Configure remote authentication through SAML

Published: 2023-07-10

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 privileges for module access, system access, and packet forensics.

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.

  • **Public 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 user privilege attributes before users can log in to the ExtraHop system through an identity provider. Values are not case sensitive and can include spaces.

The names and values of user privilege attributes must match the names and values your identity provider includes in SAML responses, which are configured when you add the ExtraHop application to a provider. For example, in Azure AD, you configure claim names and claim condition values that must match the names and values of user privilege attributes in the ExtraHop system. For more detailed examples, see the following topics:

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

Note: If a user matches multiple attribute values, the user is granted the most permissive access privilege. For example, if a user matches both Limited write and Full write values, the user is granted Full write privileges. For more information about privilege levels, see Users and user groups.

• **NDR Module Access:** NDR attributes enable users to access NDR features.

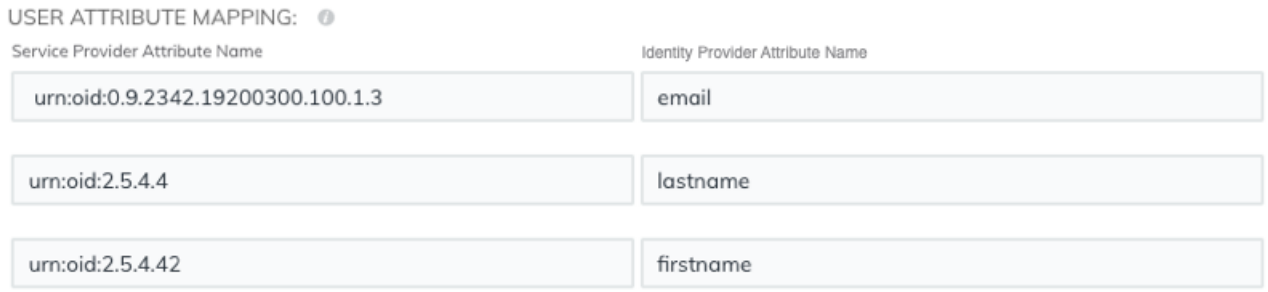
• **NPM Module Access:** NPM attributes enable users to access NPM features.

• **Packets and Session Key Access:** Packets and session key attributes enable users to access packets and session keys. Configuring packets and session key attributes is optional and only required when you have a connected ExtraHop packetstore.

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 privileges for module access, system access, and packet forensics.

Next steps

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