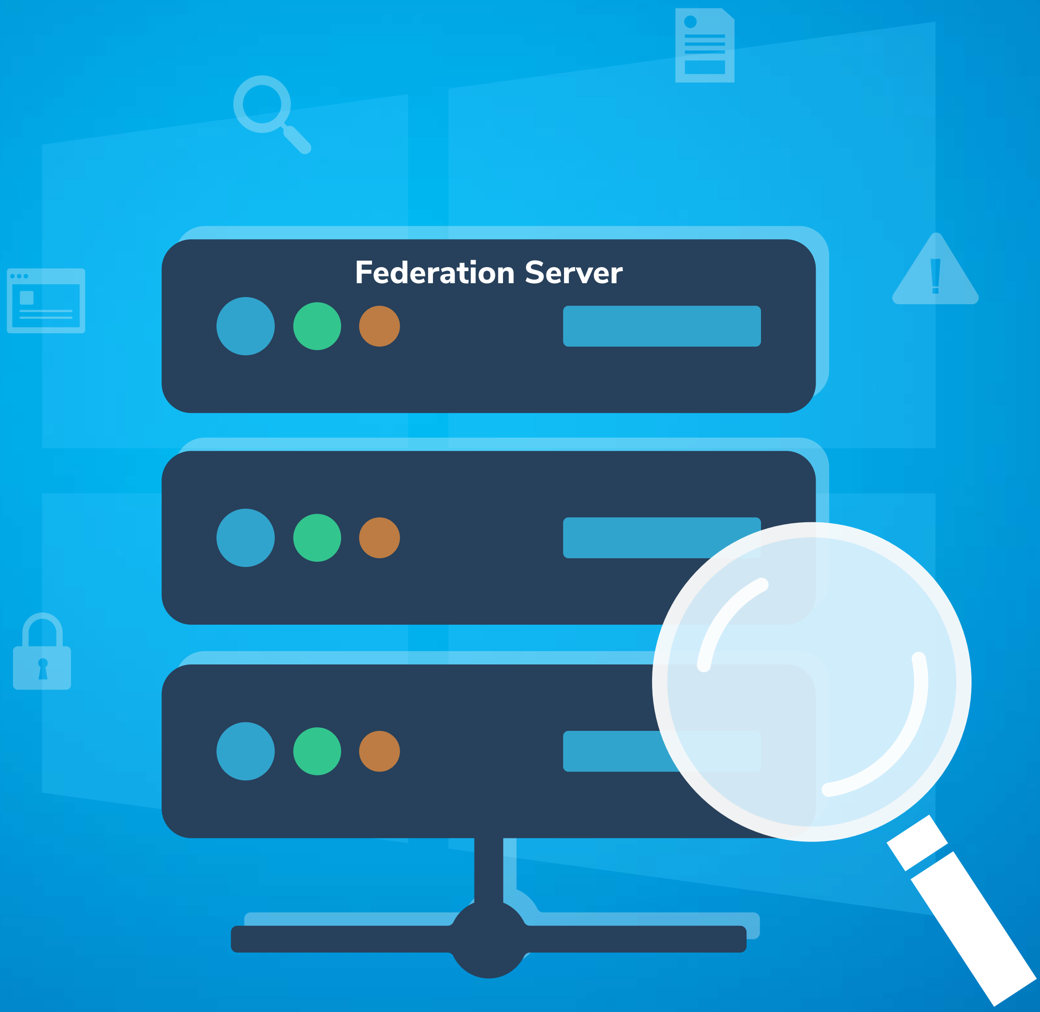
ManageEngine
ADAudit Plus

Active Directory Federation Service (AD FS) auditing guide



www.adauditplus.com

Table of Contents

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
- Windows Server 2019
- Windows Server 2022

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.

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.

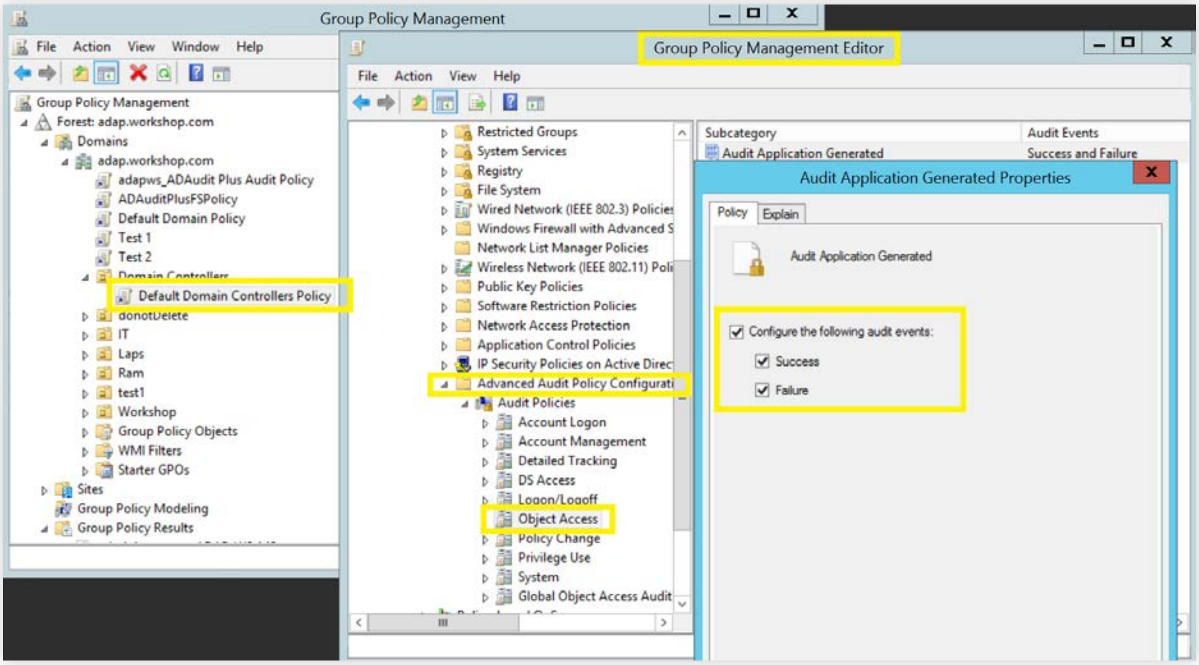
1. Log in to any computer that has the GPMC with Domain Admin credentials. Open the **GPMC,** and based on your setup, you'll either right-click **Default Domain Controllers Policy** or **ADAuditPlusMSPolicy,** then select **Edit.**

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.

2. In the Group Policy Management Editor, go to **Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies.**

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.**


Group Policy Management
Group Policy Management Editor
Default Domain Controllers Policy
Advanced Audit Policy Configurati
Object Access
Audit Application Generated Properties
Policy
Explain

Subcategory: Audit Application Generated — Audit Events: Success and Failure

☑ Configure the following audit events:
☑ Success
☑ Failure

2.2.2 Force advanced audit policies

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

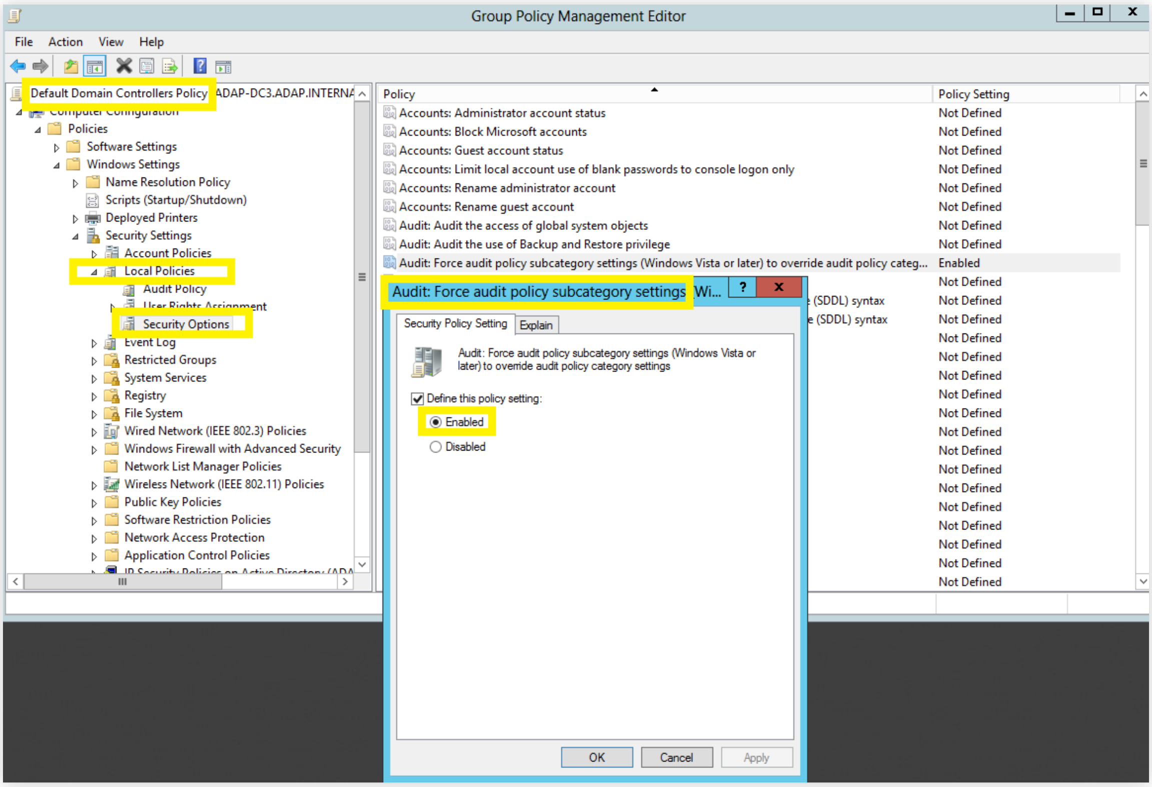
1. Log in to any computer that has the GPMC with Domain Admin credentials. Open the **GPMC,** and based on your setup, you'll either right-click **Default Domain Controllers Policy** or **ADAuditPlusMSPolicy,** then select **Edit.**

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 the audit policy in the ADAuditPlusMSPolicy GPO.

2. In the *Group Policy Management Editor,* go to **Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Security Options.**

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

4. Select **Properties,** then choose **Enabled.**



- Default Domain Controllers Policy ADAP-DC3.ADAP.INTERNA
  - Computer Configuration
    - Policies
      - Software Settings
      - Windows Settings
        - Name Resolution Policy
        - Scripts (Startup/Shutdown)
        - Deployed Printers
        - Security Settings
          - Account Policies
          - Local Policies
            - Audit Policy
            - User Rights Assignment
            - Security Options
          - Event Log
          - Restricted Groups
          - System Services
          - Registry
          - File System
          - Wired Network (IEEE 802.3) Policies
          - Windows Firewall with Advanced Security
          - Network List Manager Policies
          - Wireless Network (IEEE 802.11) Policies
          - Public Key Policies
          - Software Restriction Policies
          - Network Access Protection
          - Application Control Policies
          - IP Security Policies on Active Directory (ADA

Policy	Policy Setting
Accounts: Administrator account status	Not Defined
Accounts: Block Microsoft accounts	Not Defined
Accounts: Guest account status	Not Defined
Accounts: Limit local account use of blank passwords to console logon only	Not Defined
Accounts: Rename administrator account	Not Defined
Accounts: Rename guest account	Not Defined
Audit: Audit the access of global system objects	Not Defined
Audit: Audit the use of Backup and Restore privilege	Not Defined
Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy categ...	Enabled
	Not Defined
(SDDL) syntax	Not Defined
(SDDL) syntax	Not Defined
	Not Defined
	Not Defined
	Not Defined
	Not Defined
	Not Defined
	Not Defined
	Not Defined
	Not Defined
	Not Defined
	Not Defined
	Not Defined
	Not Defined
	Not Defined
	Not Defined

Audit: Force audit policy subcategory settings (Wi...

Security Policy Setting | Explain

Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings

☑ Define this policy setting:

● Enabled

○ Disabled

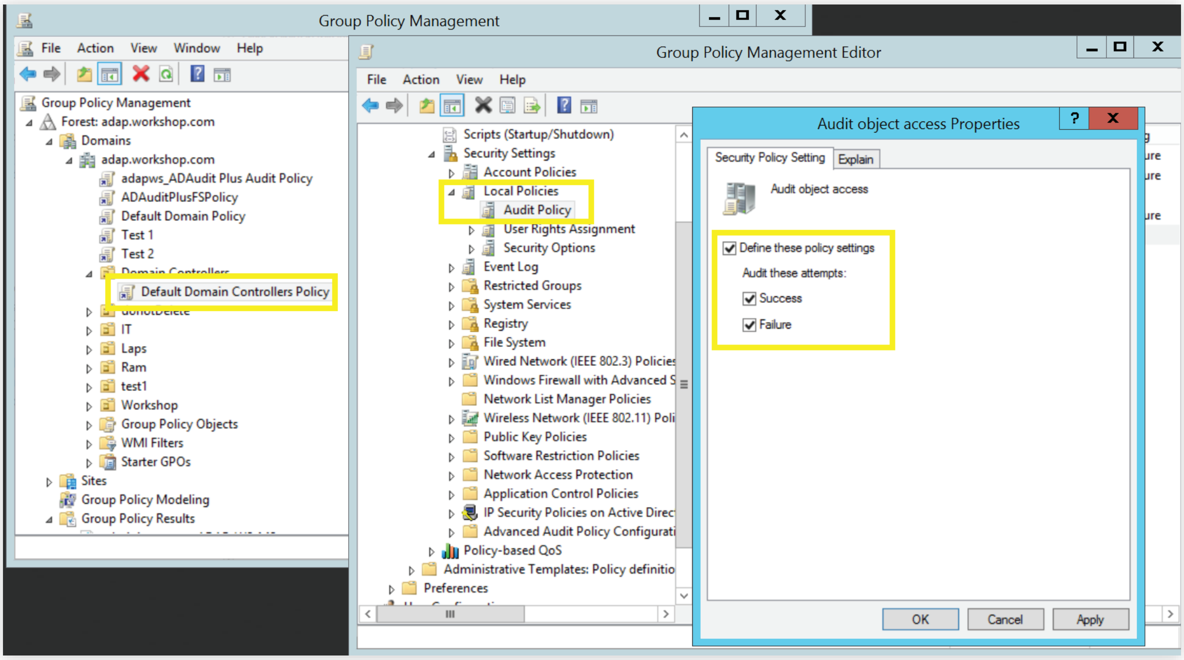
2.2.3 Configure legacy audit policies

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.

2. In the *Group Policy Management Editor*, go to **Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies.**
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.**



Audit object access

☑ Define these policy settings

Audit these attempts:

☑ Success

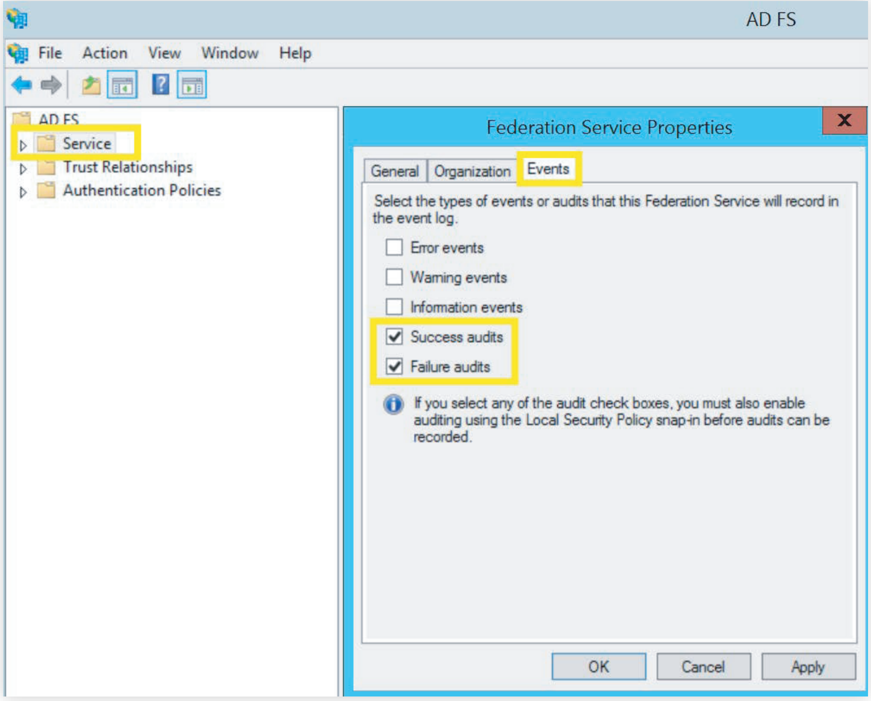
☑ Failure

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.**



Select the types of events or audits that this Federation Service will record in the event log.

☐ Error events

☐ Warning events

☐ Information events

☑ Success audits

☑ Failure audits

If you select any of the audit check boxes, you must also enable auditing using the Local Security Policy snap-in before audits can be recorded.

3.2 Configure claim rules

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

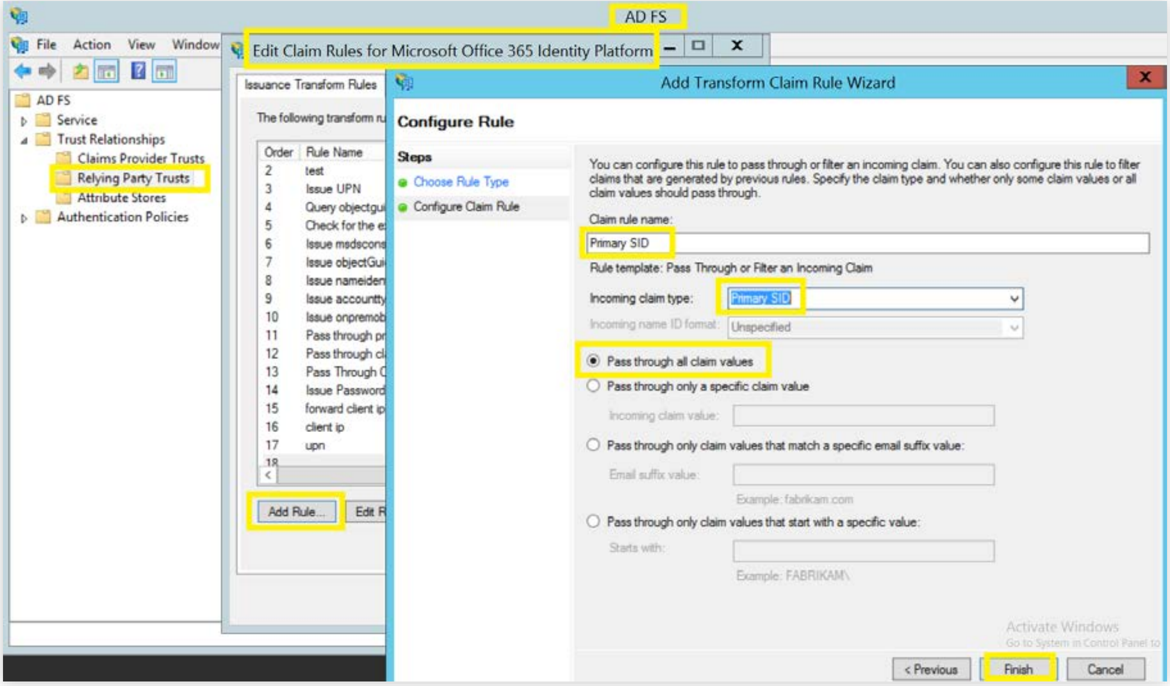
- **i.** Primary SID
- **ii.** UPN
- **iii.** Client IP
- **iv.** Inside Corporate Network
- **v.** Proxy
- **vi.** Forwarded Client IP

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.**



The following transform ru

Order	Rule Name
2	test
3	Issue UPN
4	Query objectgui
5	Check for the e
6	Issue msdscons
7	Issue objectGui
8	Issue nameiden
9	Issue accountty
10	Issue onpremob
11	Pass through pr
12	Pass through cl
13	Pass Through C
14	Issue Password
15	forward client ip
16	client ip
17	upn
18	

Configure Rule

You can configure this rule to pass through or filter an incoming claim. You can also configure this rule to filter claims that are generated by previous rules. Specify the claim type and whether only some claim values or all claim values should pass through.

Claim rule name: Primary SID

Rule template: Pass Through or Filter an Incoming Claim

Incoming claim type: Primary SID

Incoming name ID format: Unspecified

● Pass through all claim values

○ Pass through only a specific claim value

Incoming claim value:

○ Pass through only claim values that match a specific email suffix value:

Email suffix value:

Example: fabrikam.com

○ Pass through only claim values that start with a specific value:

Starts with:

Example: FABRIKAM\

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.