Configurare l'autenticazione esterna SAML SSO con AD FS per ESA e SMA

Sommario

Introduzione

In questo documento viene descritto come configurare Active Directory Federation Services come provider di identità SAML per l'autenticazione esterna su Cisco ESA e SMA.

Prerequisiti

In questo documento viene fornita una visualizzazione dell'applicazione di terze parti che i tecnici non sono in grado di visualizzare.

- Passaggi di configurazione per l'autenticazione esterna SAML (Security Assertion Markup Language) con Active Directory Federation Services (ADFS) 2012 e 2016 per le versioni più recenti di Cisco Email Security Appliance (ESA) e Security Management Appliance (SMA).
- Passaggi di base basati su esercitazioni che non includono configurazioni specifiche dell'installazione.
- Esempio funzionante di un ambiente lab che può differire da una distribuzione di produzione.

⚠ Attenzione: Completare la configurazione del provider di servizi (SP) prima di eseguire

⚠ questa procedura. Vedere .

Requisiti

- Microsoft Active Directory Federation Services (ADFS) 2012 o 2016
- L'ultima versione di Cisco Email Security Appliance (ESA) e Security Management Appliance (SMA).

Componenti usati

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.

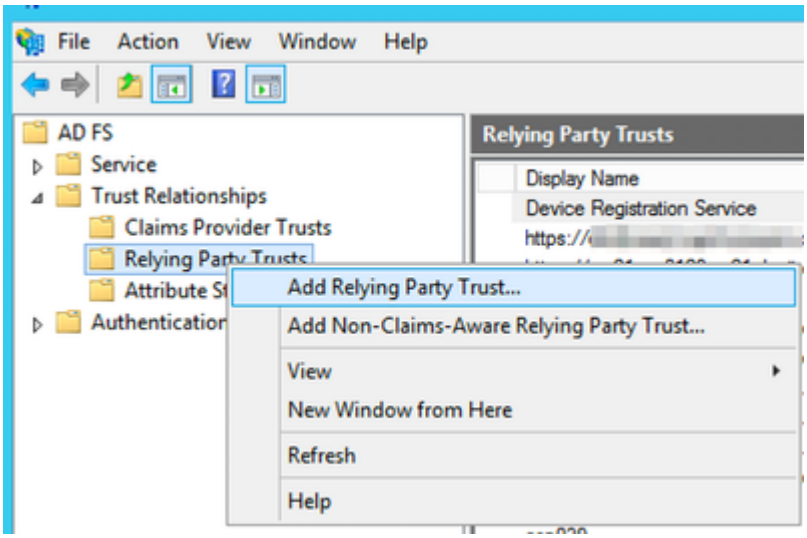
Passaggi per la configurazione IDP ADFS per SAML

Configurare l'attendibilità del componente

Utilizzare una delle due opzioni disponibili per creare l'attendibilità del componente in ADFS.

Metodo A: Creare l'attendibilità della relying party importando i metadati SP

1. Aprire la console di gestione AD FS da Strumenti di amministrazione.
2. Nella console Gestione AD FS espandere Relazioni trusted, fare clic con il pulsante destro del mouse su Trust relying party e quindi selezionare Aggiungi trust relying party.



Aggiungi attendibilità componente

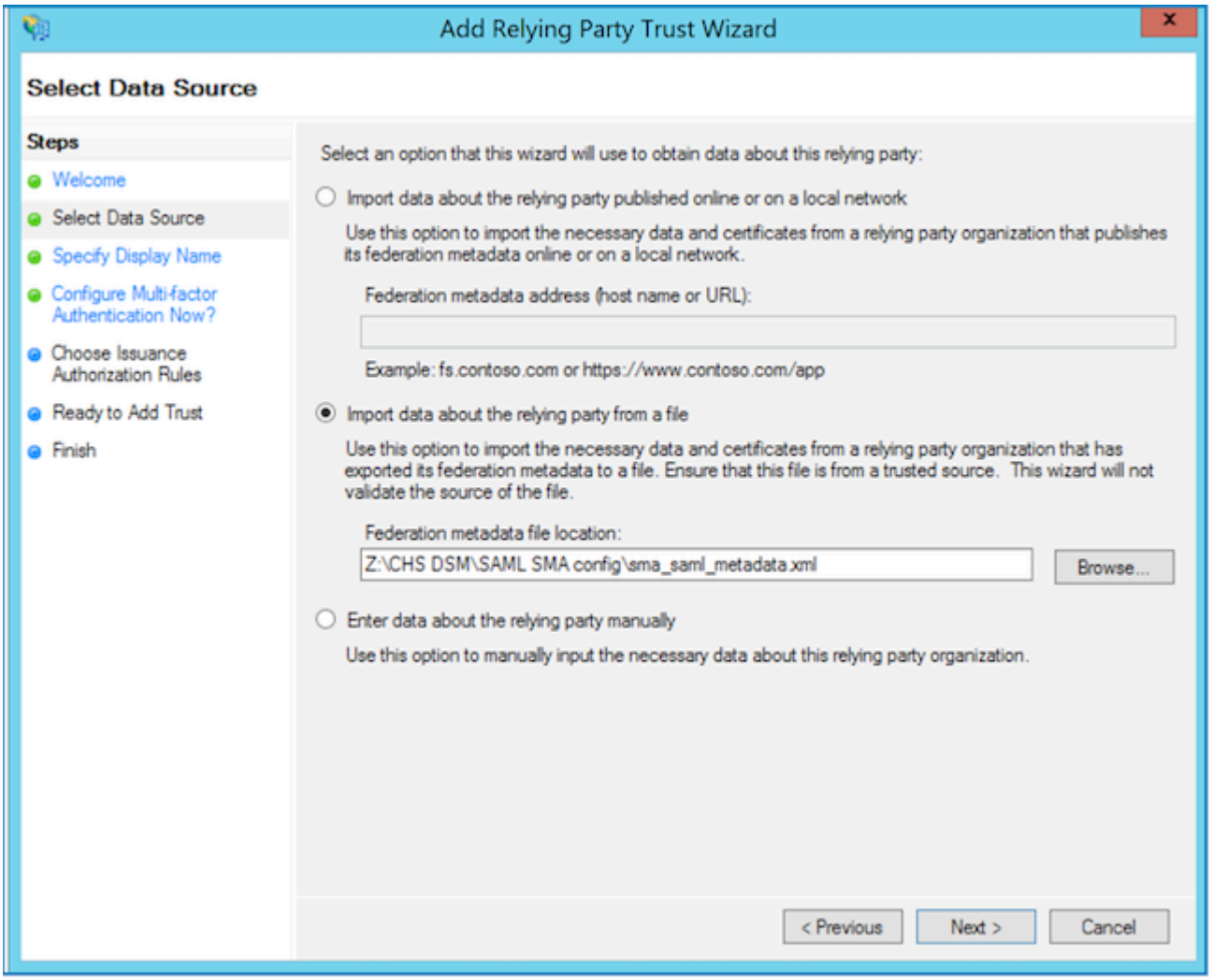
Suggerimento: Attendibilità componente Microsoft

Continuare utilizzando una delle due opzioni seguenti:

- Opzione A. Importa dati sul componente da un file. Caricare il file metadata.xml del provider di servizi ESA o SMA (SP).
- Opzione B. Immettere manualmente i dati relativi al componente. Questa opzione consente di eseguire in modo semplificato le operazioni di configurazione manuale.

Opzione A. Importa dati sul componente da un file. Caricare il file metadata.xml del provider di servizi ESA o SMA (SP).

1. Selezionare l'opzione per importare da un file i dati relativi al componente, quindi selezionare Avanti.



Importazione del file di metadati ESA/SMA

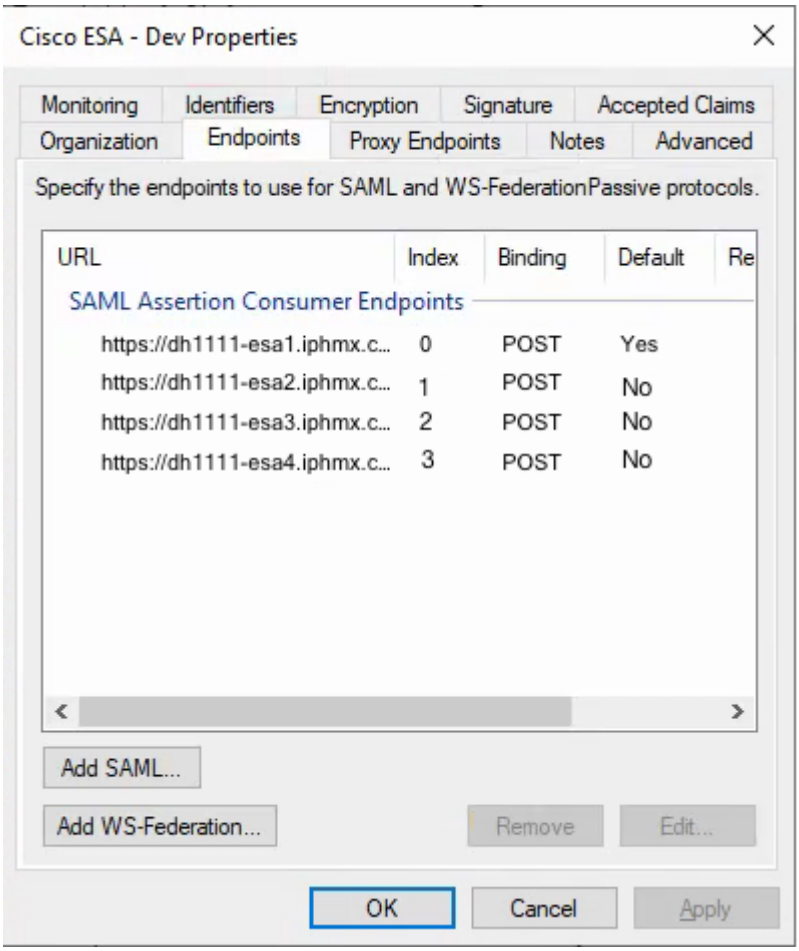
- Specificare un nome visualizzato per identificare l'attendibilità del componente, quindi selezionare due volte Avanti.
- Per le regole di autorizzazione rilascio, selezionare Autorizza tutti gli utenti, quindi selezionare Avanti.
- Nella pagina Pronto per aggiungere trust accettare le impostazioni predefinite e quindi selezionare Avanti.
- Selezionare Fine. Verrà aperta la finestra di dialogo Modifica regole attestazione per l'attendibilità del componente, illustrata in Regole di trasformazione rilascio - Attestazioni.

Proprietà trust relying party - Endpoint

Eseguire questo passaggio solo se in un cluster sono presenti più ESA.

1. Aprire Proprietà attendibilità componente > Endpoint.
2. Aggiungere ciascun indirizzo URL raggiungibile ESA, quindi selezionare OK.
3. I valori di indice vengono conteggiati da 0, ovvero 0, 1, 2 e 3.
4. Impostare una sola voce su Default = Sì.

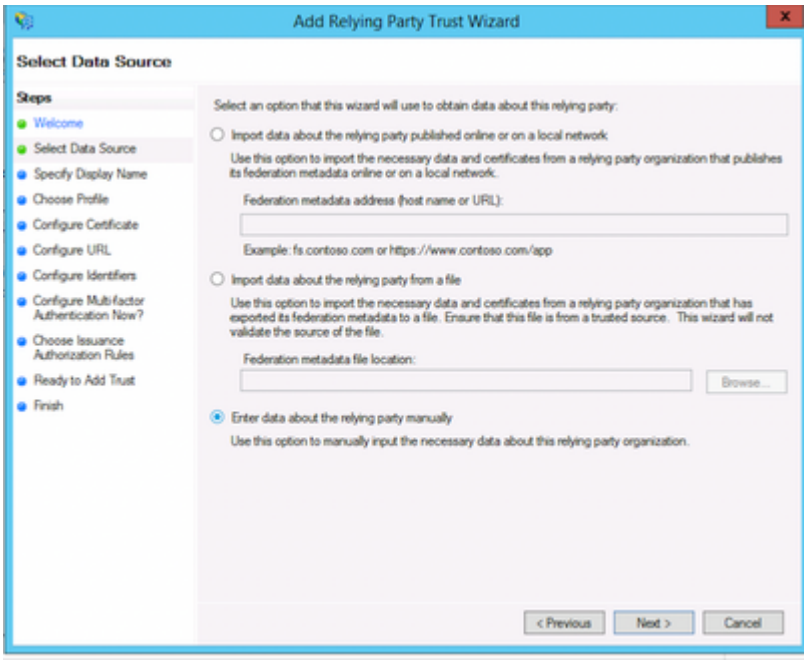
5. Impostare le voci rimanenti su Default = No.



Proprietà trust relying party - Endpoint

Opzione B. Immettere manualmente i dati relativi al componente. Questa opzione consente di eseguire in modo semplificato le operazioni di configurazione manuale.

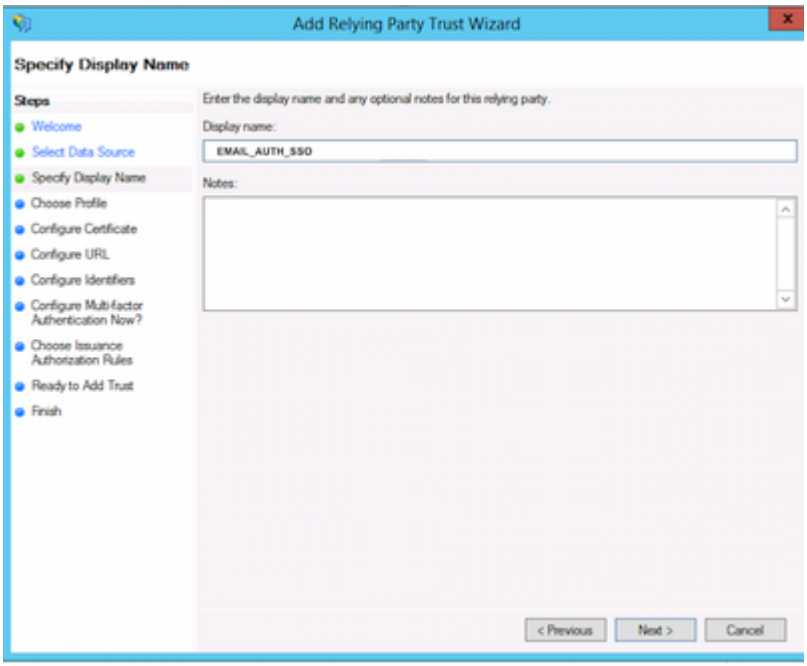
1. Selezionare Immettere manualmente i dati relativi al componente.



Aggiungi componente manualmente

Suggerimento: Nome visualizzato è il nome scelto per identificare l'attendibilità del componente per ESA o SAML SMA.

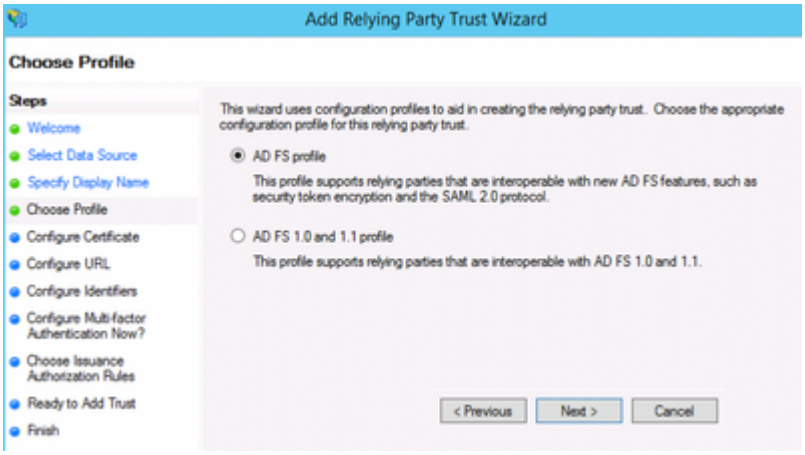
1. Immettere un nome visualizzato per il provider di servizi, ad esempio ESA_SP.



Creare un nome per il profilo di Service Provider

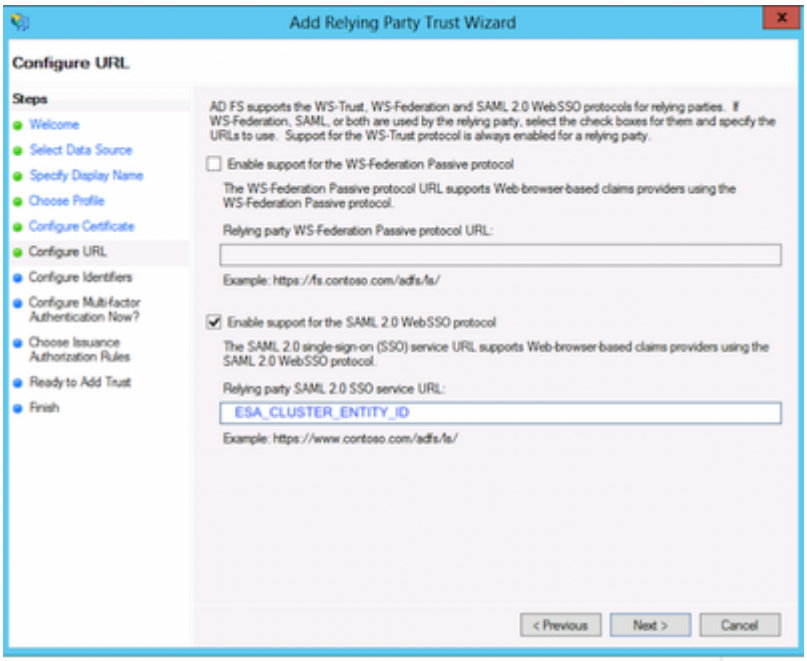
Suggerimento: Ruolo delle regole attestazione e delle regole di trasformazione emissione

1. Scegliere l'opzione di profilo Profilo ADFS.



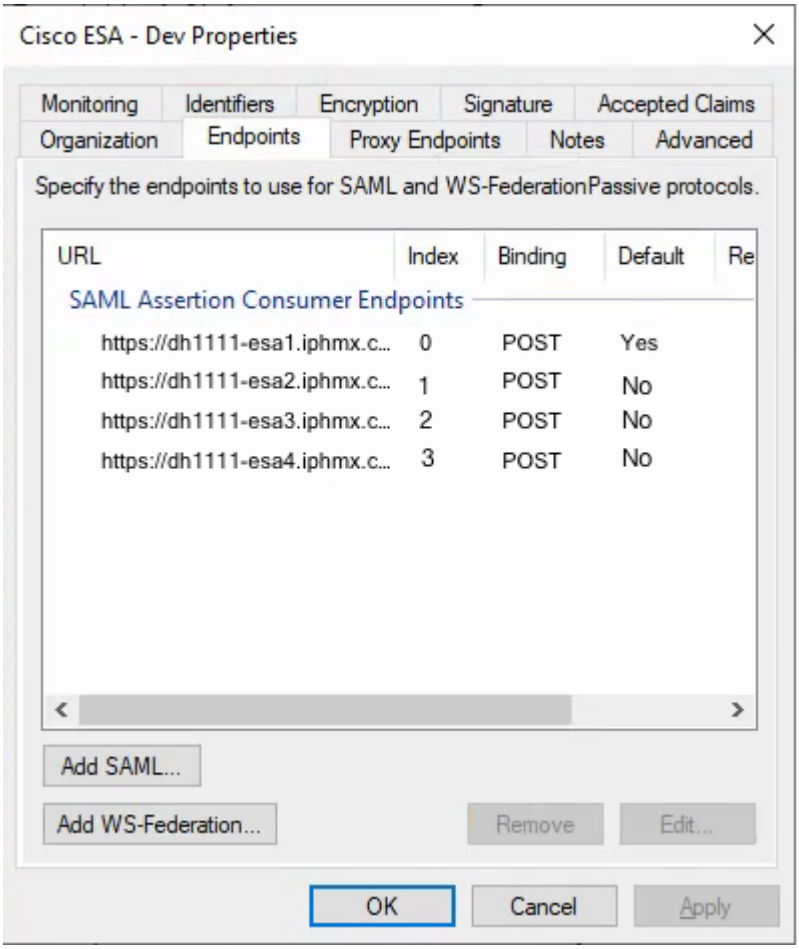
Opzione di profilo ADFS per utilizzare SAML 2.0

1. Caricare il certificato pubblico dalla configurazione del provider di servizi ESA (SP).
2. Per Configura URL, scegliere Abilita supporto per il Single Sign-On (SSO) di SAML 2.0.
3. Immettere l'URL del servizio SAML 2.0 SSO della relying party con il valore Entity ID del profilo SP.



Regole di autorizzazione rilascio - - Autorizza tutti gli utenti

1. Per le regole di autorizzazione rilascio, scegliere Consenti a tutti gli utenti di accedere a questo componente.



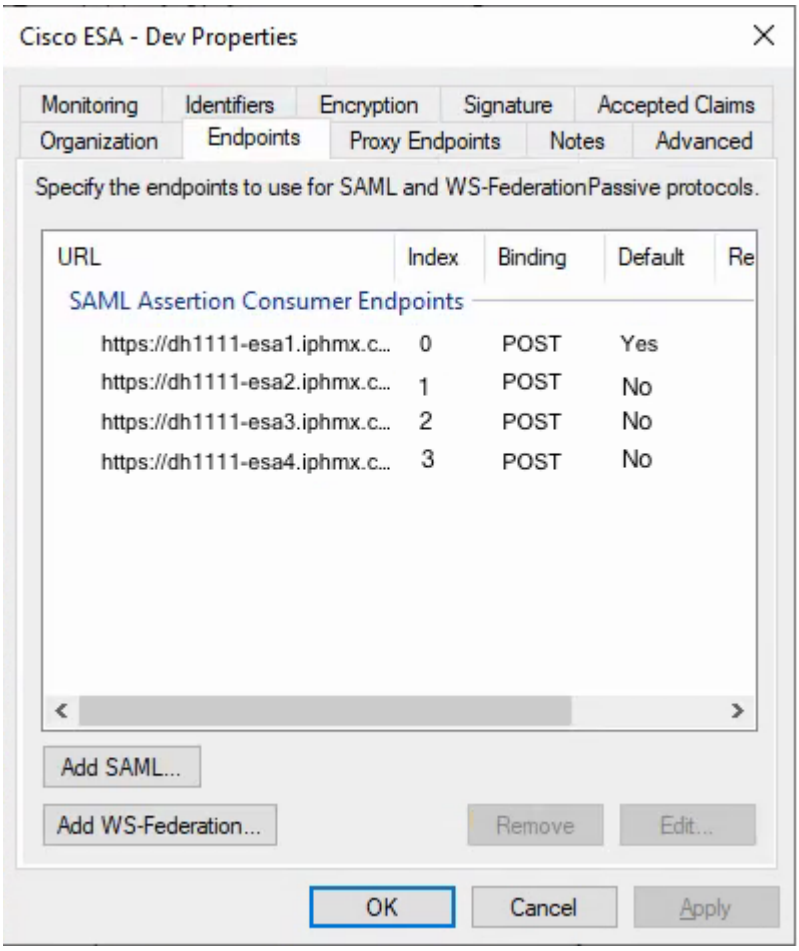
Scegli regole di autorizzazione rilascio

1. Selezionare Successivo per passare alla pagina Fine.

Configura endpoint attendibilità componente (solo cluster)

Eseguire questo passaggio solo se in un cluster sono presenti più ESA.

1. Aprire Proprietà attendibilità componente > Endpoint.
2. Aggiungere ciascun indirizzo URL raggiungibile ESA, quindi fare clic su OK.
3. Impostare i valori di indice dell'endpoint a partire da 0 (ad esempio, 0, 1, 2, 3).
4. Impostare un solo endpoint su Default = Yes. Impostare gli endpoint rimanenti su Default = No

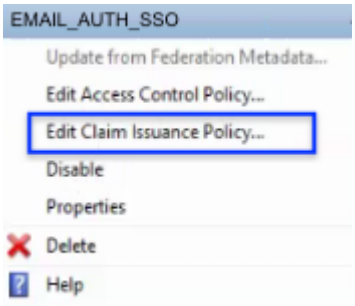


Regole di autorizzazione rilascio - Autorizza tutti gli utenti

- Il passo Fine avvia la finestra di dialogo Modifica regole attestazione per l'attendibilità del componente, descritta in Regole di trasformazione rilascio.

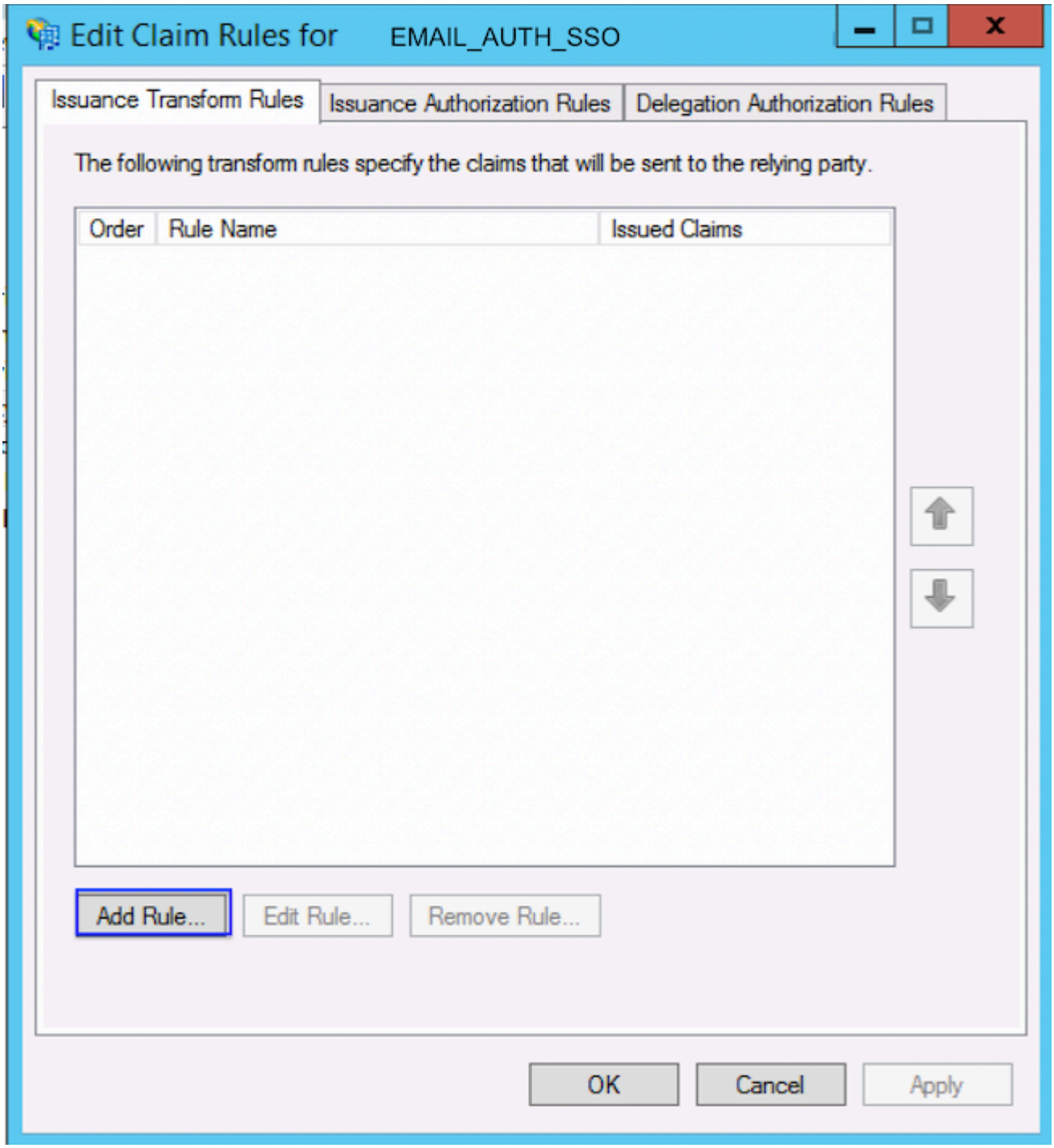
Regole di trasformazione rilascio - Attestazioni

- Selezionare Modifica criteri di rilascio attestazioni.



Modifica criteri di rilascio attestazioni

- Selezionare Aggiungi regola.

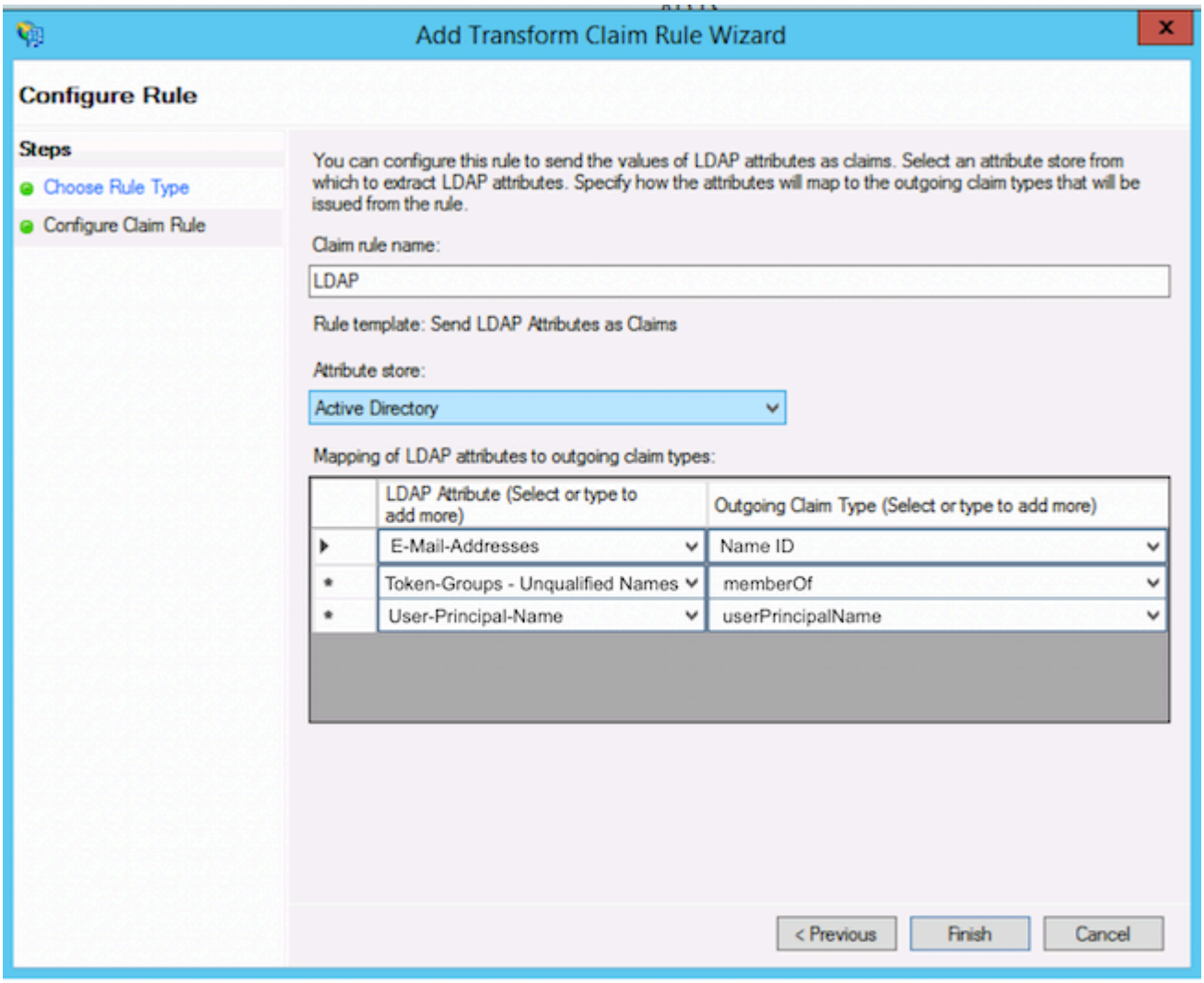


Aggiungi regola di trasformazione rilascio

I valori mostrati di seguito sono valori comuni che consentono a ESA di popolare i nomi dei gruppi nelle impostazioni di autenticazione esterna.

Suggerimento: I valori nel mapping possono variare in base alle preferenze dell'amministratore.

Suggerimento: Nell'esempio elencato, immettere manualmente i tipi di attestazione in uscita memberOf e userPrincipalName. Selezionare Name ID dall'elenco a discesa.



Trasforma regola attestazione

- Selezionare Fine.

Scarica i metadati IdP e caricali su ESA

Dopo aver completato la configurazione dell'attendibilità del componente e della regola attestazione, esportare i metadati del provider di identità (IdP) e caricarli in ESA.

⚠ Attenzione: Il riavvio del servizio ADFS può interrompere le sessioni di autenticazione attive. Se necessario, eseguire questo passaggio durante una finestra di manutenzione.

- Se necessario, riavviare il servizio ADFS.
- Eseguire i seguenti comandi:

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

- Scarica il file di metadati da questo URL:

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

- Completare e tornare al cluster ESA.

Verifica

1. In ESA o SMA, verificare che l'importazione dei metadati IdP sia stata completata correttamente.
2. Eseguire il test di un accesso amministrativo utilizzando SAML Single Sign-On (SSO).
3. Verificare che le attestazioni di gruppo previste vengano ricevute e che il mapping dei ruoli venga popolato come previsto nella configurazione dell'autenticazione esterna.

Informazioni correlate

-

- Cisco Email Security Appliance - Guide per l'utente
- Cisco Content Security Management Appliance - Guide per l'utente

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).