Configurer l'authentification unique SAML avec Microsoft Entra ID

Publié: 2025-02-04

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 le menu déroulant de la méthode d'authentification à distance, sélectionnez **SAML**.
4. Cliquez **Continuer**.
5. Cliquez **Afficher les métadonnées SP**. Vous devrez copier l'URL et l'ID d'entité du Assertion Consumer Service (ACS) 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.

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 le 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.

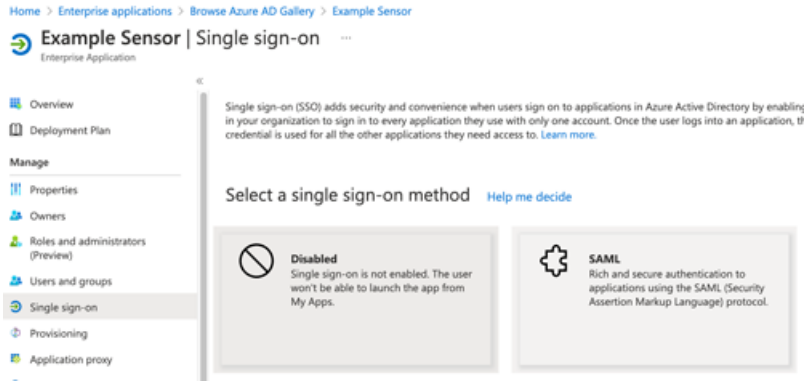
Ajouter des utilisateurs et des groupes

Vous devez affecter des utilisateurs ou des groupes à la nouvelle application pour 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 Identifier (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 le **URL de réponse (URL du service aux consommateurs d'assertion)** champ.
6. Cliquez **Enregistrer**.
7. Dans la section Certificats SAML, cliquez sur **Modifier**.
8. Dans le **Option de signature** menu déroulant, sélectionnez **Signer une réponse et une assertion SAML**
9. Dans la section Attributs et réclamations, cliquez sur **Modifier**.
10. Dans la section de réclamation requise, cliquez sur **Identifiant utilisateur unique (ID de nom)**.
11. Cliquez **Choisissez le format de l'identifiant du nom**.
12. Dans le menu déroulant, sélectionnez **Persistant**.
13. Cliquez **Enregistrer**.
14. Supprimer les éléments requis **utilisateur.mail** réclamation et toutes les réclamations supplémentaires.
15. Ajouter les noms de réclamation suivants :

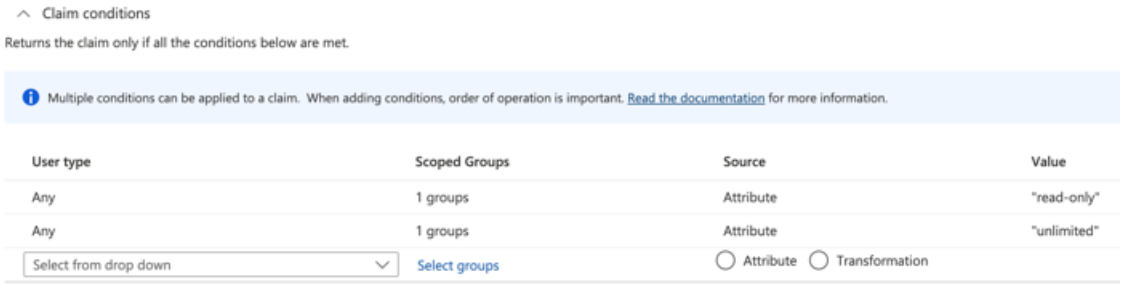
Nom de la réclamation	Valeur
`urn:oid : 2.5.4.4`	utilisateur.nom de famille
`urn:oid : 2.5.4.42`	user.givenname
`urn:oid : 0.9.2342.19200300.100.1.3`	user.userprincipalname

16. Cliquez **Ajouter une nouvelle réclamation**. Cette demande permet aux utilisateurs d'accéder au système ExtraHop avec les privilèges attribués.
    a) Tapez `niveau d'écriture` dans le champ Nom. Vous pouvez saisir le nom de votre choix, 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 correspondant en dernier lui sont attribués. Par exemple, si vous ajoutez `illimité` comme première valeur et `en 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) À partir du **Type d'utilisateur** menu déroulant, sélectionnez **N'importe lequel**.

d) En dessous **Groupes ciblés**, cliquez **Sélectionnez des groupes**, cliquez sur le nom du groupe que vous souhaitez ajouter, puis sur **Sélectionnez**.
e) En dessous **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.



g) Cliquez **Enregistrer**.

17. 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) Tapez `niveau des paquets` dans le champ Nom. Vous pouvez saisir le nom de votre choix, 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** menu déroulant, sélectionnez **N'importe lequel**.
    d) Sous Groupes ciblés, 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**.
18. Retournez à la page Attributs et réclamations et cliquez sur **Ajouter une nouvelle réclamation**. Cette réclamation attribue l'accès aux détections.
    a) Tapez `niveau de détection` dans le champ Nom. Vous pouvez saisir le nom de votre choix, 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** menu déroulant, sélectionnez **N'importe lequel**.
    d) Sous Groupes ciblés, 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 autres valeurs d'attribut sont les valeurs des conditions de réclamation.

Nom du champ	Exemple de valeur d'attribut
Nom de l'attribut	`niveau d'écriture`
Administration des systèmes et des accès	`illimité`
Privilèges d'écriture complets	`écriture_complète`
Privilèges d'écriture limités	`écriture_limitée`
Privilèges d'écriture personnels	`écriture_personnelle`
Privilèges complets en lecture seule	`full_readonly`
Privilèges de lecture seule restreints	`restricted_readonly`
Pas d'accès	`aucune`

7. Configurez l'accès au module NDR.

Nom du champ	Exemple de valeur d'attribut
Nom de l'attribut	`niveau NDR`
Accès complet	`complet`
Pas d'accès	`aucune`

8. Configurez l'accès au module NPM.

Nom du champ	Exemple de valeur d'attribut
Nom de l'attribut	`niveau NPM`

Nom du champ	Exemple de valeur d'attribut
Accès complet	`complet`
Pas d'accès	`aucune`

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.

Nom du champ	Exemple de valeur d'attribut
Nom de l'attribut	`niveau des paquets`
Paquets et clés de session	`complet_avec_touches`
Paquets uniquement	`complet`
Tranches en sachets uniquement	`tranches`
En-têtes de paquets uniquement	`en-têtes`
Pas d'accès	`aucune`

10. Cliquez **Enregistrer**.
11. Enregistrez le 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 **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.