

SAML-Single-Sign-On mit Google konfigurieren

Veröffentlicht: 2024-04-10

Sie können Ihr ExtraHop-System so konfigurieren, dass sich Nutzer über den Google-Identitätsverwaltungsdienst beim System anmelden können.

Bevor Sie beginnen

- Sie sollten mit der Verwaltung von Google Admin vertraut sein.
- Sie sollten mit der Verwaltung von ExtraHop-Systemen vertraut sein.

Bei diesen Verfahren müssen Sie Informationen zwischen dem ExtraHop-System und der Google Admin-Konsole kopieren und einfügen. Daher ist es hilfreich, jedes System nebeneinander zu öffnen.

SAML auf dem ExtraHop-System aktivieren

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. Klicken Sie im Abschnitt Zugriffseinstellungen auf **Fernauthentifizierung**.
3. Wählen Sie in der Dropdownliste Remoteauthentifizierungsmethode die Option **SAML**.
4. klicken **Weiter**.
5. klicken **SP-Metadaten anzeigen**.
6. Kopiere das ACS-URL und Entitäts-ID in eine Textdatei. Sie werden diese Informationen in einem späteren Verfahren in die Google-Konfiguration einfügen.

Fügen Sie benutzerdefinierte Benutzerattribute hinzu

1. Melden Sie sich bei der Google Admin-Konsole an.
2. klicken **Nutzer**.
3. Klicken Sie auf das Symbol Benutzerdefinierte Attribute verwalten .
4. klicken **Benutzerdefiniertes Attribut hinzufügen**.
5. Geben Sie in das Feld Kategorie ein `ExtraHop`.
6. Optional: Geben Sie eine Beschreibung in das Beschreibung Feld.
7. In der Benutzerdefinierte Felder Abschnitt, geben Sie die folgenden Informationen ein.
 - a) Geben Sie in das Feld Name `Ebene` schreiben.
 - b) Aus dem Art der Information Drop-down-Liste, wählen **Text**.
 - c) Aus dem Sichtbarkeit Drop-down-Liste, wählen **Sichtbar für die Domain**.
 - d) Aus dem Anzahl der Werte Drop-down-Liste, wählen **Einzelner Wert**.
8. Zugriff auf das NDR-Modul aktivieren
 - a) In der Name Feld, Typ `NDR-Ebene`.
 - b) Aus dem Art der Information Drop-down-Liste, wählen **Text**.
 - c) Aus dem Sichtbarkeit Drop-down-Liste, wählen **Sichtbar für die Domain**.
 - d) Aus dem Anzahl der Werte Drop-down-Liste, wählen **Einzelner Wert**.
9. NPM-Modulzugriff aktivieren
 - a) In der Name Feld, Typ `npm-Ebene`.
 - b) Aus dem Art der Information Drop-down-Liste, wählen **Text**.
 - c) Aus dem Sichtbarkeit Drop-down-Liste, wählen **Sichtbar für die Domain**.

- d) Aus dem Anzahl der Werte Drop-down-Liste, wählen **Einzelner Wert**.
10. Optional: Wenn Sie Paketspeicher verbunden haben, aktivieren Sie den Paketzugriff, indem Sie ein benutzerdefiniertes Feld mit den folgenden Informationen konfigurieren.
 - a) In der Name Feld, Typ `Paketebene`.
 - b) Aus dem Art der Information Drop-down-Liste, wählen **Text**.
 - c) Aus dem Sichtbarkeit Drop-down-Liste, wählen **Sichtbar für die Domain**.
 - d) Aus dem Anzahl der Werte Drop-down-Liste, wählen **Einzelner Wert**.
11. klicken **Hinzufügen**.

Fügen Sie Identitätsanbieterinformationen von Google zum ExtraHop-System hinzu

1. Klicken Sie in der Google Admin-Konsole auf das Hauptmenüsymbol  und wähle **Apps > SAML-Apps**.
2. Klicken Sie auf SSO für eine SAML-Anwendung aktivieren Symbol .
3. klicken **RICHE MEINE EIGENE BENUTZERDEFINIERTER APP EIN**.
4. Auf dem Google IdP-Informationen Bildschirm, klicken Sie auf **Herunterladen** Schaltfläche zum Herunterladen des Zertifikats (`GoogleIDPCertificate.pem`).
5. Kehren Sie zu den Administrationseinstellungen des ExtraHop-Systems zurück.
6. klicken **Identitätsanbieter hinzufügen**.
7. Geben Sie einen eindeutigen Namen in das Name des Anbieters Feld. Dieser Name erscheint auf der Anmeldeseite des ExtraHop-Systems.
8. Aus dem Google IdP-Informationen Bildschirm, kopiere die SSO-URL und füge sie in das SSO-URL Feld auf der ExtraHop-Appliance.
9. Aus dem Google IdP-Informationen Bildschirm, kopieren Sie die Entitäts-ID und fügen Sie sie in das Feld Entitäts-ID auf dem ExtraHop-System ein.
10. Öffne das `GoogleIDPCertificate` Kopieren Sie den Inhalt in einem Texteditor und fügen Sie ihn in den Öffentliches Zertifikat Feld auf dem ExtraHop-System.
11. Wählen Sie aus einer der folgenden Optionen aus, wie Sie Benutzer bereitstellen möchten.
 - Wählen **Automatische Bereitstellung von Benutzern** um ein neues Remote-SAML-Benutzerkonto auf dem ExtraHop-System zu erstellen, wenn sich der Benutzer zum ersten Mal anmeldet .
 - Lösche das **Automatische Bereitstellung von Benutzern** kreuzen Sie das Kästchen an und konfigurieren Sie neue Remote-Benutzer manuell über die ExtraHop-Administrationseinstellungen oder die REST-API. Zugriffs- und Berechtigungsstufen werden durch die Benutzerkonfiguration in Google bestimmt.
12. Die **Diesen Identitätsanbieter aktivieren** Die Option ist standardmäßig ausgewählt und ermöglicht es Benutzern, sich beim ExtraHop-System anzumelden. Um zu verhindern, dass sich Benutzer anmelden, deaktivieren Sie das Kontrollkästchen.
13. Konfigurieren Sie Benutzerberechtigungsattribute. Sie müssen den folgenden Satz von Benutzerattributen konfigurieren, bevor sich Benutzer über einen Identitätsanbieter beim ExtraHop-System anmelden können. Werte sind vom Benutzer definierbar; sie müssen jedoch mit den Attributnamen übereinstimmen, die in der SAML-Antwort Ihres Identity Providers enthalten sind. Bei Werten wird nicht zwischen Groß- und Kleinschreibung unterschieden und sie können Leerzeichen enthalten. Weitere Informationen zu Berechtigungsstufen finden Sie unter **Benutzer und Benutzergruppen**. [↗](#)



Wichtig: Sie müssen den Attributnamen angeben und mindestens einen anderen Attributwert konfigurieren als **Kein Zugriff** um Benutzern die Anmeldung zu ermöglichen.

Im Beispiel unten ist der Name des Attributs Feld ist das Anwendungsattribut und das Wert des Attributs ist der Benutzerfeldname, der bei der Erstellung der ExtraHop-Anwendung auf dem Identity Provider konfiguriert wurde.

Name des Feldes	Beispiel für einen Attributwert
Name des Attributs	urn:extrahop:saml:2.0:Ebene schreiben
System- und Zugriffsverwaltung	illimitiert
Volle Schreibrechte	vollendes_schreiben
Eingeschränkte Schreibrechte	begrenztes_schreiben
Persönliche Schreibrechte	persönliches_schreiben
Volle Leserechte	full_readonly
Eingeschränkte Leserechte	restricted_readonly
Kein Zugriff	keine

14. Konfigurieren Sie den Zugriff auf das NDR-Modul.

Feld	Beispiel für einen Attributwert
Name des Attributs	urn:extrahop:saml:2.0:ndrlevel
Voller Zugriff	voll
Kein Zugriff	keine

15. Konfigurieren Sie den NPM-Modulzugriff.

Feld	Beispiel für einen Attributwert
Name des Attributs	urn:extrahop:saml:2.0:npmlevel
Voller Zugriff	voll
Kein Zugriff	keine

16. Optional: Konfigurieren Sie Pakete und den Zugriff auf Sitzungsschlüssel. Die Konfiguration von Paketen und Sitzungsschlüsselattributen ist optional und nur erforderlich, wenn Sie über einen verbundenen Packetstore verfügen.

Name des Feldes	Beispiel für einen Attributwert
Name des Attributs	urn:extrahop:saml:2.0:Paketebene
Pakete und Sitzungsschlüssel	voll mit Schlüsseln
Nur Pakete	voll
Nur Pakete, Scheiben	Scheiben
Kein Zugriff	keine

17. klicken **Speichern**.
18. [Speichern Sie die laufende Konfiguration](#) .

ExtraHop-Dienstanbieterinformationen zu Google hinzufügen

1. Kehren Sie zur Google Admin-Konsole zurück und klicken Sie auf **Weiter** auf dem Google Idp-Informationen Seite, um mit Schritt 3 von 5 fortzufahren.

Step 2 of 5 ×

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. Geben Sie einen eindeutigen Namen in das Name der Anwendung Feld zur Identifizierung des ExtraHop-Systems. Jedes ExtraHop-System, für das Sie eine SAML-Anwendung erstellen, benötigt einen eindeutigen Namen.
3. Optional: Geben Sie eine Beschreibung für diese Anwendung ein oder laden Sie ein benutzerdefiniertes Logo hoch.
4. klicken **Weiter**.
5. Kopiere das URL des Assertion Consumer Service (ACS) aus dem ExtraHop-System und fügen Sie es in das ACS-URL Feld in Google Admin.



Hinweis Möglicherweise müssen Sie die ACS-URL manuell bearbeiten, wenn die URL einen nicht erreichbaren Hostnamen enthält, z. B. den Standardhostnamen des Systems `extrahop`. Wir empfehlen, dass Sie den vollqualifizierten Domänenname für das ExtraHop-System in der URL angeben.

6. Kopiere das SP-Entitäts-ID aus dem ExtraHop-System und fügen Sie es in das Entitäts-ID Feld in Google Admin.
7. Wählen Sie den **Signierte Antwort** Checkbox.

8. In der Name ID Abschnitt, belassen Sie die Standardeinstellung **Grundlegende Informationen** und **Primäre E-Mail** Einstellungen unverändert.
9. Aus dem Format der Namens-ID Drop-down-Liste, wählen **HARTNÄCKIG**.
10. klicken **Weiter**.
11. Auf dem Zuordnung von Attributen Bildschirm, klicken **NEUES MAPPING HINZUFÜGEN**.
12. Fügen Sie die folgenden Attribute genau wie gezeigt hinzu. Die ersten vier Attribute sind erforderlich. Die `packetslevel` Das Attribut ist optional und nur erforderlich, wenn Sie einen verbundenen Packetstore haben. Wenn Sie einen Packetstore haben und den nicht konfigurieren `packetslevel` Attribut, Benutzer können Paketerfassungen im ExtraHop-System nicht anzeigen oder herunterladen.

Anwendungsattribut	Kategorie	Feld „Benutzer“
<code>urn:oid:0.9.2342.19200300</code>	Grundlegende Informationen	Primäre E-Mail
<code>urn: oid: 2.5.4.4</code>	Grundlegende Informationen	Nachname
<code>urn: oid: 2.5.4.42</code>	Grundlegende Informationen	Vorname
<code>urn:extrahop:saml:2.0:Ebene schreiben</code>	ExtraHop	Ebene schreiben
<code>urn:extrahop:saml:2.0:ndr</code>	ExtraHop	NDR-Ebene
<code>urn:extrahop:saml:2.0:npm</code>	ExtraHop	npm-Ebene
<code>urn:extrahop:saml:2.0:Paketebene</code>	ExtraHop	Paketebene

13. klicken **Fertig stellen** und dann klicken **OK**.
14. klicken **Dienst bearbeiten**.
15. Wählen **Für alle an**, und klicken Sie dann auf **Speichern**.

Benutzerrechte zuweisen

1. klicken **Nutzer** um zur Tabelle aller Benutzer in Ihren Organisationseinheiten zurückzukehren.
2. Klicken Sie auf den Namen des Benutzers, dem Sie die Anmeldung am ExtraHop-System erlauben möchten.
3. In der Informationen für den Nutzer Abschnitt, klicken **Angaben zum Nutzer**.
4. Klicken Sie im Bereich ExtraHop auf **Ebene schreiben** und geben Sie eine der folgenden Berechtigungsstufen ein.
 - `illimitiert`
 - `vollendes_schreiben`
 - `begrenztes_schreiben`
 - `persönliches_schreiben`
 - `full_readonly`
 - `restricted_readonly`
 - `keine`

Hinweise zu Benutzerberechtigungen finden Sie unter [Benutzer und Benutzergruppen](#).
5. Optional: Wenn du das hinzugefügt hast `packetslevel` Attribut oben, klicken **Paketebene** und geben Sie eines der folgenden Rechte ein.
 - `voll`
 - `voll_mit_schreiben`
 - `keine`

ExtraHop

writelevel

full_write

packetslevel

full

- Optional: Wenn du das hinzugefügt hast `detectionslevel` Attribut oben, klicken **Erkennungsstufe** und geben Sie eines der folgenden Rechte ein.
 - voll
 - keine
- klicken **Speichern**.

Loggen Sie sich in das ExtraHop-System ein

- Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
- klicken **Loggen Sie sich ein mit** `<provider name>`.
- Melden Sie sich mit Ihrer E-Mail-Adresse und Ihrem Passwort bei Ihrem Anbieter an. Sie werden automatisch zur ExtraHop-Übersichtsseite weitergeleitet.