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 NTMLv2 SSO authentication. In builds 7082 and above, the Jespa JAR file has to be downloaded and added to ADAudit Plus' lib folder before enabling NTMLv2 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 ADAUGIT Plus Using an a	uthentication method other than the first factor authentication.
Single Sign On	Two-Factor Authentication
Enable Single Sign-o	n with Active Directory
NTMLv2 Authen	tication 🔘 SAML Authentication
Select Doma	ins 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.

ADAudit Plus	Jump to License 🚅 Jobs ? me Reports File Audit Server Audit Analytics Alerts Configuration Admin Support Q Search O Domain S	etting
Administration Alert Me	Login to ADAudit Plus using an authentication method other than the first factor authentication.	
Domain Settings Technicians	Single Sign On Two-Factor Authentication	
Logon Settings Schedule Reports	Enable Single Sign-on with Active Directory	
Custom Reports Disk space analysis	NTMLv2 Authentication Select Domains auto adap com	
Exclude User Accounts Business Hours	Save Settings	
Configuration	ADAudit Plus will automatically create a computer account for NTLM authentication in the domain(s) you've selected.	
Alerts/Reports	Domain Computer Account Status	
Archive Events Restore Archived Events	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 com	puter account adap	pauto	×
(!	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 o	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):

- 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

- 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

- 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.

Single Sign On Two-Factor A	uthentication		
☑ Enable Single Sign-on with Active D	lirectory		
O NTMLv2 Authentication	NTMLv2 Authentication SAML Authentication		
Configure Identity Provider	Configure Identity Provider		
Identity Provider (Id	P) Okta		
SAML Configuration Mod	de 💿 Upload Metadata File 💦 Manual Configuration		
	- Browse file - Browse ⑦		
	Sign SAML Logout Request ③		
	Sign SAML Logout Response ⑦		
Service Provider (SP) Details			
ACS/Recipient U	Recipient URL to be configured in IdP.		
Issuer URL/Entity	D http://john-4419:8081/samlLogin/5 🗈		
SP Logout U	مل http://john-4419:8081/samlLogout/ 🗈		
	Bownload X.509 Certificate		

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**.

4. 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.

5. 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.
- 3. 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.
- 4. Click Save.

Logon Settings Login to ADAudit Plus using an authentication method other than the first factor authentication.			
Single Sign On Two-Factor Auth	entication		
 Enable Single Sign-on with Active Direction NTMLv2 Authentication SAM 	tory IL Authentication		
Configure Identity Provider	Configure Identity Provider		
Identity Provider (IdP)	OneLogin 🗸		
SAML Configuration Mode	Upload Metadata File O Manual Configuration		
	- Browse file - 3700 3700 3700 3700 3700 3700 3700 37		
	Sign SAML Logout Request ③		
	Sign SAML Logout Response 🕜		
Service Provider (SP) Details			
ACS/Recipient URL	http://john-4419:8081/samlLogin/5 🗈		
	Recipient URL to be configured in IdP.		
Issuer URL/Entity ID	http://john-4419:8081/samlLogin/5 🗈		
SP Logout URL	http://john-4419:8081/samlLogout/ 🗈		

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

- 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.

Single Sign On Two-Factor Auth	entication		
✓ Enable Single Sign-on with Active Dire	ctory		
O NTMLv2 Authentication 💿 SAI	ML Authentication		
Configure Identity Provider	Configure Identity Provider		
Identity Provider (IdP)	Pingldentity 🗸		
SAML Configuration Mode	Upload Metadata File Manual Configuration		
	- Browse file - Browse ⑦		
	Sign SAML Logout Request ⑦		
	Sign SAML Logout Response ⑦		
Service Provider (SP) Details	Service Provider (SP) Details		
ACS/Recipient URL	http://john-4419:8081/samlLogin/5 🗈		
	Recipient URL to be configured in IdP.		
Issuer URL/Entity ID	http://john-4419:8081/samlLogin/5 🗈		
SP Logout URL	http://john-4419:8081/samlLogout/ 🖻		
	Download X.509 Certificate		

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.

御		AD FS	
 File Action View Window Help File Action File Action			
AD FS	Relying Party Trusts		
Service	Display Name	Enabled Type Identifier	
⊿ Irust Relationships	Device Registration Service	Yes WS-Trust um:ms-drs:mickey-adfs-dc1.mickeyadf	
	MICKEY	Yes WS-Trust me.com	
Attribute Stores			
Authentication Policies			

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.

\$	Add Relying Party Trust Wizard
Select Data Source	
Steps Welcome Select Data Source Specify Display Name Choose Profile Configure Certificate Configure URL Configure Multi factor Authentication Now? Choose Issuance Authorization Rules Ready to Add Trust Finish	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 explored 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: Browse @ Enter data about the relying party manually Use this option to manually input the necessary data about this relying party organization.
	< Previous Next > Cancel

- 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**.

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.

\$	Add Relying Party Trust Wizard
Finish	
Steps Welcome Select Data Source Specify Display Name Choose Profile Configure Certificate Configure URL Configure Identifiers Configure Multifactor Authentication Now? Choose Issuance Authorization Rules Ready to Add Trust Finish	The relying party trust was successfully added to the AD FS configuration database. You can modify this relying party trust by using the Properties dialog box in the AD FS Management snap-in. Open the Edit Claim Rules dialog for this relying party trust when the wizard closes
	Close

- 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**.

\$	Add Transform Claim Rule Wizard
Select Rule Template	
Choose Rule Type Configure Claim Rule	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 membership. If you want to only send individual group memberships, use the Send Group Membership as a Claim rule template.
	< Previous Next > 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.

%	Add Transform Claim Rule Wizard
Configure Rule	
Steps Configure Claim Rule	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. Claim rule name:

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. **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**.

M AD FS					- U X
🖬 File Action View Window Help					_ 5 ×
(+ +) 🖄 📰 📓 🗔					
AD FS	Relying Party Trusts	Actions			
 AD FS Service Revine Party Trusts Clams Provder Trusts Application Groups 	Relying Party Trusts Display Name Valdetion ADAP SSO	Endo ADSSP SSO Properties Montoring Uncertain Endorsta Pri Specfy the emports to use for SAI URL SAML Assertion Consumer E https://www.saistanter. https://www.saistanter. dd SAML Add SAML Add SAML	ied Tuen Merr pton Sgnature coy Endpoints Note ML and WS-Federation F index Binding ndpoints 0 POST POST Remove DK Cancel	tfer X Accepted Clame Accepted Clame Accepted Clame Advanced Assive protocols. Default Re No No http: Cat. Cat. Cat. Cat. Cat. Cat. Cat. Cat.	Actions Actio
	٢				>

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

- 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.

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)					
* IdP Provider Name					
IdP Provider Logo - Browse file - Browse					
SAML Configuration Mode 💿 Upload Metadata File 🛛 🔘 Manual Configuration					
- Browse file - Browse ③					
Sign SAML Logout Request ③					
Sign SAML Logout Response ③					

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.

Home > zohoadapazure > Enterprise applications Enterprise applications | All applications × Overview 🕜 Try out the new Enterprise Apps search preview! Click to enable the preview. ightarrow Overview X Diagnose and solve problems Application type Applications status Application visibility Enterprise Applications V Any ✓ Any ✓ Apply Reset Manage \wp First 50 shown, to search all of your applications, enter a display name or the application ID. All applications Name Homepage URL Object ID Application ID Application proxy Acid Test http://localhost:4200 1c21bf14-07cd-4b83-81a8-49d81d2b75af 24eee4f1-f7b6-4784-891d-44f27b4a4772 User settings • Ŷ acid_test_2 Collections https://localhost:44302/ e7e1df6a-89e4-4f55-86df-aae0072e200b e1d6ffb1-1f14-44ba-8dea-7d49100fe519 ŵ ADAudit PLus App http://localhost 8f2248b6-73c4-415a-a826-607ebdf7f979 ee4c9ff1-78a1-4719-89d3-03be7d2468c9 Security ŵ ADAudit Plus Application 5d56cf0e-7490-4073-9e62-d53b078478ed 5c01118f-c384-43d3-9efd-520c68a19af8 Conditional Access ADAudit Plus Read Disable http://localhost d0f59da3-daf2-466d-85f0-f75b15a9c732 de8c5d99-f6e1-4acd-85fa-4077bc5db62a M Consent and permissions ADAudit Plus Workshop http://localhost b7e2a186-baab-4a4a-97f6-9c04cf96aedf 3acd19d2-426a-4bf1-86e0-28d0f42f0d84 Activity Ŷ ADAuditPlus Application 9fe2ea32-e802-439c-acc2-685886c4ef6e eeeab179-22f6-44ec-a829-1f3492ef6bf9 http://localhost:9090/ Sign-in logs ŵ ADAuditPlus Deng http://localhost.com b735698b-2d36-443a-a48c-a70eb560abd6 c91c169f-a216-47b3-a7a7-0643431f4c90 🙀 Usage & insights applicationtest http://localhost:8081 24ae65a5-3b8f-41cb-aaf6-2acfd49fd919 4dac33ec-2769-48a3-a23d-6ab6d6c4c5ad Audit logs • applicaton http://localhost:8800 31bfccec-ff7e-4562-a376-3dcc339899ef 4c390f63-6982-4c27-bd1f-868f51842dd8 Provisioning logs Ŷ appps http://localhost:8800 afb52097-2f8c-4b4d-9afc-20cf63e83099 a400c451-d587-4b31-a057-fe7fb505cef7 ≸≡ Access reviews SETTEENE TANK ALOO OTAD FOELOHOHITAA 1.64006 and AEDD a7f4 nafblehfdde

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

Home > zohoadapazure > Enterprise applications >		Create your own application ×
	t feedback? aack to the legacy app gallery experience. → User Account Management : All Categories : All	Create your own application × Create your own application × Create your own application × What's the name of your app? ADAP 550 What are you looking to do with your application? Configure Application Proxy for secure remote access to an on-premises application
Cloud platforms Amazon Web Services (AWS) Goog G	le Cloud Platform Oracle	Register an application to integrate with Azure AD (App you're developing) Integrate any other application you don't find in the gallery (Non-gallery) We found the following applications that may match your entry We recommend using gallery applications when possible. ADP
On-premises applications		
Add an on-premises application Configure Azure AD Application Proxy to enable secure remote access.	Learn about Application Proxy Learn how to use Application Proxy to provide secure remote access to your on-premises applications.	M: Cor the Create

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

Home > zohoadapazure > Enterprise ADAP SSO_1 Single Enterprise Application	applications > ADAP SSO_1 e sign-on …	×
Overview	Select a single sign-on method Help me decide	
Deployment Plan		
Manage	Disabled C SAML A Password-based	
Properties	Single sign-on is not enabled. The user won't be able to launch the app from applications using the SAML (Security web browser extension or mobile app.	
A Owners	My Apps. Assertion Markup Language) protocol.	
Roles and administrators (Preview)		
Users and groups		
Single sign-on	Con Linked	
Provisioning	Link to an application in My Apps and/or Office 365 application launcher.	
Application proxy		
Self-service		
Security		
Conditional Access		
Permissions		
Token encryption		
Activity		

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.

Home > zohoadapazure > Enterprise	applicatio	ons > ADAP SSO >			Basic SAML Configuration	
ADAP SSO SAML-bas	ed Sig	jn-on …			☐ Save 🖉 Got feedback?	
«	Ţ.	Upload metadata file 🂙 Change single sign-on	mode 🛛 Test this application 🔰 🖗 Got feedback?		− Identifier (Entity ID) * ⊙	1
Deployment Plan	Set i	up Single Sign-On with SAML			The default identifier will be the audience of the SAML response for IDP-initiated SSO	I
Manage	Read	the configuration guide of for help integrating AD	MAP SSO.		Default	I
Properties	0	Basic SAML Configuration			https://john-4419:8444/samlLogin/67760b2e91b0ab186637cf295724de08a4642c62	I
A Owners		Identifier (Entity ID)	https://john-4419:8444/samlLogin/67760b2e91b0ab1866	2 Edit		
 Boles and administrators (Preview) Users and arouns 		Reply URL (Assertion Consumer Service URL)	37cf295724de08a4642c62 https://john-4419:8444/samlLogin/67760b2e91b0ab1866		Reply URL (Assertion Consumer Service URL) * ③	Ì
 Single sign-on 		Sign on URL	37ct295724de08a4642c62 Optional		The default reply URL will be the destination in the SAML response for IDP-initiated SSO	
Provisioning		Logout Url	https://john-4419:8444/samlLogout/67760b2e91b0ab186		Default	
Application proxy			63701295724de0884642062		https://john-4419:8444/samlLogin/67760b2e91b0ab186637cf295724de08a4642c62	
Self-service	2	User Attributes & Claims				
Security				/ Edit		4
🗲 Conditional Access		sumame	usersumame		Sign on URL O	
Remissions		emailaddress name	user.mail user.userprincipalname		Enter a sign on URL	
Token encryption		Unique User Identifier	user.userprincipalname			
Activity					Relay State 💿	
Sign-in logs	•	SAML Signing Certificate		🖉 Edit	Enter a relay state	
🕍 Usage & insights		Status	Active		1	Ē
Audit logs		Expiration	8/5/2024, 6:28:50 PM			L
Provisioning logs		App Federation Metadata Url	administrator@zohoadapazure.onmicrosoft.com https://login.microsoftonline.com/34e0cdfc-a347		https://john-4419:8444/samlLogout/67760b2e91b0ab186637cf295724de08a4642c62	L
E Access reviews		Certificate (Base64) Certificate (Raw) Federation Metadata XML	Download Download Download			1
	4	Set up ADAP SSO				

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.

Home > zohoadapazure > Enterprise	applications > ADAP SSO			
ADAP SSO Users a	and groups			×
«	+ Add user/group 🖉 Edit 📋 Remove 🖉 Update	Credentials 🛛 🎫 Columns 🛛 🔗 Got feedback?		
👪 Overview		A LEAST ALL ALL ALL ALL ALL ALL ALL ALL ALL AL		
Deployment Plan	The application will appear for assigned users within Wy Application will appear for assigned users within Wy Application	ps. Set visible to users? to no in properties to prevent this. I in the set of the set o		
Manage	$\mathcal P$ First 200 shown, to search all users & groups, enter a disp	lay name.		
Properties	Display Name	Object Type	Role assigned	
A Owners	AD adapauto	User	User	
 Roles and administrators (Preview) 	_			
Users and groups				
Single sign-on				
Provisioning				
Application proxy				
 Self-service 				
Security				
🐁 Conditional Access				
Token encryption				
Activity				
3 Sign-in logs				
🕍 Usage & insights				
Audit logs				
Provisioning logs				
E Access reviews				
1				

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.