Configure SAML single sign-on with Azure AD

Published: 2021-12-15

You can configure your ExtraHop system to enable users to log in to the system through the Azure AD identity management service.

Before you begin

- You should be familiar with administering Azure AD.
- You should be familiar with administering ExtraHop systems.

These procedures require you to copy and paste information between the ExtraHop system and Google Admin console, so it is helpful to have each system open side-by-side.

Enable SAML on the ExtraHop system

1. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.
2. In the Access Settings section, click **Remote Authentication**.
3. From the Remote authentication method drop-down list, select **SAML**.
4. Click **Continue**.
5. Click **View SP Metadata**. You will need to copy the Assertion Consumer Service (ACS) URL and Entity ID to paste into the Azure configuration in a later procedure.

Configure Azure

In the following procedures, you will create an enterprise application, add users and groups to the application, and configure single sign-on settings.

Create a new application

1. Log in to your Microsoft Azure portal.
2. In the Azure services section, click **Enterprise applications**.
3. Click **New application**.
4. Click **Create your own application**.
5. Type a name for the sensor in the name field. This name appears for your users on the Azure My Apps page.
6. Select **Integrate any other application you don't find in the gallery**.
7. Click **Create**.

The application Overview page appears.

Add users and groups

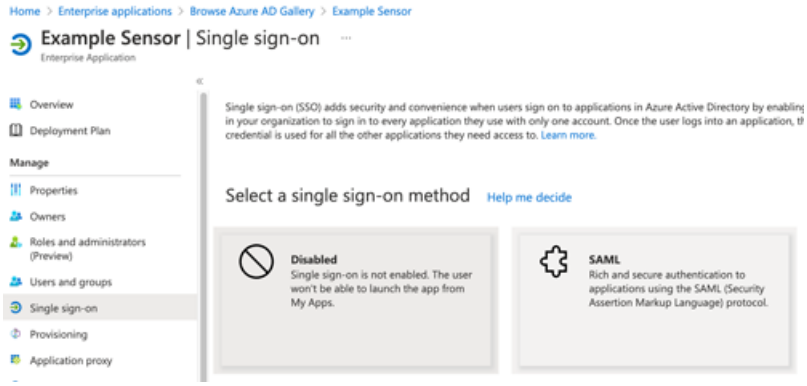
You must assign users or groups to the new application before users can log in to the ExtraHop system.

1. In the left pane, click **Users and groups**.
2. Click **Add user/group**.
3. Add your privileged users or groups and then click **Assign**.

Configure single sign-on

1. In the left pane, click **Single sign-on**.

2. Click **SAML**.



3. In the Basic SAML Configuration section, click **Edit**.
4. Type or paste the Entity ID from the ExtraHop system into the Identifier (Entity ID) field and select the **Default** checkbox. You can delete the existing `http://adapplicationregistry.onmicrosoft.com/customappsso/primary` entry.
5. Type or paste the ACS URL from the ExtraHop system into the **Reply URL (Assertion Consumer Service URL)** field.
6. Click **Save**.
7. In the Attributes & Claims section, click **Edit**.
8. In the required claim section, click **Unique User Identifier (Name ID)**.
9. Click **Choose name identifier format**.
10. From the drop-down list, select **Persistent**.
11. Click **Save**.
12. In the additional claims section, delete the **user.mail** claim from the list and replace the default claim names with the following claim names:

Claim name	Value
`urn:oid:2.5.4.4`	user.surname
`urn:oid:2.5.4.42`	user.givenname
`urn:oid:0.9.2342.19200300.100.1.3`	user.userprincipalname

13. Click **Add new claim**.This claim enables users to access the ExtraHop system with the assigned privileges. If a user is a member of more than one group, the user is granted the most permissive access privilege.
    a) Type `writelevel` in the Name field. You can type any name you want, but it must match the name you will configure on the ExtraHop system.
    b) Click **Claim conditions**.
    c) From the **User type** drop-down list, select **Any**.
    d) Under **Scoped Groups**, click **Select groups**, click the name of the group you want to add, and then click **Select**.
    e) Under **Source**, select **Attribute**.
    f) In the **Value** field, type `unlimited` or a name of your choosing that defines the privilege for this group. Repeat this step for each group that you want to assign unique privileges to. In the example below, we created a claim condition for two groups. One group is assigned unlimited privileges and the other group is assigned read-only privileges.

g) Click **Save**.

14. Return to the Attributes & Claims page and click **Add new claim**. This claim assigns access to packets and session keys.
    a) Type `packetslevel` in the Name field. You can type any name you want, but it must match the name you will configure on the ExtraHop system.
    b) Click **Claim conditions**.
    c) From the **User type** drop-down list, select **Any**.
    d) Under Scoped Groups, click **Select groups**, click the name of the group you want to add, and then click **Select**.
    e) Under Source, select **Attribute**.
    f) In the Value field, type `justpackets` or a name of your choosing that defines the privilege for this group.

Add identity provider information to the ExtraHop system

1. In the Azure SAML Signing Certificate section, next to Certificate (Base64), click Download.

   Note: For Reveal(x) 360 systems, download the Federation Metadata XML file.

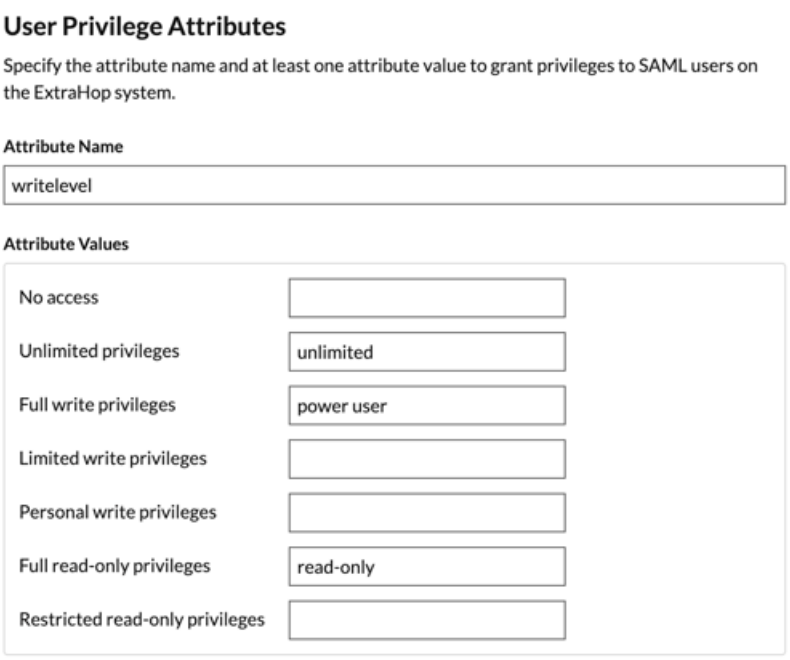
2. Open the downloaded file in a text editor and then copy and paste the contents of the file into the Public Certificate field on the ExtraHop system.
3. In Azure, copy the Login URL and paste it into the SSO URL field on the ExtraHop system.
4. In Azure, copy the Azure AD Identifier and paste it into the Entity ID field on the ExtraHop system.
5. On the ExtraHop system, choose how you would like to provision users from one of the following options.

   - Select **Auto-provision users** to create a new remote SAML user account on the ExtraHop system when the user first logs in to the system.
   - Clear the Auto-provision users checkbox to manually configure new remote users through the ExtraHop Administration settings or REST API.

   The **Enable this identity provider** option is selected by default and allows users to log in to the ExtraHop system. To prevent users from logging in, clear the checkbox. This setting does not appear on Reveal(x) 360.
6. Configure user privilege attributes. You must configure the following set of user attributes before users can log in to the ExtraHop system through an identity provider. These values are user-definable; however, they must match the attribute names that are included in the SAML response from your identity provider. Values are not case sensitive and can include spaces. For more information about privilege levels, see Users and user groups.

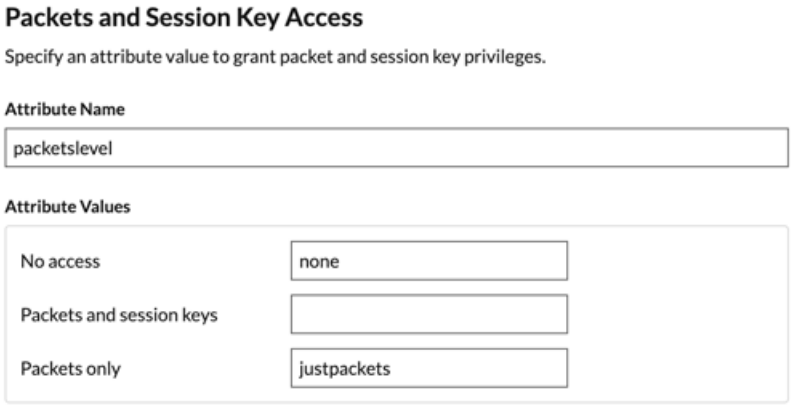
   Important: You must specify the attribute name and configure at least one attribute value other than No access before users can log in.

   In the example below, the Attribute Name field is the claim name specified when creating the ExtraHop application in Azure and the Attribute Values are the claim condition values.



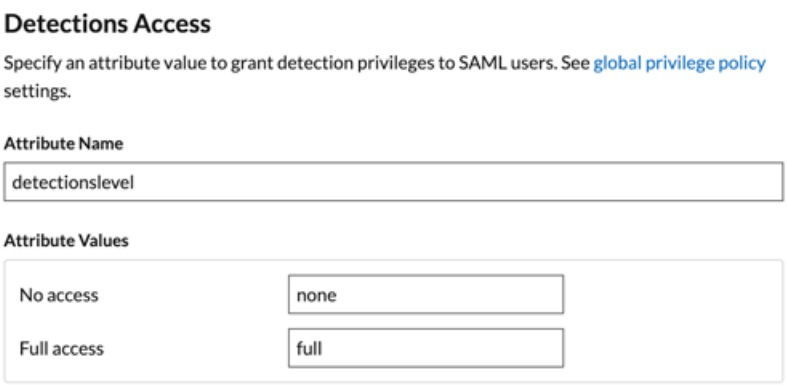
7. Optional: Configure packets and session key access. This step is optional and is only required when you have a connected Trace appliance. Users with unlimited, system and access administration (Reveal(x) 360), or system administration (Reveal(x) 360) privileges are automatically granted access to packets and session keys.

   Note: If you do not have a packet capture appliance, type NA in the Attribute Name field and leave the Attribute Values fields blank.



8. Optional: Configure detections access. This step is optional and is only required when the global privilege policy is set to Only specified users can view detections. Users with unlimited, system and access administration (Reveal(x) 360), or system administration (Reveal(x) 360) privileges are automatically granted access to detections.

   Note: If you do not want users to have access to detections, type NA in the Attribute Name field and leave the Attribute Values fields blank. Users with cloud setup privileges are automatically granted access to detections.



9. Click **Save**.
10. Save the Running Config.

Log in to the ExtraHop system

1. Log in to the ExtraHop system through `https://<extrahop-hostname-or-IP-address>`.
2. Click **Log in with <provider name>**.
3. Sign in to your provider with your email address and password. If multi-factor authentication (MFA) is configured, follow the instructions to set up your MFA app.