Configurer l'authentification unique SAML avec Okta

Publié: 2023-10-01

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 vous obligent à copier-coller des informations entre le système ExtraHop et l'interface utilisateur Okta Classic. 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. Dans la liste déroulante des méthodes d'authentification à distance, sélectionnez **SAML**.
4. Cliquez **Poursuivre**.
5. Cliquez **Afficher les métadonnées SP**. Vous devrez copier l' URL ACS et l'ID d'entité pour les coller dans la configuration Okta lors de la procédure suivante.

Configurer les paramètres SAML dans Okta

Cette procédure vous oblige à copier-coller des informations entre les paramètres d'administration d'ExtraHop et l'interface utilisateur Okta Classic. Il est donc utile que chaque interface utilisateur soit ouverte côte à côte.

1. Connectez-vous à Okta.
2. Dans le coin supérieur droit de la page, modifiez l'affichage de **Console pour développeurs** pour **Interface utilisateur classique**.

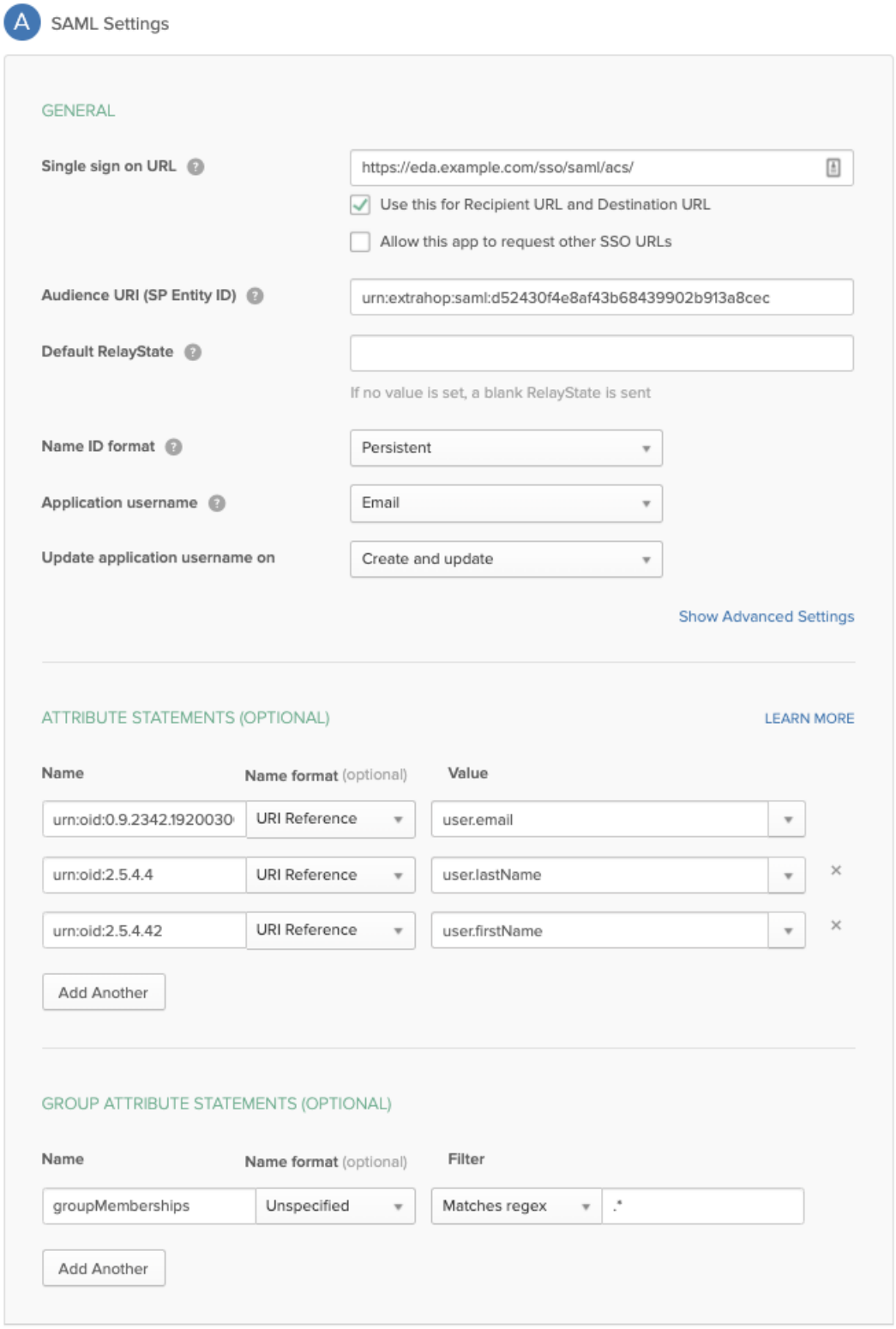
3. Dans le menu supérieur, cliquez sur **Demandes**.
4. Cliquez **Ajouter une application**.
5. Cliquez **Créer une nouvelle application**.
6. À partir du Plateforme liste déroulante, sélectionnez **Web**.
7. Pour le Méthode de connexion, sélectionnez **SAML 2.0** .
8. Cliquez **Créez**.
9. Dans le Réglages généraux section, saisissez un nom unique dans le Appli champ de nom pour identifier le système ExtraHop.

10. Optionnel : Configurez le Logo de l'application et Visibilité de l'application les champs requis pour votre environnement.
11. Cliquez **Suivant**.
12. Dans le Paramètres SAML sections, collez l'URL d'Assertion Consumer Service (ACS) du système ExtraHop dans le champ URL d'authentification unique d'Okta.

    Note: Vous devrez peut-être modifier manuellement l'URL ACS si l'URL contient un nom d'hôte inaccessible, tel que le nom d'hôte du système par défaut `extrahop`. Nous vous recommandons de spécifier le nom de domaine complet pour le système ExtraHop dans l'URL.
13. Collez l'ID d'entité SP du système ExtraHop dans le URI d'audience (ID d'entité SP) champ dans Okta.
14. À partir du Format du nom et de l'identifiant liste déroulante, sélectionnez **Persistant**.
15. À partir du Nom utilisateur de l'application liste déroulante, sélectionnez un format de nom d'utilisateur.
16. Dans le Déclarations d'attributs section, ajoutez les attributs suivants. Ces attributs identifient l'utilisateur dans l'ensemble du système ExtraHop.

Nom	Format du nom	Valeur
`urn:oid:0.9.2342.19200300.100.1.3`	Référence d'URI	utilisateur.email
`urn:oid:2.5.4.4`	Référence d'URI	Nom de famille de l'utilisateur
`urn:oid:2.5.4.42`	Référence d'URI	Nom de l'utilisateur

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



18. Cliquez **Suivant** puis cliquez sur **Finir**.
    Vous revenez à la page des paramètres de connexion.
19. Dans la section Paramètres, cliquez sur **Afficher les instructions de configuration**.
    Une nouvelle fenêtre de navigateur s'ouvre et affiche les informations nécessaires à la configuration du système ExtraHop.

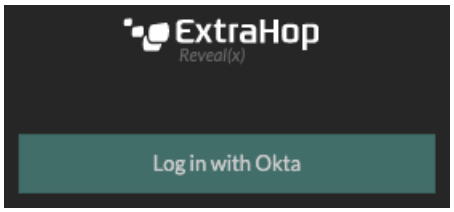
Assignez le système ExtraHop à des groupes Okta

Nous partons du principe que vous avez déjà configuré des utilisateurs et des groupes dans Okta. Si ce n'est pas le cas, consultez la documentation Okta pour ajouter de nouveaux utilisateurs et groupes.

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

Ajouter les informations du fournisseur d'identité sur le système ExtraHop

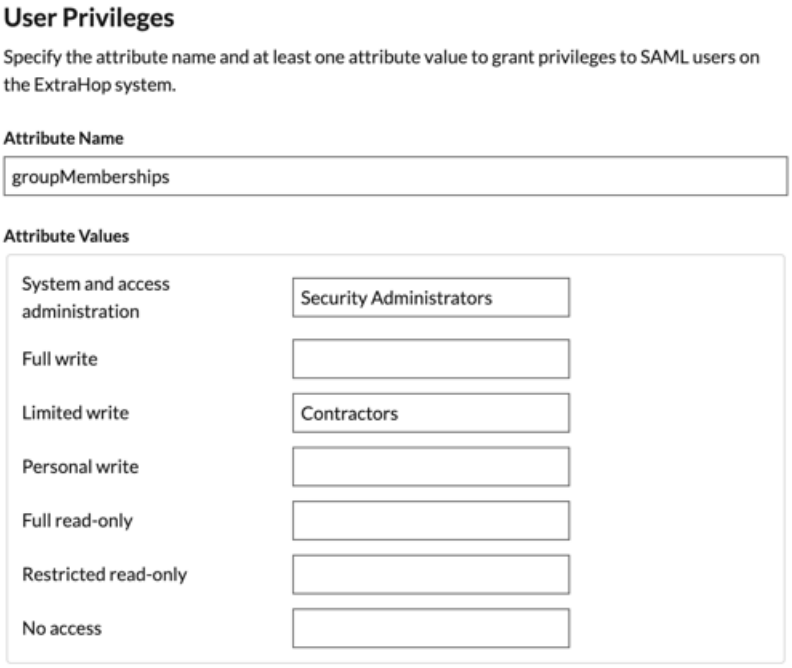
1. Retournez aux paramètres d'administration du système ExtraHop. Fermez la fenêtre de métadonnées du fournisseur de services si elle est toujours ouverte, puis cliquez sur **Ajouter un fournisseur d'identité**.
2. Entrez un nom unique dans le champ Nom du fournisseur. Ce nom apparaît sur la page de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



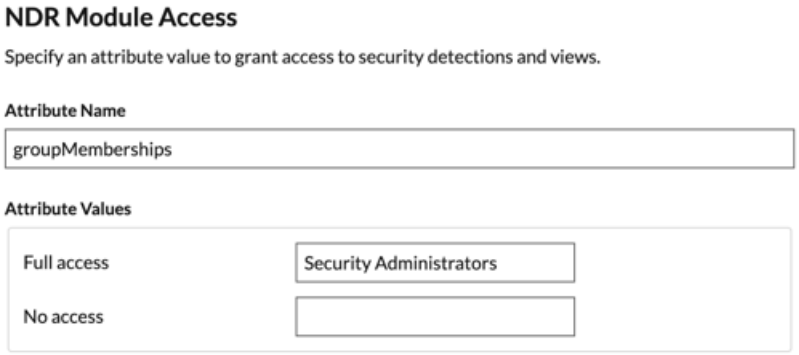
3. Depuis Okta, copiez le URL d'authentification unique du fournisseur d'identité et collez-le dans le champ URL SSO du système ExtraHop.
4. Depuis Okta, copiez le URL de l'émetteur du fournisseur d'identité et collez-le dans ID de l'entité champ sur le système ExtraHop.
5. Depuis Okta, copiez le certificat X.509 et collez-le dans Certificat public champ sur le système ExtraHop.
6. Choisissez la manière dont vous souhaitez approvisionner les utilisateurs à partir de l'une des options suivantes.
   - Sélectionnez Provisionner automatiquement les utilisateurs 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 les nouveaux utilisateurs distants via les paramètres d'administration ExtraHop ou l'API REST. Les niveaux d'accès et de privilège sont déterminés par la configuration utilisateur dans Okta.
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 avant 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 distinguent pas les majuscules et minuscules 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.

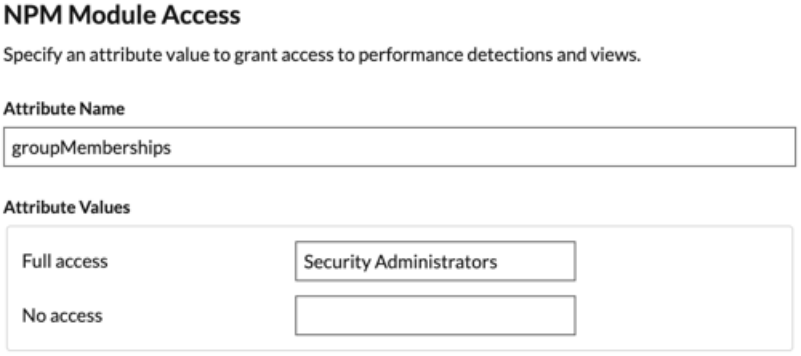
Dans les exemples ci-dessous, le Nom de l'attribut le champ est l'attribut de groupe configuré lors de la création de l'application ExtraHop sur le fournisseur d'identité et le Valeurs d'attribut sont les noms de vos groupes d'utilisateurs. Si un utilisateur est membre de plusieurs groupes, il bénéficie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



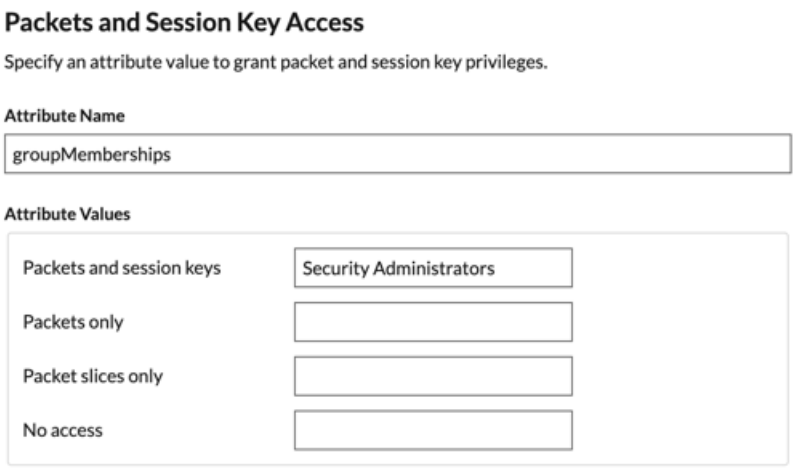
9. Configurez l'accès au module NDR.



10. Configurez l'accès au module NPM.



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



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.