

Configuration de l'authentification à distance via SAML

Publié: 2024-01-31

Vous pouvez configurer une authentification unique (SSO) sécurisée pour le système ExtraHop via un ou plusieurs fournisseurs d'identité SAML (Security Assertion Markup Language).

 **Vidéo** Consultez la formation associée : [Authentification SSO](#) 

Lorsqu'un utilisateur se connecte à un système ExtraHop configuré en tant que fournisseur de services (SP) pour l'authentification SSO SAML, le système ExtraHop demande l'autorisation au fournisseur d'identité (IdP) approprié. Le fournisseur d'identité authentifie les informations d'identification de l'utilisateur, puis renvoie l'autorisation de l'utilisateur au système ExtraHop. L'utilisateur peut alors accéder au système ExtraHop.

Les guides de configuration pour des fournisseurs d'identité spécifiques sont liés ci-dessous. Si votre fournisseur ne figure pas dans la liste, appliquez les paramètres requis par le système ExtraHop à votre fournisseur d'identité.


Les fournisseurs d'identité doivent répondre aux critères suivants :

- SAML 2.0
- Supporte les flux de connexion initiés par le SP. Les flux de connexion initiés par l'IdP ne sont pas pris en charge.
- Prise en charge des réponses SAML signées
- Supporte la liaison de redirection HTTP


L'exemple de configuration présenté dans cette procédure permet d'accéder au système ExtraHop via des attributs de groupe.

Si votre fournisseur d'identité ne prend pas en charge les déclarations d'attributs de groupe, configurez les attributs utilisateur avec les privilèges appropriés pour l'accès aux modules, l'accès au système et l'analyse des paquets .

Activer l'authentification à distance SAML

 **Avertissement** Si votre système est déjà configuré avec une méthode d'authentification à distance, la modification de ces paramètres supprimera tous les utilisateurs et les personnalisations associées créées par cette méthode, et les utilisateurs distants ne pourront pas accéder au système. Les utilisateurs locaux ne sont pas concernés.

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. Sélectionnez **SAML** dans la liste déroulante de la méthode de développement d'authentification à distance, puis cliquez sur **Continuer**.
- Cliquez **Afficher les métadonnées SP** pour afficher l' URL du service ACS (Assertion Consumer Service) et l'ID d'entité du système ExtraHop. Ces chaînes sont requises par votre fournisseur d'identité pour configurer l'authentification SSO. Vous pouvez également télécharger un fichier de métadonnées XML complet que vous pouvez importer dans la configuration de votre fournisseur d'identité.

 **Note:** L'URL ACS inclut le nom d'hôte configuré dans les paramètres réseau. Si l'URL ACS contient un nom d'hôte inaccessible, tel que le nom d'hôte du système par défaut `extrahop`, vous devez modifier l'URL lorsque vous ajoutez l' URL ACS à votre fournisseur d'identité et spécifier le nom de domaine complet (FQDN) du système ExtraHop.

- Cliquez **Ajouter un fournisseur d'identité** pour ajouter les informations suivantes :

- **Nom du fournisseur:** Tapez un nom pour identifier votre fournisseur d'identité spécifique. Ce nom apparaît sur la page de connexion du système ExtraHop après **Connectez-vous avec** texte.
- **ID d'entité:** Collez l'ID d'entité fourni par votre fournisseur d'identité dans ce champ.
- **URL SSO:** Collez l'URL d'authentification unique fournie par votre fournisseur d'identité dans ce champ.
- **Certificat public:** Collez le certificat X.509 fourni par votre fournisseur d'identité dans ce champ.
- **Provisionner automatiquement les utilisateurs:** Lorsque cette option est sélectionnée, les comptes utilisateur ExtraHop sont automatiquement créés lorsque l'utilisateur se connecte via le fournisseur d'identité. Pour contrôler manuellement quels utilisateurs peuvent se connecter, décochez cette case et configurez manuellement les nouveaux utilisateurs distants via les paramètres d'administration d'ExtraHop ou l'API REST. Tout nom d'utilisateur distant créé manuellement doit correspondre au nom d'utilisateur configuré sur le fournisseur d'identité.
- **Activer ce fournisseur d'identité:** Cette option est sélectionnée par défaut et permet aux utilisateurs de se connecter au système ExtraHop. Pour empêcher les utilisateurs de se connecter via ce fournisseur d'identité, décochez la case.
- **Attributs de privilèges utilisateur:** Vous devez configurer les attributs de privilèges utilisateur pour que les utilisateurs puissent se connecter au système ExtraHop via un fournisseur d'identité. Les valeurs ne font pas la distinction entre majuscules et minuscules et peuvent inclure des espaces.

Les noms et les valeurs des attributs de privilèges utilisateur doivent correspondre aux noms et aux valeurs que votre fournisseur d'identité inclut dans les réponses SAML, qui sont configurées lorsque vous ajoutez l'application ExtraHop à un fournisseur. Par exemple, dans Azure AD, vous configurez des noms de revendications et des valeurs de conditions de réclamation qui doivent correspondre aux noms et aux valeurs des attributs de privilèges utilisateur dans le système ExtraHop. Pour des exemples plus détaillés, consultez les rubriques suivantes :

- [Configurer l'authentification unique SAML avec JumpCloud](#)
- [Configurer l'authentification unique SAML avec Google](#)
- [Configurer l'authentification unique SAML avec Okta](#)
- [Configurer l'authentification unique SAML avec Azure AD](#)



Note: Si un utilisateur correspond à plusieurs valeurs d'attributs, il bénéficie du privilège d'accès le plus permissif. Par exemple, si un utilisateur correspond à la fois aux valeurs d'écriture limitée et d'écriture complète, il bénéficie de privilèges d'écriture complète. Pour plus d'informations sur les niveaux de privilèges, consultez [Utilisateurs et groupes d'utilisateurs](#).

- **Accès au module NDR:** Les attributs NDR permettent aux utilisateurs d'accéder aux fonctionnalités NDR.
- **Accès au module NPM:** Les attributs NPM permettent aux utilisateurs d'accéder aux fonctionnalités NPM.
- **Accès aux paquets et aux clés de session:** Les attributs des paquets et des clés de session permettent aux utilisateurs d'accéder aux paquets et aux clés de session. La configuration des paquets et des attributs de clé de session est facultative et requise uniquement lorsque vous disposez d'un stockage des paquets ExtraHop connecté.

Mappage des attributs utilisateur

Vous devez configurer l'ensemble d'attributs utilisateur suivant dans la section de mappage des attributs d'application de votre fournisseur d'identité. Ces attributs identifient l'utilisateur dans l'ensemble du système ExtraHop. Reportez-vous à la documentation de votre fournisseur d'identité pour connaître les noms de propriétés corrects lors du mappage des attributs.

Nom de l'attribut ExtraHop	Nom convivial	Catégorie	Nom de l'attribut du fournisseur d'identité
urn:oid:0.9.2342.19200300.100.1.3	email	Attribut standard	Adresse e-mail principale
urn:oid:2.5.4.4	sn	Attribut standard	Nom de famille
urn:oid:2.5.4.42	Prénom	Attribut standard	Prénom

USER ATTRIBUTE MAPPING: ⓘ

Service Provider Attribute Name

Identity Provider Attribute Name

urn:oid:0.9.2342.19200300.100.1.3

email

urn:oid:2.5.4.4

lastname

urn:oid:2.5.4.42

firstname

Déclarations d'attributs de groupe

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.

GROUP ATTRIBUTES ⓘ

include group attribute

Si votre fournisseur d'identité ne prend pas en charge les déclarations d'attributs de groupe, configurez les attributs utilisateur avec les privilèges appropriés pour l'accès aux modules, l'accès au système et l'analyse des paquets .

Prochaines étapes

- [Configurer l'authentification unique SAML avec JumpCloud](#) ↗
- [Configurer l'authentification unique SAML avec Google](#) ↗
- [Configurer l'authentification unique SAML avec Okta](#) ↗