Configure remote authentication through SAML

Published: 2023-01-26

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 ExtraHop system that is configured as a service provider (SP) for SAML SSO authentication, the ExtraHop system 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 system. 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. IdP-initiated login flows are not supported.
- Support signed SAML Responses
- Support HTTP-Redirect binding

The example configuration in this procedure enables access to the ExtraHop system through group attributes.

If your identity provider does not support group attribute statements, configure user attributes with the appropriate write, packets, and detections access privileges.

Enable SAML remote authentication

> ⚠ **Warning:** If your system is already configured with a remote authentication method, changing these settings will remove any users and associated customizations created through that method, and remote users will be unable to access the system. Local users are unaffected.

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. 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:** The ACS URL includes the hostname configured in Network Settings. If the ACS URL contains an unreachable hostname, such as the default system hostname `extrahop`, you must edit the URL when adding the ACS URL to your identity provider and specify the fully qualified domain name (FQDN) of the ExtraHop system.

- 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 Administration settings 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.

- **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. 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 to enable users to log in.

In the example below, the Attribute Name field is the group attribute configured when creating the ExtraHop application on the identity provider and the attribute value is the name of one of your user groups. If a user is a member of more than one group, the user is granted the most permissive access privilege.

- **Packets and Session Key Access:** Configuring packets and session key attributes is optional and only required when you have a connected ExtraHop packetstore.

Packets and Session Key Access

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

Attribute Name

groupMemberships

Attribute Values

No access	
Packets and session keys	Security Administrators
Packets only	

- **Detections Access:** Configuring detections attributes is optional and only required when the global privilege policy ⧉ is set to **Only specified users can view detections**. Users with Unlimited, System Administration, or System and Access Administration (Reveal(x) 360) privileges are automatically granted access to detections.

Detections Access

Specify an attribute value to grant detection privileges to SAML users. See global privilege policy settings.

Attribute Name

groupMemberships

Attribute Values

No access	
All detections	Security Administrators

User attribute mapping

You must configure the following set of user attributes in the application attribute mapping section on your identity provider. These attributes identify the user throughout the ExtraHop system. Refer to your identity provider documentation for the correct property names when mapping attributes.

ExtraHop Attribute Name	Friendly Name	Category	Identity Provider Attribute Name
urn:oid:0.9.2342.19200300.100.1.3	mail	Standard Attribute	Primary email address
urn:oid:2.5.4.4	sn	Standard Attribute	Last name
urn:oid:2.5.4.42	givenName	Standard Attribute	First name

Group attribute statements

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.

If your identity provider does not support group attribute statements, configure user attributes with the appropriate write, packets, and detections access privileges.

Next steps

- Configure SAML single sign-on with JumpCloud
- Configure SAML single sign-on with Google
- Configure SAML single sign-on with Okta