

Configure remote authentication through SAML

Published: 2020-04-01

You can configure secure, single sign-on (SSO) authentication to the ExtraHop system through one or more security assertion markup language (SAML) identity providers.

When a user logs in to an Command or Discover appliance that is configured as a service provider (SP) for SAML SSO authentication, the ExtraHop appliance requests authorization from the appropriate identity provider (IdP). The identity provider authenticates the user's credentials and then returns the authorization for the user to the ExtraHop appliance. The user is then able to access the ExtraHop system.

Configuration guides for specific identity providers are linked below. If your provider is not listed, apply the settings required by the ExtraHop system to your identity provider.

Identity providers must meet the following criteria:

- SAML 2.0
- Support SP-initiated login flows
- Support signed SAML Responses

Enable SAML remote authentication

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. Select **SAML** from the remote authentication method drop-down list and then click **Continue**.
- Click **View SP Metadata** to view the Assertion Consumer Service (ACS) URL and Entity ID of the ExtraHop system. These strings are required by your identity provider to configure SSO authentication. You can also download a complete XML metadata file that you can import into your identity provider configuration.



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 system in the URL.

- Click **Add Identity Provider** to add the following information:
 - **Provider Name:** Type a name to identify your specific identity provider. This name appears on the ExtraHop system log in page after the **Log in with** text.
 - **Entity ID:** Paste the entity ID provided by your identity provider into this field.
 - **SSO URL:** Paste the single sign-on URL provided by your identity provider into this field.
 - **Signing Certificate:** Paste the X.509 certificate provided by your identity provider into this field.
 - **Auto-provision users:** When this option is selected, ExtraHop user accounts are automatically created when the user logs in through the identity provider. To manually control which users can log in, clear this checkbox and manually configure new remote users through the ExtraHop Admin UI or REST API. Any manually-created remote username should match the username configured on the identity provider.
 - **Enable this identity provider:** This option is selected by default and allows users to log in to the ExtraHop system. To prevent users from logging in through this identity provider, clear the checkbox.

After the identity provider is configured, a table of all configured identity providers appears in a table. You can edit or delete the identity provider as needed.

Required attributes

You must configure the following set of user attributes before users can connect to the ExtraHop system through an identity provider. These attributes identify the user and allow ExtraHop-specific privileges.

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

The `packetslevel` attribute is only required if you have a connected Trace appliance.

Attribute	Friendly Name	Category	Description
<code>urn:oid:0.9.2342.19200300.100.1.3</code>	email	Standard Attribute	Primary email address
<code>urn:oid:2.5.4.4</code>	sn	Standard Attribute	Last name
<code>urn:oid:2.5.4.42</code>	givenName	Standard Attribute	First name
<code>urn:extrahop:saml:2.0.writelevel</code>	Write Level	ExtraHop Attribute	Web UI, Admin UI, and REST API privileges
<code>urn:extrahop:saml:2.0.detectionsaccesslevel</code>	Detections Access	ExtraHop Attribute	Detections access
<code>urn:extrahop:saml:2.0.packetslevel</code>	Packet and Session Key Access	ExtraHop Attribute	Packet and session key access

Privilege levels

Write level privileges must be assigned to each user to control their access to the Web UI, Admin UI, and REST API. Optionally, you can assign access to detections, and if you have a connected Trace appliance, you can assign access to packets and session keys. For more information about privilege levels, see [Users and user groups](#).

writelevel Attribute Privileges

unlimited

full_write

limited_write

personal_write

full_readonly

restricted_readonly

none

detectionsaccesslevel Attribute Privileges

full

none

packetslevel Attribute Privileges

full

full_with_keys

none

Next steps

- [Configure SAML single sign-on with Okta](#)
- [Configure SAML single sign-on with Google](#)