

SAML-Single-Sign-On mit JumpCloud konfigurieren

Veröffentlicht: 2023-09-14

Sie können Ihr ExtraHop-System so konfigurieren, dass sich Benutzer über den JumpCloud-Identitätsverwaltungsdienst am System anmelden können.

Bevor Sie beginnen

- Sie sollten mit der Verwaltung von JumpCloud vertraut sein.
- Sie sollten mit der Verwaltung von ExtraHop-Systemen vertraut sein.

Bei diesen Verfahren müssen Sie Informationen zwischen dem ExtraHop-System und JumpCloud kopieren und einfügen. Daher ist es hilfreich, jedes System nebeneinander zu öffnen.

SAML auf dem ExtraHop-System aktivieren

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. Klicken Sie im Abschnitt Zugriffseinstellungen auf **Fernauthentifizierung**.
3. Aus dem Methode zur Fernauthentifizierung Drop-down-Liste, wählen **SAML**.
4. klicken **Weiter**.
5. klicken **SP-Metadaten anzeigen**. Sie müssen die ACS-URL und die Entitäts-ID kopieren, um sie im nächsten Verfahren in die JumpCloud-Konfiguration einzufügen.

SAML-Einstellungen in JumpCloud konfigurieren

1. Melden Sie sich bei der JumpCloud-Administratorkonsole an über `https://console.jumpcloud.com/`.
2. Klicken Sie im linken Bereich unter Benutzerauthentifizierung auf **SSO**.
3. klicken **Neue Anwendung hinzufügen**.
4. klicken **Benutzerdefinierte SAML-App**.



5. Auf dem Neues SSO Seite, in der Allgemeine Informationen Abschnitt, geben Sie einen Namen zur Identifizierung des ExtraHop-Systems in der Etikett anzeigen Feld.
6. Klicken Sie auf **SSO** klicken Sie auf die Tabulatortaste und konfigurieren Sie die folgenden Felder:

- **ID der IdP-Entität:**

Geben Sie eine beliebige Zeichenfolge ein. Diese ID ist erforderlich, wenn Sie den Identity Provider auf dem ExtraHop-System konfigurieren.

- **SP-Entitäts-ID:** Geben Sie die Entitäts-ID aus dem ExtraHop-System ein oder fügen Sie sie ein.
- **ACS-URLs:** Geben Sie die URL des Assertion Consumer Service (ACS) aus dem ExtraHop-System ein oder fügen Sie sie ein.
- **SP-Zertifikat:** Lassen Sie dieses Feld leer, damit JumpCloud ein neues Zertifikat generiert. Alternativ können Sie Ihr eigenes Zertifikat vorlegen.
- **SAML-Betreffname/ID:** Wählen **E-Mail senden** aus der Drop-down-Liste.

- **SAML-Format für Betreffname/ID:** Wählen **urn:oasis:names:tc:saml:2.0:nameid-format:persistent** aus der Drop-down-Liste.
- **Signatur-Algorithmus:** Wählen **RSA-SHA256** aus der Drop-down-Liste.
- **Standard-RelayState:** Lassen Sie dieses Feld leer.
- **Anmelde-URL:** Lassen Sie dieses Feld leer.
- **IdP-URL:** Geben Sie einen identifizierenden Namen in das Feld ein. Die URL sieht ähnlich aus wie im folgenden Beispiel: `https://sso.jumpcloud.com/saml2/extrahop`.

7. In der Zuordnung von Benutzerattributen Abschnitt, klicken **Attribut hinzufügen** und geben Sie die folgenden Zeichenketten ein. Diese Attribute identifizieren den Benutzer im gesamten ExtraHop-System.

Name des Service Provider-Attributs	JumpCloud-Attributname
urn:oid:0.9.2342.19200300.100.1.3	E-Mail senden
urn: oid: 2.5.4.4	Nachname
urn: oid: 2.5.4.42	Vorname

USER ATTRIBUTE MAPPING: ⓘ

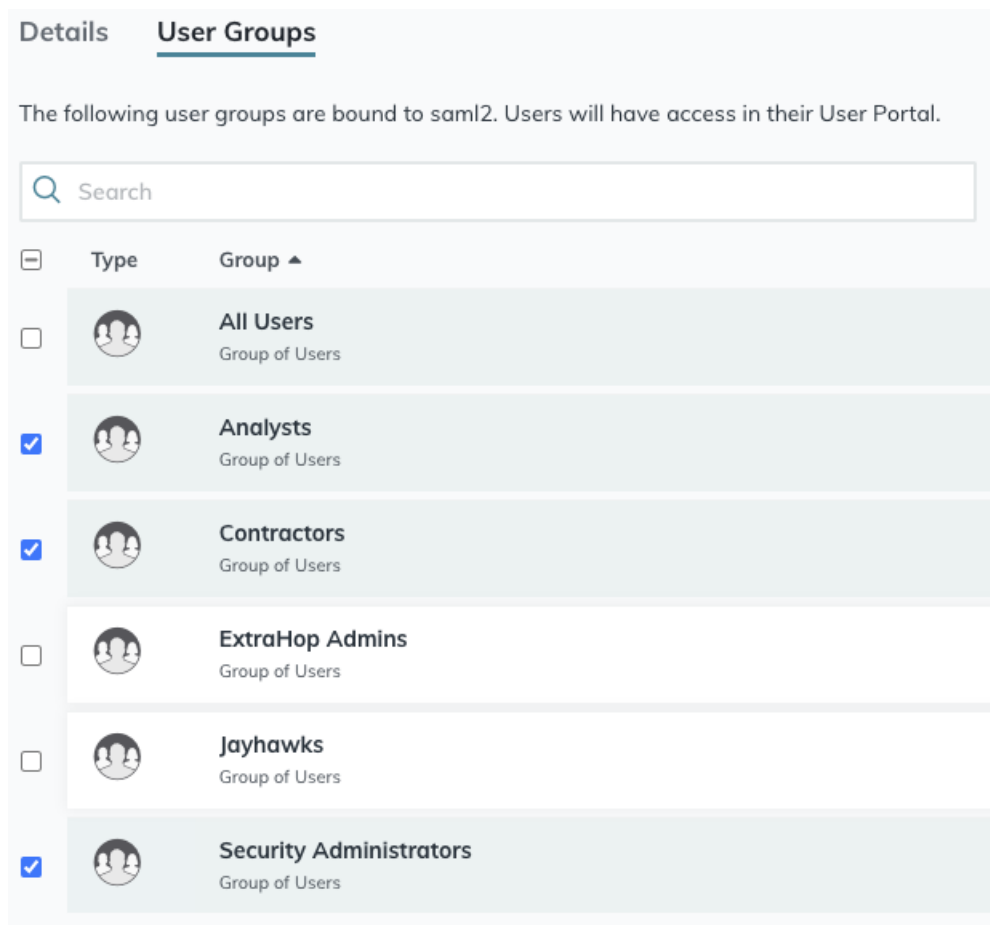
Service Provider Attribute Name	JumpCloud Attribute Name
urn:oid:0.9.2342.19200300.100.1.3	email
urn:oid:2.5.4.4	lastname
urn:oid:2.5.4.42	firstname

8. In der Attribute gruppieren Abschnitt, wählen **Gruppenattribut einbeziehen** und geben Sie einen Namen in das Feld ein, um die Gruppe zu identifizieren. Sie geben diesen Namen an, wenn Sie Benutzerberechtigungsattribute auf dem ExtraHop-System konfigurieren.

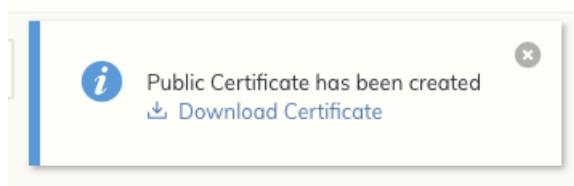
GROUP ATTRIBUTES ⓘ

include group attribute

9. Klicken Sie auf **Benutzergruppen** Registerkarte.
10. Wählen Sie alle Gruppen aus, die Zugriff auf das ExtraHop-System haben sollen. Im folgenden Beispiel werden drei Gruppen ausgewählt.




11. klicken **aktivieren**.
12. klicken **Weiter** um die neuen Einstellungen zu bestätigen.
JumpCloud generiert ein Zertifikat, nachdem die Anwendung erstellt wurde. klicken **Zertifikat herunterladen** und speichern Sie die Datei auf Ihrem Computer.



Fügen Sie Informationen zum Identitätsanbieter im ExtraHop-System hinzu

1. Kehren Sie zu den Administrationseinstellungen des ExtraHop-Systems zurück. Schließen Sie das Service Provider-Metadatenfenster, falls es noch geöffnet ist, und klicken Sie dann auf **Identitätsanbieter hinzufügen**.
2. Geben Sie einen eindeutigen Namen in das Name des Anbieters Feld. Dieser Name erscheint auf der Anmeldeseite des ExtraHop-Systems.
3. Kopieren Sie von JumpCloud die ID der IdP-Entität und füge es in das Entitäts-ID Feld auf dem ExtraHop-System.
4. Kopieren Sie von JumpCloud die IDP-URL und füge es in das SSO-URL Feld auf dem ExtraHop-System.

5. Öffne das `certificate.pem` Datei in einem Texteditor, kopieren Sie die Zertifikatsdaten und fügen Sie sie in das Öffentliches Zertifikat Feld auf dem ExtraHop-System.
6. Wählen Sie aus einer der folgenden Optionen aus, wie Sie Benutzer bereitstellen möchten.
 - Wählen Sie Benutzer automatisch bereitstellen, um ein neues Remote-SAML-Benutzerkonto auf dem ExtraHop-System zu erstellen, wenn sich der Benutzer zum ersten Mal am System anmeldet.
 - Deaktivieren Sie das Kontrollkästchen Benutzer automatisch bereitstellen und konfigurieren Sie neue Remote-Benutzer manuell über die ExtraHop-Administrationseinstellungen oder die REST-API.
7. Die **Diesen Identitätsanbieter aktivieren** Die Option ist standardmäßig ausgewählt und ermöglicht es Benutzern, sich beim ExtraHop-System anzumelden. Um zu verhindern, dass sich Benutzer anmelden, deaktivieren Sie das Kontrollkästchen.
8. Konfigurieren Sie Benutzerberechtigungsattribute. Sie müssen die folgenden Benutzerattribute konfigurieren, bevor sich Benutzer über einen Identitätsanbieter beim ExtraHop-System anmelden können. Werte sind benutzerdefiniert, müssen jedoch mit den Attributnamen übereinstimmen, die in der SAML-Antwort Ihres Identity Providers enthalten sind. Bei Werten wird nicht zwischen Groß- und Kleinschreibung unterschieden und sie können Leerzeichen enthalten. Weitere Informationen zu Berechtigungsstufen finden Sie unter [Benutzer und Benutzergruppen](#).

 **Wichtig:** Sie müssen den Attributnamen angeben und mindestens einen anderen Attributwert konfigurieren als **Kein Zugriff** um Benutzern die Anmeldung zu ermöglichen.

Im folgenden Beispiel ist der Name des Attributs Feld ist das Gruppenattribut, das bei der Erstellung der ExtraHop-Anwendung auf dem Identity Provider konfiguriert wurde, und Attributwerte sind die Namen Ihrer Benutzergruppen. Wenn ein Benutzer Mitglied von mehr als einer Gruppe ist, wird ihm die zulässige Zugriffsberechtigung gewährt.

User Privileges

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

Attribute Name

Attribute Values

System and access administration	<input type="text" value="Security Administrators"/>
Full write	<input type="text"/>
Limited write	<input type="text" value="Contractors"/>
Personal write	<input type="text"/>
Full read-only	<input type="text"/>
Restricted read-only	<input type="text"/>
No access	<input type="text"/>

9. Konfigurieren Sie den Zugriff auf das NDR-Modul.

NDR Module Access

Specify an attribute value to grant access to security detections and views.

Attribute Name

Attribute Values

Full access	<input type="text" value="Security Administrators"/>
No access	<input type="text"/>

- Konfigurieren Sie den NPM-Modulzugriff.

NPM Module Access

Specify an attribute value to grant access to performance detections and views.

Attribute Name

Attribute Values

Full access	<input type="text" value="Security Administrators"/>
No access	<input type="text"/>

- Optional: Konfigurieren Sie Pakete und den Zugriff auf Sitzungsschlüssel. Dieser Schritt ist optional und nur erforderlich, wenn Sie einen verbundenen Packetstore haben.


Packets and Session Key Access

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

Attribute Name

Attribute Values

Packets and session keys	<input type="text" value="Security Administrators"/>
Packets only	<input type="text"/>
Packet slices only	<input type="text"/>
No access	<input type="text"/>

- klicken **Speichern**.
- [Speichern Sie die laufende Konfiguration](#) .

Loggen Sie sich in das ExtraHop-System ein

- Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
- klicken **Loggen Sie sich ein mit** `<provider name>`.
- Melden Sie sich mit Ihrer E-Mail-Adresse und Ihrem Passwort bei Ihrem Anbieter an. Sie werden automatisch zur ExtraHop-Übersichtsseite weitergeleitet.