Konfigurieren Sie die Fernauthentifizierung über SAML

Veröffentlicht: 2024-02-16

Sie können die sichere SSO-Authentifizierung (Single Sign-On) für das ExtraHop-System über einen oder mehrere SAML-Identitätsanbieter (Security Assertion Markup Language) konfigurieren.

Video: Sehen Sie sich die entsprechende Schulung an: SSO-Authentifizierung

Wenn sich ein Benutzer bei einem ExtraHop-System anmeldet, das als Service Provider (SP) für die SAML-SSO-Authentifizierung konfiguriert ist, fordert das ExtraHop-System die Autorisierung vom entsprechenden Identity Provider (IdP) an. Der Identitätsanbieter authentifiziert die Anmeldedaten des Benutzers und gibt dann die Autorisierung für den Benutzer an das ExtraHop-System zurück. Der Benutzer kann dann auf das ExtraHop-System zugreifen.

Konfigurationsleitfäden für bestimmte Identitätsanbieter sind unten verlinkt. Wenn Ihr Anbieter nicht aufgeführt ist, wenden Sie die vom ExtraHop-System erforderlichen Einstellungen auf Ihren Identitätsanbieter an.

Identitätsanbieter müssen die folgenden Kriterien erfüllen:

- SAML 2.0
- Unterstützt SP-initiierte Anmeldeabläufe. IDP-initiierte Anmeldeabläufe werden nicht unterstützt.
- Unterstützt signierte SAML-Antworten
- Unterstützt HTTP-Redirect-Binding

Die Beispielkonfiguration in diesem Verfahren ermöglicht den Zugriff auf das ExtraHop-System über Gruppenattribute.

Wenn Ihr Identitätsanbieter keine Gruppenattributanweisungen unterstützt, konfigurieren Sie Benutzerattribute mit den entsprechenden Rechten für Modulzugriff, Systemzugriff und Paketforensik.

SAML-Remoteauthentifizierung aktivieren

Warnung: Wenn Ihr System bereits mit einer Fernauthentifizierungsmethode konfiguriert ist, werden durch das Ändern dieser Einstellungen alle Benutzer und zugehörigen Anpassungen entfernt, die mit dieser Methode erstellt wurden, und Remotebenutzer können nicht auf das System zugreifen. Lokale Benutzer sind nicht betroffen.

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 **SAML** aus der Dropdownliste für die Methode der Fernauthentifizierung und klicken Sie dann auf **Weiter**.

- Klicken Sie **SP-Metadaten anzeigen** um die Assertion Consumer Service (ACS) -URL und die Entitäts-ID des ExtraHop-Systems anzuzeigen. Diese Zeichenfolgen werden von Ihrem Identitätsanbieter benötigt , um die SSO-Authentifizierung zu konfigurieren. Sie können auch eine vollständige XML-Metadatendatei herunterladen, die Sie in Ihre Identitätsanbieter-Konfiguration importieren können.

  Hinweis: Die ACS-URL enthält den in den Netzwerkeinstellungen konfigurierten Hostnamen. Wenn die ACS-URL einen nicht erreichbaren Hostnamen enthält, z. B. den Standardsystemhostnamen `extrahop`, müssen Sie die URL bearbeiten, wenn Sie die ACS-URL zu Ihrem Identitätsanbieter hinzufügen, und den vollqualifizierten Domänenname (FQDN) des ExtraHop-Systems angeben.
- Klicken Sie **Identitätsanbieter hinzufügen** um die folgenden Informationen hinzuzufügen:

• **Name des Anbieters:** Geben Sie einen Namen ein, um Ihren spezifischen Identitätsanbieter zu identifizieren. Dieser Name erscheint auf der Anmeldeseite des ExtraHop-Systems nach dem **Loggen Sie sich ein mit** Text.

• **Entitäts-ID:** Fügen Sie die von Ihrem Identitätsanbieter bereitgestellte Entitäts-ID in dieses Feld ein.

• **SSO-URL:** Fügen Sie die von Ihrem Identitätsanbieter bereitgestellte Single Sign-On-URL in dieses Feld ein.

• **Öffentliches Zertifikat:** Fügen Sie das von Ihrem Identitätsanbieter bereitgestellte X.509-Zertifikat in dieses Feld ein.

• **Automatisches Provisioning von Benutzern:** Wenn diese Option ausgewählt ist, werden ExtraHop-Benutzerkonten automatisch erstellt, wenn sich der Benutzer über den Identitätsanbieter anmeldet. Um manuell zu steuern, welche Benutzer sich anmelden können, deaktivieren Sie dieses Kontrollkästchen und konfigurieren Sie neue Remote-Benutzer manuell über die ExtraHop-Administrationseinstellungen oder die REST-API. Jeder manuell erstellte Remote-Benutzername sollte mit dem auf dem Identitätsanbieter konfigurierten Benutzernamen übereinstimmen.

• **Diesen Identitätsanbieter aktivieren:** Diese Option ist standardmäßig ausgewählt und ermöglicht es Benutzern, sich beim ExtraHop-System anzumelden. Um zu verhindern, dass sich Benutzer über diesen Identitätsanbieter anmelden, deaktivieren Sie das Kontrollkästchen.

• **Attribute von Benutzerrechten:** Sie müssen Benutzerberechtigungsattribute konfigurieren, bevor sich Benutzer über einen Identitätsanbieter beim ExtraHop-System anmelden können. Bei Werten wird nicht zwischen Groß- und Kleinschreibung unterschieden und sie können Leerzeichen enthalten.

Die Namen und Werte der Benutzerberechtigungsattribute müssen mit den Namen und Werten übereinstimmen, die Ihr Identitätsanbieter in SAML-Antworten einbezieht, die konfiguriert werden, wenn Sie die ExtraHop-Anwendung zu einem Anbieter hinzufügen. In Azure AD konfigurieren Sie beispielsweise Anspruchsnamen und Anspruchsbedingungswerte, die mit den Namen und Werten der Benutzerberechtigungsattribute im ExtraHop-System übereinstimmen müssen. Ausführlichere Beispiele finden Sie in den folgenden Themen:

- SAML-Single-Sign-On mit JumpCloud konfigurieren
- SAML-Single-Sign-On mit Google konfigurieren
- SAML-Single-Sign-On mit Okta konfigurieren
- SAML-Single-Sign-On mit Azure AD konfigurieren

Hinweis Wenn ein Benutzer mehreren Attributwerten entspricht, wird dem Benutzer das Zugriffsrecht mit der höchsten Zugriffsberechtigung gewährt. Wenn ein Benutzer beispielsweise den Werten Eingeschränktes Schreiben und Vollständiges Schreiben entspricht, erhält der Benutzer volle Schreibberechtigungen. Weitere Hinweise zu Berechtigungsstufen finden Sie unter Benutzer und Benutzergruppen.

• **Zugriff auf das NDR-Modul:** NDR-Attribute ermöglichen Benutzern den Zugriff auf NDR-Funktionen.

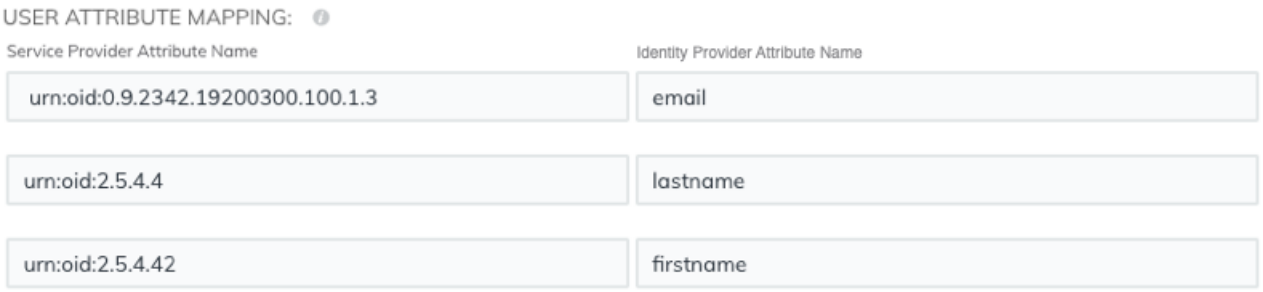
• **Zugriff auf das NPM-Modul:** NPM-Attribute ermöglichen Benutzern den Zugriff auf NPM-Funktionen.

• **Zugriff auf Pakete und Sitzungsschlüssel:** Pakete und Sitzungsschlüsselattribute ermöglichen Benutzern den Zugriff auf Pakete und Sitzungsschlüssel. Die Konfiguration von Paketen und Sitzungsschlüsselattributen ist optional und nur erforderlich, wenn Sie einen angeschlossenen ExtraHop-Paketstore haben.

Zuordnung von Benutzerattributen

Sie müssen den folgenden Satz von Benutzerattributen im Abschnitt zur Zuordnung von Anwendungsattributen auf Ihrem Identitätsanbieter konfigurieren. Diese Attribute identifizieren den Benutzer im gesamten ExtraHop-System. Die richtigen Eigenschaftsnamen beim Zuordnen von Attributen finden Sie in der Dokumentation Ihres Identitätsanbieters.

ExtraHop-Attributname	Freundlicher Name	Kategorie	Attributname des Identitätsanbieters
urn:oid:0.9.2342.19200300.100.1.3	mail	Standardattribut	Primäre E-Mail-Adresse
urn:oid:2.5.4.4	sn	Standardattribut	Nachname
urn:oid:2.5.4.42	Vorgegebener Name	Standardattribut	Vorname



Attributaussagen gruppieren

Das ExtraHop-System unterstützt Anweisungen zu Gruppenattributen, um Benutzerberechtigungen einfach allen Mitgliedern einer bestimmten Gruppe zuzuordnen. Wenn Sie die ExtraHop-Anwendung auf Ihrem Identitätsanbieter konfigurieren, geben Sie einen Gruppenattributnamen an. Dieser Name wird dann in das Feld Attributname eingegeben , wenn Sie den Identity Provider auf dem ExtraHop-System konfigurieren.

Wenn Ihr Identitätsanbieter keine Gruppenattributanweisungen unterstützt, konfigurieren Sie Benutzerattribute mit den entsprechenden Rechten für Modulzugriff, Systemzugriff und Paketforensik.

Nächste Schritte

- SAML-Single-Sign-On mit JumpCloud konfigurieren
- SAML-Single-Sign-On mit Google konfigurieren
- SAML-Single-Sign-On mit Okta konfigurieren