Installare il file di metadati in ADFS

Sommario

Introduzione

In questo documento viene descritto come installare il file di metadati in Microsoft Active Directory Federation Services (ADFS).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- ADFS
- Integrazione SAML (Security Assertion Markup Language) con Security Management Appliance

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- SMA 11.x.x
- SMA 12.x.x

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.

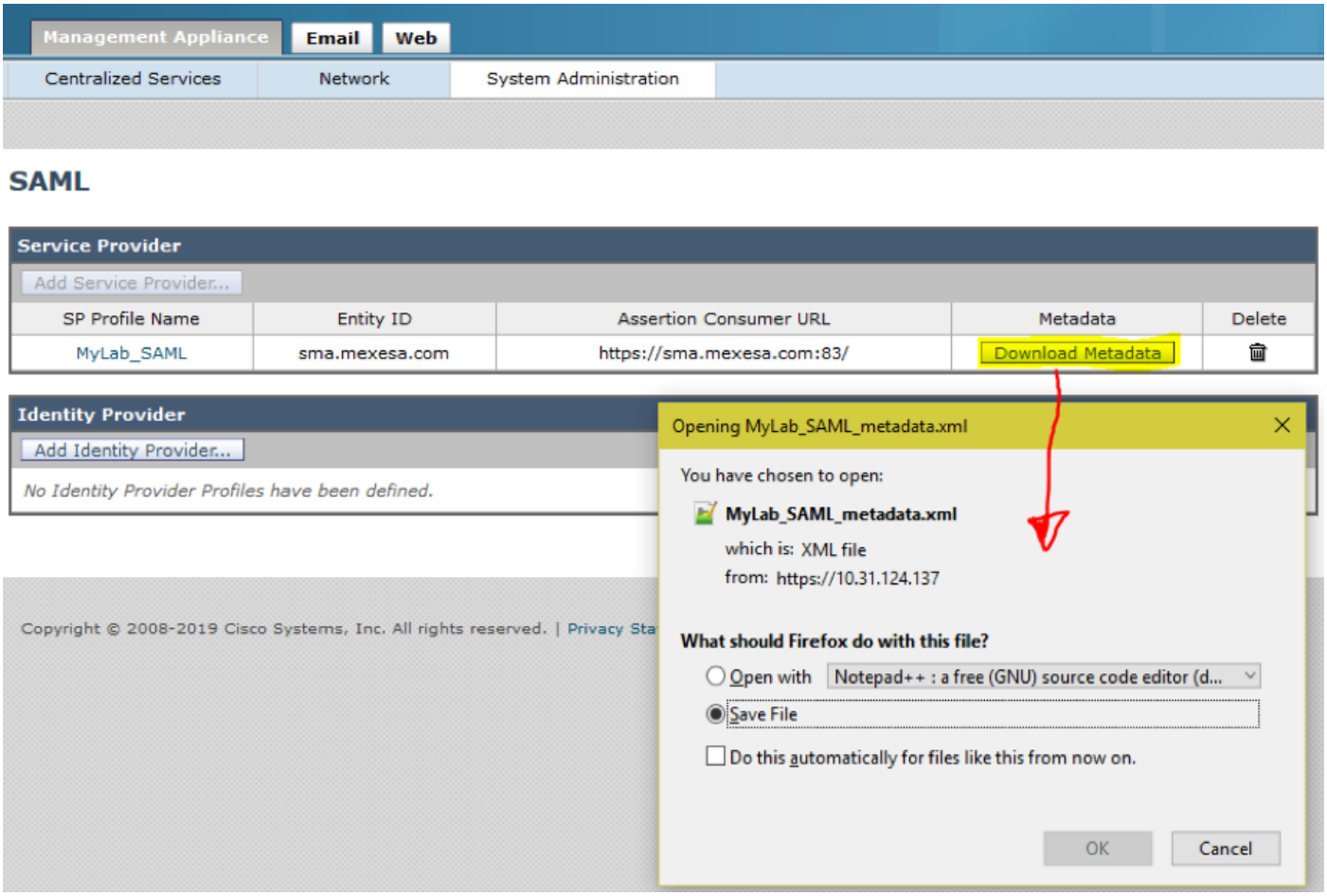
Premesse

Prima di installare il file di metadati in ADFS, verificare che siano soddisfatti i seguenti requisiti:

- SAML abilitato in SMA
- Verificare se il provider di identità utilizzato dall'organizzazione è supportato da Cisco Content Security Management Appliance. Provider di identità supportati: Microsoft Active Directory Federation Services (ADFS) 2.0Ping Identity PingFederate 7.2Cisco Web Security Appliance 9.1
- Ottenere i certificati necessari per garantire la comunicazione tra l'accessorio e il provider di identità:Se si desidera che l'accessorio firmi le richieste di autenticazione SAML o che il provider di identità crittografi le asserzioni SAML, ottenere un certificato autofirmato o un certificato da un'Autorità di certificazione (CA) attendibile e la chiave privata associata.Se si desidera che il provider di identità firmi le asserzioni SAML, ottenere il certificato del provider di identità. L'accessorio utilizza questo certificato per verificare le asserzioni SAML firmate

Configurazione

Passaggio 1. Passare all'SMA e selezionare **Amministrazione sistema > SAML > Scarica metadati**, come mostrato nell'immagine.



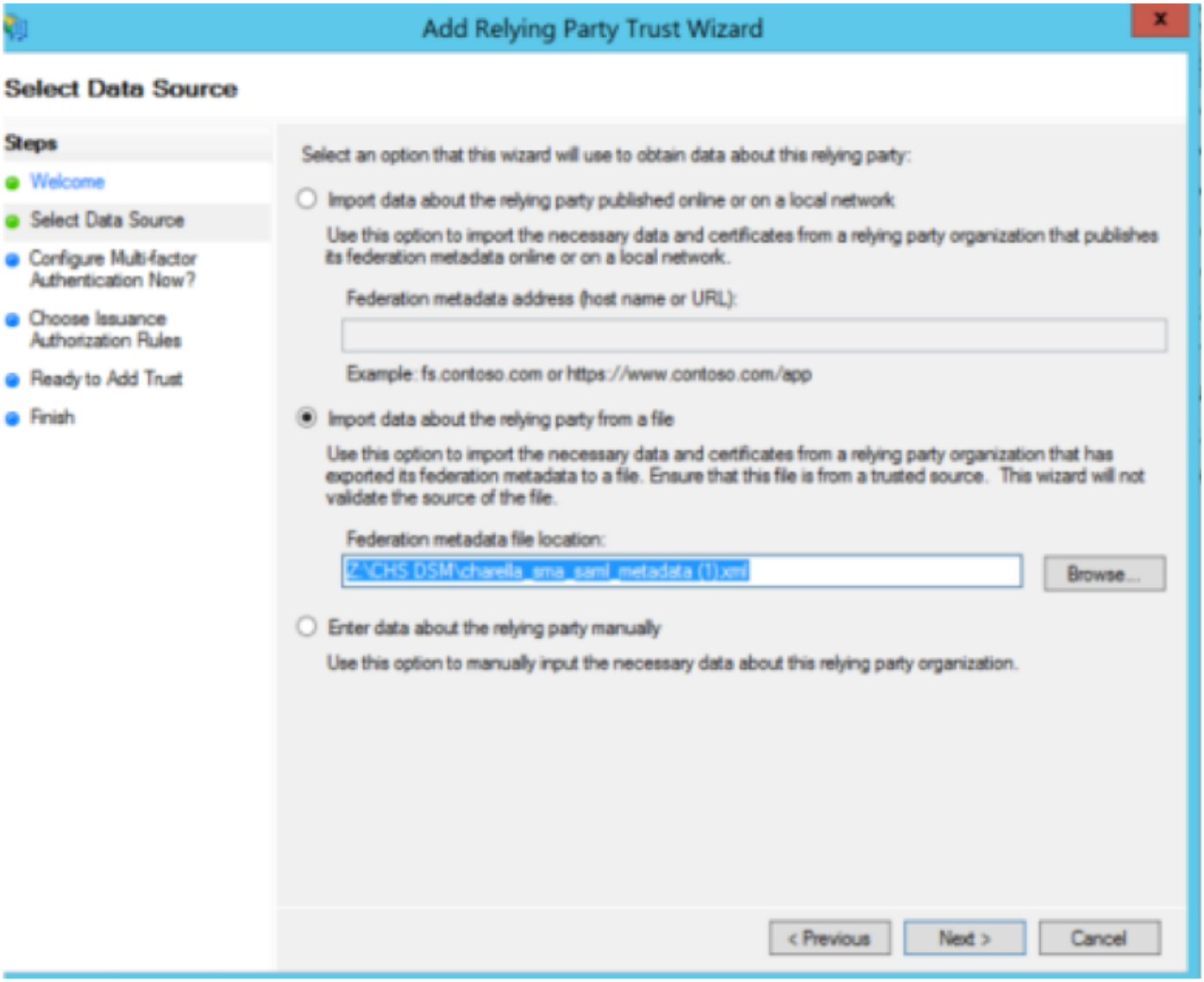
Passaggio 2. Il profilo del provider di identità viene compilato automaticamente quando il cliente carica il file di metadati ADFS. Microsoft ha un URL predefinito: **https://<Host-ADFS>/FederationMetadata/2007-06/FederationMetadata.xml.**

Passaggio 3. Dopo aver configurato entrambi i profili, è necessario modificare i metadati del profilo SP, come per il bug CSCvh30183.. L'aspetto del file di metadati è quello mostrato nell'immagine.

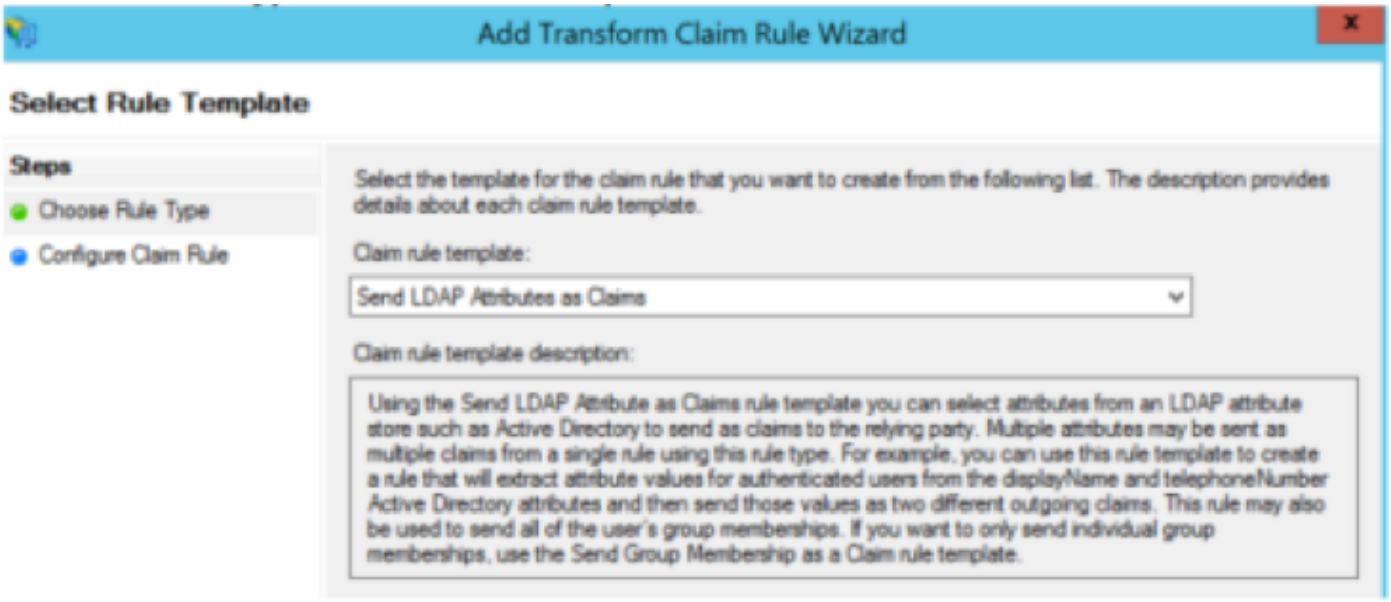
Passaggio 4. Rimuovere le informazioni evidenziate. Alla fine il file di metadati deve essere come mostrato nell'immagine.

```
<?xml version="1.0"?>
<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
      xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
      xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
      entityID="sma.mexesa.com">
  <SPSSODescriptor
      AuthnRequestsSigned="false"  WantAssertionsSigned="true"
      protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <KeyDescriptor use="signing">
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Data>
          <ds:X509Certificate>
MIIDZTCCAk2gAwIBAwIJAOjXJ35sNw2bMA0GCSqGSIb3DQEBCwUAMHIxCzAJBgNV
BAYTAk1YMRcwFQYDVQQDDA5zbWEubWV4ZXNhLmNvbTENMAsGA1UEBwwEQ0RNWDEW
MBQGA1UECgwNVGl6b25jaXRvIEluYzENMAsGA1UECAwEQ0RNWDEUMBIGA1UECwwL
SVQgU2VjdXJpdHkwHhcNMTkwNjA1MjEwNTUxWhcNMjAwNjA0MjEwNTUxWjByMQsw
CQYDVQQGEwJNWDEXMBUGA1UEAwwOc21hLm1leGVzYS5jb20xDTALBgNVBAcMBENE
TVgxFjAUBgNVBAoMDVRpem9uY2l0byBJbmMxDTALBgNVBAgMBENETVgxFDASBgNV
BAsMC0lUIFNlY3VyaXR5MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
g7kzRmL114q9TlklcTJzo8cmscu5nRXFWlohFPcJgn/oHXEUKvUnWe+9cTJQ41X4
ojbGCP75UjD8GdPczkuBxqAZgkrfgNLR8mopsxTFVWb5x68tVsTBGFNyv8Wtd+Io
MVowJ9h9Kju7kSXuYHU1BYoxfPOLyzHHcbAVYKuPM4Fi7y4jwj6rnO4jtvpZPj7B
cpWjawLlxAfUHVyvrc661Tblo0exG+hZ+AlS3B0l+6lmTNjF3IcGcGS/TE0chETx
glScUk0iMipnPEtAZey/ebyh18EpH/WViNwZkMUjINvmIFq3+LkF8As8B1Pm6YHi
L6K8W4vOEj1njtmnC/EQIQIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQBy3vxNL7jb
emMTKSRP4hycU1d69z2xGQC5e2EeyhnRgHUz7F/TEv0NkORotFii2oOJ6yGEOdWD
6+Bvj6wSBp7UoLyBdCxglyi+vK4Y/R2+iCv13pyaXkbf0QSJvYpzOg7xSjkxZm79
+ZIjQkekyCAM5N0Of1ZRrJ9oGD5qoYlZjhuD7NHmRBj7LKHRKsFVqpKet/tTXCH7
7EuB+ogT7pvrTDJ/QoIKcvYkbXuZ30JNVPxxKacjAVj/Zc1XnPBGSMxeo277ECJq
ix5aXRSxOMRRtD/72FVRAsgT3x1mBYqu/HTyOBZonGM+isJHBhRZxSOMBL+45jFY
PO1jBG5MZuWE
          </ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </KeyDescriptor>
    <KeyDescriptor use="encryption">
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Data>
          <ds:X509Certificate>
MIIDZTCCAk2gAwIBAwIJAOjXJ35sNw2bMA0GCSqGSIb3DQEBCwUAMHIxCzAJBgNV
BAYTAk1YMRcwFQYDVQQDDA5zbWEubWV4ZXNhLmNvbTENMAsGA1UEBwwEQ0RNWDEW
MBQGA1UECgwNVGl6b25jaXRvIEluYzENMAsGA1UECAwEQ0RNWDEUMBIGA1UECwwL
SVQgU2VjdXJpdHkwHhcNMTkwNjA1MjEwNTUxWhcNMjAwNjA0MjEwNTUxWjByMQsw
```

Passaggio 5. Passare all'ADFS e importare il file di metadati modificato in **Strumenti ADFS > Gestione ADFS > Aggiungi attendibilità componente**, come mostrato nell'immagine.



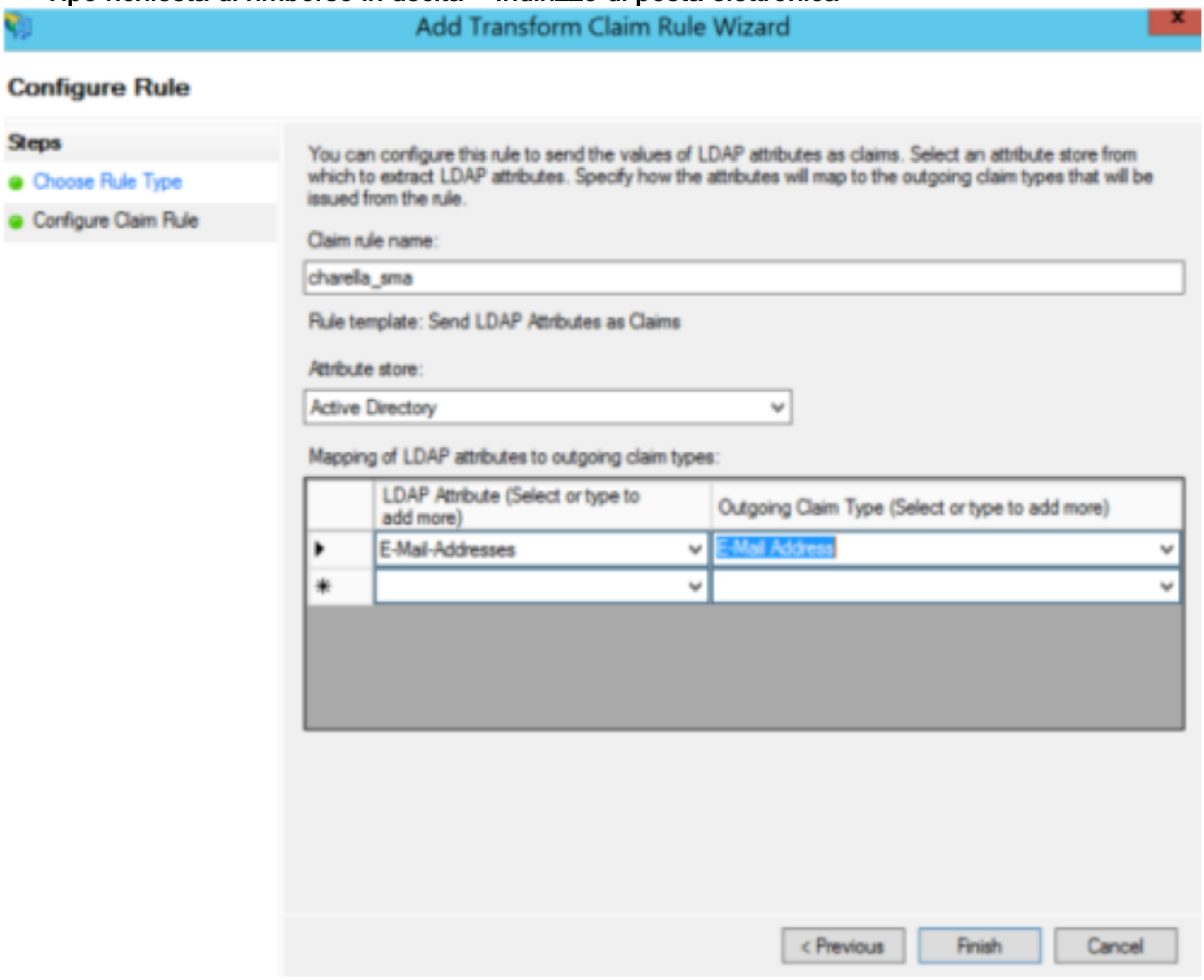
Passaggio 6. Dopo aver importato correttamente il file di metadati, configurare le regole attestazione per l'attendibilità componente appena creata, selezionare **Modello di regola attestazione > Invia attributi LDAP**, come mostrato nell'immagine.



Passaggio 7. Assegnare un nome alla regola di attestazione e selezionare **Archivio attributi > Active Directory**.

Passaggio 8. Mappare gli attributi LDAP, come mostrato nell'immagine.

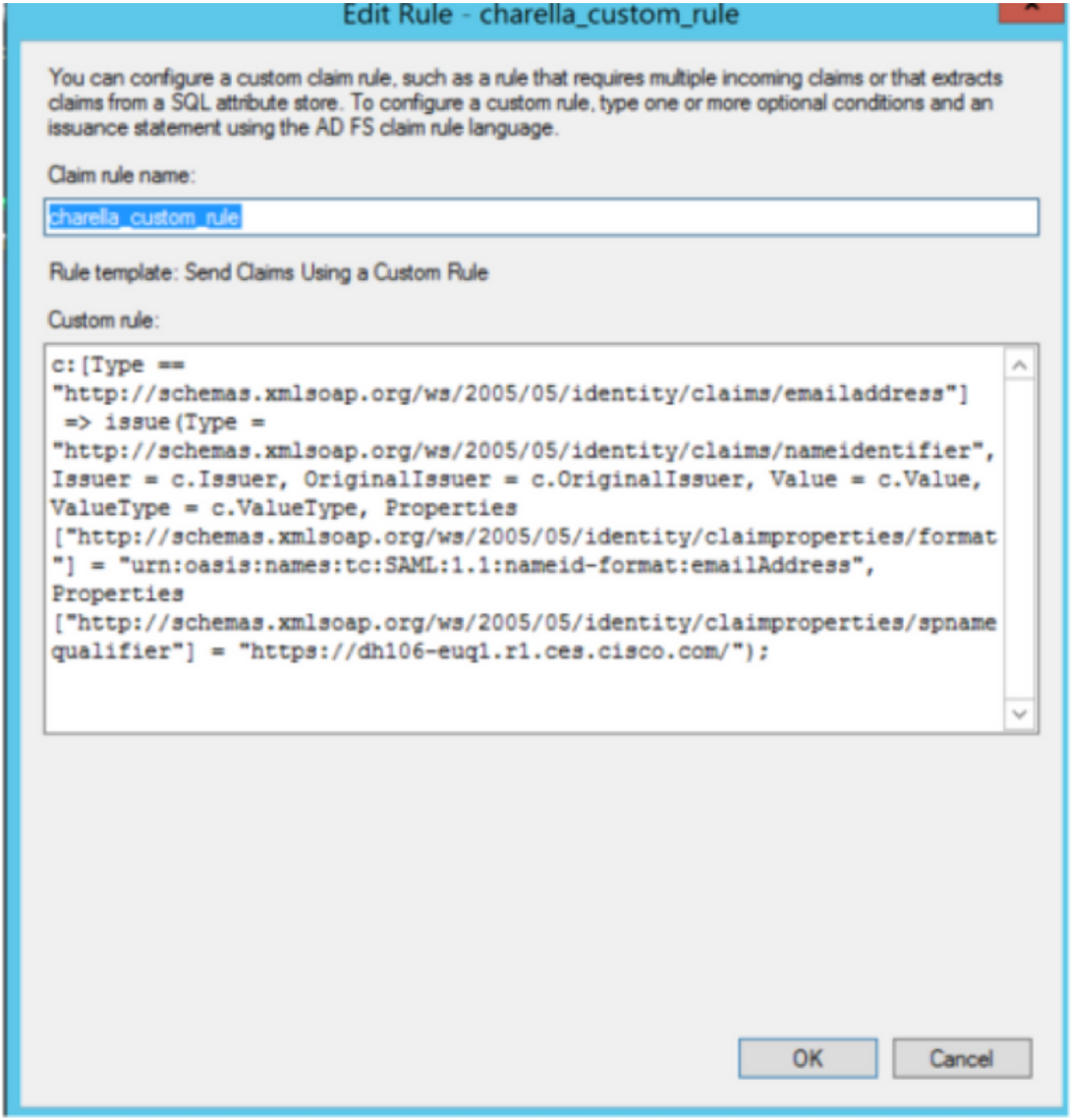
- **Attributo LDAP > Indirizzi di posta elettronica**
- **Tipo richiesta di rimborso in uscita > Indirizzo di posta elettronica**



Passaggio 9. Creare una nuova regola attestazione personalizzata con queste informazioni, come illustrato nell'immagine.

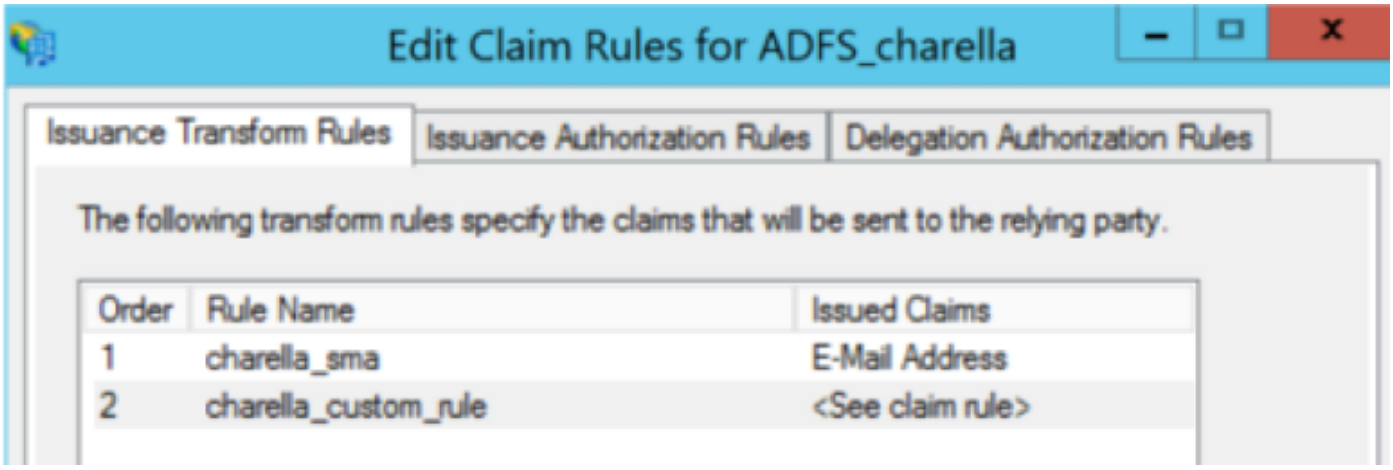
Regola personalizzata da aggiungere alla regola Attestazione personalizzata:

```
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",
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier
"] = "https://<smahostname>:83");
```



- Modificare l'URL evidenziato con il nome host e la porta SMA (se si utilizza un ambiente CES, una porta non è necessaria ma deve puntare a euq1.<allocation>.iphmx.com)

Passaggio 10. Verificare che l'ordine delle regole attestazione sia: Prima regola attestazione LDAP e seconda regola attestazione personalizzata, come mostrato nell'immagine.



Passaggio 11. Accedere all'EUQ, che deve essere reindirizzato all'host ADFS.

Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

Informazioni correlate

- CSCvh30183
- Documentazione e supporto tecnico – Cisco Systems