Configure Tenable Vulnerability Management with ADFS SAML

For FedRAMP and Non-FedRAMP Customers

Last Revised: November 07, 2023
Prerequisites

In this walkthrough, we use the DNS FQDN of adfs.example.com as the ADFS instance we are configuring. Consider that your DNS FQDN may vary when observing the steps in this guide.

This document assumes that you have previously setup and configured an ADFS instance on a set of no less than two AD Domain controllers running on Windows Server 2022:

- ADFS Main AD DC
- ADFS Web Application Proxy (WAP)

Microsoft Documentation can assist you with setting up the ADFS instances on an existing Microsoft Active Directory Domain Controller.

This document also assumes that your ADFS Main AD DC runs Active Directory Domain Services (dcpromo), includes a Certificate Authority setup, and is properly configured.

**Note:** This document assumes you update your certificates for your Active Directory Certificate Authority and your ADFS instance on a yearly basis, so that your certificate lifespan is set to one year. Your actual configuration options may vary. Please keep this in mind to avoid issues with expiring certificates when configuring your instance.
Configure MMC to Manage ADFS

To configure the Microsoft Management Console (MMC) to manage ADFS:

1. Open the MMC.exe console.

2. Click File > Add/Remove Snap-in.

   The Add or Remove Snap-ins window appears.

3. In the Available Snap-ins section, select the ADFS Management option and click Add.

   The console adds the snap-in to the Selected Snap-ins section.

4. Click OK.
Configure an ADFS Relying Party Trust

To configure an ADFS Relying Party Trust:

1. Open the MMC.exe console.

2. On the right side of the console, in the **Actions** section, click **Add Relying Party Trust**.

   ![Image of MMC console with Add Relying Party Trust highlighted]

   The **Add Relying Party Trust** wizard appears.

3. In the wizard, select the **Claims aware** radio button.
4. Click **Start**.

5. On the **Select Data Source** page, select the **Enter data about the relying party manually** radio button.
6. Click **Next**.

7. On the **Specify Display Name** page, type a **Display Name** and any **Notes** you want to include.
8. Click **Next**.

9. Because the configuration is already encrypted, on the **Configure Certificate** page, do not make any changes.

10. Click **Next**.

11. On the **Configure URL** page, type the appropriate service URL. In this example, we use `https://fedcloud.tenable.com`.
Note: For FedRAMP deployments, your Tenable sales representative provides this URL. For non-FedRAMP deployments, you must first configure SAML in Tenable Vulnerability Management to determine the appropriate URL.

12. Click Next.

13. On the Configure Identifiers page, in the Relying party trust identifier text box, type the SP Entity ID to which you connected as the Relying Party Trust identifier.
14. Click **Add**.

The wizard adds the identifier to the **Relying party trust identifiers** section.

15. Click **Next**.

16. On the **Choose Access Control Policy** page, select the appropriate access control policy for your environment.

**Note:** In some cases, you may select **Permit Everyone** and let the application determine access. In other cases, you may select **Permit a specific group** to access the relying party. In this example, we choose the latter.
17. In the **Policy** section, click the `<parameter>` hyperlink.

   The **Select Groups** window appears.

18. In the **Select Groups** window, add the specific AD group to which you want to grant access.
19. Click **OK**.

   The wizard adds the selected group where the `<parameter>` hyperlink previously was.

20. Click **Next**.

21. On the **Ready to Add Trust** page, review your configuration.
22. Click **Next**.

23. On the **Finish** page, select the **Configure claims insurance policy for this application** check box.
24. Click **Close**.
Configure ADFS Relying Party Claim Rules

Once you configure the ADFS Relying Party Trust, you must then configure the ADFS Relying Party Claim rules to allow proper communication.

To configure ADFS Relying Party Claim rules:

1. Open the MMC.exe console.

2. In the **Relying Party Trusts** folder, right-click the trust and select **Edit Claim Issuance Policy**.

   ![](image)

   The **Edit Claims Issuance Policy** window appears.

3. Configure two rules:
• Rule one:
  a. Click **Add Rule**.

The **Transform Claim Rule** wizard appears.
b. On the Select Rule Template page, in the Claim rule template drop-down, select Send LDAP Attributes as Claims.

c. Click Next.

d. On the Configure Rule page, configure the following settings:

- Claim rule name
- Attribute store — Select Active Directory
- Mapping of LDAP attributes to outgoing claim types
e. Click Finish.

Rule two:
a. Click **Add Rule**.

![Edit Claim Issuance Policy for NessusCloud](image)

The **Transform Claim Rule** wizard appears.

b. On the **Select Rule Template** page, in the **Claim rule template** drop-down, select **Transform an Incoming Claim**.
c. Click **Next**.

d. On the **Configure Rule** page, configure the following settings:

- **Claim rule name**
- **Outgoing claim type** — select **E-mail Address**
- **Outgoing name ID format** — select **Unspecified**
- **Pass through all claim values** radio button — select radio button
e. Click **Finish**.

You return to the **Edit Claims Issuance Policy** window.

4. Click **OK**.
Download your SAML Metadata File

To download your SAML Metadata.xml file:

1. In your browser, navigate to your ADFS portal.
   
   **Note:** Your login URL varies based on the DNS FQDN you configured. For example, in this case, the ADFS SSO Portal login would be: https://adfs.example.com/adfs/ls/idpinitiatedsignon.

2. Type your login credentials and click **Sign in**.

   ![Sign in](image)

   You log in to the ADFS portal.

3. In your browser, paste your specific IDP address to download the metadata.xml file. In this example, our URL is https://adfs.example.com/FederationMetadata/2007-06/FederationMetadata.xml.

   The ADFS portal downloads the metadata.xml file to your computer. Depending on your browser settings, your browser may notify you that the download is complete.
4. Open the metadata.xml file to ensure it resembles the following screenshot:
Appendix A: Configuring SAML in Tenable Vulnerability Management

To configure Tenable Vulnerability Management SAML in a FedRAMP environment:

1. Provide a copy of your metadata.xml file to your Tenable sales representative.
   The Tenable sales representative provisions your container appropriately. Once provisioned, your representative provides you with the completed URL for your Relying Party Trust.

2. Use this URL when configuring a Relying Party Trust. For more information, see Configure an ADFS Relying Party Trust.

To configure Tenable Vulnerability Management SAML in a non-FedRAMP environment:

Follow the SAML Configuration instructions in the Tenable Vulnerability Management User Guide.