Configurazione di Umbrella con ADFS versione 3.0 tramite SAML

Sommario

Introduzione

In questo documento viene descritto come configurare SAML tra Cisco Umbrella e Active Directory Federation Services (ADFS) versione 3.0.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano su Cisco Umbrella.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Panoramica

In questo articolo viene illustrato come configurare SAML tra Cisco Umbrella e Active Directory Federation Services (ADFS) versione 3.0. La configurazione di SAML con ADFS è diversa dalle altre integrazioni SAML di Umbrella in quanto non si tratta di un processo costituito da uno o due clic nella procedura guidata, ma richiede che le modifiche in ADFS funzionino correttamente.

In questo articolo vengono illustrate le modifiche da apportare per consentire la collaborazione tra SAML e ADFS. I passaggi principali consistono nel disabilitare innanzitutto la crittografia tra l'ambiente ADFS e Cisco Umbrella e quindi aggiungere alcune regole attestazione personalizzate di trasformazione rilascio all'impostazione del componente di inoltro Umbrella.

Eseguire questi passaggi solo con un ADFS funzionante esistente impostato. Il supporto Cisco Umbrella non è in grado di fornire assistenza o supporto nella configurazione di ADFS in un particolare ambiente.

Al momento queste istruzioni supportano solo ADFS versione 3.0 (Windows Server 2012 R2). È possibile che le versioni precedenti (2.0 o 2.1) o successive (4.0) di ADFS possano funzionare con l'integrazione di Umbrella SAML, ma questa operazione non è stata testata né dimostrata. Se si dispone di una versione diversa di ADFS e si desidera collaborare con i team del supporto e dei prodotti Dell per l'integrazione, contattare il supporto Cisco Umbrella.

I prerequisiti per la configurazione iniziale di SAML sono disponibili nella documentazione di Umbrella: Integrazioni delle identità: Prerequisiti. Dopo aver completato questi passaggi, è possibile continuare a utilizzare le istruzioni specifiche di ADFS riportate in questo articolo per completare la configurazione.

I passaggi nella documentazione di Umbrella indicano che è necessario caricare i metadati SAML (ADFS) in Umbrella. È possibile accedere ai metadati passando a questo URL e caricando il file XML.

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

Disabilita crittografia

1. Aprire Gestione ADFS. Espandere Relazioni di trust e selezionare Trust tra relatori.

2. Fare clic con il pulsante destro del mouse sul componente Umbrella (o qualsiasi altro componente a cui è stato assegnato un nome) e selezionare Proprietà.

3. Selezionare la scheda Cifratura.

4. Selezionare Rimuovi per rimuovere il certificato per la crittografia.

5. Selezionare OK per chiudere la schermata.

Aggiunta di nuove regole attestazione di trasformazione rilascio

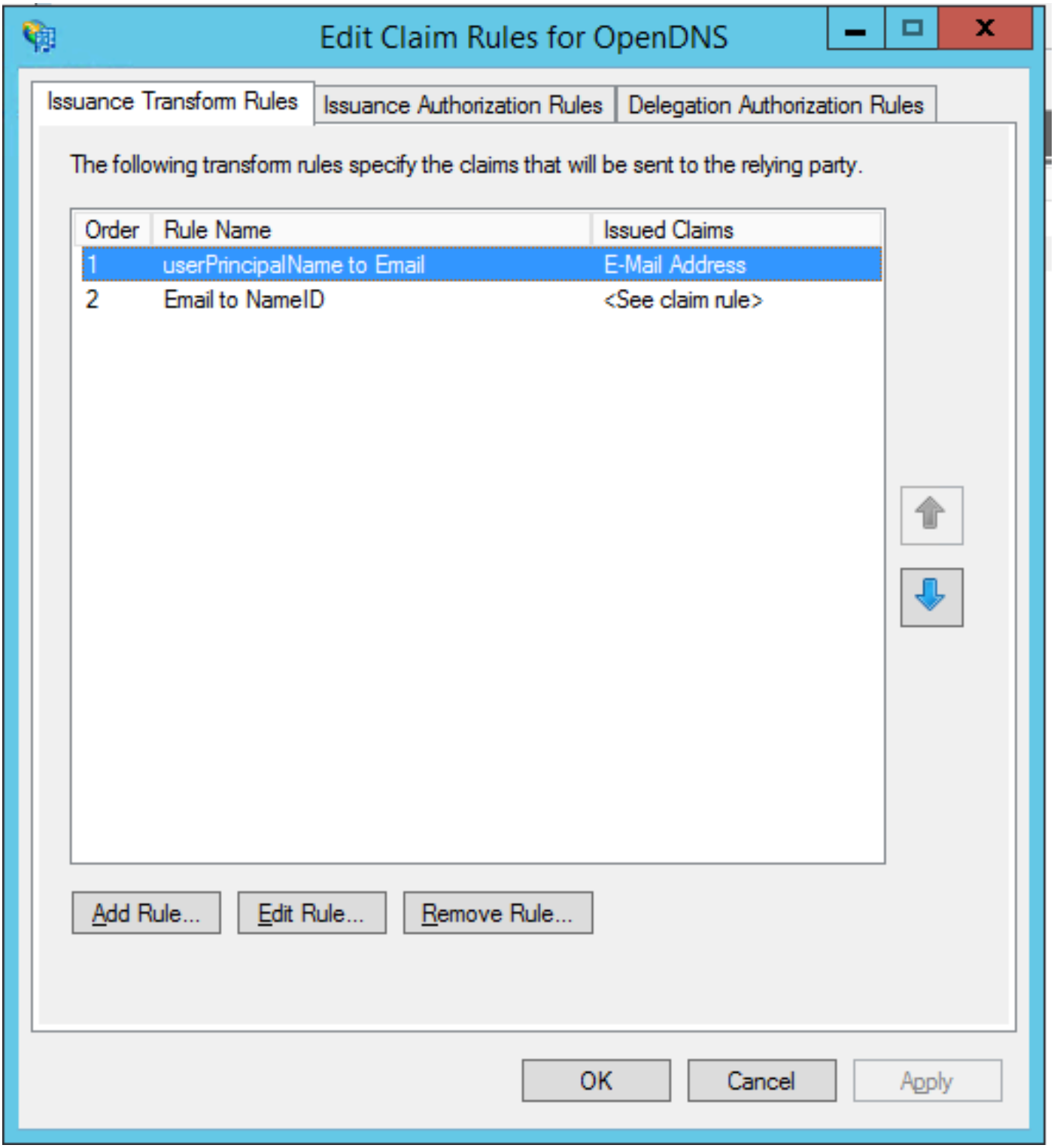
1. Aprire Gestione ADFS. Espandere Relazioni di trust e selezionare Trust tra parti di inoltro.

2. Fare clic con il pulsante destro del mouse sul componente di inoltro Umbrella (o su qualsiasi altro componente a cui è stato assegnato il nome) e selezionare Modifica regole attestazione.

3. In Regole trasformazione rilascio, selezionare Aggiungi regola.

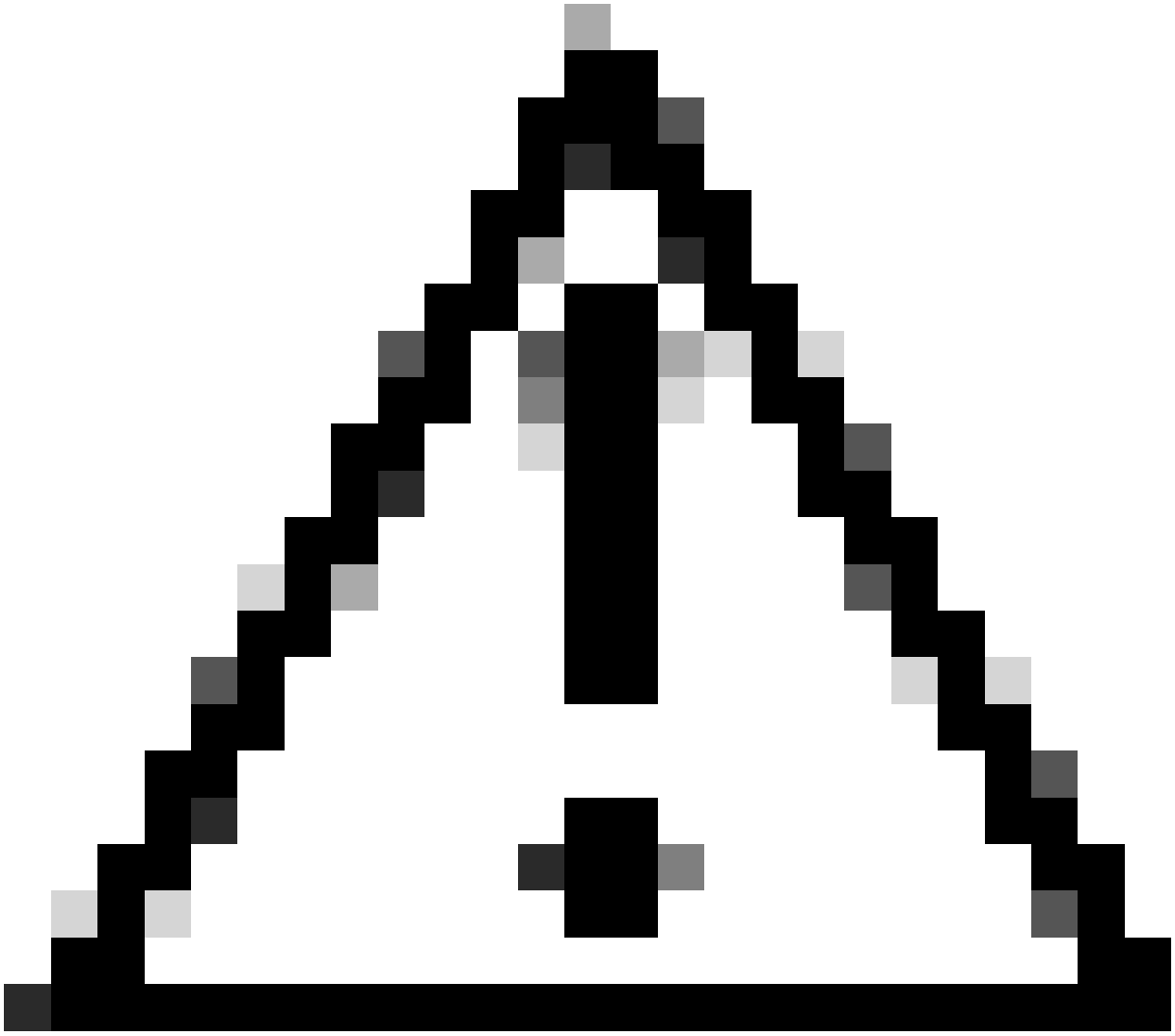
4. Selezionare Invia contestazioni utilizzando una regola personalizzata.

In questa schermata viene visualizzato l'elenco delle regole che è possibile aggiungere.



Una volta aggiunte ognuna di queste regole, l'integrazione può iniziare a funzionare.

Regole di trasformazione



Attenzione: Queste regole sono state testate e funzionanti nell'ambiente di laboratorio ADFS di Umbrella e in alcuni ambienti di produzione dei clienti. Modificarle in base al proprio ambiente.

---

da userPrincipalName a Email Address

```
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
```

Invia a 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");
```

Appendice: Accesso con attributo 'mail'

Per impostazione predefinita, ADFS autentica gli utenti in base al nome UPN (User Principal Name). Se l'indirizzo di posta elettronica dell'utente (nome account Umbrella) non corrisponde al nome UPN corrispondente, sono necessari ulteriori passaggi. Consultare il seguente articolo della Knowledge Base: Come configurare AD FS in Cisco Umbrella Dashboard per consentire gli accessi con un indirizzo di posta elettronica?

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).