SAML-Single-Sign-On mit Azure AD konfigurieren

Veröffentlicht: 2023-09-30

Sie können Ihr ExtraHop-System so konfigurieren, dass sich Benutzer über den Azure AD-Identitätsverwaltungsdienst am System anmelden können.

Bevor Sie beginnen

- Sie sollten mit der Verwaltung von Azure AD 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 parallel 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 in der Dropdownliste Remoteauthentifizierungsmethode die Option **SAML**.
4. klicken **Weiter**.
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. Melden Sie sich bei Ihrem Microsoft Azure-Portal an.
2. Klicken Sie im Bereich Azure-Dienste auf **Unternehmensanwendungen**.
3. klicken **Neue Anwendung**.
4. klicken **Erstellen Sie Ihre eigene Anwendung**.
5. Geben Sie einen Namen für den Sensor im Namensfeld. Dieser Name wird für Ihre Benutzer auf der Azure My Apps-Seite angezeigt.
6. Wählen **Integrieren Sie jede andere Anwendung, die Sie nicht in der Galerie finden**.
7. klicken **Erstellen**.

Die Seite mit der Anwendungsübersicht wird angezeigt.

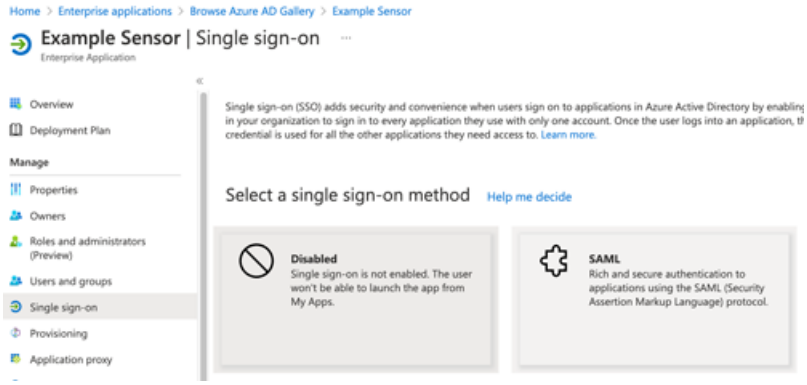
Benutzer und Gruppen hinzufügen

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 **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 **SAML**.



3. Klicken Sie im Abschnitt Basic SAML Configuration auf **Bearbeiten**.
4. Geben oder fügen Sie die Entitäts-ID aus dem ExtraHop-System in das Feld Identifier (Entity ID) ein und wählen Sie die **Standard** Checkbox. Sie können die vorhandenen 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 **Speichern**.
7. Klicken Sie im Abschnitt Attribute und Ansprüche auf **Bearbeiten**.
8. Klicken Sie im Bereich „Erforderlicher Antrag“ auf **Eindeutige Benutzerkennung (Name-ID)**.
9. klicken **Wählen Sie das Format für die Namenskennung**.
10. Wählen Sie in der Drop-down-Liste **Hartnäckig**.
11. klicken **Speichern**.
12. Löschen Sie im Abschnitt Zusätzliche Ansprüche den **benutzer.mail** fordern Sie einen Antrag aus der Liste an und ersetzen Sie die standardmäßigen Anspruchsnamen durch die folgenden Anspruchsnamen:

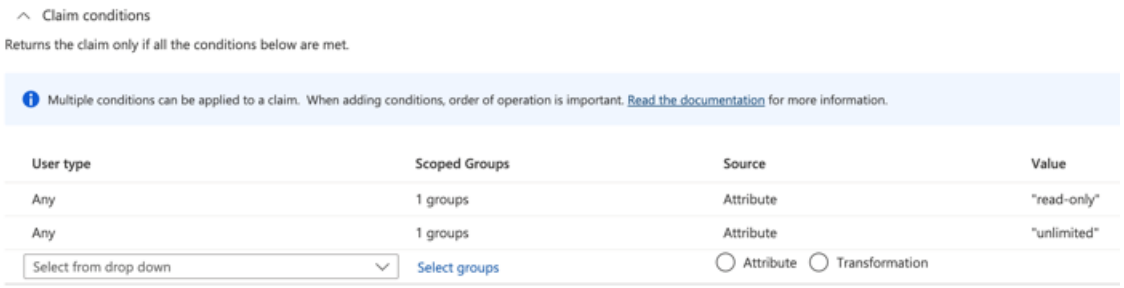
Name des Antrags	Wert
`urn: oid: 2.5.4.4`	user.name
`urn: oid: 2.5.4.42`	user.givenname
`urn:oid:0.9.2342.19200300.100.1.3`	user.userprinzipalname

13. klicken **Neuen Anspruch hinzufügen**. Dieser Anspruch ermöglicht es Benutzern, mit den zugewiesenen Rechten auf das ExtraHop-System zuzugreifen.
    a) Typ `Ebene schreiben` im Feld Name. Sie können einen beliebigen Namen eingeben, er muss jedoch mit dem Namen übereinstimmen, den Sie auf dem ExtraHop-System konfigurieren werden.
    b) klicken **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 zutreffen. Zum Beispiel, wenn Sie hinzufügen `illimitiert` als erster Wert und `nur lesbar` Wenn der zweite Wert angegeben ist und der Benutzer beide Anspruchsbedingungen erfüllt, wird dem Benutzer das Nur-Lese-Recht zugewiesen.

    c) Aus dem **Benutzertyp** Drop-down-Liste, 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 ein Name Ihrer Wahl, der das Recht für diese Gruppe definiert. Wiederholen Sie diesen Schritt für jede Gruppe, der Sie individuelle 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 **Speichern**.

14. Kehren Sie zur Seite Attribute und Ansprüche zurück und klicken Sie auf **Neuen Anspruch hinzufügen**. Dieser Anspruch weist Paketen und Sitzungsschlüsseln Zugriff 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 werden.
    b) klicken **Bedingungen für Reklamationen**.
    c) Aus dem **Benutzertyp** Drop-down-Liste, 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 in das Feld Wert ein `nur Pakete` oder ein Name Ihrer Wahl, der das Recht für diese Gruppe definiert.
    g) klicken **Speichern**.
15. Kehren Sie zur Seite Attribute und Ansprüche zurück und klicken Sie auf **Neuen Anspruch hinzufügen**. Dieser Anspruch weist Erkennungen den 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 werden.
    b) klicken **Bedingungen für Reklamationen**.
    c) Aus dem **Benutzertyp** Drop-down-Liste, 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 in das Feld Wert ein `voll` oder ein Name Ihrer Wahl , der das Recht für diese Gruppe definiert.
    g) klicken **Speichern**.

Fügen Sie dem ExtraHop-System Informationen zum Identitätsanbieter hinzu

1. Klicken Sie im Abschnitt Azure SAML Signing Certificate neben Certificate (Base64) auf Herunterladen.

   Hinweis: Laden Sie für Reveal (x) 360-Systeme die Federation Metadata 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.

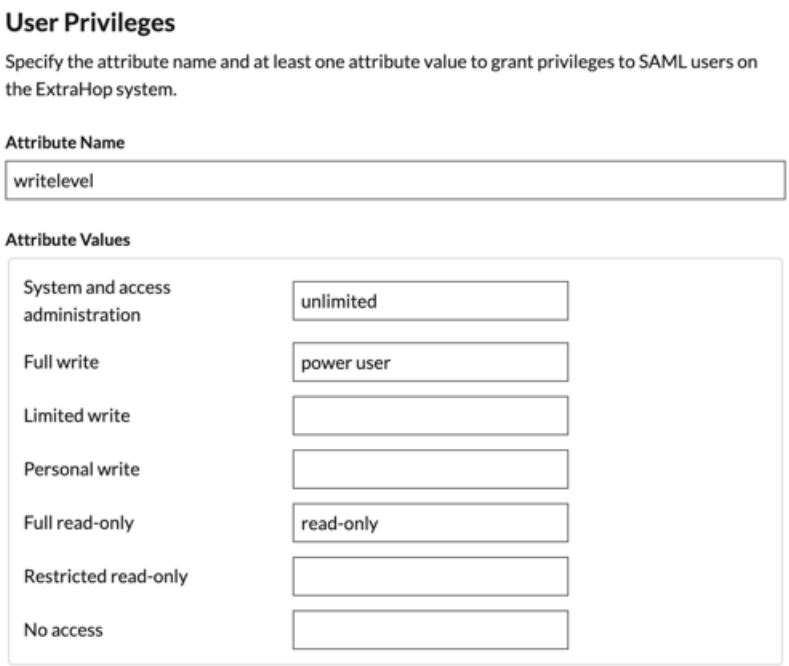
4. Kopieren Sie in Azure den Azure AD Identifier und fügen Sie ihn in das Feld Entity ID auf dem ExtraHop-System ein.
5. Wählen Sie auf dem ExtraHop-System aus einer der folgenden Optionen aus, wie Sie Benutzer bereitstellen möchten.

   - Wählen **Automatische Bereitstellung von Benutzern** um ein neues Remote-SAML-Benutzerkonto auf dem ExtraHop-System zu erstellen, wenn sich der Benutzer zum ersten Mal 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.

   Die **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 wird auf Reveal (x) 360 nicht angezeigt.
6. Konfigurieren Sie Benutzerberechtigungsattribute. Sie müssen den folgenden Satz von Benutzerattributen konfigurieren, bevor sich Benutzer über einen Identitätsanbieter beim ExtraHop-System anmelden können. Diese Werte sind benutzerdefiniert, müssen jedoch mit den Attributnamen übereinstimmen, die in der SAML-Antwort Ihres Identity Providers enthalten sind. Bei Werten wird nicht zwischen Groß- und Kleinschreibung unterschieden und sie können Leerzeichen enthalten. Weitere Informationen zu Berechtigungsstufen finden Sie unter Benutzer und Benutzergruppen.

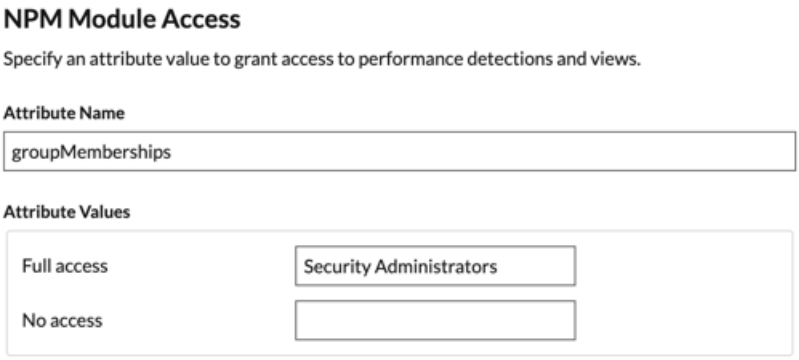
   Wichtig: Sie müssen den Attributnamen angeben und mindestens einen anderen Attributwert als Kein Zugriff konfigurieren, bevor sich Benutzer anmelden können.

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



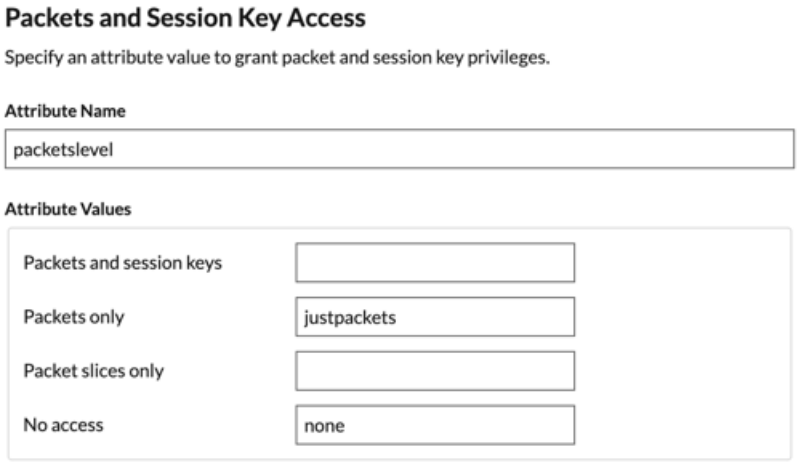
7. Konfigurieren Sie den Zugriff auf das NDR-Modul.

8. Konfigurieren Sie den NPM-Modulzugriff.



9. Optional: Konfigurieren Sie Pakete und den Zugriff auf 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 Attributwerte leer.



10. klicken **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.