

# Installare il file di metadati in ADFS

## Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Informazioni correlate](#)

## 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) 2.0 Ping Identity PingFederate 7.2 Cisco 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.

The screenshot shows the Cisco SMA configuration interface. At the top, there are tabs for 'Management Appliance', 'Email', and 'Web'. Below these are 'Centralized Services', 'Network', and 'System Administration'. The 'SAML' section is active. Under 'Service Provider', there is a table with the following data:

SP Profile Name	Entity ID	Assertion Consumer URL	Metadata	Delete
MyLab_SAML	sma.mexesa.com	https://sma.mexesa.com:83/	Download Metadata	

Below the table is the 'Identity Provider' section, which is currently empty. A dialog box titled 'Opening MyLab\_SAML\_metadata.xml' is overlaid on the interface, showing the file name and type, and asking for the action to take. The 'Save File' option is selected.

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.

```

1  <?xml version="1.0"?>
2  <EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
3      xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
4      xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
5      entityID="sma.mexesa.com">
6      <SPSSODescriptor
7          AuthnRequestsSigned="false" WantAssertionsSigned="true"
8          protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
9          <KeyDescriptor use="signing">
10             <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
11                 <ds:X509Data>
12                     <ds:X509Certificate>Bag Attributes
13                         localKeyID: D5 4F B4 DA BC 91 71 5C 53 94 4A 78 E0 4A C3 EF C4 BD 4C 8D
14                         friendlyName: sma.mexesa.com
15                         subject=/C=MX/CN=sma.mexesa.com/L=CDMX/O=Tizoncito Inc/ST=CDMX/OU=IT Security
16                         issuer=/C=MX/CN=sma.mexesa.com/L=CDMX/O=Tizoncito Inc/ST=CDMX/OU=IT Security
17                         -----BEGIN CERTIFICATE-----
18                         MIIDZTCCAk2gAwIBAwIJA0jXJ35sNw2bMA0GCSqGSIb3DQEBCwUAMHlxZAJBgNV
19                         BAYTAK1YMRcwFQYDVQQDDA5zbWEubWV4ZXXNhLmNvbTENCAsGA1UEBwwEQ0RNWDEW
20                         MBQGA1UECgwNVG16b25jaXRvIEluYzENMAsGA1UECAwEQ0RNWDEUMBIGA1UECwwL
21                         SVQgU2VjdXJpdHkwHhcNMjkwNjA0MjEwMjEwMjEwMjEwMjEwMjEwMjEwMjEwMjEw
22                         CQYDVQQGEwJNWDEwMjEwMjEwMjEwMjEwMjEwMjEwMjEwMjEwMjEwMjEwMjEwMjEw
23                         TVGxZjAUBG9wMjEwMjEwMjEwMjEwMjEwMjEwMjEwMjEwMjEwMjEwMjEwMjEwMjEw
24                         BAsMC0lUIFNlY3VyaXR5MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
25                         g7kzRmL114q9TlklcTJzo8cmscu5nRXFWlohFpcJgn/oHXEUKvUnWe+9cTJQ41X4
26                         ojbGCP75UjD8GdPczkuBxqAZgkrfgNLR8mopsxTFVWb5x68tVsTBGFNyw8Wtd+Io
27                         MVowJ9h9Kju7kSXuYHU1BYoxfPOLyzHHcbAVYKuPM4Fi7y4jwj6rn04jtvPZp7B
28                         cpWjawLlxAfUHVyvrC661Tblo0exG+hZ+AlS3B01+61mTNjF3IcGcGS/TE0chETx
29                         glScUk0iMipnPEtAZey/ebyh18EpH/WViNwZkMUjINvmIFq3+LkF8As8B1Pm6YHi
30                         L6K8W4vOEj1njtmnC/EQIQIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQB3vxNL7jb
31                         emMTKSRP4hycUld69z2xGQC5e2EeyhnRgHUz7F/TEv0NkORotFii2oOJ6yGEOdWD
32                         6+Bvj6wSBp7UoLyBdCcxglyi+vK4Y/R2+iCv13pyaXkbf0QsJvYpzOg7xSjKxZm79
33                         +ZiJQkekyCAM5N0of1ZRrJ9oGD5qoYlZjhuD7NHmRbj7LKHrKsFVqpKet/tTXCH7
34                         7EuB+ogT7pvrTDJ/QoIKcvYkbXuZ30JNVPxxKacjAVj/ZclXnPBGSMxexo277ECJq
35                         ix5aXRSxOMRRtD/72FVRAsGT3x1mBYqu/HTyOBZongM+isJHBhRZxSOMBL+45jFY
36                         PO1jBG5MZuWE
37                         -----END CERTIFICATE-----
38                     </ds:X509Certificate>
39                 </ds:X509Data>

```

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

```
1  <?xml version="1.0"?>
2  <EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
3      xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
4      xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
5      entityID="sma.mexesa.com">
6      <SPSSODescriptor
7          AuthnRequestsSigned="false" WantAssertionsSigned="true"
8          protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
9          <KeyDescriptor use="signing">
10             <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
11                 <ds:X509Data>
12                     <ds:X509Certificate>
13 MIIDZTCCAk2gAwIBAwIJA0jXJ35sNw2bMA0GCSqGSIb3DQEBCwUAMHIXCzAJBgNV
14 BAYTAK1YMRcwFQYDVQQDDA5zbWEubWV4ZlZlLnVzTENMAAGA1UEBwwEQ0RNWDEW
15 MBQGA1UECgwNVG16b25jaXRvIELuYzENMAAGA1UECAwEQ0RNWDEUMBIGA1UECwwL
16 SVQGU2VjdXJpdHkwHhcNMTkwNjA1MjEwNTUxWWhcNMjAwNjA0MjEwNTUxWjByMQsw
17 CQYDVQQGEwJNWDEwMDVBRmVudm9uY210byBjb20xDTALBgNVBAAcMBENE
18 TVGxVjAUBGNVBAoMDVRpem9uY210byBjb20xDTALBgNVBAAcMBENETVgxFDASBgNV
19 BAsMC0lUIFNlY3VyaXR5MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
20 g7kzRmL114q9TlklcTJzo8cmscu5nRXFWlohFPcJgn/oHXEUKvUnWe+9cTJQ41X4
21 ojbGCP75UjD8GdPczkuBxqAZgkrfgNLR8mopsxTFVWb5x68tVsTBGFNv8Wtd+Io
22 MVowJ9h9Kju7kSXuYHU1BYoxfPOLyzHHcbAVYKuPM4Fi7y4jwj6rnO4jtvPZPj7B
23 cpWjawLlxAfUHVvrc661Tblo0exG+hZ+AlS3B0l+6lmTNjF3IcGcGS/TE0chETx
24 glScUk0iMipnPEtAZey/ebyh18EpH/WViNwZkMUjINvmIFq3+LkF8As8B1Pm6YHi
25 L6K8W4voEj1njtmnC/EQIQIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQB3vXNL7jb
26 emMTKSRP4hycUld69z2xGQC5e2EeyhnRgHUz7F/TEv0NkORotFii2oOJ6yGEOdWD
27 6+Bvj6wSBp7UoLyBdCxglyi+vK4Y/R2+iCv13pyaXkbF0QsJvYpzOg7xSjKxZm79
28 +ZIjQkekyCAM5N0of1ZRrJ9oGD5qoYlZjhud7NHmRbj7LKHRSFVqpKet/tTXCH7
29 7EuB+ogT7pvrTDJ/QoIKcvYkbXuZ30JNVPxxKacjAVj/Zc1XnPBGSMxex277ECJq
30 ix5aXRSxOMRRtD/72FVRASgT3xlmBYqu/HTyOBZonGM+isJHBhRZxSOMBL+45jFY
31 PO1jBG5MZuWE
32             </ds:X509Certificate>
33         </ds:X509Data>
34     </ds:KeyInfo>
35 </KeyDescriptor>
36 <KeyDescriptor use="encryption">
37     <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
38         <ds:X509Data>
39             <ds:X509Certificate>
40 MIIDZTCCAk2gAwIBAwIJA0jXJ35sNw2bMA0GCSqGSIb3DQEBCwUAMHIXCzAJBgNV
41 BAYTAK1YMRcwFQYDVQQDDA5zbWEubWV4ZlZlLnVzTENMAAGA1UEBwwEQ0RNWDEW
42 MBQGA1UECgwNVG16b25jaXRvIELuYzENMAAGA1UECAwEQ0RNWDEUMBIGA1UECwwL
43 SVQGU2VjdXJpdHkwHhcNMTkwNjA1MjEwNTUxWWhcNMjAwNjA0MjEwNTUxWjByMQsw
```

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

## Add Relying Party Trust Wizard

### Select Data Source

**Steps**

- Welcome
- Select Data Source
- Configure Multi-factor Authentication Now?
- Choose Issuance Authorization Rules
- Ready to Add Trust
- Finish

Select an option that this wizard will use to obtain data about this relying party:

Import data about the relying party published online or on a local network

Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata online or on a local network.

Federation metadata address (host name or URL):

Example: fs.contoso.com or https://www.contoso.com/app

Import data about the relying party from a file

Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file.

Federation metadata file location:

Enter data about the relying party manually

Use this option to manually input the necessary data about this relying party organization.

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.

## Add Transform Claim Rule Wizard

### Select Rule Template

**Steps**

- Choose Rule Type
- Configure Claim Rule

Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.

Claim rule template:

Claim rule template description:

Using the Send LDAP Attribute as Claims rule template you can select attributes from an LDAP attribute store such as Active Directory to send as claims to the relying party. Multiple attributes may be sent as multiple claims from a single rule using this rule type. For example, you can use this rule template to create a rule that will extract attribute values for authenticated users from the displayName and telephoneNumber Active Directory attributes and then send those values as two different outgoing claims. This rule may also be used to send all of the user's group memberships. If you want to only send individual group memberships, use the Send Group Membership as a Claim rule template.

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

**Add Transform Claim Rule Wizard**

### Configure Rule

**Steps**

- Choose Rule Type
- Configure Claim Rule

You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name:

Rule template: Send LDAP Attributes as Claims

Attribute store:

Mapping of LDAP attributes to outgoing claim types:

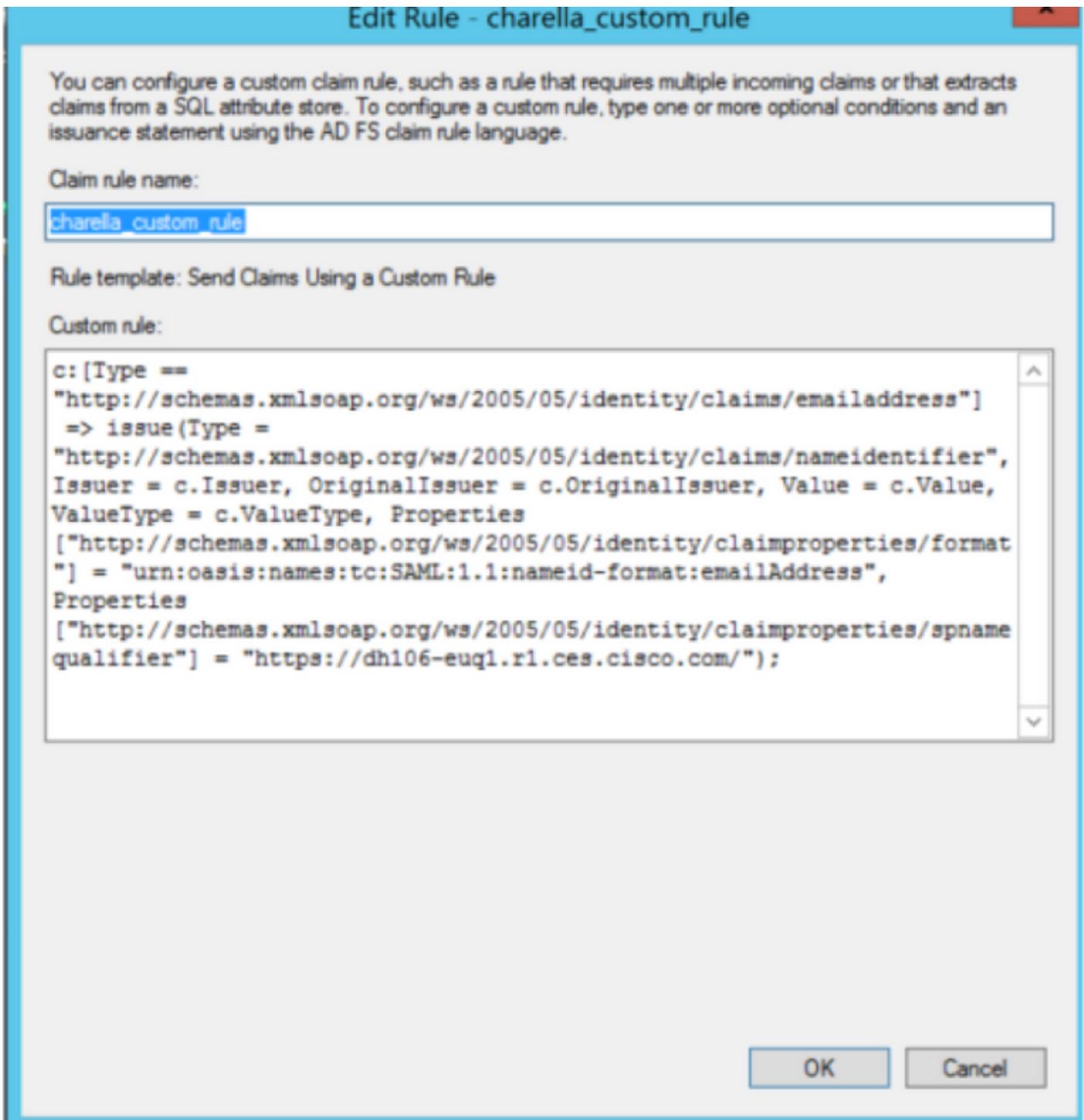
	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
▶	E-Mail-Addresses	E-Mail Address
*		

< Previous   Finish   Cancel

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

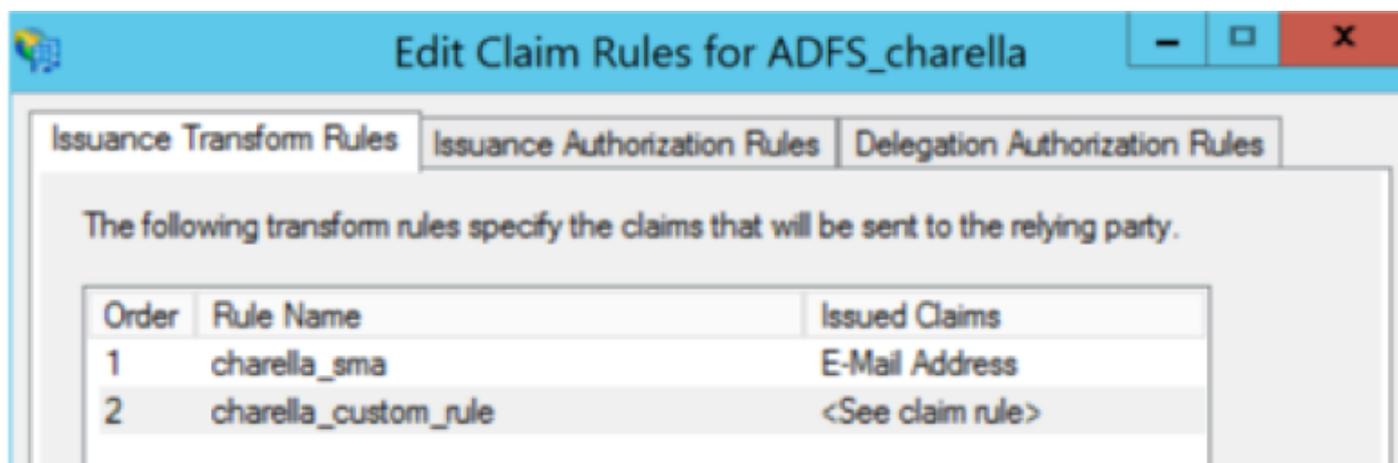
Regola personalizzata da aggiungere alla regola Attestazione personalizzata:

```
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](#)