

Configurer l'authentification unique SAML avec Google

Publié: 2024-09-26

Vous pouvez configurer votre système ExtraHop pour permettre aux utilisateurs de se connecter au système via le service de gestion des identités de Google.

Avant de commencer

- Vous devez être familiarisé avec l'administration de Google Admin.
- Vous devez être familiarisé avec l'administration des systèmes ExtraHop.

Ces procédures vous obligent à copier-coller des informations entre le système ExtraHop et la console d'administration Google. 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 le Paramètres d'accès section, cliquez sur **Authentification à distance**.
3. À partir du **méthode d'authentification à distance** liste déroulante, sélectionnez **SAML**.
4. Cliquez **Continuer**.
5. Cliquez **Afficher les métadonnées SP**.
6. Copiez le URL ACS et ID d'entité dans un fichier texte.

Vous collerez ces informations dans la configuration de Google lors d'une procédure ultérieure.

Ajouter des attributs personnalisés à l'utilisateur

1. Connectez-vous à la console d'administration Google.
2. Cliquez **Utilisateurs**.
3. Cliquez sur l'icône Gérer les attributs personnalisés .
4. Cliquez **Ajouter un attribut personnalisé**.
5. Dans le Catégorie champ, type `Hop` supplémentaire.
6. Optionnel : Dans le Descriptif champ, saisissez une description.
7. Dans le Champs personnalisés section, entrez les informations suivantes :
 - a) Dans le Nom champ, type `niveau` d'écriture.
 - b) À partir du **Type d'information** liste déroulante, sélectionnez **Texte**.
 - c) À partir du **Visibilité** liste déroulante, sélectionnez **Visible pour le domaine**.
 - d) À partir du **Nombre de valeurs** liste déroulante, sélectionnez **Valeur unique**.
8. Activez l'accès au module NDR :
 - a) Dans le Nom champ, type `niveau` NDR.
 - b) À partir du **Type d'information** liste déroulante, sélectionnez **Texte**.
 - c) À partir du **Visibilité** liste déroulante, sélectionnez **Visible pour le domaine**.
 - d) À partir du **Nombre de valeurs** liste déroulante, sélectionnez **Valeur unique**.
9. Activez l'accès au module NPM :
 - a) Dans le Nom champ, type `niveau` NPM.
 - b) À partir du **Type d'information** liste déroulante, sélectionnez **Texte**.
 - c) À partir du **Visibilité** liste déroulante, sélectionnez **Visible pour le domaine**.

- d) À partir du **Nombre de valeurs** liste déroulante, sélectionnez **Valeur unique**.
10. Optionnel : Si vous avez connecté des magasins de paquets, activez l'accès aux paquets en configurant un champ personnalisé :
 - a) Dans le Nom champ, type `niveau des paquets`.
 - b) À partir du **Type d'information** liste déroulante, sélectionnez **Texte**.
 - c) À partir du **Visibilité** liste déroulante, sélectionnez **Visible pour le domaine**.
 - d) À partir du **Nombre de valeurs** liste déroulante, sélectionnez **Valeur unique**.
11. Cliquez **Ajouter**.

Ajouter les informations du fournisseur d'identité de Google au système ExtraHop

1. Dans la console d'administration Google, cliquez sur l'icône du menu principal  et sélectionnez **Apps > Applis SAML**.
2. Cliquez sur Activer le SSO pour une application SAML icône .
3. Cliquez **CONFIGURER MA PROPRE APPLICATION PERSONNALISÉE**.
4. Sur le Informations sur Google IdP écran, cliquez sur **Télécharger** bouton pour télécharger le certificat (`GoogleIDPCertificate.pem`).
5. Revenez aux paramètres d'administration du système ExtraHop.
6. Cliquez **Ajouter un fournisseur d'identité**.
7. Dans le Nom du fournisseur dans le champ, saisissez un nom unique.
Ce nom apparaît sur la page de connexion du système ExtraHop.
8. À partir du Informations sur Google IdP écran, copiez l'URL SSO et collez-la dans URL SSO champ sur l'appliance ExtraHop.
9. À partir du Informations sur Google IdP écran, copiez l'ID d'entité et collez-le dans le champ ID d'entité du système ExtraHop.
10. Ouvrez le `GoogleIDPCertificate` dans un éditeur de texte, copiez le contenu et collez-le dans Certificat public champ sur le système ExtraHop.
11. Choisissez la manière dont vous souhaitez approvisionner les utilisateurs parmi l'une des options suivantes.
 - Sélectionnez **Provisionner automatiquement les utilisateurs** pour créer un nouveau compte utilisateur SAML distant sur le système ExtraHop lors de la première connexion de l'utilisateur.
 - Effacez le **Provisionner automatiquement les utilisateurs** cochez la case et configurez manuellement les nouveaux utilisateurs distants via les paramètres d'administration d'ExtraHop ou l'API REST. Les niveaux d'accès et de privilèges sont déterminés par la configuration de l'utilisateur dans Google.
12. 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.
13. 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. Les 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** pour permettre aux utilisateurs de se connecter.

Dans l'exemple ci-dessous, Nom de l'attribut le champ est l'attribut de l' application et Valeur de l'attribut est le nom du champ utilisateur configuré lors de la création de l'application ExtraHop sur le fournisseur d'identité.

Nom du champ	Exemple de valeur d'attribut
Nom de l'attribut	urn:extrahop:saml:2.0:writelevel
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

14. Configurez l'accès au module NDR.

Champ	Exemple de valeur d'attribut
Nom de l'attribut	urn:extrahop:saml:2.0:ndrlevel
Accès complet	complet
Pas d'accès	aucune

15. Configurez l'accès au module NPM.

Champ	Exemple de valeur d'attribut
Nom de l'attribut	urn:extrahop:saml:2.0:npmlevel
Accès complet	complet
Pas d'accès	aucune

16. Optionnel : Configurez l'accès 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 connecté.

Nom du champ	Exemple de valeur d'attribut
Nom de l'attribut	urn:extrahop:saml:2.0:packetslevel
Paquets et clés de session	complet_avec_touche
Paquets uniquement	complet
Sachets (tranches uniquement)	tranches
Pas d'accès	aucune

17. Cliquez **Enregistrer**.

18. [Enregistrez la configuration en cours](#) .

Ajouter les informations du fournisseur de services ExtraHop à Google

1. Revenez à la console d'administration Google et cliquez sur **Suivant** sur le Informations sur les adresses IP de Google page pour passer à l'étape 3 de 5.

Step 2 of 5 X

Google IdP Information

Choose from either option to setup Google as your identity provider. Please add details in the SSO config for the service provider. [Learn more](#)

Option 1

SSO URL	https://accounts.google.com/o/saml2/idp?idpid=C01ntthr1
Entity ID	https://accounts.google.com/o/saml2?idpid=C01ntthr1
Certificate	<p>Google_2020-10-31-123717_SAML2.0</p> <p>Expires Oct 31, 2020</p> <p>↓ DOWNLOAD</p>

----- OR -----

Option 2

IDP metadata	↓ DOWNLOAD
--------------	----------------------------

[PREVIOUS](#)
[CANCEL](#)
[NEXT](#)

2. Dans le Nom de l'application dans ce champ, saisissez un nom unique pour identifier le système ExtraHop.
Chaque système ExtraHop pour lequel vous créez une application SAML a besoin d'un nom unique .
3. Optionnel : Tapez une description pour cette application ou téléchargez un logo personnalisé.
4. Cliquez **Suivant**.
5. Copiez le URL du service aux consommateurs d'assertion (ACS) depuis le système ExtraHop et collez-le dans URL DE L'ACS champ dans Google Admin.

 **Note:** Vous devrez peut-être modifier manuellement l'URL ACS si celle-ci contient un nom d'hôte inaccessible, tel que le nom d'hôte du système par défaut `extrahop`. Nous vous recommandons de spécifier le nom de domaine complet pour le système ExtraHop dans l'URL.
6. Copiez le ID d'entité SP depuis le système ExtraHop et collez-le dans ID d'entité champ dans Google Admin.
7. Sélectionnez le **Réponse signée** case à cocher.
8. Dans le Nom ID section, laissez la valeur par défaut **Informations de base** et **E-mail principal** paramètres inchangés.

9. À partir du **Format d'identification du nom** liste déroulante, sélectionnez **PERSISTANT**.
10. Cliquez **Suivant**.
11. Sur le Cartographie des attributs écran, cliquez **AJOUTER UN NOUVEAU MAPPING**.
12. Ajoutez les attributs suivants exactement comme indiqué.

Les quatre premiers attributs sont obligatoires. Le `packetslevel` L'attribut est facultatif et n'est obligatoire que si vous avez un stockage des paquets connecté. Si vous avez un stockage des paquets et que vous ne configurez pas `packetslevel` attribut, les utilisateurs ne pourront pas afficher ou télécharger les captures de paquets dans le système ExtraHop.

Attribut de l'application	Catégorie	Champ utilisateur
urn:oid : 0.9.2342.19200300.100.1.3	Informations de base	E-mail principal
urn:oid : 2.5.4.4	Informations de base	Nom de famille
urn:oid : 2.5.4.42	Informations de base	Prénom
urn:extrahop:saml:2.0:write	Hop supplémentaire	niveau d'écriture
urn:extrahop:saml:2.0:ndr	Hop supplémentaire	niveau NDR
urn:extrahop:saml:2.0:npm	Hop supplémentaire	niveau NPM
urn:extrahop:saml:2.0:packetslevel	Hop supplémentaire	niveau des paquets

13. Cliquez **Terminer** puis cliquez sur **OK**.
14. Cliquez **Modifier le service**.
15. Sélectionnez **Activé pour tous**.
16. Cliquez **Enregistrer**.

Attribuer des privilèges aux utilisateurs

1. Cliquez **Les utilisateurs** pour revenir au tableau de tous les utilisateurs de vos unités organisationnelles.
 2. Cliquez sur le nom de l'utilisateur que vous souhaitez autoriser à se connecter au système ExtraHop.
 3. Dans le Informations sur l'utilisateur section, cliquez sur **Informations sur l'utilisateur**.
 4. Dans le Hop supplémentaire section, cliquez sur **niveau d'écriture** et saisissez l'un des niveaux de privilège suivants.
 - illimité
 - écriture_complète
 - écriture_limitée
 - écriture_personnelle
 - full_readonly
 - restricted_readonly
 - aucune
- Pour plus d'informations sur les privilèges utilisateur, voir [Utilisateurs et groupes d'utilisateurs](#).
5. Optionnel : Si vous avez ajouté `packetslevel` attribut ci-dessus, cliquez sur **niveau des paquets** et saisissez l'un des privilèges suivants.
 - complet
 - complet_avec_écriture
 - aucune

ExtraHop

writelevel

full_write

packetslevel

full

6. Optionnel : Si vous avez ajouté `detectionslevel` attribut ci-dessus, cliquez sur **niveau de détection** et saisissez l'un des privilèges suivants.
 - `complet`
 - `aucune`
7. Cliquez **Enregistrer**.

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. Vous êtes automatiquement dirigé vers la page d'aperçu d'ExtraHop.