

Konfigurieren des Identitätsanbieters für den Cisco Identity Service zur Aktivierung von SSO

Inhalt

- [Einleitung](#)
- [Voraussetzungen](#)
- [Anforderungen](#)
- [Verwendete Komponenten](#)
- [Hintergrundinformationen](#)
- [Überblick über SSO](#)
- [Konfigurationsübersicht](#)
- [Konfigurieren](#)
- [Authentifizierungstypen](#)
- [Aufbau einer Vertrauensbeziehung](#)
- [ADFS 2.0](#)
- [ADFS 3.0](#)
- [Signierte SAML-Assertionen für die Vertrauensstellung der vertrauenden Seite \(Cisco IDs\) aktivieren](#)
- [Konfiguration mehrerer Domänen für Federated ADFS](#)
- [Federated ADFS-Konfiguration](#)
- [Primäre ADFS-Konfiguration](#)
- [Automatischer ADFS-Zertifikatrollover](#)
- [Kerberos-Authentifizierung \(integrierte Windows-Authentifizierung\)](#)
- [Konfiguration für Microsoft Internet Explorer für IWA-Support](#)
- [Erforderliche Konfiguration für Mozilla Firefox für IWA-Support](#)
- [Konfiguration erforderlich für Google Chrome zur IWA-Unterstützung](#)
- [Weitere Konfiguration für SSO](#)
- [Überprüfung](#)
- [Fehlerbehebung](#)
- [UCCX SSO-Umgehungs-/Wiederherstellungs-URLs](#)
- [SSO deaktivieren](#)
- [Screenshots](#)
- [CCX-Administration - Nicht SSO](#)
- [CCX-Administration - SSO aktiviert](#)
- [Finesse-Anmeldung - Nicht-SSO](#)
- [Finesse-Anmeldung - SSO aktiviert](#)
- [CUIC - Nicht SSO](#)
- [CUIC - SSO aktiviert](#)

Einleitung

In diesem Dokument wird die Konfiguration des Identity Providers (IdP) für Cisco Identity Service (IdS) zur Aktivierung von Single Sign On (SSO) beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco Unified Contact Center Express (UCCX) Version 11.5 bzw. Cisco Unified Contact Center Enterprise Version 11.5 bzw. Packaged Contact Center Enterprise (PCCE) Version 11.5
- Microsoft Active Directory - AD auf Windows Server installiert
- Active Directory Federation Service (ADFS) Version 2.0/3.0

Hinweis: In den Screenshots und Beispielen wird in diesem Dokument auf UCCX verwiesen. Die Konfiguration ist jedoch in Bezug auf die Cisco IdS (UCCX/UCCE/PCCE) und die IdP ähnlich.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

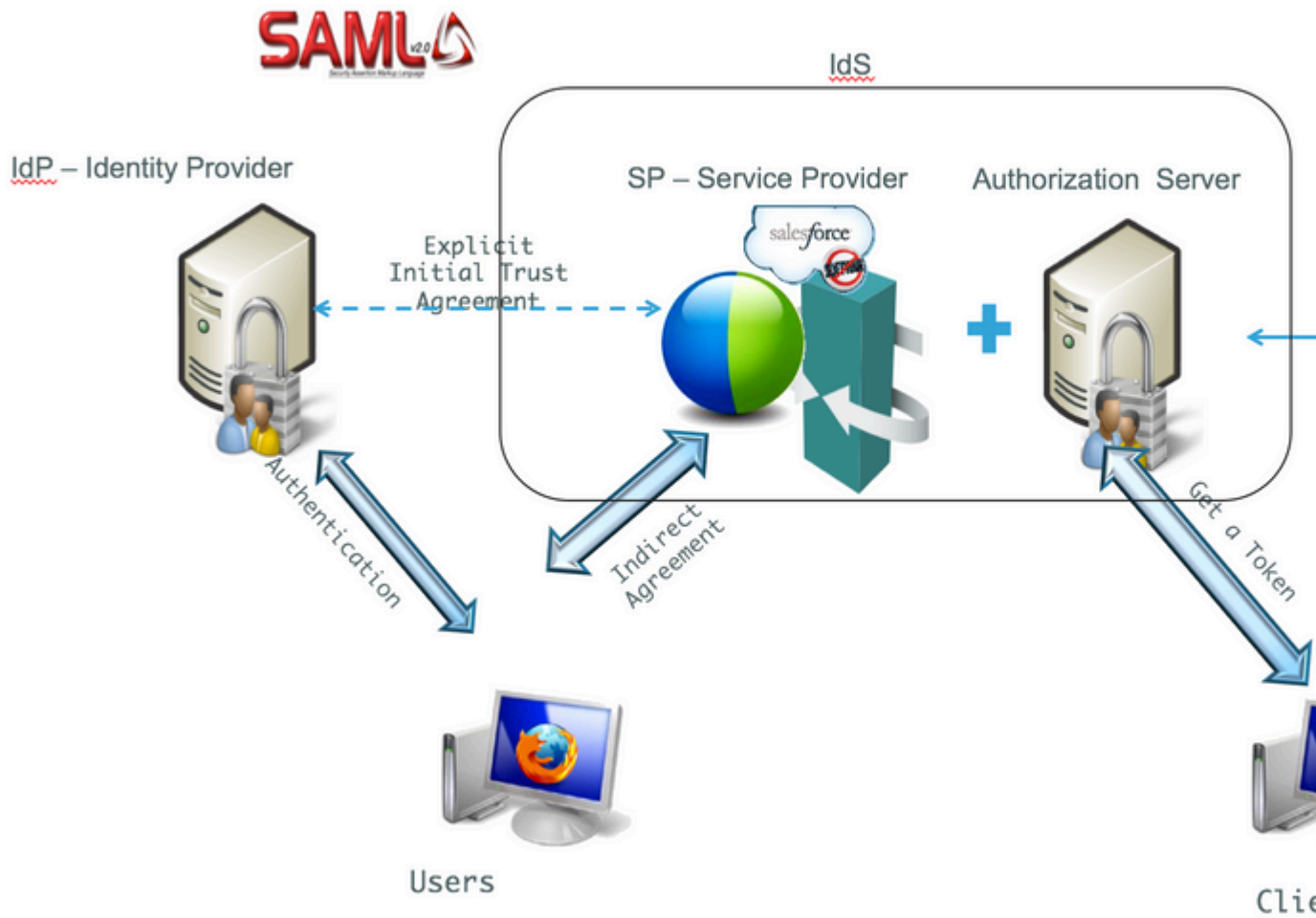
Cisco IDs-Bereitstellungsmodelle

Produkt	Bereitstellung
UCCX	Mitansässig
PCCE	Co-Resident mit CUIC (Cisco Unified Intelligence Center) und LD (Live-Daten)
UCCE	Gleichzeitige Implementierung mit CUIC und LD für 2k-Bereitstellungen Standalone für Bereitstellungen der Serien 4000 und 12000.

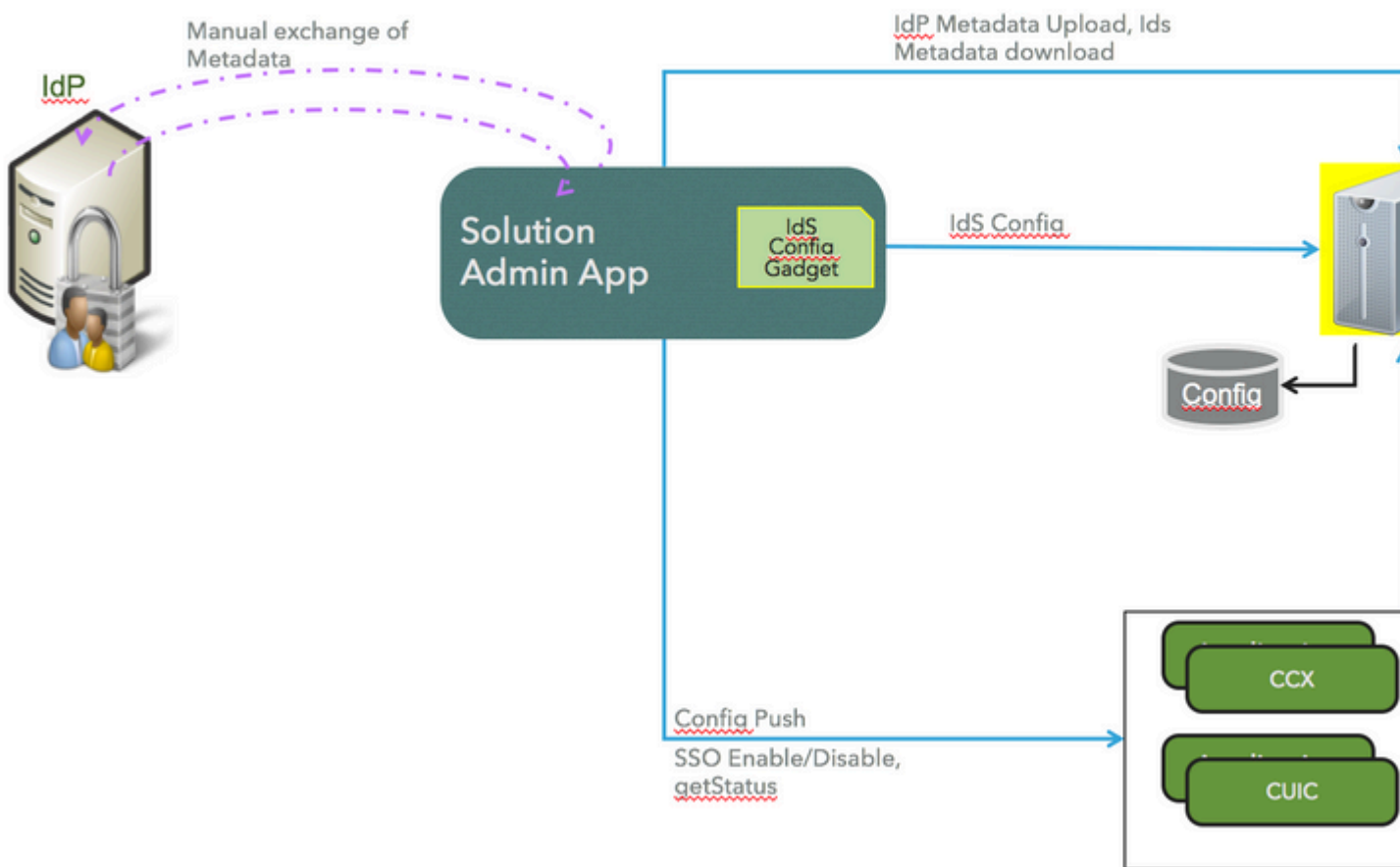
Überblick über SSO

Cisco bietet zahlreiche Services in unterschiedlichen Formen an. Als Endbenutzer sollten Sie sich nur einmal anmelden, um Zugriff auf alle Cisco Services zu erhalten. Wenn Sie Kontakte aus einer der Anwendungen und Geräte von Cisco suchen und verwalten möchten, nutzen Sie alle möglichen Quellen (Firmenverzeichnis, Outlook, mobile Kontakte, Facebook, LinkedIn, Verlauf), und lassen Sie sie auf eine standardisierte und konsistente Weise darstellen, die die erforderlichen Informationen liefert, um ihre Verfügbarkeit zu kennen und um die besten Kontaktmöglichkeiten zu erhalten.

SSO mit SAML (Security Assertion Markup Language) erfüllt diese Anforderung. SAML/SSO bietet Benutzern die Möglichkeit, sich über eine gemeinsame Konto- und Autorisierungsidentität, die IdP, bei mehreren Geräten und Services anzumelden. Die SSO-Funktion ist ab UCCX/UCCE/PCCE 11.5 verfügbar.



Konfigurationsübersicht



Konfigurieren

Authentifizierungstypen

Cisco IdS unterstützt nur die formularbasierte Authentifizierung von IdPs.

In den folgenden MSDN-Artikeln erfahren Sie, wie Sie die Formularauthentifizierung in ADFS aktivieren.

- Informationen zu ADFS 2.0 finden Sie in diesem Microsoft TechNet-Artikel: <http://social.technet.microsoft.com/wiki/contents/articles/1600.ad-fs-2-0-how-to-change-the-local-authentication-type.aspx>
- Informationen zu ADFS 3.0 finden Sie in diesem Microsoft TechNet-Artikel: <https://learn.microsoft.com/en-us/archive/blogs/josrod/enabled-forms-based-authentication-in-adfs-3-0>

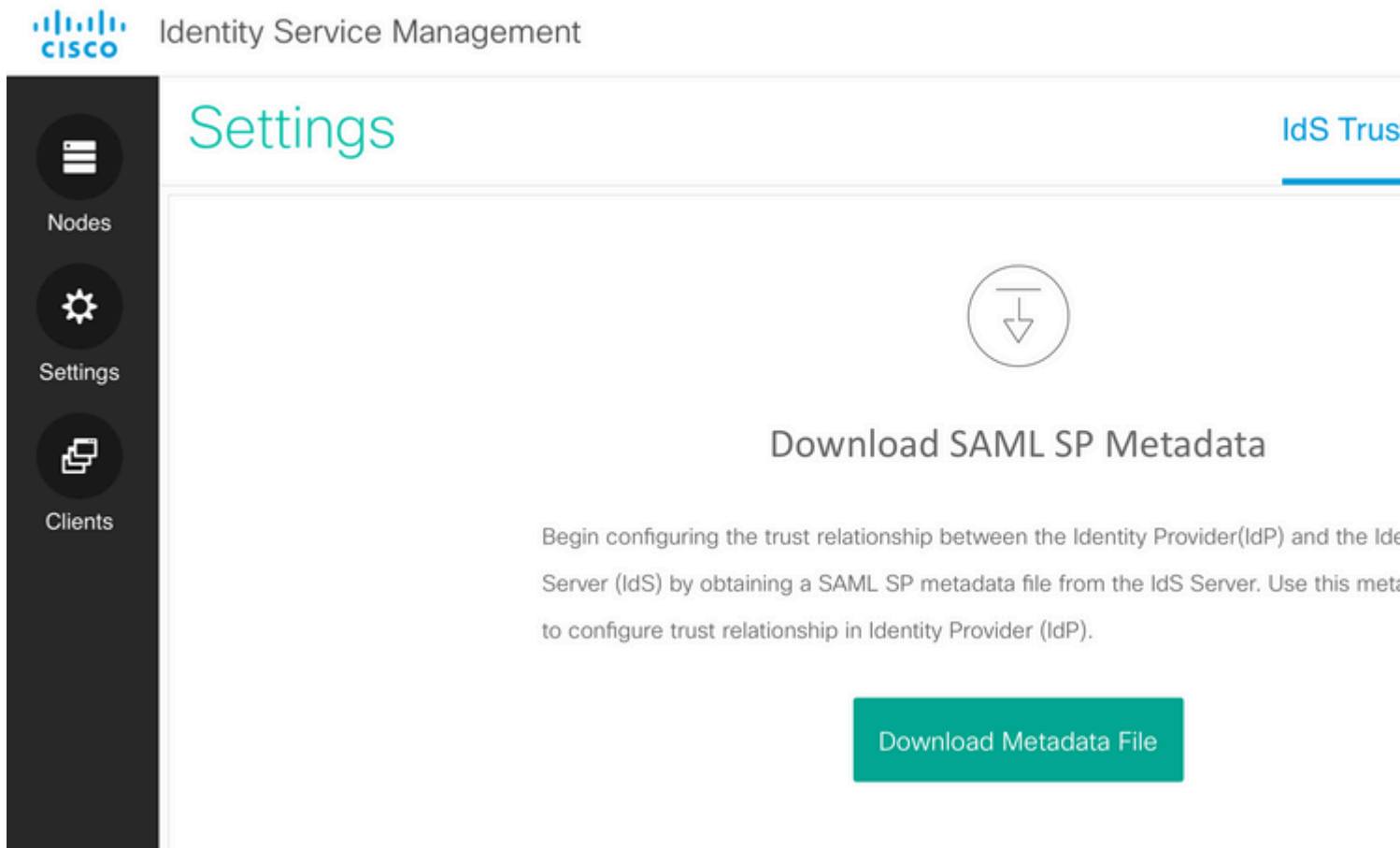
Hinweis: Cisco IdS 11.6 und höher unterstützt die formularbasierte und Kerberos-Authentifizierung. Damit die Kerberos-Authentifizierung funktioniert, müssen Sie die formularbasierte Authentifizierung deaktivieren.

Aufbau einer Vertrauensbeziehung

Führen Sie zum Onboarding und zur Ermöglichung der Verwendung von Cisco IdS für SSO durch

Anwendungen den Metadatenaustausch zwischen IdS und IdP durch.

- SAML SP-Metadatendatei herunterladen sp.xml.
- Von Settings, navigieren Sie zu IdS Trust auf der Seite "IDs Management".



The screenshot shows the Cisco Identity Service Management interface. The top left features the Cisco logo and the text 'Identity Service Management'. Below this is a dark sidebar with three icons: a hamburger menu for 'Nodes', a gear for 'Settings', and a document icon for 'Clients'. The main content area is titled 'Settings' in large teal text. On the right side of the header, 'IdS Trust' is visible. The central part of the page is titled 'Download SAML SP Metadata' and contains a circular icon with a downward arrow. Below the icon, there is a paragraph of text explaining the purpose of the metadata file. At the bottom right, there is a prominent teal button labeled 'Download Metadata File'.

- Laden Sie die IdP-Metadatendatei von der IdP von der URL herunter:
<https://<ADFSServer>/federationmetadata/2007-06/federationmetadata.xml>
- Laden Sie auf der IDs-Verwaltungsseite die IdP-Metadatendatei hoch, die im vorherigen Schritt heruntergeladen wurde.



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.

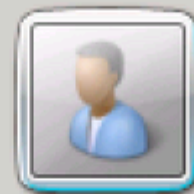
Use [file browser](#) to upload the file.

Mit diesem Verfahren werden die IDs-Metadaten hochgeladen und Anspruchsregeln hinzugefügt. Dies ist für ADFS 2.0 und 3.0 geplant.

ADFS 2.0

Schritt 1: Navigieren Sie im ADFS-Server zu Start > All Programs > Administrative Tools > ADFS 2.0 Management, wie in der Abbildung dargestellt:

- 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

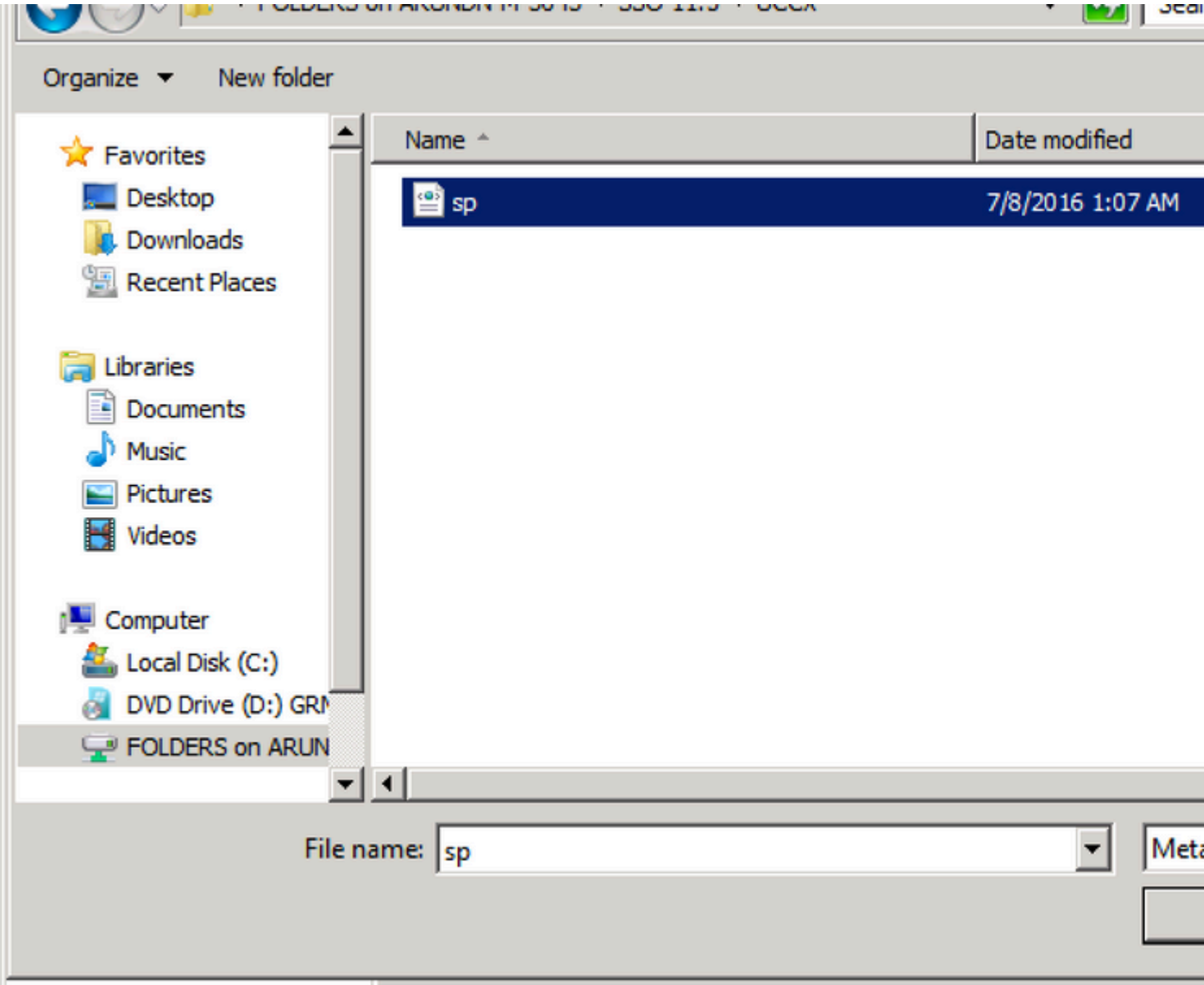
- Import data about the relying party from a file.
Use this option to import the necessary data and certificates from a relying party that has exported its federation metadata to a file. Ensure that this file is from a trusted source and do not validate the source of the file.

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

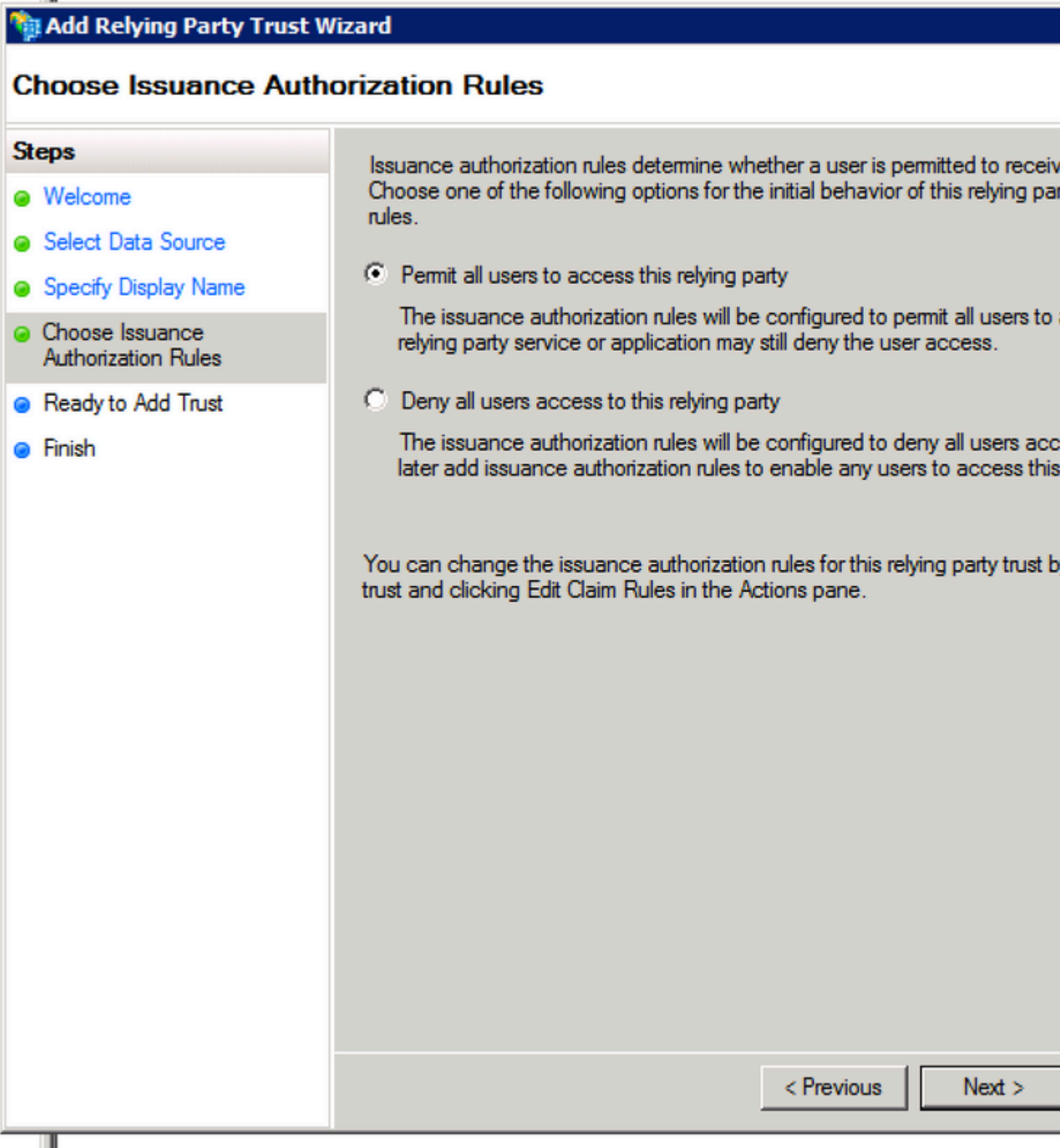
Type the display name and any optional notes for this relying party.

Display name:

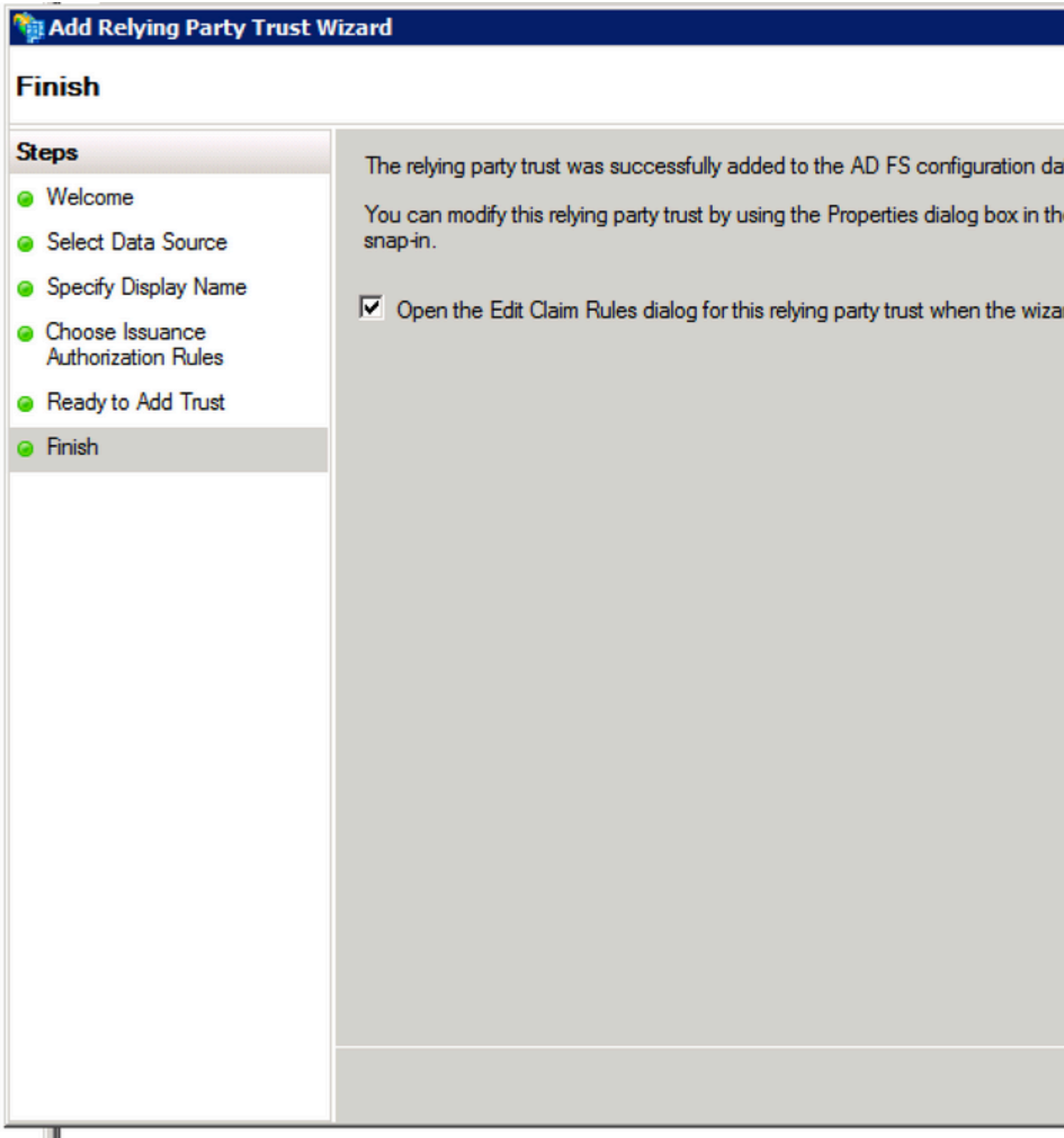
Notes:

< Previous

Next >



Schritt 4: Vollständige Einrichtung des Vertrauens der vertrauenden Seite.



Schritt 5: Wählen Sie in den Eigenschaften von Relying Party Trust die Option Identifier aus.

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


Schritt 6: Legen Sie den Bezeichner als vollqualifizierten Hostnamen des Cisco Identity Server fest, von

dem sp.xml heruntergeladen wird.

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:

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

Relying party identifiers:

Schritt 7. Klicken Sie mit der rechten Maustaste auf die Vertrauensstellung der vertrauenden Partei, und klicken Sie dann auf Edit Claim Rules.

Sie müssen zwei Anspruchsregeln hinzufügen. Die eine ist, wenn die LDAP-Attribute (Lightweight Directory Access Protocol) zugeordnet werden, während die zweite über benutzerdefinierte Anspruchsregeln erfolgt.

uid - Dieses Attribut wird für die Anwendungen benötigt, um den authentifizierten Benutzer zu identifizieren.

user_principal - Dieses Attribut wird von Cisco IdS benötigt, um den Bereich des authentifizierten Benutzers zu identifizieren.

Anspruchsregel 1:

Regel nach Namen hinzufügen NameID des Typs (die Werte des LDAP-Attributs als Ansprüche senden):

- Attributspeicher als Active Directory auswählen
- LDAP-Attribut zuordnen User-Principal-Name zu user_principal (Kleinbuchstaben)
- Wählen Sie das LDAP-Attribut aus, das verwendet werden soll als userId für Anwendungsbutzer, um sich anzumelden und sie uid (Kleinbuchstaben)

Konfigurationsbeispiel in SamAccountName ist als Benutzer-ID zu verwenden:

- Zuordnen des LDAP-Attributs SamAccountName zu uid.
- Zuordnen des LDAP-Attributs User-Principal-Name zu user_principal.

Beispielkonfiguration bei UPN als Benutzer-ID:

- Zuordnen des LDAP-Attributs User-Principal-Name zu uid.
- Zuordnen des LDAP-Attributs User-Principal-Name zu user_principal.

Konfigurationsbeispiel in PhoneNumber als Benutzer-ID:

- Ordnen Sie das LDAP-Attribut **telephoneNumber** zu uid .
- Zuordnen des LDAP-Attributs User-Principal-Name zu 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 source 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 Active Directory 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. To send individual group memberships, use the Send Group Membership as a Claim rule template.

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

< Previous

Next >

Add Transform Claim Rule Wizard

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:

Rule template: Send LDAP Attributes as Claims

Attribute store:

Mapping of LDAP attributes to outgoing claims:

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

: Sie müssen sicherstellen, dass das für die Benutzer-ID bei der CUCM-LDAP-Synchronisierung konfigurierte LDAP-Attribut mit dem LDAP-Attribut für übereinstimmt. uid in der ADFS-Anspruchsregel NameID. Dies dient zum ordnungsgemäßen Funktionieren der CUIC- und Finesse-Anmeldung.

Hinweis: Dieses Dokument verweist auf Einschränkungen für den Namen der Anspruchsregel und zeigt Namen wie NameID, FQDN (Fully Qualified Domain Name) von UCCX usw. an. Obwohl benutzerdefinierte Felder und Namen in verschiedenen Abschnitten verwendet werden können, werden die Namen der Anspruchsregeln und die Anzeigenamen durchgehend als Standard beibehalten, um die Konsistenz und die Best Practices in der Namenskonvention zu wahren.

The screenshot shows the Cisco Unified CM Administration web 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. Below the navigation menu, the page title is "LDAP System Configuration". There is a "Save" button with a floppy disk icon. Under the "Status" section, there is an information icon and the text "Status: Ready". Under the "LDAP System Information" section, there is a checkbox labeled "Enable Synchronizing from LDAP Server" which is checked. Below this, there are two dropdown menus: "LDAP Server Type" set to "Microsoft Active Directory" and "LDAP Attribute for User ID" set to "sAMAccountName". At the bottom of the configuration section, there is another "Save" button.

Anspruchsregel 2:

- Fügen Sie eine weitere Regel vom Typ "Benutzerdefinierte Anspruchsregel" mit dem Namen "Vollqualifizierter Hostname" von Cisco Identity Server hinzu, und fügen Sie diesen Regeltext hinzu.

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

- Im Cisco Identity Server-Cluster sind alle vollständig qualifizierten Hostnamen die des primären oder Herausgeberknotens von Cisco Identity Server.
- Beim <full qualified hostname of Cisco Identity Server> wird die Groß-/Kleinschreibung beachtet, sodass er genau (einschließlich der Groß-/Kleinschreibung) mit dem FQDN des Cisco Identity Server übereinstimmt.
- Beim <ADFS-Server-FQDN> wird die Groß-/Kleinschreibung beachtet, sodass er genau (einschließlich der Groß-/Kleinschreibung) mit dem ADFS-FQDN übereinstimmt.

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:

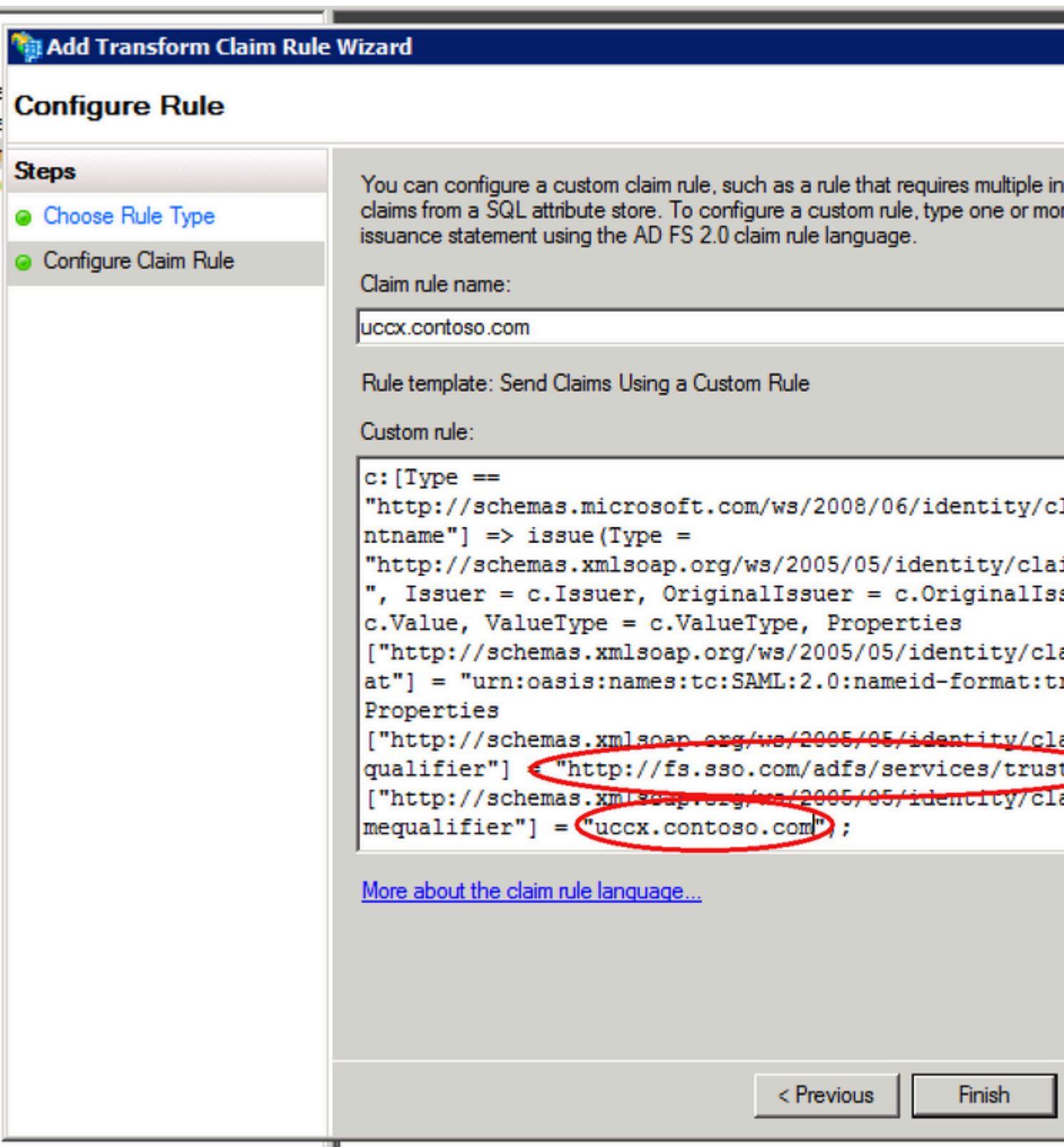
Using a custom rule, you can create rules that can't be created with a rule template written in the AD FS 2.0 claim rule language. Capabilities that require custom rules:

- 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 >



Schritt 8: Klicken Sie mit der rechten Maustaste auf die Vertrauensstellung der vertrauenden Partei, und klicken Sie dann auf **Properties** und wählen Sie die Registerkarte "Erweitert" aus, wie im Bild dargestellt.

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

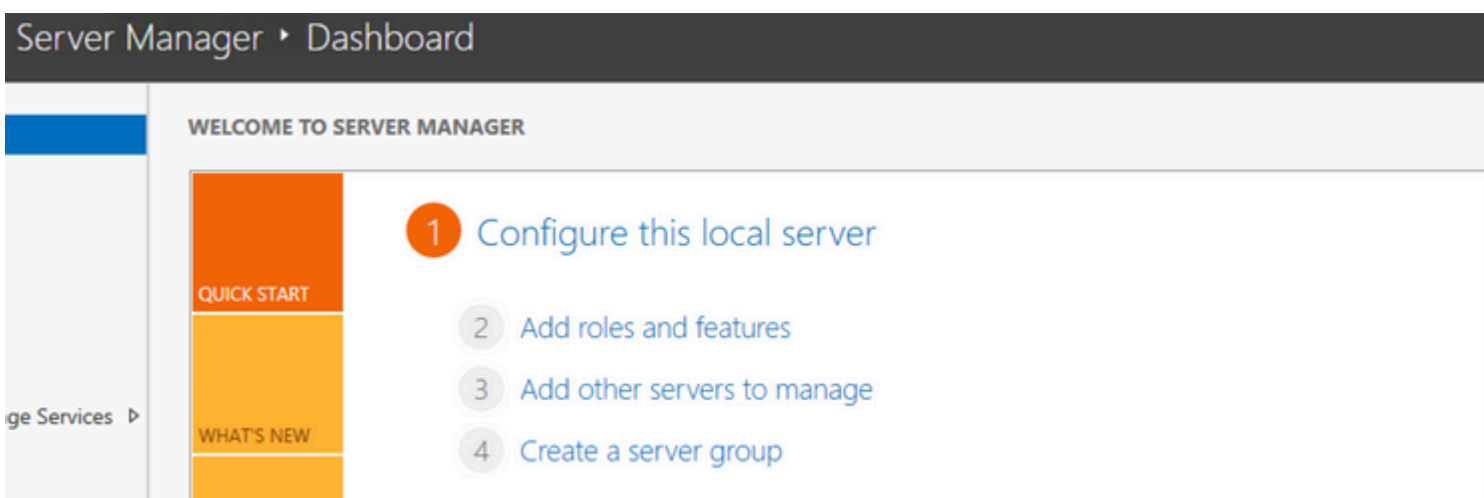
Schritt 9. Wählen Sie Secure Hash Algorithm (SHA) als SHA-256 aus, wie im Bild gezeigt.



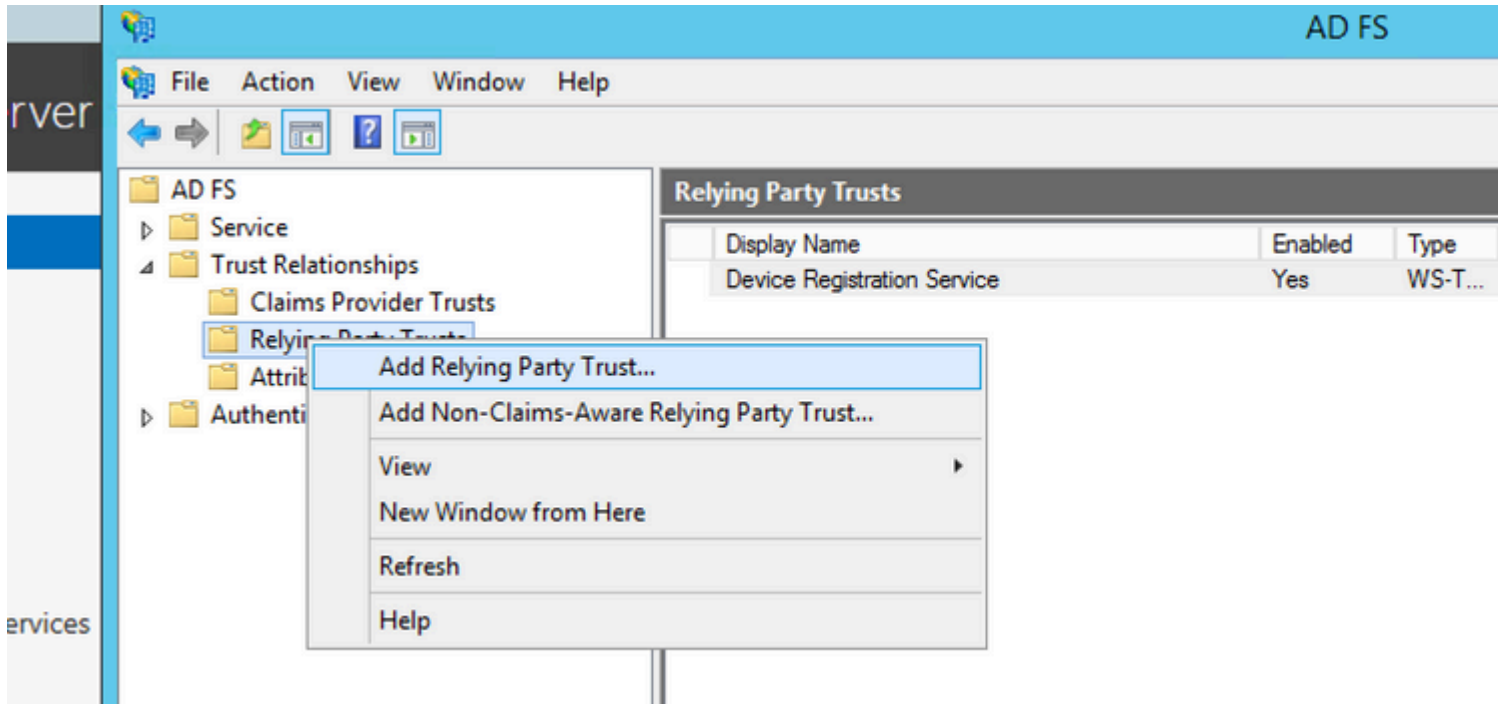
Schritt 10. Klicken Sie auf OK.

ADFS 3.0

Schritt 1: Navigieren Sie im ADFS-Server zu Server Manager > Tools > ADFS Management.



Schritt 2: Navigieren Sie zu ADFS > Trust Relationship > Relying Party Trust.



Schritt 3: Wählen Sie die Option 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.

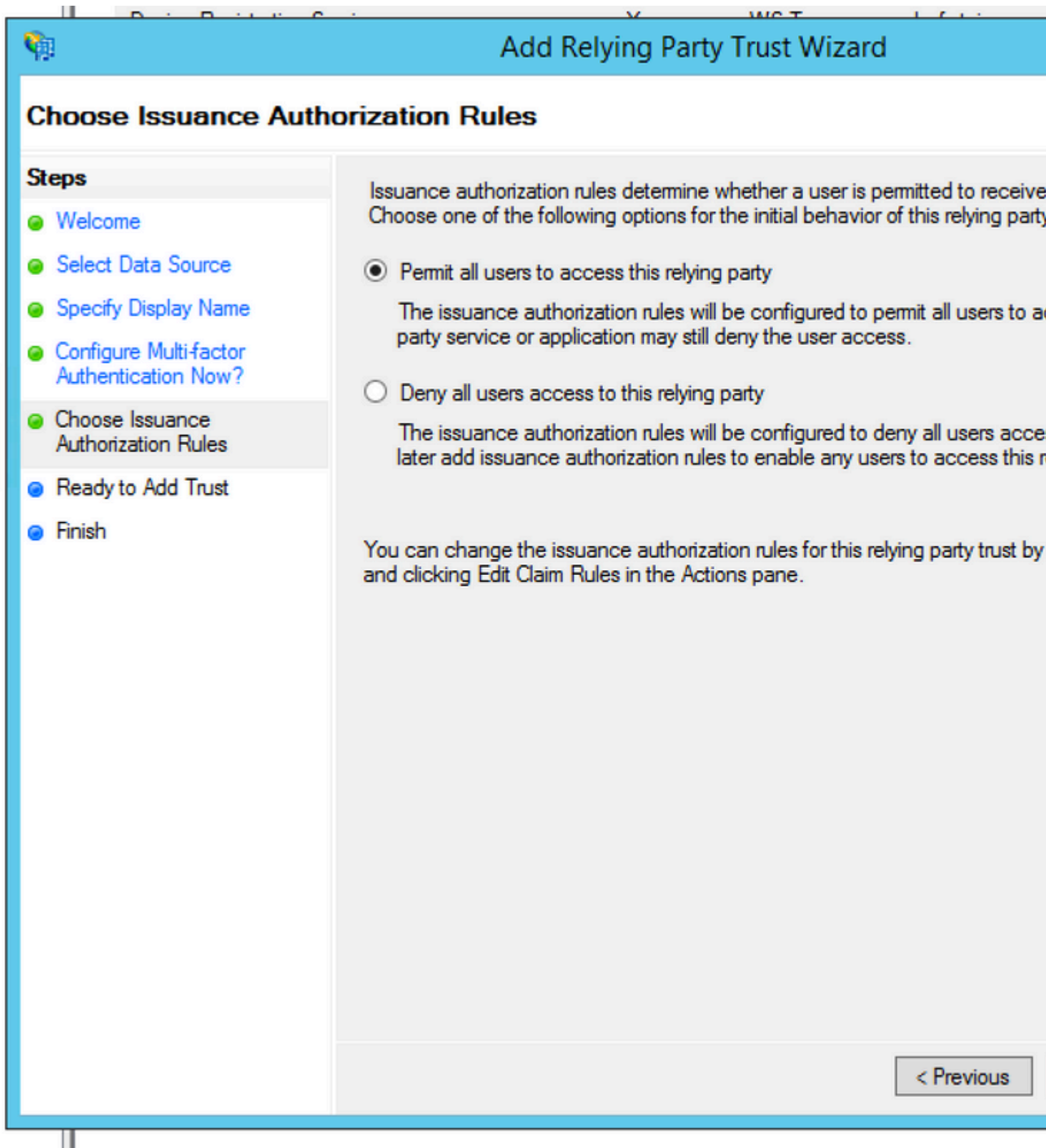
Multi-factor Authentication

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

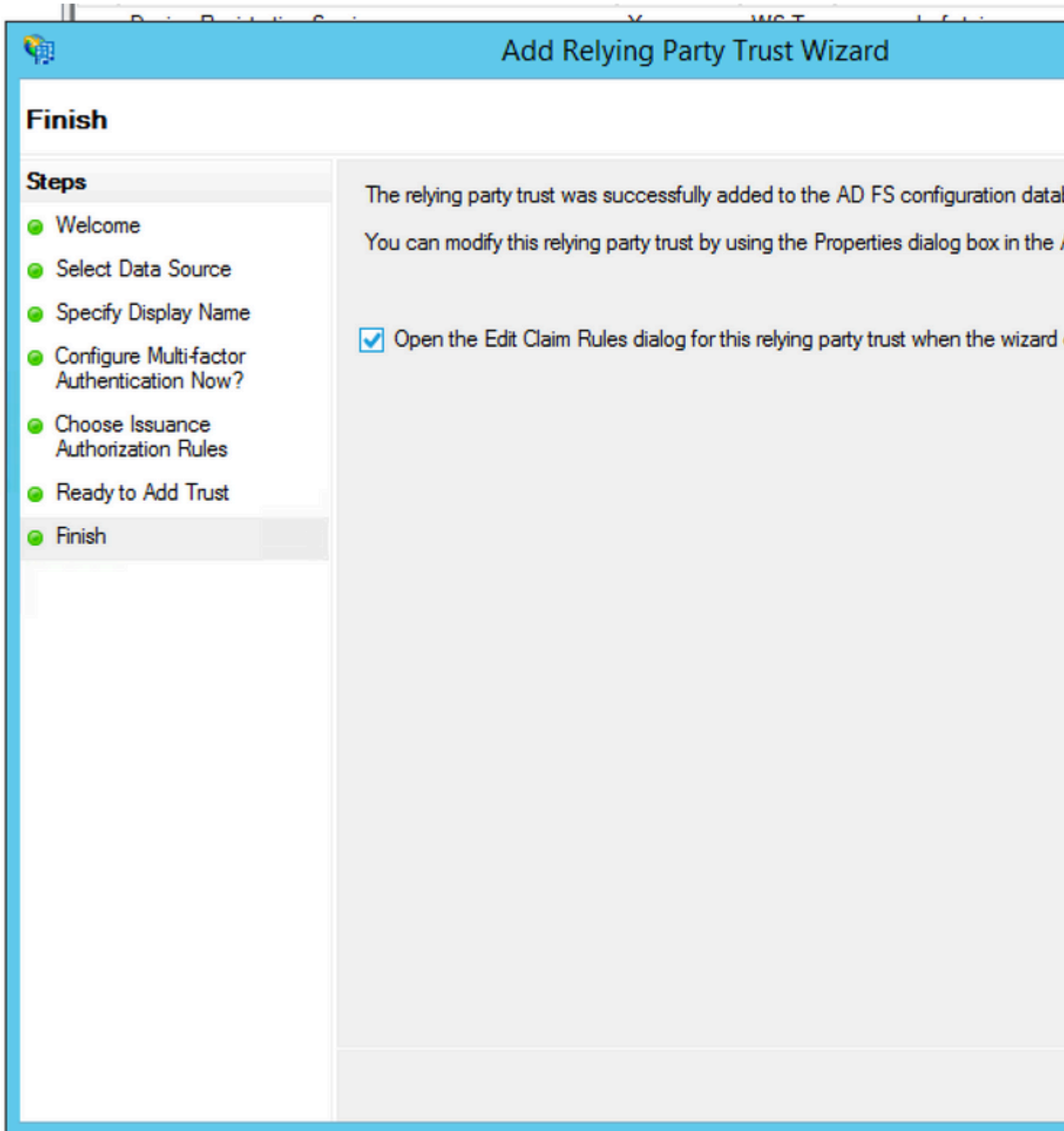
- I do not want to configure multi-factor authentication settings for this relying party trust.
- Configure multi-factor authentication settings for this relying party trust.

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



Schritt 4: Vollständige Einrichtung des Vertrauens der vertrauenden Seite.



Schritt 5: Wählen Sie in den Eigenschaften von Relying Party Trust die Option Identifier aus.

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

Schritt 6: Legen Sie den Bezeichner als vollqualifizierten Hostnamen des Cisco Identity Server fest, von dem `sp.xml` heruntergeladen wird.

uccx115p1.toi.com Properties

Organization	Endpoints	Proxy Endpoints	Notes	Advanced
Monitoring	Identifiers	Encryption	Signature	Accepted Certificates

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

Schritt 7. Klicken Sie mit der rechten Maustaste auf Vertrauenswürdigkeit der vertrauenden Partei, und klicken Sie auf Vertrauenswürdigkeit. Sie müssen zwei Anspruchsregeln hinzufügen. Die eine ist, wenn die LDAP-Attribute zugeordnet werden, w

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

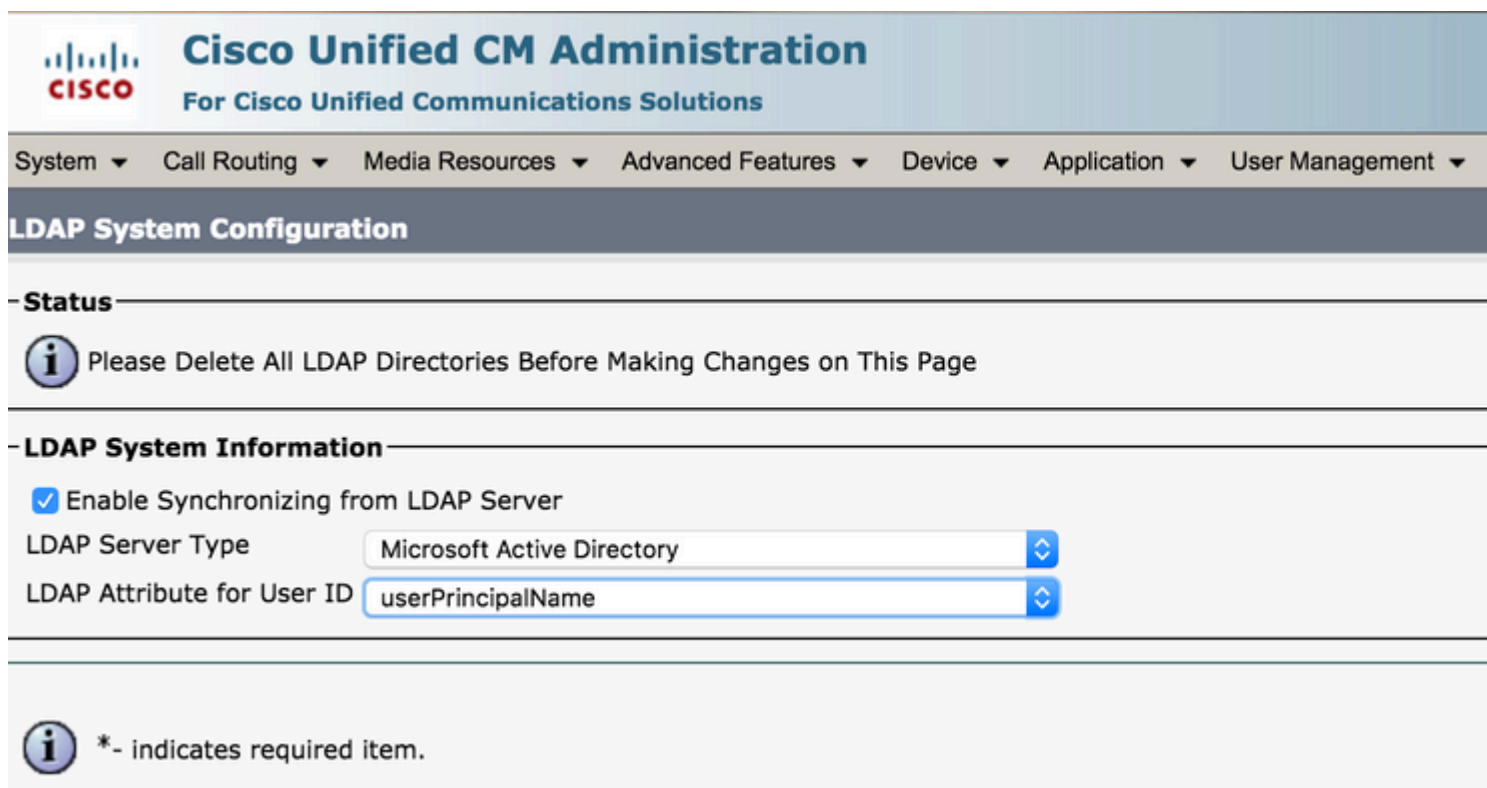
Attribute store:

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=""/>

Hinweis: Sie müssen sicherstellen, dass das für die Benutzer-ID bei der CUCM-LDAP-Synchronisierung konfigurierte LDAP-Attribut mit dem LDAP-Attribut übereinstimmt. uid in der ADFS-Anspruchsregel NameID. Dies dient der ordnungsgemäßen Funktion der CUIC- und Finesse-Anmeldung.

Hinweis: In diesem Dokument wird auf Einschränkungen für den Namen der Anspruchsregel und Anzeigenamen wie NameID, FQDN von UCCX usw. verwiesen. Obwohl benutzerdefinierte Felder und Namen in verschiedenen Abschnitten verwendet werden können, werden die Namen der Anspruchsregeln und die Anzeigenamen durchgehend als Standard beibehalten, um die Konsistenz und die bewährten Verfahren in der Namenskonvention zu erhalten.



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. The main heading is "LDAP System Configuration". Below this, there is a "Status" section with an information icon and the text: "Please Delete All LDAP Directories Before Making Changes on This Page". The "LDAP System Information" section includes 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, there is an information icon and the text: "*- indicates required item."

Anspruchsregel 2:

- Fügen Sie eine weitere Regel vom Typ "Benutzerdefinierte Anspruchsregel" mit dem Namen "Vollqualifizierter Hostname" von Cisco Identity Server hinzu, und fügen Sie diesen Regeltext hinzu.

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

- Im Cisco Identity Server-Cluster sind alle vollständig qualifizierten Hostnamen die des primären oder Herausgeberknotens von Cisco Identity Server.
- Beim <full qualified hostname of Cisco Identity Server> wird die Groß-/Kleinschreibung beachtet, sodass er genau (einschließlich der Groß-/Kleinschreibung) mit dem FQDN des Cisco Identity Server übereinstimmt.
- Beim <ADFS-Server-FQDN> wird die Groß-/Kleinschreibung beachtet, sodass er genau (einschließlich der Groß-/Kleinschreibung) mit dem ADFS-FQDN übereinstimmt.

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:  
nameid-format"] = "urn:oasis:names:tc:SAML:2.0:nameid-format:transient", Properties  
["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperty:  
nameid-qualifier"] = "http://fs.contoso.com/adfs/services/trust", Properties  
["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperty:  
nameid-issuer"] = "http://fs.contoso.com/adfs/services/trust", Properties  
["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperty:  
nameid-qualifier"] = "uccx.contoso.com");
```

OK

: Schritt 2. ist nicht erforderlich, wenn Sie ADFS 3.0 verwenden, da CmdLet bereits als Teil des Hinzufügens der Rollen und Funktionen installiert ist.

Hinweis:

Groß- und Kleinschreibung beachten, sodass die Groß- und Kleinschreibung mit dem übereinstimmt, was auf der Registerkarte Identifier der Trust-Eigenschaften der vertrauenden Partei festgelegt ist.

Hinweis: Cisco IdS unterstützt ab UCCX-Version 12.0 SHA-256. Die Vertrauensstellung der vertrauenden Partei verwendet SHA-256 zum Signieren der SAML-Anforderung und erwartet dieselbe Antwort von ADFS.

Konfiguration mehrerer Domänen für Federated ADFS

Wenn ein ADFS in einer bestimmten Domäne im Fall der Verbund-Funktion in ADFS die verbündete SAML-Authentifizierung für Benutzer in anderen konfigurierten Domänen bereitstellt, sind diese zusätzlichen Konfigurationen erforderlich.

In diesem Abschnitt bezieht sich der Begriff primäres ADFS auf das ADFS, das in IdS verwendet werden muss. Der Begriff Federated ADFS bezeichnet diejenigen ADFS, deren Benutzer sich über IdS anmelden können und somit das primäre ADFS sind.

Federated ADFS-Konfiguration

In jedem der verknüpften ADFS muss die Vertrauensstellung der vertrauenden Partei für das primäre ADFS und die Anspruchsregeln erstellt werden, die wie im vorherigen Abschnitt beschrieben konfiguriert wurden.

Primäre ADFS-Konfiguration

Für primäre ADFS ist neben der Vertrauensstellung der vertrauenden Partei für IDs diese zusätzliche Konfiguration erforderlich.

Hinzufügen Claim Provider Trust mit dem ADFS, für das der Verbund eingerichtet werden muss.

Stellen Sie im Claim Provider Trust sicher, dass die Pass through or Filter an Incoming Claim Regeln werden so konfiguriert, dass alle Anspruchswerte als Option weitergegeben werden:

- Namens-ID
- Wählen Sie die Name-ID aus dem Incoming Claim Type Absetzkasten
- Auswählen Transient als Option für das Format "Incoming NameID"
- uid: Dies ist ein benutzerdefinierter Anspruch. Geben Sie den Wert uid im Feld Incoming Claim Type Absetzkasten
- user_principale: Dies ist ein benutzerdefinierter Anspruch. Geben Sie den Wert user_principale im Feld Incoming Claim Type Absetzkasten

Fügen Sie unter Relying Party Trust for IDs (Vertrauenswürdige Partei für IDs) Folgendes hinzu: Pass through or Filter an Incoming Claim -Regeln, wobei alle Anspruchswerte als Option weitergegeben werden.

- NameIDFromSubdomäne
- Namens-ID auswählen aus Incoming Claim Type Absetzkasten
- Auswählen Transient als Option für das Format "Incoming NameID"
- uid: Dies ist ein benutzerdefinierter Anspruch. Geben Sie uid in das Feld Incoming Claim

Type Absetzkasten

- user_principale: Dies ist ein benutzerdefinierter Anspruch. Geben Sie den Wert user_principale im Feld Incoming Claim Type Absetzkasten

Automatischer ADFS-Zertifikatrollover

Der automatische Zertifikats-Rollover wird für UCCX 11.6.1 und höher unterstützt. (Dieses Problem konnte durch das Fedlet Library-Upgrade auf Version 14.0 in UCCX 11.6 behoben werden.)

Kerberos-Authentifizierung (integrierte Windows-Authentifizierung)

Die integrierte Windows-Authentifizierung (IWA) stellt einen Mechanismus für die Authentifizierung der Benutzer bereit, lässt jedoch keine Übertragung von Anmeldeinformationen über das Netzwerk zu. Wenn Sie die integrierte Windows-Authentifizierung aktivieren, arbeitet auf der Grundlage von Tickets, um Knoten die Kommunikation über ein unsicheres Netzwerk zu ermöglichen, um ihre Identität untereinander auf sichere Weise zu beweisen. Benutzer können sich nach der Anmeldung bei ihren Windows-Computern bei einer Domäne anmelden.

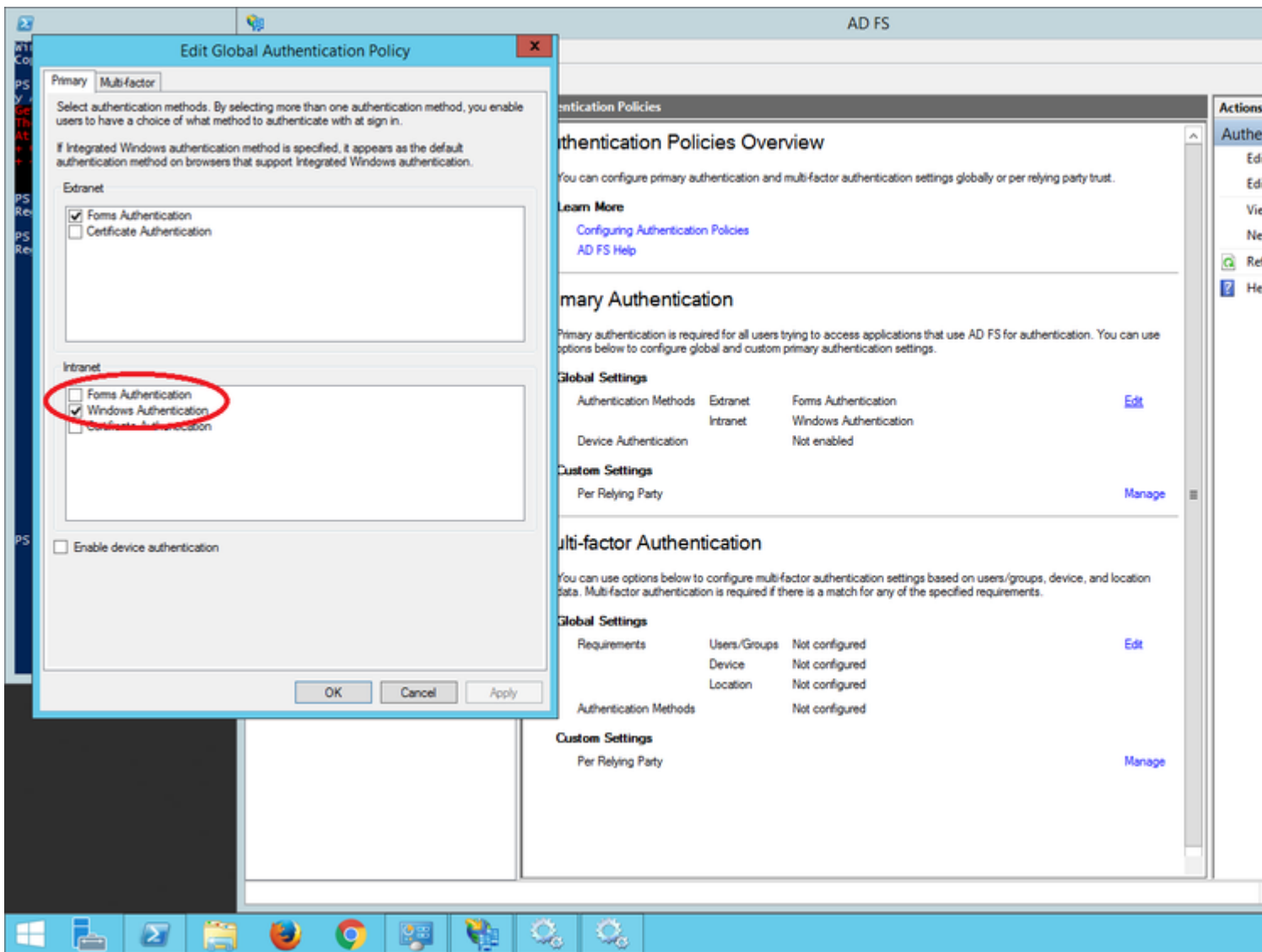
Hinweis: Die Kerberos-Authentifizierung wird nur ab Version 11.6 unterstützt.

Domänenbenutzer, die bereits beim Domänencontroller (DC) angemeldet sind, werden nahtlos bei SSO-Clients angemeldet, ohne dass die Anmeldeinformationen erneut eingegeben werden müssen. Für Benutzer ohne Domäne greift IWA auf New Technology Local Area Network Manager (NTLM) zurück, und der Anmeldedialog wird angezeigt. Die Qualifizierung für IdS mit IWA-Authentifizierung erfolgt mit Kerberos gegen ADFS 3.0.

Schritt 1: Öffnen Sie die Windows-Eingabeaufforderung, und führen Sie sie als Administrator aus, um den HTTP-Dienst beim `setspn` command `setspn -s http/`

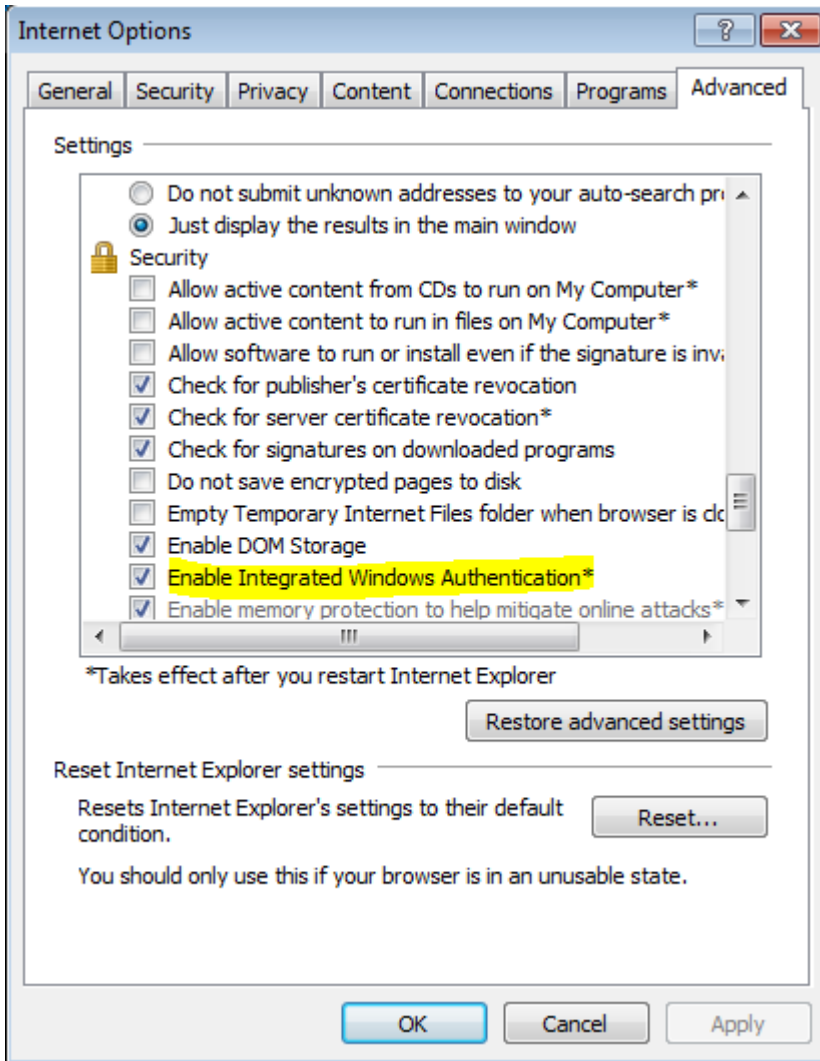
\

Schritt 2: Deaktivieren der Formularauthentifizierung und Aktivieren der Windows-Authentifizierung für Intranet-Sites Navigieren Sie zu ADFS Management > Authentication Policies > Primary Authentication > Global Settings > Edit. Vergewissern Sie sich unter Intranet, dass nur Windows-Authentifizierung aktiviert ist (deaktivieren Sie die Option Formularauthentifizierung).



Konfiguration für Microsoft Internet Explorer für IWA-Support

Schritt 1: Stellen Sie Folgendes sicher Internet Explorer > Advanced > Enable Integrated Windows Authentication ist aktiviert.



Schritt 2: ADFS-URL muss hinzugefügt werden zu Security > Intranet zones > Sites (winadcom215.uccx116.com ist die ADFS-URL).

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...

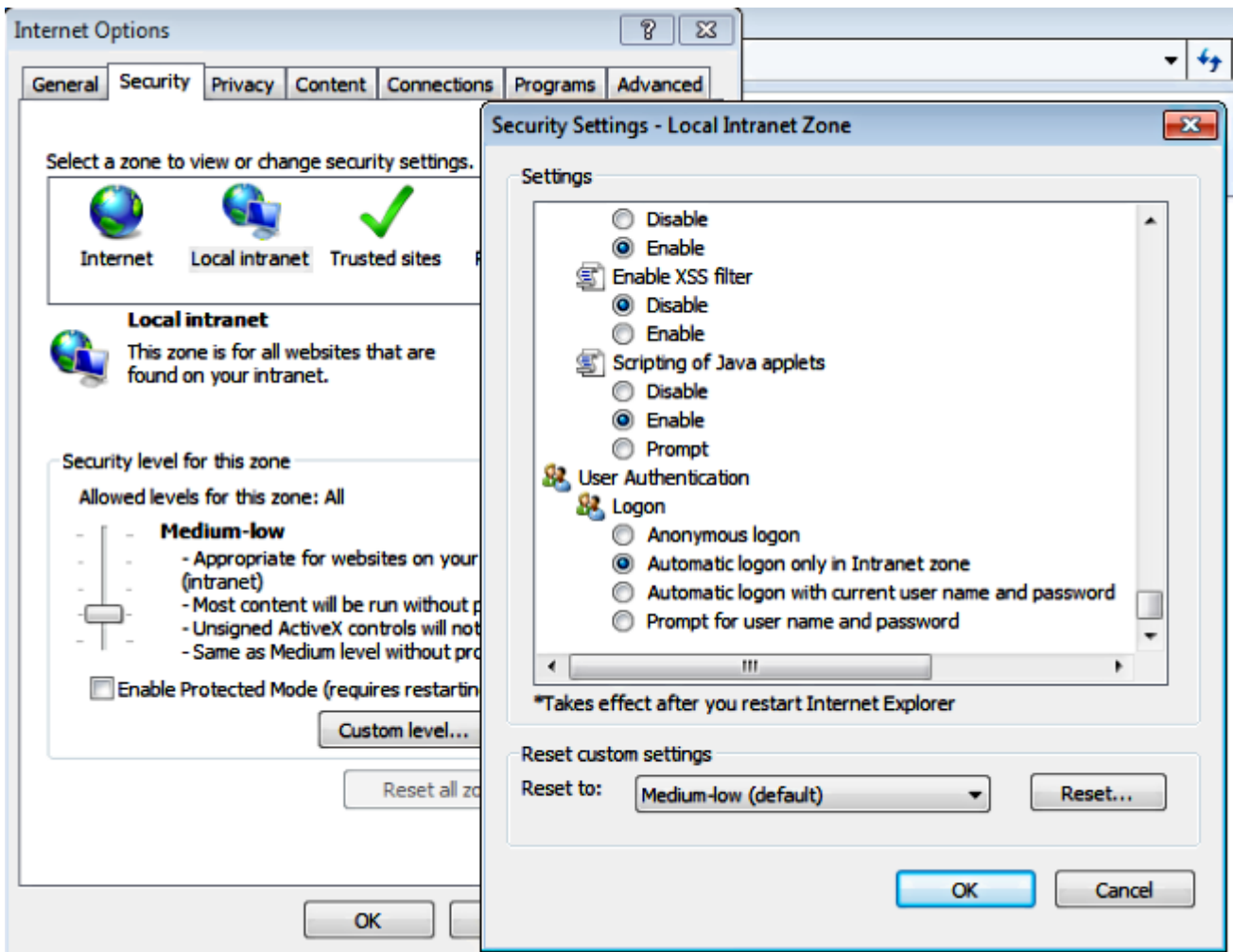
Default level

Reset all zones to default level

OK

Cancel

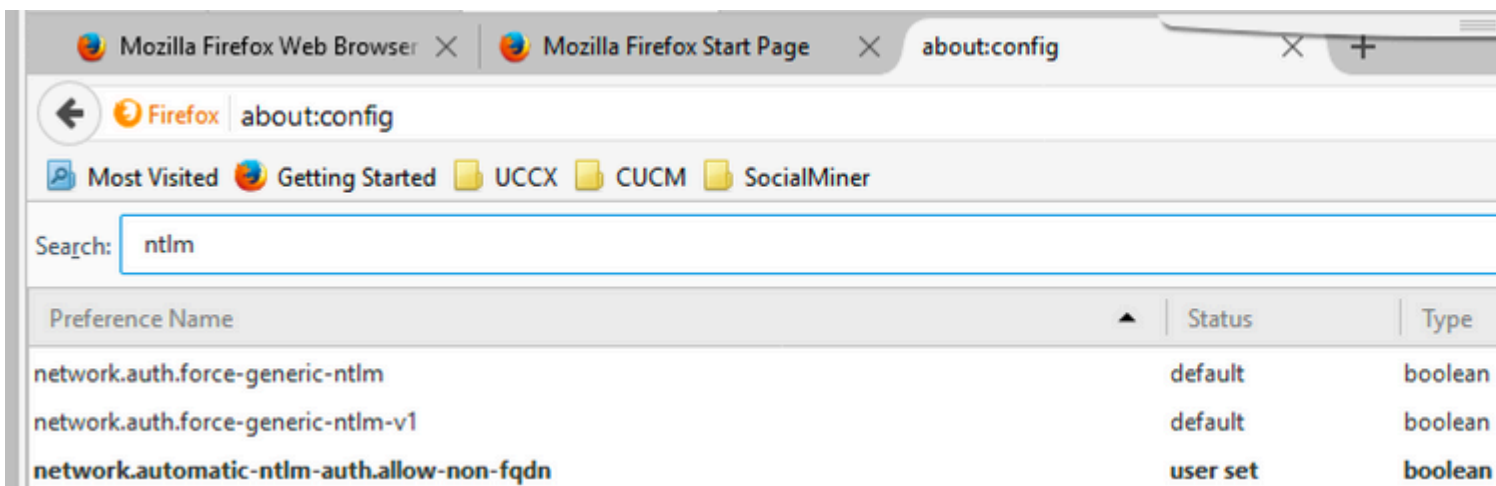
Ap



Erforderliche Konfiguration für Mozilla Firefox für IWA-Support

Schritt 1: Wechseln Sie in den Konfigurationsmodus für Firefox. Öffnen Sie Firefox, und geben Sie `about:config` in der URL. Akzeptieren Sie die Risikoubersicht.

Schritt 2: Suchen nach `ntlm` und aktivieren Sie die `network.automatic-ntlm-auth.allow-non-fqdn` und auf "true" festgelegt.



Schritt 3: Stellen Sie `network.automatic-ntlm-auth.trusted-uris` der Domäne oder explizit der ADFS-URL.

network.automatic-ntlm-auth.allow-proxies	default	bool
network.automatic-ntlm-auth.trusted-uris	user set	string
network.generic-ntlm-auth.workstation	default	string

Konfiguration erforderlich für Google Chrome zur IWA-Unterstützung

Google Chrome in Windows verwendet die Internet Explorer-Einstellungen, so konfigurieren Sie in Internet Explorer Tools > Internet Options oder in der Systemsteuerung unter Internet Options innerhalb der Unterkategorie Network and Internet.

Weitere Konfiguration für SSO

In diesem Dokument wird die Konfiguration aus dem IdP-Aspekt für SSO zur Integration in Cisco IdS beschrieben. Weitere Informationen finden Sie in den jeweiligen Produktkonfigurationsanleitungen:

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

Überprüfung

Anhand dieses Verfahrens wird ermittelt, ob die Vertrauensstellung der vertrauenden Partei zwischen Cisco IdS und IDP ordnungsgemäß eingerichtet wurde.

- Geben Sie im Browser die URL [Daraufhin wird eine Checklisten-seite angezeigt.](https://<ADFS_FQDN>/adfs/ls/IdpInitiatedSignOn.aspx?loginToRp=<IDS_FQDN> ein.
• ADFS stellt das Anmeldeformular bereit. Diese Option steht zur Verfügung, wenn die oben angegebene Konfiguration korrekt ist.
• Nach erfolgreicher Authentifizierung muss der Browser eine Umleitung zu <a href=)

Hinweis: Die Seite "Checkliste", die als Teil des Überprüfungsprozesses angezeigt wird, ist kein Fehler, sondern eine Bestätigung, dass die Vertrauensstellung ordnungsgemäß eingerichtet ist.

Fehlerbehebung

Informationen zur Fehlerbehebung finden Sie unter <https://www.cisco.com/c/en/us/support/docs/customer-collaboration/unified-contact-center-express/200662-ADFS-IdS-Troubleshooting-and-Common-Prob.html>.

UCCX SSO-Umgehungs-/Wiederherstellungs-URLs

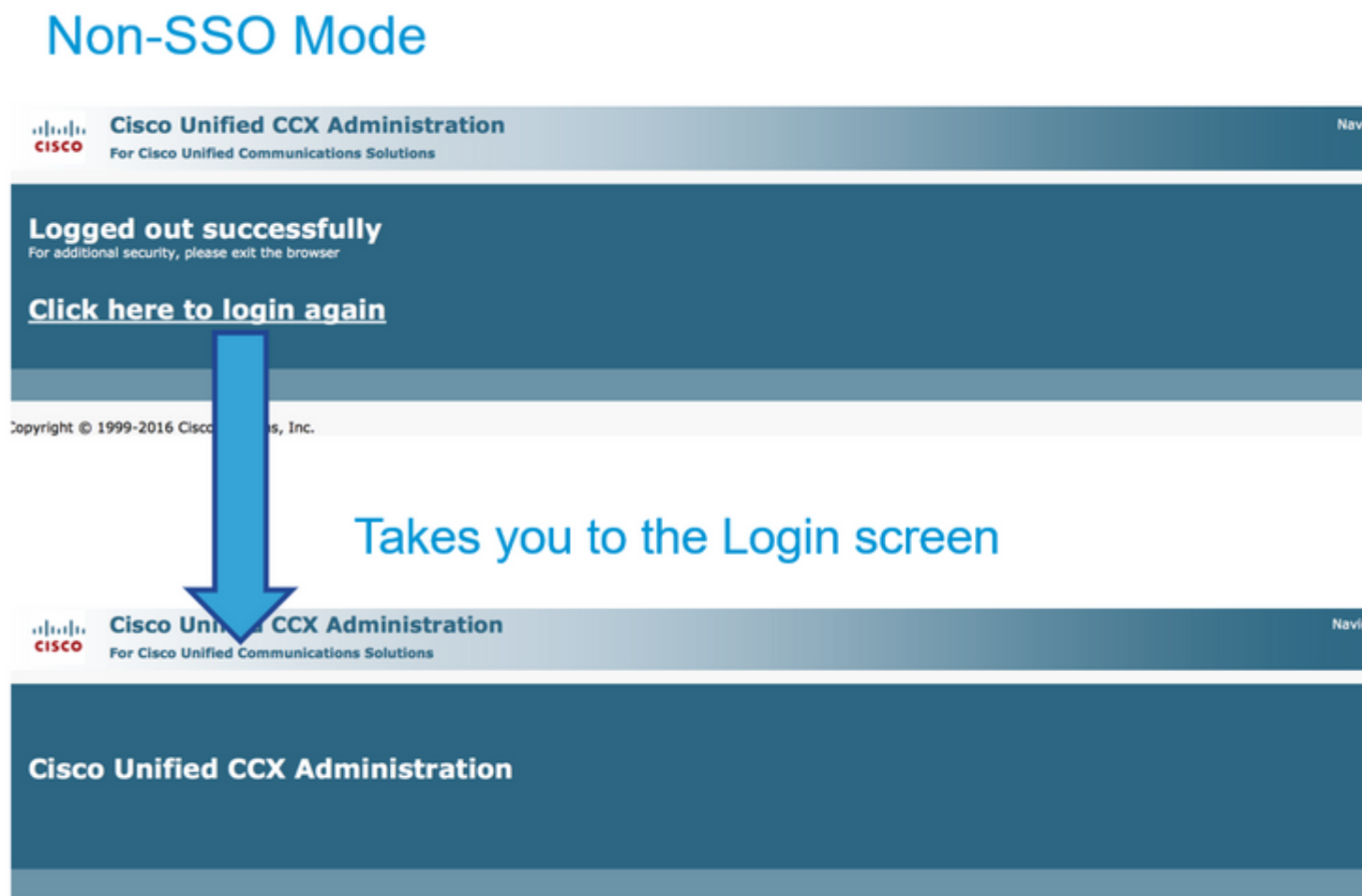
- [Cisco Unified CCX-Verwaltung](#)
- [Cisco Unified CCX Serviceability](#)

SSO deaktivieren

- GUI: Navigieren zu CCX Administration > Single Sign-On (SSO) > Disable.
- CLI: set authmode non_sso (Mit diesem Befehl muss SSO für Pub und Sub deaktiviert werden. Er kann bei einem HA-Cluster (High Availability) von einem der beiden UCCX-Knoten ausgeführt werden.)

Screenshots

CCX-Administration - Nicht_SSO



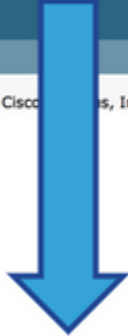
CCX-Administration - SSO aktiviert

SSO Mode

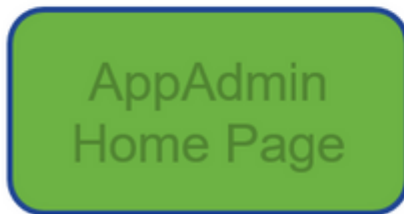
Logged out successfully

For additional security, please exit the browser

[Click here to login again](#)



Takes to the AppAdmin Home page if authenticated with IdP



Finesse-Anmeldung - Nicht-SSO



Username*

Password*

Extension*



Finesse
desktop home
page

Finesse-Anmeldung - SSO aktiviert



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

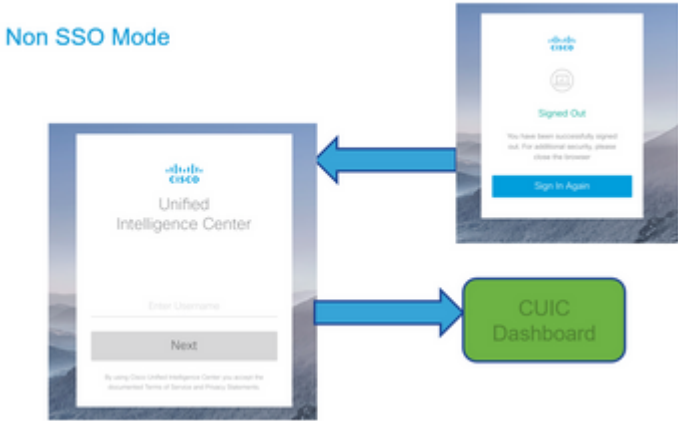
 Cisco Finesse

Username* chaitra

Extension*

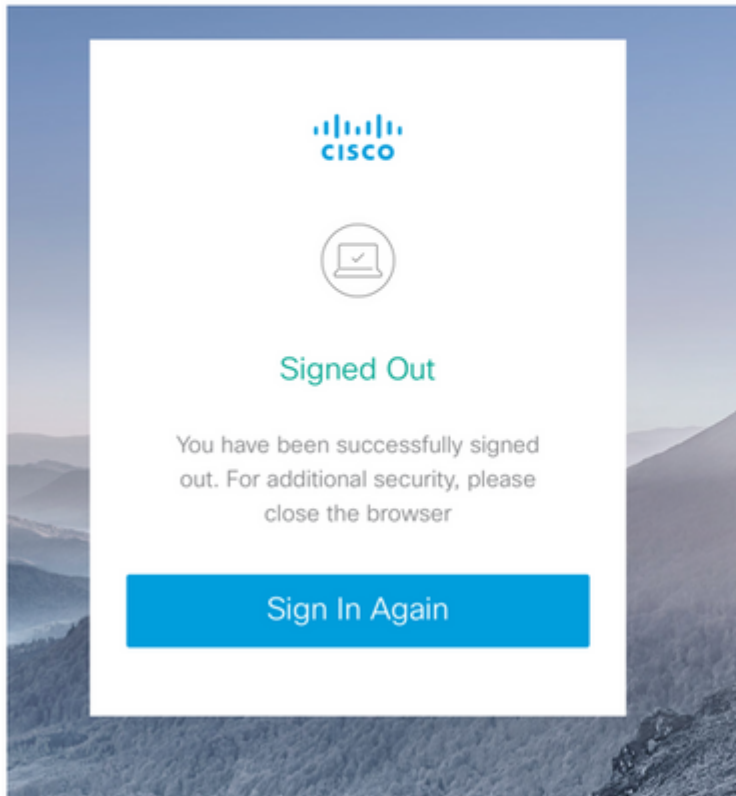


CUIC - Nicht_SSO

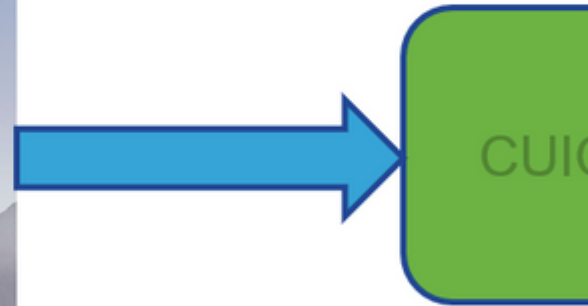


CUIC - SSO aktiviert

SSO Mode



Takes to the CUIC Dashboard if authenticated with IdP



Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.