

Configurare il provider di identità per Cisco Identity Service per abilitare SSO

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Panoramica di SSO](#)

[Panoramica della configurazione](#)

[Configurazione](#)

[Tipi di autenticazione](#)

[Stabilisci relazione di trust](#)

[ADFS 2.0](#)

[ADFS 3.0](#)

[Abilita asserzioni SAML firmate per attendibilità componente \(Cisco IdS\)](#)

[Per una configurazione multidominio per ADFS federati](#)

[Configurazione ADFS federata](#)

[Configurazione ADFS primaria](#)

[Rollover automatico dei certificati ADFS](#)

[Autenticazione Kerberos \(autenticazione integrata di Windows\)](#)

[Configurazione per il supporto di Microsoft Internet Explorer per IWA](#)

[Configurazione richiesta per Mozilla Firefox per il supporto IWA](#)

[Configurazione richiesta per Google Chrome per il supporto IWA](#)

[Ulteriore configurazione per SSO](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[URL di bypass/recupero UCCX SSO](#)

[Disabilita SSO](#)

[Acquisizioni schermo](#)

[Amministrazione CCX - Non SSO](#)

[Amministrazione CCX - SSO abilitato](#)

[Accesso Finesse - Non SSO](#)

[Accesso Finesse - SSO abilitato](#)

[CUIC - Non SSO](#)

[CUIC - SSO abilitato](#)

Introduzione

Questo documento descrive la configurazione del provider di identità (IdP) per Cisco Identity Service (IdS) per abilitare Single Sign-On (SSO).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Unified Contact Center Express (UCCX) versione 11.5 o Cisco Unified Contact Center Enterprise versione 11.5 o Packaged Contact Center Enterprise (PCCE) versione 11.5, a seconda dei casi
- Microsoft Active Directory - AD installato in Windows Server
- Active Directory Federation Service (ADFS) versione 2.0/3.0

Nota: questo documento fa riferimento a UCCX nelle immagini e negli esempi visualizzati sullo schermo, tuttavia la configurazione è simile a quella degli ID Cisco (UCCX/UCCE/PCCE) e dell'IDP.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

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

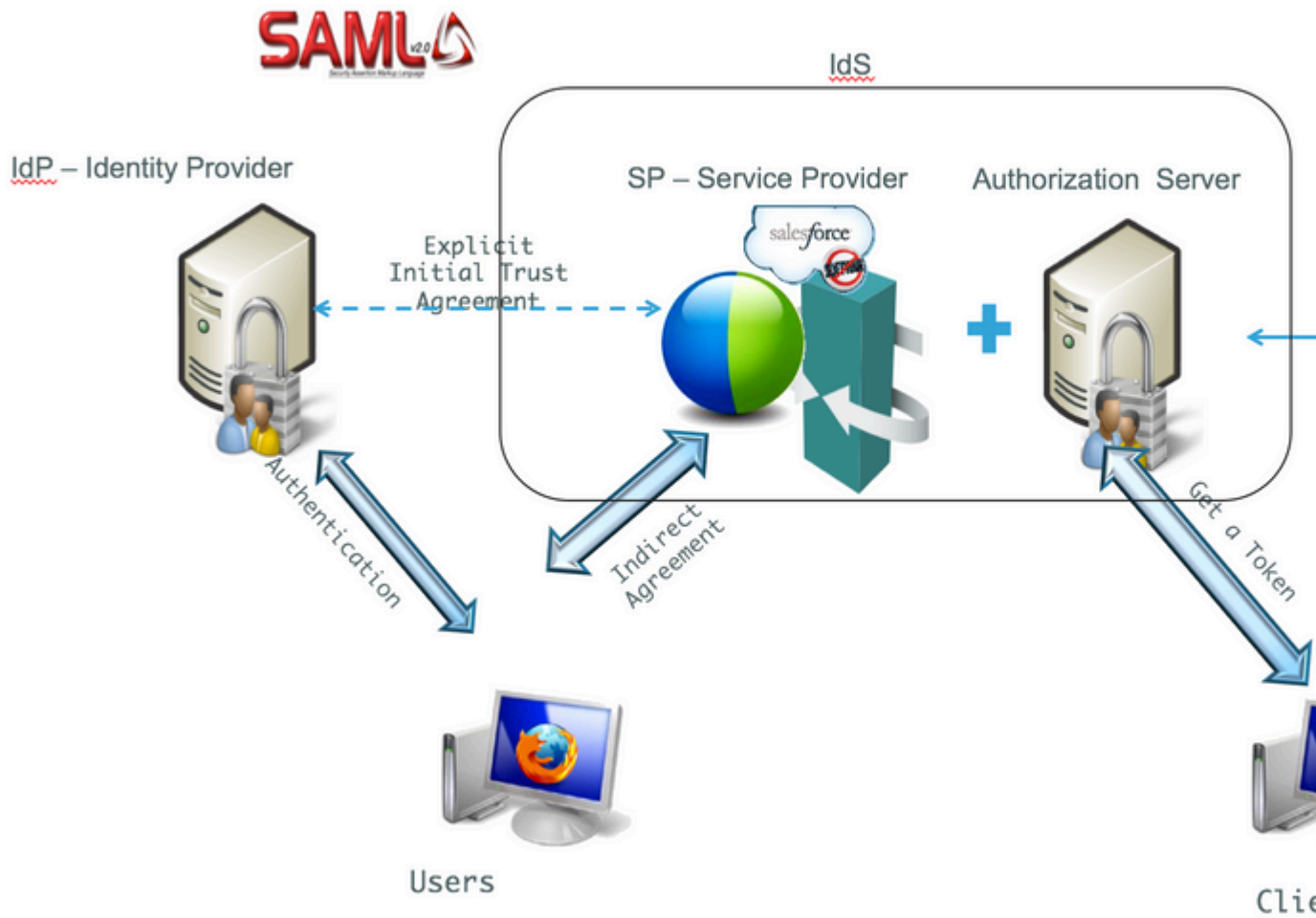
Modelli di distribuzione Cisco IdS

| Prodotto | Implementazione |
|----------|---|
| UCCX | Coresidente |
| PCCE | Coresidente con CUIC (Cisco Unified Intelligence Center) e LD (Live Data) |
| UCCE | Coresidenti con CUIC e LD per installazioni 2k. Standalone per installazioni a 4k e 12k. |

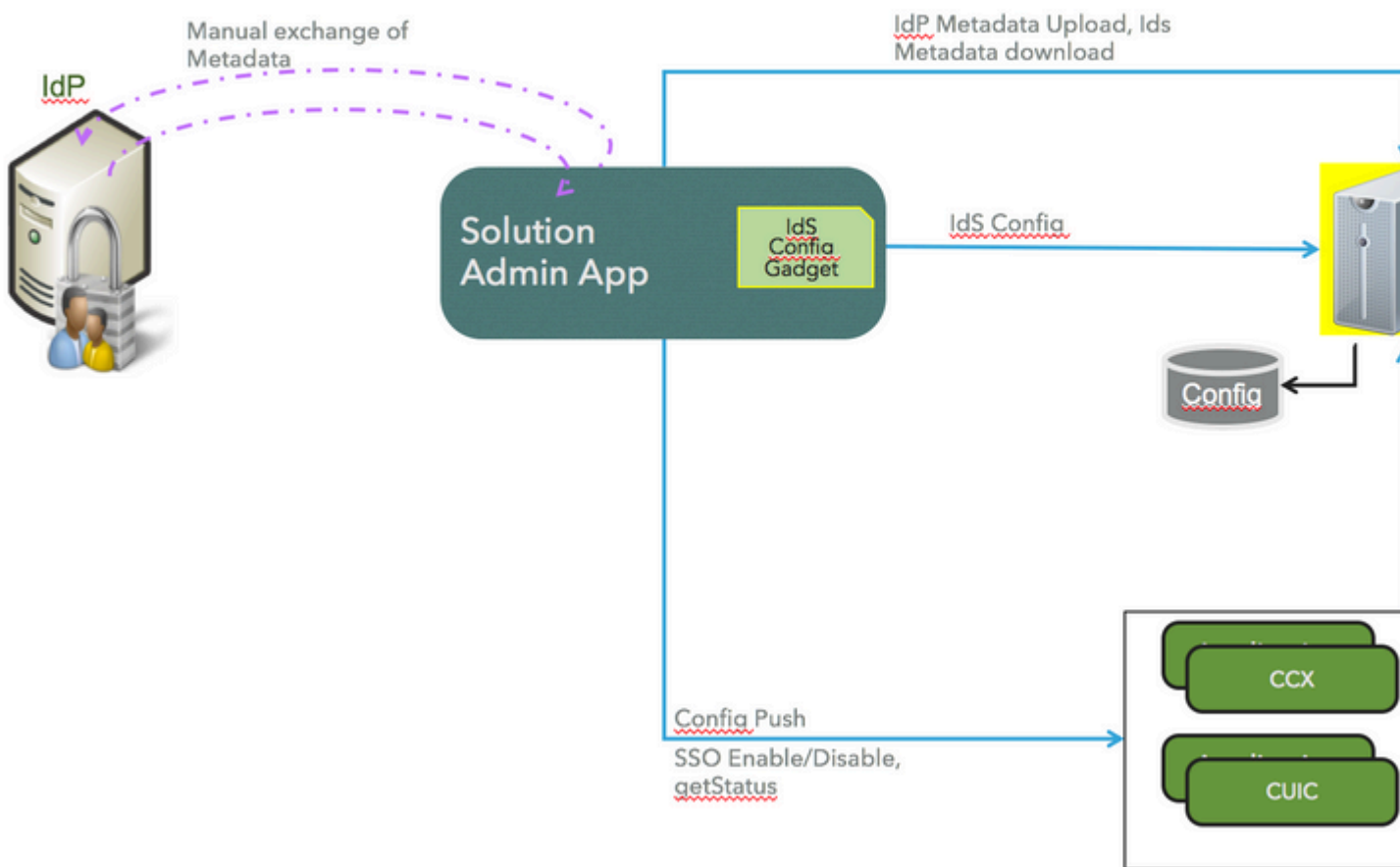
Panoramica di SSO

Cisco offre molti servizi in forme diverse e, in qualità di utente finale, si desidera accedere solo una volta per poter accedere a tutti i servizi Cisco. Per trovare e gestire i contatti di qualsiasi applicazione e dispositivo Cisco, utilizza tutte le fonti possibili (directory aziendale, Outlook, contatti mobili, Facebook, LinkedIn, cronologia) e ottieni il rendering dei contatti in modo standard e coerente, in modo da ottenere le informazioni necessarie per conoscere la loro disponibilità e come contattarli al meglio.

L'SSO con SAML (Security Assertion Markup Language) soddisfa questo requisito. SAML/SSO consente agli utenti di accedere a più dispositivi e servizi tramite un account e un'identità di autorizzazione comuni denominati IdP. La funzionalità SSO è disponibile in UCCX/UCCE/PCCE a partire dalla versione 11.5.



Panoramica della configurazione



Configurazione

Tipi di autenticazione

Cisco IdS supporta solo l'autenticazione basata su form degli IdP.

Per informazioni su come abilitare l'autenticazione basata su form in ADFS, fare riferimento a questi articoli di MSDN.

- Per ADFS 2.0 fare riferimento a questo articolo di Microsoft TechNet, <http://social.technet.microsoft.com/wiki/contents/articles/1600.ad-fs-2-0-how-to-change-the-local-authentication-type.aspx>.
- Per ADFS 3.0 fare riferimento a questo articolo di Microsoft TechNet, <https://learn.microsoft.com/en-us/archive/blogs/josrod/enabled-forms-based-authentication-in-adfs-3-0>

Nota: Cisco IdS 11.6 e versioni successive supportano sia l'autenticazione basata su form che l'autenticazione Kerberos. Affinché l'autenticazione Kerberos funzioni, è necessario disabilitare l'autenticazione basata su form.

Stabilisci relazione di trust

Per l'onboarding e per consentire alle applicazioni di utilizzare Cisco IdS per SSO, eseguire lo scambio di metadati tra IdS e IdP.

- Scaricare il file dei metadati di SAML SP `sp.xml`.
- Da Settings, passare a IdS Trust nella pagina Gestione IdS.

Identity Service Management

Settings

IdS Trust

Download SAML SP Metadata

Begin configuring the trust relationship between the Identity Provider(IdP) and the Identity Server (IdS) by obtaining a SAML SP metadata file from the IdS Server. Use this metadata to configure trust relationship in Identity Provider (IdP).

[Download Metadata File](#)

- Scaricare il file di metadati IdP dal provider di identità dall'URL:
<https://<ADFSServer>/federationmetadata/2007-06/federationmetadata.xml>
- Nella pagina Gestione IdS, caricare il file di metadati IdP scaricato nel passaggio precedente.

Settings

IdS Trus



Nodes



Settings



Clients



Upload IdP Metadata

Establish the trust relationship between the Identity Provider (IdP) and the Identity Service by obtaining a trust metadata file from the IdP and uploading it here.

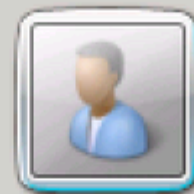
Use [file browser](#) to upload the file.

Procedura per caricare i metadati IdS e aggiungere le regole attestazione. Questa procedura è descritta per ADFS 2.0 e 3.0.

ADFS 2.0

Passaggio 1. Nel server ADFS passare a, Start > All Programs > Administrative Tools > ADFS 2.0 Management, come mostrato nell'immagine:

- Administrative Tools
 - Active Directory Administrative Center
 - Active Directory Domains and Trusts
 - Active Directory Module for Windows Po
 - Active Directory Sites and Services
 - Active Directory Users and Computers
 - AD FS 2.0 Management**
 - ADSI Edit
 - Certification Authority
 - Component Services
 - Computer Management
 - Data Sources (ODBC)
 - DNS
 - Event Viewer
 - Group Policy Management
 - Internet Information Services (IIS) Man.
 - iSCSI Initiator
 - Local Security Policy
 - Performance Monitor
 - Security Configuration Wizard
 - Server Manager



Administrator

Documents

Computer

Network

Control Panel

Devices and Printers

Administrative Tools ▶

Help and Support

Run...

Windows Security

◀ Back

Search programs and files



Log off ▶

Start



Add Relying Party Trust Wizard

Select Data Source

Steps

- Welcome
- Select Data Source
- 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 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

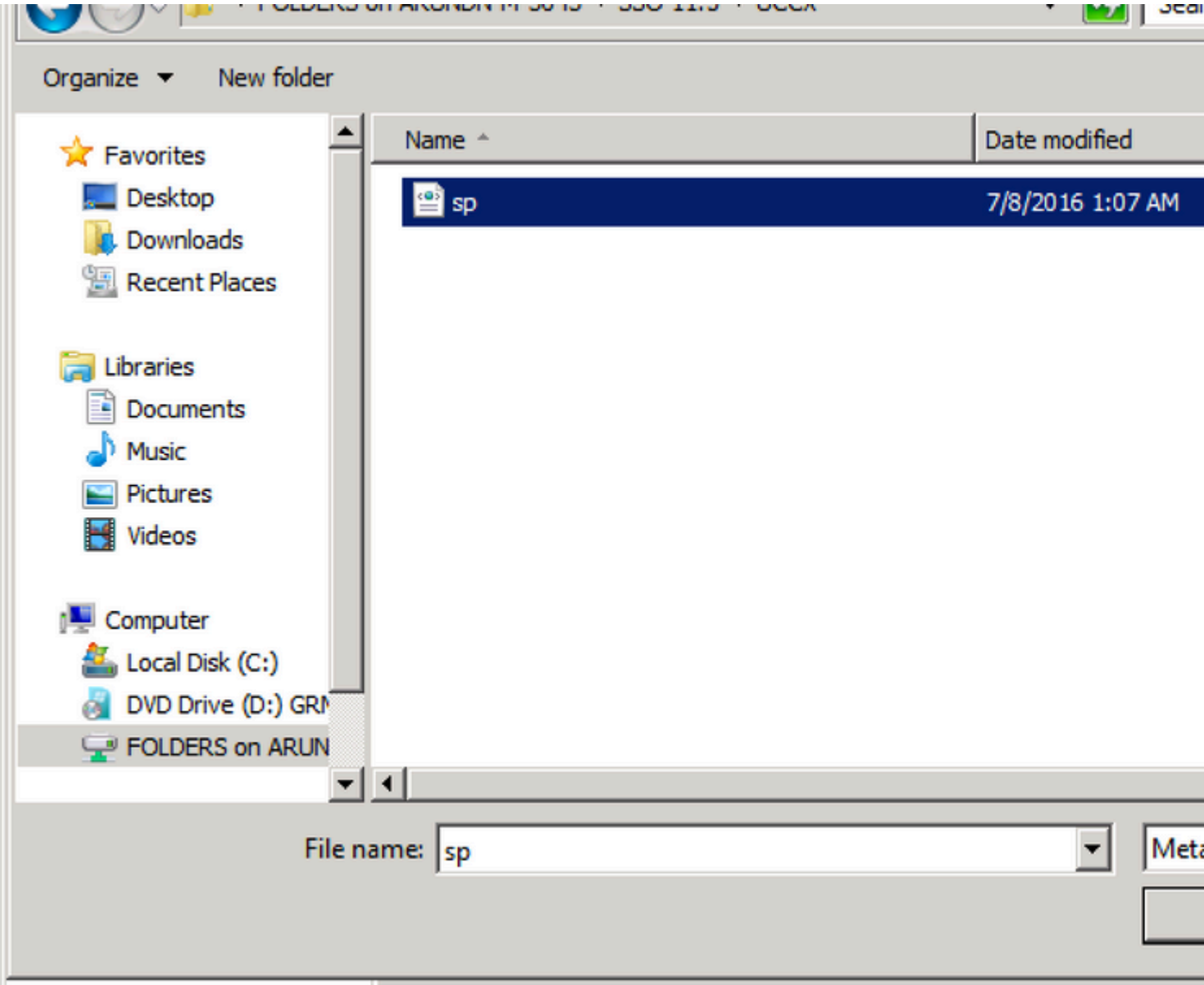
- Import data about the relying party from a file.
Use this option to import the necessary data and certificates from a relying party that has exported its federation metadata to a file. Ensure that this file is from a trusted source and do not validate the source of the file.

Federation metadata file location:

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

< Previous

Next >



Organize ▾ New folder

- ★ Favorites
 - Desktop
 - Downloads
 - Recent Places

- Libraries
 - Documents
 - Music
 - Pictures
 - Videos

- Computer
 - Local Disk (C:)
 - DVD Drive (D:) GRM
 - FOLDERS on ARUN

| Name ^ | Date modified |
|--------|---------------|
|--------|---------------|

| | |
|----|------------------|
| sp | 7/8/2016 1:07 AM |
|----|------------------|

File name:

Meta

Specify Display Name

Steps

- Welcome
- Select Data Source
- Specify Display Name
- Choose Issuance Authorization Rules
- Ready to Add Trust
- Finish

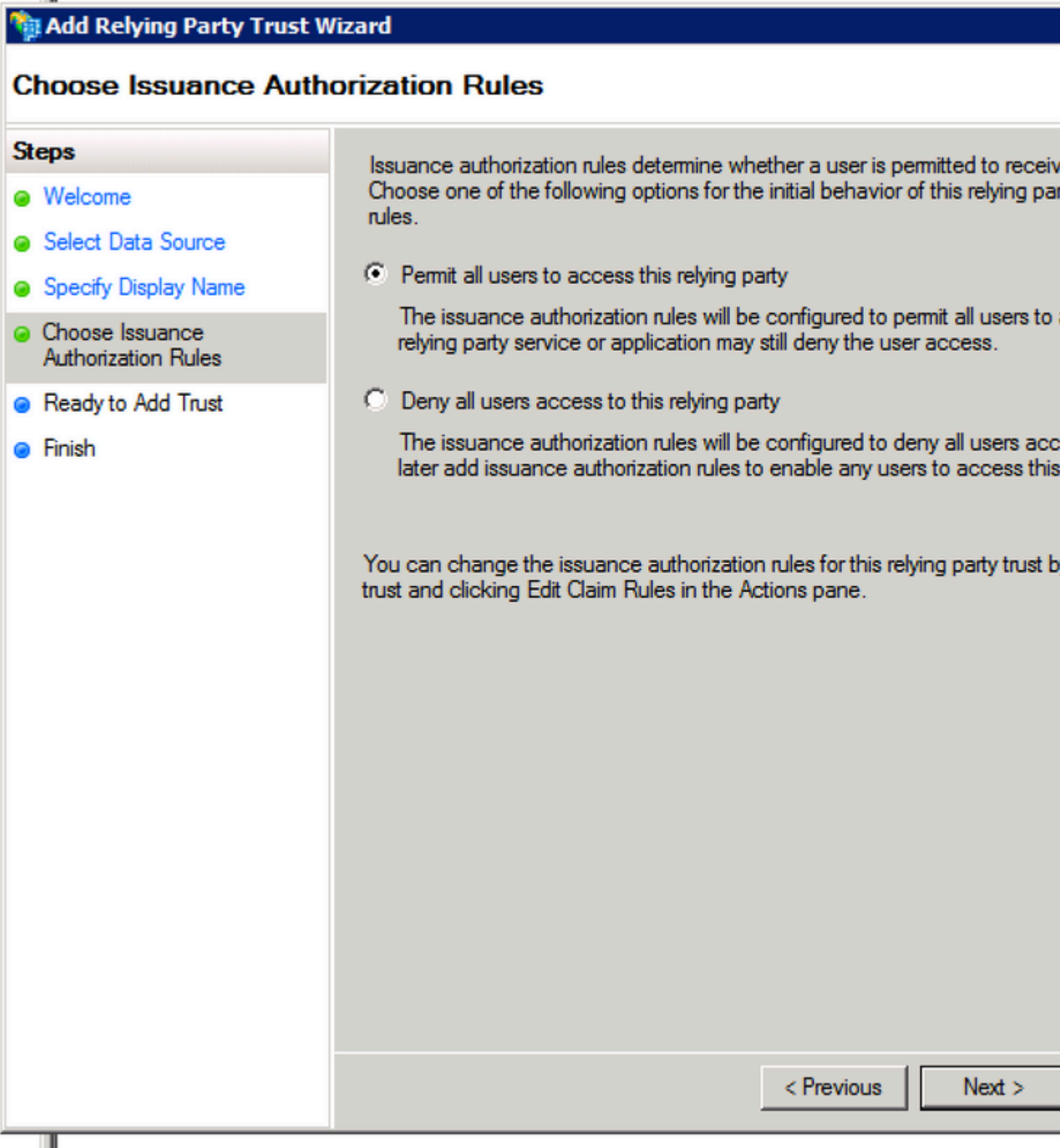
Type the display name and any optional notes for this relying party.

Display name:

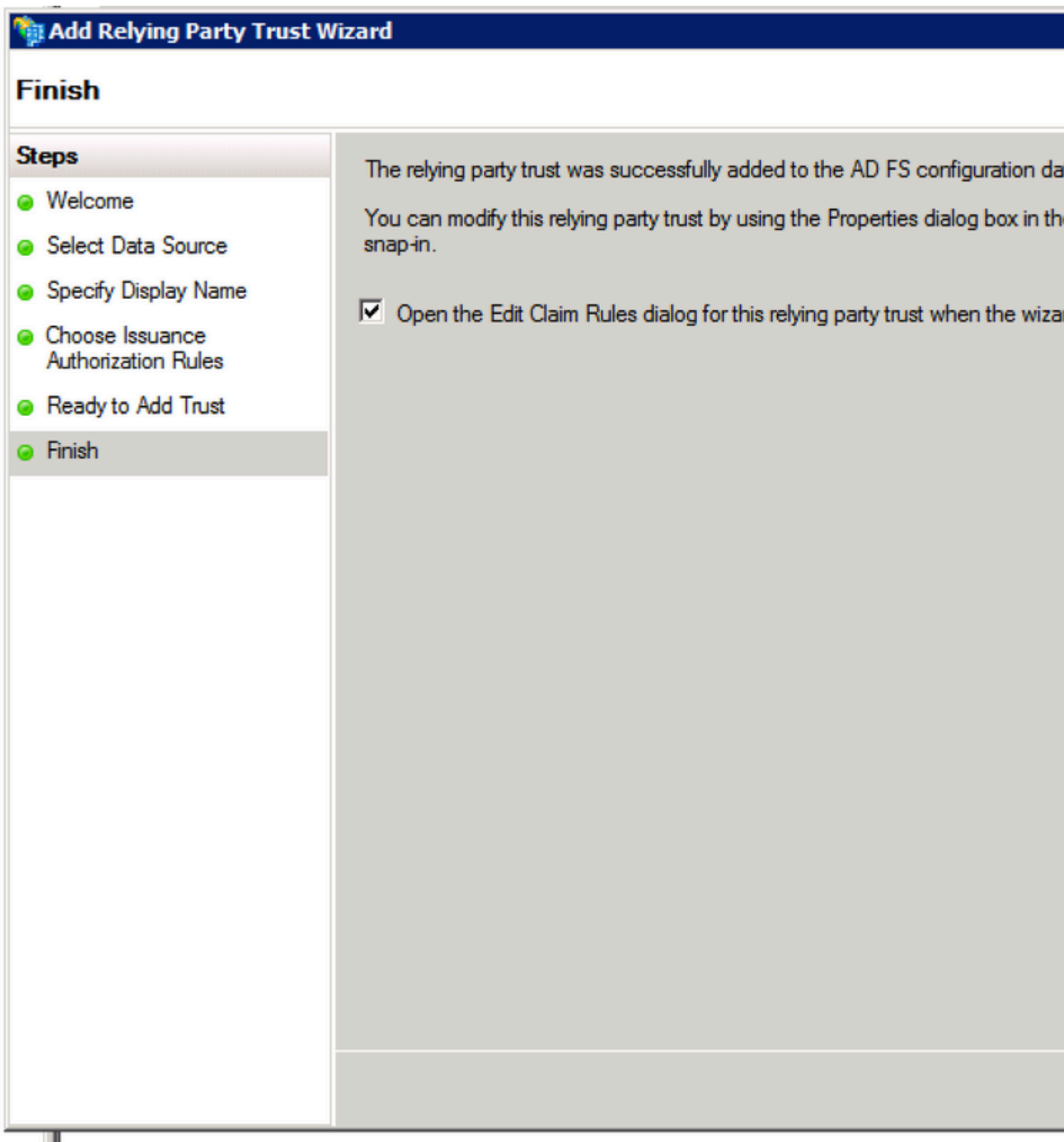
Notes:

< Previous

Next >



Passaggio 4. Completare la creazione dell'attendibilità del componente.



Passaggio 5. Nelle proprietà dell'attendibilità componente, scegliere Identifier scheda.

Relying Party Trusts

| Display Name | Enabled | Identifier |
|--------------|---------|-------------------------|
| fs. | Yes | uccx115p.uccx115eft.com |

- Update from Federation Metadata...
- Edit Claim Rules...
- Disable
- Properties**
- Delete
- Help

fs.sso.com Properties

Accepted Claims

Organization

Endpoints

Notes

Advanced

Monitoring

Identifiers

Encryption

Signature

Specify the display name and identifiers for this relying party trust.

Display name:

Relying party identifier:

Add

Example: <https://fs.contoso.com/adfs/services/trust>

Relying party identifiers:

uccx115p.uccx115eft.com

Remove

OK

Cancel

Apply

Help


Passaggio 6. Impostare l'identificatore come nome host completo di Cisco Identity Server da cui sp.xml viene

scaricato.

fs.sso.com Properties

Accepted Claims | Organization | Endpoints | Notes | Advanced
Monitoring | Identifiers | Encryption | Signature

Specify the display name and identifiers for this relying party trust.

Display name:
 

Relying party identifier:

Add

Example: <https://fs.contoso.com/adfs/services/trust>

Relying party identifiers:

Remove

OK Cancel Apply Help

Passaggio 7. Fare clic con il pulsante destro del mouse sull'attendibilità componente e quindi scegliere Edit Claim Rules.

È necessario aggiungere due regole attestazione, una quando gli attributi LDAP (Lightweight Directory Access Protocol) vengono abbinati, l'altra tramite regole attestazione personalizzate.

uid - Questo attributo è necessario per le applicazioni per identificare l'utente autenticato.

user_principal: questo attributo è richiesto dagli IdS Cisco per identificare il realm dell'utente autenticato.

Regola attestazione 1:

Aggiungere una regola per nome NameID del tipo (inviare i valori dell'attributo LDAP come attestazioni):

- Scegliere l'archivio attributi come Active Directory
- Mapping attributo LDAP User-Principal-Name a user_principal (minuscolo)
- Scegliere l'attributo LDAP da utilizzare come userId per gli utenti dell'applicazione per eseguire il login e il mapping uid (minuscolo)

Esempio di configurazione quando SamAccountName deve essere utilizzato come ID utente:

- Mappare l'attributo LDAP SamAccountName a uid.
- Mappare l'attributo LDAP User-Principal-Name a user_principal.

Configurazione di esempio quando UPN deve essere utilizzato come ID utente:

- Mappare l'attributo LDAP User-Principal-Name a uid.
- Mappare l'attributo LDAP User-Principal-Name a user_principal.

Esempio di configurazione quando PhoneNumber deve essere utilizzato come ID utente:

- Mappare l'attributo LDAP **telephoneNumber** su uid .
- Mappare l'attributo LDAP User-Principal-Name a user_principal.



- AD FS 2.0
 - Service
 - Trust Relationships
 - Claims Provider Trusts
 - Relying Party Trusts**
 - Attribute Stores

Relying Party Trusts

Edit Claim Rules for fs.sso.com

Issuance Transform Rules | Issuance Authorization Rules | Delegation A

The following transform rules specify the claims that will be sent to the r

| Order | Rule Name | Issued Claims |
|-------|-----------|---------------|
|-------|-----------|---------------|

| | | |
|--|--|--|
| | | |
|--|--|--|

Add Rule... Edit Rule... Remove Rule...

OK Cancel

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 following table provides details about each claim rule template.

Claim rule template:

Send LDAP Attributes as Claims

Claim rule template description:

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

[Tell me more about this rule template...](#)

< Previous

Next >

Configure Rule

Steps

- Choose Rule Type
- Configure Claim Rule**

You can configure this rule to send the claims which to extract LDAP attributes. Specify the LDAP attributes to be issued from the rule.

Claim rule name:

NameID

Rule template: Send LDAP Attributes as Claims

Attribute store:

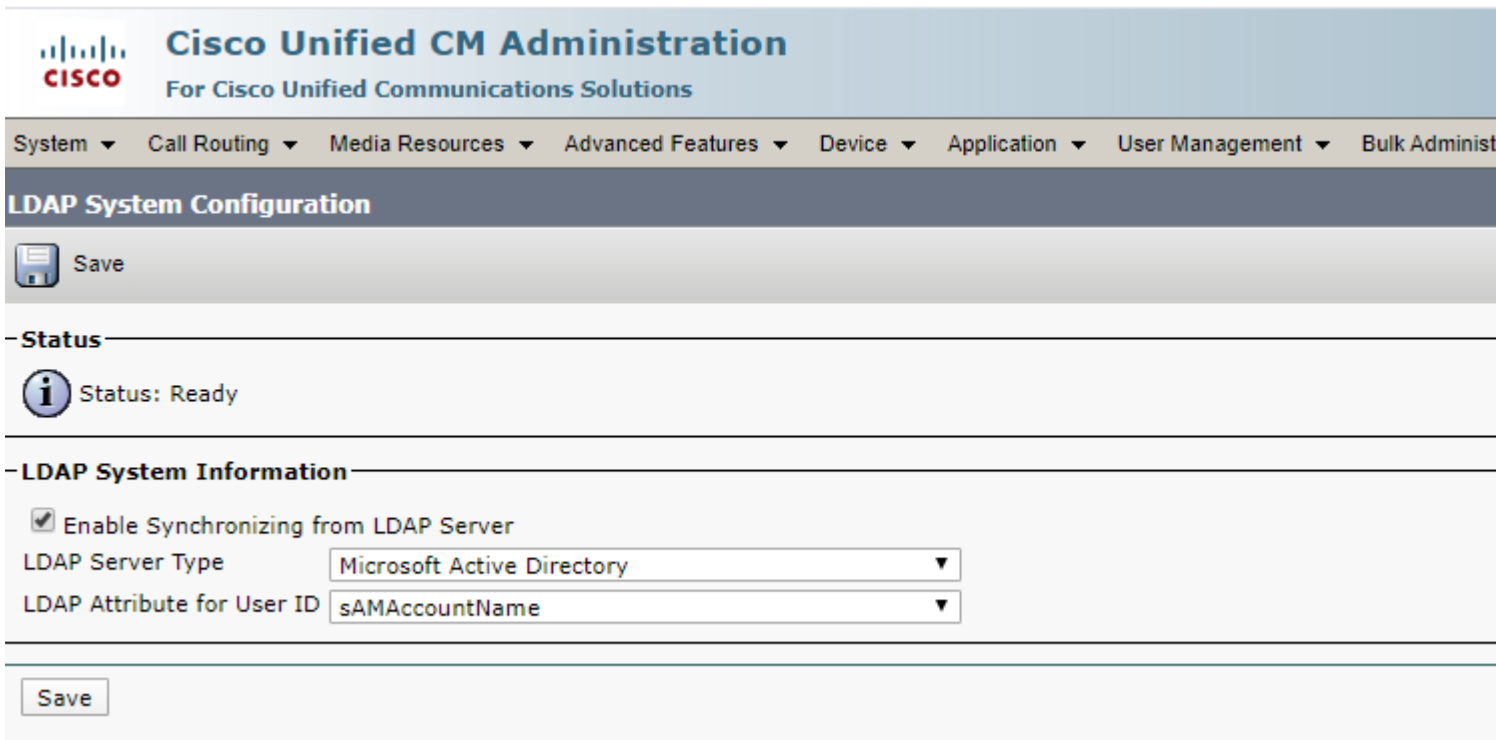
Active Directory

Mapping of LDAP attributes to outgoing claims

| | LDAP Attribute |
|---|---------------------|
| | User-Principal-Name |
| ▶ | SAM-Account-Name |
| * | |

: è necessario verificare che l'attributo LDAP configurato per l'ID utente nella sincronizzazione LDAP CUCM corrisponda a quello configurato come attributo LDAP per uid nella regola attestazione ADFS NameID. Ciò serve al corretto funzionamento del login CUIC e Finesse.

Nota: questo documento fa riferimento a vincoli relativi al nome della regola attestazione e visualizza nomi quali NomeID, Nome di dominio completo (FQDN) di UCCX e così via. Sebbene i campi e i nomi personalizzati possano essere applicabili in varie sezioni, i nomi delle regole attestazione e i nomi visualizzati vengono mantenuti standard in tutto per mantenere la coerenza e per le procedure ottimali nella convenzione di denominazione.



The screenshot shows the Cisco Unified CM Administration interface. At the top, there is a navigation menu with options: System, Call Routing, Media Resources, Advanced Features, Device, Application, User Management, and Bulk Administration. The main heading is "LDAP System Configuration". Below this, there is a "Save" button with a floppy disk icon. A section titled "Status" shows an information icon and the text "Status: Ready". Another section titled "LDAP System Information" contains a checked checkbox for "Enable Synchronizing from LDAP Server". Below this are two dropdown menus: "LDAP Server Type" set to "Microsoft Active Directory" and "LDAP Attribute for User ID" set to "sAMAccountName". A "Save" button is located at the bottom of this section.

Regola attestazione 2:

- Aggiungere un'altra regola di tipo Regola attestazione personalizzata con il nome Nome host completo di Cisco Identity Server e aggiungere il testo di questa regola.

```
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"] => issue(
```

- Nel cluster Cisco Identity Server, tutti i nomi host completi sono quelli del nodo principale o del nodo del server di pubblicazione Cisco Identity Server.
- Il nome host completo di Cisco Identity Server> fa distinzione tra maiuscole e minuscole, quindi corrisponde esattamente (maiuscole/minuscole incluse) al nome FQDN di Cisco Identity Server.
- L' <FQDN server ADFS> fa distinzione tra maiuscole e minuscole, pertanto corrisponde esattamente (inclusa la distinzione tra maiuscole e minuscole) all'FQDN ADFS.

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 list provides details about each claim rule template.

Claim rule template:

Send Claims Using a Custom Rule

Claim rule template description:

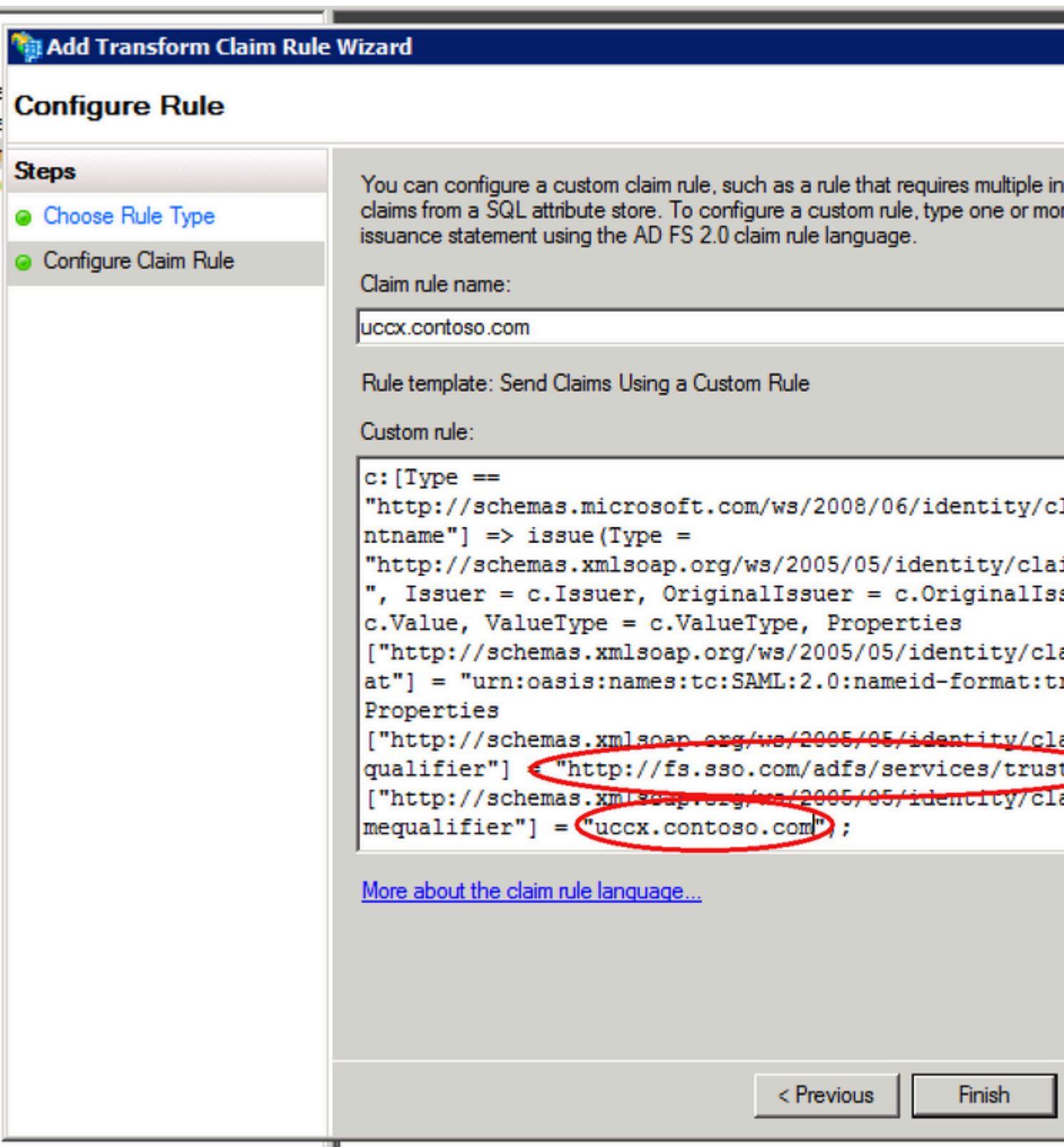
Using a custom rule, you can create rules that can't be created with a rule template written in the AD FS 2.0 claim rule language. Capabilities that require custom rules:

- Sending claims from a SQL attribute store
- Sending claims from an LDAP attribute store using a custom LDAP filter
- Sending claims from a custom attribute store
- Sending claims only when 2 or more incoming claims are present
- Sending claims only when an incoming claim value matches a complex pattern
- Sending claims with complex changes to an incoming claim value
- Creating claims for use only in later rules

[Tell me more about this rule template...](#)

< Previous

Next >



Passaggio 8. Fare clic con il pulsante destro del mouse sull'attendibilità componente e quindi scegliere Properties e scegliere la scheda avanzate, come illustrato nell'immagine.

fs.sso.com Properties

Monitoring

Identifiers

Encryption

Signature

Accepted Claims

Organization

Endpoints

Notes

Advanced

Specify the secure hash algorithm to use for this relying party trust.

Secure hash algorithm:

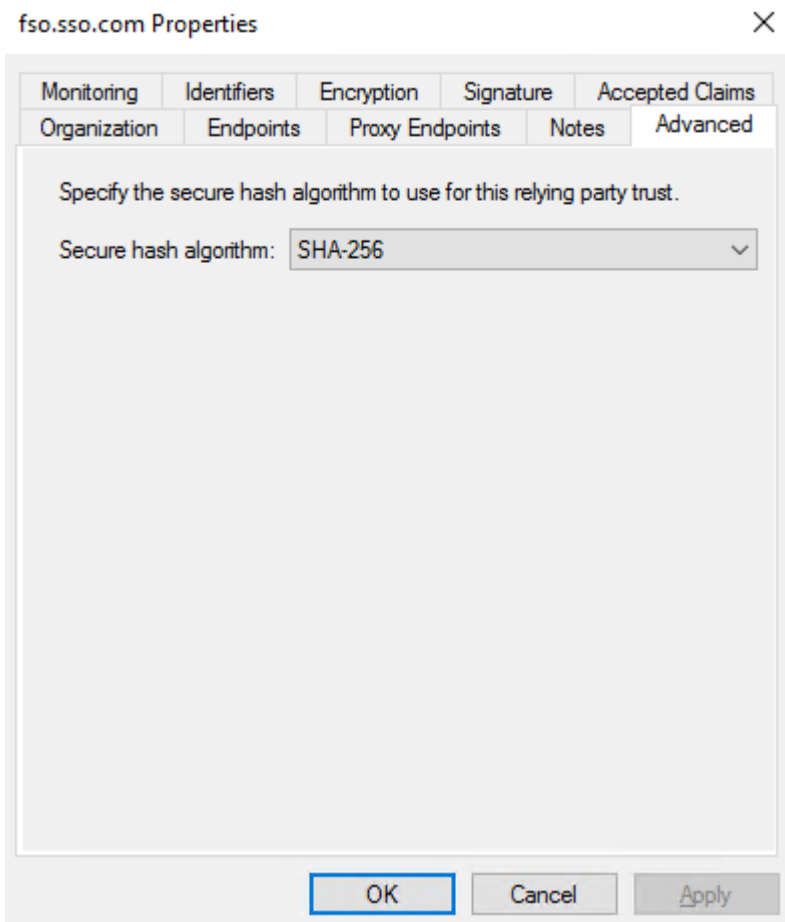
OK

Cancel

Apply

Help

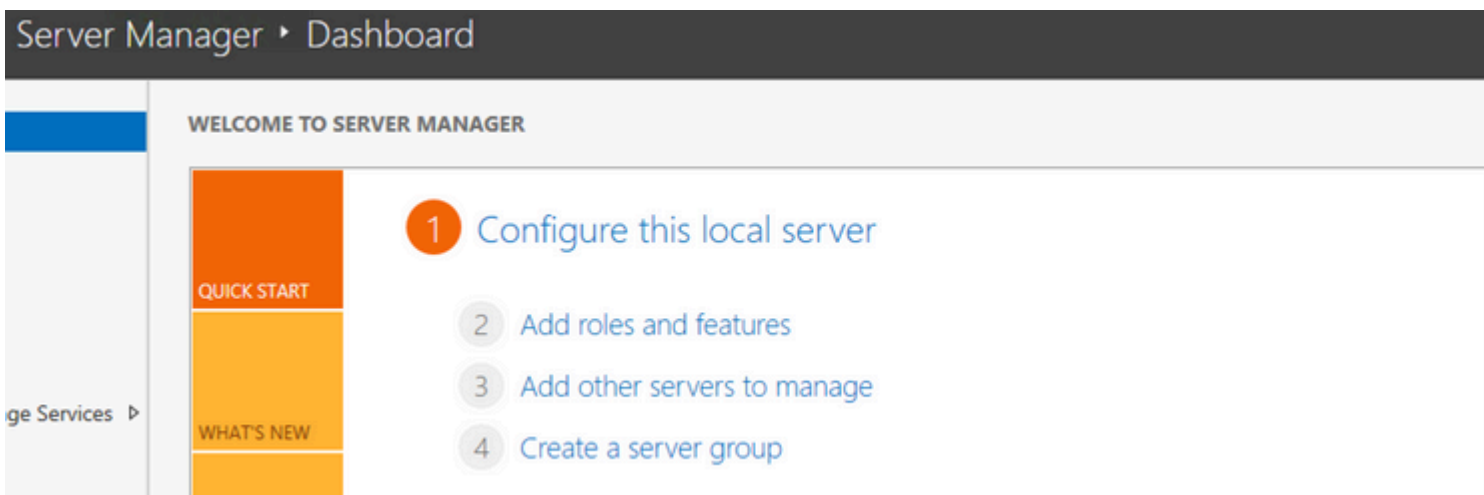
Passaggio 9. Come mostrato nell'immagine, scegliere SHA (Secure Hash Algorithm) come SHA-256.



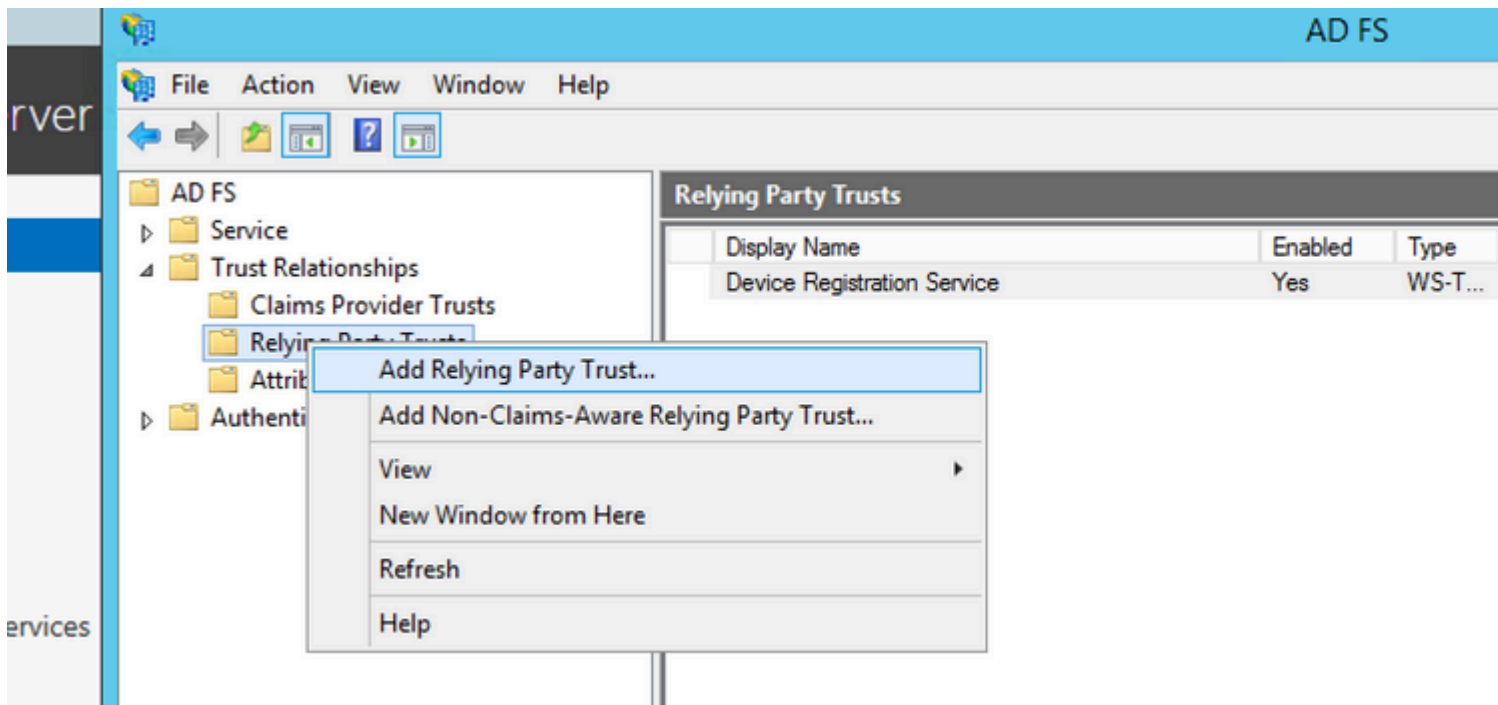
Passaggio 10. Clic ok.

ADFS 3.0

Passaggio 1. Nel server ADFS passare a Server Manager > Tools > ADFS Management.



Passaggio 2. Passa a ADFS > Trust Relationship > Relying Party Trust.



Passaggio 3. Scegliere l'opzione Import data about the relying party from a file.



Add Relying Party Trust Wizard

Welcome

Steps

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

Welcome to the Add Relying Party Trust Wizard

This wizard will help you add a new relying party trust to the AD FS configuration to consume claims in security tokens that are issued by this Federation Service for authorization decisions.

The relying party trust that this wizard creates defines how this Federation Service issues claims to the relying party and issues claims to it. You can define issuance transform rules for issuance after you complete the wizard.

< Previous



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 that has published 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 that has exported its federation metadata to a file. Ensure that this file is from a trusted source and 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.

< Previous

Add Relying Party Trust Wizard

Browse for Metadata File...



<< SSO 11.5 >> Pod1



Search

Organize

New folder



Downloads



Recent places



This PC



Desktop



Documents



Downloads



FOLDERS on ARU



Music



Pictures



Videos



Local Disk (C:)



DVD Drive (D:) IR

Name

Date modified

sp

8/18/2016 8:26 PM

File name:

sp

Meta

< Previous



Add Relying Party Trust Wizard

Specify Display Name

Steps

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

Enter the display name and any optional notes for this relying party.

Display name:

Notes:

< Previous



Add Relying Party Trust Wizard

Steps

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

Configure multi-factor authentication settings for this relying party trust. Multi-factor authentication is required if there is a match for any of the specified requirements.

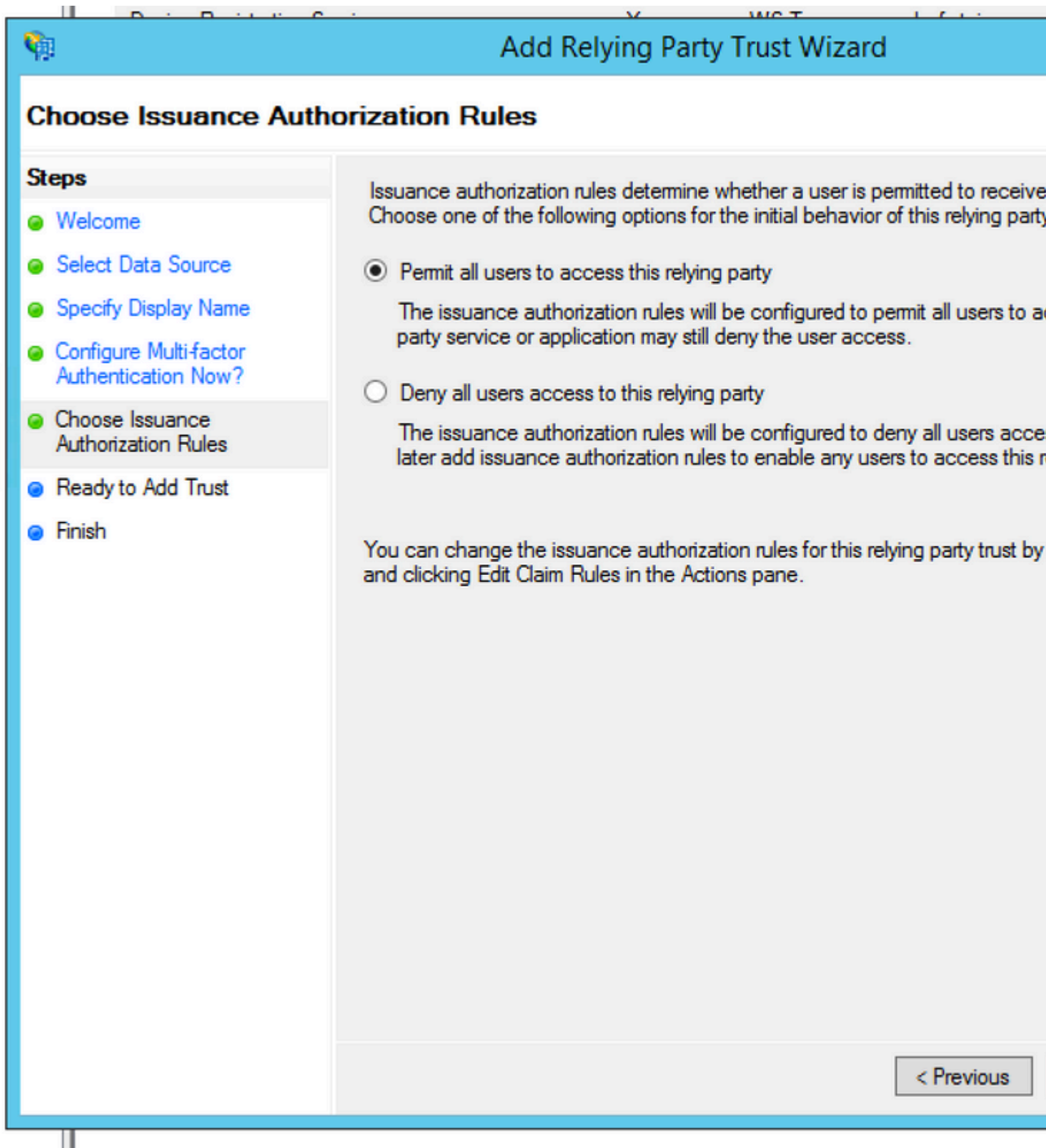
Multi-factor Authentication

| Requirements | Users/Groups | Not configured |
|--------------|--------------|----------------|
| | Device | Not configured |
| | Location | Not configured |

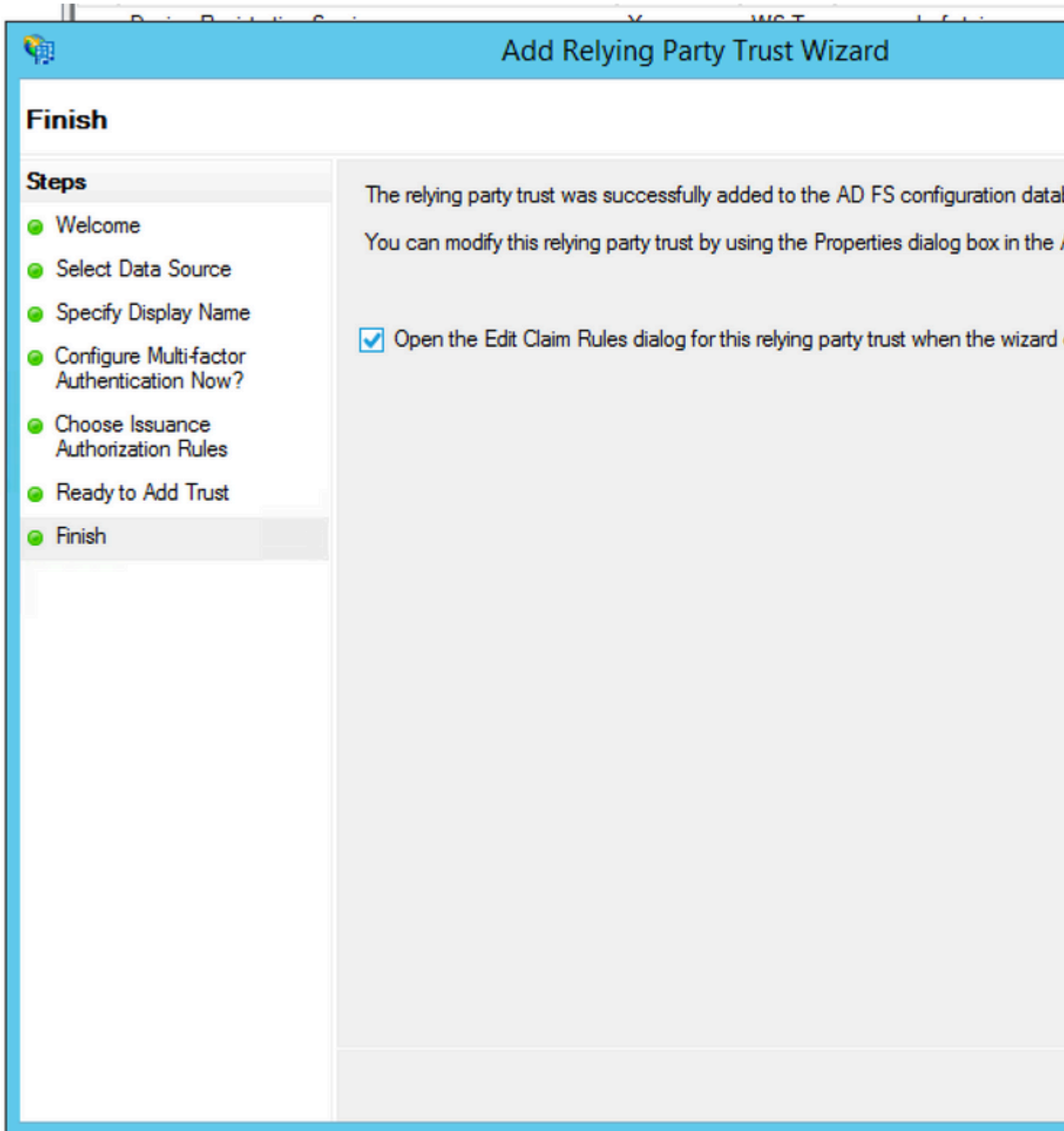
- I do not want to configure multi-factor authentication settings for this relying party trust.
- Configure multi-factor authentication settings for this relying party trust.

You can also configure multi-factor authentication settings for this relying party trust in the **Authentication Policies** node. For more information, see [Configuring Authentication Policies](#).

< Previous



Passaggio 4. Completare la creazione dell'attendibilità del componente.



Add Relying Party Trust Wizard

Finish

Steps

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

The relying party trust was successfully added to the AD FS configuration data.
You can modify this relying party trust by using the Properties dialog box in the AD FS console.

Open the Edit Claim Rules dialog for this relying party trust when the wizard finishes.

Passaggio 5. Nelle proprietà dell'attendibilità componente, scegliere Identifier scheda.

Relying Party Trusts

| Display Name | Enabled | Type | Identifier |
|-----------------------------|---------|---------|--------------|
| Device Registration Service | Yes | WS-T... | um.ms-drs.fs |
| uccx115p1.toi.com | Yes | WS-T... | uccx115p1.t |

- Update from Federation Metadata...
- Edit Claim Rules...
- Disable
- Properties**
- Delete
- Help

uccx115p1.toi.com Properties

Organization

Endpoints

Proxy Endpoints

Notes

Advanced

Monitoring

Identifiers

Encryption

Signature

Accepted Claims

Specify the display name and identifiers for this relying party trust.

Display name:

Relying party identifier:

Add

Example: <https://fs.contoso.com/adfs/services/trust>

Relying party identifiers:

Remove

OK

Cancel

Apply

Passaggio 6. Impostare l'identificatore come nome host completo di Cisco Identity Server da cui `sp.xml` viene scaricato.

uccx115p1.toi.com Properties

Organization

Endpoints

Proxy Endpoints

Notes

Advanced

Monitoring

Identifiers

Encryption

Signature

Accepted Claims

Specify the display name and identifiers for this relying party trust.

Display name:

uccx.contoso.com



Relying party identifier:

Add

Example: <https://fs.contoso.com/adfs/services/trust>

Relying party identifiers:

uccx115p1.toi.com

Remove

OK

Cancel

Apply

user_principal: questo attributo è richiesto dagli IdS Cisco per identificare il realm dell'utente autenticato.

Regola attestazione 1:

Aggiungere una regola per nome NameID di tipo (inviare i valori dell'attributo LDAP come attestazioni):

- Scegliere l'archivio attributi come Active Directory
- Mapping attributo LDAP User-Principal-Name a user_principal (minuscolo)
- Scegliere l'attributo LDAP da utilizzare come userId per consentire agli utenti dell'applicazione di eseguire il login e il mapping uid(minuscolo)

Configurazione di esempio quando SamAccountName deve essere utilizzato come ID utente:

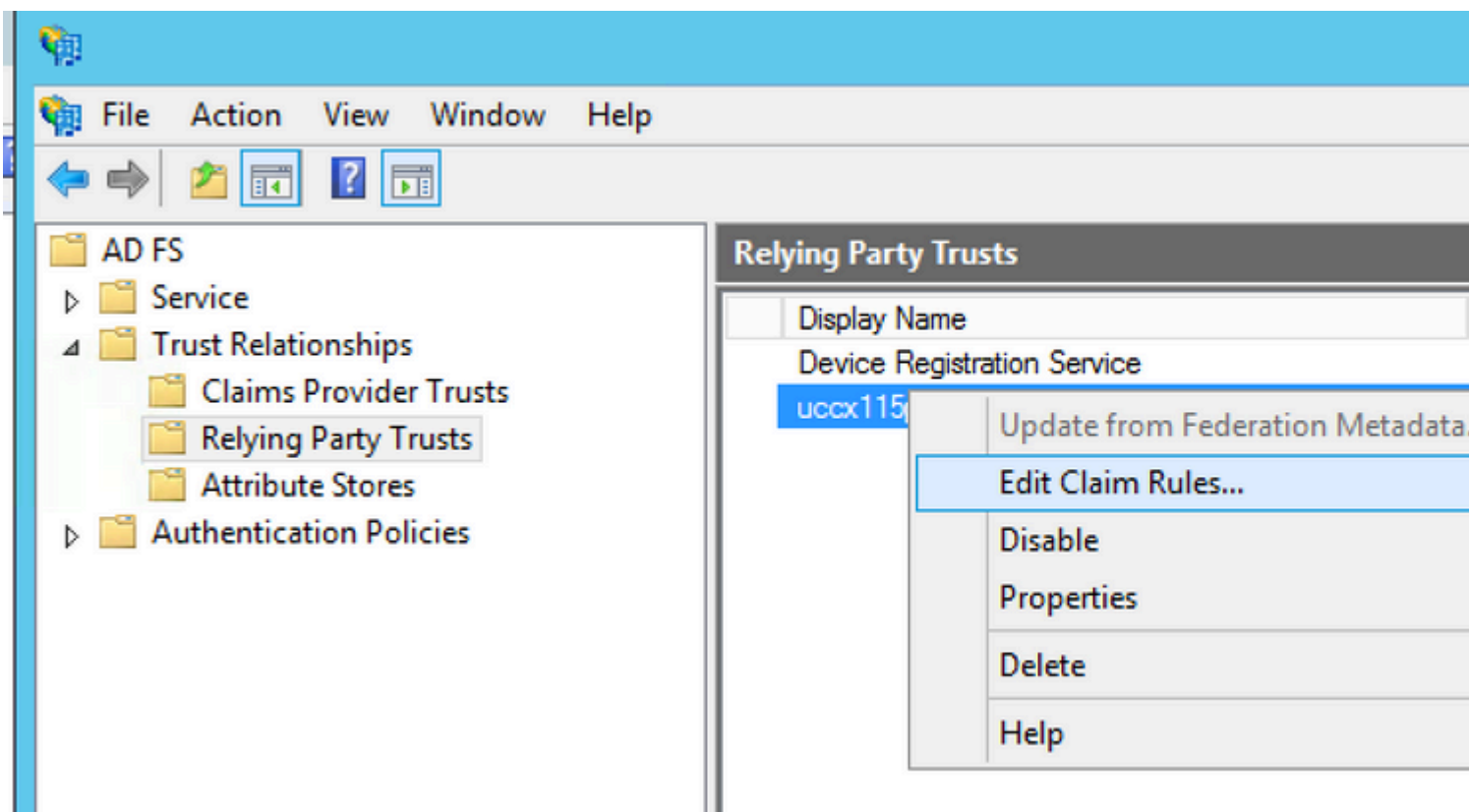
- Mappare l'attributo LDAP SamAccountName a uid.
- Mappare l'attributo LDAP User-Principal-Name a user_principal.

Esempio di configurazione in cui l'UPN deve essere utilizzato come ID utente:

- Mappare l'attributo LDAP User-Principal-Name a uid.
- Mappare l'attributo LDAP User-Principal-Name a user_principal.

Configurazione di esempio quando PhoneNumber deve essere utilizzato come ID utente:

- Mappare l'attributo LDAP telephoneNumber a uid.
- Mappare l'attributo LDAP User-Principal-Name a user_principal.



Help

File Action View Window Help

AD FS

- Service
- Trust Relationships
 - Claims Provider Trusts
 - Relying Party Trusts

Relying Party Trusts

| Display Name |
|-----------------------------|
| Device Registration Service |
| uccx115p1.toi.com |

Edit Claim Rules for uccx115p1.toi.com

Issuance Transform Rules Issuance Authorization Rules Delegation Authorization Rules

The following transform rules specify the claims that will be sent to the relying party.

| Order | Rule Name | Issued Claims |
|-------|-----------|---------------|
|-------|-----------|---------------|

Add Rule... Edit Rule... Remove Rule...

OK Cancel Apply

msdcs.toi.com | Reliving Party Trusts

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. Specify which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types issued from the rule.

Claim rule name:

Rule template: Send LDAP Attributes as Claims

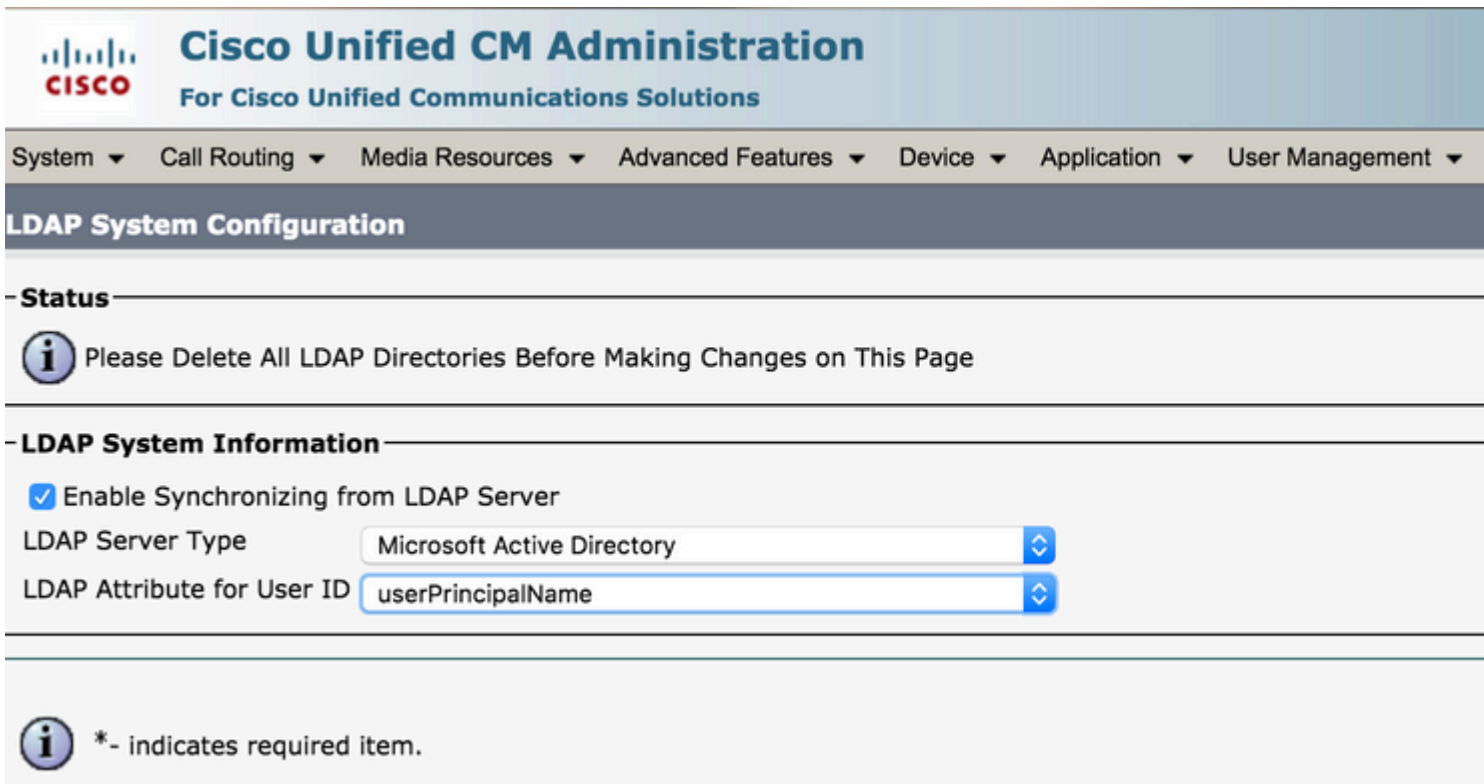
Attribute store:

Mapping of LDAP attributes to outgoing claim types:

| | LDAP Attribute (Select or type to add more) | Outgoing Claim Type (Select) |
|---|---|-------------------------------|
| | SAM-Account-Name <input type="text" value=""/> | uid |
| ▶ | User-Principal-Name <input type="text" value=""/> | user_principal |
| * | <input type="text" value=""/> | <input type="text" value=""/> |

Nota: è necessario verificare che l'attributo LDAP configurato per l'ID utente nella sincronizzazione LDAP CUCM corrisponda a quello configurato come attributo LDAP per uid nella regola di attestazione ADFS NameID. Ciò serve per il corretto funzionamento del login CUIC e Finesse.

Nota: questo documento fa riferimento a vincoli relativi al nome della regola attestazione e ai nomi visualizzati, ad esempio NameID, FQDN di UCCX e così via. Sebbene i campi e i nomi personalizzati possano essere applicabili in varie sezioni, i nomi delle regole attestazione e i nomi visualizzati vengono mantenuti standard in tutto per garantire la coerenza e per ottimizzare le procedure nella convenzione di denominazione.



The screenshot shows the Cisco Unified CM Administration interface. At the top, there is a navigation menu with options: System, Call Routing, Media Resources, Advanced Features, Device, Application, and User Management. Below this is the page title "LDAP System Configuration". A status message reads: "Please Delete All LDAP Directories Before Making Changes on This Page". Under the "LDAP System Information" section, there is a checked checkbox for "Enable Synchronizing from LDAP Server". Below this are two dropdown menus: "LDAP Server Type" set to "Microsoft Active Directory" and "LDAP Attribute for User ID" set to "userPrincipalName". At the bottom, a note states: "*- indicates required item."

Regola attestazione 2:

- Aggiungere un'altra regola di tipo Regola attestazione personalizzata con il nome Nome host completo di Cisco Identity Server e aggiungere il testo di questa regola.

```
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"] => issue(
```

- Nel cluster Cisco Identity Server, tutti i nomi host completi sono quelli del nodo principale o del nodo del server di pubblicazione Cisco Identity Server.
- Il nome host completo di Cisco Identity Server> fa distinzione tra maiuscole e minuscole, quindi corrisponde esattamente (maiuscole/minuscole incluse) al nome FQDN di Cisco Identity Server.
- L' <FQDN server ADFS> fa distinzione tra maiuscole e minuscole, pertanto corrisponde esattamente (inclusa la distinzione tra maiuscole e minuscole) all'FQDN ADFS.

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 details about each claim rule template.

Claim rule template:

Send Claims Using a Custom Rule

Claim rule template description:

Using a custom rule, you can create rules that can't be created with a rule written in the AD FS claim rule language. Capabilities that require custom rules include:

- Sending claims from a SQL attribute store
- Sending claims from an LDAP attribute store using a custom LDAP filter
- Sending claims from a custom attribute store
- Sending claims only when 2 or more incoming claims are present
- Sending claims only when an incoming claim value matches a complex pattern
- Sending claims with complex changes to an incoming claim value
- Creating claims for use only in later rules

< Previous

Edit Rule - uccx115p1.toi.com

You can configure a custom claim rule, such as a rule that requires multiple incoming claims claims from a SQL attribute store. To configure a custom rule, type one or more optional conditions and an issuance statement using the AD FS claim rule language.

Claim rule name:

uccx.contoso.com

Rule template: Send Claims Using a Custom Rule

Custom rule:

```
c:[Type ==  
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windows  
name"]  
=> issue (Type =  
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameid",  
Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value =  
c.Value, ValueType = c.ValueType, Properties  
["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperty:  
"] = "urn:oasis:names:tc:SAML:2.0:nameid-format:transient", Property  
["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperty:  
qualifier"] = "http://fs.contoso.com/adfs/services/trust", Property  
["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperty:  
qualifier"] = "uccx.contoso.com");
```

OK

: il passaggio 2. non è necessario se si utilizza ADFS 3.0 poiché il cmdlet è già installato come parte dell'aggiunta di ruoli e funzionalità.

Nota: la

rileva la distinzione tra maiuscole e minuscole, pertanto corrisponde (inclusa la distinzione tra maiuscole e minuscole) a quanto impostato nella scheda Identificatore delle proprietà Attendibilità componente.

Nota: da UCCX versione 12.0 Cisco IdS supporta SHA-256. L'attendibilità del componente utilizza SHA-256 per firmare la richiesta SAML e si aspetta la stessa risposta da ADFS.

Per una configurazione multidominio per ADFS federati

Nel caso della federazione in ADFS, in cui un ADFS in un particolare dominio fornisce l'autenticazione SAML federata per gli utenti in altri domini configurati, sono necessarie ulteriori configurazioni.

In questa sezione il termine ADFS primario si riferisce agli ADFS che devono essere utilizzati negli IdS. Il termine ADFS federato indica gli ADFS, i cui utenti possono accedere tramite IdS e quindi sono gli ADFS primari.

Configurazione ADFS federata

In ognuno degli ADFS federati è necessario creare la relazione di trust della relying party per gli ADFS primari e le regole attestazione configurate come indicato nella sezione precedente.

Configurazione ADFS primaria

Per gli ADFS primari, oltre all'attendibilità del componente per gli ID, è necessaria questa configurazione aggiuntiva.

Aggiungi Claim Provider Trust con ADFS a cui deve essere impostata la federazione.

Nell'attendibilità del provider di attestazioni, verificare che Pass through or Filter an Incoming Claim le regole sono configurate con l'opzione pass-through tutti i valori attestazione:

- ID nome
- Scegliere ID nome dal menu Incoming Claim Type dropdown
- Scegli Transient come opzione per il formato NameID in ingresso
- uid: attestazione personalizzata. Immettere il valore uid nel campo Incoming Claim Type dropdown
- user_principal: questa è un'attestazione personalizzata. Digitare il valore user_principal nel campo Incoming Claim Type dropdown

Nell'attendibilità del componente per gli ID, aggiungere Pass though or Filter an Incoming Claim regole con pass-through tutti i valori attestazione come opzione.

- NomeIDFromSottodominio
- Scegli ID nome da Incoming Claim Type dropdown
- Scegli Transient come opzione per il formato NameID in ingresso
- uid: attestazione personalizzata. Digitare il valore uid nel campo Incoming Claim Type dropdown
- user_principal: questa è un'attestazione personalizzata. Digitare il valore user_principal nel campo Incoming Claim Type dropdown

Rollover automatico dei certificati ADFS

Il rollover automatico dei certificati è supportato per UCCX 11.6.1 e versioni successive. (L'aggiornamento alla versione 14.0 della libreria Fedlet in UCCX 11.6 ha risolto il problema).

Autenticazione Kerberos (autenticazione integrata di Windows)

L'autenticazione integrata di Windows (IWA) fornisce un meccanismo per l'autenticazione degli utenti ma non consente la trasmissione delle credenziali in rete. Quando si attiva l'autenticazione integrata di Windows, funziona sulla base di ticket per consentire ai nodi di comunicare su una rete non protetta al fine di dimostrare la propria identità l'uno all'altro in modo sicuro. Consente agli utenti di accedere a un dominio dopo aver effettuato l'accesso ai computer Windows.

Nota: l'autenticazione Kerberos è supportata solo dalla versione 11.6 e successive.

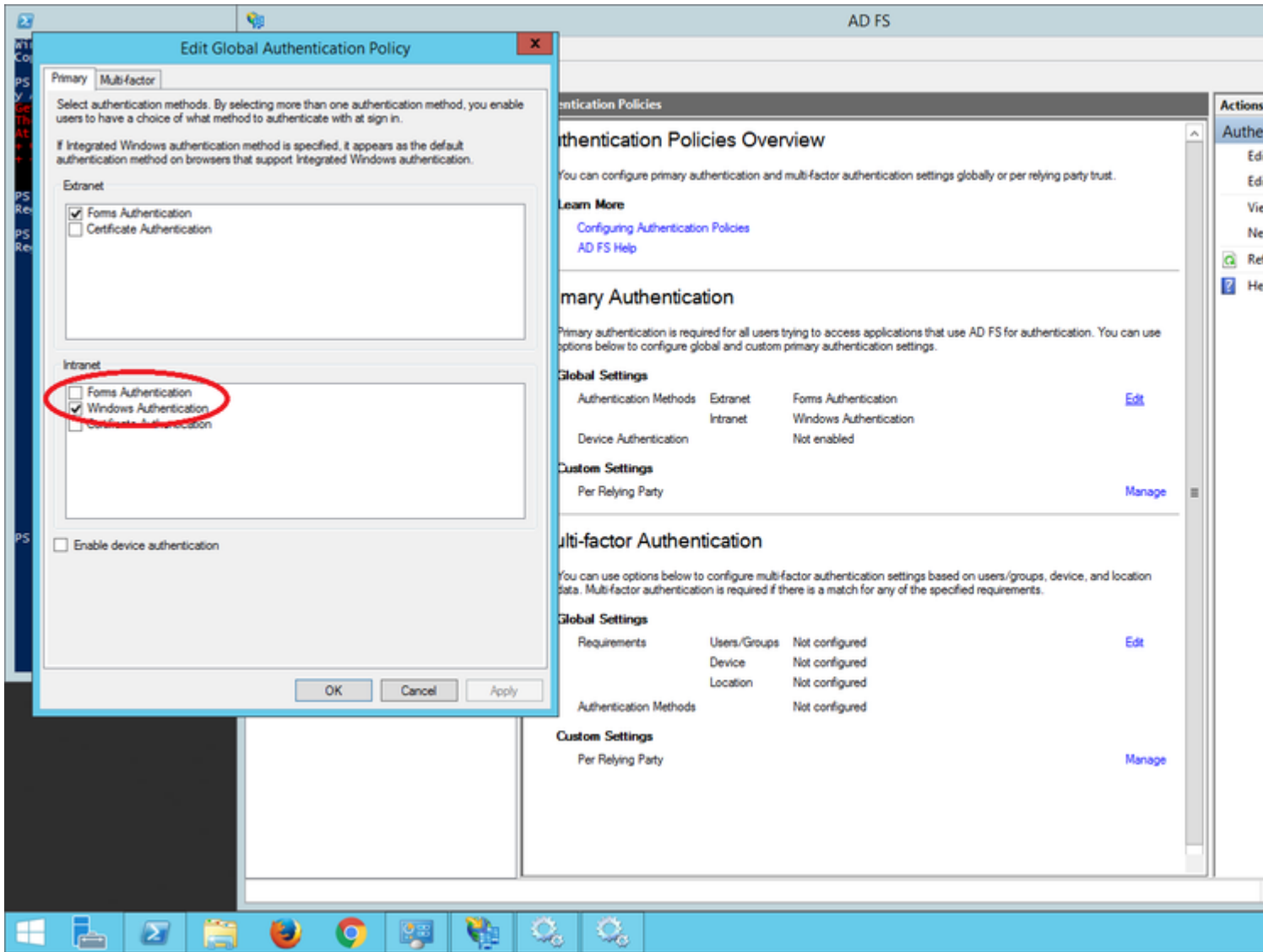
Gli utenti di dominio già connessi al controller di dominio vengono connessi senza problemi ai client SSO senza che sia necessario immettere nuovamente le credenziali. Per gli utenti non di dominio, IWA ritorna a New Technology Local Area Network Manager (NTLM) e viene visualizzata la finestra di dialogo di accesso. La qualifica per gli ID con autenticazione IWA viene eseguita con Kerberos rispetto ad ADFS 3.0.

Passaggio 1. Aprire il prompt dei comandi di Windows ed eseguire come utente Admin per registrare il servizio HTTP con setspn comando `setspn -s http/`

\

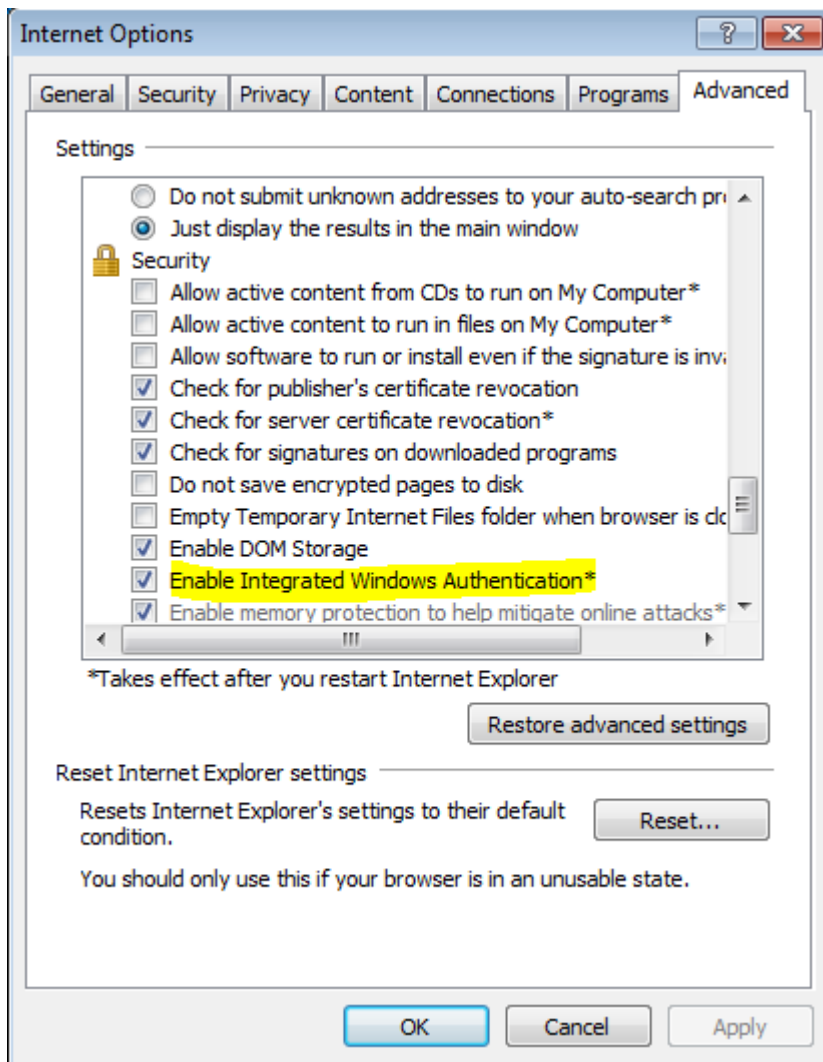
.

Passaggio 2. Disabilita autenticazione basata su form e abilita l'autenticazione di Windows per i siti Intranet. Passa a ADFS Management > Authentication Policies > Primary Authentication > Global Settings > Edit. In Intranet verificare che sia selezionata solo l'opzione Autenticazione di Windows (deselezionare Autenticazione modulo).



Configurazione per il supporto di Microsoft Internet Explorer per IWA

Passaggio 1. Accertarsi che Internet Explorer > Advanced > Enable Integrated Windows Authentication è selezionato.



Passaggio 2. L'URL ADFS deve essere aggiunto a Security > Intranet zones > Sites (winadcom215.uccx116.com è l'URL ADFS).

Internet Options



Local intranet



You can add and remove websites from this zone. All websites in this zone will use the zone's security settings.

Add this website to the zone:

Add

Websites:

hcp://system
http://localhost
https://localhost
winadcom215.uccx116.com

Remove

Require server verification (https:) for all sites in this zone

Close

Enable Protected Mode (requires restarting Internet Explorer)

Custom level...

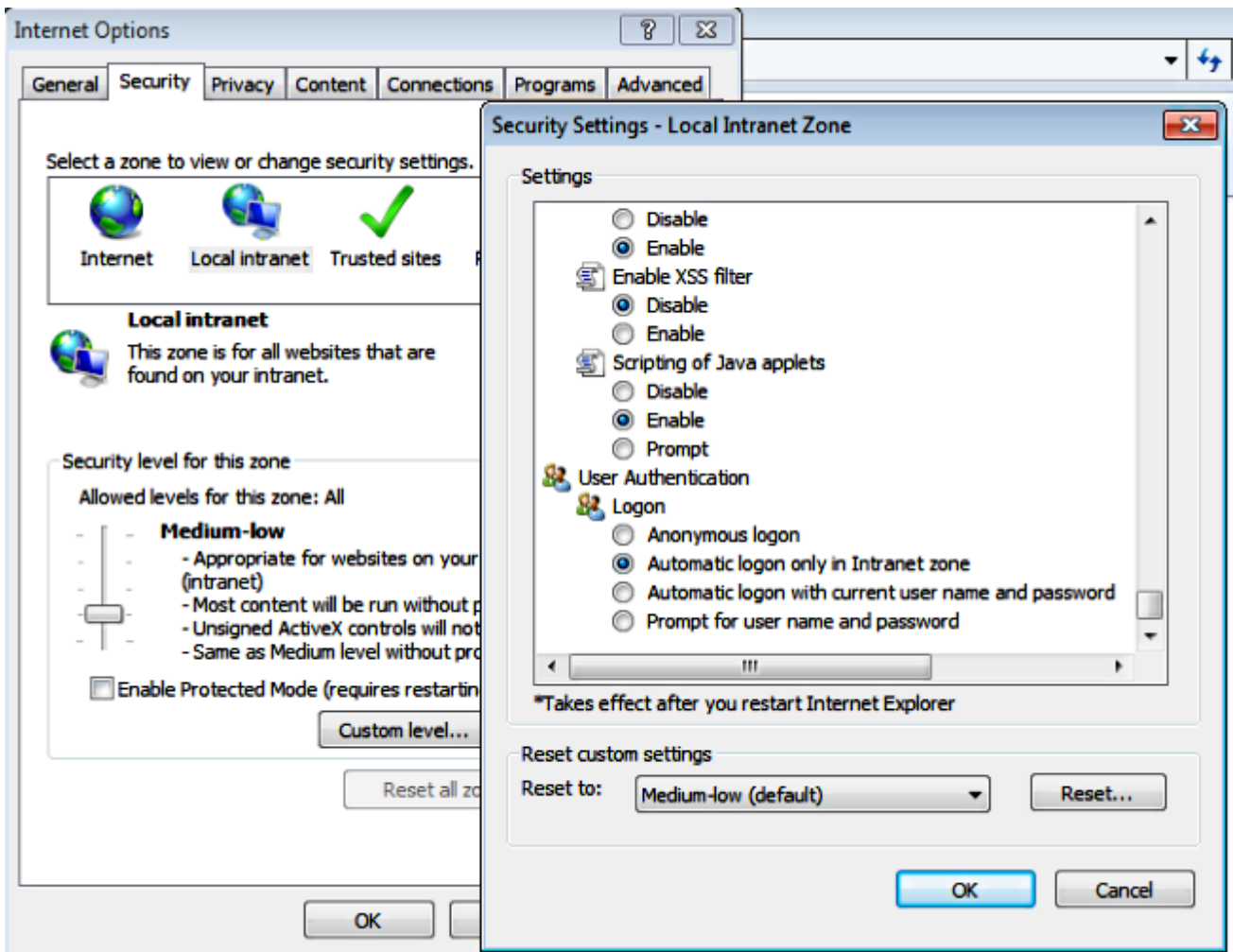
Default level

Reset all zones to default level

OK

Cancel

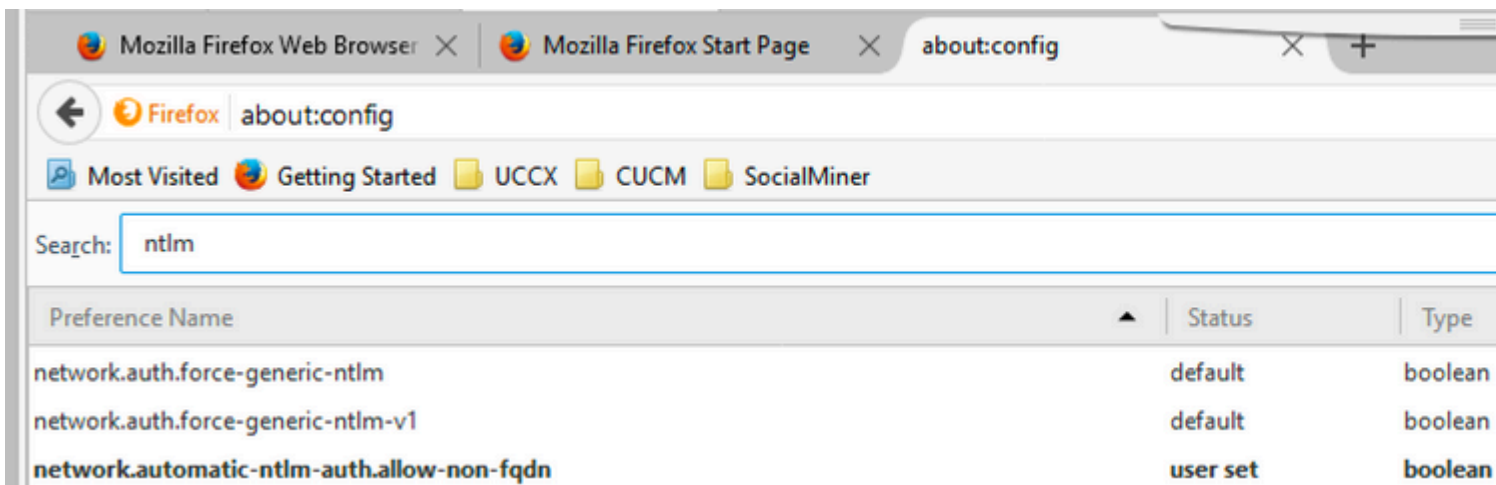
Ap



Configurazione richiesta per Mozilla Firefox per il supporto IWA

Passaggio 1. Accedere alla modalità di configurazione di Firefox. Aprire Firefox e immettere `about:config` nell'URL. Accetta la dichiarazione sui rischi.

Passaggio 2. Cerca `ntlm` e abilitare `network.automatic-ntlm-auth.allow-non-fqdn` e impostarlo su `true`.



Passaggio 3. Impostare la `network.automatic-ntlm-auth.trusted-uris` al dominio o esplicitamente all'URL ADFS.

| | | |
|--|----------|--------|
| <code>network.automatic-ntlm-auth.allow-proxies</code> | default | bool |
| <code>network.automatic-ntlm-auth.trusted-uris</code> | user set | string |
| <code>network.generic-ntlm-auth.workstation</code> | default | string |

Configurazione richiesta per Google Chrome per il supporto IWA

Google Chrome in Windows utilizza le impostazioni di Internet Explorer, quindi configurare in Internet Explorer Tools > Internet Options o dal Pannello di controllo in Internet Options all'interno della sottocategoria Network and Internet.

Ulteriore configurazione per SSO

In questo documento viene descritta la configurazione dell'elemento IdP per l'SSO da integrare con l'elemento Cisco IdS. Per ulteriori informazioni, consultare le guide alla configurazione dei singoli prodotti:

- [UCCX](#)
- [UCCE](#)
- [PCCE](#)

Verifica

Questa procedura viene utilizzata per determinare se l'attendibilità del componente è stabilita correttamente tra Cisco IdS e IDP.

- Dal browser immettere l'URL https://<ADFS_FQDN>/adfs/ls/IdpInitiatedSignOn.aspx?loginToRp=<IDS_FQDN>
- ADFS fornisce il modulo di accesso. Questa opzione è disponibile quando la configurazione indicata è corretta.
- Se l'autenticazione ha esito positivo, il browser deve reindirizzare a https://<IDS_FQDN>:8553/ids/saml/response, quindi viene visualizzata una pagina con l'elenco di controllo.

Nota: la pagina Elenco di controllo visualizzata come parte del processo di verifica non è un errore ma una conferma della corretta creazione del trust.

Risoluzione dei problemi

Per la risoluzione dei problemi, consultare il documento <https://www.cisco.com/c/en/us/support/docs/customer-collaboration/unified-contact-center-express/200662-ADFS-IdS-Troubleshooting-and-Common-Prob.html>.

URL di bypass/recupero UCCX SSO

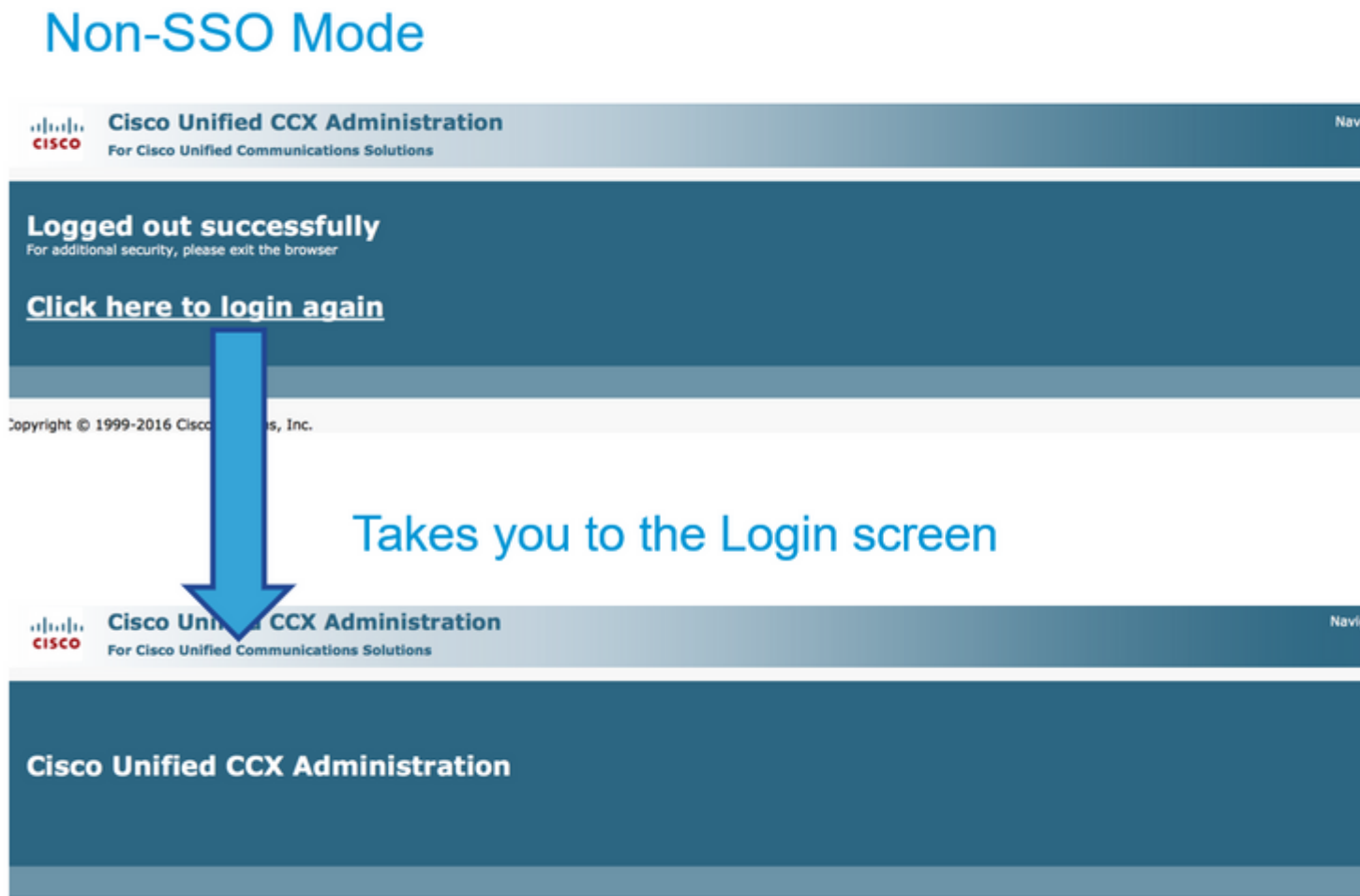
- [Amministrazione Cisco Unified CCX](#)
- [Manutenzione di CCX unificato Cisco](#)

Disabilita SSO

- GUI: Passa a CCX Administration > Single Sign-On (SSO) > Disable.
- CLI: set authmode non_sso (questo comando deve disabilitare l'SSO sia per Pub che Sub - può essere eseguito da entrambi i nodi UCCX in caso di cluster ad alta disponibilità).

Acquisizioni schermo

Amministrazione CCX - Non_SSO

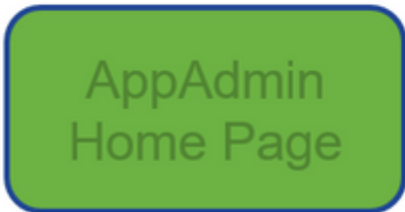


Amministrazione CCX - SSO abilitato

SSO Mode



Takes to the AppAdmin Home page if authenticated with IdP



Accesso Finesse - Non SSO



Username*

Password*

Extension*



Finesse
desktop home
page

Accesso Finesse - SSO abilitato



User is redirected to AD login

Sign In

adfs-sha256.yoddhasad.com

Type your user name and password.

User name: Example: Domain\username

Password:



Redirected to landing page

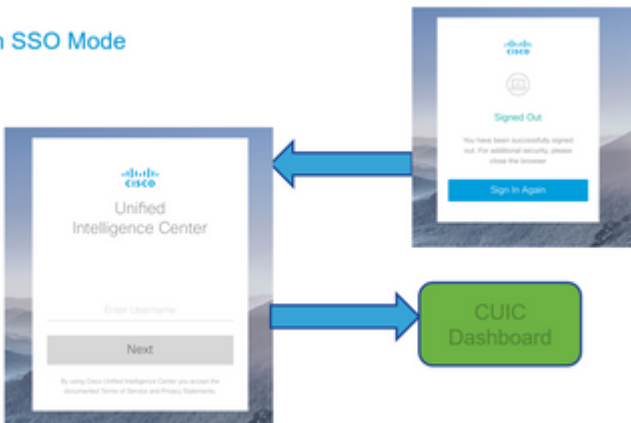
Username* chaitra

Extension*



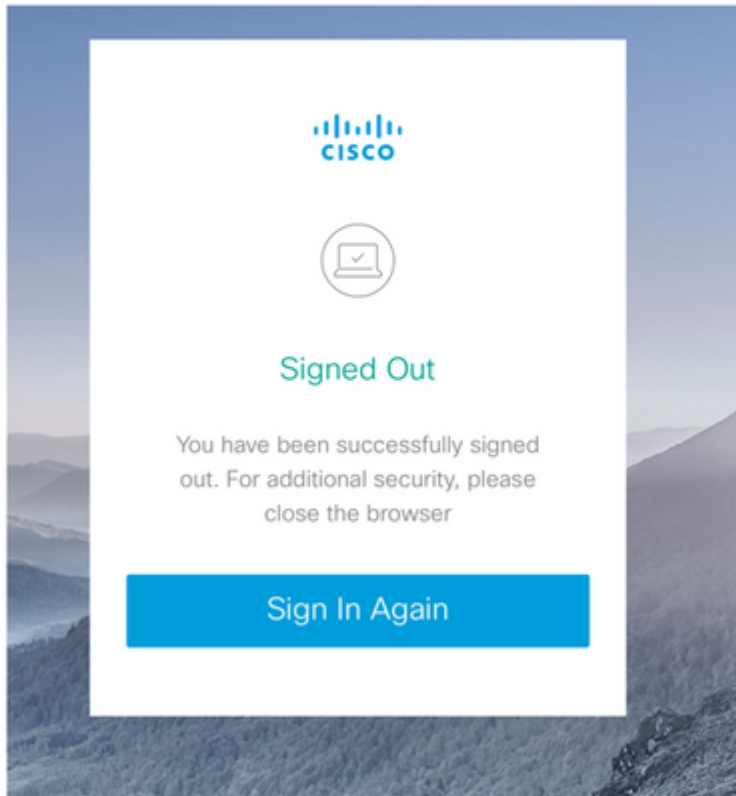
CUIC - Non_SSO

Non SSO Mode

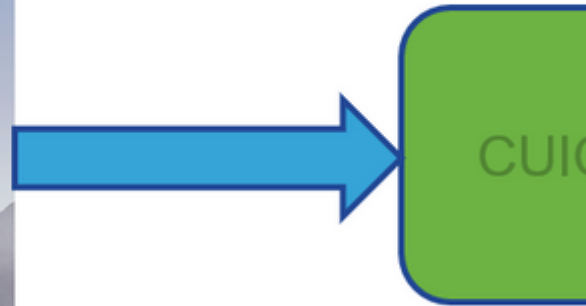


CUIC - SSO abilitato

SSO Mode



Takes to the CUIC Dashboard if authenticated with IdP



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).