SAML-Single-Sign-On mit Okta konfigurieren

Veröffentlicht: 2024-08-09

Sie können Ihr ExtraHop-System so konfigurieren, dass sich Benutzer über den Okta Identity Management Service beim System anmelden können.

Bevor Sie beginnen

- Sie sollten mit der Verabreichung von Okta vertraut sein. Diese Verfahren basieren auf der Okta Classic-Benutzeroberfläche. Wenn Sie Okta über die Developer Console konfigurieren, ist das Verfahren möglicherweise etwas anders.
- Sie sollten mit der Verwaltung von ExtraHop-Systemen vertraut sein.

Bei diesen Verfahren müssen Sie Informationen zwischen dem ExtraHop-System und der Okta Classic-Benutzeroberfläche 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**.

   Sie müssen die ACS-URL und die Entitäts-ID kopieren, um sie im nächsten Verfahren in die Okta-Konfiguration einzufügen.

SAML-Einstellungen in Okta konfigurieren

Bei diesem Verfahren müssen Sie Informationen zwischen den ExtraHop-Administrationseinstellungen und der Okta Classic-Benutzeroberfläche kopieren und einfügen. Daher ist es hilfreich, wenn alle Benutzeroberflächen nebeneinander geöffnet sind.

1. Loggen Sie sich bei Okta ein.
2. Ändern Sie in der oberen rechten Ecke der Seite die Ansicht von **Entwicklerkonsole** zu **Klassische Benutzeroberfläche**.

3. Klicken Sie im oberen Menü auf **Anwendungen**.
4. Klicken Sie **Anwendung hinzufügen**.
5. Klicken Sie **Neue App erstellen**.
6. Aus dem Plattform Dropdownliste, wählen **Netz**.
7. Für die Anmeldemethode, wählen **SAML 2.0** .
8. Klicken Sie **Erstellen**.
9. In der Allgemeine Einstellungen Abschnitt, in der App Namensfeld, geben Sie einen eindeutigen Namen ein, um das ExtraHop-System zu identifizieren.
10. Optional: Konfiguriere die Logo der App und Sichtbarkeit der App Felder, die für Ihre Umgebung erforderlich sind.

11. Klicken Sie **Weiter**.
12. In der SAML-Einstellungen Fügen Sie in den Abschnitten die URL des Assertion Consumer Service (ACS) aus dem ExtraHop-System in das Feld Single Sign On URL in Okta ein.

    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.
13. Fügen Sie die SP Entity ID aus dem ExtraHop-System in das Zielgruppen-URI (SP-Entitäts-ID) Feld in Okta.
14. Aus dem **Namens-ID-Format** Dropdownliste, wählen **Hartnäckig**.
15. Aus dem **Nutzername der Anwendung** Wählen Sie in der Dropdownliste ein Benutzernamenformat aus.
16. In der Angaben zu Attributen Abschnitt, fügen Sie die folgenden Attribute hinzu.

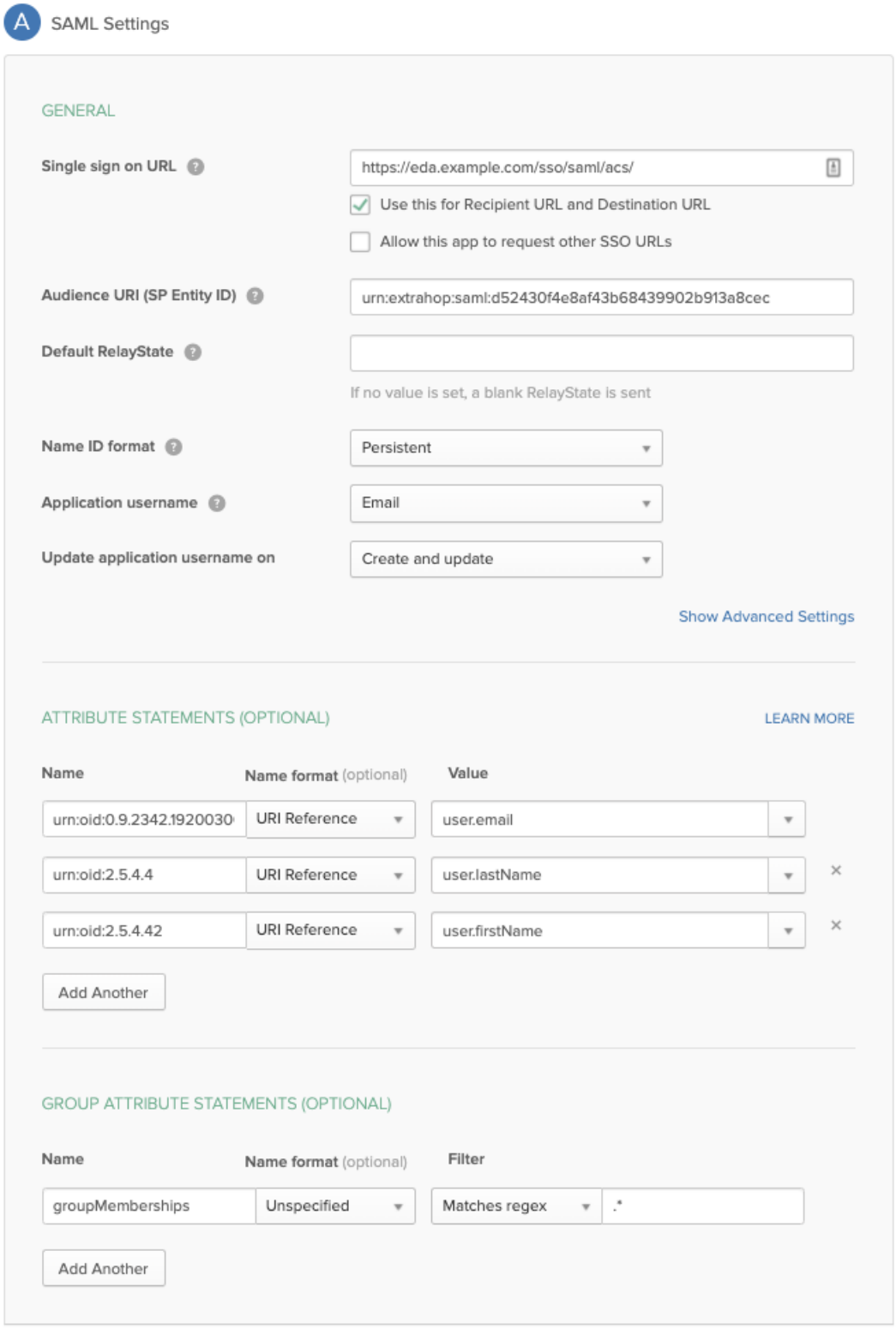
    Diese Attribute identifizieren den Benutzer im gesamten ExtraHop-System.

Name	Format des Namens	Wert
`urn:oid:0.9.2342.19200300.100.1.3`	URI-Referenz	Benutzer.E-Mail
`urn:oid:2.5.4.4`	URI-Referenz	Benutzer.Nachname
`urn:oid:2.5.4.42`	URI-Referenz	Benutzer.Vorname

17. In der Anweisung zu Gruppenattributen Abschnitt, in der Name Feld, geben Sie eine Zeichenfolge ein und konfigurieren Sie einen Filter.

    Sie geben den Namen des Gruppenattributs an, wenn Sie Benutzerberechtigungsattribute im ExtraHop-System konfigurieren.

    Die folgende Abbildung zeigt eine Beispielkonfiguration.



18. Klicken Sie **Weiter** und klicken Sie dann **Fertig**.
    Sie kehren zurück zum Einstellungen für die Anmeldung Seite.
19. In der Einstellungen Abschnitt, klicken Sie **Anweisungen zur Einrichtung anzeigen**.
    Ein neues Browserfenster wird geöffnet und zeigt Informationen an, die für die Konfiguration des ExtraHop-Systems erforderlich sind.

Weisen Sie das ExtraHop-System Okta-Gruppen zu

Wir gehen davon aus, dass Sie bereits Benutzer und Gruppen in Okta konfiguriert haben. Falls nicht, schlagen Sie in der Okta-Dokumentation nach, um neue Benutzer und Gruppen hinzuzufügen.

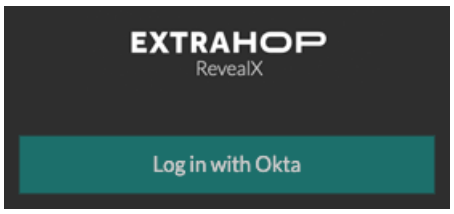
1. Wählen Sie im Menü Verzeichnis **Gruppen**.
2. Klicken Sie auf den Gruppennamen.
3. klicken **Apps verwalten**.
4. Suchen Sie den Namen der Anwendung, die Sie für das ExtraHop-System konfiguriert haben, und klicken Sie auf **Zuweisen**.
5. klicken **Erledigt**.

Fügen Sie Informationen zum Identitätsanbieter im ExtraHop-System hinzu

1. Kehren Sie zu den Administrationseinstellungen auf dem ExtraHop-System zurück.

   Schließen Sie das Service Provider-Metadatenfenster, falls es noch geöffnet ist, und klicken Sie dann auf **Identitätsanbieter hinzufügen**.
2. In der Name des Anbieters Feld, geben Sie einen eindeutigen Namen ein.

   Dieser Name erscheint auf der Anmeldeseite des ExtraHop-Systems.



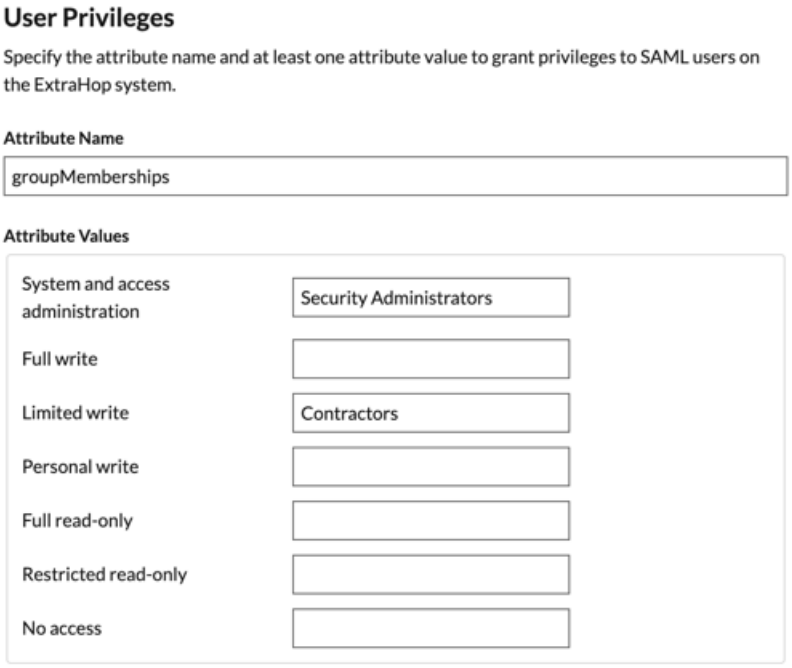
3. Kopieren Sie aus Okta das URL für einmaliges Anmelden des Identitätsanbieters und fügen Sie es in das SSO-URL-Feld auf dem ExtraHop-System ein.
4. Kopieren Sie aus Okta das URL des Ausstellers des Identitätsanbieters und füge es in das Entitäts-ID Feld auf dem ExtraHop-System.
5. Kopieren Sie das X.509-Zertifikat von Okta und fügen Sie es in das Öffentliches Zertifikat Feld auf dem ExtraHop-System.
6. Wählen Sie aus einer der folgenden Optionen aus, wie Sie Benutzer bereitstellen möchten.
   - Wählen Sie Benutzer automatisch bereitstellen, um ein neues Remote-SAML-Benutzerkonto auf dem ExtraHop-System zu erstellen, wenn sich der Benutzer zum ersten Mal anmeldet.
   - Deaktivieren Sie das Kontrollkästchen Benutzer automatisch bereitstellen und konfigurieren Sie neue Remote-Benutzer manuell über die ExtraHop-Administrationseinstellungen oder die REST-API. Zugriffs- und Berechtigungsstufen werden durch die Benutzerkonfiguration in Okta bestimmt.
7. 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.
8. Konfigurieren Sie Benutzerberechtigungsattribute.

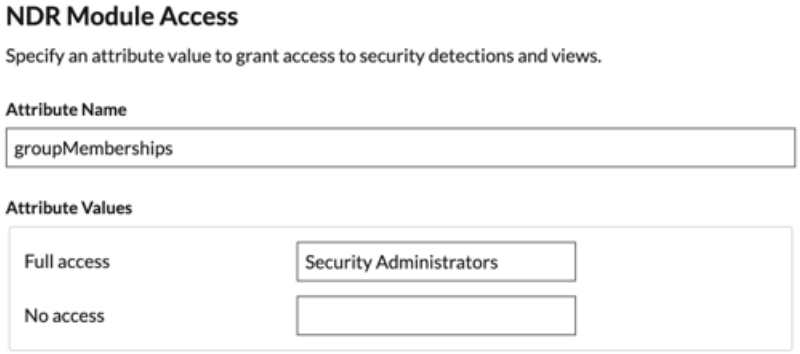
   Sie müssen die folgenden Benutzerattribute konfigurieren, bevor sich Benutzer über einen Identitätsanbieter beim ExtraHop-System anmelden können. Werte sind benutzerdefinierbar; sie müssen jedoch mit den Attributnamen übereinstimmen, die in der SAML-Antwort Ihres Identitätsanbieters enthalten sind. Bei 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.

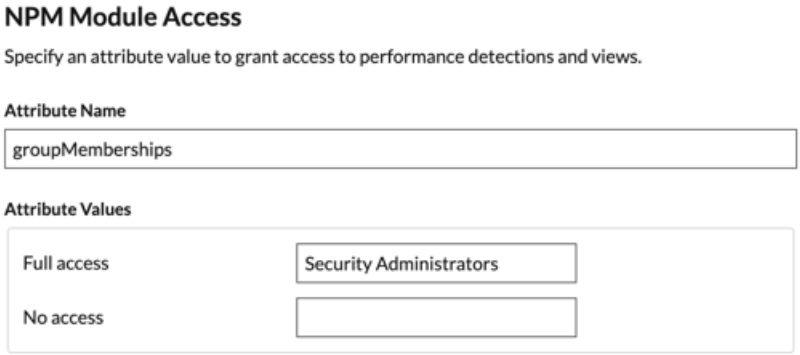
In den folgenden Beispielen ist Name des Attributs Feld ist das Gruppenattribut, das bei der Erstellung der ExtraHop-Anwendung auf dem Identity Provider konfiguriert wurde, und Attributwerte sind die Namen Ihrer Benutzergruppen. Wenn ein Benutzer Mitglied von mehr als einer Gruppe ist, wird ihm das Zugriffsrecht mit den meisten Berechtigungen gewährt.



9. Konfigurieren Sie den NDR-Modulzugriff.



10. Konfigurieren Sie den NPM-Modulzugriff.



11. Optional: Konfigurieren Sie den Zugriff auf Pakete und Sitzungsschlüssel.

Dieser Schritt ist optional und nur erforderlich, wenn Sie einen verbundenen Packetstore und das Packet Forensics Modul haben.

12. Klicken Sie **Speichern**.
13. Speichern Sie die laufende Konfigurationsdatei.

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.