

Configurer l'authentification unique SAML avec Okta

Publié: 2023-09-19

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

Avant de commencer

- Vous devez être familiarisé avec l'administration d'Okta. Ces procédures sont basées sur l'interface utilisateur Okta Classic. Si vous configurez Okta via la Developer Console, la procédure peut être légèrement différente.
- Vous devez être familiarisé avec l'administration des systèmes ExtraHop.

Ces procédures nécessitent de copier et coller des informations entre le système ExtraHop et l'interface utilisateur Okta Classic, il est donc utile d'avoir les deux systèmes ouverts côte à côte.

Activer 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. Dans la liste déroulante Méthode d'authentification à distance, sélectionnez **SAML**.
4. Cliquez sur **Continuer**.
5. Cliquez sur **View SP Metadata (Afficher les métadonnées SP)**. Vous devrez copier l'URL ACS et l'ID d'entité pour les coller dans la configuration Okta dans la procédure suivante.

Configurer les paramètres SAML dans Okta


Cette procédure nécessite de copier et de coller des informations entre les paramètres d'administration d'ExtraHop et l'interface Okta Classic, il est donc utile d'avoir les deux interfaces ouvertes côte à côte.

1. Connectez-vous à Okta.
2. Dans le coin supérieur droit de la page, passez de la **console de développement** à l'**interface utilisateur classique**.



3. Dans le menu supérieur, cliquez sur **Applications**.
4. Cliquez sur **Ajouter une application**.
5. Cliquez sur **Créer une nouvelle application**.
6. Dans la liste déroulante Platform, sélectionnez **Web**.
7. Pour la méthode de connexion, sélectionnez **SAML 2.0**.
8. Cliquez sur **Créer**.
9. Dans la section General Settings (Paramètres généraux), saisissez un nom unique dans le champ App name (Nom de l'application) pour identifier le système ExtraHop.
10. Optionnel : Configurez les champs Logo de l'application et Visibilité de l'application en fonction de votre environnement.

11. Cliquez sur **Suivant**.
12. Dans les sections Paramètres SAML, collez l'URL du service consommateur d'assertions (ACS) du système ExtraHop dans le champ URL d'authentification unique d'Okta.

 **Note:** Vous devrez peut-être modifier manuellement l'URL ACS si elle contient un nom d'hôte inaccessible, tel que le nom d'hôte par défaut du système `extrahop`. Nous vous recommandons de spécifier le nom de domaine complet du système ExtraHop dans l'URL.
13. Collez l'ID de l'entité SP du système ExtraHop dans le champ Audience URI (ID de l'entité SP) dans Okta.
14. Dans la liste déroulante Name ID format, sélectionnez **Persistent**.
15. Dans la liste déroulante Nom d'utilisateur de l'application, sélectionnez un format de nom d'utilisateur.
16. Dans la section Attribute Statements, ajoutez les attributs suivants. Ces attributs permettent d'identifier l'utilisateur dans le système ExtraHop.

| Nom | Format du nom | Valeur |
|--|---------------|-----------------------------|
| <code>urn:oid:0.9.2342.19200300</code> | Référence URI | <code>user.email</code> |
| <code>urn:oid:2.5.4.4</code> | Référence URI | <code>user.lastName</code> |
| <code>urn:oid:2.5.4.42</code> | Référence URI | <code>user.firstName</code> |

17. Dans la section Déclaration d'attribut de groupe, saisissez une chaîne dans le champ Nom et configurez un filtre. Vous spécifierez le nom de l'attribut de groupe lorsque vous configurerez les attributs de privilège de l'utilisateur sur le système ExtraHop.
La figure suivante présente un exemple de configuration.

A SAML Settings

GENERAL

Single sign on URL ? ⓘ

Use this for Recipient URL and Destination URL

Allow this app to request other SSO URLs

Audience URI (SP Entity ID) ?

Default RelayState ?

If no value is set, a blank RelayState is sent

Name ID format ?

Application username ?

Update application username on

[Show Advanced Settings](#)

ATTRIBUTE STATEMENTS (OPTIONAL) [LEARN MORE](#)

| Name | Name format (optional) | Value |
|---|--|---|
| <input type="text" value="urn:oid:0.9.2342.1920030"/> | <input type="text" value="URI Reference"/> | <input type="text" value="user.email"/> |
| <input type="text" value="urn:oid:2.5.4.4"/> | <input type="text" value="URI Reference"/> | <input type="text" value="user.lastName"/> ✕ |
| <input type="text" value="urn:oid:2.5.4.42"/> | <input type="text" value="URI Reference"/> | <input type="text" value="user.firstName"/> ✕ |

GROUP ATTRIBUTE STATEMENTS (OPTIONAL)

| Name | Name format (optional) | Filter |
|---|--|--|
| <input type="text" value="groupMemberships"/> | <input type="text" value="Unspecified"/> | <input type="text" value="Matches regex"/> <input type="text" value=".*"/> |

18. Cliquez sur **Next (Suivant)**, puis sur **Finish (Terminer)**.
La page Sign On settings (Paramètres de connexion) s'affiche à nouveau.
19. Dans la section Paramètres, cliquez sur **Afficher les instructions de configuration**.
Une nouvelle fenêtre de navigateur s'ouvre et affiche les informations requises pour configurer le système ExtraHop.

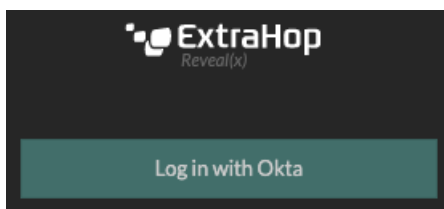
Affecter le système ExtraHop aux groupes Okta

Nous supposons que vous avez déjà configuré des utilisateurs et des groupes dans Okta. Si ce n'est pas le cas, reportez-vous à la documentation d'Okta pour ajouter de nouveaux utilisateurs et groupes.

1. Dans le menu Annuaire, sélectionnez **Groupes**.
2. Cliquez sur le nom du groupe.
3. Cliquez sur **Manage Apps (Gérer les applications)**.
4. Localisez le nom de l'application que vous avez configurée pour le système ExtraHop et cliquez sur **Attribuer**.
5. Cliquez sur **Terminé**.

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

1. Retournez dans les paramètres d'administration du système ExtraHop. Fermez la fenêtre des métadonnées du fournisseur de services si elle est encore ouverte, puis cliquez sur **Ajouter un fournisseur d'identité**.
2. Saisissez un nom unique dans le champ Nom du fournisseur. Ce nom apparaît sur la page de connexion du système ExtraHop.



3. Depuis Okta, copiez l'URL d'authentification unique du fournisseur d'identité et collez-la dans le champ URL d'authentification unique du système ExtraHop.
4. Dans Okta, copiez l'URL de l'émetteur du fournisseur d'identité et collez-la dans le champ ID de l'entité du système ExtraHop.
5. Depuis Okta, copiez le certificat X.509 et collez-le dans le champ Certificat public du système ExtraHop.
6. Choisissez l'une des options suivantes pour provisionner les utilisateurs.
 - Sélectionnez Auto-provision users pour créer un nouveau compte utilisateur SAML distant sur le système ExtraHop lorsque l'utilisateur se connecte pour la première fois.
 - Décochez la case Approvisionnement automatique des utilisateurs et configurez manuellement de nouveaux utilisateurs distants via les paramètres d'administration d'ExtraHop ou l'API REST. Les niveaux d'accès et de privilège sont déterminés par la configuration de l'utilisateur dans Okta.
7. L'option **Activer ce fournisseur d'identité** 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 des privilèges des utilisateurs. Vous devez configurer l'ensemble des attributs utilisateur suivants avant que les utilisateurs puissent se connecter au système ExtraHop par l'intermédiaire d'un fournisseur d'identité. Les valeurs sont définies par l'utilisateur, mais elles doivent correspondre aux noms d'attributs inclus dans la réponse SAML de votre fournisseur d'identité. Les valeurs ne sont pas sensibles à la casse et peuvent inclure des espaces. Pour plus d'informations sur les niveaux de privilèges, voir [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, le champ Nom de l'attribut est l'attribut de groupe configuré lors de la création de l'application ExtraHop sur le fournisseur d'identité et les Valeurs de l'attribut sont les noms de vos groupes d'utilisateurs. Si un utilisateur est membre de plusieurs groupes, il se voit accorder le privilège d'accès le plus permissif.

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"/> |

- Optionnel : Configurez l'accès aux paquets et aux clés de session. La configuration des attributs des paquets et des clés de session est facultative et n'est requise que lorsque vous disposez d'un packetstore connecté. Les utilisateurs disposant de privilèges illimités se voient automatiquement accorder l'accès aux paquets et aux clés de session.

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"/> |

- Optionnel : Configurer l'accès aux détections. La configuration des attributs de détection est facultative et n'est requise que lorsque la [stratégie de privilèges globale](#) est définie sur **Seuls les utilisateurs spécifiés peuvent voir les détections**. Les utilisateurs disposant de privilèges illimités ont automatiquement accès aux détections.

Detections Access

Specify an attribute value to grant detection privileges to SAML users. See [global privilege policy settings](#).

Attribute Name

Attribute Values

| | |
|----------------|--|
| All detections | <input type="text" value="Security Administrators"/> |
| No access | <input type="text"/> |

11. Cliquez sur **Enregistrer**.
12. [Enregistrez la configuration en cours d'exécution](#).

Connectez-vous au système ExtraHop

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Cliquez sur **Se connecter avec** *<nom du fournisseur>*.
3. Connectez-vous à votre fournisseur à l'aide de votre adresse électronique et de votre mot de passe. Vous êtes automatiquement dirigé vers la page de présentation d'ExtraHop.