

Configure SAML single sign-on with Okta

Published: 2020-04-27

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

Before you begin

- You should be familiar with administrating Okta. These procedures are based on the Okta Classic UI. If you are configuring Okta through the Developer Console, the procedure might be slightly different.
- You should be familiar with administrating ExtraHop systems.

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

Enable SAML on the ExtraHop system

1. Log in to the Administration page 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 ACS URL and Entity ID to paste into the Okta configuration in the next procedure.

Configure SAML settings in Okta

This procedure requires you to copy and paste information between the ExtraHop Admin UI and the Okta Classic UI, so it is helpful to have each UI open side-by-side.

1. Log in to Okta.
2. In the upper-right corner of the page, change the view from **Developer Console** to **Classic UI**.



3. From the top menu, click **Applications**.
4. Click **Add Application**.
5. Click **Create New App**.
6. From the Platform drop-down list, select **Web**.
7. For the Sign on method, select **SAML 2.0**.
8. Click **Create**.
9. In the General Settings section, type a unique name in the App name field to identify the ExtraHop system.
10. Optional: Configure the App logo and App visibility fields as required for your environment.
11. Click **Next**.
12. In the SAML Settings sections, paste the Assertion Consumer Service (ACS) URL from the ExtraHop system into the Single sign on URL field in Okta.



Note: You might need to manually edit the ACS URL if the URL contains an unreachable hostname, such as the default appliance hostname "extrahop". We recommend that you specify the fully qualified domain name for the ExtraHop appliance in the URL.

13. Paste the SP Entity ID from the ExtraHop system into the Audience URI (SP Entity ID) field in Okta.
14. From the Name ID format drop-down list, select **Persistent**.
15. From the Application username drop-down list, select a username format.
16. In the Attribute Statements section, add the following statements exactly as shown. The first four attributes are required. The **user.packetsLevel** and **user.detectionsAccessLevel** attributes are optional. If you have a Trace appliance and you do not configure the **user.packetsLevel** attribute, users will be unable to view or download packet captures in the ExtraHop Web UI.

Name	Name format	Value
<code>urn:oid:0.9.2342.19200300.1001.3</code>	URI Reference	user.email
<code>urn:oid:2.5.4.4</code>	URI Reference	user.lastName
<code>urn:oid:2.5.4.42</code>	URI Reference	user.firstName
<code>urn:extrahop:saml:2.0:writeLevel</code>	URI Reference	user.writeLevel
<code>urn:extrahop:saml:2.0:packetsLevel</code>	URI Reference	user.packetsLevel
<code>urn:extrahop:saml:2.0:detectionsAccessLevel</code>	URI Reference	user.detectionsAccessLevel

The following figure shows a completed example.

A SAML Settings

GENERAL

Single sign on URL ?

Use this for Recipient URL and Destination URL

Allow this app to request other SSO URLs

Audience URI (SP Entity ID) ?

Default RelayState ?

If no value is set, a blank RelayState is sent

Name ID format ?

Application username ?

[Show Advanced Settings](#)

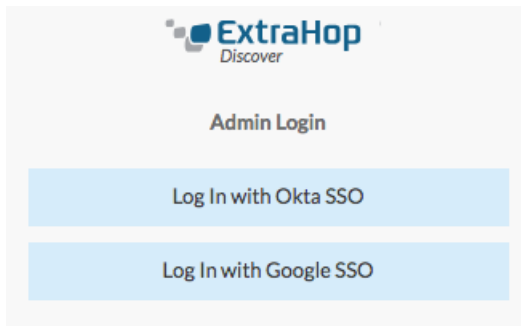
ATTRIBUTE STATEMENTS (OPTIONAL) [LEARN MORE](#)

Name	Name format (optional)	Value	
<input type="text" value="urn:oid:0.9.2342.19200301"/>	<input type="text" value="URI Reference"/>	<input type="text" value="user.email"/>	<input type="text" value="x"/>
<input type="text" value="urn:oid:2.5.4.4"/>	<input type="text" value="URI Reference"/>	<input type="text" value="user.lastName"/>	<input type="text" value="x"/>
<input type="text" value="urn:oid:2.5.4.42"/>	<input type="text" value="URI Reference"/>	<input type="text" value="user.firstName"/>	<input type="text" value="x"/>
<input type="text" value="urn:extrahop:saml:2.0:writ"/>	<input type="text" value="URI Reference"/>	<input type="text" value="user.writeLevel"/>	<input type="text" value="x"/>
<input type="text" value="urn:extrahop:saml:2.0:pack"/>	<input type="text" value="URI Reference"/>	<input type="text" value="user.packetsLevel"/>	<input type="text" value="x"/>

- Click **Next** and then click **Finish**.
You are returned to the Sign On settings page.
- In the Settings section, click **View Setup Instructions**.
A new browser window opens and displays information that is required to configure the ExtraHop system.

Add identity provider information on the ExtraHop system

- Return to the Admin UI on the ExtraHop system. Close the Service Provider metadata window if it is still open, and then click **Add Identity Provider**.
- Type a unique name in the Provider Name field. This name appears on the ExtraHop system login page.



3. From Okta, copy the Identity provider single sign-on URL and paste into the SSO URL field on the ExtraHop system.
4. From Okta, copy the Identity Provider Issuer URL and paste into the Entity ID field on the ExtraHop system.
5. From Okta, copy the X.509 certificate and paste into the Signing Certificate field on the ExtraHop system.
6. 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 appliance.
 - Clear the Auto-provision users checkbox and manually configure new remote users through the ExtraHop Admin UI or REST API. Access and privilege levels are determined by the user configuration in Okta.
7. 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.
8. Click **Save**.
9. [Save the Running Config](#).

Configure user privilege attributes in Okta

You must add ExtraHop privilege attributes to Okta. These attributes enable you to assign write-level, detections-level, and packet-level access to your Okta users. You only need to configure user privilege attributes once in your Okta environment. These attributes can then be assigned to any Okta user profile.

Configure write access

1. Return to the main administration page in Okta.
2. From the Directory menu, select **Profile Editor**.
3. Click **Okta** in the left pane to locate the built-in Okta user.
4. In the Actions column, click **Profile**.

Profile Editor

5. In the Attributes section, click **Add Attribute**.
6. From the Data type drop-down menu, select **string**.
7. In the Display Name field, type `Write Level`.
8. In the Variable name field, type `writeLevel`.

9. Click **Save and Add Another**.

Configure detections access

The `Detections Access Level` attribute is only required when the [global privilege policy](#) is set to **Only specified users can view detections**.

1. From the Data type drop-down menu, select **string**.
2. In the Display name field, type `Detections Access Level`.
3. In the Variable name field, type `user.detectionsAccessLevel`.

Add Attribute

Data type: string

Display name: Detections Access Level

Variable name: user.detectionsAccessLevel

Description:

Enum: Define enumerated list of values

Attribute Length: Between

min: min

and

max: max

Attribute required: Yes

Buttons: Cancel, Save, Save and Add Another

4. Click **Save and Add Another**.

Configure packet access

1. From the Data type drop-down menu, select **string**.
2. In the Display Name field, type `Packets Level`.
3. In the Variable name field, type `packetsLevel`.

Add Attribute

Data type	<input type="text" value="string"/>
Display name ?	<input type="text" value="Packets Level"/>
Variable name ?	<input type="text" value="packetsLevel"/>
Description	<input type="text"/>
Enum	<input type="checkbox"/> Define enumerated list of values
Attribute Length	<input type="text" value="Between"/> <input type="text" value="min"/> and <input type="text" value="max"/>
Attribute required	<input type="checkbox"/> Yes

4. Click **Save**.

Assign the ExtraHop system to Okta users

We assume that you already have users configured in Okta. If you do not, refer to the Okta documentation to add new users.

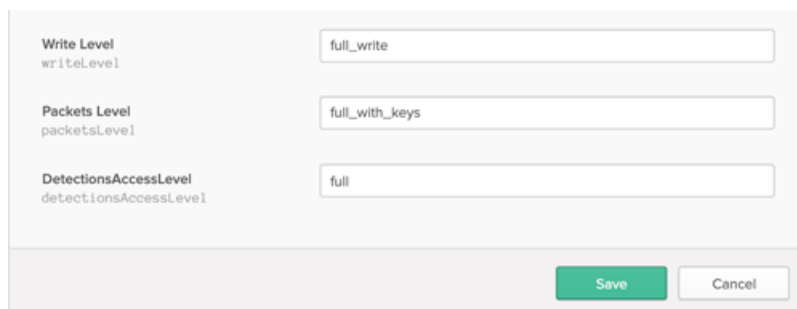
1. From the Directory menu, select **People**.
2. Click the name of the user.
3. Click **Assign Applications**.
4. Locate the name of the application you configured for the ExtraHop system and click **Assign**.

5. Confirm the email address in the User Name field and then click **Save and Go Back**.
6. Click **Done**.
7. Click **Profile**.
8. Click **Edit**.
9. In the Write Level field, type one of the following user types:

- unlimited
- full_write
- limited_write
- personal_write
- full_readonly
- restricted_readonly

For information about user privileges, see [Users and user groups](#).

10. Optional: If you configured the `user.packetLevel` attribute in the first procedure, configure the Packets Level field by typing one of the following user types:
 - full
 - full_with_keys
 - none
11. Optional: If you configured the `user.detectionsAccessLevel` attribute in the first procedure, type one of the following access types in the Detections Access Level field:
 - full
 - none



Write Level writeLevel	full_write
Packets Level packetsLevel	full_with_keys
DetectionsAccessLevel detectionsAccessLevel	full

12. Click **Save**.
Users must have an active Okta account with a valid password before they can log in to the ExtraHop system.

Log in to the ExtraHop system

1. Open a new browser window and enter the URL of the ExtraHop Web UI.
2. Click **Log in with <provider name>**.
3. Sign into your provider with your email address and password. You are automatically directed to the ExtraHop Dashboards page.