group.

c. In the **Default roles** box, select the default role you want to use for the group. For example, if the group is for Administrator use only, select **Global Administrator**.

9. Click **Save**.

   Tenable Identity Exposure saves your changes, and your SAML configuration is ready for use.

Additional Resources

For more information on Okta IdP configuration, see the following resources:

- Okta Developer Portal
- Create SAML App Integrations
- Build a Single Sign-On Integration
- Create a SAML Integration in Okta

Tenable Identity Exposure: Microsoft Entra ID IdP

One of the most common IdPs used to configure SAML with Tenable Identity Exposure is Microsoft Entra ID. The following steps guide you through the configuration process from start to finish.

Manual configuration requires the following:

- **URL of the SAML server**: A value that corresponds to the **Login URL** within Microsoft Entra ID.
- **Assert endpoint of the Tenable.ad service provider**: A value that corresponds to the **Reply URL** within Microsoft Entra ID.
- **Trusted Certificate Authorities**: The SAML server certificate in PEM-encoded format, beginning with `-----BEGIN CERTIFICATE -----` and ending with `-----END CERTIFICATE -----`, provided by Microsoft Entra ID in the **Certificate (Base 64)** section.

Enable Tenable Identity Exposure SAML

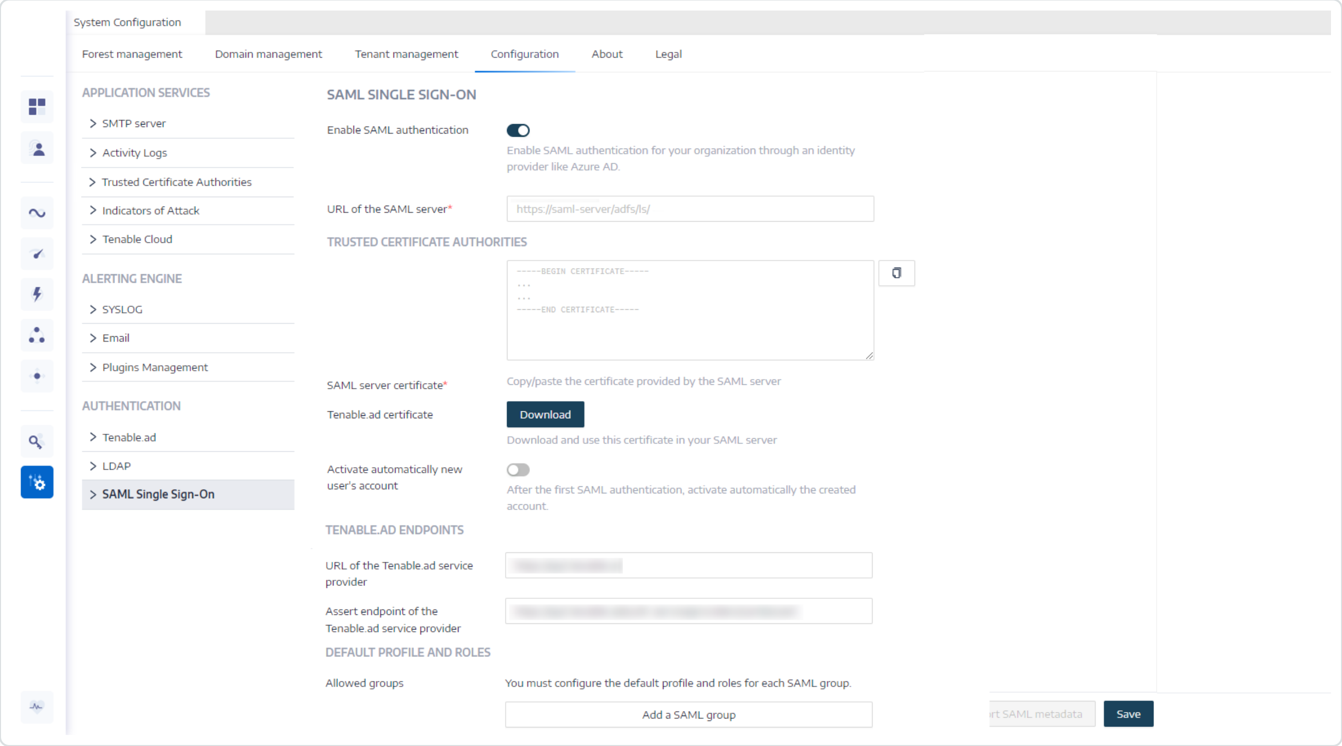
The first step in configuring SAML for use with Tenable Identity Exposure is to enable the configuration in the Tenable Identity Exposure application. Then, you can download your certificate file to use in your IdP.

To enable the Tenable Identity Exposure SAML configuration:

1. In your browser, navigate to Tenable Identity Exposure.
2. Navigate to **Systems** > **Configuration**.

   The configuration pane appears.
3. Under the **Authentication** section, click **SAML Single Sign-on**.
4. Click the **Enable SAML authentication** toggle.

   A SAML information form appears.



SAML SINGLE SIGN-ON

Enable SAML authentication ●

Enable SAML authentication for your organization through an identity provider like Azure AD.

URL of the SAML server* https://saml-server/adfs/ls/

TRUSTED CERTIFICATE AUTHORITIES

```
-----BEGIN CERTIFICATE-----
...
...
-----END CERTIFICATE-----
```

SAML server certificate* Copy/paste the certificate provided by the SAML server

Tenable.ad certificate Download

Download and use this certificate in your SAML server

Activate automatically new user's account ○

After the first SAML authentication, activate automatically the created account.

TENABLE.AD ENDPOINTS

URL of the Tenable.ad service provider [redacted]

Assert endpoint of the Tenable.ad service provider [redacted]

DEFAULT PROFILE AND ROLES

Allowed groups You must configure the default profile and roles for each SAML group.

Add a SAML group

5. In the **Tenable.ad Certificate** section, click **Download**.

   Your browser downloads the certificate needed to connect with your IdP.
6. In the **Tenable.ad Endpoints** section, copy the following values for use within your IdP:
   - **URL of the Tenable.ad service provider**
   - **Assert endpoint of the Tenable.ad service provider**

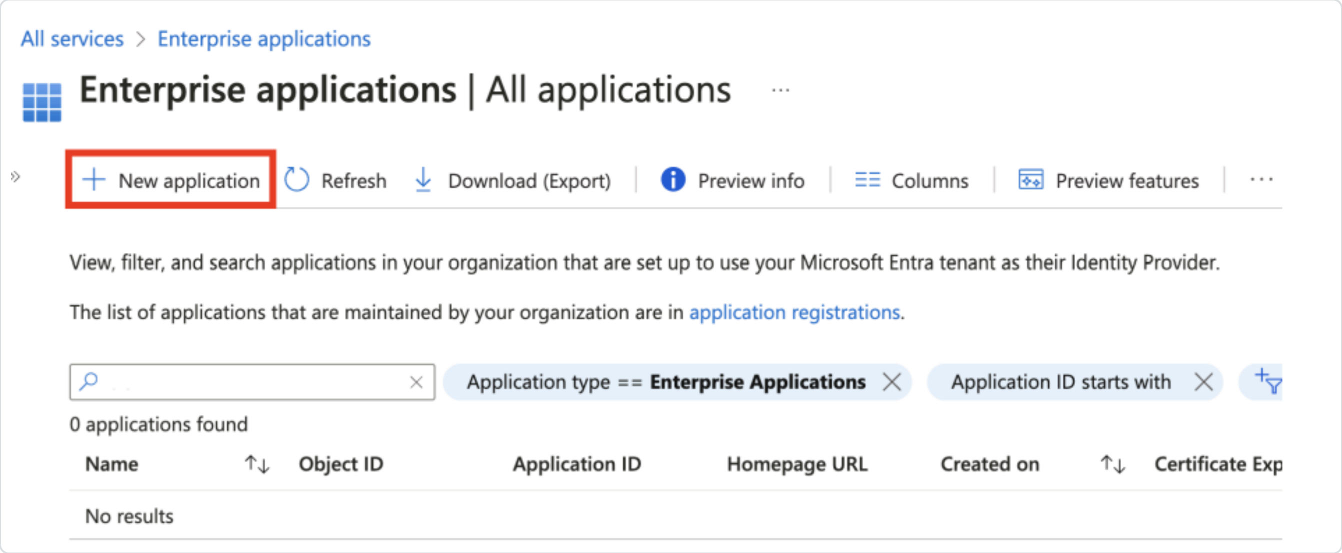
You can now use the downloaded certificate and copied values to set up the connection with your IdP.

Microsoft Entra ID: Create Application and Upload Certificate

Now that you have enabled the Tenable Identity Exposure SAML configuration, you can create a Tenable application in Microsoft Entra ID.

1. In your browser, navigate to the Azure Admin portal.
2. In the navigation menu, navigate to **All services** > **Enterprise Applications**.

   The application gallery appears.

   All services > Enterprise applications

   Enterprise applications | All applications

   View, filter, and search applications in your organization that are set up to use your Microsoft Entra tenant as their Identity Provider.

   The list of applications that are maintained by your organization are in application registrations.

   Application type == **Enterprise Applications**

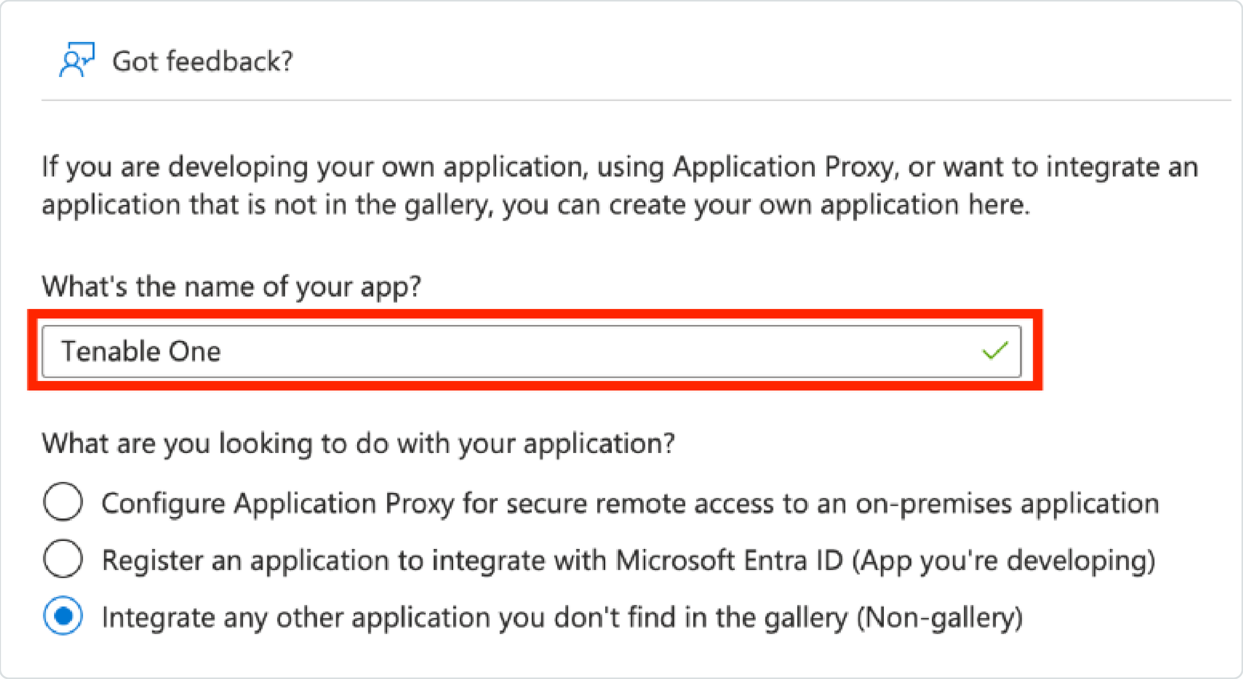
   Application ID starts with

   0 applications found

Name	Object ID	Application ID	Homepage URL	Created on	Certificate Exp
No results					

3. Click **Create your own application**.

   The **Create your own application** window appears.



Got feedback?

If you are developing your own application, using Application Proxy, or want to integrate an application that is not in the gallery, you can create your own application here.

What's the name of your app?

Tenable One ✓

What are you looking to do with your application?

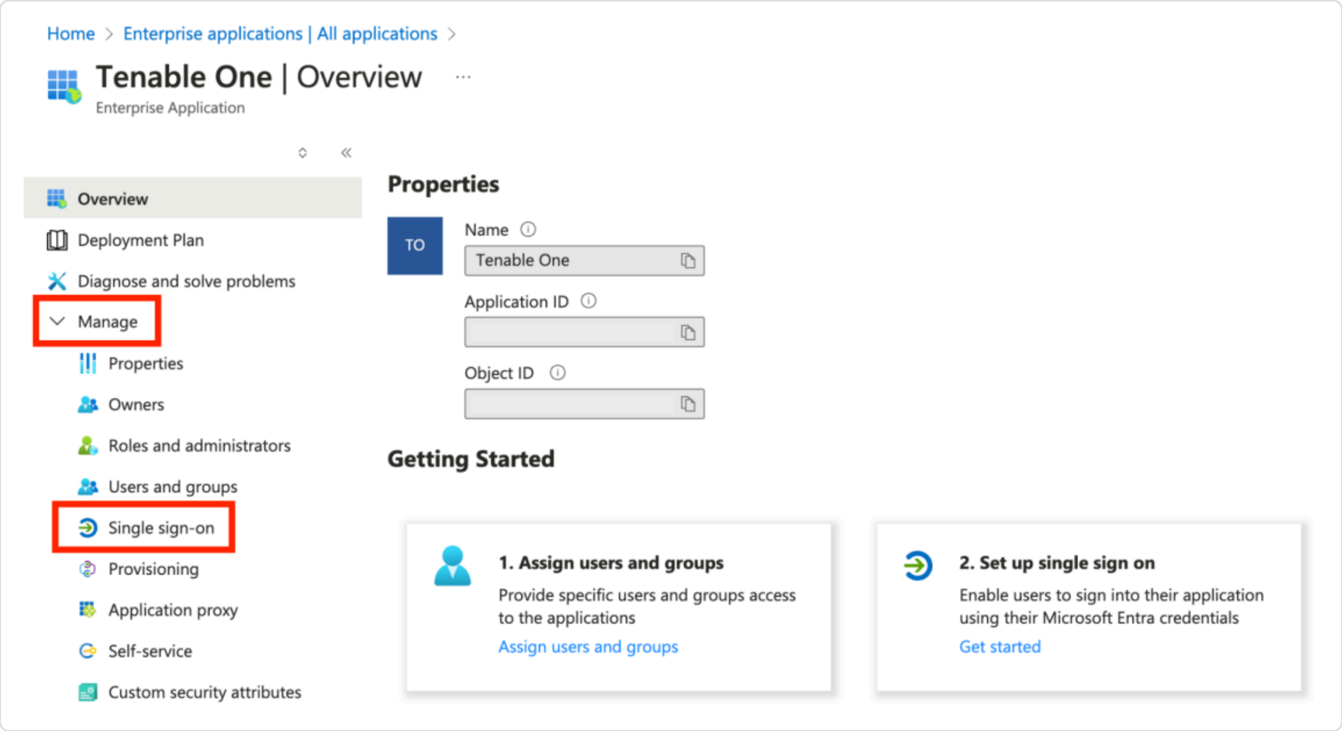
○ Configure Application Proxy for secure remote access to an on-premises application

○ Register an application to integrate with Microsoft Entra ID (App you're developing)

● Integrate any other application you don't find in the gallery (Non-gallery)

4. In the **What's the name of your app?** text box, type a name for your application.
5. In the **What are you looking to do with your application** section, select the **Integrate any other application you don't find in the gallery** radio button.
6. Click **Create**.

   Microsoft Entra ID redirects you to the application overview page.
7. In the **Getting Started** section, click the **Set up single sign on** tile.



Properties

Name: Tenable One

Application ID:

Object ID:

Getting Started

1. Assign users and groups

Provide specific users and groups access to the applications

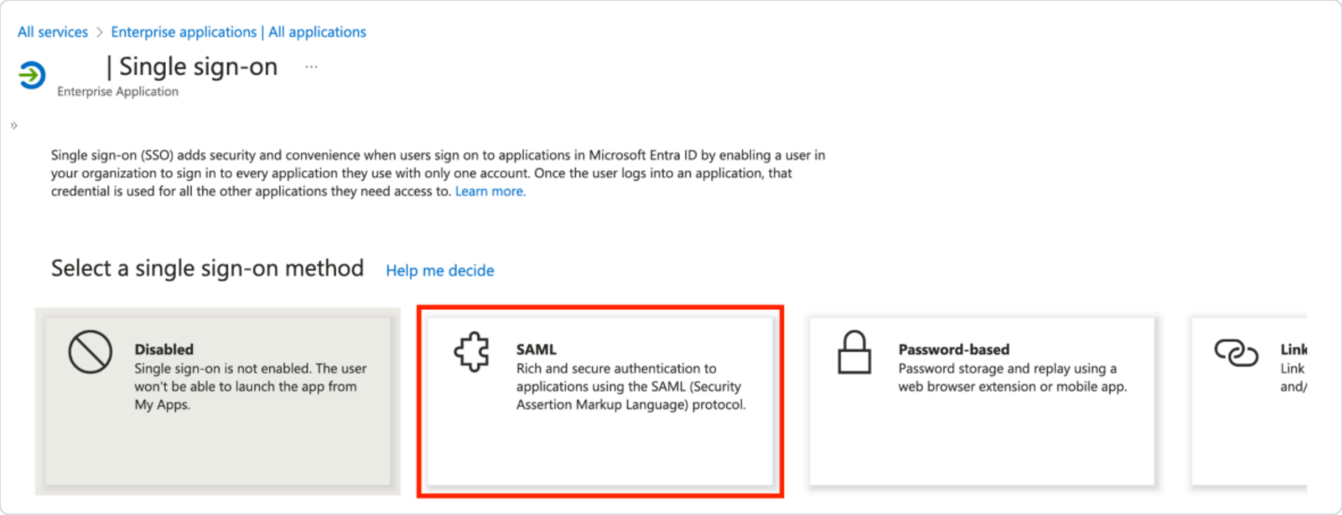
Assign users and groups

2. Set up single sign on

Enable users to sign into their application using their Microsoft Entra credentials

Get started

The **Single Sign-on** options appear.



Single sign-on (SSO) adds security and convenience when users sign on to applications in Microsoft Entra ID by enabling a user in your organization to sign in to every application they use with only one account. Once the user logs into an application, that credential is used for all the other applications they need access to. Learn more.

Select a single sign-on method Help me decide

Disabled
Single sign-on is not enabled. The user won't be able to launch the app from My Apps.

SAML
Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.

Password-based
Password storage and replay using a web browser extension or mobile app.

Link
Link and/

8. Click the **SAML** tile.

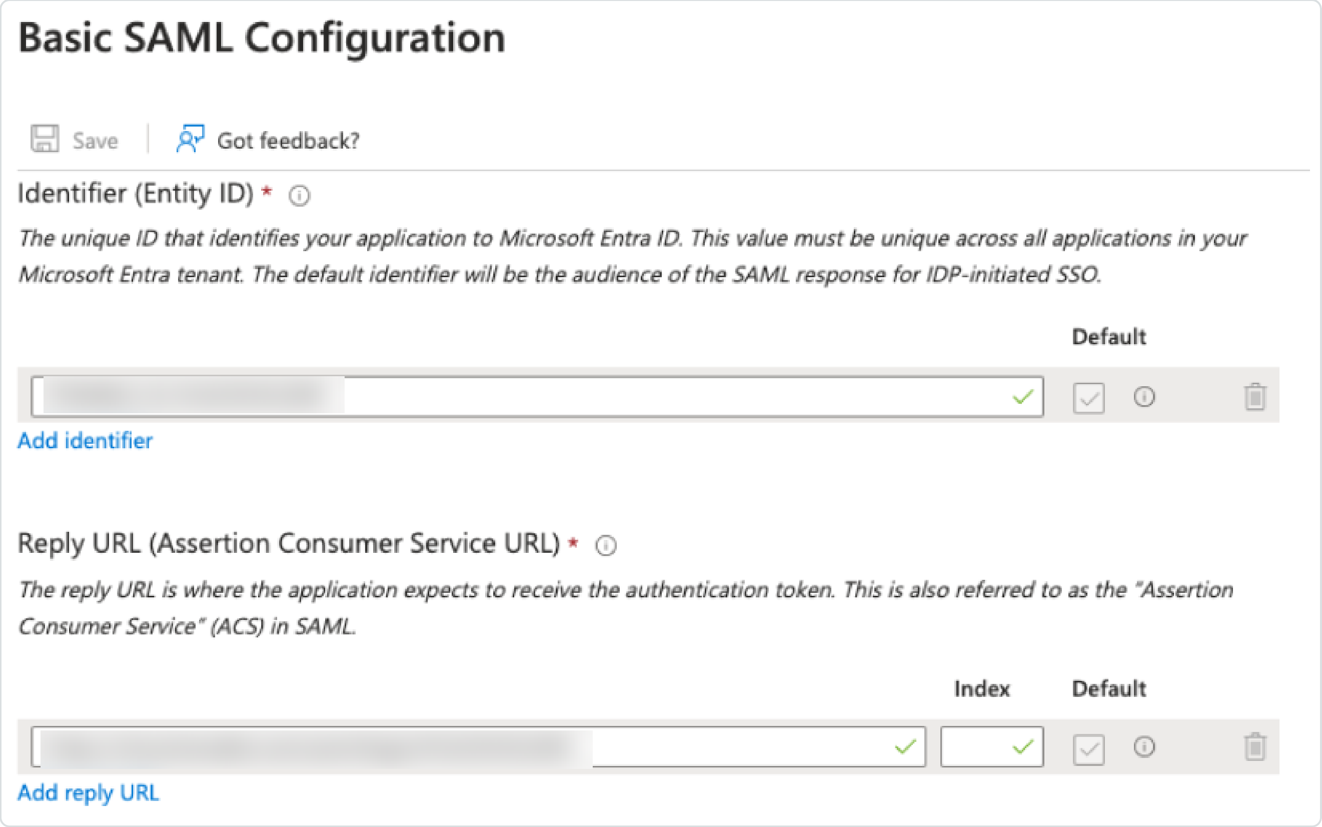
   The **SAML-based Sign-on** page appears.

9. On the **Basic SAML Configuration** tile, click the ••• button.

   Action items appear.

10. Click **Edit**.

    The **Basic SAML Configuration** page appears.



Basic SAML Configuration

Identifier (Entity ID) *

The unique ID that identifies your application to Microsoft Entra ID. This value must be unique across all applications in your Microsoft Entra tenant. The default identifier will be the audience of the SAML response for IDP-initiated SSO.

Reply URL (Assertion Consumer Service URL) *

The reply URL is where the application expects to receive the authentication token. This is also referred to as the "Assertion Consumer Service" (ACS) in SAML.

11. In the **Identifier (Entity ID)** text box, paste the **URL of the Tenable.ad service provider** value you copied from Tenable Identity Exposure.

12. In the **Reply URL** text box, paste the **Assert endpoint of the Tenable.ad service provider** value you copied from Tenable Identity Exposure.

13. On the **User Attributes & Claims** tile, click the ••• button.

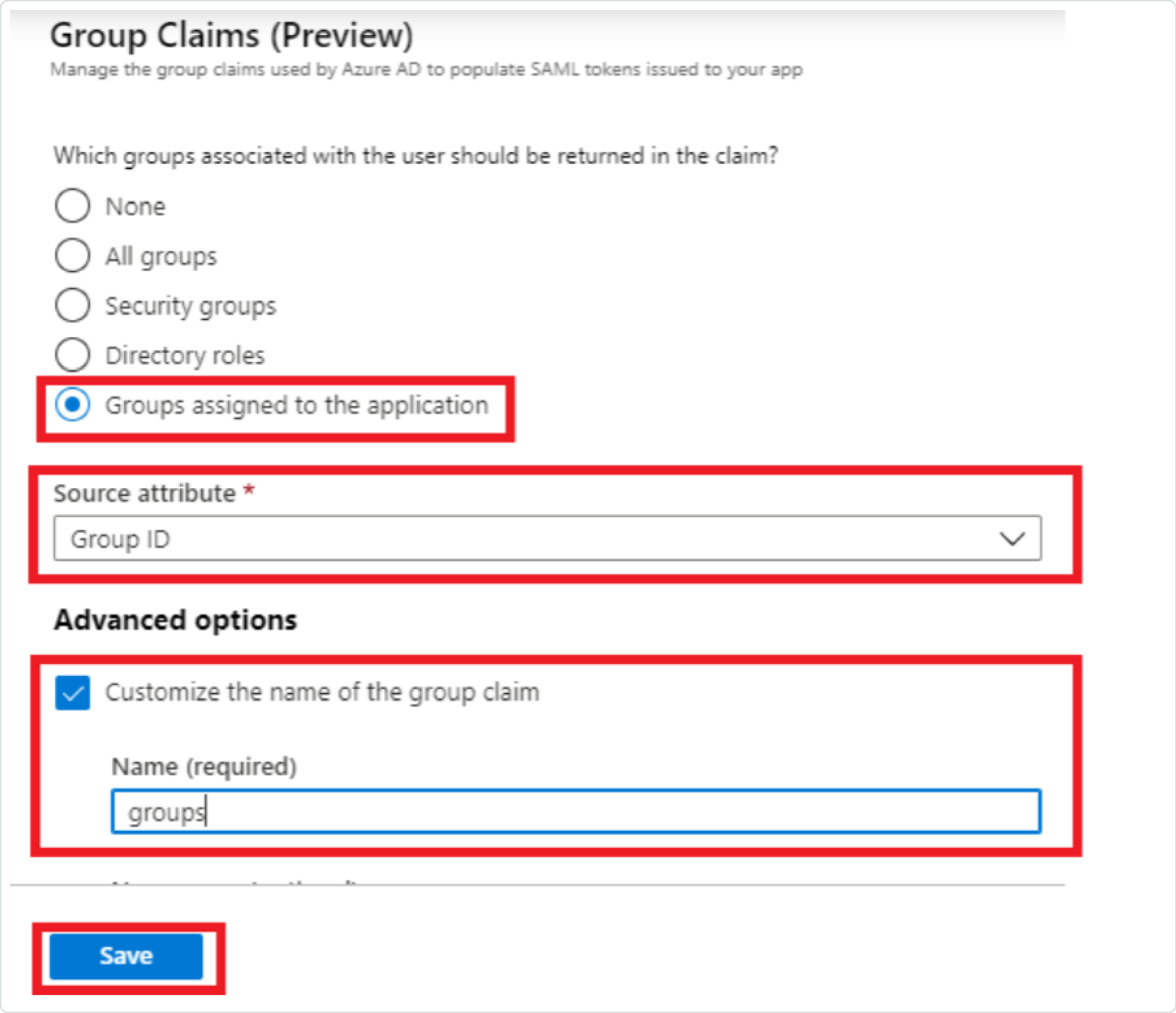
    Action options appear.

14. Click **Edit**.

    The **User Attributes & Claims** page appears.

15. Click **Add a group claim**.

    The **Group Claim** preview appears.



Group Claims (Preview)

Manage the group claims used by Azure AD to populate SAML tokens issued to your app

Which groups associated with the user should be returned in the claim?

○ None

○ All groups

○ Security groups

○ Directory roles

● Groups assigned to the application

Source attribute *

Group ID

Advanced options

☑ Customize the name of the group claim

Name (required)

groups

16. Select the **Groups assigned to the application** radio button.

17. In the **Source Attribute** drop-down, select **Group ID**.

18. Select the **Customize the name of the group claim** checkbox.

19. In the **Name** text box, type **groups**.

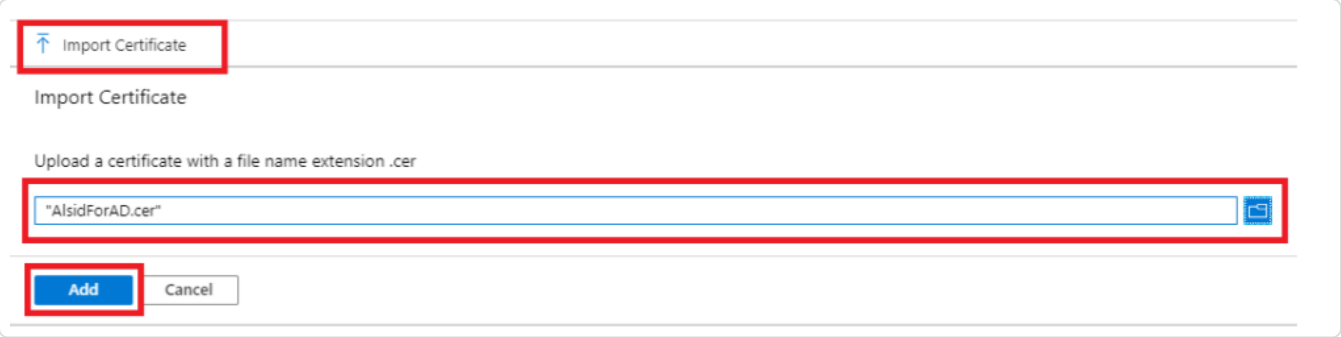
20. Click **Save**.

    You return to the **SAML-based Sign-on** page.

21. In the left navigation menu, click **Token Encryption**.

Encryption options appear.

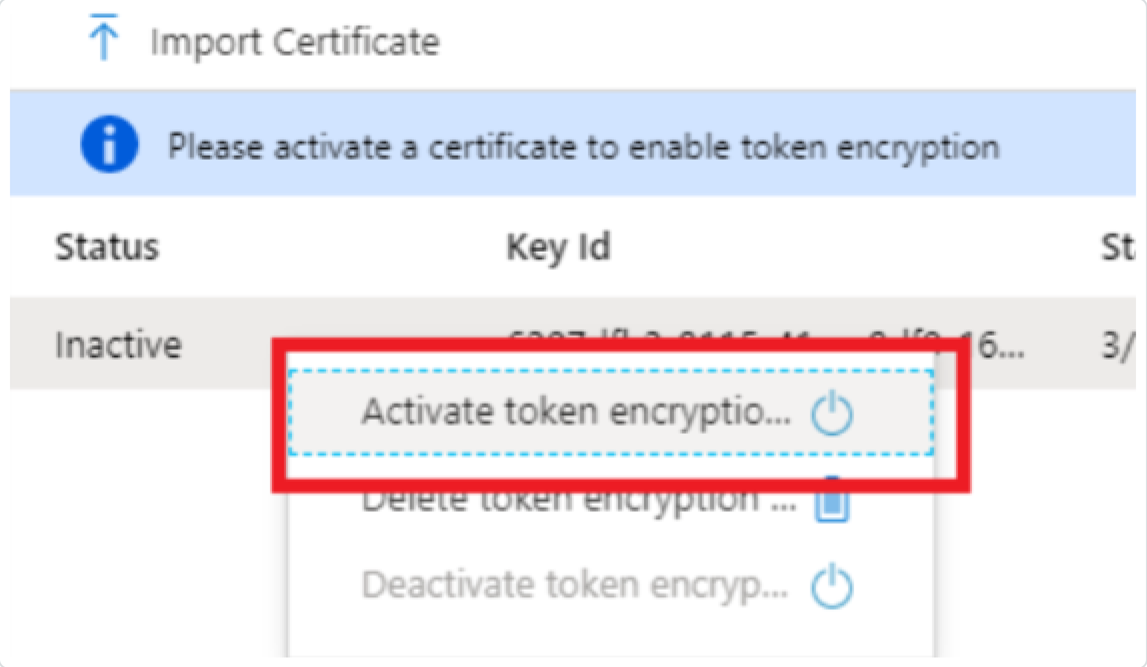
22. Click **Import Certificate**.



23. In your file manager, select the certificate you downloaded from Tenable Identity Exposure.

24. Click **Add**.

25. Right-click the newly uploaded certificate and click **Activate Token Encryption**.



Import Certificate
Please activate a certificate to enable token encryption
Status
Key Id
St
Inactive
6...
3/
Activate token encryptio...
Delete token encryption ...
Deactivate token encryp...

Create Microsoft Entra ID Groups and Assign Users

To create groups and assign users:

1. In Microsoft Entra ID, in the left navigation menu, click **Users and Groups**.

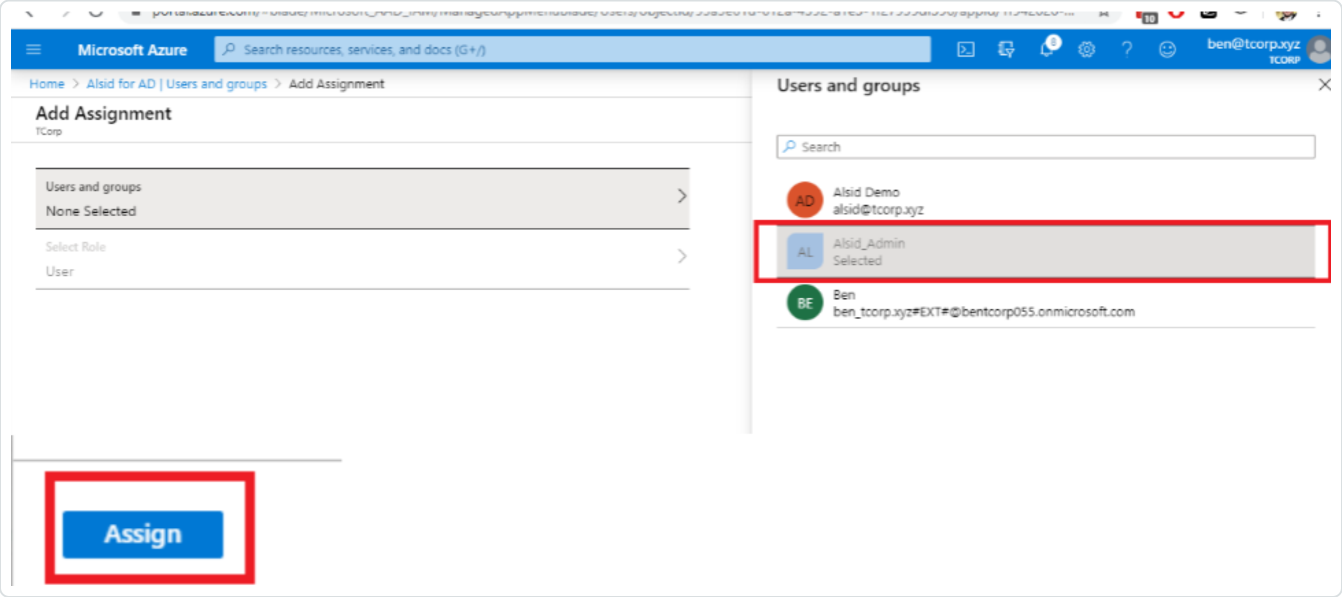
   The **Users and Groups** page appears.

2. Click **Add User**.

   The **Add Assignment** page appears.

3. Click the Users and Groups section.

4. In the selection plane, select the users and/or groups you want to assign to the group for use with Tenable Identity Exposure.

   Users and groups: None Selected

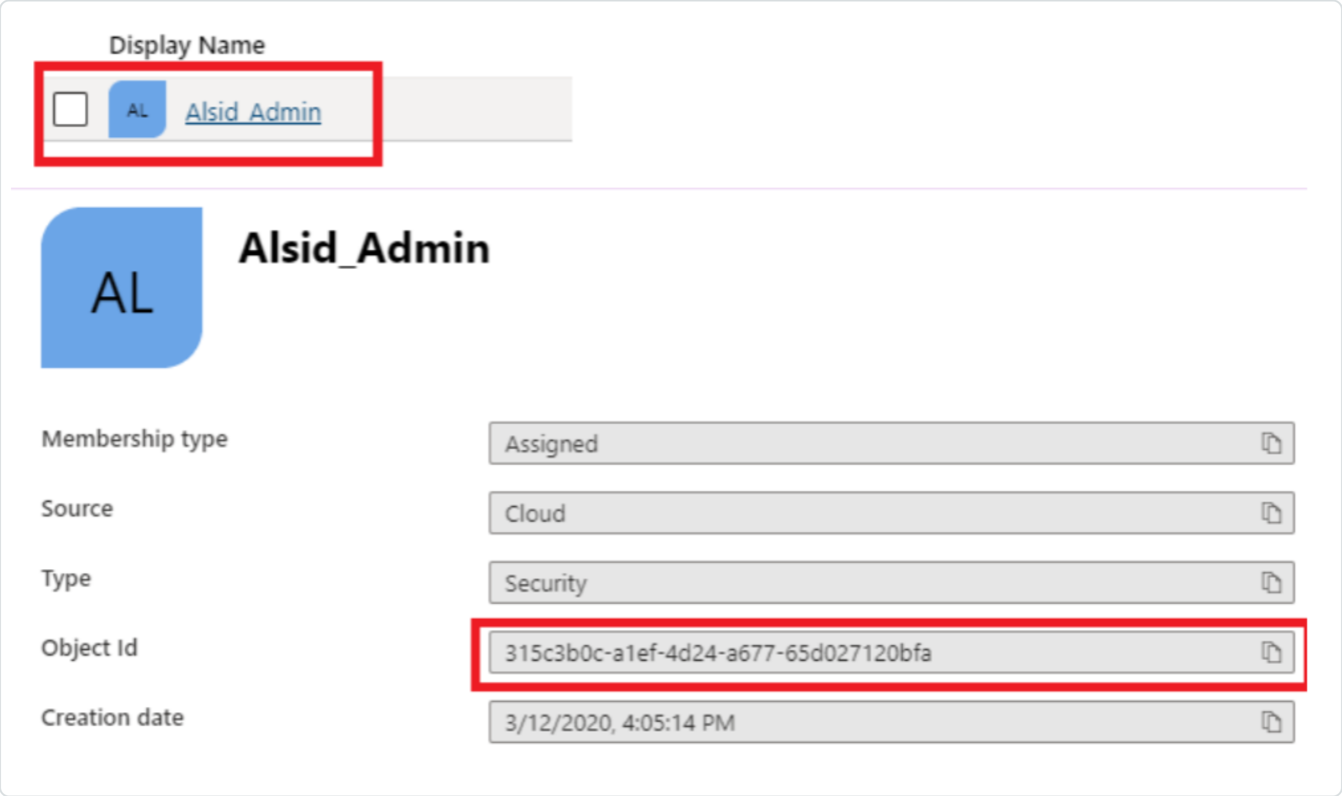
   Select Role: User

   AD Alsid Demo alsid@tcorp.xyz

   AL Alsid_Admin Selected

   BE Ben ben_tcorp.xyz#EXT#@bentcorp055.onmicrosoft.com

5. For each user or group you add, click the name and copy the **Object ID** for later use within Tenable Identity Exposure.



□ AL Alsid_Admin

Alsid_Admin

AL

Membership type: Assigned

Source: Cloud

Type: Security

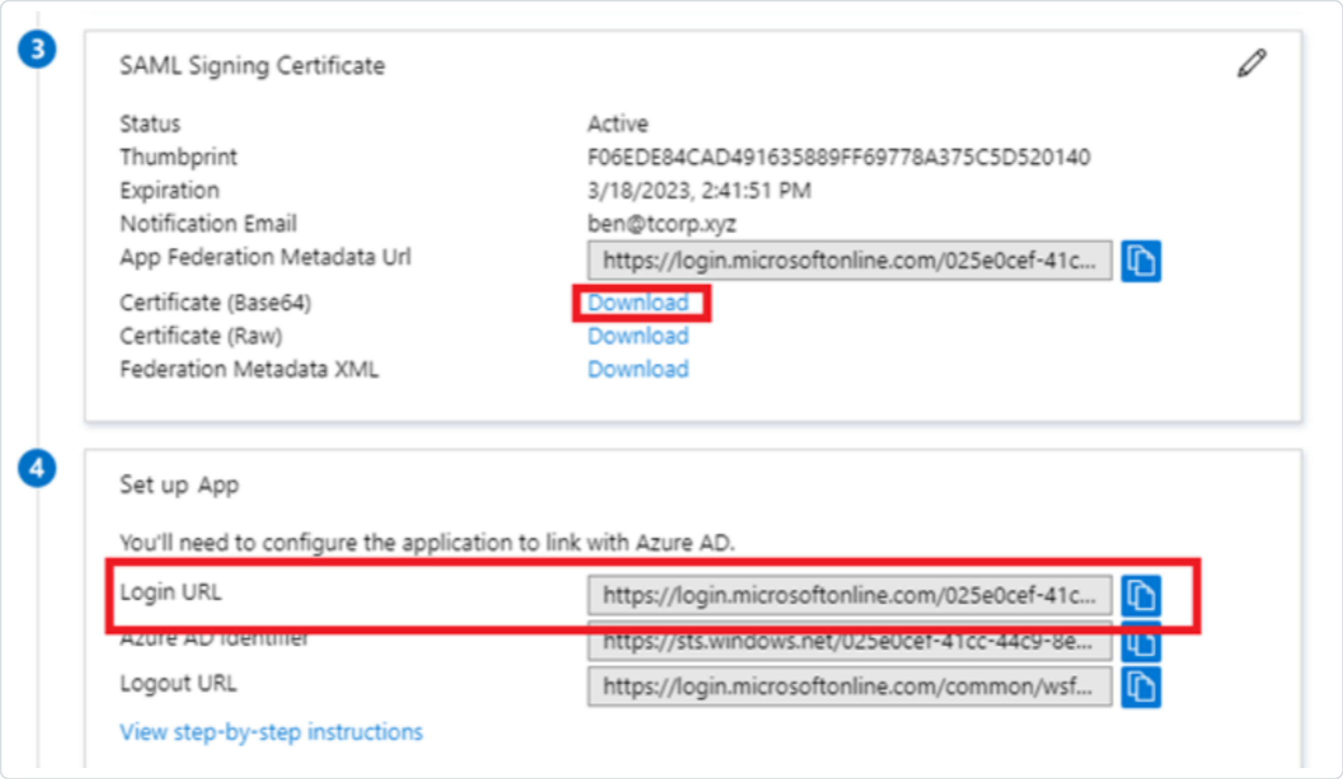
Object Id: 315c3b0c-a1ef-4d24-a677-65d027120bfa

Creation date: 3/12/2020, 4:05:14 PM

Tip: You'll later paste this as the **SAML group name** within Tenable Identity Exposure.

6. Navigate back to the **SAML-based Sign-on** page.

7. On the **SAML Certificates** tile, in the **Certificate (Base 64)** section, click **Download**.



3 SAML Signing Certificate

Status	Active
Thumbprint	F06EDE84CAD491635889FF69778A375C5D520140
Expiration	3/18/2023, 2:41:51 PM
Notification Email	ben@tcorp.xyz
App Federation Metadata Url	https://login.microsoftonline.com/025e0cef-41c...
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

4 Set up App

You'll need to configure the application to link with Azure AD.

Login URL	https://login.microsoftonline.com/025e0cef-41c...
Azure AD Identifier	https://sts.windows.net/025e0cef-41cc-44c9-8e...
Logout URL	https://login.microsoftonline.com/common/wsf...

View step-by-step instructions

Your browser downloads the certificate.

> **Tip:** You'll later paste the contents of this certificate in the **Trusted Certificate Authorities** section of Tenable Identity Exposure.

8. In the **Set up App** section, copy the **Login URL** for later use within Tenable Identity Exposure.

> **Tip:** You'll later paste this as the **URL of the SAML server** within Tenable Identity Exposure.

You can now finish your SAML configuration within the Tenable Identity Exposure application.

Finalize the Tenable Identity Exposure SAML Configuration

Once you've set up your application within your IdP, you can finalize your SAML configuration via the Tenable Identity Exposure interface.

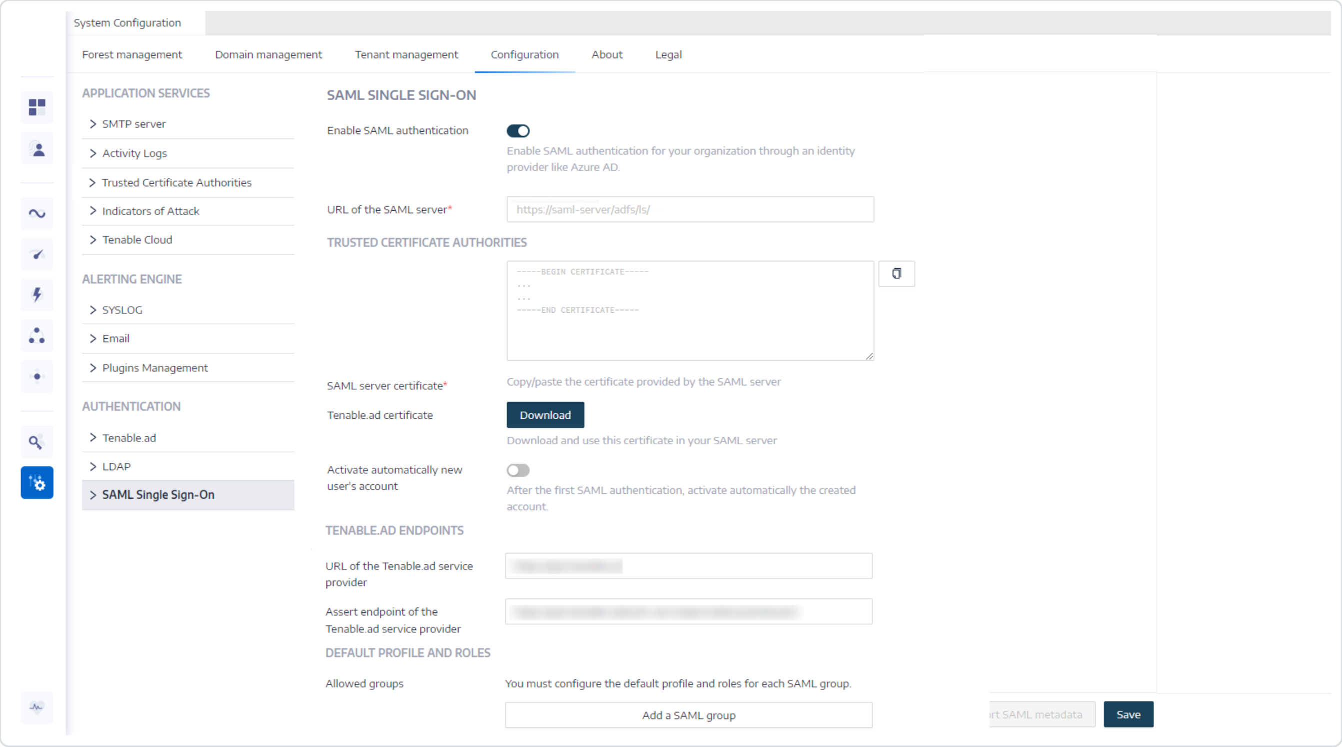
To finalize the Tenable Identity Exposure SAML configuration:

1. In your browser, navigate to Tenable Identity Exposure.
2. Navigate to **Systems** > **Configuration**.

The configuration pane appears.

3. Under the **Authentication** section, click **SAML Single Sign-on**.
4. Click the **Enable SAML authentication** toggle.

   A SAML information form appears.



System Configuration

Forest management | Domain management | Tenant management | Configuration | About | Legal

APPLICATION SERVICES
- SMTP server
- Activity Logs
- Trusted Certificate Authorities
- Indicators of Attack
- Tenable Cloud

ALERTING ENGINE
- SYSLOG
- Email
- Plugins Management

AUTHENTICATION
- Tenable.ad
- LDAP
- SAML Single Sign-On

SAML SINGLE SIGN-ON

Enable SAML authentication ●
Enable SAML authentication for your organization through an identity provider like Azure AD.

URL of the SAML server* https://saml-server/adfs/ls/

TRUSTED CERTIFICATE AUTHORITIES

```
-----BEGIN CERTIFICATE-----
...
...
-----END CERTIFICATE-----
```

SAML server certificate* Copy/paste the certificate provided by the SAML server

Tenable.ad certificate Download
Download and use this certificate in your SAML server

Activate automatically new user's account ○
After the first SAML authentication, activate automatically the created account.

TENABLE.AD ENDPOINTS

URL of the Tenable.ad service provider [redacted]

Assert endpoint of the Tenable.ad service provider [redacted]

DEFAULT PROFILE AND ROLES

Allowed groups You must configure the default profile and roles for each SAML group.

Add a SAML group

rt SAML metadata | Save

5. In the **URL of the SAML server** box, paste the value you copied from your IdP. This value identifies the SAML server where Tenable Identity Exposure must connect.
6. In the **Trusted Certificate Authorities** box, paste certificate values that you copied from your IdP, beginning with `-----BEGIN CERTIFICATE -----` and ending with `-----END CERTIFICATE -----`.
7. Enable the **Activate automatically new user's account** toggle.
8. In the **Default Profiles and Roles** section, configure at least one **Allowed Group**. This group name should match the name and description of the group you created in your IdP.

- **A group for your administrators that matches the group you created in your IdP:**

   a. In the **SAML group name** text box, type the name of the group you created in your IdP.

   b. In the **Default profile** text box, select the default profile you want to use for the group.

   c. In the **Default roles** box, select the default role you want to use for the group. For example, if the group is for Administrator use only, select **Global Administrator**.

9. Click **Save**.

   Tenable Identity Exposure saves your changes, and your SAML configuration is ready for use.

Additional Resources

For more information on Microsoft Entra ID IdP configuration, see the following resources:

- Microsoft Entra ID Developer Portal
- SAML Authentication with Microsoft Entra ID
- Use a SAML 2.0 IdP for Single Sign On

SAML for Tenable Security Center

You can configure Tenable Security Center to accept credentials from your SAML identity provider. This allows for an additional layer of security, where the SAML credentials are certified for use within Tenable Security Center. Once you enable SAML for a user, they can log in to Tenable Security Center directly through their identity provider, which automatically signs them in and redirects them to the Tenable Security Center landing page.

While several configuration steps occur directly in the Tenable user interface, the entire SAML configuration process includes several processes across multiple applications. This guide describes three of the most commonly used Identity Providers (IdPs) and how to configure them for use with Tenable Security Center SAML from start to finish.

Considerations for Advanced SAML Features

Because Tenable Security Center cannot accept private keys to decrypt SAML assertions, Tenable Security Center does not support SAML assertion encryption. If you want to configure SAML authentication in Tenable Security Center, choose an identity provider that does not require assertion encryption and confirm that assertion encryption is not enabled.

For information about Tenable Security Center communications encryption, see Encryption Strength.

> **Note:** Tenable Support does not assist with configuring or troubleshooting advanced SAML features.

To get started, see the following topics:

- Tenable Security Center: Okta IdP
- Tenable Security Center: Microsoft Entra ID IdP
- Tenable Security Center: Microsoft ADFS IdP
- Troubleshooting and Common Errors

Tenable Security Center: Okta IdP

One of the most common IdPs used to configure SAML with Tenable Security Center is Okta. The following steps guide you through the configuration process from start to finish.

Manual configuration requires the following:

- Login URL: A custom URL in the following format:

  ```
  https://PLACEHOLDER/saml/module.php/saml/sp/saml2-acs.php/1
  ```

  Where *PLACEHOLDER* is the IP address or hostname for your Tenable Security Center instance.

- Audience URI (SP Entity ID): A custom ID in the following format:

  ```
  https://tenable.sc
  ```

> **Note:** This value must be in URL format.

- A certificate within the SAML metadata object that matches the data originally sent to Tenable.

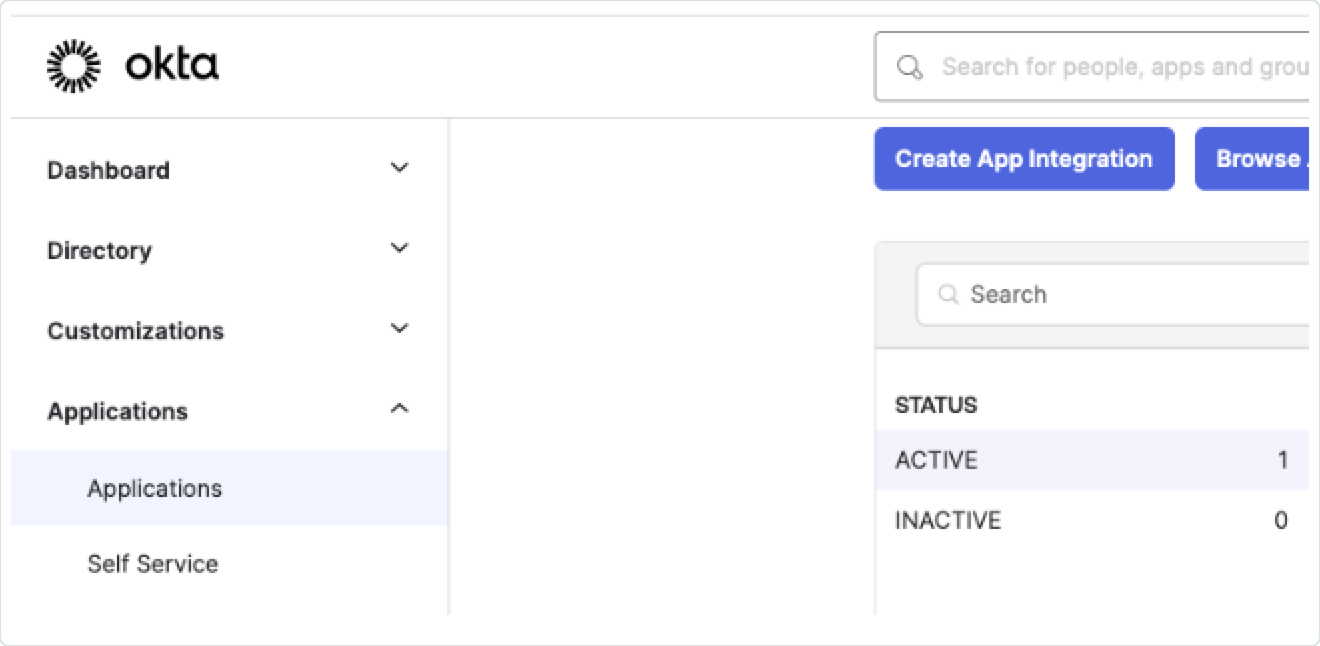
> **Note:** Tenable does not support the use of multiple certificates and only extracts the first certificate from the metadata object. If the object includes multiple certificates, you must specify which certificate to use if it is not the first one listed.

Okta: Create Initial Application Integration

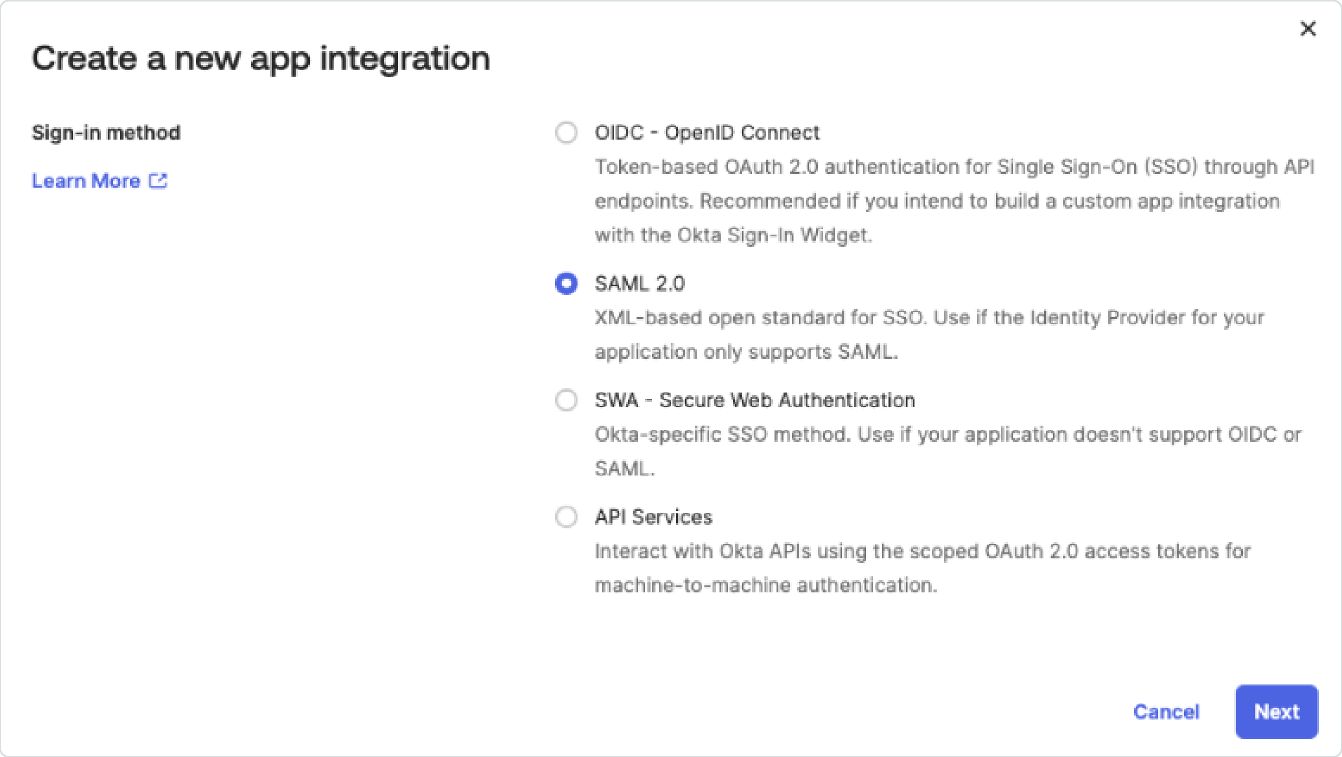
To create an application integration in Okta:

1. In your browser, navigate to the Okta Admin portal.
2. In the left navigation menu, click **Applications** > **Applications**.
3. Click **Create App Integration**.

   The **Create a new app integration** window appears.



4. Select the **SAML 2.0** radio button.



Create a new app integration

Sign-in method

Learn More

○ OIDC - OpenID Connect
Token-based OAuth 2.0 authentication for Single Sign-On (SSO) through API endpoints. Recommended if you intend to build a custom app integration with the Okta Sign-In Widget.

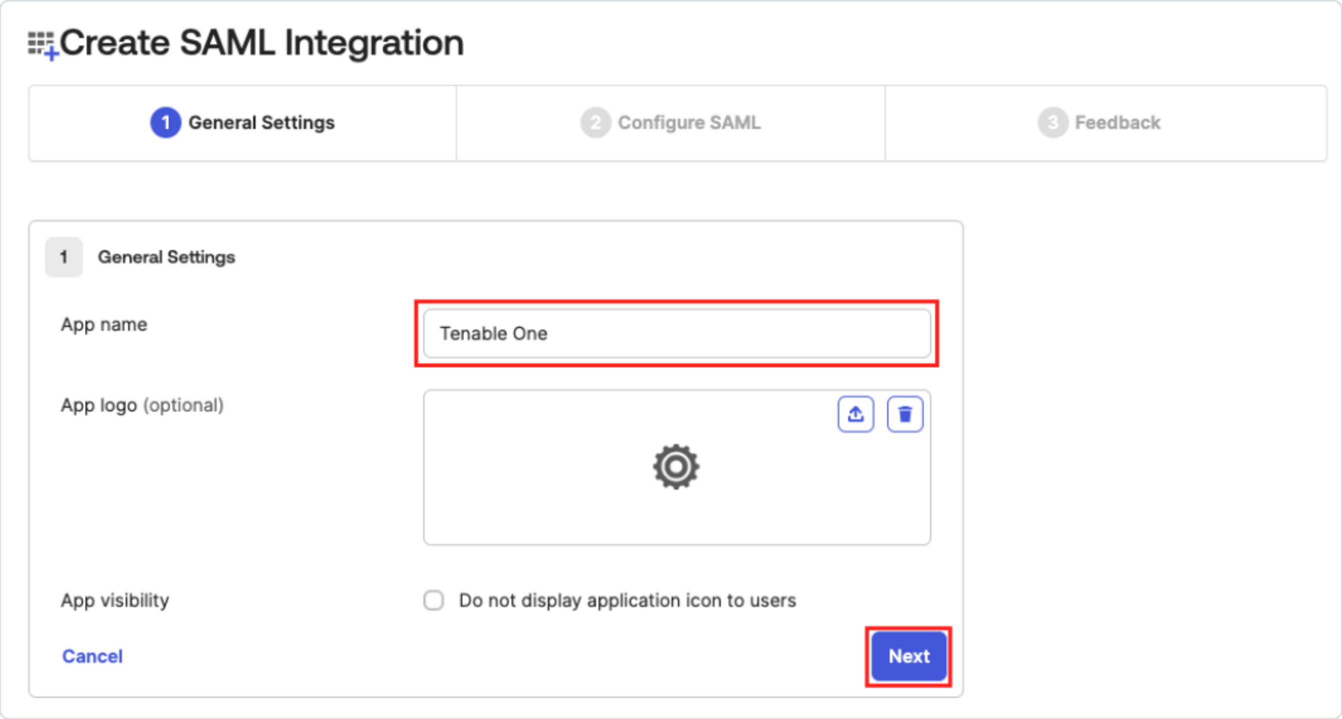
● SAML 2.0
XML-based open standard for SSO. Use if the Identity Provider for your application only supports SAML.

○ SWA - Secure Web Authentication
Okta-specific SSO method. Use if your application doesn't support OIDC or SAML.

○ API Services
Interact with Okta APIs using the scoped OAuth 2.0 access tokens for machine-to-machine authentication.

5. Click **Next**.

   The **General Settings** options appear.



Create SAML Integration

1 General Settings

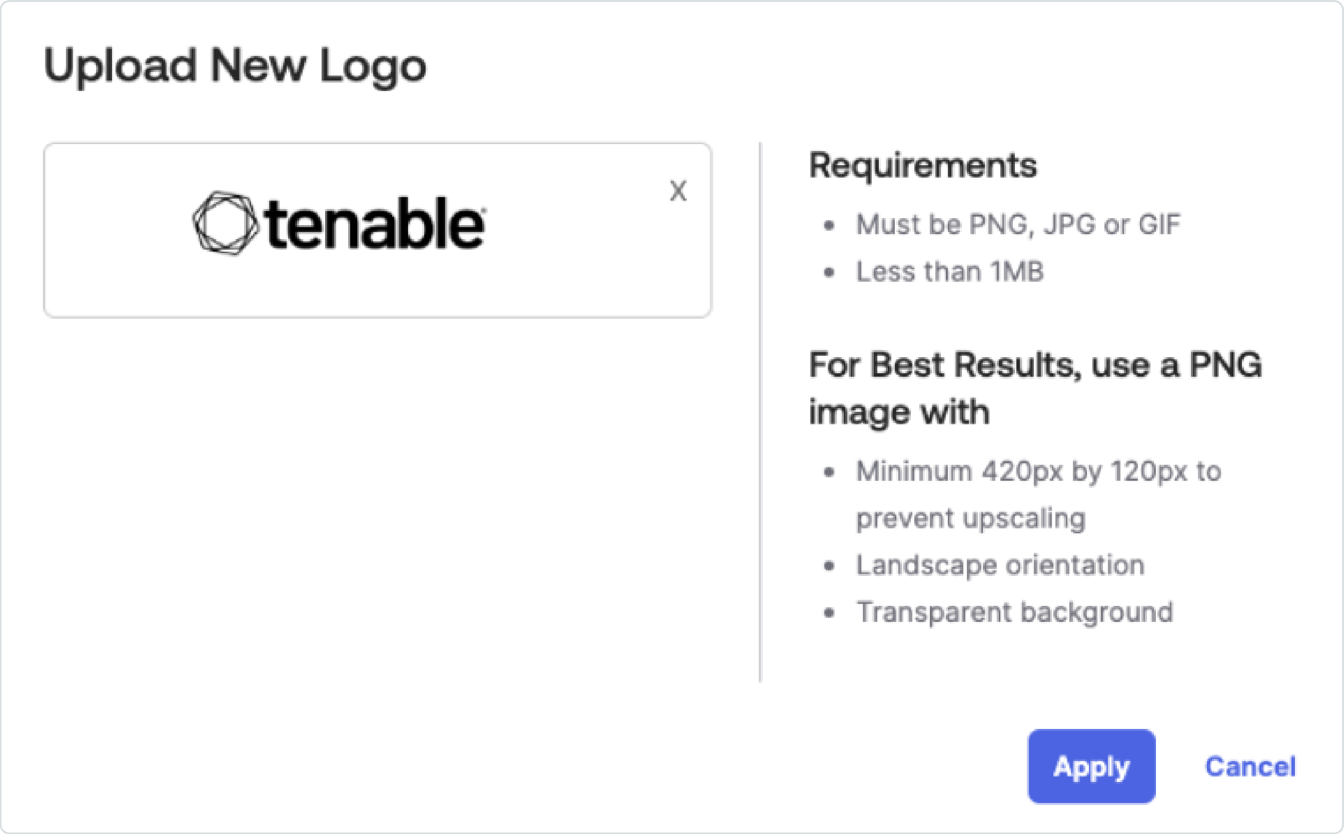
App name: Tenable One

App logo (optional)

App visibility: □ Do not display application icon to users

6. In the **App name** text box, type a name for your application.

7. (Optional) To add a custom logo for the application, in the **App logo** section, upload a .png, .jpeg, or .gif file and click **Apply**.



Upload New Logo

Requirements

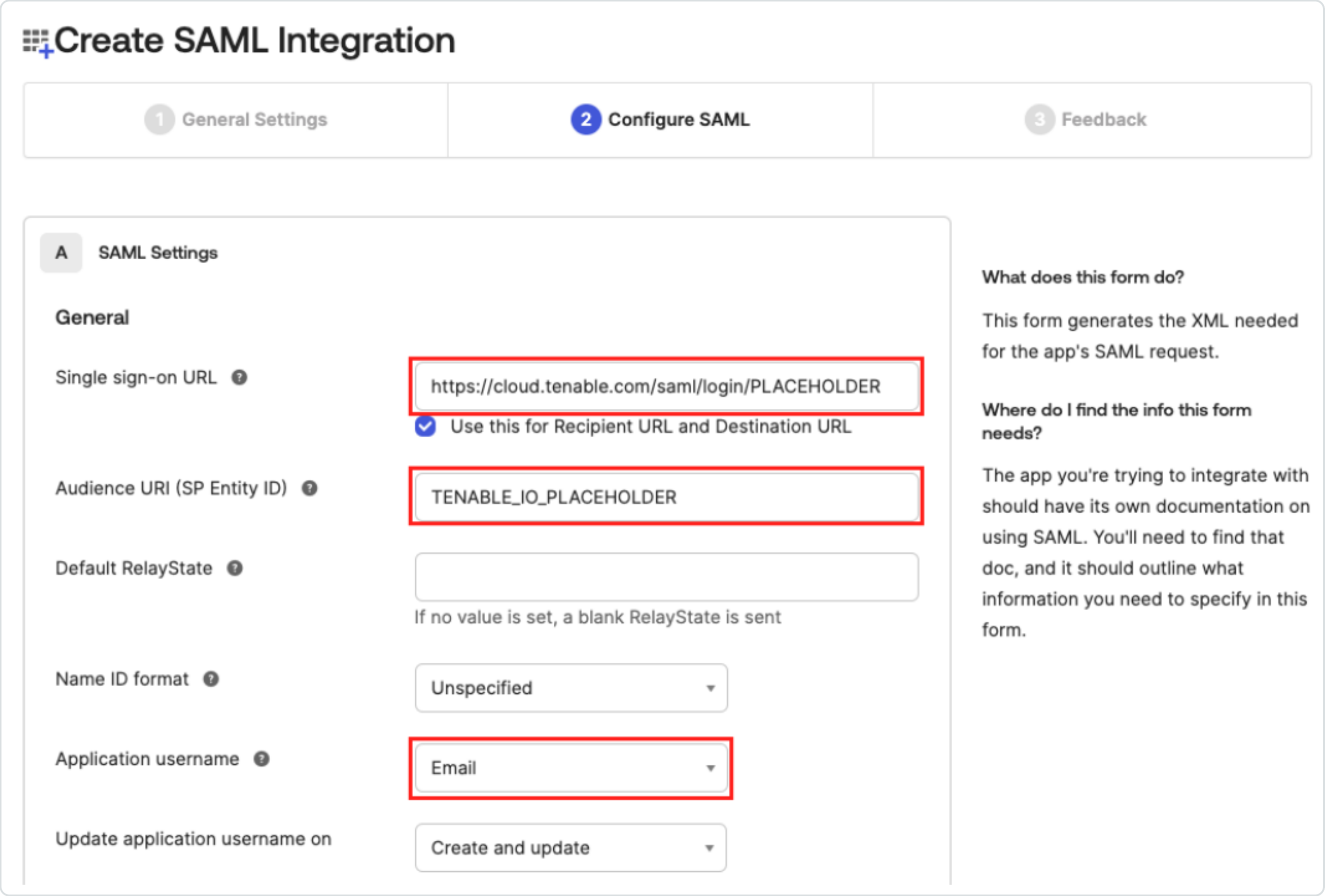
- Must be PNG, JPG or GIF
- Less than 1MB

For Best Results, use a PNG image with

- Minimum 420px by 120px to prevent upscaling
- Landscape orientation
- Transparent background

8. Click **Next**.

   The **Configure SAML** options appear.



General

Single sign-on URL: https://cloud.tenable.com/saml/login/PLACEHOLDER

☑ Use this for Recipient URL and Destination URL

Audience URI (SP Entity ID): TENABLE_IO_PLACEHOLDER

Default RelayState:

If no value is set, a blank RelayState is sent

Name ID format: Unspecified

Application username: Email

Update application username on: Create and update

What does this form do?

This form generates the XML needed for the app's SAML request.

Where do I find the info this form needs?

The app you're trying to integrate with should have its own documentation on using SAML. You'll need to find that doc, and it should outline what information you need to specify in this form.

9. In the **Single sign-on URL** text box, type the following URL:

   ```
   https://PLACEHOLDER/saml/module.php/saml/sp/saml2-acs.php/1
   ```

   Where *PLACEHOLDER* is the IP address or hostname for your Tenable Security Center instance.

10. Select the **Use this for Recipient URL and Destination URL** checkbox.

11. In the **Audience URI (SP Identity ID)** text box, type the following placeholder text:

    ```
    https://tenable.sc
    ```

12. Ensure the **Default RelayState** text box is blank.

13. In the **Name ID format** drop-down, select **Unspecified**.

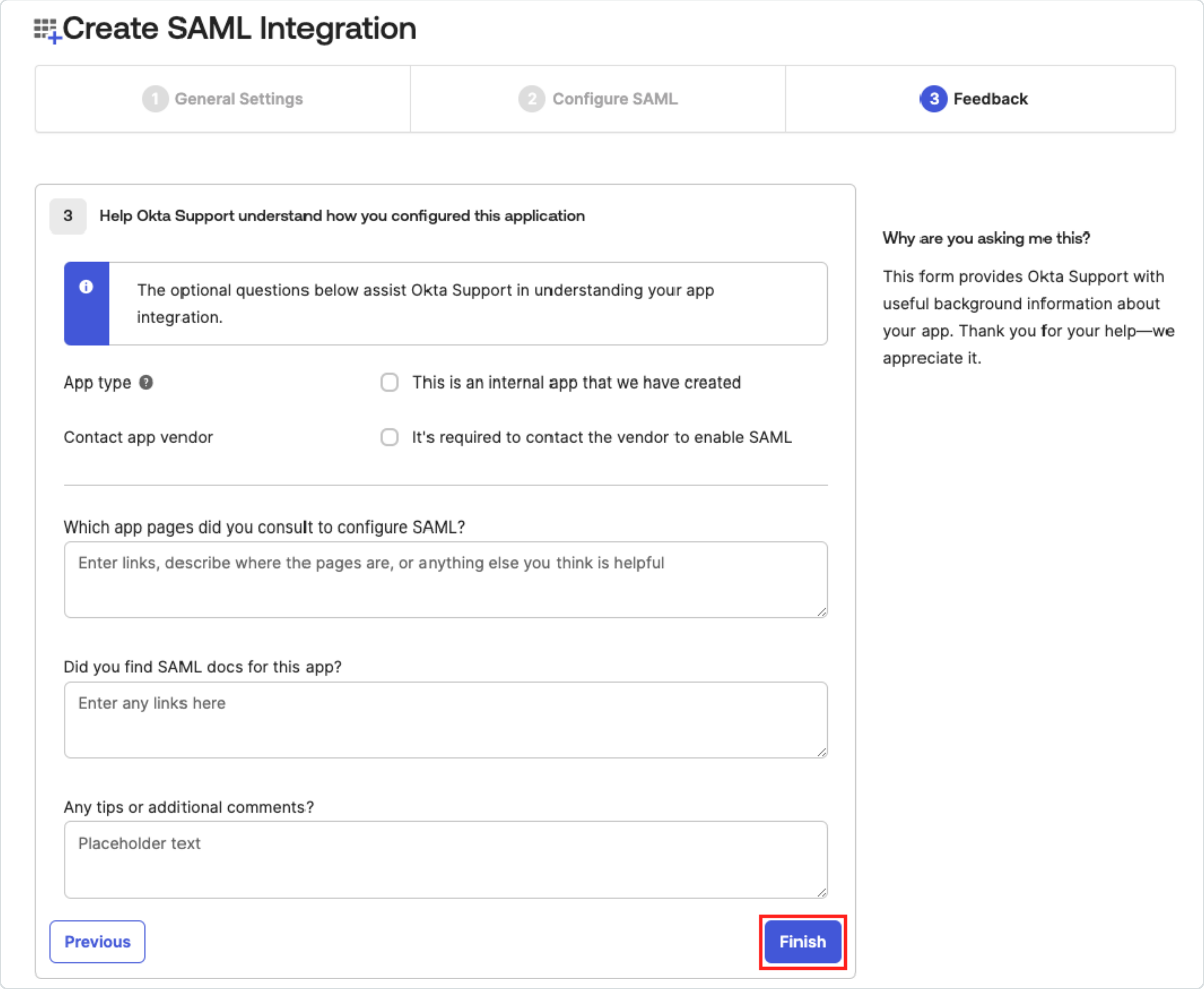
14. In the **Application username** drop-down, select **Email**.

15. In the **Update application username on** drop-down, select **Create and update**.

16. Do not change any other configuration options.

17. Click **Next**.

    The **Feedback** options appear.



Create SAML Integration

3 Help Okta Support understand how you configured this application

The optional questions below assist Okta Support in understanding your app integration.

App type □ This is an internal app that we have created

Contact app vendor □ It's required to contact the vendor to enable SAML

Which app pages did you consult to configure SAML?

Enter links, describe where the pages are, or anything else you think is helpful

Did you find SAML docs for this app?

Enter any links here

Any tips or additional comments?

Placeholder text

Why are you asking me this?

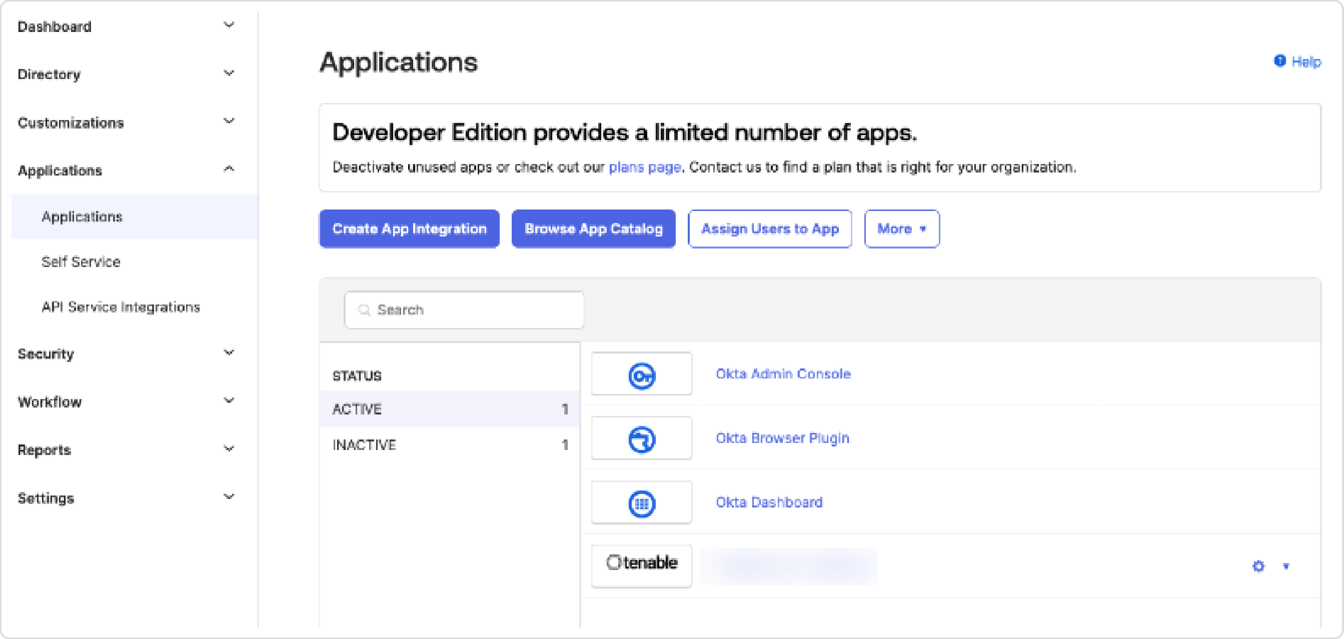
This form provides Okta Support with useful background information about your app. Thank you for your help—we appreciate it.

18. (Optional) Provide any feedback you want to include.

19. Click **Finish**.

    Okta saves your application configuration.

20. In the applications list, select the newly added application configuration.



Developer Edition provides a limited number of apps.

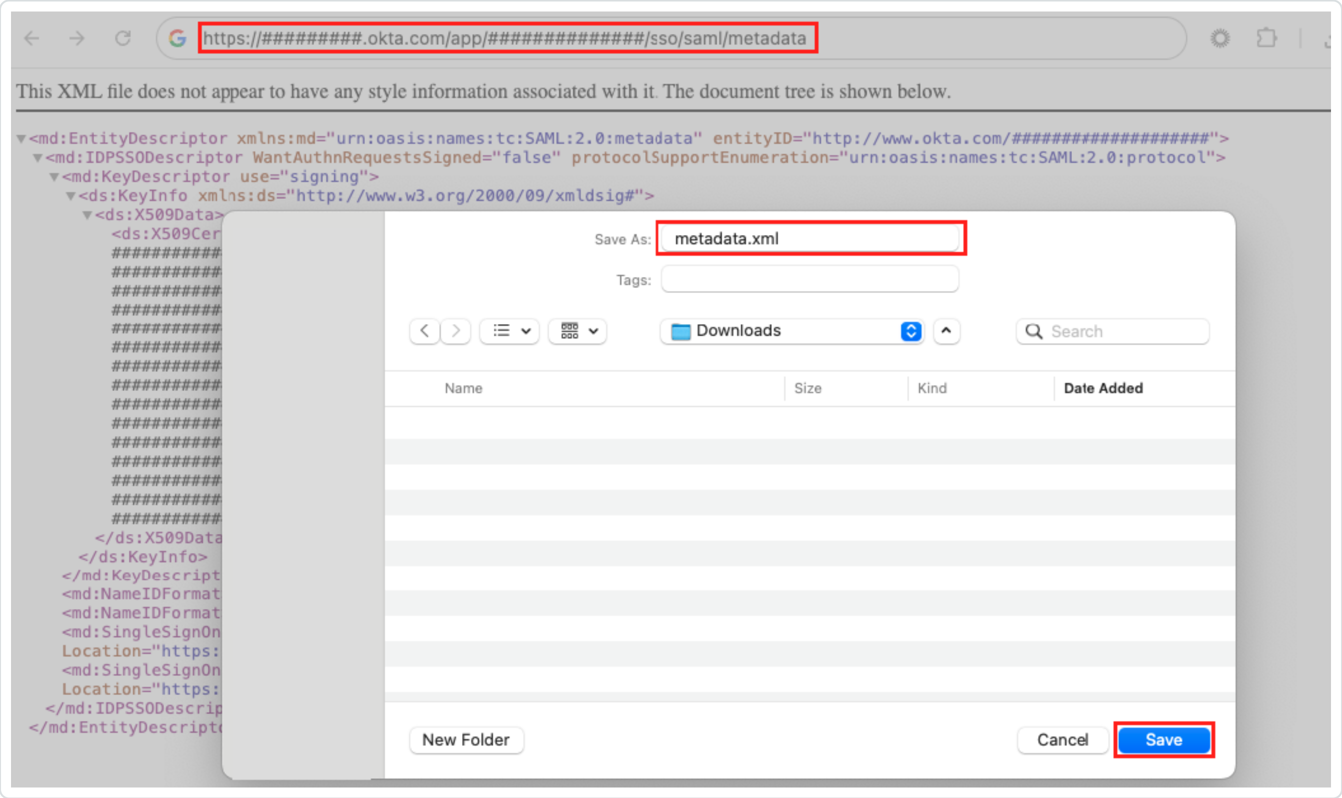
Deactivate unused apps or check out our plans page. Contact us to find a plan that is right for your organization.

Application details appear.

21. In the **Actions** drop-down menu, click **View IdP Metadata**.

    Okta redirects you to another page, where you can view the metadata file.

22. In your browser, save the resulting file as *metadata.xml*.



https://#########.okta.com/app/##############/sso/saml/metadata

This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
▼<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" entityID="http://www.okta.com/####################">
  ▼<md:IDPSSODescriptor WantAuthnRequestsSigned="false" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    ▼<md:KeyDescriptor use="signing">
      ▼<ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        ▼<ds:X509Data>
            <ds:X509Cer
            ###########
            ###########
            ###########
            ###########
            ###########
            ###########
            ###########
            ###########
            ###########
            ###########
            ###########
            ###########
            ###########
            ###########
            ###########
          </ds:X509Data
        </ds:KeyInfo>
      </md:KeyDescript
      <md:NameIDFormat
      <md:NameIDFormat
      <md:SingleSignOn
      Location="https:
      <md:SingleSignOn
      Location="https:
    </md:IDPSSODescrip
  </md:EntityDescript
```

Save As: metadata.xml

Tags:

Your browser downloads the metadata.xml file.

Enable Tenable Security Center SAML

Once you have downloaded your medata.xml file, you can use it to configure SAML in Tenable Security Center. You can configure this directly in the Tenable Security Center application.

To set up the Tenable Security Center SAML configuration:

1. In your browser, navigate to Tenable Security Center.
2. In the left navigation, click **System** > **Configuration**.

   The **Configuration** page appears.
3. Click the **SAML** button.

   The **SAML Configuration** page appears.
4. In the **General** section, confirm the **SAML** toggle is enabled.
5. In the **Source** drop-down box, select **Import**.

The page updates to display additional options.

6. In the **Type** drop-down box, select **SAML 2.0**.
7. Click **Choose File** and browse to the SAML metadata file from your identity provider.

   > **Note:** The metadata file must match the **Type** you selected. If Tenable Security Center rejects the file, contact your identity provider for assistance.

8. Click **Submit**.

   Tenable Security Center saves your configuration.

9. For the configuration you just created, click **Download SAML Configuration XML**.

   Your browser downloads the metadata.xml file. You can now use this file for final configuration in your IdP.

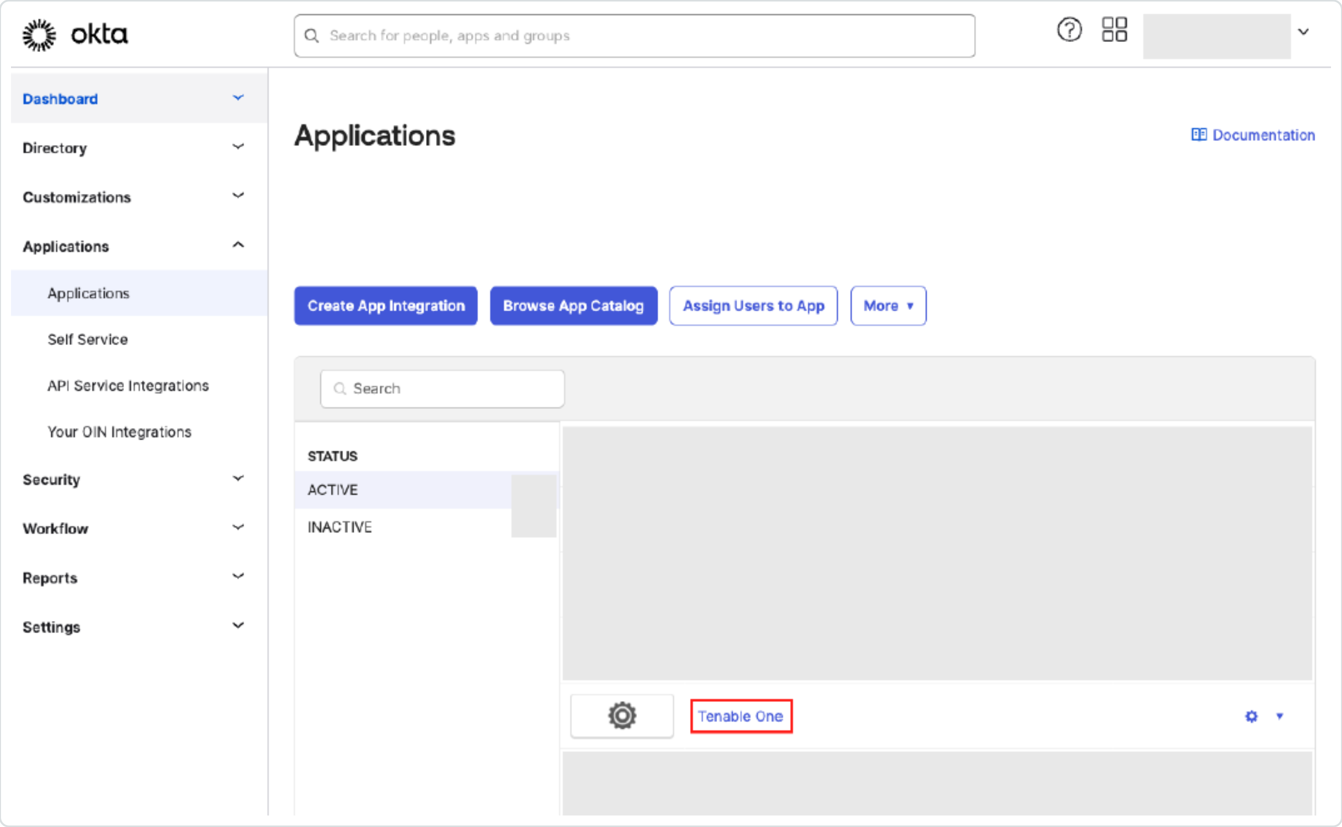
Okta: Configure Final Application Integration and Upload Metadata

Now that you have downloaded the completed metadata file, you can use that file to create a permanent Tenable application in Okta.

1. In your browser, navigate to the Okta Admin portal.
2. In the left navigation menu, click **Applications** > **Applications**.

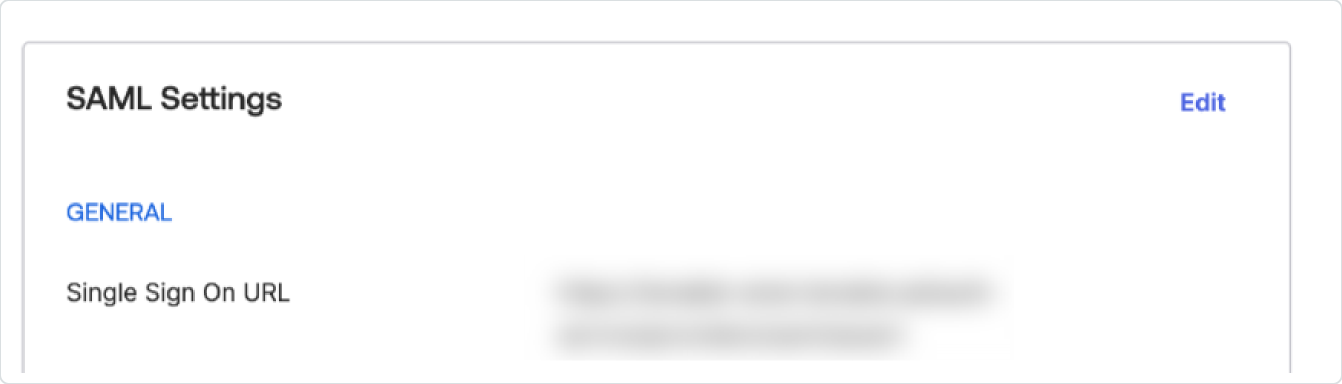
   The **Applications** page appears.

3. Click **Browse App Catalog**.



4. Select the application [you previously created](#).

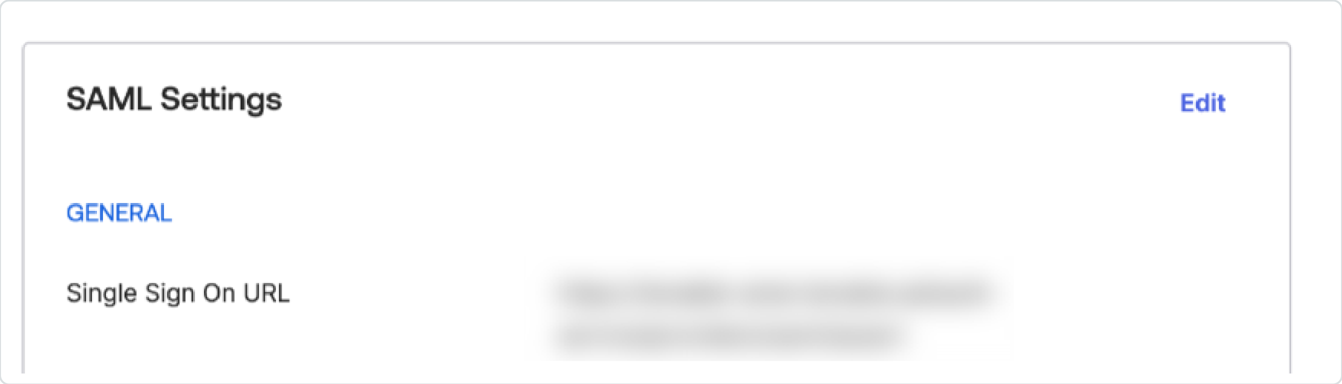
5. In the **SAML Settings** section, click **Edit**.



The **Edit SAML Integration** window appears.

6. Click **Next**.

The **Configure SAML** options appear.



7. In the **Single sign-on URL** text box, type the URL listed in the metadata.xml file that you downloaded from Tenable Security Center.

   > **Tip:** This URL is in the following format: https://*PLACEHOLDER*/saml/module.php/saml/sp/saml2-acs.php/1

8. In the **Audience URI (SP Identity ID)** text box, type ID listed in the metadata.xml file that you downloaded from Tenable Security Center.

   > **Tip:** This ID is in the following format: https://tenable.sc

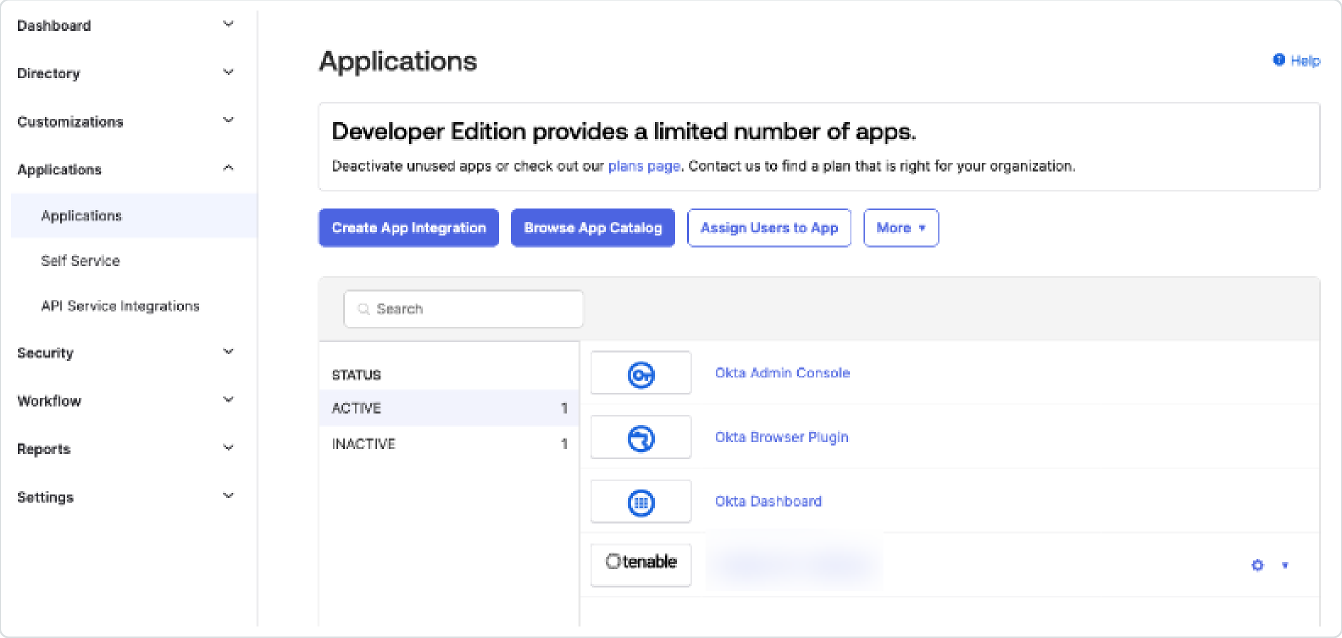
9. Click **Save**.

   Okta saves your changes to the application.

Assign the Okta Application to your Users

To assign the application to your users or groups:

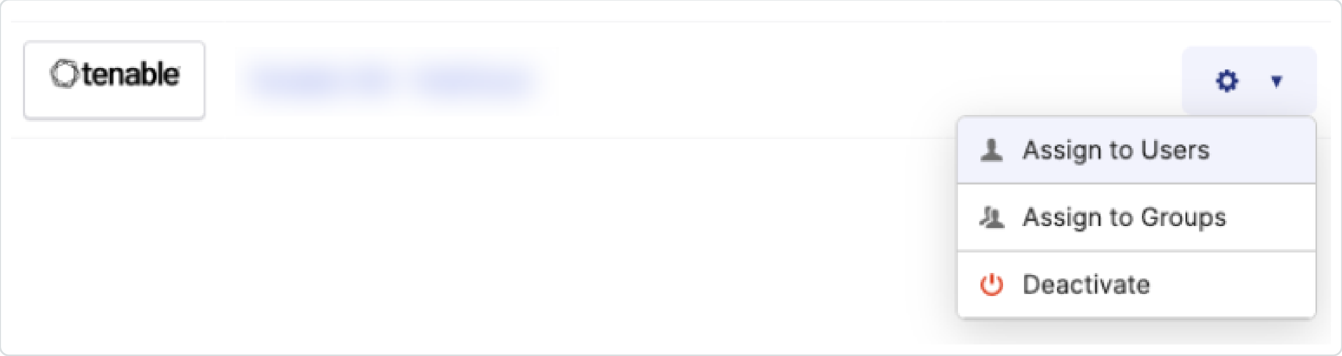
1. In the left navigation menu, click **Applications** > **Applications**.



Developer Edition provides a limited number of apps.

Deactivate unused apps or check out our plans page. Contact us to find a plan that is right for your organization.

2. Next to your newly created application configuration, click the ⚙ button.



3. Assign the application to one or more users or groups:

   - Click **Assign to Users**.
   - Click **Assign to Groups**.

   An **Assign** window appears.

4. Next to the user or group to which you want to assign the application, click **Assign**.

   A confirmation window appears.

5. Click **Save and Go Back**.

6. Repeat for each user or group to which you want to assign the application.

7. Click **Done**.

   Okta saves your changes, and you can now configure the final piece of the SAML configuration within Tenable Security Center.

Finalize the Tenable Security Center SAML Configuration

Once you've set up your application within your IdP, you can finalize your SAML configuration via the Tenable Security Center interface.

To finalize the Tenable Security Center SAML configuration:

1. Log in to Tenable Security Center via the user interface.

   > **Note:** You must log in with a user account belonging to the organization where you want to create a new user.

2. Click **Users** > **Users**.

   The **Users** page appears.

3. Click **Add**.

   The **Add User** page appears.

4. (Optional) Type a **First Name** and **Last Name** for the user.

5. In the **Type** drop-down list, select **SAML**.

6. In the **Username** box, type the user's SAML username exactly as it appears in the IdP user configuration that you created for the user.

7. Select a **Time Zone**.

8. (Optional) Select a **Scan Result Default Timeframe**.

9. (Optional) Enable **Cached Fetching**.

10. Select a **Role**. For more information, see User Roles in the Tenable Security Center User Guide.

11. Select a **Group**. For more information, see Organizations and Groups in the Tenable Security Center User Guide.
12. (Optional) To customize the user's object and user account management permissions, modify the **Group Permissions**. For more information, see Custom Group Permissions in the Tenable Security Center User Guide.
13. (Optional) To share an asset list with the user, select an **Asset**. For more information, see Assets in the Tenable Security Center User Guide.
14. (Optional) Type **Contact Information** for the user.
15. Click **Submit**.

    Tenable Security Center saves your changes, and your SAML configuration is ready for use.

Additional Resources

For more information on Okta IdP configuration, see the following resources:

- Okta Developer Portal
- Create SAML App Integrations
- Build a Single Sign-On Integration
- Create a SAML Integration in Okta

Tenable Security Center: Microsoft Entra ID IdP

One of the most common IdPs used to configure SAML with Tenable One is Microsoft Entra ID. The following steps guide you through the configuration process from start to finish.

Manual configuration requires the following:

- Reply URL: A custom URL in the following format:

  ```
  https://PLACEHOLDER/saml/module.php/saml/sp/saml2-acs.php/1
  ```

Where *PLACEHOLDER* is the IP address or hostname for your Tenable Security Center instance.

- Identifier (Entity ID): A custom ID in the following format:

```
https://tenable.sc
```

> **Note:** This value must be in URL format.

- A certificate within the SAML metadata object that matches the data originally sent to Tenable.

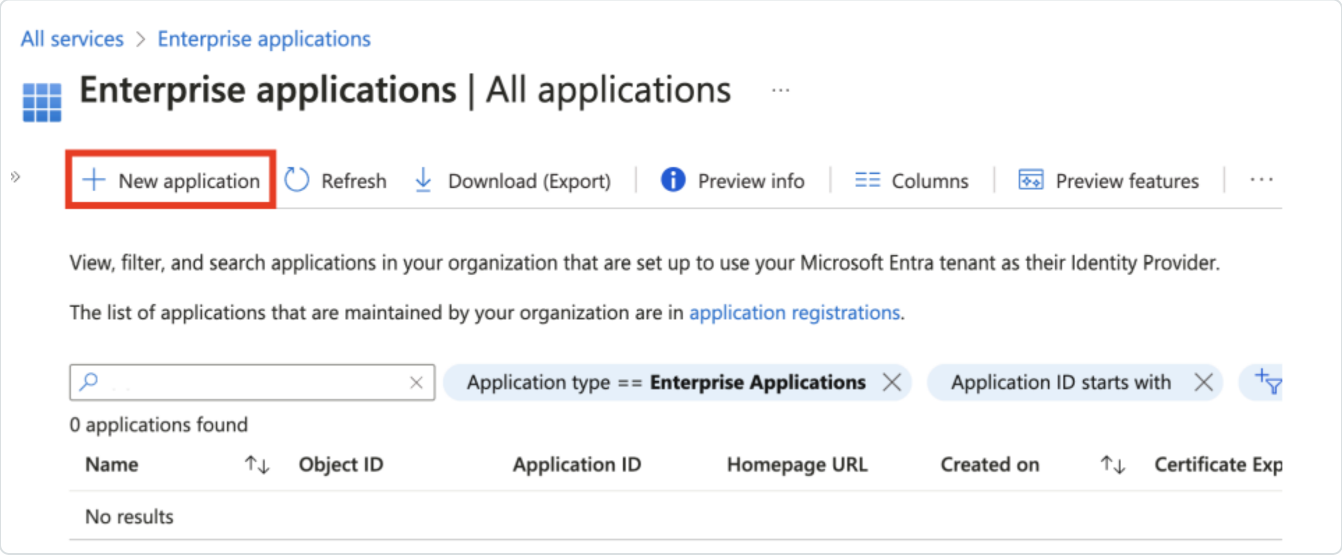
> **Note:** Tenable does not support the use of multiple certificates and only extracts the first certificate from the metadata object. If the object includes multiple certificates, you must specify which certificate to use if it is not the first one listed.

Microsoft Entra ID: Create Initial Application

To create an application in Microsoft Entra ID:

1. In your browser, navigate to the Azure Admin portal.
2. In the navigation menu, navigate to **All services** > **Enterprise Applications**.

   The application gallery appears.



All services > Enterprise applications
Enterprise applications | All applications
New application
Refresh
Download (Export)
Preview info
Columns
Preview features

View, filter, and search applications in your organization that are set up to use your Microsoft Entra tenant as their Identity Provider.

The list of applications that are maintained by your organization are in application registrations.

Application type == **Enterprise Applications**

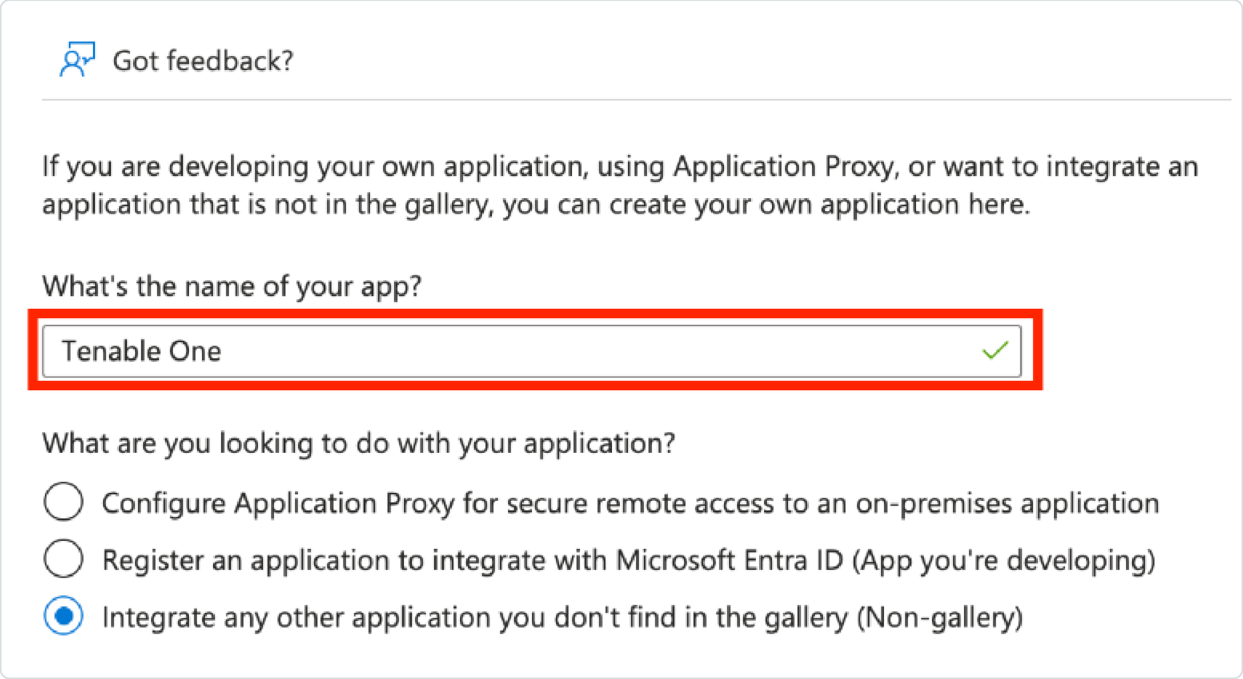
Application ID starts with

0 applications found

Name	Object ID	Application ID	Homepage URL	Created on	Certificate Exp
No results					

3. Click **Create your own application**.

   The **Create your own application** window appears.



Got feedback?

If you are developing your own application, using Application Proxy, or want to integrate an application that is not in the gallery, you can create your own application here.

What's the name of your app?

Tenable One ✓

What are you looking to do with your application?

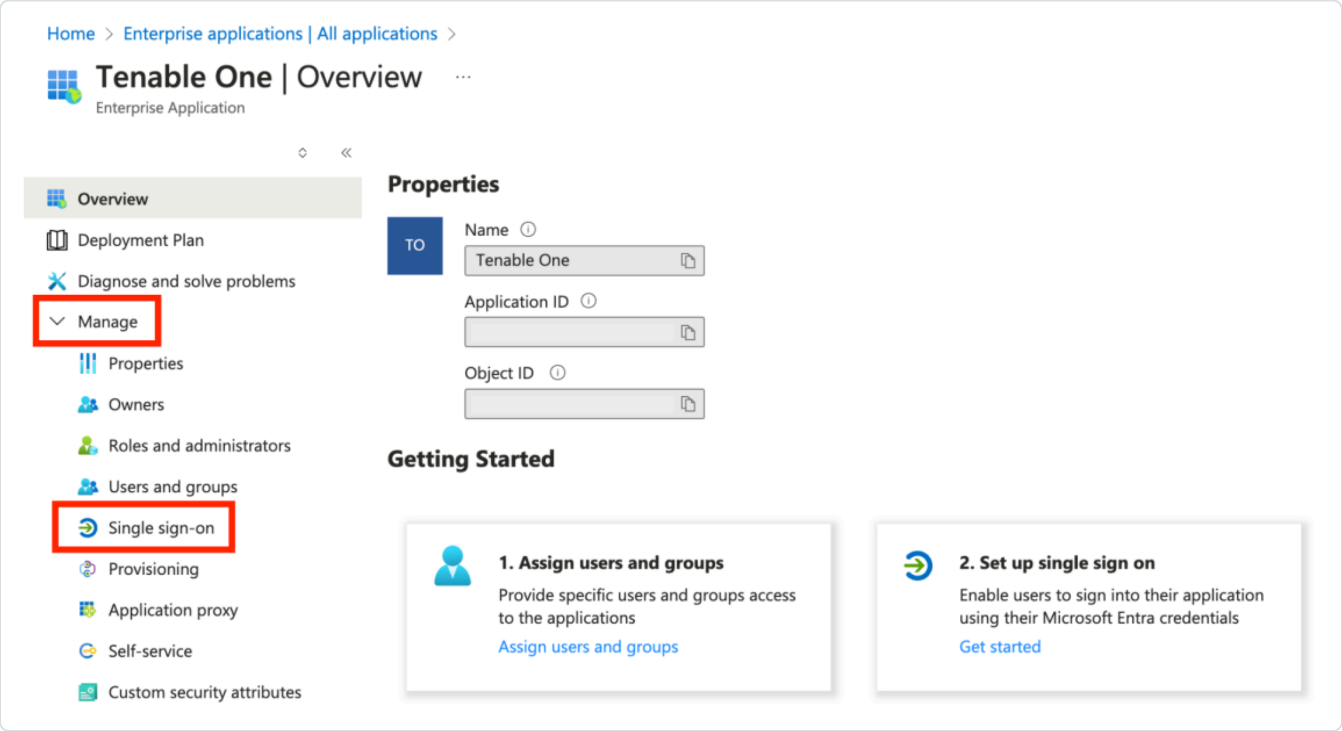
○ Configure Application Proxy for secure remote access to an on-premises application

○ Register an application to integrate with Microsoft Entra ID (App you're developing)

● Integrate any other application you don't find in the gallery (Non-gallery)

4. In the **What's the name of your app?** text box, type a name for your application.
5. In the **What are you looking to do with your application** section, select the **Integrate any other application you don't find in the gallery** radio button.
6. Click **Create**.

   Microsoft Entra ID redirects you to the application overview page.
7. In the **Getting Started** section, click the **Set up single sign on** tile.



Home > Enterprise applications | All applications >

Tenable One | Overview ...

Enterprise Application

Properties

TO

Name: Tenable One

Application ID

Object ID

Getting Started

1. Assign users and groups

Provide specific users and groups access to the applications

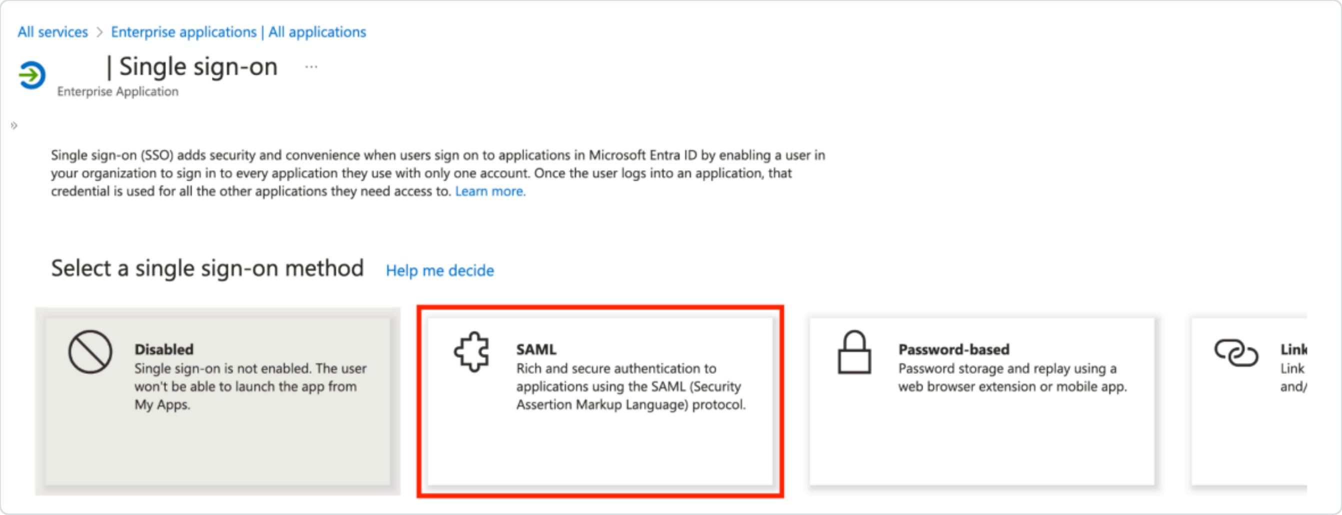
Assign users and groups

2. Set up single sign on

Enable users to sign into their application using their Microsoft Entra credentials

Get started

The **Single Sign-on** options appear.



All services > Enterprise applications | All applications

| Single sign-on ...

Enterprise Application

Single sign-on (SSO) adds security and convenience when users sign on to applications in Microsoft Entra ID by enabling a user in your organization to sign in to every application they use with only one account. Once the user logs into an application, that credential is used for all the other applications they need access to. Learn more.

Select a single sign-on method   Help me decide

Disabled
Single sign-on is not enabled. The user won't be able to launch the app from My Apps.

SAML
Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.

Password-based
Password storage and replay using a web browser extension or mobile app.

Link
Link and/

8. Click the **SAML** tile.

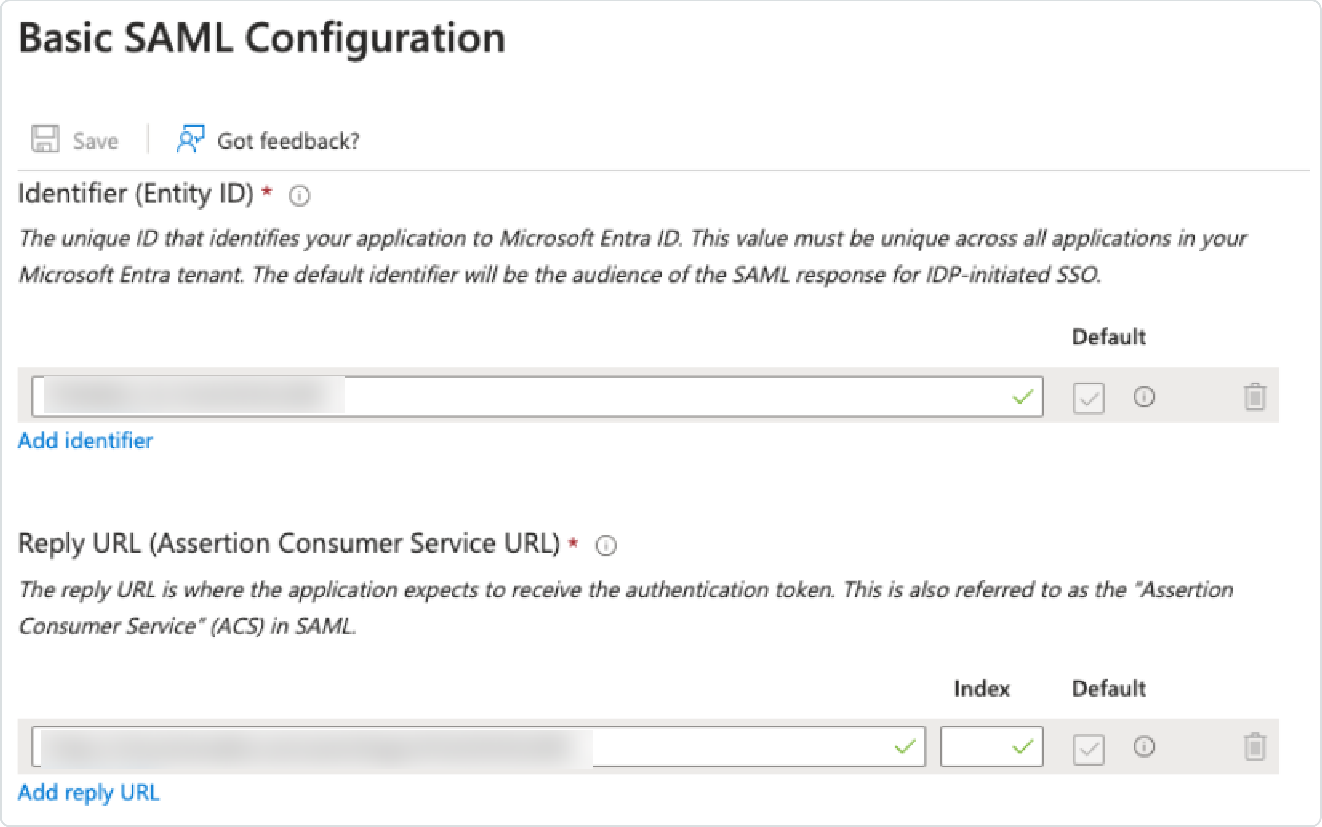
   The **SAML-based Sign-on** page appears.

9. On the **Basic SAML Configuration** tile, click the ••• button.

   Action items appear.

10. Click **Edit**.

    The **Basic SAML Configuration** page appears.

    Basic SAML Configuration

    Identifier (Entity ID) *

    The unique ID that identifies your application to Microsoft Entra ID. This value must be unique across all applications in your Microsoft Entra tenant. The default identifier will be the audience of the SAML response for IDP-initiated SSO.

	Default
[redacted] ✓	☑

    Reply URL (Assertion Consumer Service URL) *

    The reply URL is where the application expects to receive the authentication token. This is also referred to as the "Assertion Consumer Service" (ACS) in SAML.

	Index	Default
[redacted] ✓	✓	☑

11. In the **Identifier (Entity ID)** text box, type the following text:

    ```
    https://tenable.sc
    ```

12. In the **Reply URL** text box, type the following text:

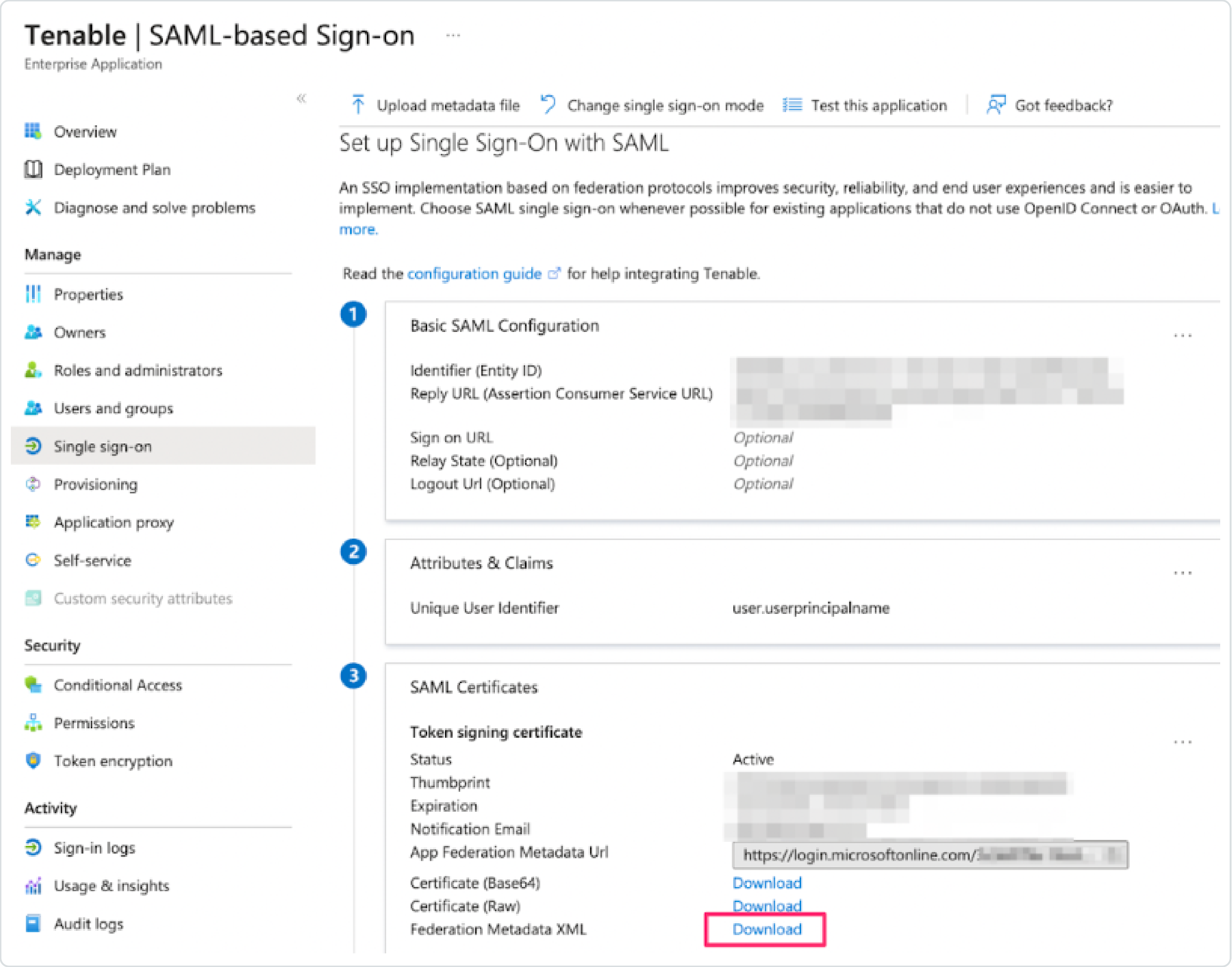
    ```
    https://PLACEHOLDER/saml/module.php/saml/sp/saml2-acs.php/1
    ```

    Where *PLACEHOLDER* is the IP address or hostname for your Tenable Security Center instance.

13. Click **Save**.

    You return to the **SAML-based Sign-on** page.

14. On the **SAML Certificates** tile, in the **Federation Metadata XML** section, click **Download**.



Tenable | SAML-based Sign-on ...

Enterprise Application

«

Upload metadata file | Change single sign-on mode | Test this application | Got feedback?

Overview

Deployment Plan

Diagnose and solve problems

Manage

Properties

Owners

Roles and administrators

Users and groups

Single sign-on

Provisioning

Application proxy

Self-service

Custom security attributes

Security

Conditional Access

Permissions

Token encryption

Activity

Sign-in logs

Usage & insights

Audit logs

Set up Single Sign-On with SAML

An SSO implementation based on federation protocols improves security, reliability, and end user experiences and is easier to implement. Choose SAML single sign-on whenever possible for existing applications that do not use OpenID Connect or OAuth. L more.

Read the configuration guide for help integrating Tenable.

1 Basic SAML Configuration ...

Identifier (Entity ID)	[redacted]
Reply URL (Assertion Consumer Service URL)	
Sign on URL	Optional
Relay State (Optional)	Optional
Logout Url (Optional)	Optional

2 Attributes & Claims ...

Unique User Identifier	user.userprincipalname

3 SAML Certificates

Token signing certificate ...

Status	Active
Thumbprint	[redacted]
Expiration	
Notification Email	
App Federation Metadata Url	https://login.microsoftonline.com/[redacted]
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

Your browser downloads the metadata.xml file.

Enable Tenable Security Center SAML

Once you have downloaded your medata.xml file, you can use it to configure SAML in Tenable Security Center. You can configure this directly in the Tenable Security Center application.

To set up the Tenable Security Center SAML configuration:

1. In your browser, navigate to Tenable Security Center.
2. In the left navigation, click **System** > **Configuration**.

   The **Configuration** page appears.

3. Click the **SAML** button.

   The **SAML Configuration** page appears.

4. In the **General** section, confirm the **SAML** toggle is enabled.

5. In the **Source** drop-down box, select **Import**.

   The page updates to display additional options.

6. In the **Type** drop-down box, select **SAML 2.0**.

7. Click **Choose File** and browse to the SAML metadata file from your identity provider.

   > **Note:** The metadata file must match the **Type** you selected. If Tenable Security Center rejects the file, contact your identity provider for assistance.

8. Click **Submit**.

   Tenable Security Center saves your configuration.

9. For the configuration you just created, click **Download SAML Configuration XML**.

   Your browser downloads the metadata.xml file. You can now use this file for final configuration in your IdP.

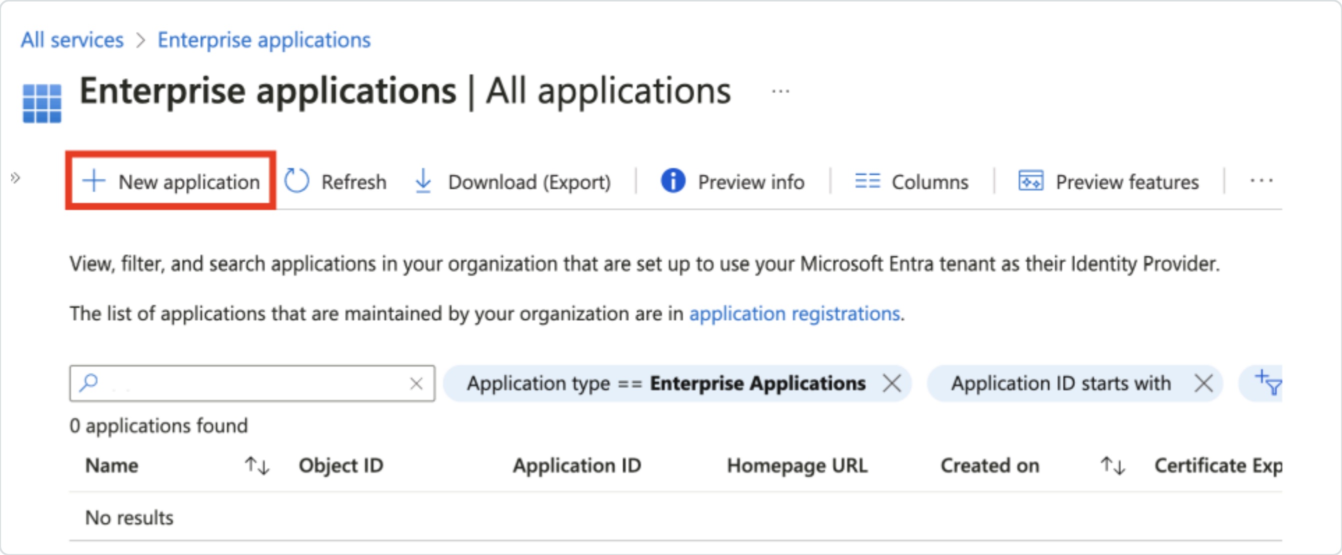
Microsoft Entra ID: Configure Final Application and Upload Metadata

Now that you have downloaded the completed metadata file, you can upload that file to your Tenable application in Microsoft Entra ID.

1. In your browser, navigate to the Azure Admin portal.

2. In the navigation menu, navigate to **All services** > **Enterprise Applications**.

   The application gallery appears.


All services > Enterprise applications
Enterprise applications | All applications
New application
Refresh
Download (Export)
Preview info
Columns
Preview features
Application type == Enterprise Applications
Application ID starts with

View, filter, and search applications in your organization that are set up to use your Microsoft Entra tenant as their Identity Provider.

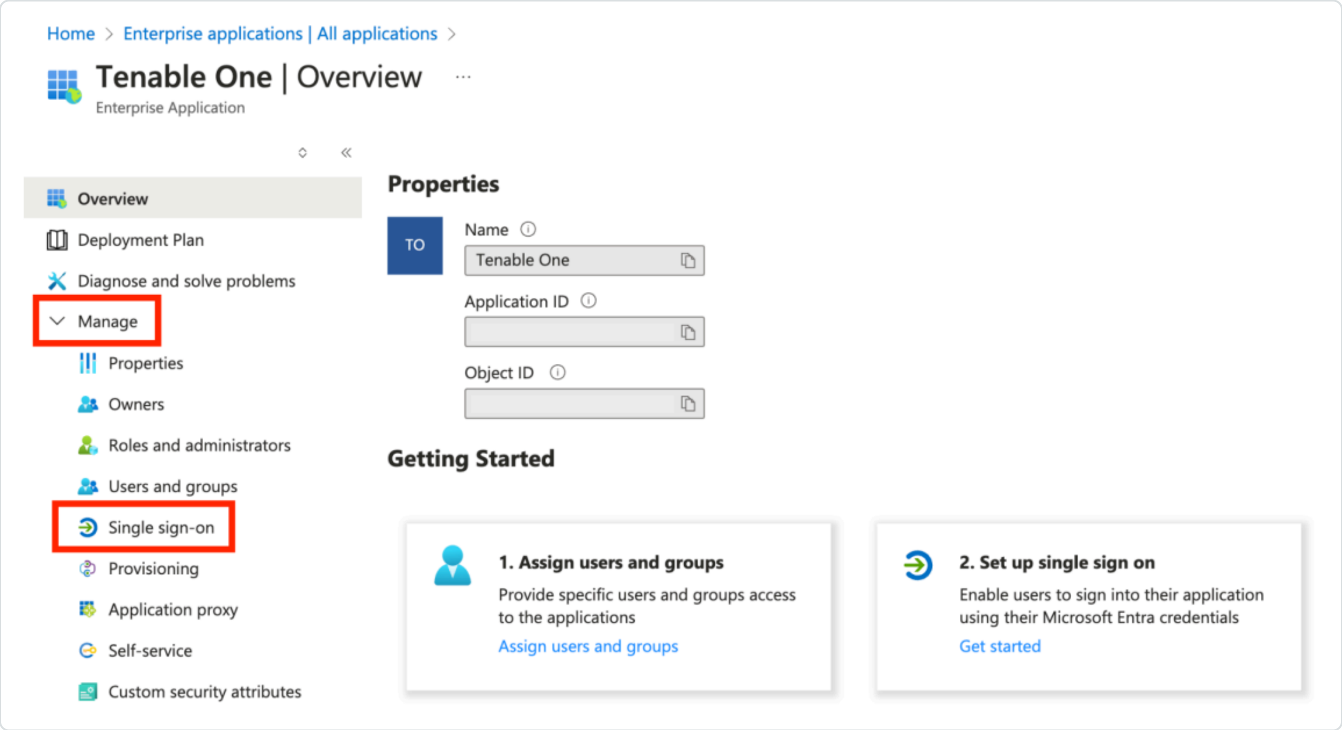
The list of applications that are maintained by your organization are in application registrations.

0 applications found

Name	Object ID	Application ID	Homepage URL	Created on	Certificate Exp
No results					

3. Select the newly created application.

4. In the **Getting Started** section, click the **Set up single sign on** tile.



Name: Tenable One

Application ID:

Object ID:

1. Assign users and groups
Provide specific users and groups access to the applications
Assign users and groups

2. Set up single sign on
Enable users to sign into their application using their Microsoft Entra credentials
Get started

5. Click **Upload Metadata file**.

6. In your file manager, select the Service Provider metadata.xml file that you downloaded from Tenable Security Center.

   Microsoft Entra ID imports the metadata from the file.

7. Click **Save**.

   Microsoft Entra ID saves your changes to the permanent application.

Create and Assign Microsoft Entra ID Users

To create groups and assign users:

1. In Microsoft Entra ID, in the left navigation menu, click **Users and Groups**.

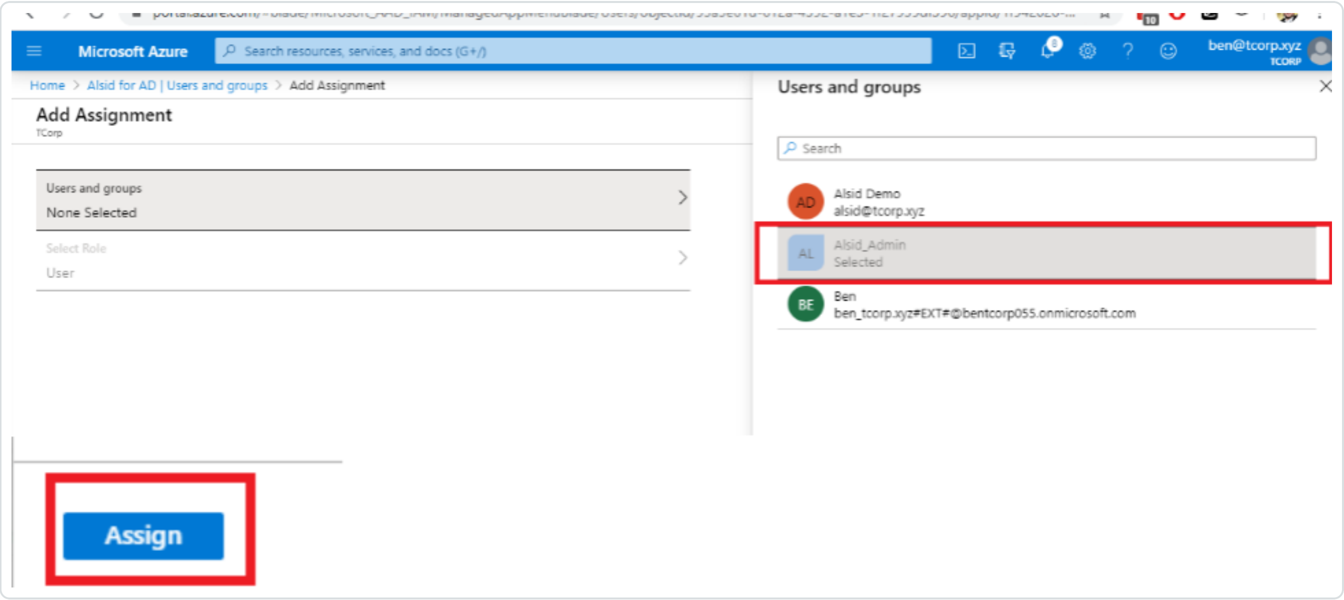
   The **Users and Groups** page appears.

2. Click **Add User**.

   The **Add Assignment** page appears.

3. Click the Users and Groups section.

4. In the selection plane, select the users and/or groups you want to assign to the group for use with Tenable Security Center.



5. Once you've selected the users you want to assign, click **Assign**.

Microsoft Entra ID saves your changes, and you can now finish your SAML configuration within the Tenable Security Center application.

Finalize the Tenable Security Center SAML Configuration

Once you've set up your application within your IdP, you can finalize your SAML configuration via the Tenable Security Center interface.

To finalize the Tenable Security Center SAML configuration:

1. Log in to Tenable Security Center via the user interface.

   > **Note:** You must log in with a user account belonging to the organization where you want to create a new user.

2. Click **Users** > **Users**.

   The **Users** page appears.

3. Click **Add**.

   The **Add User** page appears.

4. (Optional) Type a **First Name** and **Last Name** for the user.
5. In the **Type** drop-down list, select **SAML**.
6. In the **Username** box, type the user's SAML username exactly as it appears in the IdP user configuration that you created for the user.
7. Select a **Time Zone**.
8. (Optional) Select a **Scan Result Default Timeframe**.
9. (Optional) Enable **Cached Fetching**.
10. Select a **Role**. For more information, see User Roles in the Tenable Security Center User Guide.
11. Select a **Group**. For more information, see Organizations and Groups in the Tenable Security Center User Guide.

12. (Optional) To customize the user's object and user account management permissions, modify the **Group Permissions**. For more information, see Custom Group Permissions in the Tenable Security Center User Guide.

13. (Optional) To share an asset list with the user, select an **Asset**. For more information, see Assets in the Tenable Security Center User Guide.

14. (Optional) Type **Contact Information** for the user.

15. Click **Submit**.

    Tenable Security Center saves your changes, and your SAML configuration is ready for use.

Additional Resources

For more information on Microsoft Entra ID IdP configuration, see the following resources:

- Microsoft Entra ID Developer Portal
- SAML Authentication with Microsoft Entra ID
- Use a SAML 2.0 IdP for Single Sign On

Tenable Security Center: Microsoft ADFS IdP

One of the most common IdPs used to configure SAML with Tenable Security Center is Microsoft ADFS. The following steps guide you through the configuration process from start to finish.

Manual configuration requires the following:

- Login URL: A custom URL in the following format:

  ```
  https://PLACEHOLDER/saml/module.php/saml/sp/saml2-acs.php/1
  ```

  Where *PLACEHOLDER* is the IP address or hostname for your Tenable Security Center instance.

- Audience URI (SP Entity ID): A custom ID in the following format:

```
https://tenable.sc
```

> **Note:** This value must be in URL format.

- A certificate within the SAML metadata object that matches the data originally sent to Tenable.

> **Note:**Tenable does not support the use of multiple certificates and only extracts the first certificate from the metadata object. If the object includes multiple certificates, you must specify which certificate to use if it is not the first one listed.

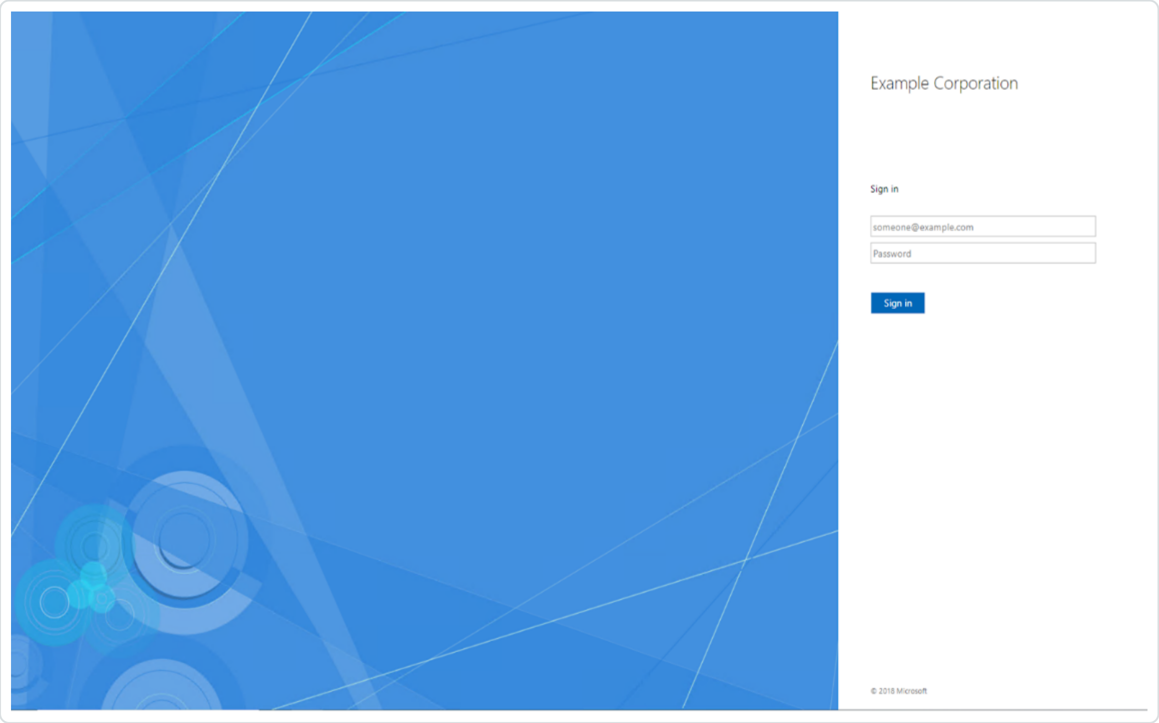
ADFS: Download your SAML Metadata File

To download your SAML Metadata.xml file:

1. Navigate to your ADFS console.

   > **Note:** Your login URL varies based on the DNS FQDN you configured. For example, in this case, the ADFS SSO Portal login would be: *https://adfs.example.com/adfs/ls/idpinitiatedsignon*.

2. Type your login credentials and click **Sign In**.

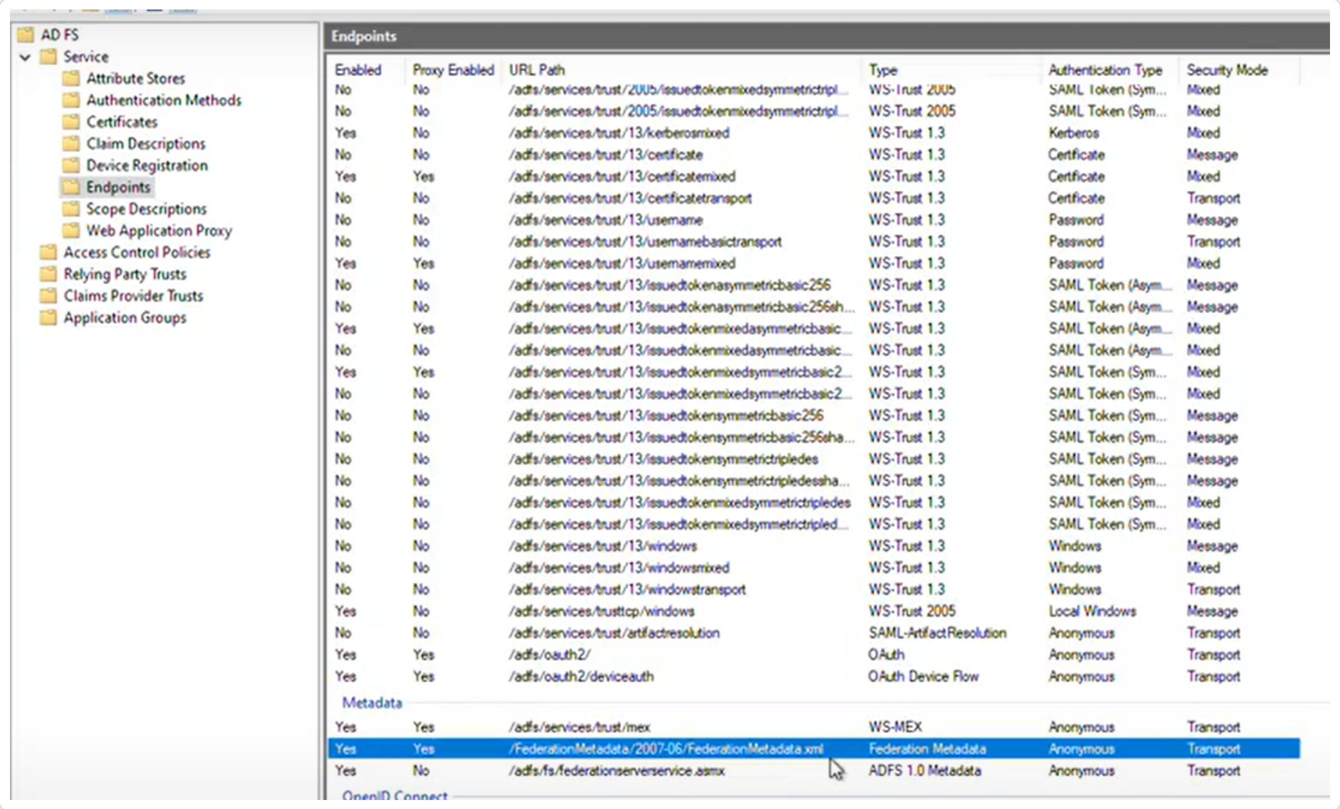


You log in to the console.

3. In the left menu, navigate to **Service** > **Endpoints**.

   The **Endpoints** page appears.

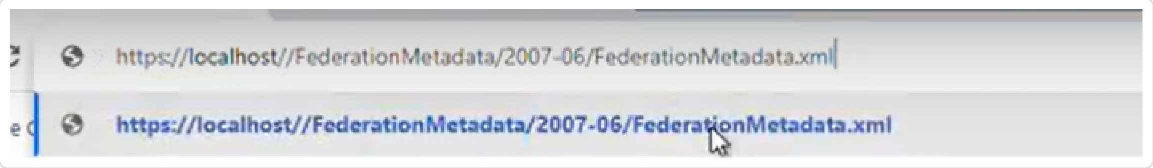
4. In the **Metadata** section, copy the URL in the **Federation Metadata** row.



Endpoints

Enabled	Proxy Enabled	URL Path	Type	Authentication Type	Security Mode
No	No	/adfs/services/trust/2005/issuedtokenmixedsymmetrictripl...	WS-Trust 2005	SAML Token (Sym...	Mixed
No	No	/adfs/services/trust/2005/issuedtokenmixedsymmetrictripl...	WS-Trust 2005	SAML Token (Sym...	Mixed
Yes	No	/adfs/services/trust/13/kerberosmixed	WS-Trust 1.3	Kerberos	Mixed
No	No	/adfs/services/trust/13/certificate	WS-Trust 1.3	Certificate	Message
Yes	Yes	/adfs/services/trust/13/certificatemixed	WS-Trust 1.3	Certificate	Mixed
No	No	/adfs/services/trust/13/certificatetransport	WS-Trust 1.3	Certificate	Transport
No	No	/adfs/services/trust/13/usemame	WS-Trust 1.3	Password	Message
No	No	/adfs/services/trust/13/usemamebasictransport	WS-Trust 1.3	Password	Transport
Yes	Yes	/adfs/services/trust/13/usemamemixed	WS-Trust 1.3	Password	Mixed
No	No	/adfs/services/trust/13/issuedtokenasymmetricbasic256	WS-Trust 1.3	SAML Token (Asym...	Message
No	No	/adfs/services/trust/13/issuedtokenasymmetricbasic256sh...	WS-Trust 1.3	SAML Token (Asym...	Message
Yes	Yes	/adfs/services/trust/13/issuedtokenmixedasymmetricbasic...	WS-Trust 1.3	SAML Token (Asym...	Mixed
No	No	/adfs/services/trust/13/issuedtokenmixedasymmetricbasic...	WS-Trust 1.3	SAML Token (Asym...	Mixed
Yes	Yes	/adfs/services/trust/13/issuedtokenmixedsymmetricbasic2...	WS-Trust 1.3	SAML Token (Sym...	Mixed
No	No	/adfs/services/trust/13/issuedtokenmixedsymmetricbasic2...	WS-Trust 1.3	SAML Token (Sym...	Mixed
No	No	/adfs/services/trust/13/issuedtokensymmetricbasic256	WS-Trust 1.3	SAML Token (Sym...	Message
No	No	/adfs/services/trust/13/issuedtokensymmetricbasic256sha...	WS-Trust 1.3	SAML Token (Sym...	Message
No	No	/adfs/services/trust/13/issuedtokensymmetrictripledes	WS-Trust 1.3	SAML Token (Sym...	Message
No	No	/adfs/services/trust/13/issuedtokensymmetrictripledessha...	WS-Trust 1.3	SAML Token (Sym...	Message
No	No	/adfs/services/trust/13/issuedtokenmixedsymmetrictripledes	WS-Trust 1.3	SAML Token (Sym...	Mixed
No	No	/adfs/services/trust/13/issuedtokenmixedsymmetrictripled...	WS-Trust 1.3	SAML Token (Sym...	Mixed
No	No	/adfs/services/trust/13/windows	WS-Trust 1.3	Windows	Message
No	No	/adfs/services/trust/13/windowsmixed	WS-Trust 1.3	Windows	Mixed
No	No	/adfs/services/trust/13/windowstransport	WS-Trust 1.3	Windows	Transport
Yes	No	/adfs/services/trusttcp/windows	WS-Trust 2005	Local Windows	Message
No	No	/adfs/services/trust/artifactresolution	SAML-ArtifactResolution	Anonymous	Transport
Yes	Yes	/adfs/oauth2/	OAuth	Anonymous	Transport
Yes	Yes	/adfs/oauth2/deviceauth	OAuth Device Flow	Anonymous	Transport
Metadata					
Yes	Yes	/adfs/services/trust/mex	WS-MEX	Anonymous	Transport
Yes	Yes	/FederationMetadata/2007-06/FederationMetadata.xml	Federation Metadata	Anonymous	Transport
Yes	No	/adfs/fs/federationserverservice.asmx	ADFS 1.0 Metadata	Anonymous	Transport
OpenID Connect					

5. In your browser, type `https://localhost/` and then paste the metadata URL you copied.



https://localhost//FederationMetadata/2007-06/FederationMetadata.xml

https://localhost//FederationMetadata/2007-06/FederationMetadata.xml

6. On your keyboard, press **Enter**.

   Your browser downloads the metadata file.

Enable Tenable Security Center SAML

Once you have downloaded your medata.xml file, you can use it to configure SAML in Tenable Security Center. You can configure this directly in the Tenable Security Center application.

To set up the Tenable Security Center SAML configuration:

1. In your browser, navigate to Tenable Security Center.
2. In the left navigation, click **System** > **Configuration**.

   The **Configuration** page appears.
3. Click the **SAML** button.

   The **SAML Configuration** page appears.
4. In the **General** section, confirm the **SAML** toggle is enabled.
5. In the **Source** drop-down box, select **Import**.

   The page updates to display additional options.
6. In the **Type** drop-down box, select **SAML 2.0**.
7. Click **Choose File** and browse to the SAML metadata file from your identity provider.

   > **Note:** The metadata file must match the **Type** you selected. If Tenable Security Center rejects the file, contact your identity provider for assistance.
8. Click **Submit**.

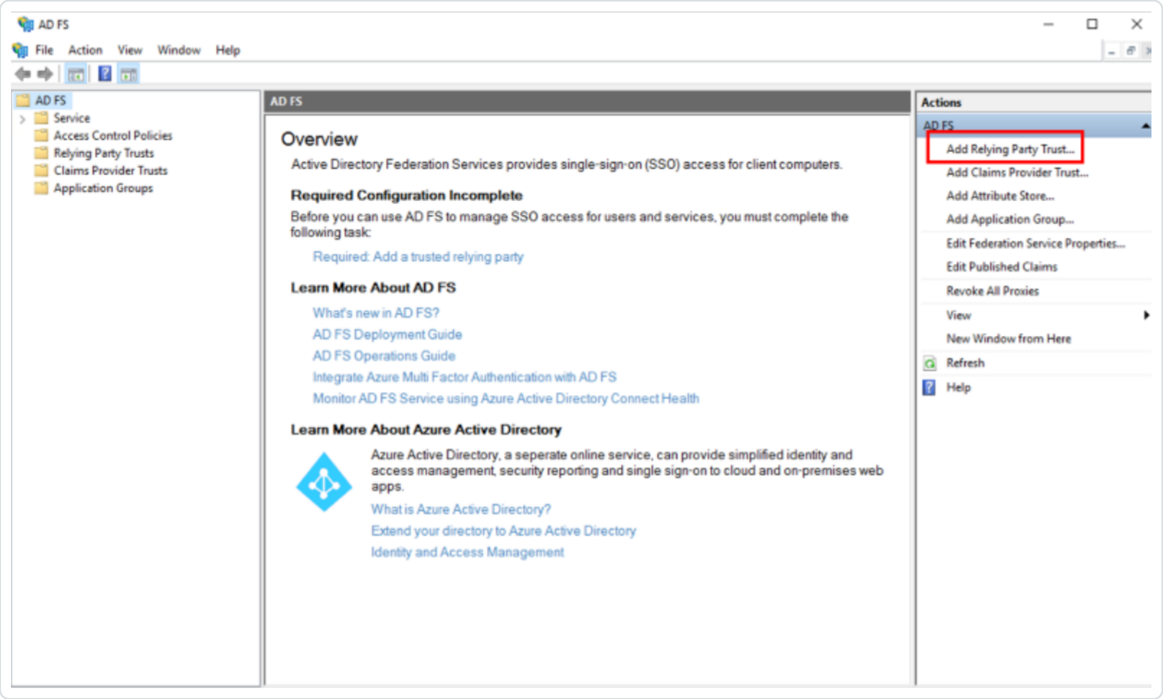
   Tenable Security Center saves your configuration.
9. For the configuration you just created, click **Download SAML Configuration XML**.

   Your browser downloads the metadata.xml file. You can now use this file for final configuration in your IdP.

ADFS: Configure Final Application, Upload Metadata, and Configure Relying Party Trusts

Now that you have downloaded the completed metadata file, you can upload that file to your Tenable application in the ADFS console.

1. Open the MMC.exe console.
2. On the right side of the console, in the **Actions** section, click **Add Relying Party Trust**.



Overview

Active Directory Federation Services provides single-sign-on (SSO) access for client computers.

Required Configuration Incomplete

Before you can use AD FS to manage SSO access for users and services, you must complete the following task:

Required: Add a trusted relying party

Learn More About AD FS

What's new in AD FS?
AD FS Deployment Guide
AD FS Operations Guide
Integrate Azure Multi Factor Authentication with AD FS
Monitor AD FS Service using Azure Active Directory Connect Health

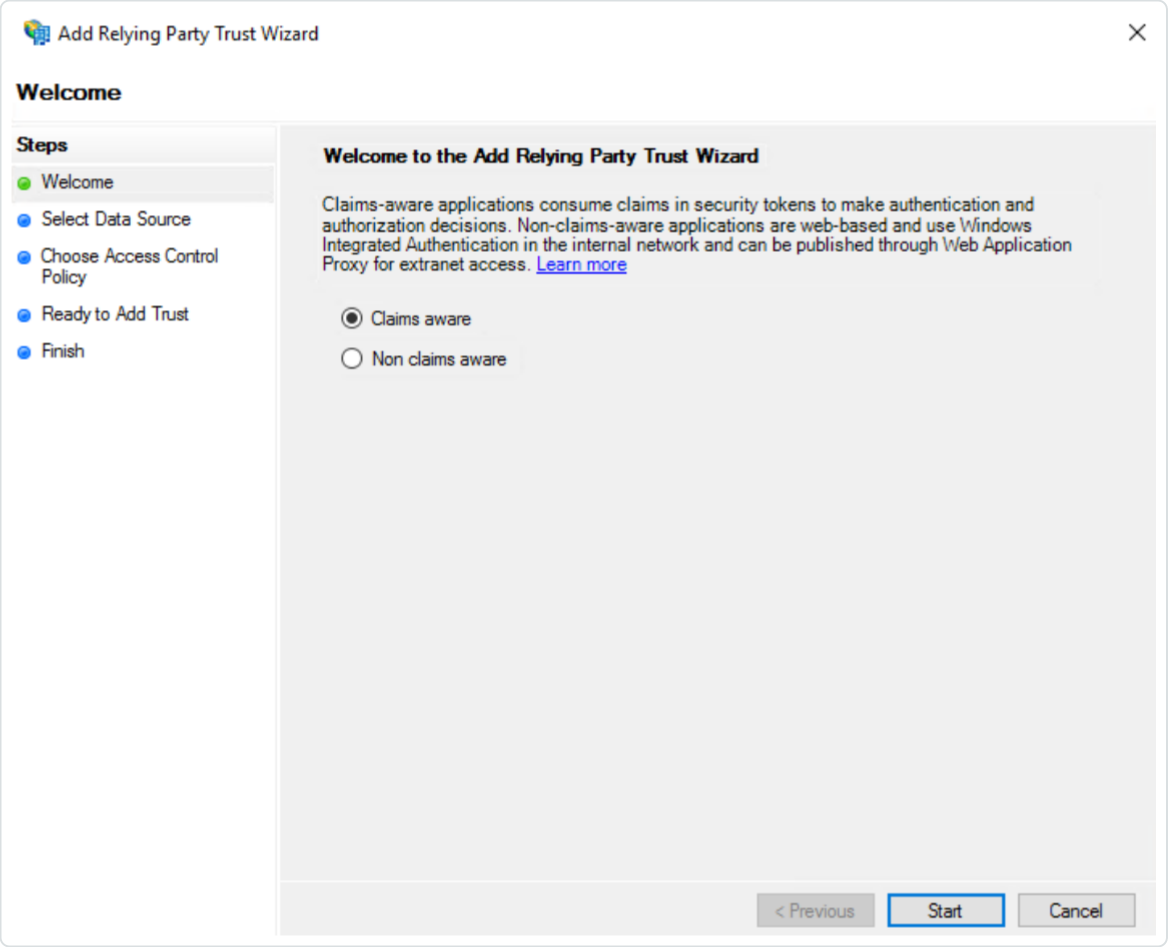
Learn More About Azure Active Directory

Azure Active Directory, a seperate online service, can provide simplified identity and access management, security reporting and single sign-on to cloud and on-premises web apps.

What is Azure Active Directory?
Extend your directory to Azure Active Directory
Identity and Access Management

The **Add Relying Party Trust** wizard appears.

3. In the wizard, select the **Claims aware** radio button.



Welcome to the Add Relying Party Trust Wizard

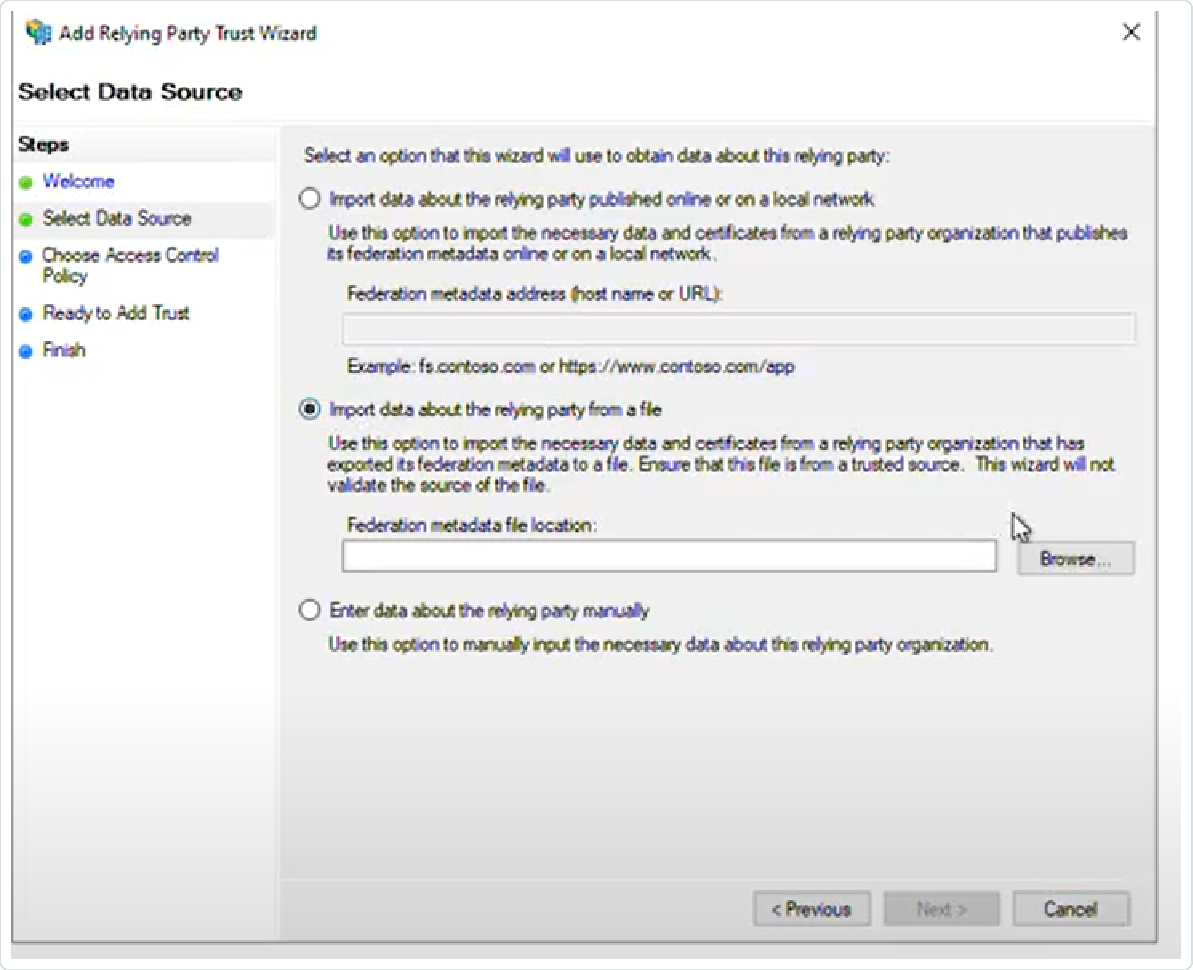
Claims-aware applications consume claims in security tokens to make authentication and authorization decisions. Non-claims-aware applications are web-based and use Windows Integrated Authentication in the internal network and can be published through Web Application Proxy for extranet access. Learn more

● Claims aware

○ Non claims aware

4. Click **Start**.

5. On the **Select Data Source** page, select the **Import data about the relying party from a file** radio button.



Select Data Source

Select an option that this wizard will use to obtain data about this relying party:

○ Import data about the relying party published online or on a local network

Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata online or on a local network.

Federation metadata address (host name or URL):

Example: fs.contoso.com or https://www.contoso.com/app

● Import data about the relying party from a file

Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file.

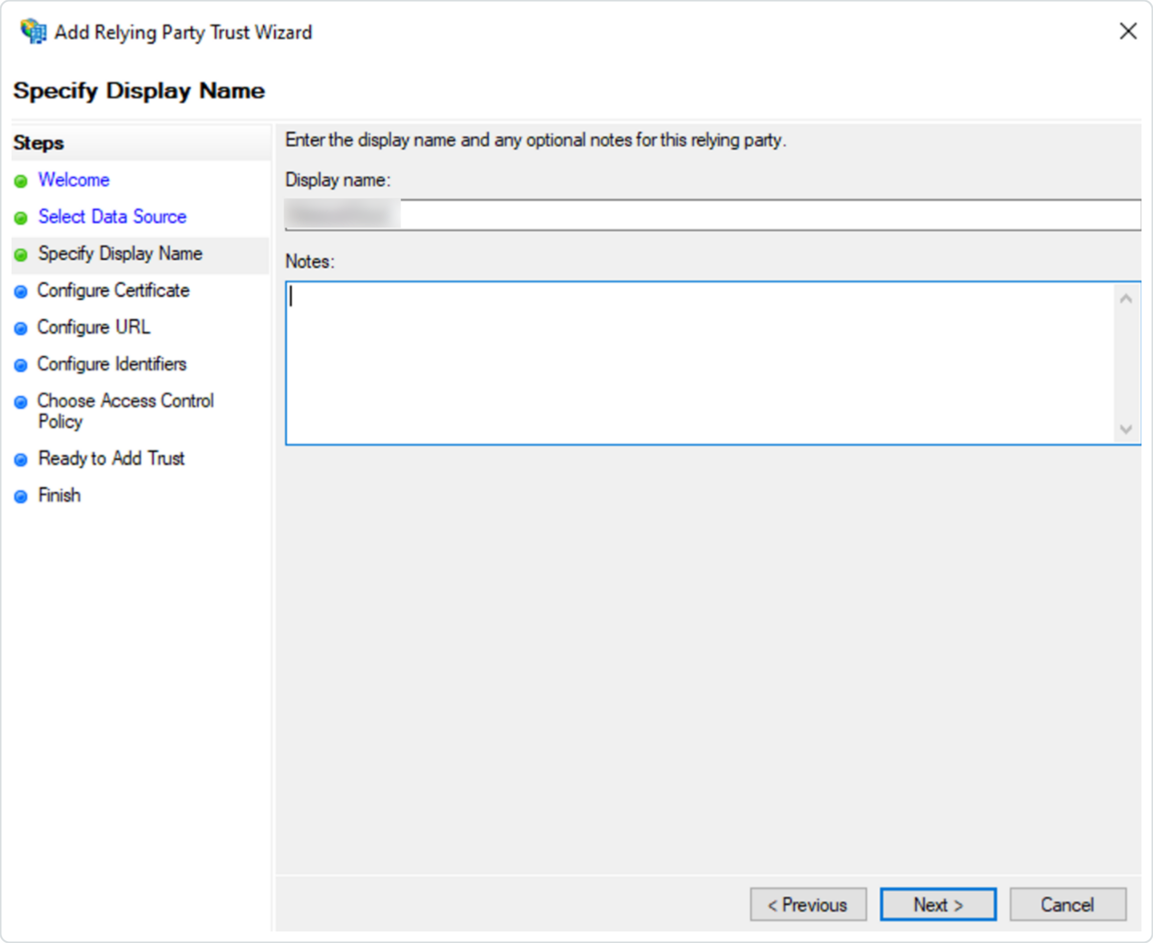
Federation metadata file location:

○ Enter data about the relying party manually

Use this option to manually input the necessary data about this relying party organization.

6. Click the **Browse** button.
7. In your file manager, select the Service Provider metadata.xml file that you downloaded from Tenable Security Center.

   Microsoft ADFS imports the metadata from the file.
8. Click **Next**.
9. On the **Specify Display Name** page, type a **Display Name** and any **Notes** you want to include.



Add Relying Party Trust Wizard

Specify Display Name

Enter the display name and any optional notes for this relying party.

Display name: [redacted]

Notes:

10. Click **Next**.

11. On the **Choose Access Control Policy** page, select **Permit Everyone**

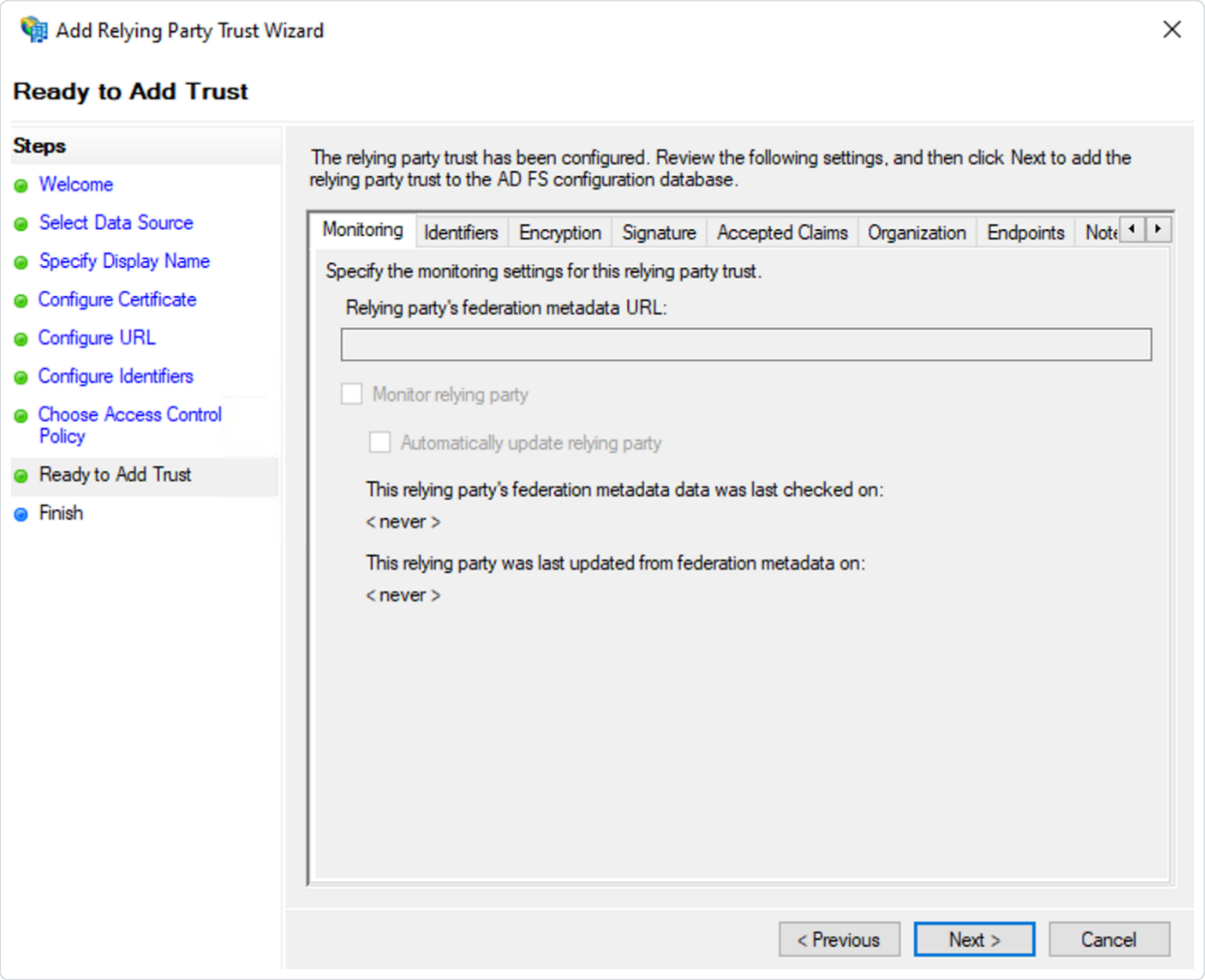
12. Click **Next**.

13. On the **Configure Identifiers** page, on the Identifiers tab, ensure the **Relying party trust identifier** lists the following:

```
https://tenable.sc
```

14. Click **Next**.

15. On the **Ready to Add Trust** page, review your configuration.



Add Relying Party Trust Wizard

Ready to Add Trust

The relying party trust has been configured. Review the following settings, and then click Next to add the relying party trust to the AD FS configuration database.

Specify the monitoring settings for this relying party trust.

Relying party's federation metadata URL:

□ Monitor relying party

□ Automatically update relying party

This relying party's federation metadata data was last checked on:

< never >

This relying party was last updated from federation metadata on:

< never >

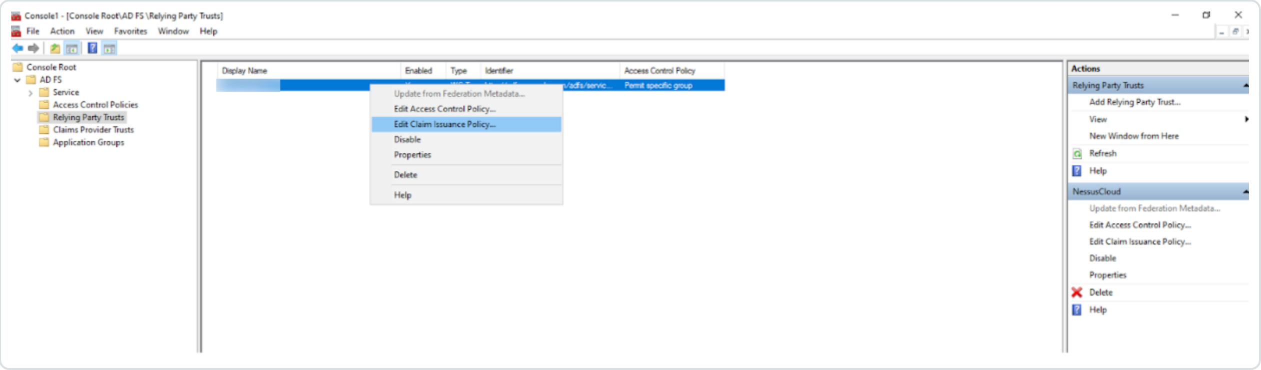
16. Click **Next**.

17. On the **Finish** page, select the **Configure claims insurance policy for this application** checkbox.

18. Click **Close**.

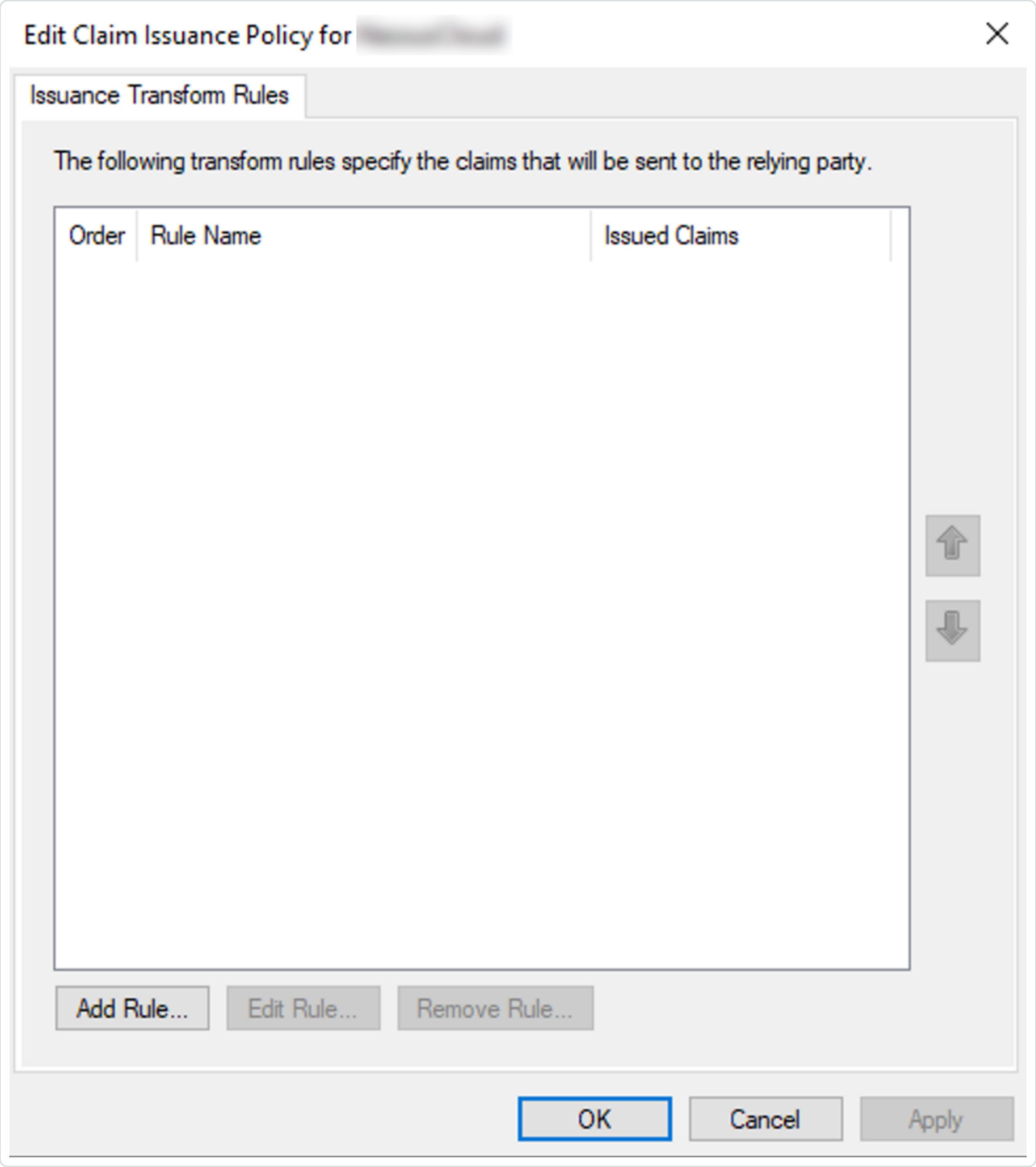
    You return to the **Relying Party Trusts** folder.

19. Right-click the trust you created and select **Edit Claim Issuance Policy**.



The **Edit Claims Issuance Policy** window appears.

20. Click **Add Rule**.


Edit Claim Issuance Policy for [redacted]

The following transform rules specify the claims that will be sent to the relying party.

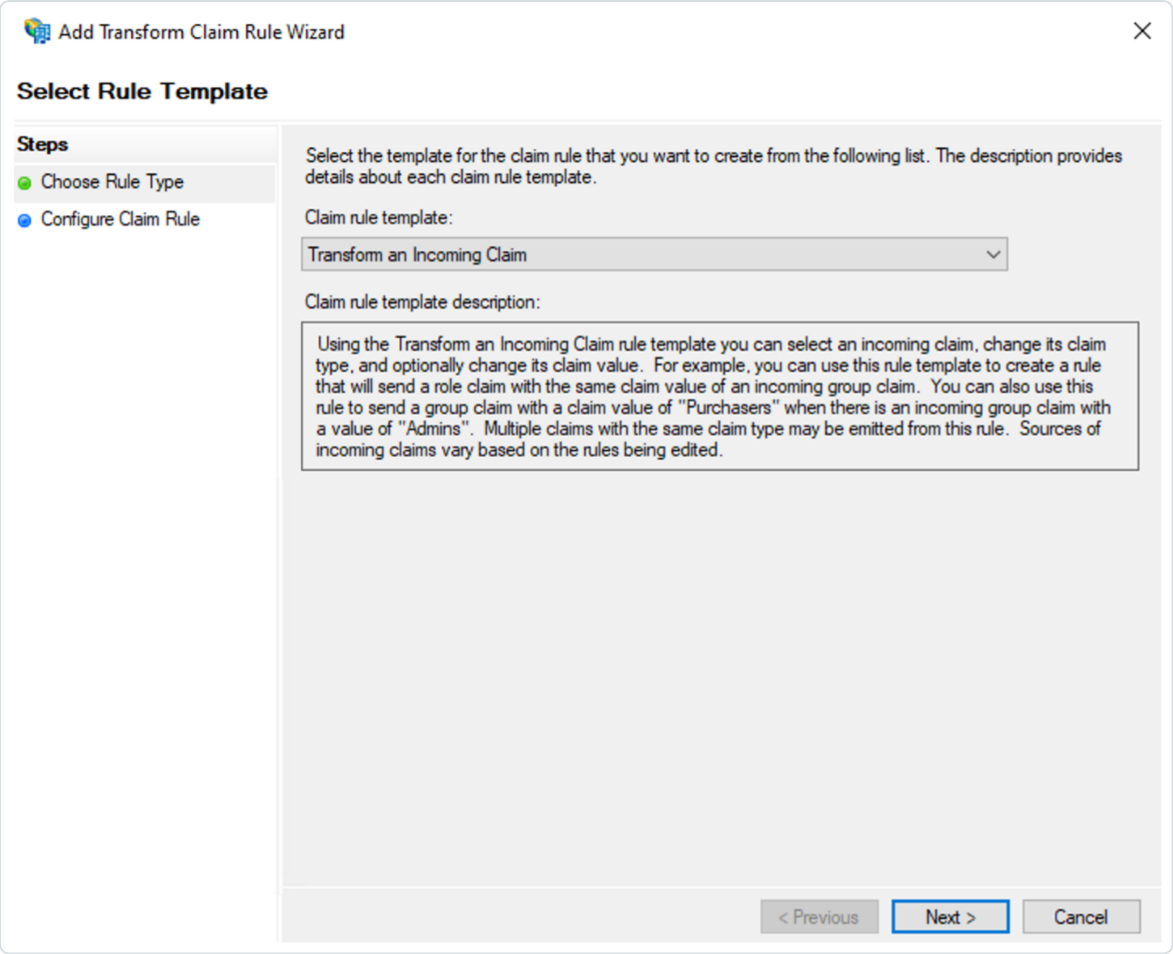
Order	Rule Name	Issued Claims

The **Transform Claim Rule** wizard appears.

21. Configure two rules:

- Rule one:

  a. On the **Select Rule Template** page, in the **Claim rule template** drop-down, select **Transform an Incoming Claim**.



Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.

Claim rule template:

Transform an Incoming Claim

Claim rule template description:

Using the Transform an Incoming Claim rule template you can select an incoming claim, change its claim type, and optionally change its claim value. For example, you can use this rule template to create a rule that will send a role claim with the same claim value of an incoming group claim. You can also use this rule to send a group claim with a claim value of "Purchasers" when there is an incoming group claim with a value of "Admins". Multiple claims with the same claim type may be emitted from this rule. Sources of incoming claims vary based on the rules being edited.

  b. Click **Next**.

  c. On the **Configure Rule** page, configure the following settings:

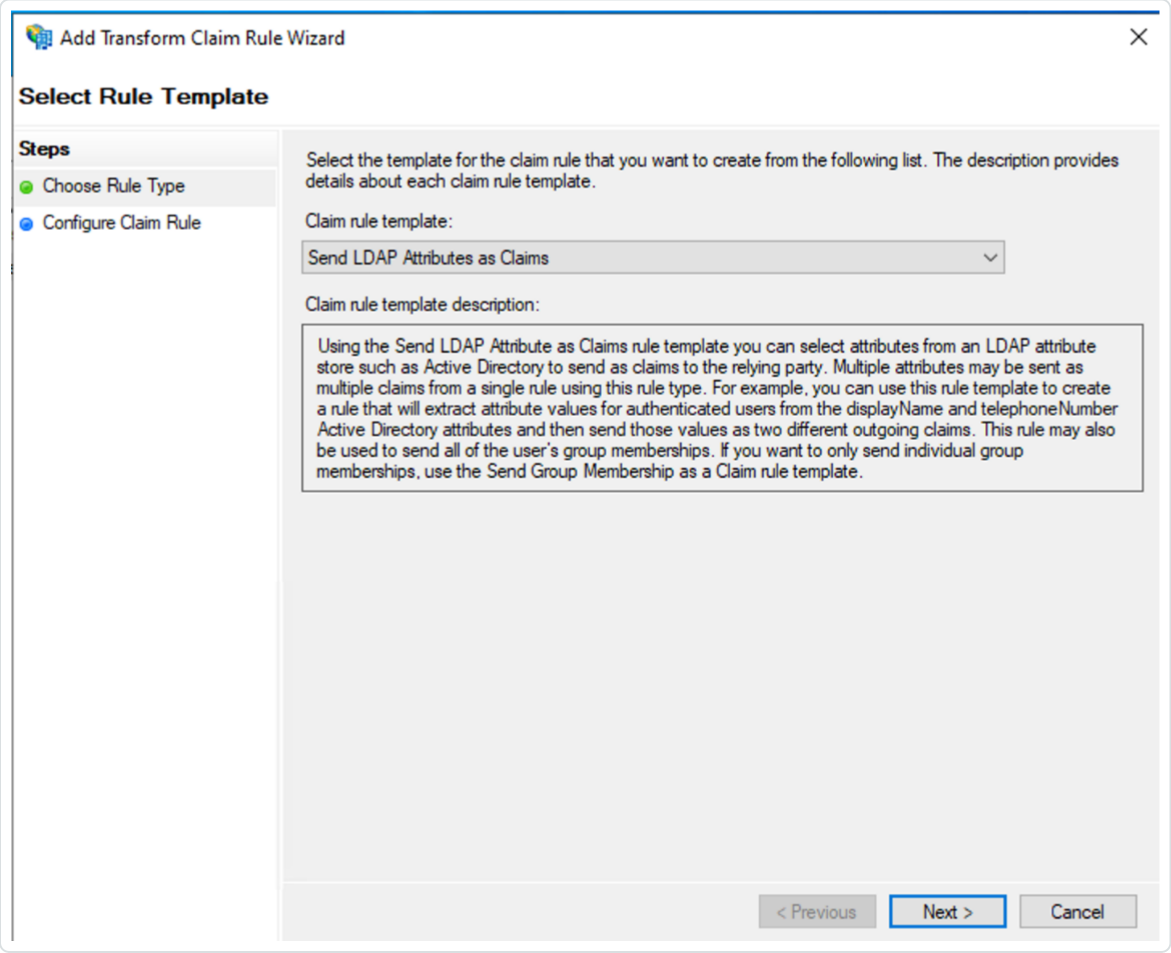
    - **Claim rule name**
    - **Incoming claim type** — select **Email address** or **UPN**.
    - **Outgoing claim type** — select **Name ID**

- **Outgoing name ID format** — select **Transient Identifier**
- **Pass through all claim values** radio button — select radio button

d. Click **Finish**.

- Rule one:

a. On the **Select Rule Template** page, in the **Claim rule template** drop-down, select **Send LDAP Attributes as Claims**.



Add Transform Claim Rule Wizard

Select Rule Template

Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.

Claim rule template: Send LDAP Attributes as Claims

Claim rule template description:

Using the Send LDAP Attribute as Claims rule template you can select attributes from an LDAP attribute store such as Active Directory to send as claims to the relying party. Multiple attributes may be sent as multiple claims from a single rule using this rule type. For example, you can use this rule template to create a rule that will extract attribute values for authenticated users from the displayName and telephoneNumber Active Directory attributes and then send those values as two different outgoing claims. This rule may also be used to send all of the user's group memberships. If you want to only send individual group memberships, use the Send Group Membership as a Claim rule template.

b. Click **Next**.

c. On the **Configure Rule** page, configure the following settings:

- **Claim rule name**
- **Attribute store** — Select **Active Directory**
- **LDAP Attribute** — Select **E-Mail Addresses**.
- **Outgoing Claim Type**, select **E-Mail Addresses**.

d. Click **Finish**.

You return to the **Edit Claims Issuance Policy** window.

22. Click **Apply**.

23. Click **OK**.

Microsoft ADFS saves your changes, and your SAML configuration is ready for use.

Additional Resources

For more information on Microsoft ADFS IdP configuration, see the following resources:

- Microsoft ADFS Overview
- Microsoft ADFS Developer Portal
- Use a SAML 2.0 IdP for Single Sign On

SAML for Tenable One

You can configure Tenable One products to accept credentials from your SAML identity provider. This allows for an additional layer of security, where the SAML credentials are certified for use within Tenable One. Once you enable SAML for a user, they can log in to Tenable One directly through their identity provider, which automatically signs them in and redirects them to the Tenable One Workspace landing page.

These instructions apply to the Tenable One product suite as well as the following products purchased individually. For more information, see the table on the Welcome page.

- Tenable Vulnerability Management
- Tenable Web App Scanning

- Tenable Cloud Security
- Tenable Attack Surface Management

While several configuration steps occur directly in the Tenable user interface, the entire SAML configuration process includes several processes across multiple applications. This guide describes three of the most commonly used Identity Providers (IdPs) and how to configure them for use with Tenable One SAML from start to finish.

Important: Because Tenable One cannot accept private keys to decrypt SAML assertions, Tenable One does not support SAML assertion encryption. If you want to configure SAML authentication in Tenable One, choose an identity provider that does not require assertion encryption and confirm that assertion encryption is not enabled.

To get started, see the following topics:

- Tenable One: Okta IdP
- Tenable One: Ping Identity IdP
- Tenable One: Google Workspace IdP
- Tenable One: Microsoft Entra ID IdP
- Troubleshooting and Common Errors

SAML for Tenable One

You can configure Tenable One products to accept credentials from your SAML identity provider. This allows for an additional layer of security, where the SAML credentials are certified for use within Tenable One. Once you enable SAML for a user, they can log in to Tenable One directly through their identity provider, which automatically signs them in and redirects them to the Tenable One Workspace landing page.

These instructions apply to the Tenable One product suite as well as the following products purchased individually. For more information, see the table on the Welcome page.

- Tenable Vulnerability Management
- Tenable Web App Scanning

- Tenable Cloud Security
- Tenable Attack Surface Management

While several configuration steps occur directly in the Tenable user interface, the entire SAML configuration process includes several processes across multiple applications. This guide describes three of the most commonly used Identity Providers (IdPs) and how to configure them for use with Tenable One SAML from start to finish.

> **Important:** Because Tenable One cannot accept private keys to decrypt SAML assertions, Tenable One does not support SAML assertion encryption. If you want to configure SAML authentication in Tenable One, choose an identity provider that does not require assertion encryption and confirm that assertion encryption is not enabled.

To get started, see the following topics:

- Tenable One: Okta IdP
- Tenable One: Ping Identity IdP
- Tenable One: Google Workspace IdP
- Tenable One: Microsoft Entra ID IdP
- Troubleshooting and Common Errors

SAML for Tenable One

You can configure Tenable One products to accept credentials from your SAML identity provider. This allows for an additional layer of security, where the SAML credentials are certified for use within Tenable One. Once you enable SAML for a user, they can log in to Tenable One directly through their identity provider, which automatically signs them in and redirects them to the Tenable One Workspace landing page.

These instructions apply to the Tenable One product suite as well as the following products purchased individually. For more information, see the table on the Welcome page.

- Tenable Vulnerability Management
- Tenable Web App Scanning

- Tenable Cloud Security
- Tenable Attack Surface Management

While several configuration steps occur directly in the Tenable user interface, the entire SAML configuration process includes several processes across multiple applications. This guide describes three of the most commonly used Identity Providers (IdPs) and how to configure them for use with Tenable One SAML from start to finish.

Important: Because Tenable One cannot accept private keys to decrypt SAML assertions, Tenable One does not support SAML assertion encryption. If you want to configure SAML authentication in Tenable One, choose an identity provider that does not require assertion encryption and confirm that assertion encryption is not enabled.

To get started, see the following topics:

- Tenable One: Okta IdP
- Tenable One: Ping Identity IdP
- Tenable One: Google Workspace IdP
- Tenable One: Microsoft Entra ID IdP
- Troubleshooting and Common Errors

SAML for Tenable One

You can configure Tenable One products to accept credentials from your SAML identity provider. This allows for an additional layer of security, where the SAML credentials are certified for use within Tenable One. Once you enable SAML for a user, they can log in to Tenable One directly through their identity provider, which automatically signs them in and redirects them to the Tenable One Workspace landing page.

These instructions apply to the Tenable One product suite as well as the following products purchased individually. For more information, see the table on the Welcome page.

- Tenable Vulnerability Management
- Tenable Web App Scanning

- Tenable Cloud Security
- Tenable Attack Surface Management

While several configuration steps occur directly in the Tenable user interface, the entire SAML configuration process includes several processes across multiple applications. This guide describes three of the most commonly used Identity Providers (IdPs) and how to configure them for use with Tenable One SAML from start to finish.

> **Important:** Because Tenable One cannot accept private keys to decrypt SAML assertions, Tenable One does not support SAML assertion encryption. If you want to configure SAML authentication in Tenable One, choose an identity provider that does not require assertion encryption and confirm that assertion encryption is not enabled.

To get started, see the following topics:

- Tenable One: Okta IdP
- Tenable One: Ping Identity IdP
- Tenable One: Google Workspace IdP
- Tenable One: Microsoft Entra ID IdP
- Troubleshooting and Common Errors

Troubleshooting and Common Errors

General Troubleshooting

Ensure the IdP information includes the following:

- SSO URL/Login URL/Reply URL: The URL provided by Tenable (for example, https://cloud.tenable.com/saml/login/xxxxxxxxxxxxxxxxxxxxx)
- Recipient URL = The recipient URL provided by Tenable (as listed above)
- Destination URL = The destination URL provided by Tenable (as listed above)
- Audience Restriction (Entity ID) = A unique ID per SAML configuration.

- Check if the NameID parameter is set to Unspecified. Sometimes this works initially because the default was “user.email”, but in some cases may need to be reconfigured:
  - Choose the NameID format and the application username sent to your application in the SAML response (for example EmailAddress and Email)
  - In the Attribute Statements (optional) section, type the SAML attributes to be shared with your application. For example:
    - Name (in SAML application) Value (in Idp profile)
    - FirstName user.firstName
    - LastName user.lastName
    - Email user.email (edited)

Common IdP Misconfigurations

Reminder: Tenable does not support SP-Initiated SAML flow.

- Tenable SAML is IdP-initiated. As such, the most common errors are due to IdP misconfiguration. The most common errors are an incorrect Entity ID or attempting to log in with a username that is not in the correct format (user@domain.com).
- If user auto provisioning is disabled, ensure the user already exists in the container where the SAML configuration was created.
- Ensure that the certificate setup in the IdP configuration matches the certificate in the SP (Tenable application SAML) configuration, otherwise, the SP (Tenable application) rejects authentication.
- If there are multiple SAML configurations for the same container, ensure the correct SP metadata is uploaded to the correct/matching IdP configuration that the IdP metadata was originally provided from.

Error Messaging

The following are some of the most common IDP misconfiguration errors:

“incorrectly signed, or missing field”

This error typically indicates something is wrong with the certificate/s in the idp.xml file. Since Tenable currently only uses the top certificate in the file, this error could indicate your XML certificates are out of order. Identify the primary certificate with the customer. Usually, you can mitigate this error by manually selecting the correct certificate within the Tenable product.

Alternatively, the certificate may be expired. Inspect the file and make sure it does not include any expired certificates.

“This Username does not exist.”

Verify the following:

- The NameID
- The transform claim rule for the incoming claim is set to Email
- The outgoing claim type is configured to NameID

The signature may be showing as not validated in Splunk. Work with Tenable Support to use the correct certificate.

{"statusCode":401,"error":"Unauthorized","message":"Missing authentication"}

This error is usually caused because the user is not a part of the correct group configured within their IdP. Review the instructions for your IdP and ensure that the appropriate users and groups are created within your IdP so they can be linked to your Tenable application.

“{"error":"SAML login attempt failed."}”

The container has likely expired. Contact Tenable Support to review the Splunk logs for supporting information.

If the error includes the following warning:

```
WARN [2022-xxxxx 13:38:06,520][dw-38 - POST /saml/login/xxxxxxxxxxx][X-
Request-Uuid=xxxxxxxxxxxx][c.t.c.w.m.manager.UserManager] id-269: user-
```

```
locate: Could not find a user: CacheLoader returned null for key
(usernamexxxxxxxx)
```

Their IDP.xml file is passing what appears to be just {lastname}{firstname_firsttwo} instead of {lastname}{firstname_firsttwo}@{domain}. The customer must adjust their claim and/or transform rules accordingly.

“{"error":"SAML login attempt failed - the SAML IdP configuration was found, but no username could be extracted from the SAML message (could be incorrectly signed, or missing a field)."}”

The following error in Splunk indicates SAML was not configured when the user attempted to log in with their username and password.

```
User[username=xxxxxxx@domain.com] is not permitted to authenticate with a
password
```

“SAML validation failed against container xxxxxx-xxxxxxxxxx- org.opensaml.xml.validation. ValidationException: Assertion audience does not include issuer”

The problem is with the customer SAML assertion configuration. In the IDP.xml file, check the Audience URI or SP Entity ID parameters. Additionally, verify the NameID parameter is in the correct format.

Example: Manually Verify a SAML Payload

The following code block is an example of a payload that could be used to manually verify a payload from any IdP.

```
<samlp:Response xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" ID="pfxb5fecfdb-d5fa-15d3-b5ad-
11b536934de7" Version="2.0" IssueInstant="2024-07-
18T18:24:35Z"><saml:Issuer>https://app.onelogin.com/saml/metadata/b9eb8883-9b3e-46c9-9a45-
5f7416126842</saml:Issuer><ds:Signature
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"><ds:SignedInfo><ds:CanonicalizationMethod
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/><ds:SignatureMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/><ds:Reference URI="#pfxb5fecfdb-
```

```
d5fa-15d3-b5ad-11b536934de7"><ds:Transforms><ds:Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/><ds:Transform
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/></ds:Transforms><ds:DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/><ds:DigestValue>8V8eFYjAL6I41w9JYDINV
sr4AZo=</ds:DigestValue></ds:Reference></ds:SignedInfo><ds:SignatureValue>...</ds:SignatureV
alue><ds:KeyInfo><ds:X509Data><ds:X509Certificate>MIID3...</ds:X509Certificate></ds:X509Data>
</ds:KeyInfo></ds:Signature><samlp:Status><samlp:StatusCode
Value="urn:oasis:names:tc:SAML:2.0:status:Success"/></samlp:Status><saml:Assertion
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance" Version="2.0" ID="pfx1f4d6d80-506e-e027-c18c-5e85ac6d924d" IssueInstant="2024-07-
18T18:24:35Z"><saml:Issuer>https://app.onelogin.com/saml/metadata/b9eb8883-9b3e-46c9-9a45-
5f7416126842</saml:Issuer><ds:Signature
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"><ds:SignedInfo><ds:CanonicalizationMethod
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/><ds:SignatureMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/><ds:Reference URI="#pfx1f4d6d80-
506e-e027-c18c-5e85ac6d924d"><ds:Transforms><ds:Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/><ds:Transform
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/></ds:Transforms><ds:DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/><ds:DigestValue>clPz/vMiLfFvQZE1E3fmgV
O68DA=</ds:DigestValue></ds:Reference></ds:SignedInfo><ds:SignatureValue>U1glVB...</ds:Signa
tureValue><ds:KeyInfo><ds:X509Data><ds:X509Certificate>MIID3DCCA...</ds:X509Certificate></ds:
X509Data></ds:KeyInfo></ds:Signature><saml:Subject><saml:NameID
Format="urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress">saml_jit_
test@tenable.com</saml:NameID><saml:SubjectConfirmation
Method="urn:oasis:names:tc:SAML:2.0:cm:bearer"><saml:SubjectConfirmationData
NotOnOrAfter="2024-07-18T18:27:35Z"
Recipient=""/></saml:SubjectConfirmation></saml:Subject><saml:Conditions NotBefore="2024-07-
18T18:21:35Z" NotOnOrAfter="2024-07-
18T18:27:35Z"><saml:AudienceRestriction><saml:Audience>TENABLE_IO_e0eafdb2-e306-4ce7-
b87d-
c17f760cb717</saml:Audience></saml:AudienceRestriction></saml:Conditions><saml:AuthnStatem
ent AuthnInstant="2024-07-18T18:24:34Z" SessionNotOnOrAfter="2024-07-19T18:24:35Z"
SessionIndex="_2e134fe6-aa86-49c7-9eb1-
```

```
0d29a683ed1c"><saml:AuthnContext><saml:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport</saml:AuthnContextClassRef></saml:AuthnContext></saml:AuthnStatement><saml:AttributeStatement><saml:Attribute
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
Name="groups"><saml:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">SOME_AD_GROUP</saml:AttributeValue></saml:Attribute></saml:AttributeStatement></saml:Assertion></samlp:Response>
```

Important! The attribute name, `groups`, and its value, must match the group name you set within your application. For reference, see the following snippet from the above code block:
`<saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" Name="groups"><saml:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">GROUP_NAME</saml:AttributeValue></saml:Attribute>`