

Configurer l'authentification unique SAML avec Microsoft Entra ID

Publié: 2024-07-03

Vous pouvez configurer votre système ExtraHop pour permettre aux utilisateurs de s'y connecter via le service de gestion des identités Microsoft Entra ID.

Avant de commencer

- Vous devez être familiarisé avec l'administration de Microsoft Entra ID.
- Vous devez être familiarisé avec l'administration des systèmes ExtraHop.

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

Configuration d'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.

Création d'une nouvelle application

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

La page de présentation de l'application s'affiche.

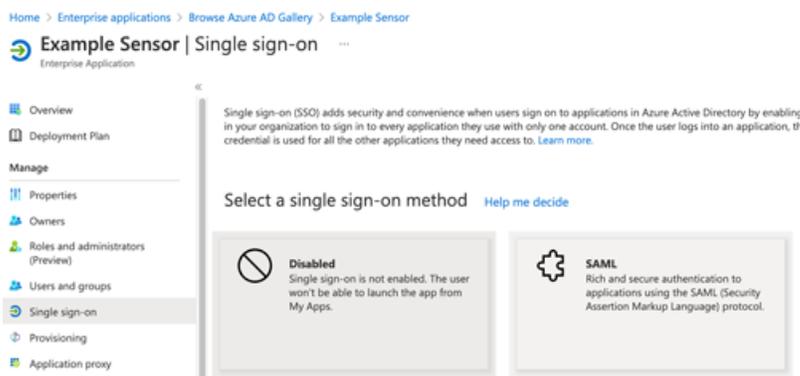
Ajouter des utilisateurs et des groupes

Vous devez attribuer 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 **Ajouter un utilisateur/un groupe**.
3. Ajoutez vos utilisateurs ou groupes privilégiés, puis cliquez sur **Attribuer**.

Configuration de l'authentification unique

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



3. Dans la section Configuration SAML de base, cliquez sur **Modifier**.
4. Tapez ou collez l'ID d'entité du système ExtraHop dans le champ Identifiant (ID d'entité) et sélectionnez **Par défaut** case à cocher. Vous pouvez supprimer l'existant `http://adapplicationregistry.onmicrosoft.com/customappsso/primary` entrée.
5. Tapez ou collez l'URL ACS du système ExtraHop dans **URL de réponse (URL du service client Assertion)** champ.
6. Cliquez **Enregistrer**.
7. Dans la section Attributs et revendications, cliquez sur **Modifier**.
8. Dans la section de réclamation requise, cliquez sur **Identifiant utilisateur unique (ID de nom)**.
9. Cliquez **Choisissez le format de l'identifiant de nom**.
10. Dans la liste déroulante, sélectionnez **Persistant**.
11. Cliquez **Enregistrer**.
12. Dans la section des réclamations supplémentaires, supprimez **utilisateur.mail** revendiquez depuis la liste et remplacez les noms de réclamation par défaut par les noms de réclamation suivants :

Nom de la réclamation	Valeur
urn:oid:2.5.4.4	nom d'utilisateur
urn:oid:2.5.4.42	utilisateur.givenname
urn:oid:0.9.2342.19200300.100.1.3	user.userprincipalname

13. Cliquez **Ajouter une nouvelle réclamation**. Cette réclamation permet aux utilisateurs d'accéder au système ExtraHop avec les privilèges assignés.
 - a) Type `niveau d'écriture` dans le champ Nom. Vous pouvez taper le nom que vous voulez, mais il doit correspondre au nom que vous allez configurer sur le système ExtraHop.
 - b) Cliquez **Conditions de réclamation**.
 - ⚠ **Important:** L'ordre dans lequel vous ajoutez les conditions est important. Si un utilisateur répond à plusieurs conditions de réclamation, les privilèges correspondants en dernier lui sont attribués. Par exemple, si vous ajoutez `illimité` comme première valeur et `lecture seule` lorsque la deuxième valeur est atteinte et que l'utilisateur répond aux deux conditions de réclamation, le privilège de lecture seule est attribué à l'utilisateur.
 - c) À partir du **Type d'utilisateur** liste déroulante, sélectionnez **N'importe lequel**.
 - d) Sous **Groupes délimités**, cliquez **Sélectionnez des groupes**, cliquez sur le nom du groupe que vous souhaitez ajouter, puis sur **Sélectionnez**.

- e) Sous **La source**, sélectionnez **Attribut**.
- f) Dans le **Valeur** champ, type `illimité` ou un nom de votre choix qui définit les privilèges 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 réclamation pour deux groupes. Un groupe se voit attribuer des privilèges de lecture seule et l'autre des privilèges d'administration du système et des accès.

^ Claim conditions

Returns the claim only if all the conditions below are met.

i Multiple conditions can be applied to a claim. When adding conditions, order of operation is important. [Read the documentation](#) for more information.

User type	Scoped Groups	Source	Value
Any	1 groups	Attribute	"read-only"
Any	1 groups	Attribute	"unlimited"

Select from drop down Attribute Transformation

- g) Cliquez **Enregistrer**.
14. Retournez à la page Attributs et réclamations et cliquez sur **Ajouter une nouvelle réclamation**. Cette réclamation attribue l'accès aux paquets et aux clés de session.
 - a) Type `niveau des paquets` dans le champ Nom. Vous pouvez taper le nom que vous voulez, mais il doit correspondre au nom que vous allez configurer sur le système ExtraHop.
 - b) Cliquez **Conditions de réclamation**.
 - c) À partir du **Type d'utilisateur** liste déroulante, sélectionnez **N'importe lequel**.
 - d) Sous Groupes délimités, cliquez sur **Sélectionnez des groupes**, cliquez sur le nom du groupe que vous souhaitez ajouter, puis sur **Sélectionnez**.
 - e) Sous Source, sélectionnez **Attribut**.
 - f) Dans le champ Valeur, tapez `juste des paquets` ou un nom de votre choix qui définit les privilèges de ce groupe.
 - g) Cliquez **Enregistrer**.
 15. Retournez à la page Attributs et réclamations et cliquez sur **Ajouter une nouvelle réclamation**. Cette réclamation attribue l'accès aux détections.
 - a) Type `niveau de détection` dans le champ Nom. Vous pouvez taper le nom que vous voulez, mais il doit correspondre au nom que vous allez configurer sur le système ExtraHop.
 - b) Cliquez **Conditions de réclamation**.
 - c) À partir du **Type d'utilisateur** liste déroulante, sélectionnez **N'importe lequel**.
 - d) Sous Groupes délimités, cliquez sur **Sélectionnez des groupes**, cliquez sur le nom du groupe que vous souhaitez ajouter, puis sur **Sélectionnez**.
 - e) Sous Source, sélectionnez **Attribut**.
 - f) Dans le champ Valeur, tapez `complet` ou un nom de votre choix qui définit les privilèges de ce groupe.
 - g) Cliquez **Enregistrer**.

Ajouter les informations du fournisseur d'identité au système ExtraHop

1. Dans la section Certificat de signature Azure SAML, à côté de Certificat (Base64), cliquez sur Télécharger.
 -  **Note:** Pour les systèmes RevealX 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 Microsoft Entra ID et collez-le dans le champ Entity ID du système ExtraHop.
5. Sur le système ExtraHop, 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 au système.
 - Décochez la case Provisionnement automatique des utilisateurs pour configurer manuellement les nouveaux utilisateurs distants via les paramètres d'administration d'ExtraHop ou l'API REST.

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. Ce paramètre n'apparaît pas sur RevealX 360 .

6. 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. Ces 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 avant que les utilisateurs puissent se connecter.

Dans l'exemple ci-dessous, le champ Nom de l'attribut est le nom de la revendication spécifié lors de la création de l'application ExtraHop dans Azure et les valeurs des attributs sont les valeurs des conditions de réclamation.

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="unlimited"/>
Full write	<input type="text" value="power user"/>
Limited write	<input type="text"/>
Personal write	<input type="text"/>
Full read-only	<input type="text" value="read-only"/>
Restricted read-only	<input type="text"/>
No access	<input type="text"/>

7. Configurez l'accès au module NDR.

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"/>

8. Configurez l'accès au module NPM.

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"/>

9. 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.



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

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"/>
Packets only	<input type="text" value="justpackets"/>
Packet slices only	<input type="text"/>
No access	<input type="text" value="none"/>

10. Cliquez **Enregistrer**.
11. Enregistrez le [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. Si l'authentification multifactorielle (MFA) est configurée, suivez les instructions pour configurer votre application MFA.