Ajoutez votre propre fournisseur d'identité à Reveal (x) 360

Publié: 2023-11-14

Le système Reveal (x) 360 inclut un fournisseur d'identité (IdP) par défaut qui vous permet de gérer vos utilisateurs qui accèdent au système ExtraHop. Si votre entreprise dispose déjà d'un fournisseur d'identité (IdP) qui prend en charge le langage SAML (Security Assertion Markup Language) 2.0, vous pouvez configurer l'IdP pour gérer vos utilisateurs sur le système ExtraHop.

Pour ajouter votre fournisseur d'identité, vous allez mapper les attributs relatifs à l'identité de l'utilisateur et à l' accès au système entre votre IdP et le système ExtraHop, et vous allez générer un fichier XML de métadonnées contenant le certificat IdP et les informations d'attribut.

Conseil: Les procédures vous obligent à copier-coller des informations entre le système ExtraHop et votre IdP. Il est donc utile que chaque système soit ouvert côte à côte.

Pré-requis

Avant d'ajouter votre fournisseur d'identité (IdP), passez en revue ces considérations.

Fournisseur de système et d'identité

Vérifiez les exigences du système et de l'IdP suivantes :

- Vous devez disposer d'un compte utilisateur ExtraHop avec des privilèges d'administration du système et des accès pour configurer Reveal (x) 360.
- Les fournisseurs d'identité doivent répondre aux critères suivants :
  - ÉCHANTILLON 2.0
  - Prenez en charge les flux de connexion initiés par SP. Les flux de connexion initiés par l'IdP ne sont pas pris en charge.
  - Soutenir les réponses SAML signées
  - Supporte la liaison par redirection HTTP
- Vous devez disposer d'un certificat de fournisseur d'identité valide. Si le certificat expire, l'authentification unique à la console ExtraHop Reveal (x) 360 est désactivée pour tous les utilisateurs de votre organisation et les modifications de configuration du système échoueront.

  Conseil: Le système ExtraHop envoie automatiquement des notifications d'expiration des certificats IdP à tous les utilisateurs ayant Privilèges d' administration du système et des accès. Les e-mails sont envoyés 1 mois, 2 semaines et 1 semaine avant la date d'expiration du certificat. Obtenez un nouveau certificat auprès de votre fournisseur d'identité et mettez à jour la configuration de votre IdP.

Réponses SAML

Assurez-vous que toutes les réponses SAML répondent aux conditions suivantes :

- Les réponses du fournisseur d'identité SAML doivent contenir une restriction d'audience. Par exemple :

```
<saml:AudienceRestriction>
  <saml:Audience>urn:amazon:cognito:sp:yourUserPoolID
</saml:AudienceRestriction>
```

- Les réponses doivent contenir un `InResponseTo` élément dans le `Response` objet qui correspond à l'ID de demande dans la demande d'authentification. Par exemple :

```
<samlp:Response ... InResponseTo="originalSAMLrequestId">
```

- UN `SubjectConfirmationData` l'attribut a `Recipient` et `InResponseTo` valeurs définies. Par exemple :

```
<saml:SubjectConfirmation>
  <saml:SubjectConfirmationData … Recipient="https://yourUserPoolDomain/
saml2/idpresponse" InResponseTo="originalSAMLrequestId">
</saml:SubjectConfirmation>
```

Pour plus d'informations sur la configuration de l'authentification unique (SSO) pour le système ExtraHop via les fournisseurs d'identité SAML, voir Configuration de l'authentification à distance via SAML.

Passez en revue les types d'accès et les niveaux de privilège de Reveal (x) 360

Il existe quatre types d'accès, chacun avec ses propres niveaux de privilèges, que vous pouvez accorder à vos utilisateurs dans Reveal (x) 360 : accès aux privilèges utilisateur, accès aux paquets et aux clés de session, accès au module NDR (Network Detection and Response) et accès au module NPM (Network Performance Management).

Familiarisez-vous avec les types d'accès suivants et les niveaux de privilèges associés. Vous allez mapper les noms d'attributs entre les deux systèmes dans les procédures de ce guide.

Voir Privilèges utilisateur pour découvrir ce que les utilisateurs peuvent faire pour chaque niveau de privilège dans Reveal (x) 360.

Accès privilégié de l'utilisateur

Accorde aux utilisateurs des privilèges de lecture et d'écriture dans l'ensemble du système. Huit niveaux de privilèges sont disponibles : administration du système et des accès, administration système, écriture complète, écriture limitée, écriture personnelle, lecture complète, lecture seule restreinte et aucun.

Accès aux paquets et aux clés de session

Permet aux utilisateurs de visualiser et de télécharger des captures de paquets, avec ou sans possibilité de télécharger les clés de session : pas d'accès, tranches de paquets uniquement, paquets uniquement, paquets et clés de session.

Accès au module NDR

Permet aux utilisateurs de consulter les détections de sécurité et les flux de travail : accès interdit ou accès complet.

Accès au module NPM

Permet aux utilisateurs de visualiser les détections de performances du réseau et les flux de travail : accès inexistant ou accès complet.

Si vous souhaitez uniquement accorder à vos utilisateurs l'accès aux niveaux de privilège pour l'écriture complète et la lecture complète, sans accès aux paquets et pour la détection complète, créez une feuille de calcul similaire à l'exemple suivant :

Type d'accès	Nom du niveau de privilège dans Reveal (x) 360	Valeur d'attribut dans votre IdP
Accès privilégié de l'utilisateur	Rédaction complète	Écriture complète
Accès privilégié de l'utilisateur	Lecture seule complète	En lecture seule
Accès aux paquets	Pas d'accès	Aucune

Type d'accès	Nom du niveau de privilège dans Reveal (x) 360	Valeur d'attribut dans votre IdP
Accès au module NDR	Accès complet	NDR complet
Accès au module NPM	Accès complet	NPM complet

Ajoutez votre application SAML IdP à Reveal (x) 360

1. Connectez-vous à Reveal (x) 360.
2. Cliquez sur Paramètres système en haut à droite de la page, puis cliquez sur **Toute l'administration**.
3. Cliquez **Accès utilisateur**.
4. Notez l'URL et l'identifiant de l'entité Assertion Consumer Service (ACS), que vous allez coller dans la configuration de votre IdP.
5. Collez l'URL ACS de Reveal (x) 360 dans le **URL ACS** champ sur votre IdP.
6. Collez l'ID d'entité SP de Reveal (x) 360 dans le **ID de l'entité SP** champ sur votre IdP.

Prochaines étapes
Laissez les paramètres IdP ouverts et configurez ensuite les mappages d'attributs.

Configurer les attributs qui identifient l'utilisateur

Vous devez configurer des attributs sur votre IdP qui identifient l'utilisateur dans l'ensemble du système ExtraHop par son prénom, son nom de famille et son adresse e-mail. Reportez-vous à la documentation de votre fournisseur d'identité pour connaître les noms de propriété corrects lors du mappage de ces attributs ou déclarations d'attributs.

Effectuez les étapes suivantes sur votre IdP.

1. Dans la section de mappage des attributs de l'application, ajoutez trois attributs.
2. Dans le premier attribut, sélectionnez **courriel** ou similaire. (Par exemple, dans Okta, cet attribut est appelé **utilisateur.email**.)
3. Pour le fournisseur de services, collez la chaîne suivante : `urn:oid:0.9.2342.19200300.100.1.3`
4. Dans le deuxième attribut, sélectionnez **nom de famille** ou similaire. (Par exemple, dans Okta, cet attribut est appelé **Nom de famille de l'utilisateur**.)
5. Pour le fournisseur de services, collez la chaîne suivante : `urn:oid:2.5.4.4`
6. Dans le troisième attribut, sélectionnez **prénom** ou similaire. (Par exemple, dans Okta, cet attribut est appelé **Nom de l'utilisateur**.)
7. Pour le fournisseur de services, collez la chaîne suivante : `urn:oid:2.5.4.42`

Dans Okta, par exemple, la section de mappage des attributs doit ressembler à ce qui suit :

Nom d'attribut du fournisseur de services (Reveal (x) 360)	Nom d'attribut du fournisseur d'identité (Okta)
`urn:oid:0.9.2342.19200300.100.1.3`	**utilisateur.email**
`urn:oid:2.5.4.4`	**Nom de famille de l'utilisateur**
`urn:oid:2.5.4.42`	**Nom de l'utilisateur**

Configuration des attributs pour l'accès au système

Vous devez configurer les attributs de votre fournisseur d'identité pour autoriser les utilisateurs à accéder au système ExtraHop. Vous pouvez saisir n'importe quel nom pour ces attributs, mais ils doivent correspondre à celui que vous configurerez ultérieurement dans Reveal (x) 360.

Vous devez créer au moins un attribut pour l'accès aux privilèges utilisateur. L'accès par paquets, NDR et NPM est facultatif, mais nous vous recommandons de créer ces attributs dès maintenant.

Important: Les valeurs d'attribut doivent comporter moins de 2 000 caractères.

1. Dans la section de mappage des attributs de l'application, ajoutez quatre attributs.
2. Dans le premier attribut, sélectionnez personnalisé ou similaire et saisissez un nom descriptif pour les privilèges utilisateur, tel que `niveau d'écriture`.
3. Pour le fournisseur de services, tapez un terme descriptif pour identifier l'attribut dans Reveal (x) 360, tel que `écrire`.
4. Dans le deuxième attribut, sélectionnez personnalisé ou similaire et saisissez un nom descriptif pour l'accès aux paquets, tel que `niveau des paquets`.
5. Pour le fournisseur de services, tapez un terme descriptif pour identifier l'attribut dans Reveal (x) 360, tel que `paquets`.
6. Dans le troisième attribut, sélectionnez personnalisé ou similaire et saisissez un nom descriptif pour l'accès au module NDR, tel que `niveau NDR`.
7. Pour le fournisseur de services, tapez un terme descriptif pour identifier l'attribut dans Reveal (x) 360, tel que `ndr`.
8. Dans le quatrième attribut, sélectionnez personnalisé ou similaire et tapez un nom descriptif pour l'accès au module NPM, tel que `niveau npm`.
9. Pour le fournisseur de services, tapez un terme descriptif pour identifier l'attribut dans Reveal (x) 360, tel que `npm`.
10. Enregistrez les paramètres, puis exportez le fichier XML de métadonnées de l'application.

Dans Okta, par exemple, la section de mappage des attributs doit ressembler à ce qui suit :

Nom d'attribut du fournisseur de services (Reveal (x) 360)	Nom d'attribut du fournisseur d'identité (IdP)
`écrire`	niveau d'écriture
`paquets`	niveau des paquets
`ndr`	niveau NDR
`npm`	niveau npm

Configurez les informations de votre fournisseur d'identité dans Reveal (x) 360

Voici quelques points à prendre en compte. Avant d'effectuer les étapes suivantes, assurez-vous d'avoir identifié les niveaux de privilège que vous souhaitez accorder à vos utilisateurs pour chaque type d'accès au système.

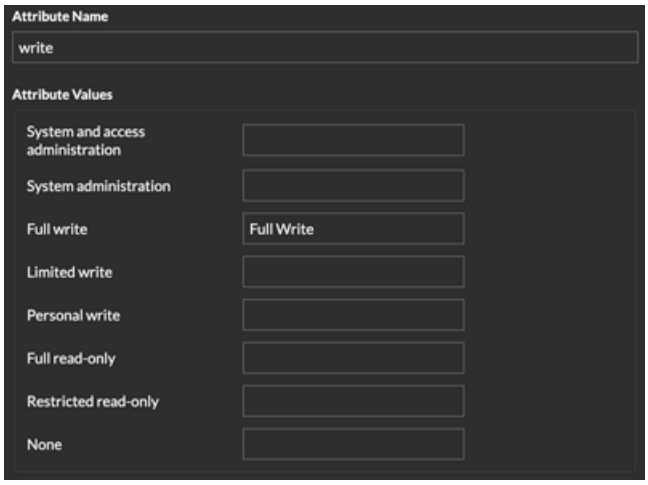
1. Dans Reveal (x) 360, sur la page Accès utilisateur, cliquez sur **Ajouter un fournisseur d'identité**.
2. Dans le **Nom du fournisseur** dans ce champ, saisissez un nom pour identifier votre fournisseur d'identité spécifique. Ce nom apparaît sur la page de connexion au système ExtraHop.

   Le nom doit respecter les directives suivantes :

   - Ne doit inclure que des points, des traits d'union et des caractères alphanumériques
   - Doit comporter entre 3 et 32 caractères

3. Ouvrez le fichier de métadonnées que vous avez exporté lors de la procédure précédente, puis copiez-collez le contenu dans **Métadonnées du fournisseur (XML)** champ.
4. Faites défiler l'écran jusqu'au Attributs de privilèges utilisateur section. Il existe trois sections, une pour chacun des types d'accès.
5. Dans le **Nom de l'attribut** dans ce champ, saisissez le nom que vous avez configuré sur votre IdP pour l'accès aux privilèges utilisateur.
6. Dans notre exemple ci-dessus, nous avons spécifié `écrire`. Dans le **Valeurs d'attribut** dans les champs, saisissez les noms des niveaux de privilèges que vous avez identifiés pour vos utilisateurs. Dans la figure ci-dessous, nous avons spécifié `Écriture complète` pour le **Privilèges d'écriture complets** valeur.

   Important: Vous devez spécifier **Nom de l'attribut** et configurez au moins une valeur d'attribut autre que **Aucune** pour permettre aux utilisateurs de se connecter.



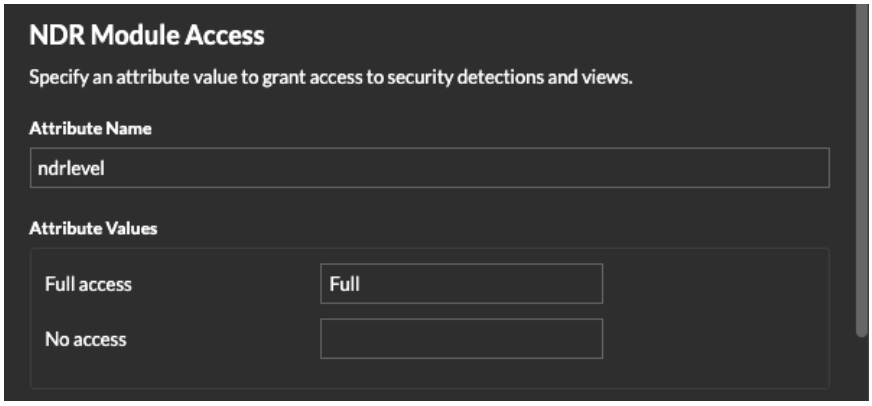
7. Faites défiler l'écran jusqu'au Accès aux paquets et aux clés de session section.

   La configuration des paquets et des attributs de clé de session est facultative et n'est requise que si vous disposez d'un stockage des paquets connecté. Si vous n'avez pas de stockage des paquets, tapez `NA` dans le **Nom de l'attribut** remplissez le champ et quittez le **Valeur d'attribut** champs vides.
8. Dans le **Nom de l'attribut** dans ce champ, saisissez le nom que vous avez configuré sur votre IdP pour l'accès aux paquets. Dans notre exemple ci-dessus, nous avons spécifié `paquets`.
9. Dans le **Valeurs d'attribut** dans les champs, saisissez les noms des niveaux de privilèges que vous avez créés pour vos utilisateurs. Dans la figure ci-dessous, nous avons spécifié `Aucune`.

10. Faites défiler l'écran jusqu'au Accès au module NDR section.

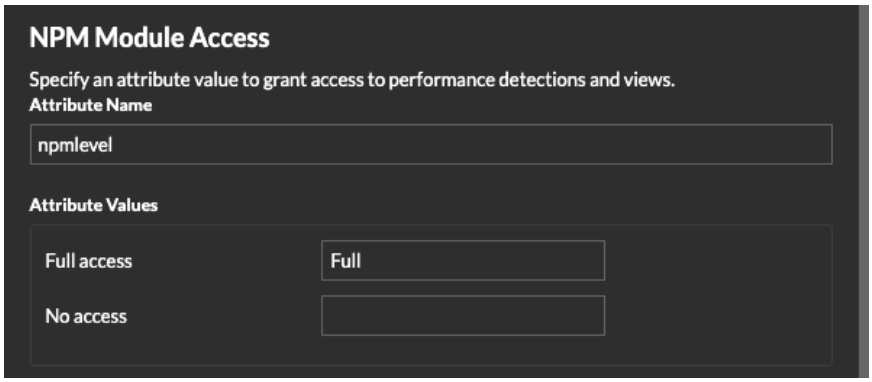
Configurez l'attribut d'accès au module NDR si vous souhaitez que les utilisateurs aient accès aux détections de sécurité et aux flux de travail. Sinon, tapez NA dans **Nom de l'attribut** champ et quittez le **Valeurs d'attribut** champs vides.

11. Dans le **Nom de l'attribut** dans ce champ, saisissez le nom que vous avez configuré sur votre IdP pour accéder au module NDR. Dans notre exemple ci-dessus, nous avons spécifié `niveau NDR`.
12. Dans le **Valeurs d'attribut** dans les champs, saisissez les noms des niveaux de privilèges que vous avez créés pour vos utilisateurs. Dans la figure ci-dessous, nous avons spécifié `Complet`.



13. Faites défiler l'écran jusqu'au Accès au module NPM section.

    Configurez l'attribut d'accès au module NPM si vous souhaitez que les utilisateurs aient accès aux détections de performances et aux flux de travail. Sinon, tapez NA dans **Nom de l'attribut** champ et quittez le **Valeurs d'attribut** champs vides.
14. Dans le **Nom de l'attribut** dans ce champ, saisissez le nom que vous avez configuré sur votre IdP pour accéder au module NPM. Dans notre exemple ci-dessus, nous avons spécifié `niveau npm`.
15. Dans le **Valeurs d'attribut** dans les champs, saisissez les noms des niveaux de privilèges que vous avez créés pour vos utilisateurs. Dans la figure ci-dessous, nous avons spécifié `Complet`.



16. Cliquez **Enregistrer**. L'enregistrement et l'activation de la configuration IdP sur le système peuvent prendre jusqu'à deux minutes.

Attribuez des privilèges aux utilisateurs de votre IdP

Vous pouvez désormais ajouter des attributs d'accès au système et les niveaux de privilèges associés à vos utilisateurs existants. Vous pouvez attribuer plusieurs privilèges à un utilisateur, mais celui-ci bénéficie toujours du privilège le plus élevé lorsqu'il se connecte au système.

Conseil Le système ExtraHop prend en charge les déclarations d'attributs de groupe pour associer facilement les privilèges des utilisateurs à tous les membres d'un groupe spécifique. Lorsque vous configurez l' application ExtraHop sur votre fournisseur d'identité, spécifiez un nom d'attribut de groupe. Ce nom est ensuite saisi dans le champ Nom de l'attribut lorsque vous configurez le fournisseur d'identité sur le système ExtraHop.

1. Dans votre IdP, sélectionnez l'utilisateur auquel vous souhaitez accorder des privilèges.
2. Ajoutez un attribut pour le type d'accès que vous avez défini précédemment, tel que writelevel.
3. Sur la même ligne, ajoutez le nom que vous avez spécifié pour le niveau de privilège, tel que Full Write.

La figure suivante montre un exemple de ces attributs dans JumpCloud :

Afficher les utilisateurs dans Reveal (x) 360

Les utilisateurs apparaissent sur la page Utilisateurs de Reveal (x) 360 après leur première connexion. Si un utilisateur n'apparaît pas dans le tableau, cela signifie qu'il n'est pas correctement authentifié et autorisé. Contactez le support ExtraHop si vous avez besoin d'aide.

1. Connectez-vous à Reveal (x) 360.
2. Cliquez sur Paramètres du système en haut à droite de la page, puis cliquez sur **Toute l'administration**.
3. Cliquez **Accès utilisateur**. Les utilisateurs qui se connectent avec succès au système apparaissent dans le tableau de la page Utilisateurs de Reveal (x) 360. Le tableau affiche le nom du fournisseur d'identité et les privilèges attribués à chaque utilisateur.
4. Cliquez sur un nom d'utilisateur pour voir les détails de l'utilisateur ou pour le supprimer du système.

Important: Lorsque vous supprimez un utilisateur, vous devez également révoquer son accès au système ExtraHop via votre IdP. Dans le cas contraire, l'utilisateur pourra peut-être se reconnecter.

Mettre à jour les paramètres du fournisseur d'identité

Lorsque vous modifiez la configuration de votre fournisseur d'identité, par exemple en régénérant le certificat IdP, vous devez exporter le nouveau fichier XML de métadonnées et mettre à jour les paramètres du fournisseur d'identité sur Reveal (x) 360.

Avant de commencer
Assurez-vous de supprimer les données indésirables, telles qu'un certificat IdP expiré, du fichier XML de métadonnées.

1. Connectez-vous à votre fournisseur d'identité.
2. Sélectionnez l'application ExtraHop sur votre fournisseur d'identité et exportez le fichier XML de métadonnées mis à jour.

3. Ouvrez le fichier XML dans un éditeur de texte et copiez-en le contenu.
4. Connectez-vous à Reveal (x) 360 avec un compte utilisateur doté de privilèges d' administration du système et des accès.
5. Cliquez sur l'icône des paramètres système puis cliquez sur **Accès utilisateur**.
6. Dans le Configuration SAML section, cliquez **Modifier le fournisseur d'identité**.
7. Collez le contenu du fichier XML dans Métadonnées du fournisseur XML champ.
8. Cliquez **Enregistrer**.

Important: Tous les utilisateurs actifs seront déconnectés après avoir enregistré la configuration mise à jour.