Configurer l'authentification unique SAML avec JumpCloud

Publié: 2025-02-13

Vous pouvez configurer votre système ExtraHop pour permettre aux utilisateurs de se connecter au système via le service de gestion des identités JumpCloud.

Avant de commencer

- Vous devez être familiarisé avec l'administration de JumpCloud.
- Vous devez être familiarisé avec l'administration des systèmes ExtraHop.

Ces procédures vous obligent à copier-coller des informations entre le système ExtraHop et JumpCloud. Il est donc utile d'ouvrir chaque système côte à côte.

Activez SAML sur le système ExtraHop

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans la section Paramètres d'accès, cliquez sur **Authentification à distance**.
3. À partir du méthode dqu`authentification à distance menu déroulant, sélectionnez **SAML**.
4. Cliquez **Continuer**.
5. Cliquez **Afficher les métadonnées SP**. Vous devrez copier l' URL ACS et l'ID d'entité à coller dans la configuration JumpCloud lors de la procédure suivante .

Configurer les paramètres SAML dans JumpCloud

1. Connectez-vous à la console d'administration de JumpCloud via `https://console.jumpcloud.com/`.
2. Dans le volet de gauche, sous Authentification utilisateur, cliquez sur **SSO**.
3. Cliquez **Ajouter une nouvelle application**.
4. Cliquez **Application SAML personnalisée**.

5. Sur le Nouveau SSO page, dans la Informations générales section, saisissez un nom pour identifier le système ExtraHop dans le Étiquette d'affichage champ.
6. Cliquez sur **SSO** onglet et configurez les champs suivants :

   • **ID d'entité IdP:**

   Tapez n'importe quelle chaîne de caractères. Cet ID est requis lorsque vous configurez le fournisseur d'identité sur le système ExtraHop.

   • **ID d'entité SP:** Tapez ou collez l'ID d'entité depuis le système ExtraHop.

   • **URL ACS:** Tapez ou collez l'URL ACS (Assertion Consumer Service) depuis le système ExtraHop.

   • **Certificat SP:** Laissez ce champ vide pour que JumpCloud génère un nouveau certificat. Vous pouvez également fournir votre propre certificat.

   • **Identifiant du sujet SAML:** Sélectionnez **courriel** depuis le menu déroulant.

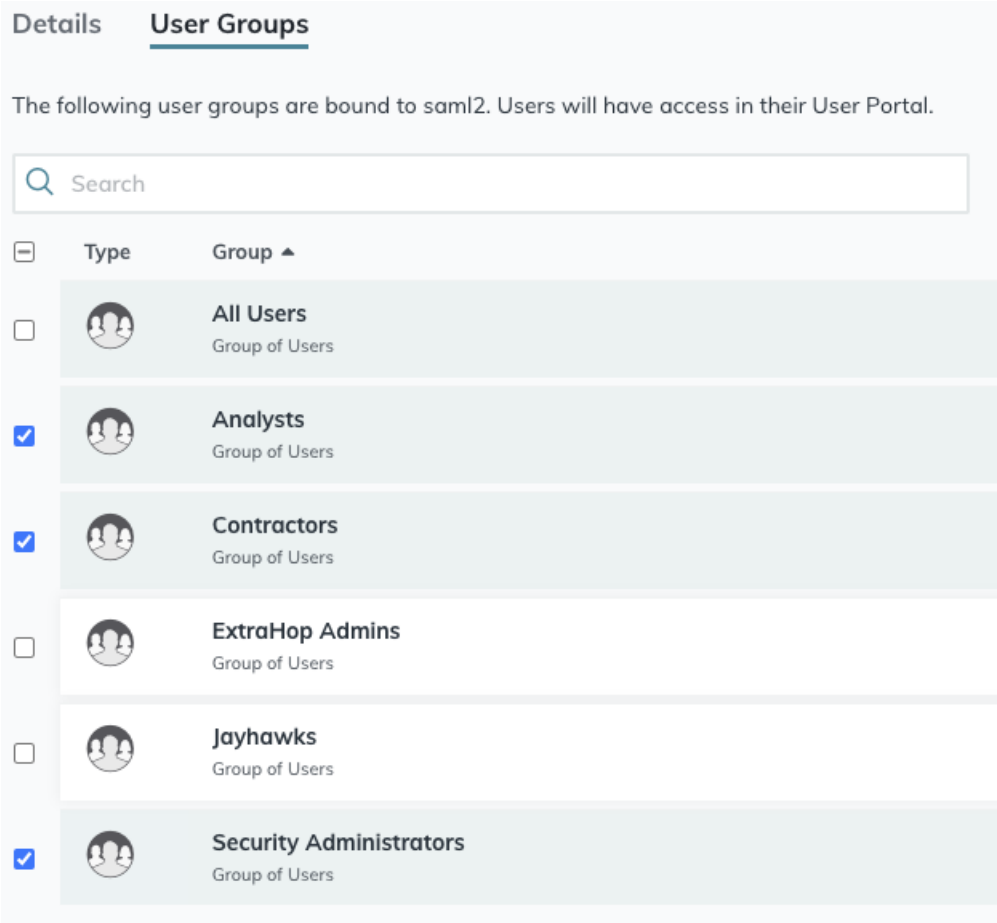
- **Format SAML (nom du sujet et de l'identifiant):** Sélectionnez **urn:oasis:names:tc:saml:2.0:NameID - Format : persistant** depuis le menu déroulant.
- **Algorithme de signature:** Sélectionnez **RSA-SHA256** depuis le menu déroulant.
- **État du relais par défaut:** Laissez ce champ vide.
- **URL de connexion:** Laissez ce champ vide.
- **URL de l'IdP:** Tapez un nom d'identification dans le champ. L'URL ressemble à l'exemple suivant : `https://sso.jumpcloud.com/saml2/extrahop`.

7. Dans le Mappage des attributs utilisateur section, cliquez sur **ajouter un attribut** et saisissez les chaînes suivantes. Ces attributs identifient l'utilisateur dans l'ensemble du système ExtraHop.

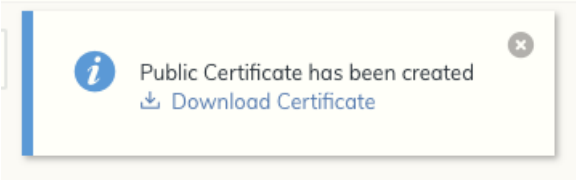
Nom de l'attribut du fournisseur de services	Nom de l'attribut JumpCloud
urn:oid : 0.9.2342.19200300.100.1.3	courriel
urn:oid : 2.5.4.4	nom de famille
urn:oid : 2.5.4.42	prénom

8. Dans le Attributs du groupe section, sélectionnez **inclure l'attribut de groupe** et saisissez un nom dans le champ pour identifier le groupe. Vous spécifierez ce nom lorsque vous configurerez les attributs de privilèges utilisateur sur le système ExtraHop.

9. Cliquez sur **Groupes d'utilisateurs** onglet.
10. Sélectionnez tous les groupes qui doivent avoir accès au système ExtraHop. Trois groupes sont sélectionnés dans l'exemple ci-dessous.



11. Cliquez **activer**.
12. Cliquez **Continuer** pour confirmer les nouveaux paramètres.
JumpCloud génère un certificat après la création de l'application. Cliquez **Télécharger le certificat** et enregistrez le fichier sur votre ordinateur.



Ajouter des informations sur le fournisseur d'identité sur le système ExtraHop

1. Revenez aux paramètres d'administration du système ExtraHop. Fermez la fenêtre de métadonnées du fournisseur de services si elle est toujours ouverte, puis cliquez sur **Ajouter un fournisseur d'identité**.
2. Tapez un nom unique dans le Nom du fournisseur champ. Ce nom apparaît sur la page de connexion du système ExtraHop.
3. Depuis JumpCloud, copiez le ID d'entité IdP et collez-le dans ID d'entité champ sur le système ExtraHop.
4. Depuis JumpCloud, copiez le URL IDP et collez-le dans URL SSO champ sur le système ExtraHop.
5. Ouvrez le `certificate.pem` dans un éditeur de texte, copiez les données du certificat et collez-les dans Certificat public champ sur le système ExtraHop.

6. Choisissez la manière dont vous souhaitez approvisionner les utilisateurs parmi l'une des options suivantes.
   - Sélectionnez Auto-provisionnement des utilisateurs pour créer un nouveau compte utilisateur SAML distant sur le système ExtraHop lorsque l'utilisateur se connecte pour la première fois au système.
   - Décochez la case Provisionnement automatique des utilisateurs et configurez manuellement les nouveaux utilisateurs distants via les paramètres d'administration ExtraHop ou l'API REST.
7. Le **Activer ce fournisseur d'identité** L'option est sélectionnée par défaut et permet aux utilisateurs de se connecter au système ExtraHop. Pour empêcher les utilisateurs de se connecter, décochez la case.
8. Configurez les attributs de privilèges utilisateur. Vous devez configurer l'ensemble d'attributs utilisateur suivant pour que les utilisateurs puissent se connecter au système ExtraHop via un fournisseur d' identité. Les valeurs peuvent être définies par l'utilisateur ; elles doivent toutefois correspondre aux noms d'attributs inclus dans la réponse SAML de votre fournisseur d'identité. Les valeurs ne font pas la distinction entre majuscules et minuscules et peuvent inclure des espaces. Pour plus d' informations sur les niveaux de privilèges, consultez Utilisateurs et groupes d'utilisateurs..

   Important: Vous devez spécifier le nom de l'attribut et configurer au moins une valeur d'attribut autre que **Pas d'accès** pour permettre aux utilisateurs de se connecter.

   Dans les exemples ci-dessous, Nom de l'attribut Le champ est l'attribut de groupe configuré lors de la création de l'application ExtraHop sur le fournisseur d' identité et les autres valeurs d'attribut sont les noms de vos groupes d'utilisateurs . Si un utilisateur est membre de plusieurs groupes, il bénéficie du privilège d'accès le plus permissif.

Nom du champ	Exemple de valeur d'attribut
Nom de l'attribut	`Adhésions à des groupes`
Administration des systèmes et des accès	`Administrateurs système`
Privilèges d'écriture complets	`Analystes principaux`
Privilèges d'écriture limités	`Analystes`
Privilèges d'écriture personnels	`Analystes juniors`
Privilèges complets en lecture seule	`Gestionnaires Web`
Privilèges de lecture seule restreints	`Entrepreneurs`
Pas d'accès	`Stagiaires`

9. Configurez l'accès au module NDR.

Nom du champ	Exemple de valeur d'attribut
Nom de l'attribut	`Adhésions à des groupes`
Accès complet	`Opérations de sécurité`
Pas d'accès	`Stagiaires`

10. Configurez l'accès au module NPM.

Nom du champ	Exemple de valeur d'attribut
Nom de l'attribut	`Adhésions à des groupes`
Accès complet	`Opérations de performance`
Pas d'accès	`Stagiaires`

11. Optionnel : Configurez l'accès aux paquets et aux clés de session. Cette étape est facultative et n'est requise que si vous disposez d'un stockage des paquets connecté et du module Packet Forensics.

Nom du champ	Exemple de valeur d'attribut
Nom de l'attribut	`Adhésions à des groupes`
Paquets et clés de session	`Administrateurs système`
Paquets uniquement	`Analystes principaux`
Tranches en sachets uniquement	`Analystes`
En-têtes de paquets uniquement	`Analystes juniors`
Pas d'accès	`Stagiaires`

12. Cliquez **Enregistrer**.
13. Enregistrez la configuration en cours.

Connectez-vous au système ExtraHop

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Cliquez **Connectez-vous avec** *<provider name>*.
3. Connectez-vous à votre fournisseur à l'aide de votre adresse e-mail et de votre mot de passe. Vous êtes automatiquement dirigé vers la page d'aperçu d'ExtraHop.