ADAudit Plus
Single Sign-On
Table of Contents

1. NTLM authentication
   1.1 To enable NTLM-based single sign-on  2
   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
   2.6 Troubleshooting tips for SAML-based SSO  16
1. NTLM authentication

1.1 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.

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.
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.

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:
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 Chrome, and click on Customize and control Google Chrome located in the top right-hand corner of the screen. Scroll to the bottom, and click Advanced. Under System, click Open proxy settings.

2. In the search bar, type Internet Options and then select it. 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.

3. 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.

2. 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.

3. 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:
- 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.
2.2 Configuring single sign-on to ADAudit Plus using OneLogin

Step 2: Configure Okta in ADAudit Plus


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.

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**


2. 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**.
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**
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/955060d1d15d6bb8166c13b8b6e10144e5f755c953
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.
14. From the Claim rule template drop-down, select Send LDAP Attributes as Claims, and click Next.

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.
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.

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:

```xml
<useRelayStateForIdpInitiatedSignOn enabled="true" />
```

Sample code:

```xml
<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 -EnableRelayStateForIdPIPInitiatedSignon $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.
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.
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.