SAML-Single-Sign-On mit Google konfigurieren

Veröffentlicht: 2024-08-09

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. In der Auf Einstellungen zugreifen Abschnitt, klicken **Fernauthentifizierung**.
3. Aus dem **Methode der Fernauthentifizierung** Dropdownliste, wählen **SAML**.
4. Klicken Sie **Weiter**.
5. Klicken Sie **SP-Metadaten anzeigen**.
6. Kopieren Sie das ACS-URL und Entitäts-ID in eine Textdatei.
   Sie werden diese Informationen in einem späteren Verfahren in die Google-Konfiguration einfügen.

Benutzerdefinierte Benutzerattribute hinzufügen

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

d) Aus dem **Anzahl der Werte** Dropdownliste, wählen **Einzelner Wert**.

10. Optional: Wenn Sie Paketspeicher verbunden haben, aktivieren Sie den Paketzugriff, indem Sie ein benutzerdefiniertes Feld konfigurieren:
    a) In der Name Feld, Typ `Paketebene`.
    b) Aus dem **Art der Information** Dropdownliste, wählen **Text**.
    c) Aus dem **Sichtbarkeit** Dropdownliste, wählen **Sichtbar für Domain**.
    d) Aus dem **Anzahl der Werte** Dropdownliste, wählen **Einzelner Wert**.
11. Klicken Sie **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 **RICHTE MEINE EIGENE BENUTZERDEFINIERTE 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 auf dem ExtraHop-System zurück.
6. klicken **Identitätsanbieter hinzufügen**.
7. In der Name des Anbieters Feld, geben Sie einen eindeutigen Namen ein.

   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 .
    - Löschen Sie das **Automatische Bereitstellung von Benutzern** Markieren Sie das Kontrollkästchen 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. Das **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 die folgenden Benutzerattribute konfigurieren, bevor sich Benutzer über einen Identitätsanbieter beim ExtraHop-System anmelden können. Werte sind benutzerdefinierbar; sie müssen jedoch mit den Attributnamen übereinstimmen, die in der SAML-Antwort Ihres Identitätsanbieters enthalten sind. Bei Werten wird nicht zwischen Groß - und Kleinschreibung unterschieden und sie können Leerzeichen enthalten. Weitere Hinweise 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 Attributwert ist der Name des Benutzerfeldes, 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	`voll_schreiben`
Eingeschränkte Schreibrechte	`begrenztes_schreiben`
Persönliche Schreibrechte	`persönliches_schreiben`
Volle Nur-Lese-Rechte	`voll_schreibgeschützt`
Eingeschränkte Nur-Lese-Rechte	`restricted_readonly`
Kein Zugriff	`keine`

14. Konfigurieren Sie den NDR-Modulzugriff.

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`

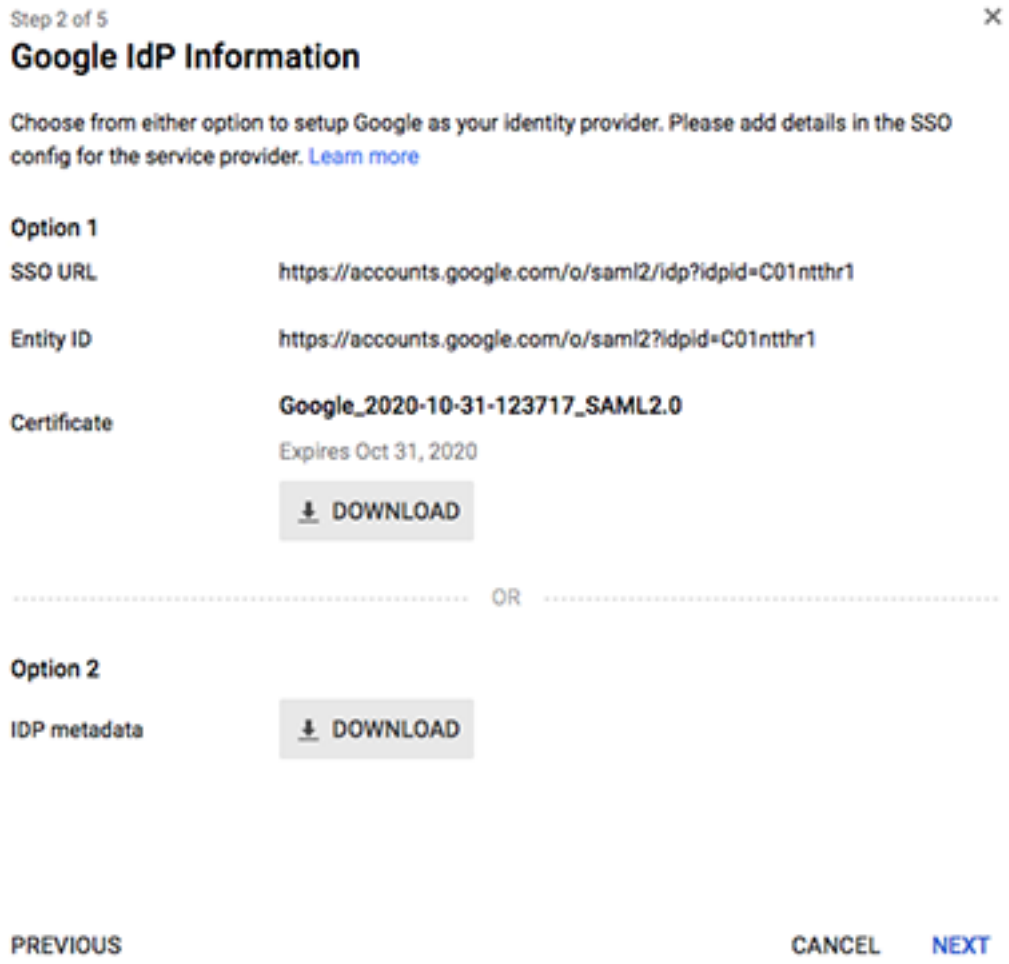
16. Optional: Konfigurieren Sie den Zugriff auf Pakete und Sitzungsschlüssel.
    Die Konfiguration von Paketen und Sitzungsschlüsselattributen ist optional und nur erforderlich , wenn Sie einen verbundenen Packetstore haben.

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`
Pakete nur in Segmenten	`Scheiben`
Kein Zugriff	`keine`

17. Klicken Sie **Speichern**.
18. Speichern Sie die laufende Konfiguration.

Fügen Sie Informationen zum ExtraHop-Dienstanbieter zu Google hinzu

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.



2. In der Name der Anwendung Feld, geben Sie einen eindeutigen Namen ein, um das ExtraHop-System zu identifizieren.

   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 Sie **Weiter**.
5. Kopieren Sie das URL des Assertion Consumer Service (ACS) aus dem ExtraHop-System und füge es ein 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 Standardsystemhostnamen `extrahop`. Wir empfehlen Ihnen, den vollqualifizierten Domänenname für das ExtraHop-System in der URL anzugeben.
6. Kopieren Sie das SP-Entitäts-ID aus dem ExtraHop-System und füge es ein in das Entitäts-ID Feld in Google Admin.
7. Wählen Sie die **Signierte Antwort** Ankreuzfeld.

8. In der Name ID Abschnitt, belassen Sie die Standardeinstellung **Grundlegende Informationen** und **Primäre E-Mail** Einstellungen unverändert.
9. Aus dem **Namens-ID-Format** Dropdownliste, wählen **HARTNÄCKIG**.
10. Klicken Sie **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. Das `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	Benutzerfeld
`urn:oid:0.9.2342.19200300.100.1.3`	Grundlegende Informationen	Primäre E-Mail
`urn:oid:2.5.4.4`	Grundlegende Informationen	Nachname
`urn:oid:2.5.4.42`	Grundlegende Informationen	Vorname
`urn:extrahop:saml:2.0:Ebene schreiben`	ExtraHop	Level schreiben
`urn:extrahop:saml:2.0:ndrlevel`	ExtraHop	ndr-Niveau
`urn:extrahop:saml:2.0:npmlevel`	ExtraHop	npm-Ebene
`urn:extrahop:saml:2.0:Paketebene`	ExtraHop	Paketebene

13. Klicken Sie **Fertig** und klicken Sie dann **OK**.
14. Klicken Sie **Dienst bearbeiten**.
15. Wählen **An für alle**.
16. Klicken Sie **Speichern**.

Benutzerrechte zuweisen

1. Klicken Sie **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 ermöglichen möchten.
3. In der Informationen zum Nutzer Abschnitt, klicken **Angaben zum Nutzer**.
4. In der ExtraHop Abschnitt, klicken **Level schreiben** und geben Sie eine der folgenden Berechtigungsstufen ein.

   - `illimitiert`
   - `voll_schreiben`
   - `begrenztes_schreiben`
   - `persönliches_schreiben`
   - `voll_schreibgeschützt`
   - `restricted_readonly`
   - `keine`

   Hinweise zu Benutzerrechten 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`

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

Loggen Sie sich in das ExtraHop-System ein

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