Konfigurieren der externen SAML SSO-Authentifizierung mit AD FS für die ESA und SMA

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie die Active Directory-Verbunddienste als SAML-Identitätsanbieter für die externe Authentifizierung auf der Cisco ESA und SMA konfiguriert werden.

Voraussetzungen

Dieses Dokument bietet eine Ansicht der Drittanbieteranwendung, die Techniker sonst nicht sehen können.

- Konfigurationsschritte für die externe SAML-Authentifizierung (Security Assertion Markup Language) mit den Active Directory Federation Services (AD FS) 2012 und 2016 für die neuesten Versionen der Cisco Email Security Appliance (ESA) und Security Management Appliance (SMA).
- Grundlegende, laborbasierte Schritte, die keine speziellen bereitstellungsspezifischen Konfigurationen enthalten.

- Ein Arbeitsbeispiel aus einer Laborumgebung, das sich von einer Produktionsbereitstellung unterscheiden kann.

⚠ Vorsicht: Schließen Sie vor diesem Verfahren die Konfiguration des Service Providers (SP) ab. Siehe .

Anforderungen

- Microsoft Active Directory Federation Services (AD FS) 2012 oder 2016
- Cisco Email Security Appliance (ESA) und Security Management Appliance (SMA) aktuelle Version

Verwendete Komponenten

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

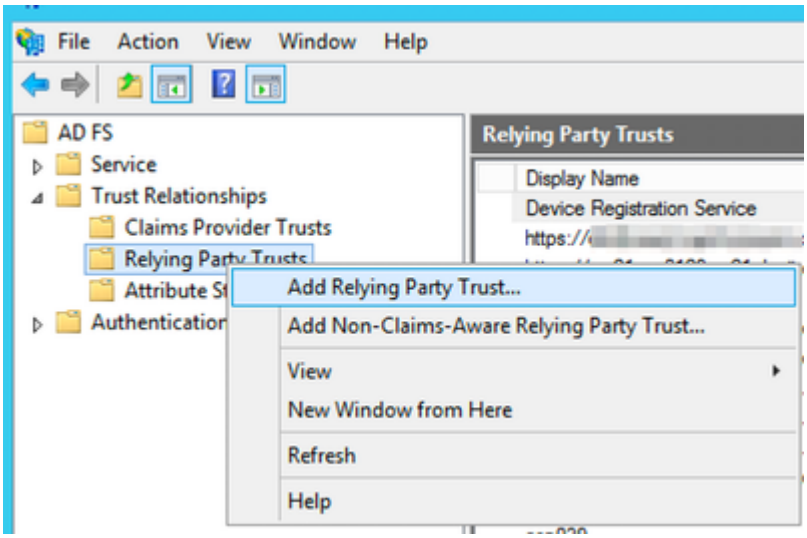
Schritte für die ADFS-IDP-Konfiguration für SAML

Vertrauenswürdigkeit der vertrauenden Seite konfigurieren

Verwenden Sie eine von zwei Optionen, um die Vertrauensstellung der vertrauenden Partei in AD FS zu erstellen.

Methode A: Erstellen der Vertrauensstellung der vertrauenden Partei durch Importieren von SP-Metadaten

1. Öffnen Sie die AD FS-Verwaltungskonsole über die Verwaltungs-Tools.
2. Erweitern Sie in der AD FS-Verwaltungskonsole die Option Vertrauenswürdige Beziehungen, klicken Sie mit der rechten Maustaste auf Vertrauenswürdige Partei, und wählen Sie dann Vertrauenswürdige Partei hinzufügen aus.



Vertrauenswürdigkeit von vertrauenden Parteien hinzufügen

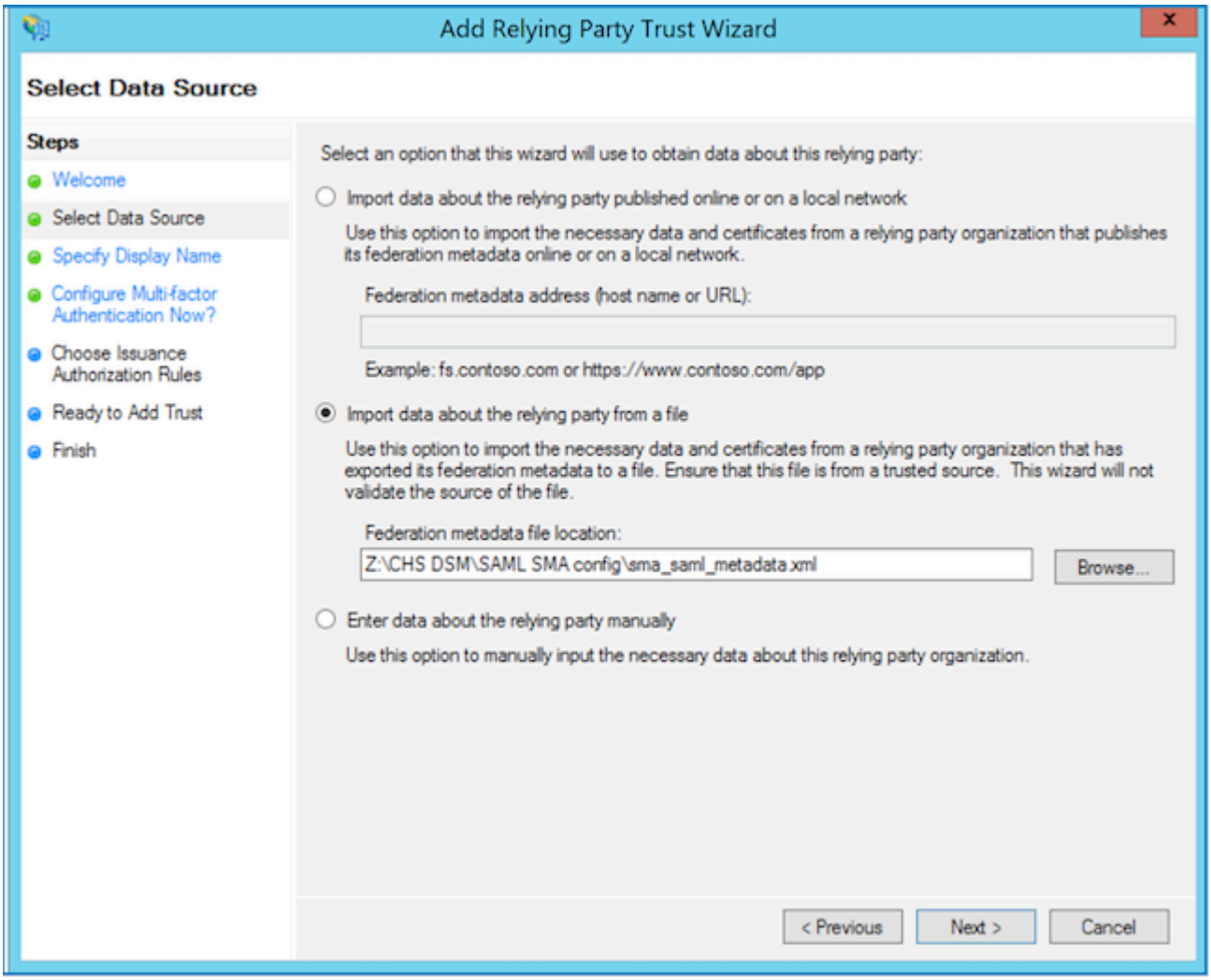
Tipp: Vertrauenswürdige Parteien von Microsoft

Fahren Sie mit einer von zwei Optionen fort:

- Option A: Daten über die vertrauende Partei aus einer Datei importieren. Laden Sie die Datei metadaten.xml des ESA- oder SMA-Dienstanbieters (SP) hoch.
- Option B: Geben Sie Daten über die vertrauende Seite manuell ein. Diese Option führt Sie durch die manuelle Konfiguration.

Option A: Daten über die vertrauende Partei aus einer Datei importieren. Laden Sie die Datei metadaten.xml des ESA- oder SMA-Dienstanbieters (SP) hoch.

1. Wählen Sie die Option zum Importieren von Daten über die vertrauende Partei aus einer Datei aus, und wählen Sie dann Weiter aus.



ESA/SMA-Metadatendatei importieren

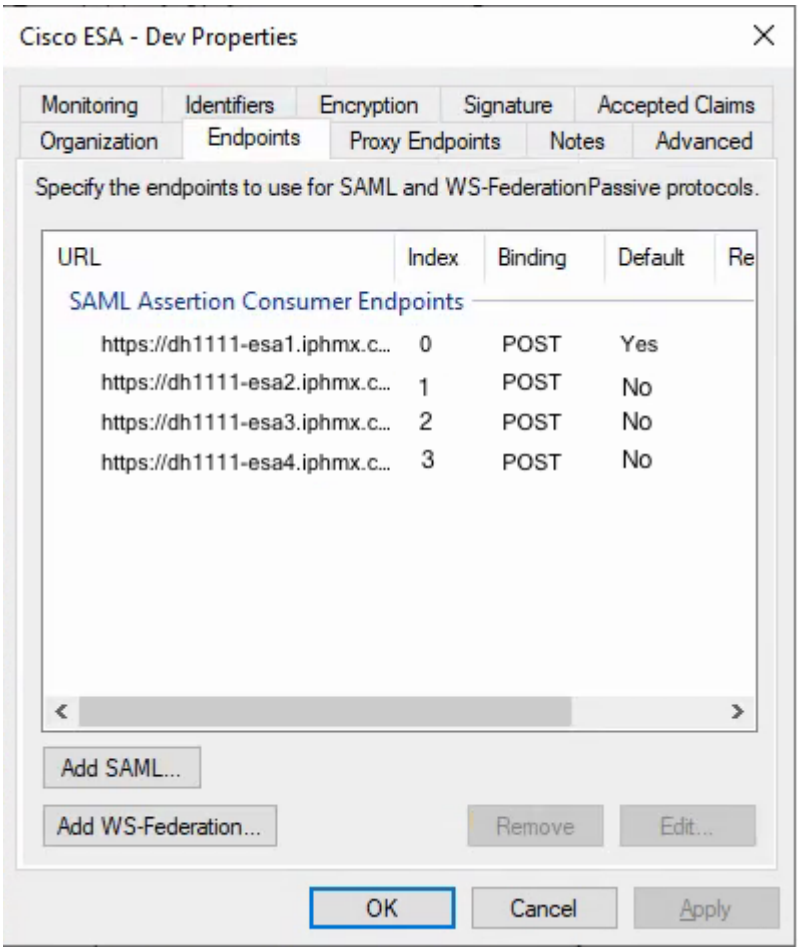
- Geben Sie einen Anzeigenamen an, um diese Vertrauensstellung der vertrauenden Seite zu identifizieren, und wählen Sie dann zweimal Weiter aus.
- Wählen Sie für Autorisierungsregeln die Option Alle Benutzer zulassen und dann Weiter aus.
- Akzeptieren Sie auf der Seite Bereit für das Hinzufügen von Vertrauenswürdigkeit die Standardeinstellungen, und wählen Sie dann Weiter aus.
- Wählen Sie Beenden. Daraufhin wird der Dialog Anspruchsregeln bearbeiten für die Vertrauensstellung der vertrauenden Seite geöffnet, der unter Issuance Transform Rules - Claims (Ausstellungstransformationsregeln - Ansprüche) behandelt wird.

Vertrauenswürdige Eigenschaften von vertrauenden Parteien - Endgeräte

Führen Sie diesen Schritt nur aus, wenn mehrere ESAs in einem Cluster vorhanden sind.

1. Öffnen Sie Vertrauenswürdige Eigenschaften der vertrauenden Partei > Endpunkte.
2. Fügen Sie jede für die ESA erreichbare URL-Adresse hinzu, und wählen Sie dann OK aus.
3. Die Indexwerte zählen von 0, d. h. 0, 1, 2 und 3.
4. Setzen Sie nur einen Eintrag auf Default = Yes.

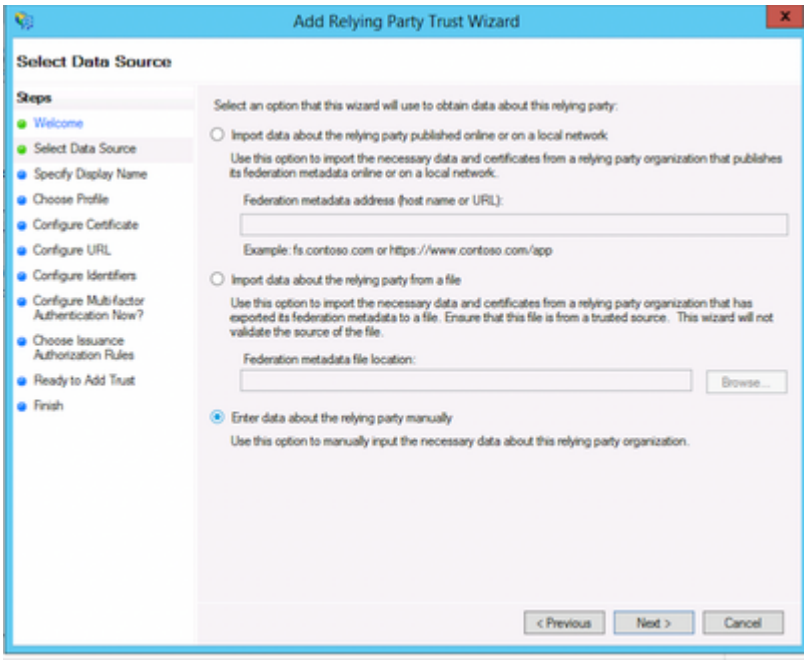
5. Setzen Sie die übrigen Einträge auf Default = No.



Vertrauenswürdige Eigenschaften von vertrauenden Parteien - Endgeräte

Option B: Geben Sie Daten über die vertrauende Seite manuell ein. Diese Option führt Sie durch die manuelle Konfiguration.

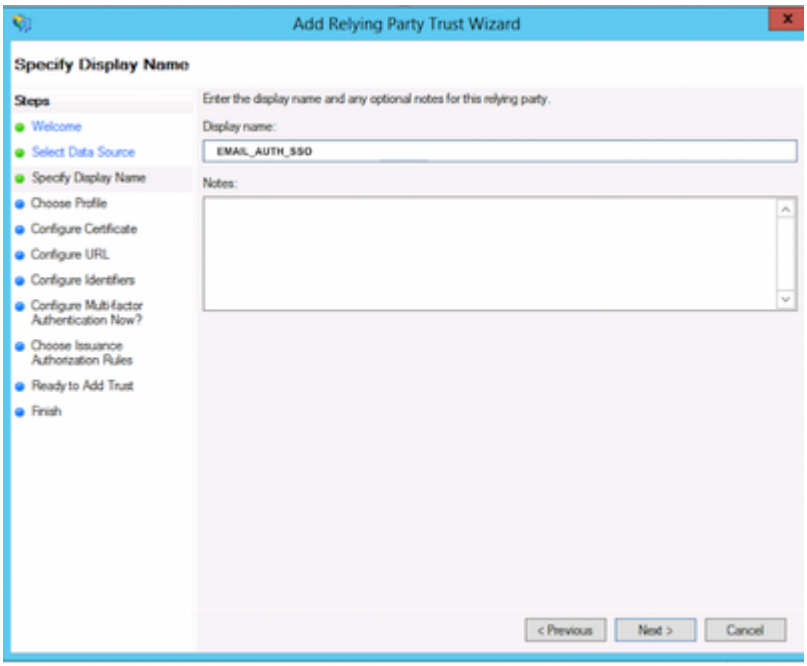
1. Wählen Sie Daten über die vertrauende Seite manuell eingeben aus.



Vertrauende Partei manuell hinzufügen

Tipp: Der Anzeigename ist der Name, unter dem Sie die Vertrauensstellung der vertrauenden Seite für die ESA oder SMA SAML identifizieren.

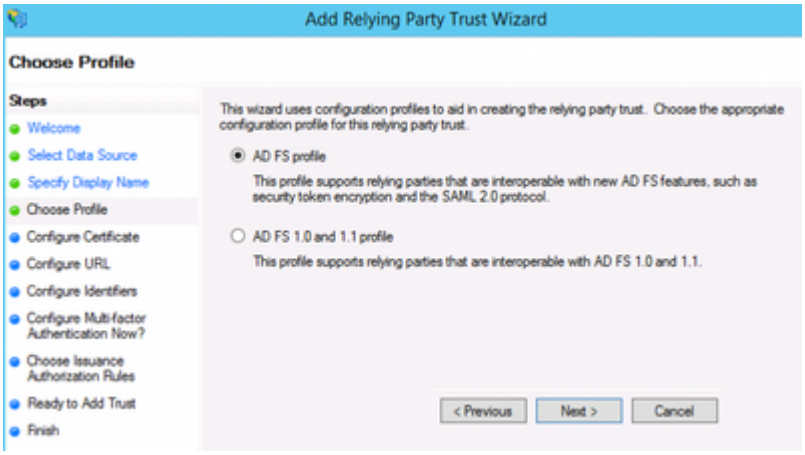
1. Geben Sie einen Anzeigenamen für den Service Provider ein, z. B. ESA_SP.



Erstellen eines Namens für das Service Provider-Profil

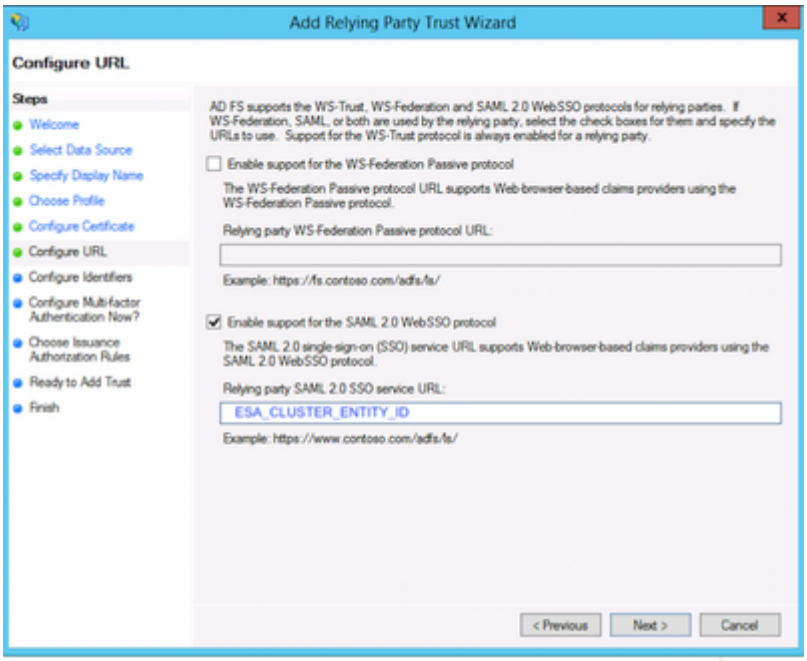
Tipp: [Rolle der Forderungsregeln und Ausstellungsregeln]

1. Wählen Sie die Profiloption AD FS-Profil.



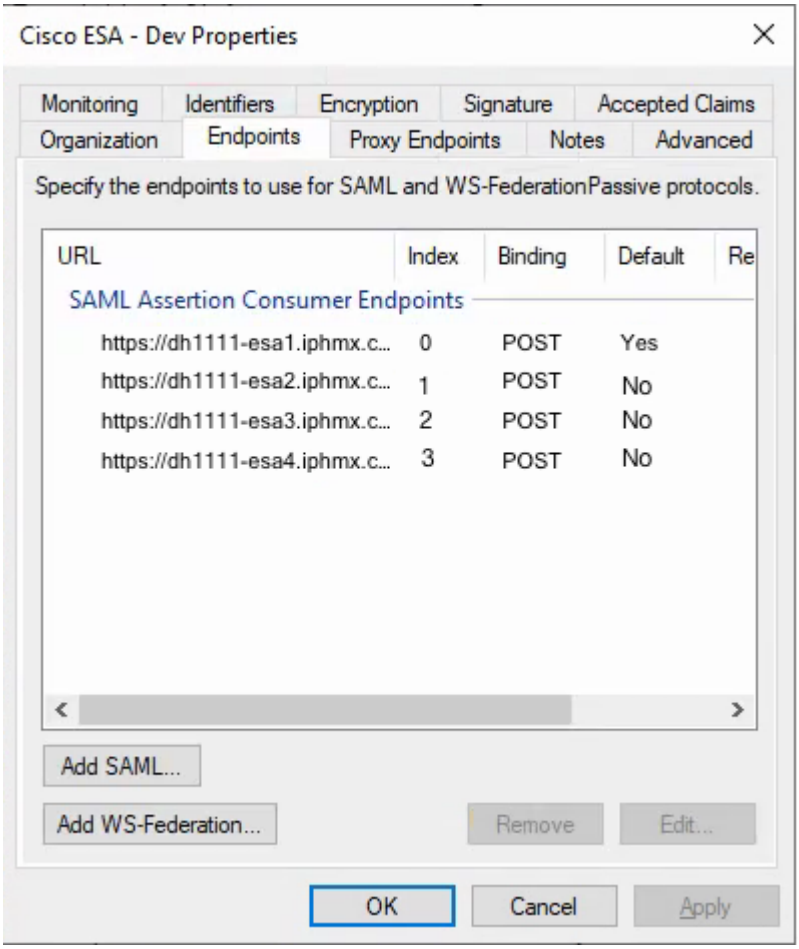
AD FS-Profiloption zur Verwendung von SAML 2.0

1. Laden Sie das öffentliche Zertifikat aus der Konfiguration des ESA-Dienstanbieters (SP).
2. Wählen Sie für Configure URL Enable support for the SAML 2.0 single-sign-on (SSO) aus.
3. Geben Sie die SAML 2.0 SSO-Service-URL der vertrauenden Partei mit dem Entitäts-ID-Wert des SP-Profils ein.



Autorisierungsregeln für die Ausstellung - -Alle Benutzer zulassen

1. Wählen Sie für die Autorisierungsregeln die Option Allen Benutzern den Zugriff auf diese vertrauende Seite erlauben aus.



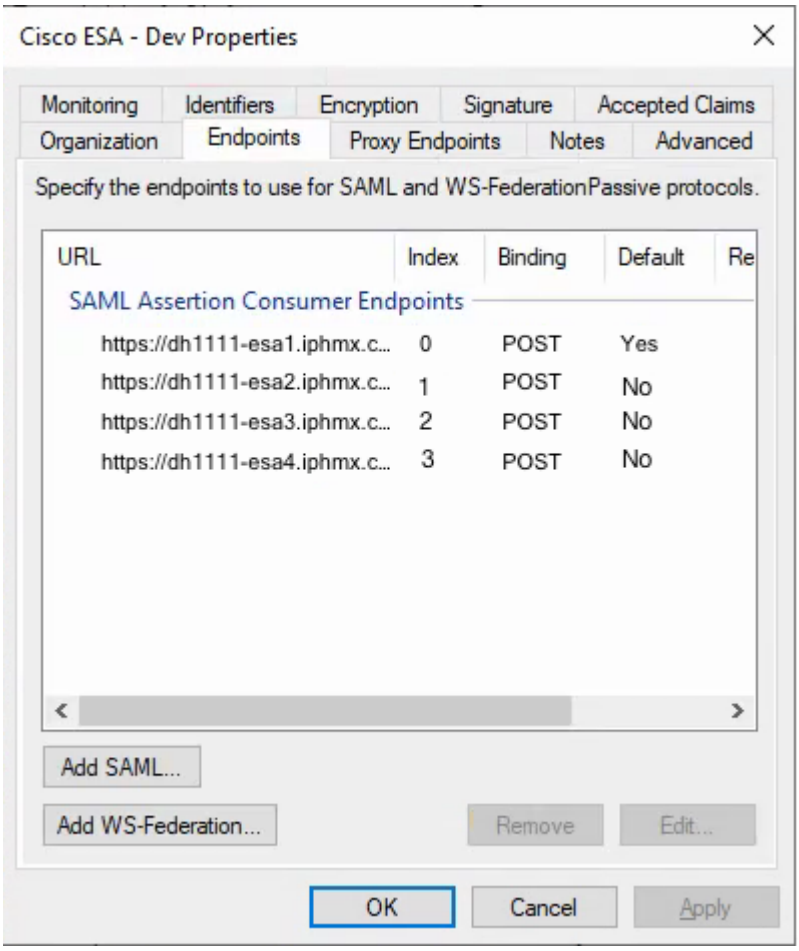
Autorisierungsregeln für die Ausgabe auswählen

1. Wählen Sie Weiter, um zur Seite "Fertig stellen" zu gelangen.

Vertrauenswürdige Endpunkte der vertrauenden Seite konfigurieren (nur Cluster)

Führen Sie diesen Schritt nur aus, wenn mehrere ESAs in einem Cluster vorhanden sind.

1. Öffnen Sie Vertrauenswürdige Eigenschaften der vertrauenden Partei > Endpunkte.
2. Fügen Sie alle für die ESA erreichbaren URL-Adressen hinzu, und klicken Sie dann auf OK.
3. Legen Sie die Werte für den Endpunktindex ab 0 fest (z. B. 0, 1, 2, 3).
4. Setzen Sie nur einen Endpunkt auf Default = Yes. Setzen Sie die verbleibenden Endpunkte auf Standard = Nein.

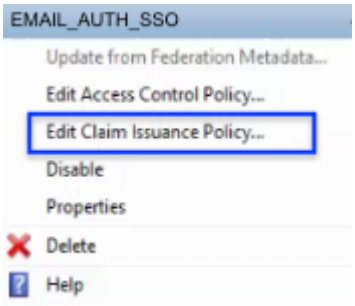


Autorisierungsregeln für die Ausstellung - Alle Benutzer zulassen

- Mit dem Schritt "Beenden" wird der Dialog Anspruchsregeln bearbeiten für die Vertrauensstellung der vertrauenden Seite eingeleitet, der unter "Ausstellungstransformationsregeln" behandelt wird.

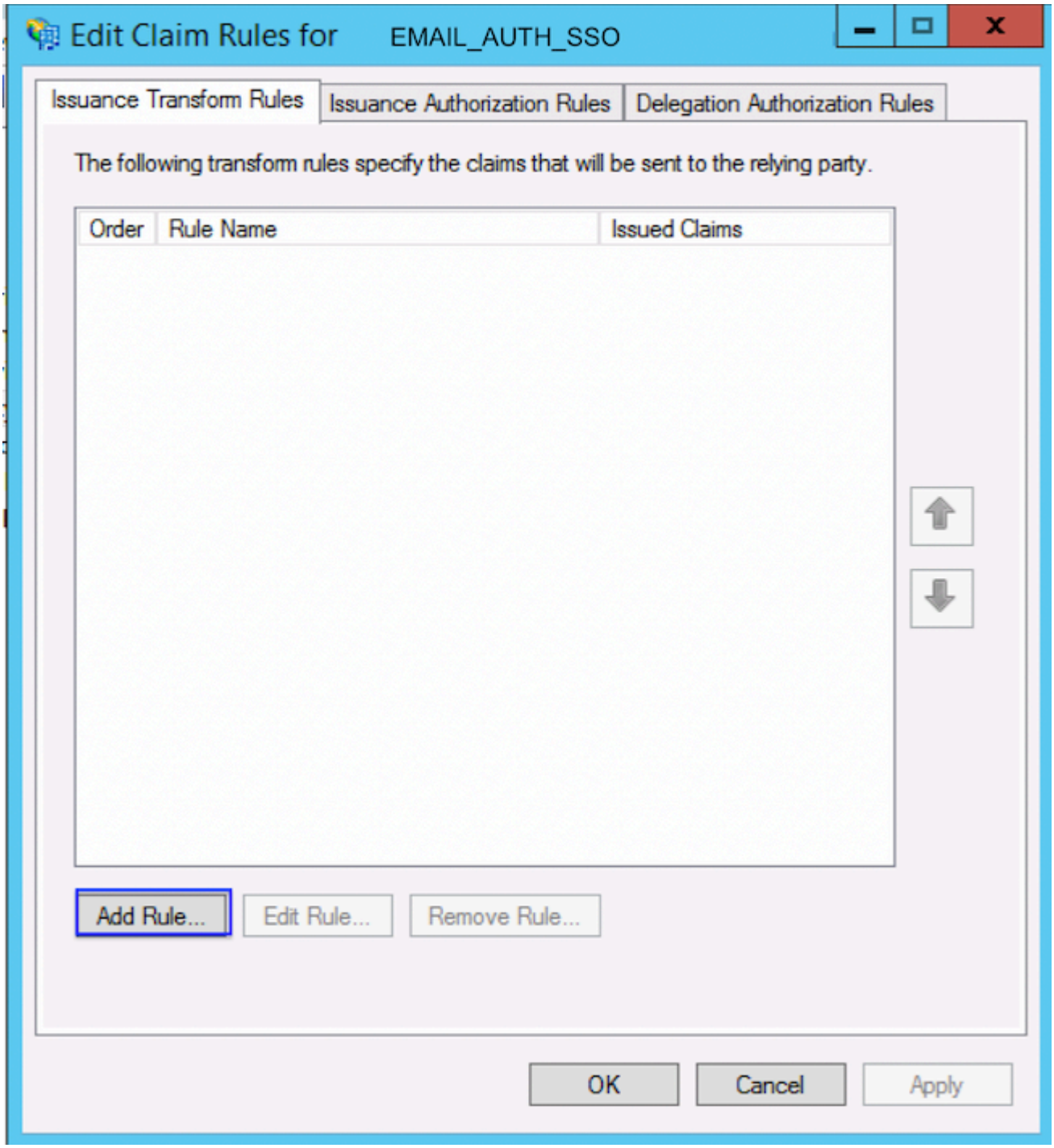
Ausstellungstransformationsregeln - Forderungen

- Wählen Sie Ausstellungsrichtlinie für Ansprüche bearbeiten aus.



Richtlinie für die Forderungsausstellung bearbeiten

- Wählen Sie Regel hinzufügen aus.

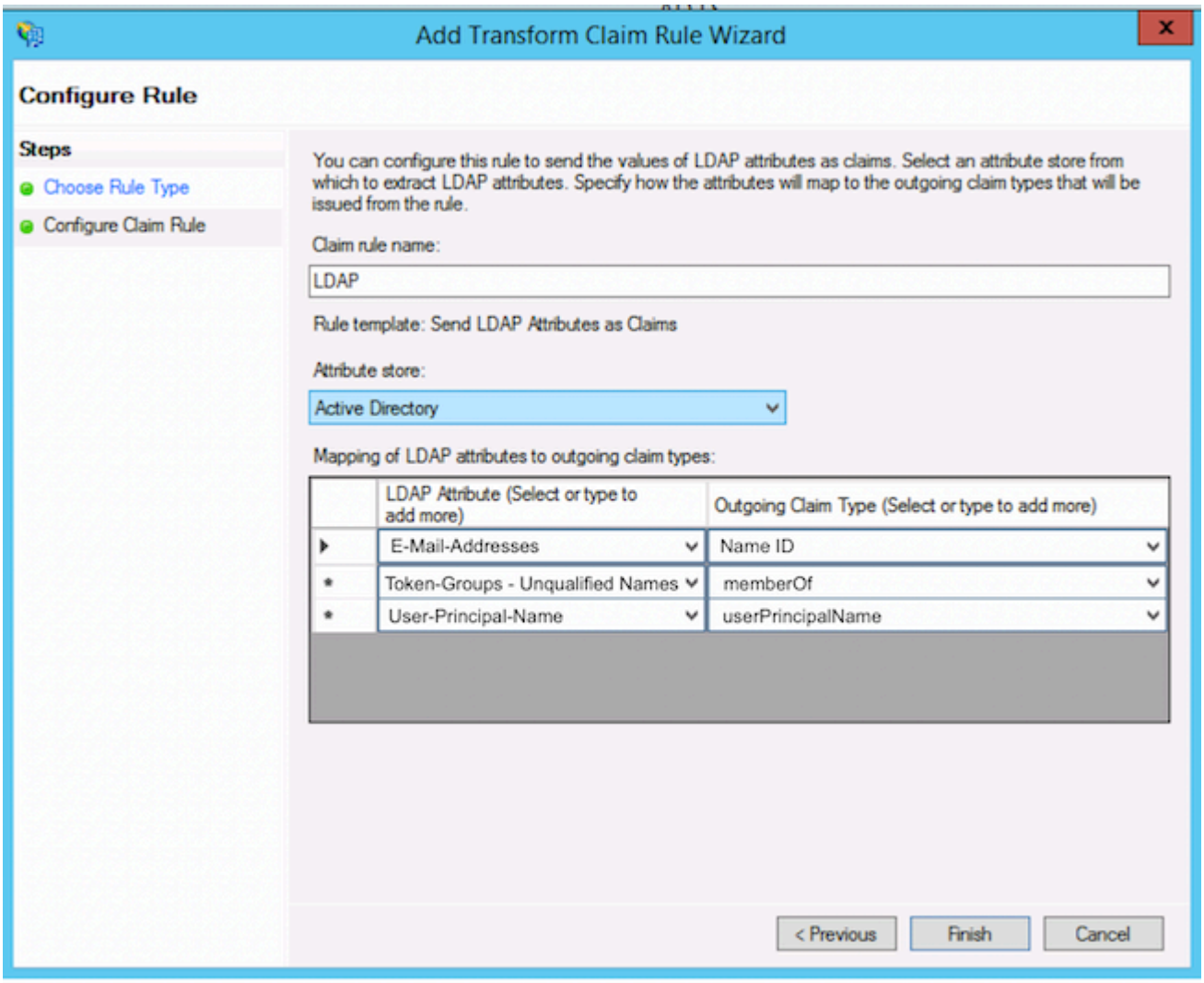


Ausstellungs-Transformationsregel hinzufügen

Bei den hier gezeigten Werten handelt es sich um allgemeine Werte, mit denen die ESA die Gruppennamen in den externen Authentifizierungseinstellungen übernehmen kann.

Tipp: Die Werte in der Zuordnung können je nach Administratoreinstellung variieren.

Tipp: Geben Sie in dem aufgeführten Beispiel die ausgehenden Anspruchstypen memberOf und userPrincipalName manuell ein. Wählen Sie Name ID aus der Dropdown-Liste aus.



Anspruchsregel umwandeln

- Wählen Sie Beenden.

IdP-Metadaten herunterladen und in ESA hochladen

Nachdem Sie die Konfiguration der Vertrauensstellung der vertrauenden Seite und der Anspruchsregel abgeschlossen haben, exportieren Sie die IdP-Metadaten (Identity Provider) und laden Sie sie in die ESA hoch.

⚠ Vorsicht: Beim Neustart des AD FS-Dienstes können aktive Authentifizierungssitzungen unterbrochen werden. Führen Sie diesen Schritt bei Bedarf während eines Wartungsfensters durch.

- Starten Sie den AD FS-Dienst bei Bedarf neu.
- Führen Sie folgende Befehle aus:

```
net stop adfssrv
net start adfssrv
```

- Laden Sie die Metadatendatei von dieser URL herunter:

https://myserver.domain.com/FederationMetadata/2007-06/FederationMetadata.xml

- Beenden Sie das ESA-Cluster, und kehren Sie zum ESA-Cluster zurück.

Überprüfung

1. Bestätigen Sie in der ESA oder SMA, dass der IdP-Metadatenimport erfolgreich abgeschlossen wurde.
2. Testen Sie eine Administratoranmeldung mithilfe von SAML Single Sign-on (SSO).
3. Überprüfen Sie, ob die erwarteten Gruppenansprüche empfangen werden und ob die Rollenzuordnung wie erwartet in die externe Authentifizierungskonfiguration übernommen wird.

Zugehörige Informationen

-

- Cisco Email Security Appliance – Endbenutzerhandbücher
- Cisco Content Security Management Appliance - Benutzerhandbücher

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.