Active Directory Federation Service (AD FS) auditing guide
# Table of Contents

Document summary .................................................. 3

1. Configure AD FS servers in ADAudit Plus .......................... 4

2. Configure audit policies in your domain .......................... 4
   2.1 Automatic configuration ........................................... 4
   2.2 Manual configuration ............................................... 4
       2.2.1 Configure advanced audit policies .......................... 4
       2.2.2 Force advanced audit policies .............................. 5
       2.2.3 Configure legacy audit policies ............................ 6

3. Configure AD FS servers for auditing in your domain .............. 7
   3.1 Enable auditing .................................................. 7
   3.2 Configure claims .................................................. 8
   3.3 Configure extranet lockout ....................................... 9

4. FAQ ................................................................. 10
Document summary

Microsoft Active Directory Federation Services (AD FS) helps organizations provide users with single sign-on (SSO) capabilities, making it easier for them to access systems and applications across organizational boundaries.

ADAudit Plus is a real-time auditing and user behavior analytics solution that offers insight on users’ federated access. With ADAudit Plus, you can track all authentication attempts recorded by AD FS in the security event log, and get insightful reports on AD FS logon success and failure.

Click here to see what else ADAudit Plus has to offer.

ADAudit Plus enables you to audit the following versions of Windows Server and AD FS respectively:

- Windows Server 2008/2008 R2
- Windows Server 2012/2012 R2
- Windows Server 2016

This guide takes you through the process of setting up ADAudit Plus and your AD FS servers for real-time auditing.
1. Configure AD FS servers in ADAudit Plus

Note: If AD FS has been installed on a domain controller, configure the Active Directory domain and the domain controller in ADAudit Plus. Click here to see how.

If AD FS has been installed on a Windows server, configure the Windows server in ADAudit Plus. Click here to see how.

ADAudit Plus can automatically configure the required audit policies for AD FS auditing.

Note: If AD FS has been installed on a domain controller, click here to learn how to enable automatic configurations.

If AD FS has been installed on a Windows server, click here to learn how to enable automatic configurations.

2. Configure audit policies in your domain

Audit policies must be configured to ensure that events are logged whenever any activity occurs.

2.1 Automatic configuration

ADAudit Plus can automatically configure the required audit policies for AD FS auditing.

Note: If AD FS has been installed on a domain controller, click here to learn how to enable automatic configurations.

If AD FS has been installed on a Windows server, click here to learn how to enable automatic configurations.

2.2 Manual configuration

2.2.1 Configure advanced audit policies

Advanced audit policies help administrators exercise granular control over which activities get recorded in the logs, helping cut down on event noise. We recommend configuring advanced audit policies on Windows Server 2008 and above.

1. Log in to any computer that has the GPMC with Domain Admin credentials. Open the GPMC, and based on your setup, you’ll either right-click Default Domain Controllers Policy or ADAuditPlusMSPolicy, then select Edit.

Note: If AD FS has been installed on a domain controller, configure the audit policy in the Default Domain Controllers Policy GPO. If AD FS has been installed on a Windows server, configure audit policy in the ADAuditPlusMSPolicy GPO.


3. Double-click Audit Policy.
4. Right-click on Audit Application Generated in the right pane. Select Properties, then check the boxes next to Success and Failure.

2.2.2 Force advanced audit policies

When using advanced audit policies, ensure that they are forced over legacy audit policies.

1. Log in to any computer that has the GPMC with Domain Admin credentials. Open the GPMC, and based on your setup, you’ll either right-click Default Domain Controllers Policy or ADAuditPlus MSPolicy, then select Edit.

Note: If AD FS has been installed on a domain controller, configure the audit policy in the Default Domain Controllers Policy GPO. If AD FS has been installed on a Windows server, configure the audit policy in the ADAuditPlus MSPolicy GPO.


3. Right-click Audit: Force audit policy subcategory settings from the right pane.

4. Select Properties, then choose Enabled.
2.2.3 Configure legacy audit policies

Due to the unavailability of advanced audit policies in Windows Server 2003 and earlier versions, legacy audit policies need to be configured for these types of servers.

1. Log in to any computer that has the GPMC with Domain Admin credentials. Open the GPMC, and based on your setup, you'll either right-click Default Domain Controllers Policy or ADAuditPlusMSPolicy, then select Edit.

Note: If AD FS has been installed on a domain controller, configure the audit policy in the Default Domain Controllers Policy GPO. If AD FS has been installed on a Windows server, configure audit policy in the ADAuditPlusMSPolicy GPO.


3. Double-click Audit Policy.

4. Right-click on the Object Access policy in the right pane. Select Properties, then check the boxes next to Success and Failure.
3. Configure AD FS servers for auditing in your domain

3.1 Enable auditing

Log in to the AD FS server with Domain Admin credentials. Open the AD FS management console, right-click Service > Edit Federation Service Properties > Events.

Check the boxes next to Success audits and Failure audits.
3.2 Configure claim rules

For each relying party that needs to be audited, the following six claim rules need to be added:

i. Primary SID
ii. UPN
iii. Client IP
iv. Inside Corporate Network
v. Proxy
vi. Forwarded Client IP

To check which claim rules have already been added:

1. Log in to the AD FS server with Domain Admin credentials.
2. Open the AD FS management console > Trust Relationships > Relying Party Trusts.
3. Right-click on the relying party > Edit Claim Rules (or Edit Claim Issuance Policy in case of Windows 2016), and check if all six of the above claim rules have been added.

To add any missing claim rules:

1. Log in to the AD FS server with Domain Admin credentials. Open the AD FS management console > Trust Relationships > Relying Party Trusts.
2. Right-click on the relying party > Edit Claim Rules (or Edit Claim Issuance Policy in case of Windows 2016).
3. Click Add Rule. From the Claim rule template drop down, select Pass Through or Filter an Incoming Rule and click Next.
4. In the Claim rule name field, enter a suitable name.
5. Under Incoming claim type, select the claim rule type which you need to add, and select Pass through all claim values.
6. Click Finish.
3.3 Configure extranet lockout

1. Log in to the **AD FS server** with Domain Admin credentials. Open **Windows PowerShell**, and execute the below command:

```
Set-AdfsProperties -EnableExtranetLockout $true -ExtranetLockoutThreshold <Threshold_value> -ExtranetObservationWindow (New-Timespan -Minutes <time_in_minutes>)
```

In the above command, set appropriate values for:

- `<Threshold_value>`, an integer value that defines the maximum number of bad password attempts.
- `<time_in_minutes>`, the time in minutes that determines how long the user account will be soft-locked out for.

**Note**: Extranet lockout settings can be configured only if an AD FS proxy is used in your environment. The AD FS proxy server need not be configured in the ADAudit Plus console.
4. FAQ

1. How do I verify if the desired audit policies are configured?
   Log in to any computer that has the GPMC with Domain Admin credentials. Open the GPMC, right-click Group Policy Results, and open the Group Policy Results Wizard. Select the computer and user (current user), then verify if the desired settings defined in step 2.2 are configured.

2. How do I verify if the desired events are getting logged?
   Log in to any computer with Domain Admin credentials. Open Run, and type eventvwr.msc. Right-click on Event Viewer. Connect to the target computer, then verify if events corresponding to the configured audit policies are getting logged. For example, Event ID 1200 should get logged when Success audit events is configured under the Audit Application Generated Subcategory, under the Object Access Category (refer to step 2.2.1).

3. What do I do if:
   - AD FS logon success and failure data is unavailable?
     Check if audit policies (refer to step 2.2.1) and AD FS auditing (refer to step 3.1) are configured.
   - Primary SID, UPN, Client IP, Inside Corporate Network, Proxy or Forwarded Client IP data is unavailable?
     Check if the corresponding claim rules have been configured (refer to step 3.2).
   - Extranet lockout data is unavailable?
     Check if extranet lockout settings have been configured (refer to step 3.3).

4. Do I need to configure a proxy server in my environment in order to configure extranet lockout settings?
   Yes, extranet lockout settings can be configured only if an AD FS proxy is used in your environment. The AD FS proxy server need not be configured in the ADAudit Plus console.