

Add your own identity provider to RevealX 360

Published: 2024-05-15

The RevealX 360 system includes a default identity provider (IdP) that enables you to manage your users who access the ExtraHop system. If your company already has an identity provider (IdP) that supports security assertion markup language (SAML) 2.0, you can configure the IdP to manage your users on the ExtraHop system.

To add your identity provider, you will map attributes for user identity and system access between your IdP and the ExtraHop system, and you will generate a metadata XML file that contains the IdP certificate and the attribute information.



Tip: These procedures require you to copy and paste information between the ExtraHop system and your IdP, so it is helpful to have each system open side-by-side.

Prerequisites

Before adding your identity provider (IdP), review these considerations.

System and identity provider

Verify these system and IdP requirements:

- You must have an ExtraHop user account with System and Access Administration privileges to configure RevealX 360.
- Identity providers must meet the following criteria:
 - SAML 2.0
 - Support SP-initiated login flows. IdP-initiated login flows are not supported.
 - Support signed SAML Responses
 - Support HTTP-Redirect binding
- You must have a valid identity provider certificate. If the certificate expires, single sign-on to the ExtraHop RevealX 360 console is disabled for all users in your organization, and system configuration changes will fail.



Tip: The ExtraHop system automatically sends IdP certificate expiration notifications to all users with [System and Access Administration privileges](#). Emails are sent 1 month, 2 weeks, and 1 week prior to the certificate expiration date. Obtain a new certificate from your identity provider and [update your IdP configuration](#).

SAML responses

Ensure that all SAML responses meet these conditions:

- Responses by the SAML identity provider must contain an audience restriction. For example:

```
<saml:AudienceRestriction>
  <saml:Audience>urn:amazon:cognito:sp:yourUserPoolID
</saml:AudienceRestriction>
```

- Responses must contain an `InResponseTo` element in the `Response` object that matches the request ID in the authentication request. For example:

```
<samlp:Response ... InResponseTo="originalSAMLrequestId">
```

- A `SubjectConfirmationData` attribute has `Recipient` and `InResponseTo` values set. For example:

```
<saml:SubjectConfirmation>
  <saml:SubjectConfirmationData ... Recipient="https://yourUserPoolDomain/
saml2/idpresponse" InResponseTo="originalSAMLrequestId">
</saml:SubjectConfirmation>
```

For more information on configuring single sign-on (SSO) authentication to the ExtraHop system through SAML identity providers, see [Configure remote authentication through SAML](#).

Review RevealX 360 access types and privilege levels

There are four types of access, each with their own privilege levels, that you can grant to your users in RevealX 360: user privilege access, packets and session keys access, Network Detection and Response (NDR) module access, and Network Performance Management (NPM) module access.

Familiarize yourself with the following access types and their associated privilege levels. You will map attribute names between both systems in the procedures in this guide.

See [User privileges](#) to learn what users can do in each privilege level in RevealX 360.

User privilege access

Grants users read and write privileges throughout the system. There are 8 available privilege levels: system and access administration, system administration, full write, limited write, personal write, full read-only, restricted read-only, and none.

Packets and session keys access

Grants users the ability to view and download packet captures, with or without the ability to download session keys: No access, Packet slices only, Packets only, or Packets and session keys.

NDR module access

Grants users the ability to view security detections and workflows: No access or Full access.


NPM module access

Grants users the ability to view network performance detections and workflows: No access or Full access.

If you only want to grant your users access to privilege levels for Full write and Full read-only, no packet access, and full detection access, create a worksheet similar to the following example:

Access Type	Privilege Level Name in RevealX 360	Attribute Value in your IdP
User privilege access	Full write	Full Write
User privilege access	Full read-only	Read-Only
Packets access	No access	None
NDR module access	Full access	Full NDR
NPM module access	Full access	Full NPM

Add your IdP SAML application to RevealX 360

1. Log into RevealX 360.
2. Click System Settings  at the top right of the page and then click **All Administration**.
3. Click **User Access**.

- Note the Assertion Consumer Service (ACS) URL and Entity ID, which you will paste into your IdP configuration.
- Paste the ACS URL from RevealX 360 into the **ACS URL** field on your IdP.
- Paste the SP Entity ID from RevealX 360 into the **SP Entity ID** field on your IdP.

Next steps

Leave the IdP settings open and configure attribute mappings next.

Configure attributes that identify the user

You must configure attributes on your IdP that identify the user throughout the ExtraHop system by their first name, last name, and email address. Refer to your identity provider documentation for the correct property names when mapping these attributes or attribute statements.

Complete the following steps on your IdP.

- In the application attribute mapping section, add three attributes.
- In the first attribute, select **email** or similar. (For example, in Okta, this attribute is called **user.email**.)
- For the Service Provider, paste the following string: `urn:oid:0.9.2342.19200300.100.1.3`
- In the second attribute, select **last name** or similar. (For example, in Okta, this attribute is called **user.lastName**.)
- For the Service Provider, paste the following string: `urn:oid:2.5.4.4`
- In the third attribute, select **first name** or similar. (For example, in Okta, this attribute is called **user.firstName**.)
- For the Service Provider, paste the following string: `urn:oid:2.5.4.42`


In Okta for example, the attribute mapping section should look similar to the following:

Service Provider Attribute Name (RevealX 360)	Identity Provider Attribute Name (Okta)
<code>urn:oid:0.9.2342.19200300.100.1.3</code>	user.email
<code>urn:oid:2.5.4.4</code>	user.lastName
<code>urn:oid:2.5.4.42</code>	user.firstName

Configure attributes for system access

You must configure attributes on your identity provider to grant users access to the ExtraHop system. You can type any name for these attributes, but they must match what you configure later in RevealX 360.

You must create at least one attribute for user privilege access. Packet, NDR, and NPM access is optional, but we recommend you create these attributes now.

 **Important:** Attribute values must be less than 2,000 characters.

- In the application attribute mapping section, add four attributes.
- In the first attribute, select custom or similar and type a descriptive name for user privileges, such as `writelevel`.
- For the Service Provider, type a descriptive term to identify the attribute in RevealX 360, such as `write`.
- In the second attribute, select custom or similar and type a descriptive name for packet access, such as `packetslevel`.
- For the Service Provider, type a descriptive term to identify the attribute in RevealX 360, such as `packets`.

6. In the third attribute, select custom or similar and type a descriptive name for NDR module access, such as `ndrlevel`.
7. For the Service Provider, type a descriptive term to identify the attribute in RevealX 360, such as `ndr`.
8. In the fourth attribute, select custom or similar and type a descriptive name for NPM module access, such as `npmlevel`.
9. For the Service Provider, type a descriptive term to identify the attribute in RevealX 360, such as `npm`.
10. Save the settings and then export the application metadata XML file.


In Okta for example, the attribute mapping section should look similar to the following:

Service Provider Attribute Name (RevealX 360)	Identity Provider Attribute Name (IdP)
<code>write</code>	<code>writelevel</code>
<code>packets</code>	<code>packetslevel</code>
<code>ndr</code>	<code>ndrlevel</code>
<code>npm</code>	<code>npmlevel</code>

Configure your identity provider information in RevealX 360

Here are some considerations before you complete the following steps, make sure you have identified the privilege levels you want to grant for your users for each type of system access

1. In RevealX 360, on the User Access page, click **Add Identity Provider**.
2. In the **Provider Name** field, type a name to identify your specific identity provider. This name appears on the ExtraHop system log in page.
The name must meet the following guidelines:
 - Must only include periods, hyphens, and alphanumeric characters
 - Must be between 3 and 32 characters in length
3. Open the metadata file you exported in the previous procedure, and then copy and paste the contents into the **Provider Metadata (XML)** field.
4. Scroll to the User Privilege Attributes section. There are three sections, one for each of the access types.
5. In the **Attribute Name** field, type the name you configured on your IdP for user privilege access.
6. In our example above, we specified `write`. In the **Attribute Values** fields, type the names of the privilege levels you identified for your users. In the figure below, we specified `Full Write` for the **Full write privileges** value.

 **Important:** You must specify the **Attribute Name** and configure at least one attribute value other than **None** to enable users to log in.

Attribute Name

write

Attribute Values

System and access administration	<input type="text"/>
System administration	<input type="text"/>
Full write	Full Write
Limited write	<input type="text"/>
Personal write	<input type="text"/>
Full read-only	<input type="text"/>
Restricted read-only	<input type="text"/>
None	<input type="text"/>

7. Scroll to the Packets and Session Key Access section.
Configuring packets and session key attributes is optional and is only required if you have a connected packetstore. If you do not have a packetstore, type `NA` in the **Attribute Name** field and leave the **Attribute Value** fields blank.
8. In the **Attribute Name** field, type the name you configured on your IdP for packets access. In our example above, we specified `packets`.
9. In the **Attribute Values** fields, type the names of the privilege levels you created for your users. In the figure below, we specified `None`.

Packets and Session Key Access

Specify an attribute value to grant packet and session key privileges.

Attribute Name

packets

Attribute Values

Packets and session keys	<input type="text"/>
Packets only	<input type="text"/>
Packet slices only	<input type="text"/>
No access	None

10. Scroll to the NDR Module Access section.
Configure the NDR module access attribute if you want users to have access to security detections and workflows. Otherwise, type `NA` in the **Attribute Name** field and leave the **Attribute Values** fields blank.
11. In the **Attribute Name** field, type the name you configured on your IdP for NDR module access. In our example above, we specified `ndrlevel`.
12. In the **Attribute Values** fields, type the names of the privilege levels you created for your users. In the figure below, we specified `Full`.

13. Scroll to the NPM Module Access section.

Configure the NPM module access attribute if you want users to have access to performance detections and workflows. Otherwise, type NA in the **Attribute Name** field and leave the **Attribute Values** fields blank.

14. In the **Attribute Name** field, type the name you configured on your IdP for NPM module access. In our example above, we specified `npmlevel`.
15. In the **Attribute Values** fields, type the names of the privilege levels you created for your users. In the figure below, we specified `Full`.

16. Click **Save**. It can take up to two minutes for the IdP configuration to be saved and enabled on the system.

Assign privileges to users in your IdP

You can now add system access attributes and their associated privilege levels to your existing users. You can assign multiple privileges to a user, but the user is always granted the highest privilege when they log in to the system.



Tip: The ExtraHop system supports group attribute statements to easily map user privileges to all members of a specific group. When you configure the ExtraHop application on your identity provider, specify a group attribute name. This name is then entered in the Attribute Name field when you configure the identity provider on the ExtraHop system.


1. In your IdP, select the user you want to grant privileges to.
2. Add an attribute for the type of access you previously defined, such as `writelevel`.
3. In the same row, add the name you specified for the privilege level, such as `Full Write`.

The following figure shows an example of these attributes in JumpCloud:

^ **Custom Attributes**


Create and store custom attributes for this user. Attribute field names must be unique.


add new custom attribute

writelevel	Full Write	
packetslevel	None	
ndrlevel	Full	
npmlevel	Full	

View users in RevealX 360

Users appear on the Users page in RevealX 360 after they log in the first time. If a user does not appear in the table, they are not successfully being authenticated and authorized. Contact ExtraHop Support if you need assistance.

1. Log in to RevealX 360.
2. Click System Settings  at the top right of the page and then click **All Administration**.
3. Click **User Access**. Users that successfully log in to the system appear in the table on the Users page in RevealX 360. The table displays the name of the identity provider and the assigned privileges for each user.
4. Click on a user name to see user details or to delete the user from the system.


 **Important:** When you delete a user, you must also revoke user access to the ExtraHop System through your IdP. Otherwise, the user might be able to log in again.

Update identity provider settings

When you make changes to your identity provider configuration, for example, regenerating the IdP certificate, you must export the new metadata XML file and update the identity provider settings on RevealX 360.

Before you begin

Ensure that you remove unwanted data, such as an expired IdP certificate, from the metadata XML file.

1. Log in to your identity provider.
2. Select the ExtraHop application on your identity provider and export the updated metadata XML file.
3. Open the XML file in a text editor and copy the contents.
4. Log in to RevealX 360 with a user account that has System and access administration privileges.
5. Click the System Settings icon  and then click **User Access**.
6. In the SAML Configuration section, click **Edit Identity Provider**.
7. Paste the contents of the XML file into the Provider Metadata XML field.
8. Click **Save**.

 **Important:** All active users will be logged out after saving the updated configuration.