Konfigurieren von Umbrella mit ADFS Version 3.0 mithilfe von SAML

Inhalt

Einleitung

In diesem Dokument wird die Konfiguration von SAML zwischen Cisco Umbrella und Active Directory Federation Services (ADFS) Version 3.0 beschrieben.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf Cisco Umbrella.

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.

Überblick

In diesem Artikel wird erläutert, wie SAML zwischen Cisco Umbrella und Active Directory Federation Services (ADFS) Version 3.0 konfiguriert wird. Die Konfiguration von SAML mit ADFS unterscheidet sich von den anderen SAML-Integrationen von Umbrella, da es sich nicht um einen Ein- oder Zwei-Klick-Prozess im Assistenten handelt, sondern Änderungen in ADFS erforderlich sind, um ordnungsgemäß zu funktionieren.

Dieser Artikel enthält detaillierte Änderungen, die Sie vornehmen müssen, damit SAML und ADFS zusammenarbeiten. Die wichtigsten Schritte bestehen darin, zuerst die Verschlüsselung zwischen Ihrer ADFS-Umgebung und Cisco Umbrella zu deaktivieren und dann der Einstellung der Umbrella-Weiterleitungspartei einige benutzerdefinierte Anspruchsregeln für die Issuance Transform hinzuzufügen.

Führen Sie diese Schritte nur mit einer vorhandenen, funktionierenden ADFS-Einrichtung durch. Cisco Umbrella Support kann keine Unterstützung oder Unterstützung bei der Konfiguration von ADFS in einer bestimmten Umgebung leisten.

Von diesen Anweisungen wird derzeit nur die ADFS-Version 3.0 (Windows Server 2012 R2) unterstützt. Es ist möglich, dass ältere (2.0 oder 2.1) oder neuere (4.0) Versionen von ADFS mit der Umbrella SAML-Integration arbeiten können, dies wurde jedoch nicht getestet oder bewiesen. Wenn Sie eine andere Version von ADFS haben und daran interessiert sind, mit unseren Support- und Produktteams bei der Integration zusammenzuarbeiten, wenden Sie sich an den Cisco Umbrella Support.

Die Voraussetzungen für die erste SAML-Einrichtung finden Sie in der Umbrella-Dokumentation: Identitätsintegrationen: Voraussetzungen. Nach Abschluss dieser Schritte können Sie die ADFS-spezifischen Anweisungen in diesem Artikel verwenden, um die Konfiguration abzuschließen.

In den Schritten in der Umbrella-Dokumentation wird erwähnt, dass Sie Ihre SAML (ADFS)-Metadaten auf Umbrella hochladen müssen. Sie können auf die Metadaten zugreifen, indem Sie zu dieser URL navigieren und dann die XML-Datei hochladen.

```
https://{your-ADFS-domain-name}/federationmetadata/2007-06/federationmetadata.xml
```

Verschlüsselung deaktivieren

1. Öffnen Sie die AD FS-Verwaltung. Erweitern Sie Trust Relationships, und wählen Sie Relying Party Trusts aus.

2. Klicken Sie mit der rechten Maustaste auf die Umbrella-vertrauende Partei (oder wie Sie sie benannt haben) und wählen Sie Eigenschaften.

3. Wählen Sie die Registerkarte Verschlüsselung.

4. Wählen Sie Entfernen, um das Zertifikat für die Verschlüsselung zu entfernen.

5. Wählen Sie OK, um den Bildschirm zu schließen.

Neue Ausgabe hinzufügen Anspruchsregeln umwandeln

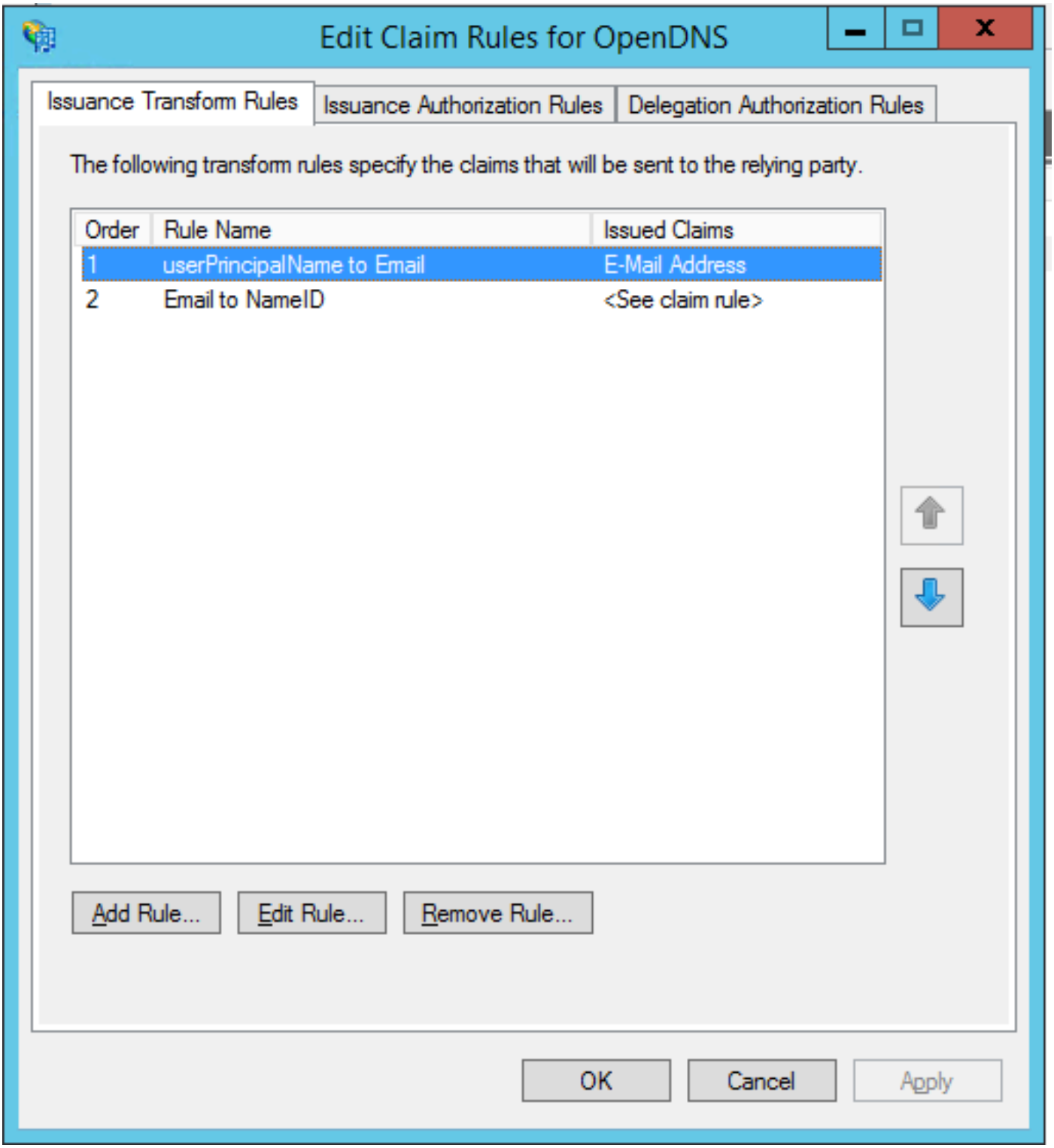
1. Öffnen Sie die AD FS-Verwaltung. Erweitern Sie Vertrauensbeziehungen, und wählen Sie Vertrauenswürdige Partei weiterleiten aus.

2. Klicken Sie mit der rechten Maustaste auf die Umbrella-Weiterleitungspartei (oder wie Sie sie benannt haben) und wählen Sie Anspruchsregeln bearbeiten aus.

3. Wählen Sie unter "Ausstellungstransformationsregeln" die Option "Regel hinzufügen".

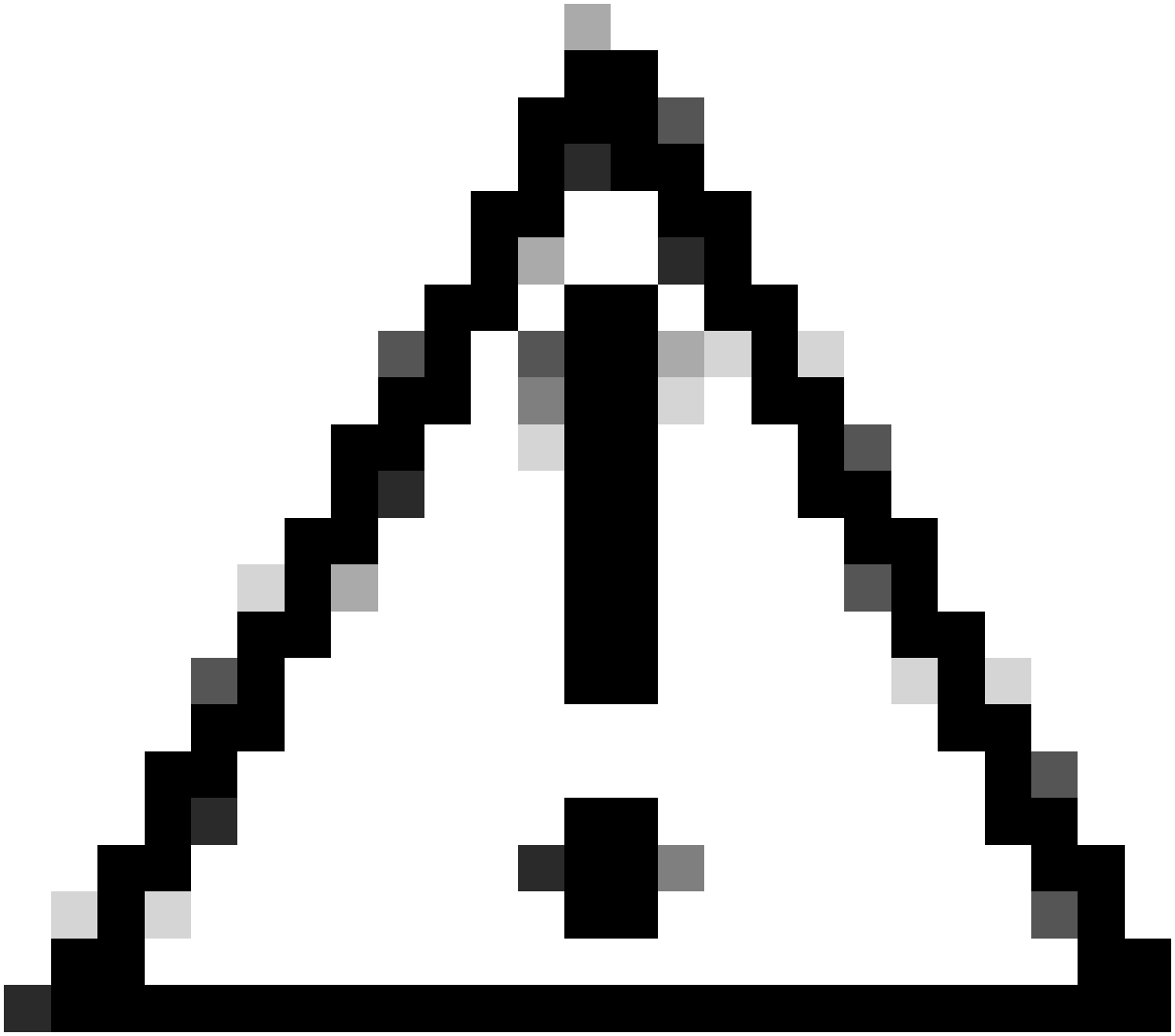
4. Wählen Sie Anträge mithilfe einer benutzerdefinierten Regel senden aus.

Eine Liste der Regeln, die Sie hinzufügen können, finden Sie in diesem Screenshot.



Sobald Sie diese Regeln hinzufügen, kann die Integration beginnen zu funktionieren.

Regeln umwandeln



Vorsicht: Diese Regeln wurden sowohl in der ADFS-Laborumgebung von Umbrella als auch in einigen wenigen Produktionsumgebungen getestet und funktionieren. Passen Sie sie an Ihre Umgebung an.

---

userPrincipalName in E-Mail-Adresse

```
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname", Issuer == "AD A
=> issue(store = "Active Directory", types = ("http://schemas.xmlsoap.org/ws/2005/05/identity/claims/em
```

E-Mail an NameID

```
c:[Type == "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"]
=> issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier",
Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType = c.ValueType,
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"]
= "urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress");
```

Anhang: Anmeldung mit 'mail'-Attribut

Standardmäßig authentifiziert ADFS Benutzer anhand ihres UPN (User Principal Name, Benutzerprinzipalname). Wenn die E-Mail-Adresse Ihres Benutzers (Umbrella-Kontoname) nicht mit seiner UPN übereinstimmt, sind zusätzliche Schritte erforderlich. Weitere Informationen finden Sie in diesem Knowledge Base-Artikel: Wie konfiguriere ich AD FS im Cisco Umbrella Dashboard, damit ich mich mit einer E-Mail-Adresse anmelden kann?

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.