Konfigurieren Sie die Fernauthentifizierung über SAML

Veröffentlicht: 2025-02-12

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

Wichtig: Dieses Handbuch ist nur für RevealX Enterprise. Informationen zu RevealX 360 finden Sie unter Ermöglichen Sie die Sensorzugriffskontrolle über Ihren eigenen Identitätsanbieter.

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

Bevor Sie beginnen

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.

Sie können die Fernauthentifizierung mit SAML auf diesem 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** Drop-down-Menü, wählen **SAML**.
4. Klicken Sie **Weiter**.
5. klicken **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 nach unten scrollen, um die Metadaten als XML-Datei herunterzuladen , 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.

6. klicken **Identitätsanbieter hinzufügen**.
7. In der Name des Anbieters Feld, geben Sie einen Namen ein, um Ihren spezifischen Identitätsanbieter zu identifizieren.

   Dieser Name erscheint auf der Anmeldeseite des ExtraHop-Systems nach dem Text Anmelden mit Text.
8. In der Entitäts-ID Feld, fügen Sie die von Ihrem Identitätsanbieter bereitgestellte Entitäts-ID ein.
9. In der SSO-URL Fügen Sie in dieses Feld die von Ihrem Identitätsanbieter bereitgestellte Single Sign-On-URL ein.
10. In der Öffentliches Zertifikat Fügen Sie in dieses Feld das X.509-Zertifikat ein, das von Ihrem Identitätsanbieter bereitgestellt wurde.
11. Wählen Sie die **Automatische Bereitstellung von Benutzern** Kontrollkästchen, um anzugeben , dass ExtraHop-Benutzerkonten automatisch erstellt werden, 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.
12. Wählen Sie die **Diesen Identitätsanbieter aktivieren** Kontrollkästchen, um Benutzern die Anmeldung am ExtraHop-System zu ermöglichen.

    Dies ist standardmäßig aktiviert. Um zu verhindern, dass sich Benutzer über diesen Identitätsanbieter anmelden, deaktivieren Sie das Kontrollkästchen.
13. In der Attribute von Benutzerrechten Abschnitt, Konfiguration von Benutzerberechtigungsattributen.

    Dies muss abgeschlossen sein, 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 Microsoft Entra ID konfigurieren Sie beispielsweise Anspruchsnamen und Anspruchsbedingungswerte, die mit den Namen und Werten der Benutzerberechtigungsattribute im ExtraHop-System übereinstimmen müssen.

    Hinweis: Wenn ein Benutzer mehreren Attributwerten entspricht, wird dem Benutzer das Zugriffsrecht mit den meisten Berechtigungen 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.

    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 Microsoft Entra ID konfigurieren
14. In der Zugriff auf das NDR-Modul Abschnitt, Konfiguration von Attributen, um Benutzern den Zugriff auf NDR-Funktionen zu ermöglichen.

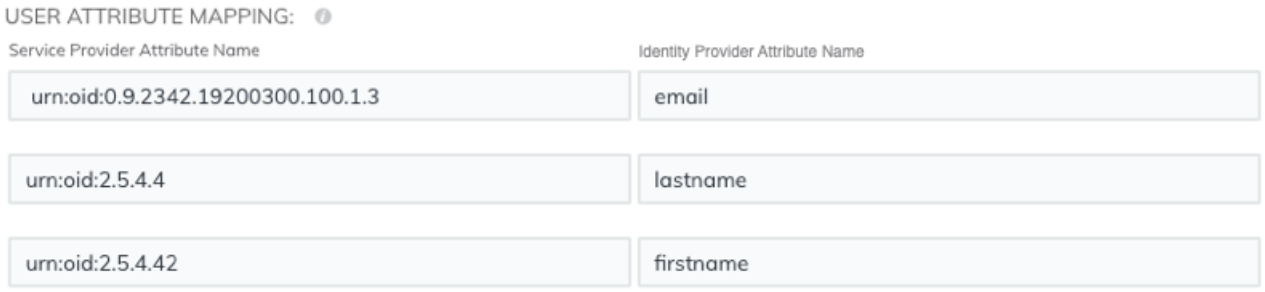
15. In der Zugriff auf das NPM-Modul Abschnitt, Konfigurieren Sie Attribute, um Benutzern den Zugriff auf NPM-Funktionen zu ermöglichen.
16. In der Zugriff auf Pakete und Sitzungsschlüssel Abschnitt, konfigurieren Sie Attribute, um Benutzern den Zugriff auf Pakete und Sitzungsschlüssel zu ermöglichen.

    Die Konfiguration von Paketen und Sitzungsschlüsselattributen ist optional und nur erforderlich , wenn Sie einen angeschlossenen ExtraHop-Paketstore haben.
17. Klicken Sie **Speichern**.

Zuordnung von Benutzerattributen

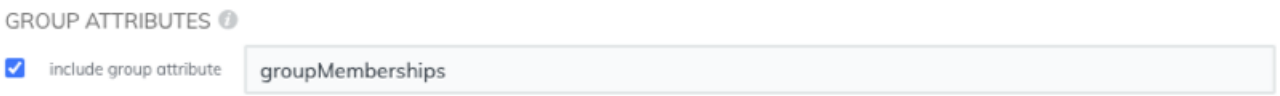
Sie müssen den folgenden Satz von Benutzerattributen im Abschnitt zur Zuordnung von Anwendungsattributen auf Ihrem Identitätsanbieter konfigurieren. Diese Attribute identifizieren den Benutzer im gesamten ExtraHop-System. Die richtigen Eigenschaftsnamen beim Zuordnen von Attributen finden Sie in der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

ExtraHop-Attributname	Freundlicher Name	Kategorie	Attributname des Identitätsanbieters
`urn:oid:0.9.2342.19200300.100.1.3`	`0.9.2342.19200300.100.1.3`	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 Name des Attributs Feld, 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.

Die nächsten Schritte

Nachdem Sie die Remote-Authentifizierung über SAML konfiguriert haben, überprüfen Sie diese Aufgaben.

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