

ManageEngine  
**ADAudit Plus**

# ADAudit Plus Single Sign-On



# Table of Contents

1. NTLM authentication	1
1.1 To enable NTLM-based single sign-on	1
1.2 To modify existing single sign-on settings	2
1.3 Troubleshooting steps for NTLM-based SSO	3
1.3.1 Change browser settings to allow single sign-on	3
1.3.2 Check the computer account configuration	4
2. SAML authentication	5
2.1 Configuring single sign-on to ADAudit Plus using Okta	5
2.2 Configuring single sign-on to ADAudit Plus using OneLogin	6
2.3 Configuring single sign-on to ADAudit Plus using Ping Identity	8
2.4 Configuring single sign-on to ADAudit Plus using Active Directory Federation Services (AD FS)	9
2.5 Configuring single sign-on to ADAudit Plus using a custom identity provider	15
2.5.1 Configuring single sign-on to ADAudit Plus using any custom identity provider	15
2.5.2 Configuring single sign-on to ADAudit Plus using Azure	16
2.6 Troubleshooting tips for SAML-based SSO	19

# 1. NTLM authentication

## 1.1 To enable NTLM-based single sign-on

**Note:**

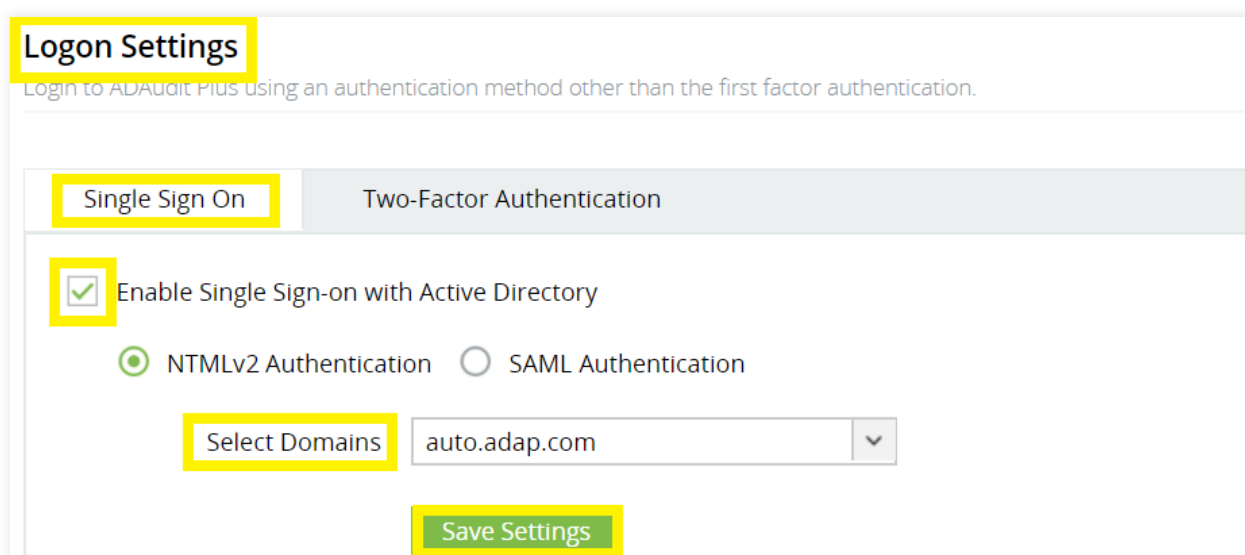
ADAudit Plus uses Jespa for NTLMv2 SSO authentication. In builds 7082 and above, the Jespa JAR file has to be downloaded and added to ADAudit Plus' lib folder before enabling NTLMv2 SSO. To do this:

1. Download the latest [Jespa JAR file](#).
2. Extract the downloaded ZIP file, move the JAR files to <Installation\_folder>\ManageEngine\ADAudit Plus\lib, and restart ADAudit Plus.

If you are running build 7081 or older and have NTLMv2 SSO enabled, you can continue using this feature without any changes.

**To enable NTLM-based single sign-on:**

1. Log in to the ADAudit Plus web console.
2. Navigate to Admin > Administration > Logon Settings.
3. Check the Enable Single Sign-On box.
4. Select the domains from the *Select Domains* drop-down. These are the domains that contain the user accounts used to access ADAudit Plus.
5. Click Save Settings.



**Logon Settings**

Login to ADAudit Plus using an authentication method other than the first factor authentication.

**Single Sign On** Two-Factor Authentication

☒ Enable Single Sign-on with Active Directory

☒ NTLMv2 Authentication ☐ SAML Authentication

**Select Domains** auto.adap.com

**Save Settings**

### Note:

If ADAudit Plus is installed as a service, ensure that ADAudit Plus is run using a service account with admin privileges:

- Click **Start > Run > Type services.msc**.
- Locate the **ManageEngine ADAudit Plus** service.
- Right-click on the **service**, and select **Properties > Log On > This account**.
- Check if suitable credentials are used. If not, enter suitable credentials.

## 1.2 To modify existing single sign-on settings

1. Log in to the ADAudit Plus web console.
2. Navigate to **Admin > Administration > Logon Settings**.
3. Click on the domain that you wish to modify the settings for.

Domain	Computer Account	Status
adapauto	ADSCOMPUTERIXB	Configured

4. In the *Modify computer account* window that pops-up, enter the **Computer Name** and **Password** in the respective fields.
5. If the computer is not already in the domain, check the box next to **Create this computer account in the domain** to create a computer with the provided credentials.
6. Under *Advanced*, if the **DNS Servers** and **DNS Site** are not filled automatically after entering the computer name and password, enter them manually.
7. Click **Save**.

**Note:**

- To find the IP address of the DNS server: Open Command Prompt from a machine belonging to the domain that you have selected, type `ipconfig /all` and press **Enter**. The first IP address displayed under *DNS Server* is the IP address of the DNS server.
- To identify the DNS site: Open Active Directory Sites and Services on the left tree, expand *Sites*, and identify the site on which the Domain Controller configured under the selected domain appears. This is the DNS site.

**Modify computer account** adapauto

! A computer account is mandatory to configure SSO using NTLM. [Learn more...](#)

Domain: adapauto

\* Computer Name: ADSCOMPUTERLXB  
eg: testaccount

\* Password: .....

☒ Create this computer account in the domain

**Advanced**

DNS Servers: 172.24.156.241  
eg: 192.168.1.1

DNS Site: Default-First-Site-Name  
eg: Nearest Site

**Save** Cancel

## 1.3 Troubleshooting steps for NTLM-based SSO

### 1.3.1 Change browser settings to allow single sign-on

Trusted sites are the sites in which NTLM authentication can occur seamlessly. If SSO has failed, then the most probable cause is that ADAudit Plus isn't a part of your browser's trusted sites.

To add the URLs of ADAudit Plus in the trusted sites list, follow the steps given below:

**Internet Explorer (IE):**

1. Open Internet Explorer, and click on Tools located in the top right-hand corner of the screen.  
Then go to Internet Options > Security. Under *Select a zone to view or change security settings*, select Local Intranet > Sites.
2. If you're using any versions lower than IE 11, add the URL of ADAudit Plus to the list of intranet sites.  
If you're using IE 11, click on Advanced, and add the URL of ADAudit Plus to the list of intranet sites.
3. Click Close > OK. Finally, close all browser sessions, and reopen the browser.

**Google Chrome**

1. Open Control Panel > Network and Internet > Internet Options. In the Internet Properties window that opens, click Security > Local Intranet > Sites > Advanced, and add the URL of ADAudit Plus to the list of intranet sites.
2. Click Close > OK. Finally, close all browser sessions, and reopen the browser.

**Mozilla Firefox**

1. Open Firefox, and type about:config in the address bar. Click Accept the risk and continue.  
In the search field, type network.automatic-ntlm-auth.trusted-uris.  
Click the edit icon next to network.automatic-ntlm-auth.trusted-uris, and type the URL of ADAudit Plus. Use a comma to separate multiple URLs.
2. Click OK. Finally, close all browser sessions, and reopen the browser.

**Note:**

- It's recommended that you close all browser sessions after adding the URL to the trusted sites list for the changes to take effect.
- Google Chrome and Internet Explorer use the same internet settings. Changing the settings either in Internet Explorer or in Chrome will enable NTLM SSO in both browsers.

**1.3.2 Check the computer account configuration**

Status: Error in Creating Computer Account. This error can be due to any of the reasons listed below:

**1. Invalid domain credentials in ADAudit Plus**

The credentials of the user account specified in the domain settings section might have expired.

To update the credentials:

- Log in to the ADAudit Plus web console with admin credentials.
- Click on Domain Settings, hover over the relevant domain, click on Modify credentials, and update the username and password.

## 2. Domain controllers (DC) are not accessible from ADAudit Plus

ADAudit Plus might not be able reach the specified DCs. To add another DC that ADAudit Plus can access:

- Log in to the **ADAudit Plus web console** with admin credentials.
- Click **Domain Settings**, select the relevant domain, click **Add Domain Controller**, and specify the name of the relevant DC.

## 3. Non-conformance to password policy

The password of the automatically created computer accounts for NTLM authentication might not be meeting the domain password policy settings. To create a computer account manually and assign it a password that meets the complexity requirements of the domain policy settings, follow the steps given below:

- Log in to **ADAudit Plus web console** with admin credentials. Navigate to **Admin > Administration > Logon Settings > Single Sign-On**. Check the box next to **Enable Single Sign-On**, and select **NTLMv2 Authentication**.
- Click on the error message **Error in creating a new computer account** in the status column next to the domain in which you wish to create a computer account.
- Create a computer account manually by entering a **Computer Name** and **Password**.

# 2. SAML authentication

You can set up single sign-on to access ADAudit Plus through any of these popular identity providers.

### Note:

SAML-based SSO cannot be enabled if a reverse proxy is enabled.

## 2.1 Configuring single sign-on to ADAudit Plus using Okta

### Step 1: Configure ADAudit Plus in Okta

1. Log in to the Okta portal.
2. Under the *Apps* tab, click **Add Application > Create New App**.
3. Select **Web** as the *Platform* and **SAML 2.0** as the *Sign on method*, and click **Create**.
4. In *General Settings*, enter the **SAML application name** (for example, **ADAudit Plus**) in the *App name* field. Upload a logo for the application if needed, and click **Next**.
5. In the *Configure SAML* section, enter the values for: **Single sign on URL** and **Audience URL**.
6. Click **Finish**.

### Note:

- To find the values for the Single sign-on URL and Audience URI, log in to the ADAudit Plus console, navigate to **Admin > Administration > Logon Settings > Single Sign-On**. Check the box next to **Enable Single Sign-On**, and select **SAML Authentication > Identity Provider (IdP) > Okta**. Copy the **ACS/Recipient URL** value, and paste it in the *Single sign-on URL* field. Copy the **Issuer URL/Entity ID** value, and paste it in the *Audience URI* field.
7. Once the configuration is complete, navigate to the **Sign on** tab to download the identity provider metadata file.

**Step 2: Configure Okta in ADAudit Plus**

1. Log in to the ADAudit Plus web console with admin credentials. Navigate to Admin > Administration > Logon Settings > Single Sign-On. Check the box next to Enable Single Sign-On, and select SAML Authentication.
2. Select Okta from the *Identity Provider (IdP)* drop-down. Under *SAML Configuration Mode*, select Upload Metadata File. Click Browse and upload the metadata file obtained at the end of the Step 1.
3. If you want to enable single logout, follow these steps:
  - Copy the Issuer URL/Entity ID and SP Logout URL, and download the X.509 Certificate.
  - Log in to Okta, go to the Configure SAML page, and click Show Advanced Settings.
  - Check the Enable Single Logout option, paste the Issuer URL/Entity ID in *SP Issuer* field and the SP Logout URL in the *Single Logout URL* field.
  - Click Browse next to *Signature Certificate*, and select the X.509 Certificate you downloaded.
  - Click Upload Certificate.
4. Click Save.

The screenshot shows the ADAudit Plus configuration interface for Single Sign-On. The 'Single Sign On' tab is active. The 'Enable Single Sign-on with Active Directory' checkbox is checked. Under 'SAML Authentication', the 'Upload Metadata File' radio button is selected. In the 'Configure Identity Provider' section, 'Okta' is selected for the Identity Provider (IdP). The 'SAML Configuration Mode' is set to 'Upload Metadata File'. The 'Browse' button next to the file upload field is highlighted. In the 'Service Provider (SP) Details' section, the 'Issuer URL/Entity ID' and 'SP Logout URL' fields are highlighted. The 'ACS/Recipient URL' field contains 'http://john-4419:8081/samlLogin/5'. The 'Download X.509 Certificate' link is also highlighted.

## 2.2 Configuring single sign-on to ADAudit Plus using OneLogin

**Step 1: Configure ADAudit Plus in OneLogin**

1. Log in to the OneLogin portal.
2. Click on the Apps tab, select Add Apps > SAML Test Connector (IdP).
3. Enter the Display Name, and upload the icon for the application. Click Save.



- Under the *Configuration* tab, enter the values for ACS (Consumer) URL Validator and ACS (Consumer) URL.

**Note:**

To find the values for the ACS (Consumer) URL Validator and ACS (Consumer) URL, log in to the ADAudit Plus console, navigate to **Admin > Administration > Logon Settings > Single Sign-On**. Check the box next to **Enable Single Sign-On**, and select **SAML Authentication > Identity Provider (IdP) > OneLogin**. Copy the ACS/Recipient URL value, and paste it in these two fields.

- Click **More Actions** in the top panel. Click **SAML Metadata** to download the metadata file, and click **Save**.

**Step 2: Configure OneLogin in ADAudit Plus**

- Log in to the ADAudit Plus web console with admin credentials. Navigate to **Admin > Administration > Logon Settings > Single Sign-On**. Check the box next to **Enable Single Sign-On**, and select **SAML Authentication**.
- Select **OneLogin** from the *Identity Provider (IdP)* drop-down. Under **SAML Configuration Mode**, select **Upload Metadata File**. Click **Browse**, and upload the metadata file obtained at the end of Step 1.
- If you want to enable Single Logout, copy the **SP Logout URL** in ADAudit Plus, and paste it in the **Single Logout URL** field in OneLogin's **Configuration** page.
- Click **Save**.

The screenshot shows the 'Logon Settings' page in the ADAudit Plus console. The 'Single Sign On' tab is selected. Under 'Single Sign-On with Active Directory', the checkbox is checked. 'SAML Authentication' is selected. In the 'Configure Identity Provider' section, 'OneLogin' is chosen as the Identity Provider (IdP). 'Upload Metadata File' is selected as the SAML Configuration Mode, and the 'Browse' button is highlighted. In the 'Service Provider (SP) Details' section, the 'SP Logout URL' field is highlighted, showing the value 'http://john-4419:8081/samlLogout/'.

**Logon Settings**  
Login to ADAudit Plus using an authentication method other than the first factor authentication.

**Single Sign On** | Two-Factor Authentication

☒ Enable Single Sign-on with Active Directory

☐ NTMLv2 Authentication ☒ SAML Authentication

**Configure Identity Provider**

Identity Provider (IdP) **OneLogin**

SAML Configuration Mode ☒ Upload Metadata File ☐ Manual Configuration

- Browse file - **Browse** ?

☐ Sign SAML Logout Request ?

☐ Sign SAML Logout Response ?

**Service Provider (SP) Details**

ACS/Recipient URL  ?  
Recipient URL to be configured in IdP.

Issuer URL/Entity ID  ?

**SP Logout URL**  ?

## 2.3 Configuring single sign-on to ADAudit Plus using Ping Identity

### Step 1: Configure ADAudit Plus in Ping Identity

1. Log in to the Ping Identity portal.
2. Click Applications > My Applications > SAML > Add Application > New SAML Application.
3. On the Application Details page, enter Application Name, Application Description, and Category. You can choose to assign an application icon. Click Continue to Next Step.
4. On the Application Configuration page, provide the ACS URL and Entity ID.

**Note:**

To find the values for the ACS URL and Entity ID, log in to the ADAudit Plus console, navigate to Admin > Administration > Logon Settings > Single Sign-On. Check the box next to Enable Single Sign-On, and select SAML Authentication > Identity Provider (IdP) > Ping Identity. Copy the ACS/Recipient URL value, and paste it in the ACS URL field. Copy the Issuer URL/Entity ID value, and paste it in the Entity ID field.

5. Click Save & Publish.
6. Once the configuration is complete, the metadata file can be downloaded.

### Step 2: Configure Ping Identity in ADAudit Plus

1. Log in to the ADAudit Plus web console with admin credentials. Navigate to Admin > Administration > Logon Settings > Single Sign-On. Check the box next to Enable Single Sign-On, and select SAML Authentication.
2. Select Okta from the Identity Provider (IdP) drop-down. Under SAML Configuration Mode, select Upload Metadata File. Click Browse, and upload the metadata file obtained at the end of Step 1.
3. If you want to enable single logout, follow these steps:
  - Copy the SP Logout URL in ADAudit Plus, and paste it in the Single Logout Endpoint field in Ping Identity's SAML Application page.
  - Download the X.509 Certificate in ADAudit Plus. In Ping Identity's SAML Application page, click on Browse next to Primary Verification Certificate, and upload the downloaded certificate.
4. Click Save.

## 2.4 Configuring single sign-on to ADAudit Plus using Active Directory Federation Services (AD FS)

### Step 1: Configure ADAudit Plus in AD FS

#### Prerequisites

To configure AD FS for identity verification in ADAudit Plus, you need:

1. To install the AD FS server. The detailed steps for installing and configuring AD FS can be found in this [Microsoft article](#).
2. An SSL certificate to sign your AD FS login page and the fingerprint for that certificate.

#### Configuration steps

##### Note:

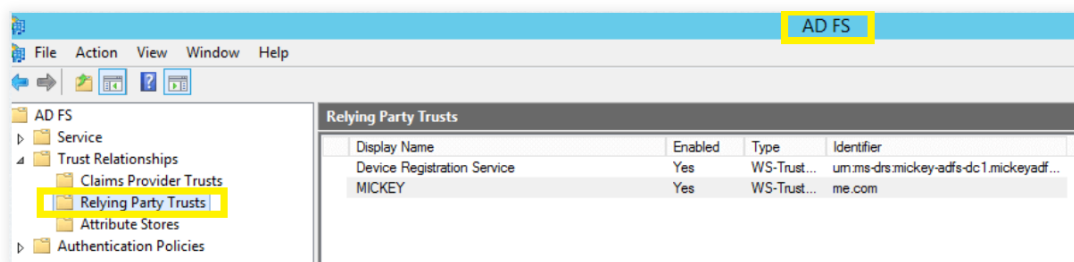
Only the Forms Authentication method is configured for users trying to access ADAudit Plus through AD FS authentication. You can view this setting in the AD FS console under **Authentication Policies > Primary Authentication > Global Settings**.

#### Claim rules and Relying Party Trust

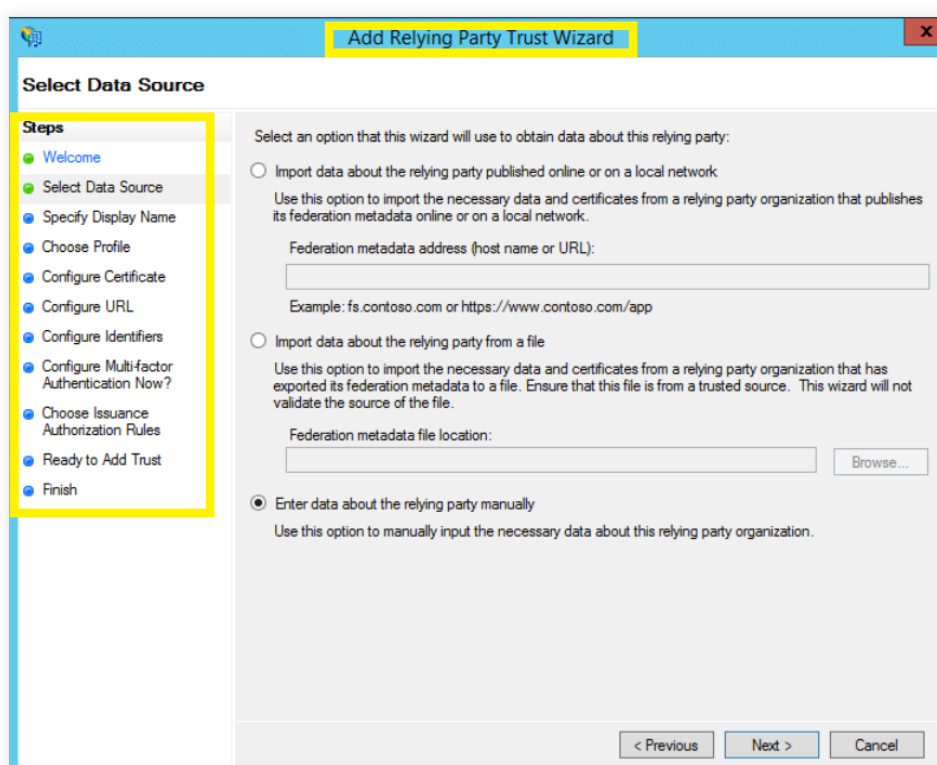
During configuration, you will need to add a Relying Party Trust and create claim rules. A Relying Party Trust is created to establish the connection between two applications for authentication purposes by verifying claims.

In this case, AD FS will trust the relying party (ADAudit Plus) and authenticate users based on the claims generated. Claims are generated from claim rules by applying certain conditions on them. A claim is an attribute that is used for identifying an entity to establish access. For example, the Active Directory SAMAccountName.

1. Open the AD FS Management console.
2. The connection between AD FS and ADAudit Plus is created using a Relying Party Trust (RPT). Select the Relying Party Trusts folder.



3. Click Actions > Add Relying Party Trust. When the *Add Relying Party Trust Wizard* opens, click **Start**.
4. In the *Select Data Source* page, click on **Enter Data About the Party Manually**, and click **Next**.



5. In the **Specify Display Name** page, enter a display name of your choice and add additional notes if required. Click **Next**.
6. In the **Choose Profile** page, click **AD FS profile**. Click **Next**.
7. In the **Configure Certificate** page, the default settings would have already been applied. Click **Next**.

8. In the **Configure URL** page, check the box next to **Enable Support for the SAML 2.0 WebSSO** protocol. The relying party SAML 2.0 SSO service URL will be the ACS URL of ADAudit Plus.

**Note:**

There is no trailing slash at the end of the URL. For example:

https://ADAuditPlus-server/samlLogin/955060d15d6bb8166c13b8b6e10144e5f755c953

To get the ACS URL value, open the ADAudit Plus console, navigate to **Admin >**

**Administration > Logon Settings > Single Sign-On**. Check the box next to **Enable Single Sign-On**, and select **SAML Authentication > Identity Provider (IdP) > ADFS**. You can find the ACS URL/Recipient URL value here.

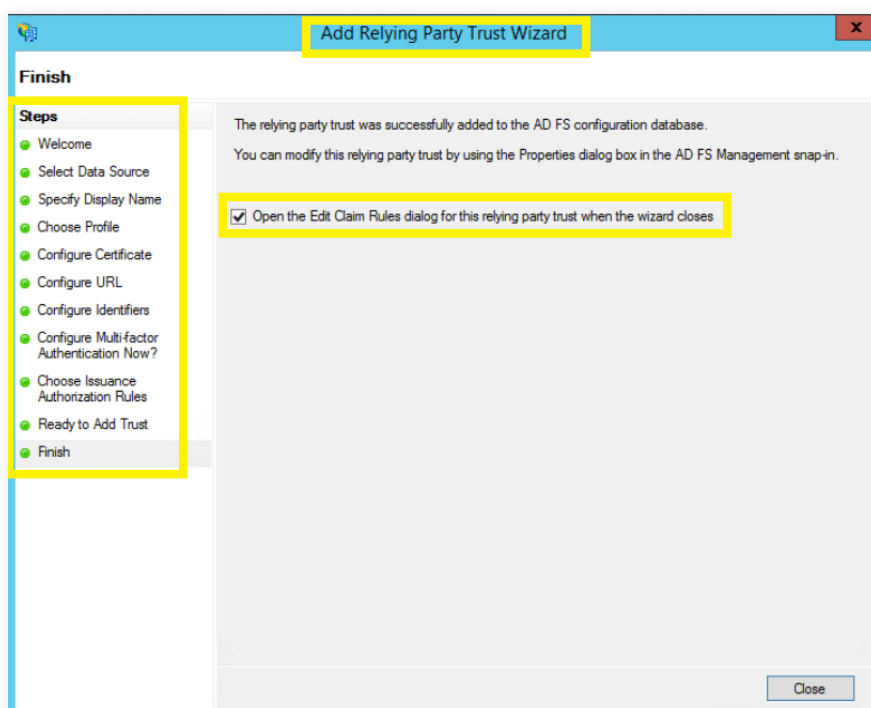
9. On the *Configure Identifiers* page, in the *Relying party trust identifiers* field, paste the Entity ID value.

**Note:**

To find the Entity ID value, log in to the ADAudit Plus console, navigate to **Admin >**

**Administration > Logon Settings > Single Sign-On**. Check the box next to **Enable Single Sign-On**, and select **SAML Authentication > Identity Provider (IdP) > ADFS**. You can find the Entity ID value here.

10. In the *Configure Multi-factor Authentication Now?* page, you can choose to configure multi-factor authentication settings for the relying party trust. Click **Next**.
11. In the *Choose Issuance Authorization Rules* page, you can choose to **Permit all users to access** this relying party. Click **Next**.
12. The next two pages will display an overview of the settings you have configured. In the *Finish* page, click **Close** to exit the wizard.
- Keep the **Open the Edit Claim Rules dialog for this relying party trust when the wizard closes** option selected to open the Claim Rules editor automatically.



13. In *Claim Rules Editor*, under the *Issuance Transform Rules* tab, click **Add Rule**.

14. From the *Claim rule template* drop-down, select **Send LDAP Attributes as Claims**, and click **Next**.

The screenshot shows the 'Add Transform Claim Rule Wizard' dialog box. The title bar is 'Add Transform Claim Rule Wizard'. The main heading is 'Select Rule Template'. On the left, under 'Steps', there are two steps: 'Choose Rule Type' (selected with a green dot) and 'Configure Claim Rule' (with a blue dot). The main area contains instructions: '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.' Below this, 'Claim rule template:' is followed by a dropdown menu showing 'Send LDAP Attributes as Claims'. Under 'Claim rule template description:', there is a text box explaining that this template allows selecting attributes from an LDAP attribute store (like Active Directory) to send as claims. At the bottom, there are buttons for '< Previous', 'Next >', and 'Cancel'.

15. In the *Configure claim rule* page, provide a **Claim rule name**, and select **Active Directory** from the *Attribute store* drop-down. In the *LDAP Attribute* column, select **User-Principal-Name**. In the *Outgoing Claim Type* column, select **Name ID**, and click **Finish**.

The screenshot shows the 'Add Transform Claim Rule Wizard' dialog box, now on the 'Configure Rule' step. The title bar is 'Add Transform Claim Rule Wizard'. The main heading is 'Configure Rule'. On the left, under 'Steps', 'Choose Rule Type' is now greyed out, and 'Configure Claim Rule' is selected with a green dot. The main area contains instructions: 'You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.' Below this, 'Claim rule name:' is followed by a text box containing 'ADAP SSO Claims'. 'Rule template:' is 'Send LDAP Attributes as Claims'. 'Attribute store:' is followed by a dropdown menu showing 'Active Directory'. Below this is a section 'Mapping of LDAP attributes to outgoing claim types:' containing a table. The table has two columns: 'LDAP Attribute (Select or type to add more)' and 'Outgoing Claim Type (Select or type to add more)'. The first row shows 'User-Principal-Name' mapped to 'Name ID'. There is a second row with a '\*' in the first column and an empty dropdown in the second. At the bottom, there are buttons for '< Previous', 'Finish', and 'Cancel'.

LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
User-Principal-Name	Name ID
*	

16. You can now view the rule that has been created. Click OK.

17. Next, download the metadata file by clicking on the Identity Provider metadata link.

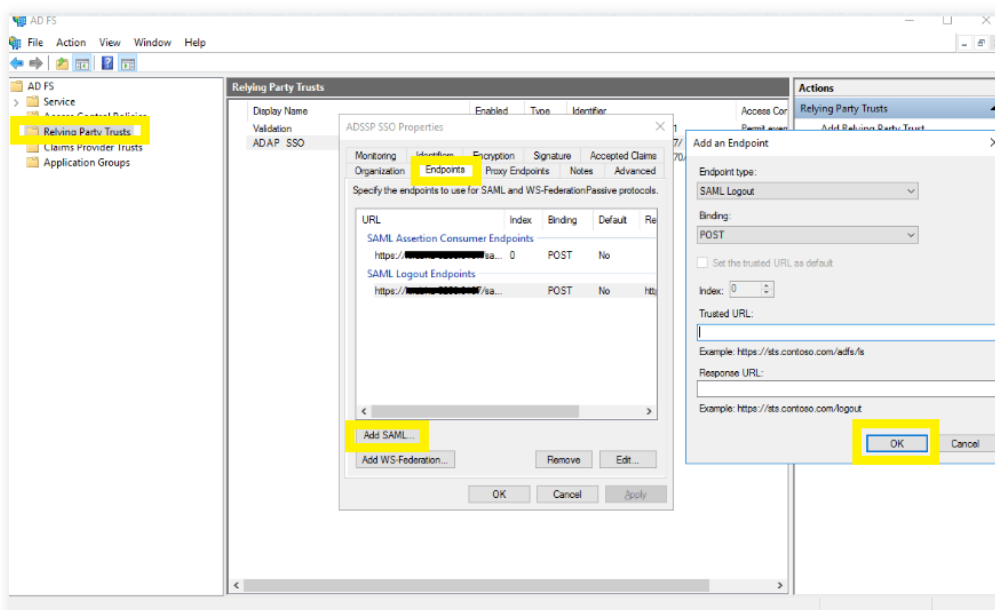
For example: [https://<server\\_name>/FederationMetadata/2007-06/FederationMetadata.xml](https://<server_name>/FederationMetadata/2007-06/FederationMetadata.xml).

**Note:**

Replace <server\_name> with the AD FS hostname.

Save this file, as you will need it while configuring SAML authentication in ADAudit Plus.

18. Navigate back to Relaying Party Trusts, and find the rule you've created. Right-click on the rule, and click Properties. In the window that opens, click on Endpoints > Add SAML > OK.



19. In the *Trusted URL* field, paste the SP Logout URL.

**Note:**

To get the SP Logout URL, open the ADAudit Plus console, navigate to Admin > Administration > Logon Settings > Single Sign-On. Check the box next to Enable Single Sign-On, and select SAML Authentication > Identity Provider (IdP) > ADFS. You can find the SP Logout URL value here. Click OK.

20. Next, click on Signature, and upload the X.509 Certificate.

**Note:**

To get the X.509 Certificate, open the ADAudit Plus console, navigate to Admin > Administration > Logon Settings > Single Sign-On. Check the box next to Enable Single Sign-On, and select SAML Authentication > Identity Provider (IdP) > ADFS. You can find the X.509 Certificate here. Click OK.

## Step 2: Configure AD FS in ADAudit Plus

### Prerequisites

Enable RelayState in AD FS.

### For Windows Server 2012

- Navigate to the  
`%systemroot%\ADFS\Microsoft.IdentityServer.Servicehost.exe.config`  
file in your AD FS server.
- In the `<microsoft.identityServer.web>` section, enter the following code:  
`<useRelayStateForIdpInitiatedSignOn enabled="true" />`  
Sample code:  
`<microsoft.identityServer.web>`  
.....  
`<useRelayStateForIdpInitiatedSignOn enabled="true" />`  
`</microsoft.identityServer.web>`
- Restart the AD FS server.

### For Windows Server 2016:

- Open an elevated PowerShell Prompt (right-click PowerShell, and select Run as administrator) in your AD FS server.
- Run the following command to enable IdP-initiated SSO: `Set-ADFSProperties -EnableIdPInitiatedSignonPage $true`
- Run the following code to enable RelayState: `Set-ADFSProperties -EnableRelayStateForIDPInitiatedSignon $true`
- Restart the AD FS server.

Log in to the ADAudit Plus web console with admin credentials, and navigate to **Admin > Administration > Logon Settings > Single Sign-On**. Check the box next to **Enable Single Sign-On**, and select **SAML Authentication > Identity Provider (IdP) > ADFS**. Click **Browse**, and upload the metadata file you downloaded from [Step 1: 17](#). Click **Save**.

### Accessing ADAudit Plus through AD FS

1. To access ADAudit Plus, use the URL provided below:  
`https:// <ADFSserver>/adfs/ls/idpinitiatedsignon.aspx`  
Where *ADFSserver* is the server in which AD FS is deployed.
2. In the AD FS web console, select **ADAudit Plus** from the list of applications.



## 2.5 Configuring single sign-on to ADAudit Plus using a custom identity provider

### 2.5.1 Configuring single sign-on to ADAudit Plus using any custom identity provider

You can configure any custom identity provider of your choice to enable single sign-on to access ADAudit Plus. To do this, follow these steps:

#### Configure a custom identity provider in ADAudit Plus:

Log in to the ADAudit Plus web console with admin credentials, and navigate to **Admin > Administration > Logon Settings > Single Sign-On**. Check the box next to **Enable Single Sign-On**, and select **SAML Authentication > Identity Provider (IdP) > Custom Identity Provider**. Upload the **metadata file** of the custom identity provider, and click **Save**.

The screenshot displays the 'Logon Settings' page in the ADAudit Plus web console. The 'Single Sign On' tab is selected. Under 'Enable Single Sign-on with Active Directory', the 'SAML Authentication' radio button is chosen. The 'Configure Identity Provider' section is expanded, showing 'Custom Provider' selected for the Identity Provider (IdP). The 'IdP Provider Name' field is empty. For the 'IdP Provider Logo', the '- Browse file -' button is visible. Under 'SAML Configuration Mode', 'Upload Metadata File' is selected, and the '- Browse file -' button is highlighted with a yellow box, with a 'Browse' button next to it. There are also checkboxes for 'Sign SAML Logout Request' and 'Sign SAML Logout Response', both of which are currently unchecked.

**Logon Settings**  
Login to ADAudit Plus using an authentication method other than the first factor authentication.

**Single Sign On** | Two-Factor Authentication

☒ Enable Single Sign-on with Active Directory

☐ NTMLv2 Authentication ☒ SAML Authentication

**Configure Identity Provider**

Identity Provider (IdP) **Custom Provider**

\* IdP Provider Name

IdP Provider Logo

SAML Configuration Mode ☒ Upload Metadata File ☐ Manual Configuration

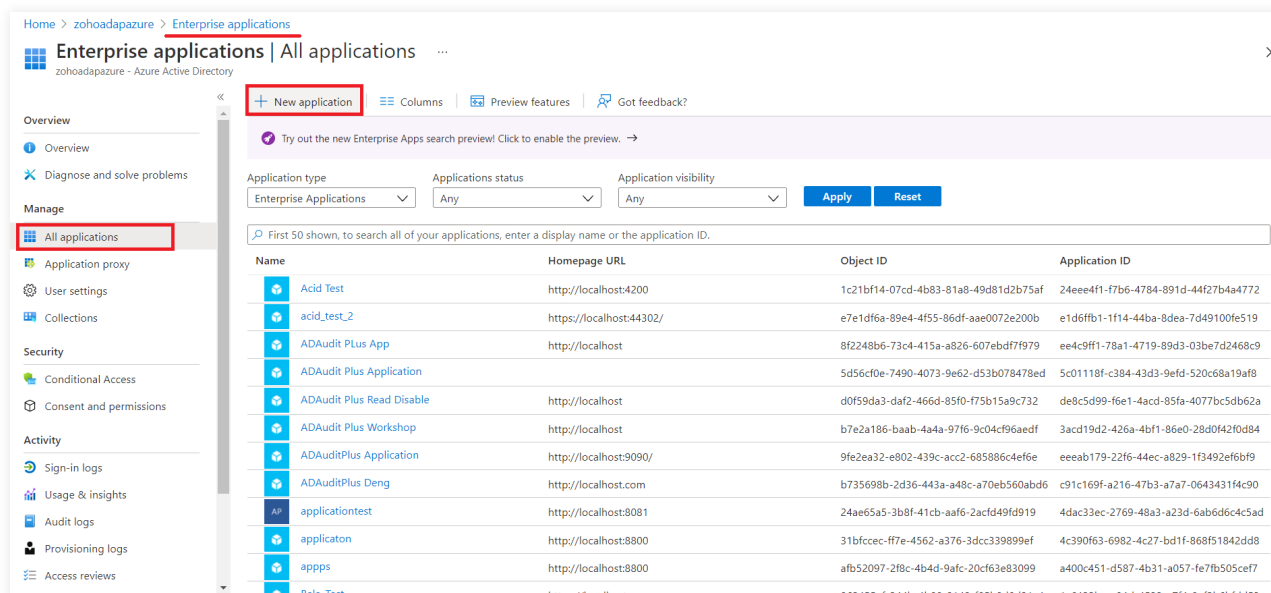
?

☐ Sign SAML Logout Request ?

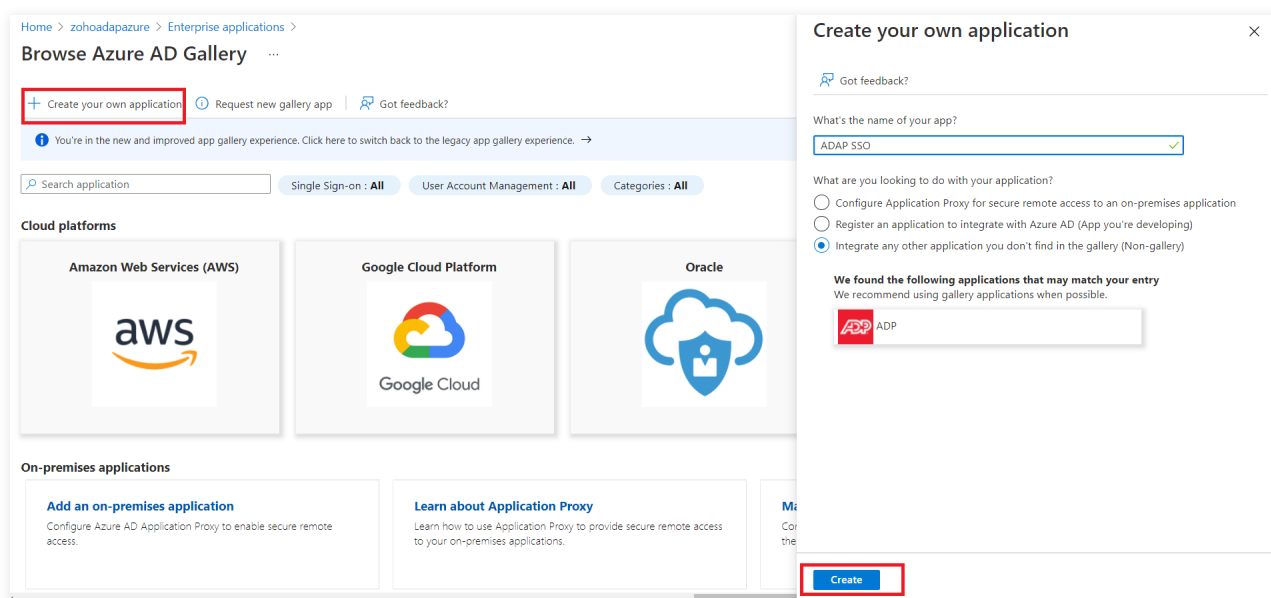
☐ Sign SAML Logout Response ?

## 2.5.2 Configuring single sign-on to ADAudit Plus using Azure

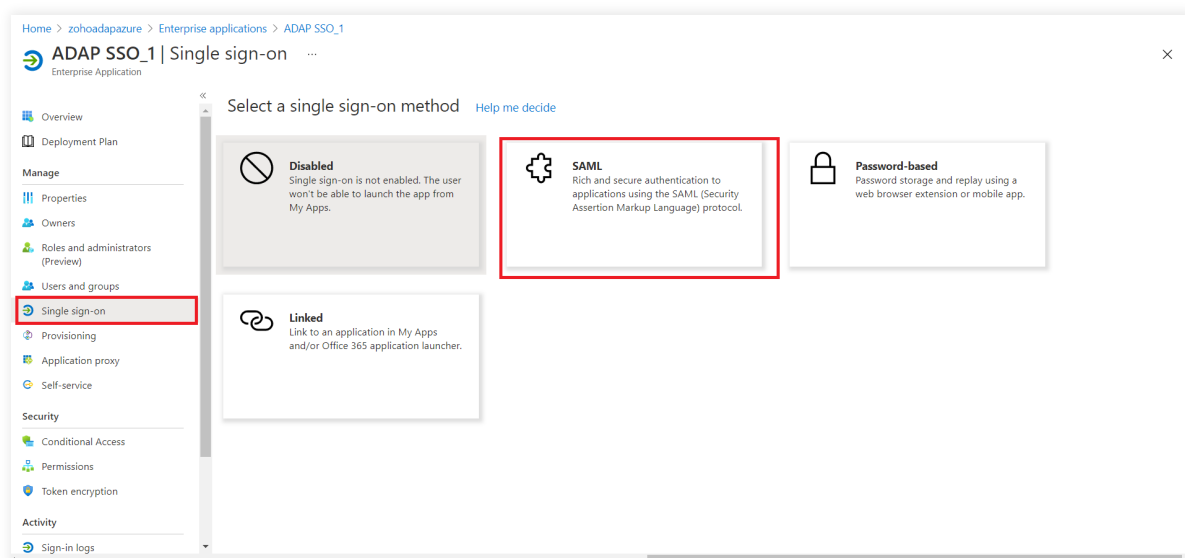
1. Login to your Azure Portal and navigate to Enterprise Applications > All Applications > New Application.



2. In the New Application page, click Create your own Application > Give a name for the application and click Create.



3. In your application, click Single Sign-On > SAML.



4. Under Set up Single Sign-On with SAML > Basic SAML Configuration, click Edit.

- Copy the ACS URL from ADAudit Plus and paste the it under Identifier and Reply URL.

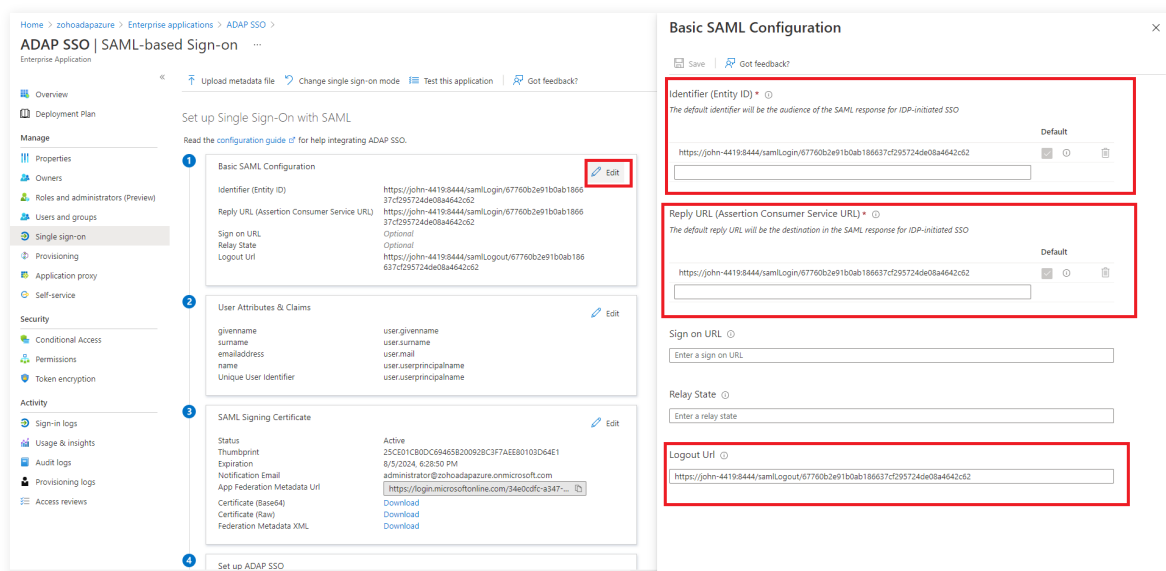
### Note:

To find the values for the ACS URL, log in to the ADAudit Plus console, navigate to Admin > Administration > Logon Settings > Single Sign-On. Check the box next to Enable Single Sign-On, and select SAML Authentication > Identity Provider (IdP) > Custom Identity Provider. You can find the ACS URL value here.

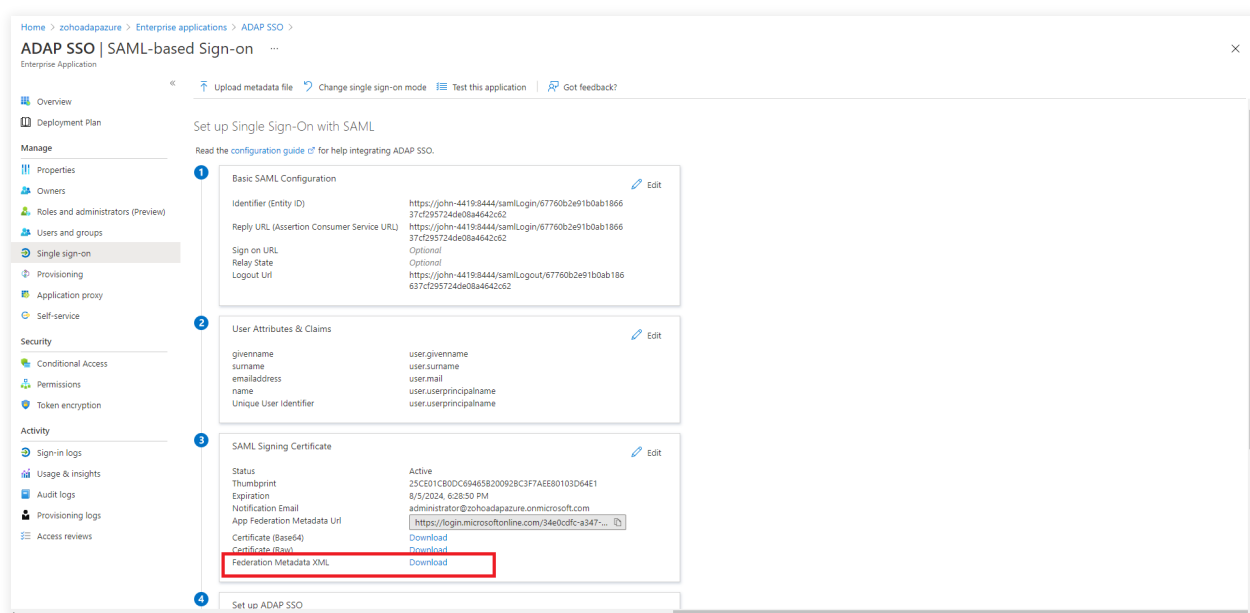
- Copy Logout URL from ADAudit Plus and paste it under Logout URL.

### Note:

To get the Logout URL, log in to the ADAudit Plus console, navigate to Admin > Administration > Logon Settings > Single Sign-On. Check the box next to Enable Single Sign-On, and select SAML Authentication > Identity Provider (IdP) > Custom Identity Provider. You can find the Logout URL value here.

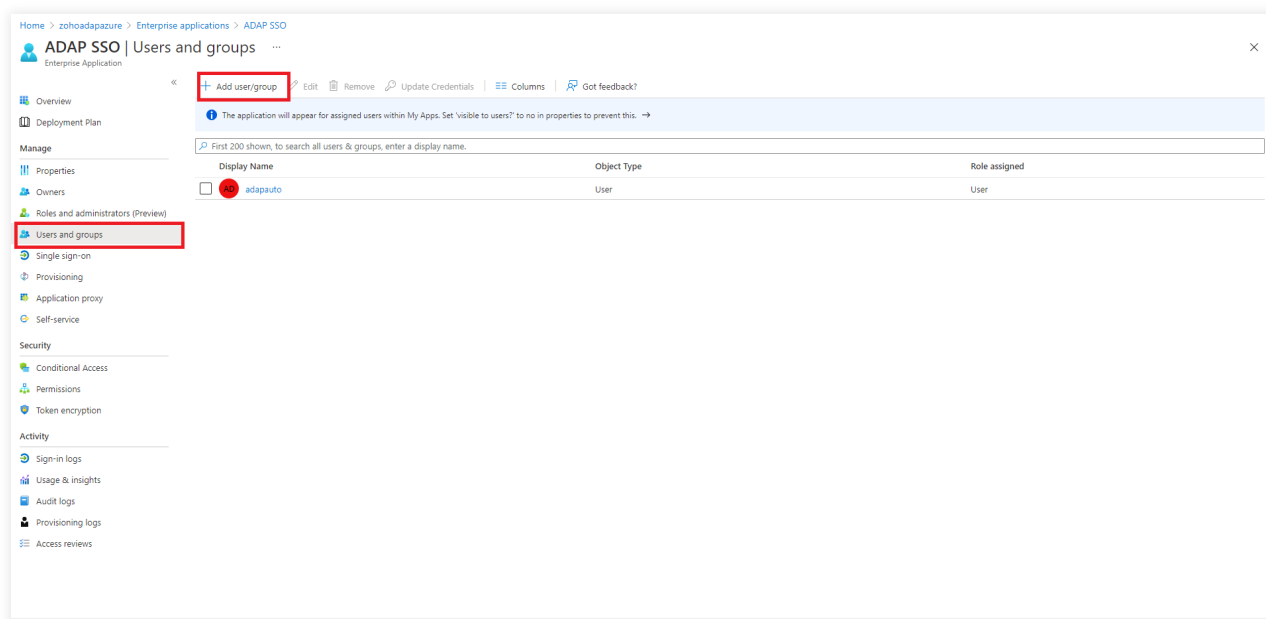


## 5. Click Download against Federation Metadata XML.



6. Log in to the ADAudit Plus console, navigate to **Admin > Administration > Logon Settings > Single Sign-On**. Check the box next to **Enable Single Sign-On**, and select **SAML Authentication > Identity Provider (IdP) > Custom Identity Provider > Enter a suitable name against the IdP Provider Name field > Upload the Federation Metadata XML file downloaded in the previous step > Click Save**.

7. In the Azure portal, click **Users and Groups > Add the required users and groups**.



## 2.6 Troubleshooting tips for SAML-based SSO

1. **Error:** Unable to connect. The requested page could not be loaded.

This error can occur when:

- Direct access to the URL is restricted.
- The product is being accessed from multiple tabs.

**Solution:** Re-enter the ACS/Recipient URL in the respective IdP console, and try again.

**Note:**

To find the value for ACS/Recipient URL, log in to the ADAudit Plus console, navigate to **Admin > Administration > Logon Settings > Single Sign-On**. Check the box next to **Enable Single Sign-On**, and select **SAML Authentication > Identity Provider (IdP)**. Select the relevant IdP. You can find the ACS/Recipient URL value here.

## Our Products

AD360 | Log360 | ADManager Plus | ADSelfService Plus | DataSecurity Plus | M365 Manager Plus

ManageEngine  
**ADAudit Plus**

ManageEngine ADAudit Plus is a real-time change auditing and user behavior analytics solution that helps keep your Active Directory, Azure AD, Windows servers, and workstations secure and compliant.

\$ Get Quote

Download