SAML-Single-Sign-On mit Microsoft Entra ID konfigurieren

Veröffentlicht: 2025-02-04

Sie können Ihr ExtraHop-System so konfigurieren, dass sich Benutzer über den Microsoft Entra ID-Identitätsverwaltungsdienst am System anmelden können.

Bevor Sie beginnen

- Sie sollten mit der Verwaltung von Microsoft Entra ID vertraut sein.
- Sie sollten mit der Verwaltung von ExtraHop-Systemen vertraut sein.

Bei diesen Verfahren müssen Sie Informationen zwischen dem ExtraHop-System und Azure 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 im Dropdownmenü Methode der Fernauthentifizierung die Option **SAML**.
4. klicken **Fortfahren**.
5. klicken **SP-Metadaten anzeigen**. Sie müssen die URL und die Entitäts-ID des Assertion Consumer Service (ACS) kopieren, um sie in einem späteren Verfahren in die Azure-Konfiguration einzufügen.

Azure konfigurieren

In den folgenden Verfahren erstellen Sie eine Unternehmensanwendung, fügen der Anwendung Benutzer und Gruppen hinzu und konfigurieren Single-Sign-On-Einstellungen.

Erstellen Sie eine neue Anwendung

1. Loggen Sie sich in Ihr Microsoft Azure-Portal ein.
2. Klicken Sie im Abschnitt Azure-Dienste auf **Unternehmensanwendungen**.
3. Klicken Sie **Neue Anwendung**.
4. Klicken Sie **Erstellen Sie Ihre eigene Anwendung**.
5. Geben Sie einen Namen für Sensor im Namensfeld. Dieser Name wird für Ihre Benutzer auf der Azure-Seite „Meine Apps“ angezeigt.
6. Wählen **Integrieren Sie jede andere Anwendung, die Sie nicht in der Galerie finden**.
7. Klicken Sie **Erstellen**.

Die Seite mit der Anwendungsübersicht wird angezeigt.

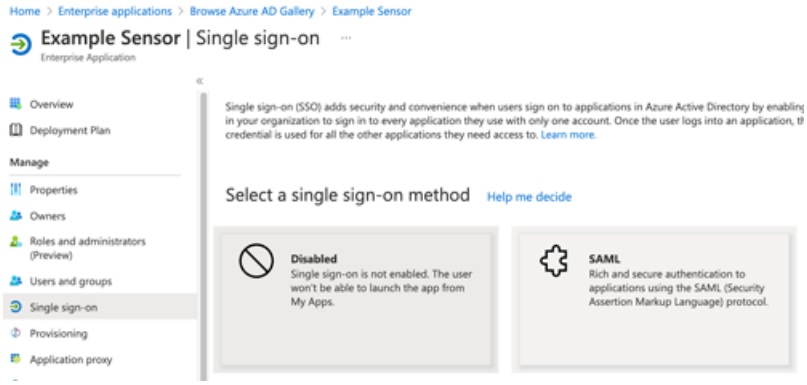
Benutzer und Gruppen hinzufügen

Sie müssen der neuen Anwendung Benutzer oder Gruppen zuweisen, bevor sich Benutzer am ExtraHop-System anmelden können.

1. Klicken Sie im linken Bereich auf **Benutzer und Gruppen**.
2. Klicken Sie **Benutzer/Gruppe hinzufügen**.
3. Fügen Sie Ihre privilegierten Benutzer oder Gruppen hinzu und klicken Sie dann auf **Zuweisen**.

Single Sign-On konfigurieren

1. Klicken Sie im linken Bereich auf **Einmaliges Anmelden**.
2. Klicken Sie **SAML**.



3. Klicken Sie im Abschnitt Basic SAML Configuration auf **Bearbeiten**.
4. Geben Sie die Entitäts-ID aus dem ExtraHop-System in das Feld Identifier (Entity ID) ein oder fügen Sie sie ein und wählen Sie die **Standard** Ankreuzfeld. Sie können das vorhandene löschen `http://adapplicationregistry.onmicrosoft.com/customappsso/primary` Eintrag.
5. Geben Sie die ACS-URL aus dem ExtraHop-System ein oder fügen Sie sie in das **Antwort-URL (Assertion Consumer Service-URL)** Feld.
6. Klicken Sie **Speichern**.
7. Klicken Sie im Abschnitt SAML-Zertifikate auf **Bearbeiten**.
8. In der **Option zum Signieren** Drop-down-Menü, wählen **SAML-Antwort und -Assertion signieren**
9. Klicken Sie im Abschnitt Attribute und Ansprüche auf **Bearbeiten**.
10. Klicken Sie im Abschnitt „Erforderlicher Antrag“ auf **Eindeutige Benutzerkennung (Namen-ID)**.
11. Klicken Sie **Wählen Sie das Format der Namenskennung**.
12. Wählen Sie aus dem Drop-down-Menü **Hartnäckig**.
13. Klicken Sie **Speichern**.
14. Löschen Sie das erforderliche **Benutzer.mail** Anspruch und alle zusätzlichen Ansprüche.
15. Fügen Sie die folgenden Anspruchsnamen hinzu:

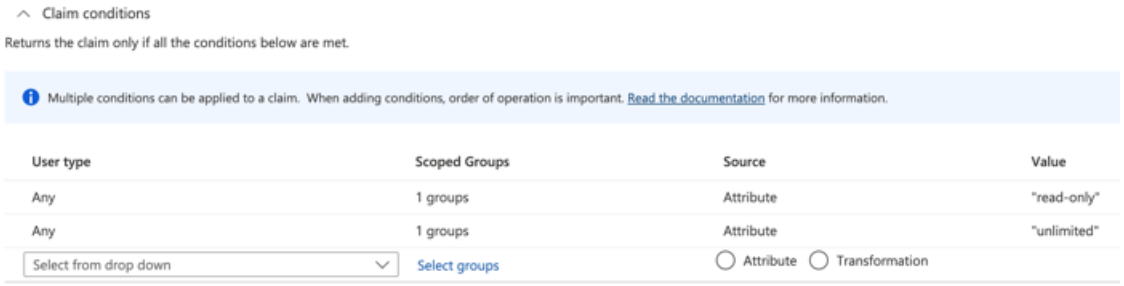
Name des Antrags	Wert
`urn:oid:2.5.4.4`	Benutzer.Familienname
`urn:oid:2.5.4.42`	user.givenname
`urn:oid:0.9.2342.19200300.100.1.3`	user.userprincipalname

16. Klicken Sie **Neuen Anspruch hinzufügen**. Dieser Anspruch ermöglicht Benutzern den Zugriff auf das ExtraHop-System mit den zugewiesenen Rechten.
    a) Typ `Level schreiben` im Feld Name. Sie können einen beliebigen Namen eingeben, er muss jedoch mit dem Namen übereinstimmen, den Sie auf dem ExtraHop-System konfigurieren.
    b) Klicken Sie **Bedingungen für Reklamationen**.

    Wichtig: Die Reihenfolge, in der Sie die Bedingungen hinzufügen, ist wichtig. Wenn ein Benutzer mehrere Anspruchsbedingungen erfüllt, werden ihm die Rechte zugewiesen, die zuletzt erfüllt wurden. Wenn Sie beispielsweise hinzufügen `illimitiert` als erster Wert und `nur lesbar` Wenn der zweite Wert angegeben ist und der Benutzer beide Anspruchsbedingungen erfüllt, wird dem Benutzer die Leseberechtigung zugewiesen.

    c) Aus dem **Benutzertyp** Drop-down-Menü, wählen **Irgendein**.

d) Unter **Gruppen mit Geltungsbereich**, klicken **Gruppen auswählen**, klicken Sie auf den Namen der Gruppe, die Sie hinzufügen möchten, und klicken Sie dann auf **Wählen**.
e) Unter **Quelle**, wählen **Attribut**.
f) In der **Wert** Feld, Typ `illimitiert` oder einen Namen Ihrer Wahl, der das Privileg für diese Gruppe definiert. Wiederholen Sie diesen Schritt für jede Gruppe, der Sie eindeutige Rechte zuweisen möchten. Im folgenden Beispiel haben wir eine Anspruchsbedingung für zwei Gruppen erstellt. Einer Gruppe werden nur Leserechte zugewiesen, und der anderen Gruppe werden System- und Zugriffsadministrationsrechte zugewiesen.



g) Klicken Sie **Speichern**.

17. Kehren Sie zur Seite „Attribute und Ansprüche“ zurück und klicken Sie auf **Neuen Anspruch hinzufügen**. Dieser Anspruch weist den Zugriff auf Pakete und Sitzungsschlüssel zu.
    a) Typ `Paketebene` im Feld Name. Sie können einen beliebigen Namen eingeben, er muss jedoch mit dem Namen übereinstimmen, den Sie auf dem ExtraHop-System konfigurieren.
    b) Klicken Sie **Bedingungen für Reklamationen**.
    c) Aus dem **Benutzertyp** Drop-down-Menü, wählen **Irgendein**.
    d) Klicken Sie unter Bereichsgruppen auf **Gruppen auswählen**, klicken Sie auf den Namen der Gruppe, die Sie hinzufügen möchten, und klicken Sie dann auf **Wählen**.
    e) Wählen Sie unter Quelle **Attribut**.
    f) Geben Sie im Feld Wert Folgendes ein `nur Pakete` oder einen Namen Ihrer Wahl, der das Privileg für diese Gruppe definiert.
    g) Klicken Sie **Speichern**.
18. Kehren Sie zur Seite „Attribute und Ansprüche“ zurück und klicken Sie auf **Neuen Anspruch hinzufügen**. Dieser Anspruch weist Erkennungen Zugriff zu.
    a) Typ `Erkennungsstufe` im Feld Name. Sie können einen beliebigen Namen eingeben, er muss jedoch mit dem Namen übereinstimmen, den Sie auf dem ExtraHop-System konfigurieren.
    b) Klicken Sie **Bedingungen für Reklamationen**.
    c) Aus dem **Benutzertyp** Drop-down-Menü, wählen **Irgendein**.
    d) Klicken Sie unter Bereichsgruppen auf **Gruppen auswählen**, klicken Sie auf den Namen der Gruppe, die Sie hinzufügen möchten, und klicken Sie dann auf **Wählen**.
    e) Wählen Sie unter Quelle **Attribut**.
    f) Geben Sie im Feld Wert Folgendes ein `voll` oder einen Namen Ihrer Wahl , der das Privileg für diese Gruppe definiert.
    g) klicken **Speichern**.

Fügen Sie dem ExtraHop-System Informationen zum Identitätsanbieter hinzu

1. Klicken Sie im Abschnitt Azure SAML-Signaturzertifikat neben Zertifikat (Base64) auf Herunterladen.

   Hinweis: Laden Sie für RevealX 360-Systeme die Federation-Metadaten-XML-Datei herunter.

2. Öffnen Sie die heruntergeladene Datei in einem Texteditor und kopieren Sie dann den Inhalt der Datei und fügen Sie ihn in das Feld Öffentliches Zertifikat auf dem ExtraHop-System ein.

3. Kopieren Sie in Azure die Anmelde-URL und fügen Sie sie in das SSO-URL-Feld auf dem ExtraHop-System ein.
4. Kopieren Sie in Azure den Microsoft Entra ID Identifier und fügen Sie ihn in das Feld Entity ID auf dem ExtraHop-System ein.
5. Wählen Sie im ExtraHop-System aus einer der folgenden Optionen aus, wie Sie Benutzer bereitstellen möchten.

   - Wählen **Automatisches Provisioning von Benutzern** um ein neues Remote-SAML-Benutzerkonto auf dem ExtraHop-System zu erstellen, wenn sich der Benutzer zum ersten Mal am System anmeldet.
   - Deaktivieren Sie das Kontrollkästchen Benutzer automatisch bereitstellen, um neue Remote-Benutzer manuell über die ExtraHop-Administrationseinstellungen oder die REST-API zu konfigurieren.

   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. Diese Einstellung erscheint nicht auf RevealX 360 .
6. Konfigurieren Sie Benutzerberechtigungsattribute. Sie müssen die folgenden Benutzerattribute konfigurieren, bevor sich Benutzer über einen Identitätsanbieter beim ExtraHop-System anmelden können. Diese 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 als Kein Zugriff konfigurieren, bevor sich Benutzer anmelden können.

   Im folgenden Beispiel ist das Feld Attributname der Anspruchsname, der bei der Erstellung der ExtraHop-Anwendung in Azure angegeben wurde, und die anderen Attributwerte sind die Anspruchsbedingungswerte.

Feldname	Beispiel für einen Attributwert
Name des Attributs	`Level schreiben`
System- und Zugriffsverwaltung	`illimitiert`
Volle Schreibrechte	`voll_schreiben`
Eingeschränkte Schreibrechte	`begrenztes_schreiben`
Persönliche Schreibrechte	`persönliches_schreiben`
Volle Nur-Lese-Rechte	`voll_schreibgeschützt`
Eingeschränkte Leserechte	`restricted_readonly`
Kein Zugriff	`keine`

7. Konfigurieren Sie den NDR-Modulzugriff.

Feldname	Beispiel für einen Attributwert
Name des Attributs	`ndr-Niveau`
Voller Zugriff	`voll`
Kein Zugriff	`keine`

8. Konfigurieren Sie den NPM-Modulzugriff.

Feldname	Beispiel für einen Attributwert
Name des Attributs	`npm-Ebene`
Voller Zugriff	`voll`
Kein Zugriff	`keine`

9. Optional: Konfigurieren Sie den Zugriff auf Pakete und Sitzungsschlüssel. Dieser Schritt ist optional und nur erforderlich, wenn Sie einen verbundenen Packetstore haben.

   Hinweis: Wenn Sie keinen Packetstore haben, geben Sie NA in das Feld Attributname ein und lassen Sie die Felder für Attributwerte leer.

Feldname	Beispiel für einen Attributwert
Name des Attributs	`Paketebene`
Pakete und Sitzungsschlüssel	`voll_mit_Schlüsseln`
Nur Pakete	`voll`
Nur Paketsegmente	`Scheiben`
Nur Paket-Header	`Kopfzeilen`
Kein Zugriff	`keine`

10. Klicken Sie **Speichern**.
11. Speichern Sie die Konfiguration ausführen.

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. Wenn die Multi-Faktor-Authentifizierung (MFA) konfiguriert ist, folgen Sie den Anweisungen zur Einrichtung Ihrer MFA-App.