Configurer l'authentification unique SAML avec Azure AD

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 Azure AD.

Avant de commencer

- Vous devez être familiarisé avec l'administration d'Azure AD.
- Vous devez être familiarisé avec l'administration des systèmes ExtraHop.

Ces procédures nécessitent de copier et de coller des informations entre le système ExtraHop et Azure, 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 de l'Assertion Consumer Service (ACS) et l'ID de l'entité pour les coller dans la configuration Azure lors d'une procédure ultérieure.

Configurer Azure

Dans les procédures suivantes, vous allez créer une application d'entreprise, ajouter des utilisateurs et des groupes à l'application et configurer les paramètres d'authentification unique.

Créer une nouvelle application

1. Connectez-vous à votre portail Microsoft Azure.
2. Dans la section Services Azure, cliquez sur **Applications d'entreprise**.
3. Cliquez sur **Nouvelle application**.
4. Cliquez sur **Créer votre propre application**.
5. Saisissez un nom pour le capteur dans le champ Nom. Ce nom apparaît pour vos utilisateurs sur la page Azure My Apps.
6. Sélectionnez **Intégrer toute autre application que vous ne trouvez pas dans la galerie**.
7. Cliquez sur **Créer**.

La page Présentation de l'application s'affiche.

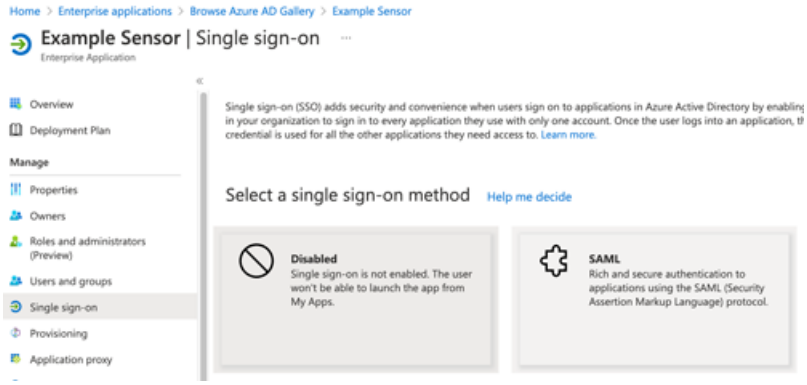
Ajouter des utilisateurs et des groupes

Vous devez affecter des utilisateurs ou des groupes à la nouvelle application avant que les utilisateurs puissent se connecter au système ExtraHop.

1. Dans le volet de gauche, cliquez sur **Utilisateurs et groupes**.
2. Cliquez sur **Ajouter un utilisateur/groupe**.
3. Ajoutez vos utilisateurs ou groupes privilégiés, puis cliquez sur **Attribuer**.

Configurer l'authentification unique

1. Dans le volet de gauche, cliquez sur **Connexion unique**.
2. Cliquez sur **SAML**.



3. Dans la section Basic SAML Configuration, cliquez sur **Edit**.
4. Saisissez ou collez l'ID d'entité du système ExtraHop dans le champ Identifiant (ID d'entité) et cochez la case **Par défaut**. Vous pouvez supprimer l'`entrée`http://adapplicationregistry.onmicrosoft.com/customappsso/primary existante.
5. Saisissez ou collez l'URL ACS du système ExtraHop dans le champ**Reply URL (Assertion Consumer Service URL)**.
6. Cliquez sur **Enregistrer**.
7. Dans la section Attributs et réclamations, cliquez sur **Modifier**.
8. Dans la section réclamation requise, cliquez sur **Identifiant unique de l'utilisateur (Name ID)**.
9. Cliquez sur **Choose name identifier format (Choisir le format de l'identifiant de nom**).
10. Dans la liste déroulante, sélectionnez **Persistant**.
11. Cliquez sur **Enregistrer**.
12. Dans la section des réclamations supplémentaires, supprimez la réclamation **user.mail** de la liste et remplacez les noms de réclamations par défaut par les noms de réclamations suivants :

Nom de la déclaration	Valeur
`urn:oid:2.5.4.4`	user.surname
`urn:oid:2.5.4.42`	utilisateur.prénom
`urn:oid:0.9.2342.19200300.100.1.3`	user.userprincipalname

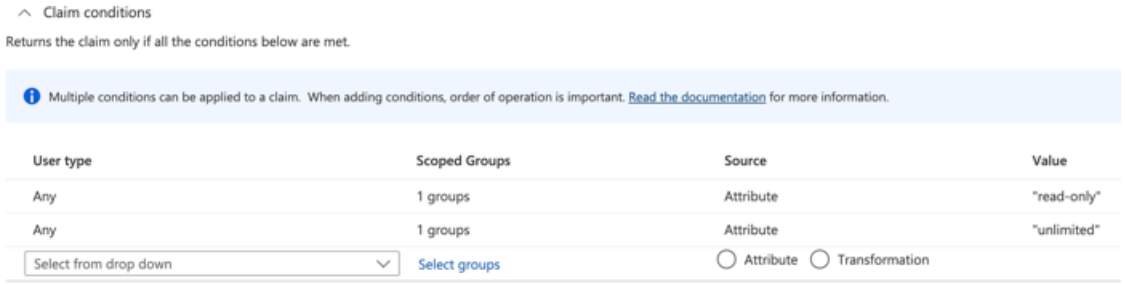
13. Cliquez sur **Ajouter une nouvelle demande**. Cette demande permet aux utilisateurs d'accéder au système ExtraHop avec les privilèges attribués.
    a) Tapez `writelevel` dans le champ Name (Nom). Vous pouvez saisir le nom de votre choix, mais il doit correspondre au nom que vous configurerez sur le système ExtraHop.
    b) Cliquez sur **Claim conditions (Conditions de réclamation**).

    Important: L'ordre dans lequel vous ajoutez les conditions est important. Si un utilisateur répond à plusieurs conditions de réclamation, il se voit attribuer les privilèges qui correspondent à la dernière condition. Par exemple, si vous ajoutez `illimité` comme première valeur et `lecture seule` comme deuxième valeur et que l'utilisateur répond aux deux conditions de réclamation, l'utilisateur se voit attribuer le privilège de lecture seule.

    c) Dans la liste déroulante **Type d'utilisateur**, sélectionnez **Tous**.
    d) Sous **Groupes délimités**, cliquez sur **Sélectionner des groupes**, cliquez sur le nom du groupe que vous souhaitez ajouter, puis cliquez sur **Sélectionner**.

e) Sous **Source**, sélectionnez **Attribut**.

f) Dans le champ **Valeur**, saisissez `illimitéou` un nom de votre choix qui définit le privilège de ce groupe. Répétez cette étape pour chaque groupe auquel vous souhaitez attribuer des privilèges uniques. Dans l'exemple ci-dessous, nous avons créé une condition de demande pour deux groupes. Un groupe se voit attribuer des privilèges de lecture seule et l'autre groupe se voit attribuer des privilèges d'administration du système et des accès.



g) Cliquez sur **Enregistrer**.

14. Retournez à la page Attributs et revendications et cliquez sur **Ajouter une nouvelle revendication**. Cette revendication attribue l'accès aux paquets et aux clés de session.
    a) Tapez `packetslevel` dans le champ Name (Nom). Vous pouvez saisir le nom de votre choix, mais il doit correspondre à celui que vous configurerez sur le système ExtraHop.
    b) Cliquez sur **Claim conditions (Conditions de réclamation**).
    c) Dans la liste déroulante **User type (Type d'utilisateur**), sélectionnez **Any (Tous)**.
    d) Sous Scoped Groups (Groupes délimités), cliquez sur **Select groups (Sélectionner des groupes**), cliquez sur le nom du groupe que vous souhaitez ajouter, puis sur **Select (Sélectionner)**.
    e) Sous Source, sélectionnez **Attribut**.
    f) Dans le champ Valeur, saisissez `justpackets` ou un nom de votre choix qui définit le privilège de ce groupe.
    g) Cliquez sur **Enregistrer**.
15. Revenez à la page Attributs et revendications et cliquez sur **Ajouter une nouvelle revendication**. Cette revendication attribue l'accès aux détections.
    a) Tapez `detectionslevel` dans le champ Name (Nom). Vous pouvez saisir le nom de votre choix, mais il doit correspondre à celui que vous configurerez sur le système ExtraHop.
    b) Cliquez sur **Claim conditions (Conditions de réclamation**).
    c) Dans la liste déroulante **Type d'utilisateur**, sélectionnez **N'importe lequel**.
    d) Sous Scoped Groups (Groupes délimités), cliquez sur **Select groups (Sélectionner des groupes**), cliquez sur le nom du groupe que vous souhaitez ajouter, puis sur **Select (Sélectionner)**.
    e) Sous Source, sélectionnez **Attribut**.
    f) Dans le champ Valeur, saisissez `full` ou un nom de votre choix qui définit le privilège de ce groupe.
    g) Cliquez sur **Enregistrer**.

Ajouter les informations relatives au fournisseur d'identité au système ExtraHop

1. Dans la section Certificat de signature SAML Azure, à côté de Certificat (Base64), cliquez sur Télécharger.

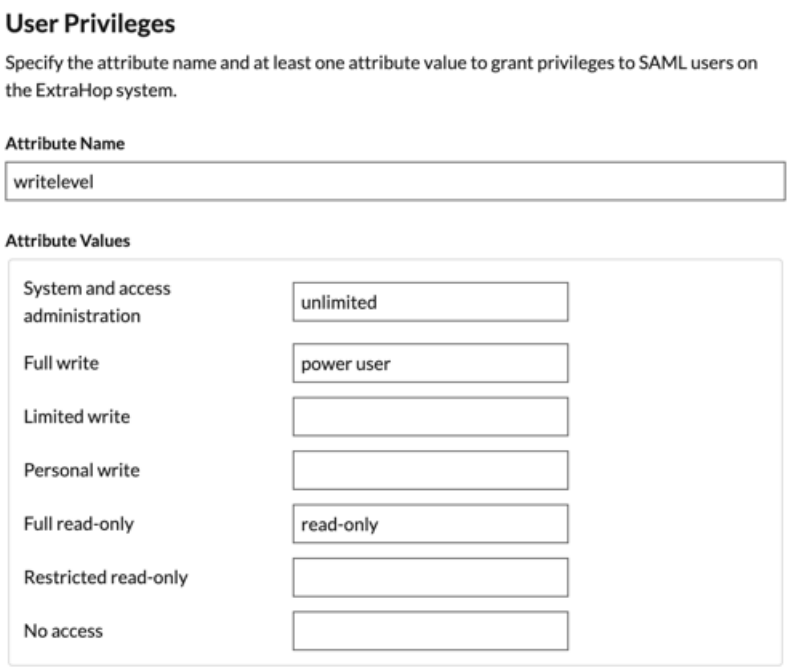
   Note: Pour les systèmes Reveal(x) 360, téléchargez le fichier XML de métadonnées de fédération.
2. Ouvrez le fichier téléchargé dans un éditeur de texte, puis copiez et collez le contenu du fichier dans le champ Certificat public du système ExtraHop.
3. Dans Azure, copiez l'URL de connexion et collez-la dans le champ URL SSO du système ExtraHop.

4. Dans Azure, copiez l'identifiant Azure AD et collez-le dans le champ Entity ID du système ExtraHop.
5. Sur le système ExtraHop, 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 au système.
   - Décochez la case Approvisionnement automatique des utilisateurs pour configurer manuellement de nouveaux utilisateurs distants via les paramètres d'administration d'ExtraHop ou l'API REST.

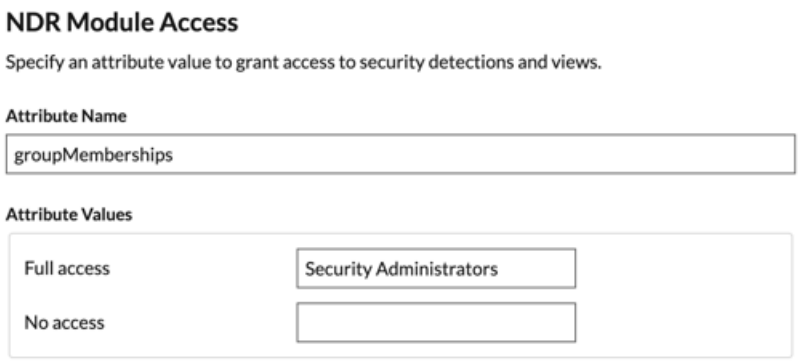
   L'option **Activer ce fournisseur d'identité** est sélectionnée par défaut et permet aux utilisateurs de se connecter au système ExtraHop. Pour empêcher les utilisateurs de se connecter, décochez la case. Ce paramètre n'apparaît pas sur Reveal(x) 360.
6. Configurez les attributs des privilèges des utilisateurs. 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. Ces valeurs peuvent être définies par l'utilisateur ; toutefois, 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 que les utilisateurs puissent se connecter.

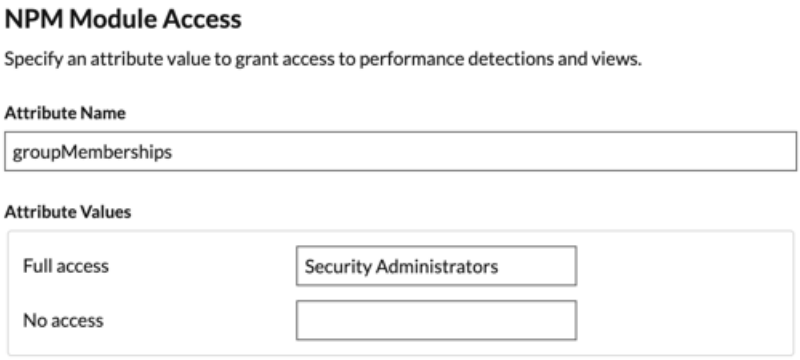
   Dans l'exemple ci-dessous, le champ Nom de l'attribut est le nom de la demande spécifié lors de la création de l'application ExtraHop dans Azure et les Valeurs de l'attribut sont les valeurs de la condition de la demande.



7. Configurer l'accès au module NDR.

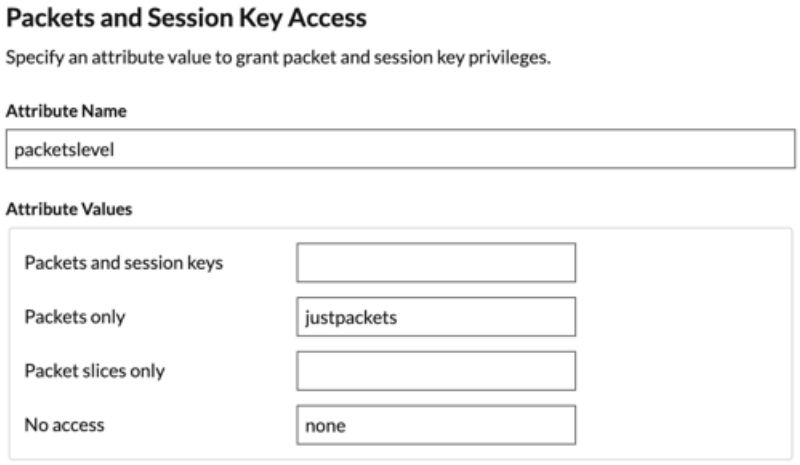


8. Configurer l'accès au module NPM.



9. 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 packetstore connecté.

   Note: Si vous n'avez pas de packetstore, tapez NA dans le champ Nom de l'attribut et laissez les champs Valeurs de l'attribut vides.



10. Cliquez sur **Save (Enregistrer)**.
11. 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 avec votre adresse e-mail et votre mot de passe. Si l'authentification multifactorielle (MFA) est configurée, suivez les instructions pour configurer votre application MFA.