

Add your own identity provider to Reveal(x) 360

Published: 2021-08-31

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

Before you begin

You must have an ExtraHop Okta user account with OktaAdmin or ApplianceAdmin privileges to configure Reveal(x) 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



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.

Review Reveal(x) 360 access types and privilege levels

There are three types of access, each with their own privilege levels, that you can grant to your users in Reveal(x) 360: user privilege access, packet access, and detections 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 Reveal(x) 360.

User privilege access

Grants users read and write privileges throughout the system. There are 7 available privilege levels: None, Cloud setup, Full write, Limited write, Personal write, Full read-only, and Restricted read-only.

Packet access

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

Detections access

Grants users the ability to view detections: 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 Reveal(x) 360	Attribute Value in your IdP
User privilege access	Full write privilege	Full Write
User privilege access	Full read-only privilege	Read-Only
Packets access	No access	None
Detections access	Full access	Full

Create an application in your IdP

1. Log into Reveal(x) 360.
2. Click the System Settings icon at the top right of the page and then click **Administration**.
3. Click **User Access**.
4. Note the Assertion Consumer Service (ACS) URL and Entity ID, which you will paste into your IdP configuration.
5. Paste the ACS URL from Reveal(x) 360 into the **ACS URL** field on your IdP.
6. Paste the SP Entity ID from Reveal(x) 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.

 **Important:** Reveal(x) 360 expects the SAML assertions for authenticated users to have from one to three single-valued attributes. Multi-valued attributes like group membership lists are not currently supported.

1. In the application attribute mapping section, add three attributes.
2. In the first attribute, select **email** or similar. (For example, in Okta, this attribute is called **user.email**.)
3. For the Service Provider, paste the following string: `urn:oid:0.9.2342.19200300.100.1.3`
4. In the second attribute, select **last name** or similar. (For example, in Okta, this attribute is called **user.lastName**.)
5. For the Service Provider, paste the following string: `urn:oid:2.5.4.4`
6. In the third attribute, select **first name** or similar. (For example, in Okta, this attribute is called **user.firstName**.)
7. 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 (Reveal(x) 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 Reveal(x) 360.

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

Important: Reveal(x) 360 expects the SAML assertions for authenticated users to have from one to three single-valued attributes. Multi-valued attributes like group membership lists are not currently supported.

1. In the application attribute mapping section, add three attributes.
2. In the first attribute, select custom or similar and type a descriptive name for user privileges, such as `writelevel`.
3. For the Service Provider, type a descriptive term to identify the attribute in Reveal(x) 360, such as `write`.
4. In the second attribute, select custom or similar and type a descriptive name, such as `packetslevel`.
5. For the Service Provider, type a descriptive term to identify the attribute in Reveal(x) 360, such as `packets`.
6. In the third attribute, select custom or similar and type a descriptive name, such as `detectionslevel`.
7. For the Service Provider, type a descriptive term to identify the attribute in Reveal(x) 360, such as `detections`.
8. 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 (Reveal(x) 360)	Identity Provider Attribute Name (IdP)
<code>write</code>	<code>writelevel</code>
<code>packets</code>	<code>packetslevel</code>
<code>detections</code>	<code>detectionslevel</code>

Configure your identity provider information in Reveal(x) 360

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 Reveal(x) 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.
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.

User Privilege Attributes

Specify the attribute name and at least one attribute value to grant privileges to SAML users on the ExtraHop system.

Attribute Name

Attribute Values

None	<input type="text"/>
Cloud setup privileges	<input type="text"/>
Full write privileges	<input type="text" value="Full Write"/>
Limited write privileges	<input type="text"/>
Personal write privileges	<input type="text"/>
Full read-only privileges	<input type="text"/>
Restricted read-only privileges	<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 packet capture appliance. If you do not have a packet capture appliance, type `NA` in the **Attribute Name** field and leave the **Attribute Value** fields blank. Users with cloud setup privileges are automatically granted access to packets and session keys.
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

Attribute Values

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

10. Scroll to the Detections Access section.
Configuring detections attributes is optional. 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.
11. In the **Attribute Name** field, type the name you configured on your IdP for detections access. In our example above, we specified `detections`.
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. 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.

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, packetslevel, or detectionslevel.
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:

View users in Reveal(x) 360

Users appear on the Users page in Reveal(x) 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 Reveal(x) 360.
2. Click the System Settings icon at the top right of the page and then click **Administration**.
3. Click **User Access**. Users that successfully log in to the system appear in the table on the Users page in Reveal(x) 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.