ç,ºæ€ï¿½ç§'èº«ä»½æœï¿½å‹™é…ï¿½ç½®èº«ä»½æ

ç›®éŒ„

ç°¡ä»‹

æœ¬æ–‡ä»‹ç´¹ç,ºæ€ï¿½ç§'èº«ä»½æœï¿½å‹™(IdS)é…ï¿½ç½®èº«ä»½æ��ä¾›ç¨ ‹å¼¢(IdP)ä¥å•Ÿç”¨å–®ä

å¿…è¦ï¿½æ¢ï¿½ä»¶

éœ€æ±‚

æ€ç§'å»ºè°æ,¨çžè§£ä»¥ä¸‹ä¸»é¡Œï¼š

- Cisco Unified Contact Center Express(UCCX)ç‰ˆæœ¬11.5æ˜–Cisco Unified Contact Center Enterpriseç‰ˆæœ¬11.5æ˜–Packaged Contact Center Enterprise(PCCE)ç‰ˆæœ¬11.5ï¼ˆå¦‚æžœé©ç”¨ï¼‰
- Microsoft Active Directory - Windows Serverä¸Šå®‰è£ç„AD
- Active Directoryè¯¯å®ˆè°«ä½©—è‰æœ€å‹™(ADFS)ç‰ˆæœ¬2.0/3.0

è¨»ï¼šæœ¬æ–‡æª”åœ¨èž¢å¹•æˆªåœ–å'Œç¤ºä¾‹ä¸•ç”¨äº†UCCXï¼Œä½†æ˜¯å…¶é…ç½®ä¹Ÿé€‚ç”¨äºCisco IdS(UCCX/UCCE/PCCE)å'ŒIdPç›¸ä¼¼ã€‚

æŽ¡ç”¨å…ƒä»¶

æœ¬æ–‡ä»¶ä¸çš„è³‡è¨Šå¹šè»Ÿé«”ç‰ˆæœ¬ã€‚

æœ¬æ–‡ä¸çš„è³‡è¨Šæ˜¯æ ¹æ“šç‰¹å®šå¯¦é©—å®¤ç’°å¢ƒä¸çš„è£ç½®æ‰€å»ºç«‹ã€‚æ–‡ä¸使用的所有裝置均已清除（預設）組態。如果您的網路處於實時運作中，請確保您瞭解任何命令可能造成的影響。

èƒŒæ™¯è³‡è¨Š

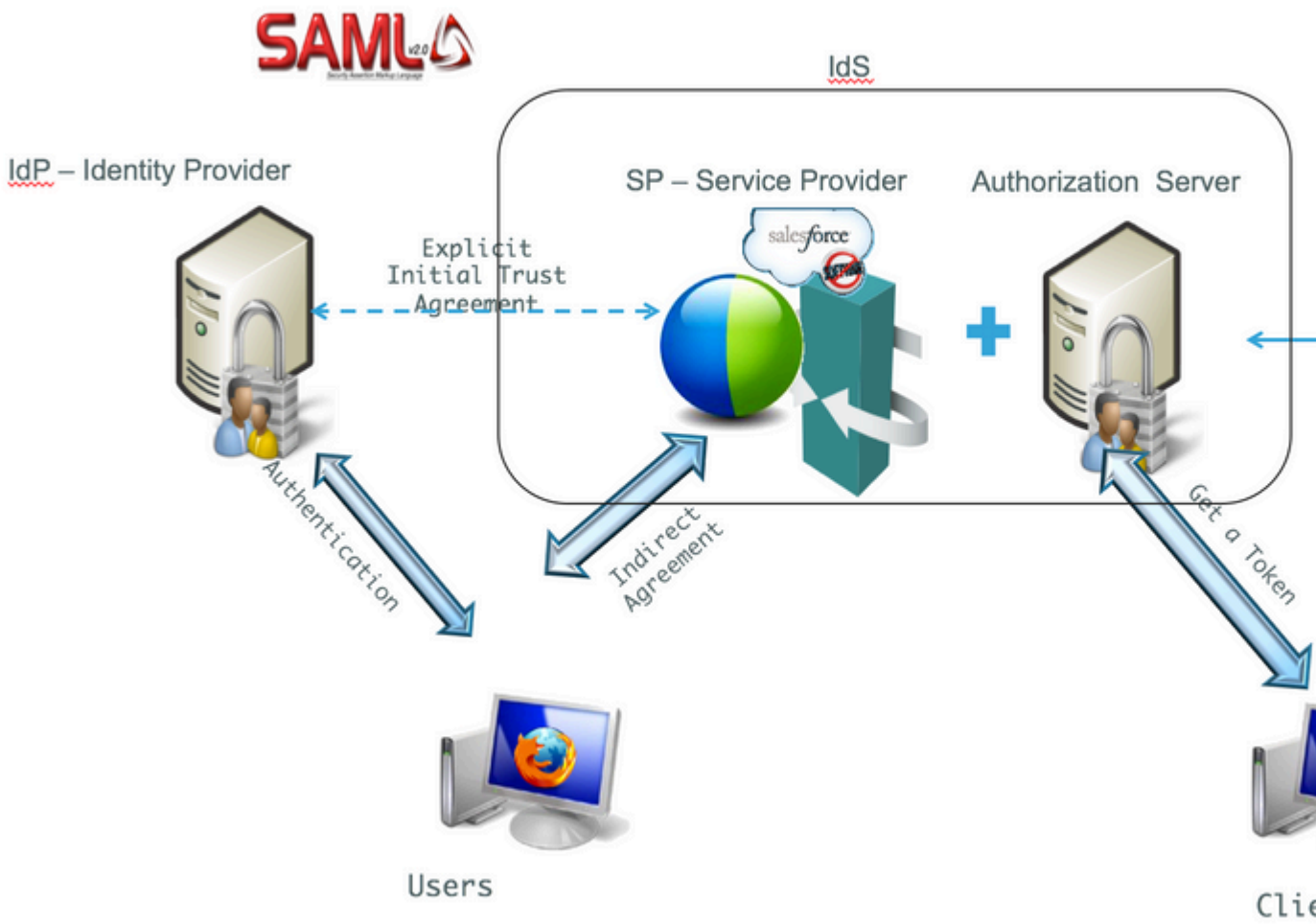
Cisco IdSéƒ¨ç½²æ¡å¼

ç”¢å“	éƒ¨ç½²
UCCX	å…±ä½è€...
PCCE	èˆ‡CUICï¼ˆæ€§ç‘çµ±ä¸€æƒ...å ±ä¸¿ï¼‰å'ŒLDï¼ˆå•³æ™‚è³‡æ–™ï¼‰å...å˜
UCCE	èˆ‡CUICå'ŒLDå…±é§•ä»¥é€²è¡Œ2kéƒ¨ç½²ã€‚ ç•¨ç«‹å¼•ï¼Œé©©ç”¨æ–¼4kå'Œ12kéƒ¨ç½²ã€‚

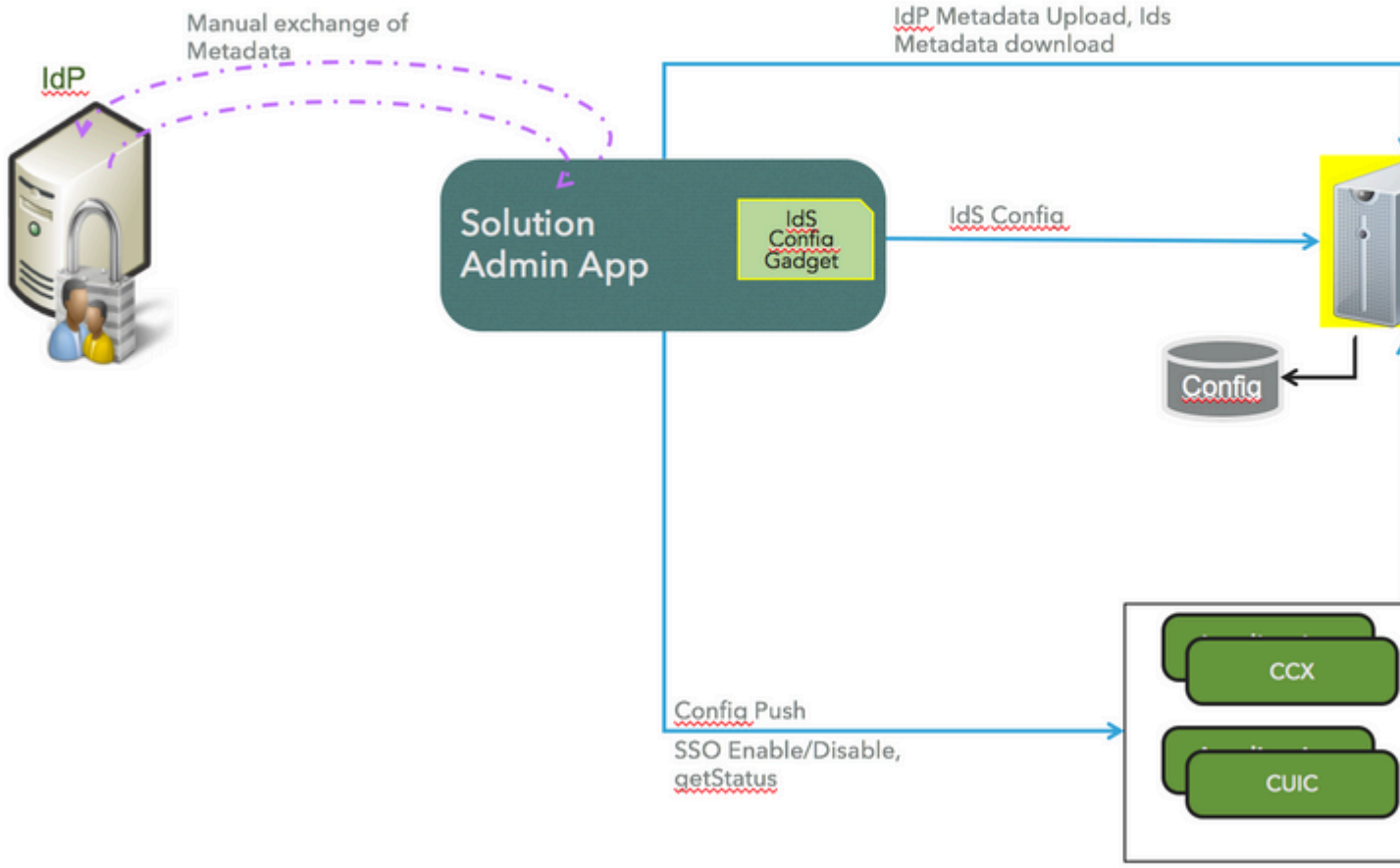
SSOæ¦‚è¿°

æ€ç§'ä»¥ä¸•å•Œçš„å½¢å¼•æ••ä¾›å¤šç¨®æœ€å‹™ï¼Œç¨ä½¿ç”¨è€…èº«ä»½æ,¨å•ªé

ä½¿ç”¨SAMLï¼ˆå®‰全æ–·è¨€æžè¨€ï¼‰çš„SSOé•¢å•'æ¤è¦•æ±,ã€,SAML/SSOå...•è¨±ä½¿ç
11.5å•Šæ›´é«˜ç‰ˆæœ¬ä¸•ç”¨ã€,


SAML 2.0
IdS
IdP – Identity Provider
SP – Service Provider
Authorization Server
salesforce
Explicit
Initial Trust
Agreement
Authentication
Indirect
Agreement
Get a Token
Users
Clie

çµæ…‹æ¦‚è§€



è¨å®š

é©—è‰ža‹å^¥

Cisco IdSå*f*…æ”¯æ´IdPçš„åŸºæ–¼è¡¨å–®çš„è°«ä»½é©—è‰ã€‚

è«‹å€fé–±é€™äº›MSDNæ–‡ç« ä»¥çžè§£å¦‚ä½•åœ¨ADFSä¸•Ÿç”¨è¡¨å–®è°«ä»½é©—è‰ã€‚

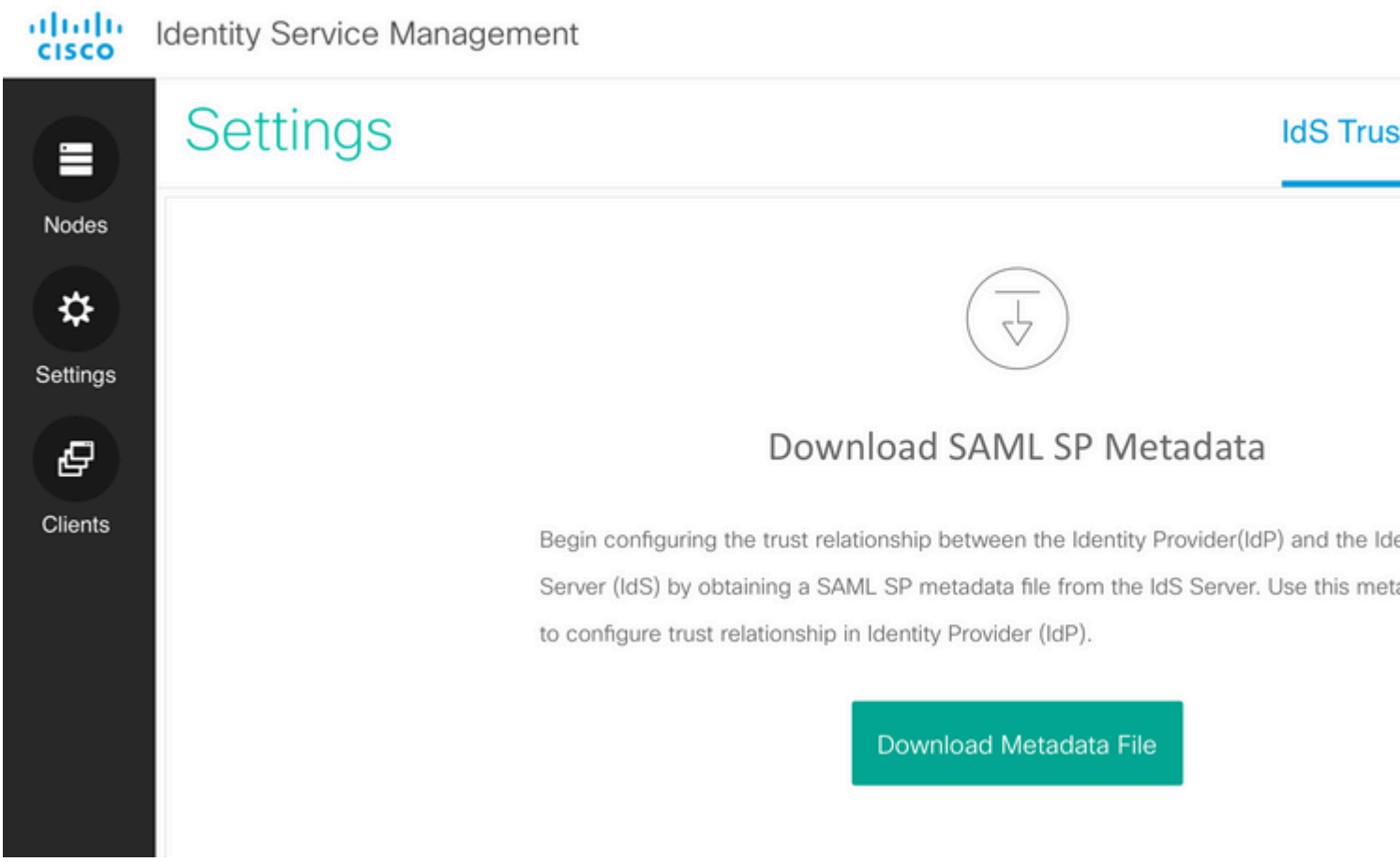
- æœ‰é—œADFS 2.0çš„è³‡è¨Šï¼Œè«‹å€fé–±æ¤Microsoft TechNetæ–‡ç« ï¼Œ http://social.technet.microsoft.com/wiki/contents/articles/1600.ad-fs-2-0-how-to-change-the-local-authentication-type.aspxã€‚
- æœ‰é—œADFS 3.0çš„è³‡è¨Šï¼Œè«‹å€fé–±æ¤Microsoft TechNetæ–‡ç« ï¼Œ https://learn.microsoft.com/en-us/archive/blogs/josrod/enabled-forms-based-authentication-in-adfs-3-0

æ³¨æ„:Cisco IdS 11.6å€Šæ›´é«˜ç‰ˆæœ¬å€Œæ™‚,æ”¯æ´åŸºæ–¼è¡¨å–®çš„è°«ä»½é©—è‰Kerberosè

å»ºç«‹ä¿¡ä»»é—œä¿‚

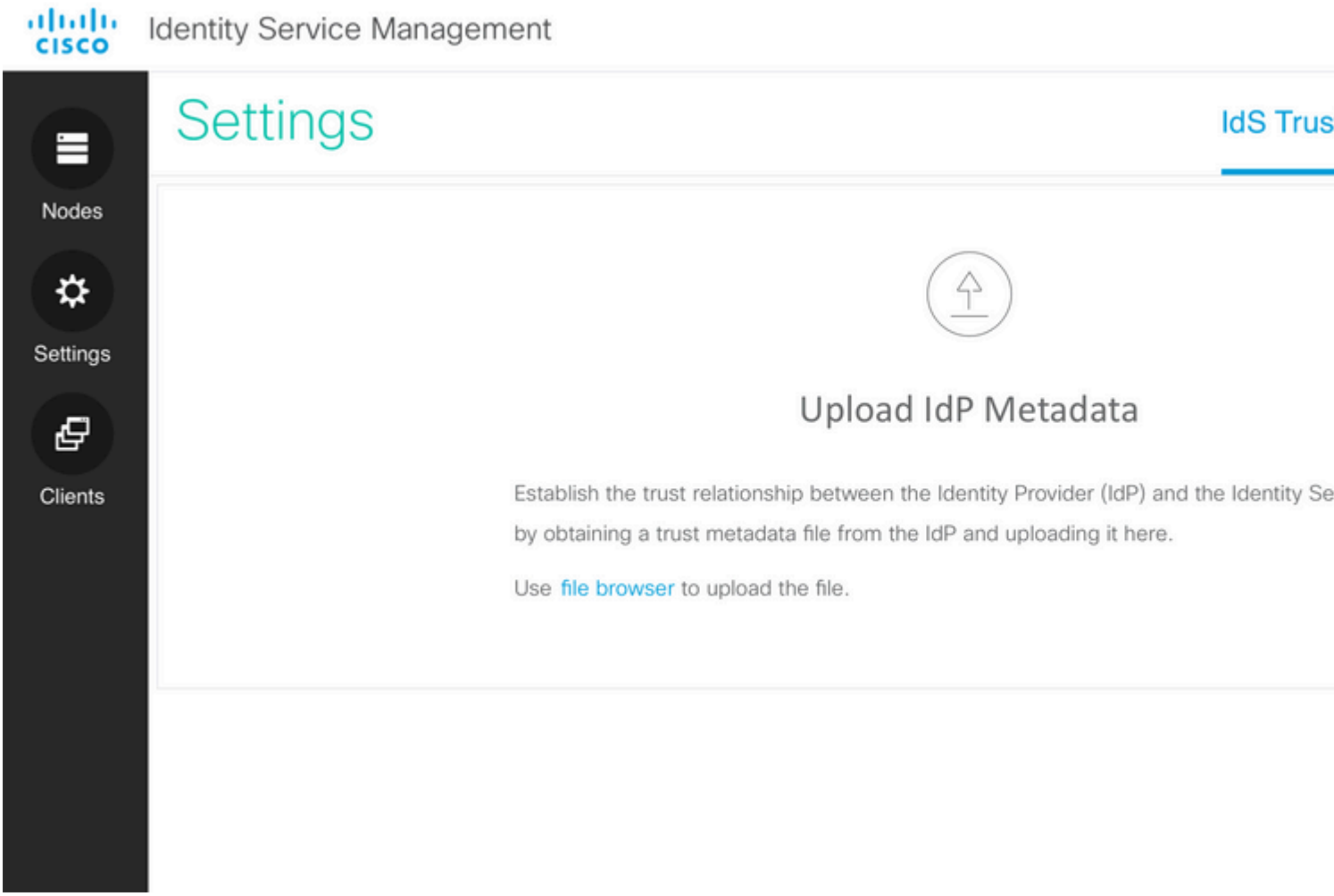
å°

- ä¸‹è¼‰SAML SPå¾Œè¨è³‡æ–™æª”æ¡ˆ sp.xml.
- è‡ª Settingsï¼Œå°Žèˆªè‡³ IdS Trust é ç±¤ã€‚



- å¾žURLçš„IdPä¸‹è¼‰IdPå¾Œè¨è³‡æ–™æª”æ¡ˆï¼š https://<ADFSServer>/federationmetadata/2007-06/federationmetadata.xml

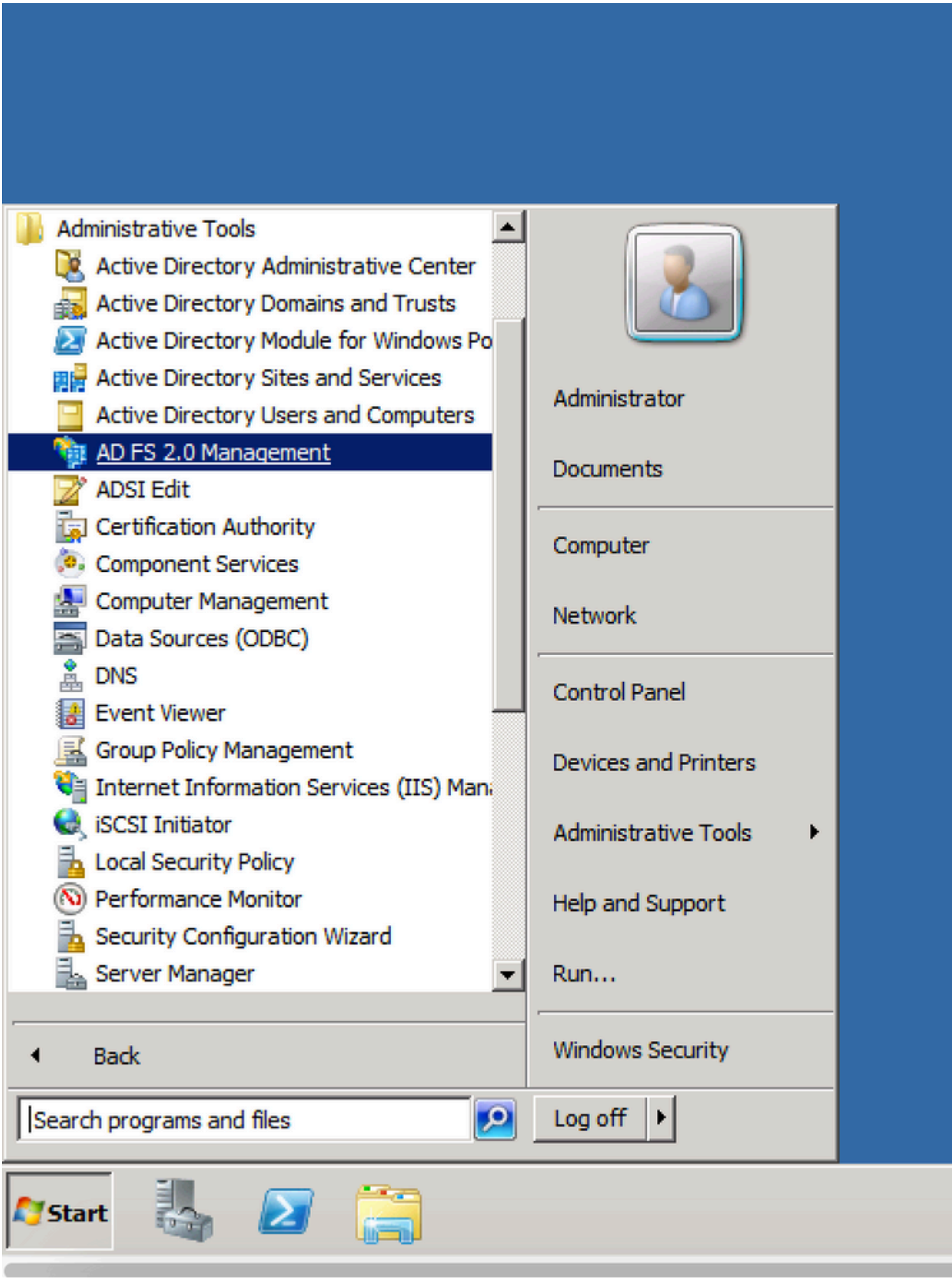
- åœ¨ã€ŒIdSç®¡ç†ã€é ç±¤ä¸Šå‚³åœ¨ä¸Šä¸€æ¥¤ä¸‹è¼‰çš„IdPå¾Œè¨è³‡æ–™æª”ã

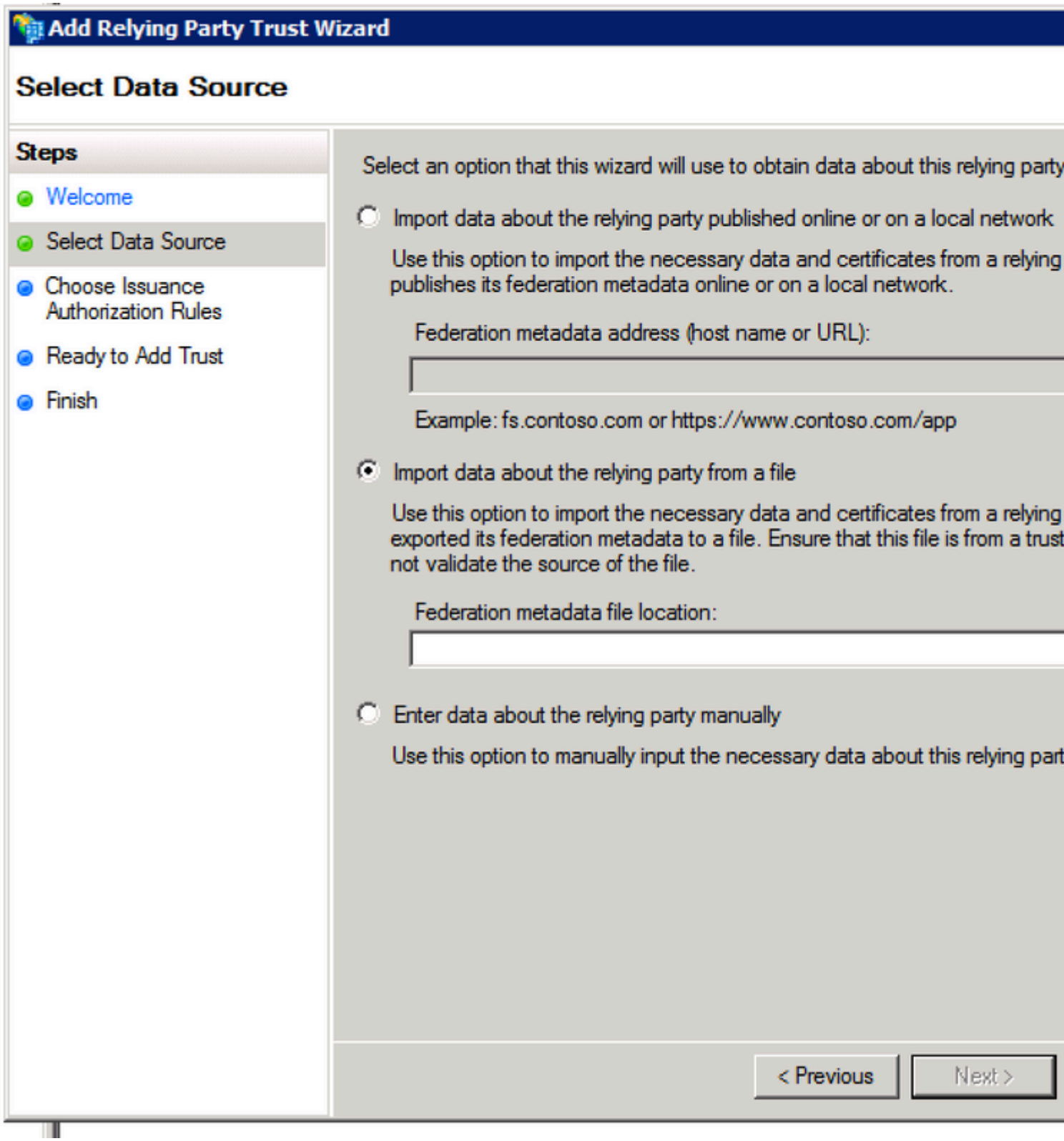


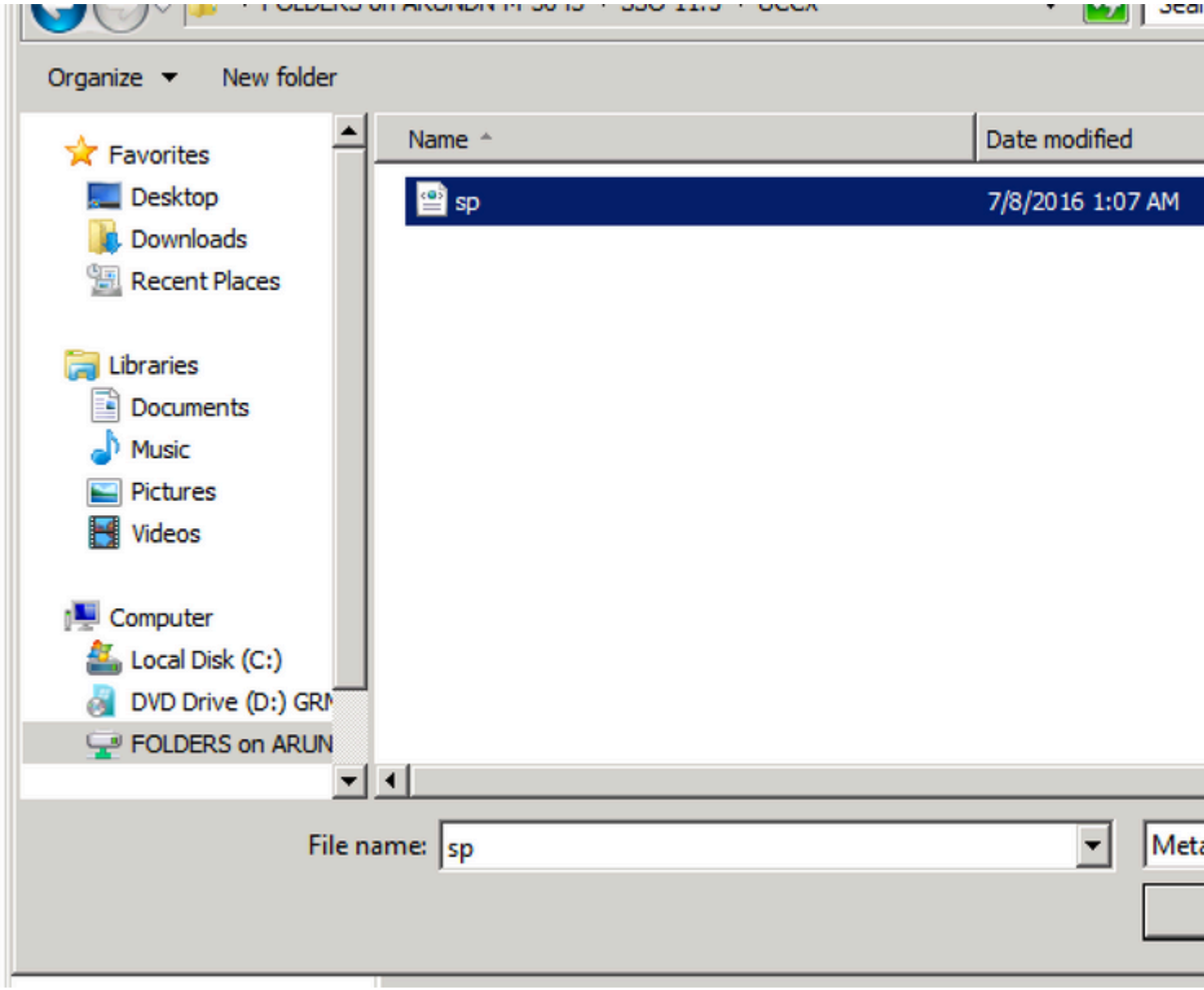
é€™æ˜¯ä¸Šå‚³IdSå¾Œè¨³æ–™å’Œæ–°å¢žå®£å‘Šè¦�å‰‡çš„é�Žç¨‹ã€‚ADFS 2.0å’Œ3.0å°�æ¤å�šä°†æ¦‚è¿°ã€‚

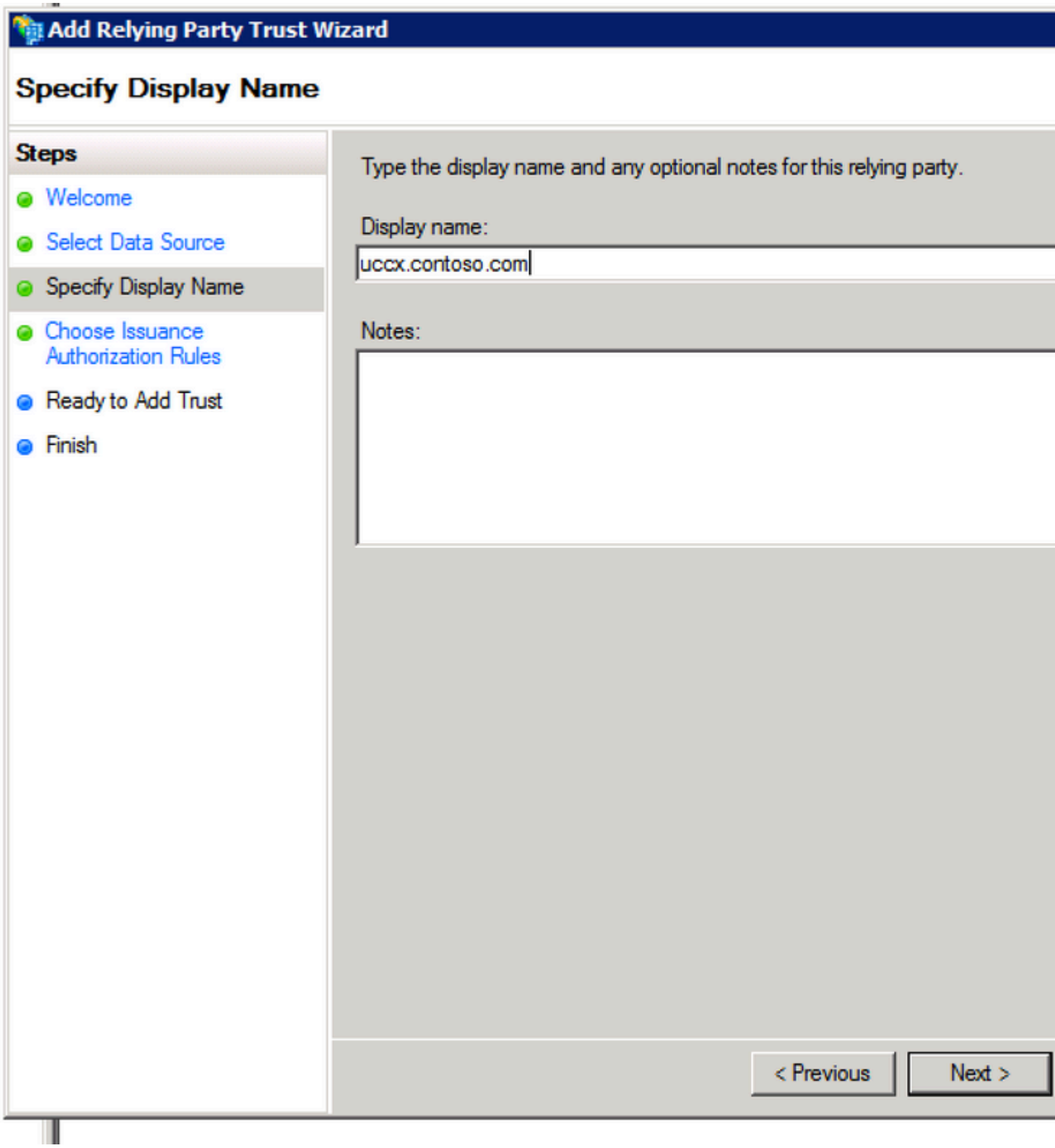
ADFS 2.0

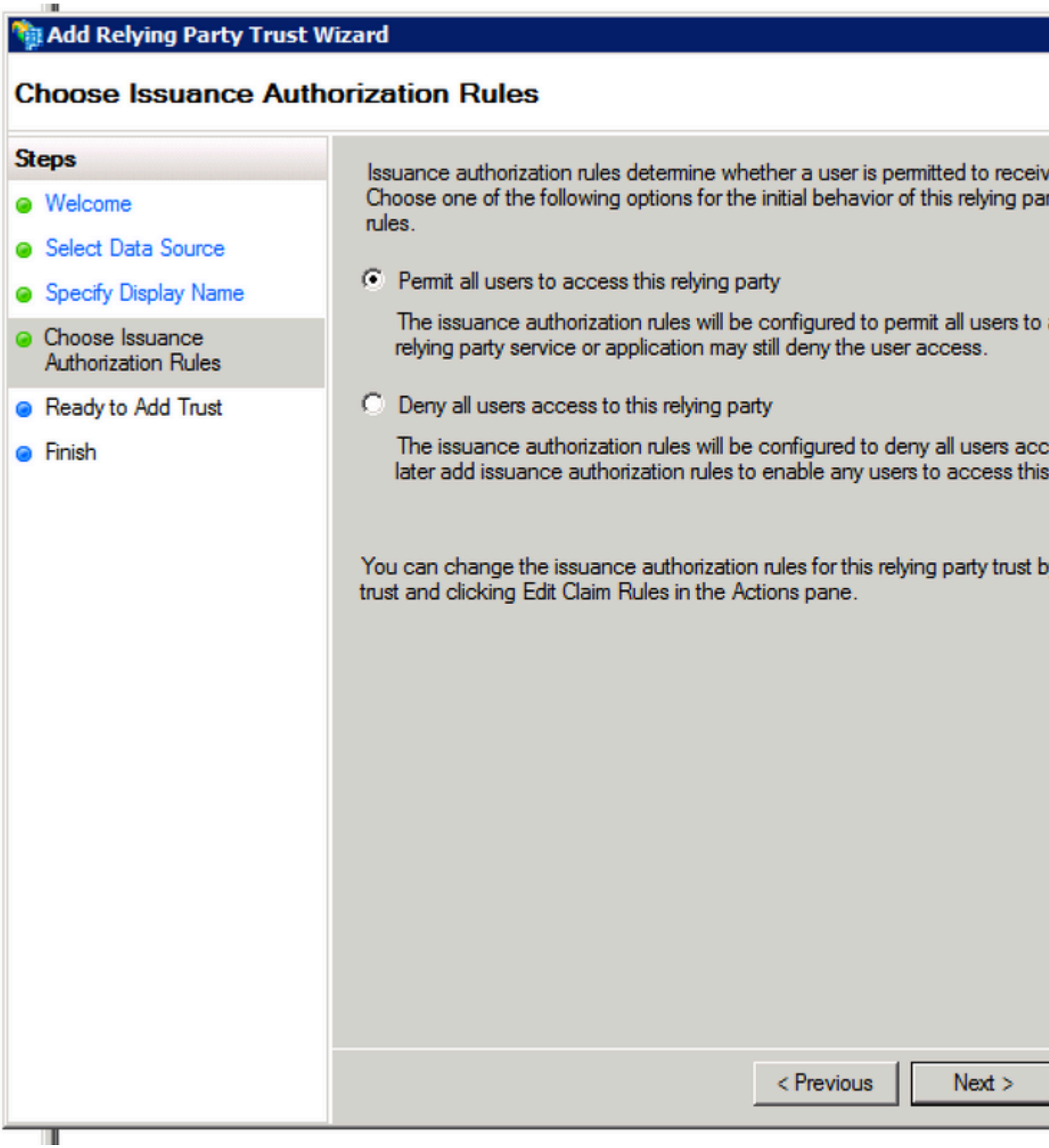
æ¥é©Ÿ1.åœ¨ADFSä¼ºæœ�å™¨ä¸Œå°Žèˆªå^°ï¼Œ Start > All Programs > Administrative Tools > ADFS 2.0 Managementä¸ï¼Œå¦‚æ–‡ç¤ºï¼š


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
Back
Search programs and files
Administrator
Documents
Computer
Network
Control Panel
Devices and Printers
Administrative Tools
Help and Support
Run...
Windows Security
Log off
Start

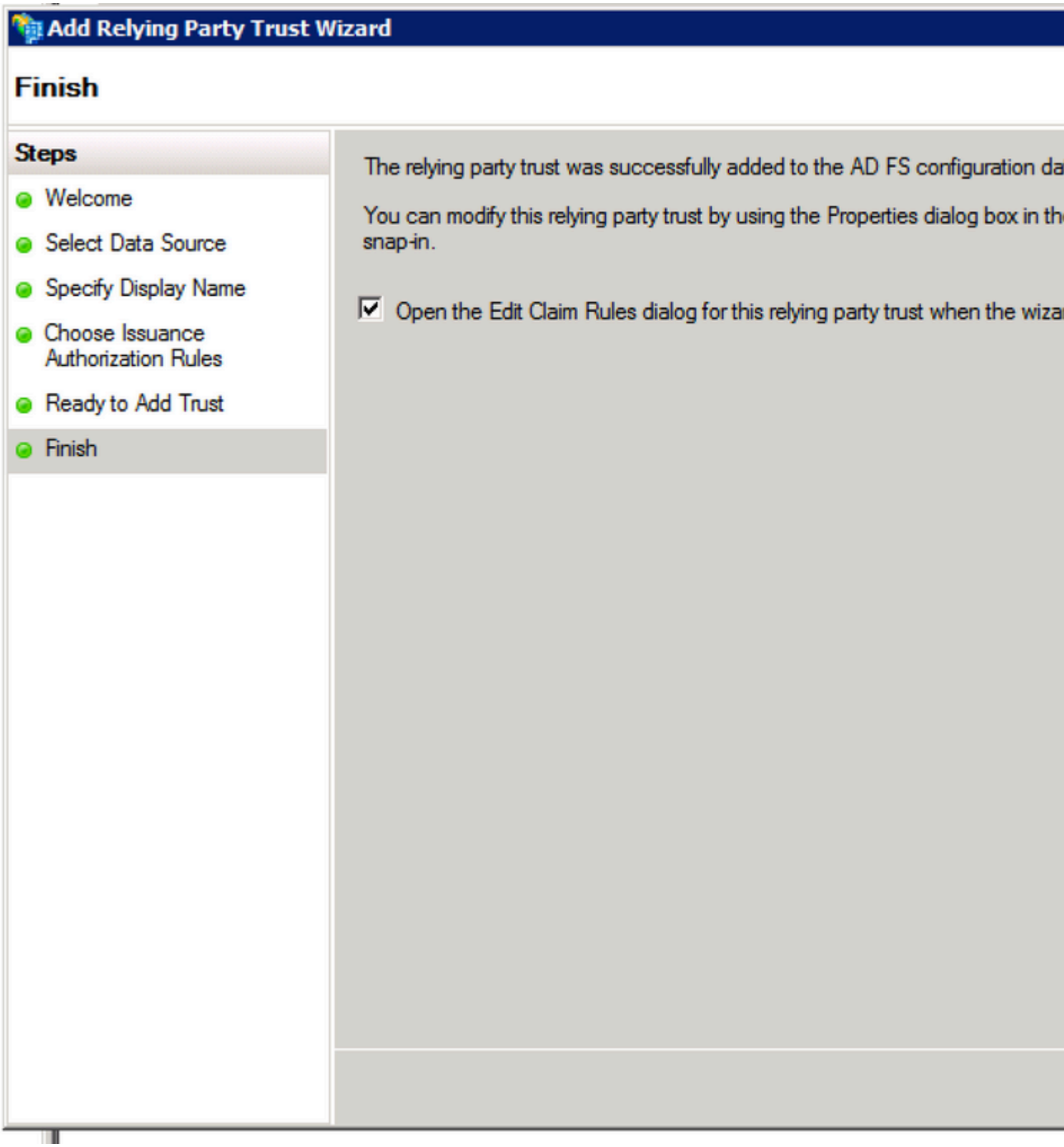

Add Relying Party Trust Wizard
Select Data Source
Steps
Welcome
Select Data Source
Choose Issuance Authorization Rules
Ready to Add Trust
Finish
Select an option that this wizard will use to obtain data about this relying party
Import data about the relying party published online or on a local network
Use this option to import the necessary data and certificates from a relying
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
exported its federation metadata to a file. Ensure that this file is from a trust
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 part
< Previous
Next >


Organize
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Computer
Local Disk (C:)
DVD Drive (D:) GR
FOLDERS on ARUN
Name
Date modified
sp
7/8/2016 1:07 AM
File name:
sp

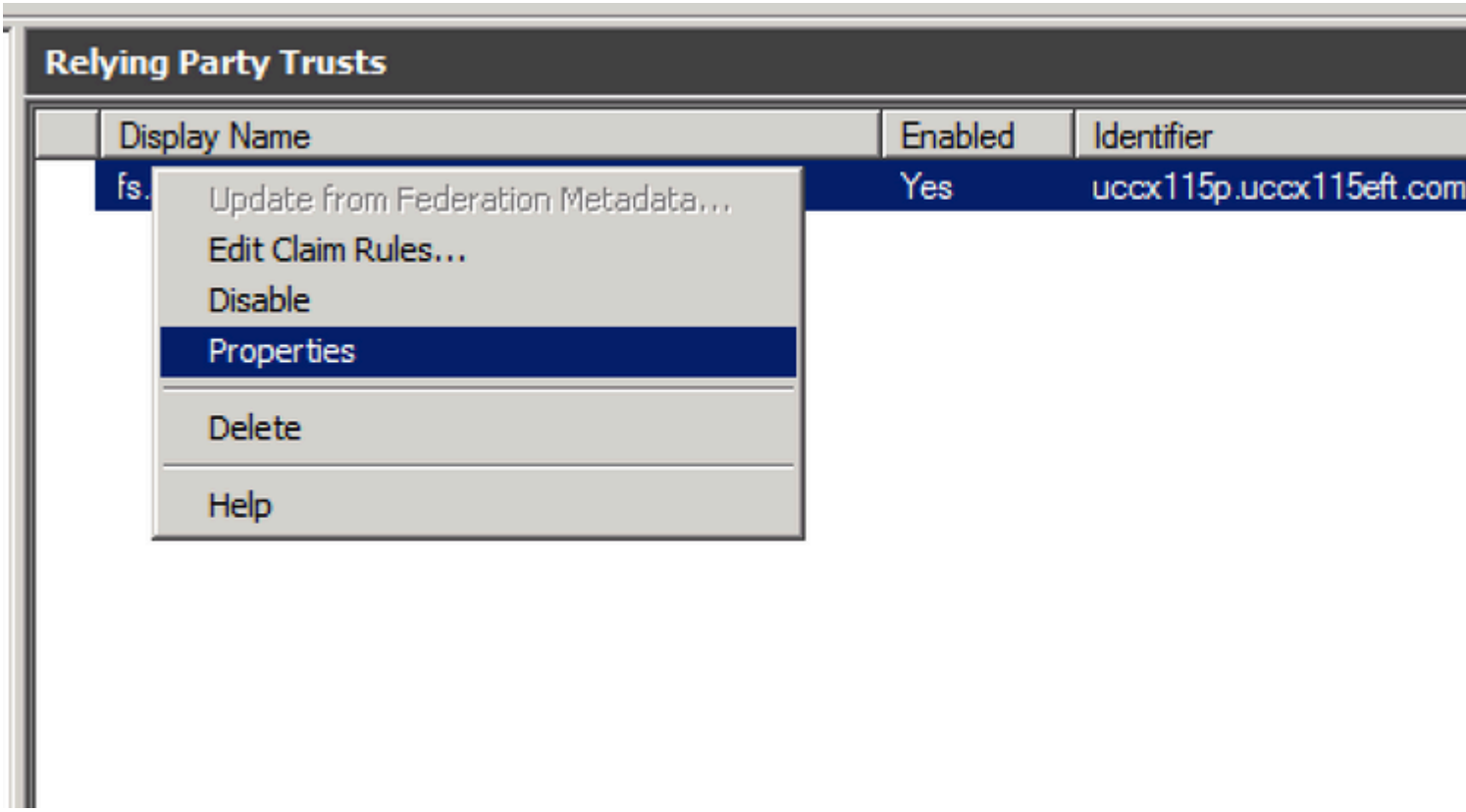

Add Relying Party Trust Wizard
Specify Display Name
Steps
Welcome
Select Data Source
Specify Display Name
Choose Issuance Authorization Rules
Ready to Add Trust
Finish
Type the display name and any optional notes for this relying party.
Display name:
uccx.contoso.com
Notes:
< Previous
Next >

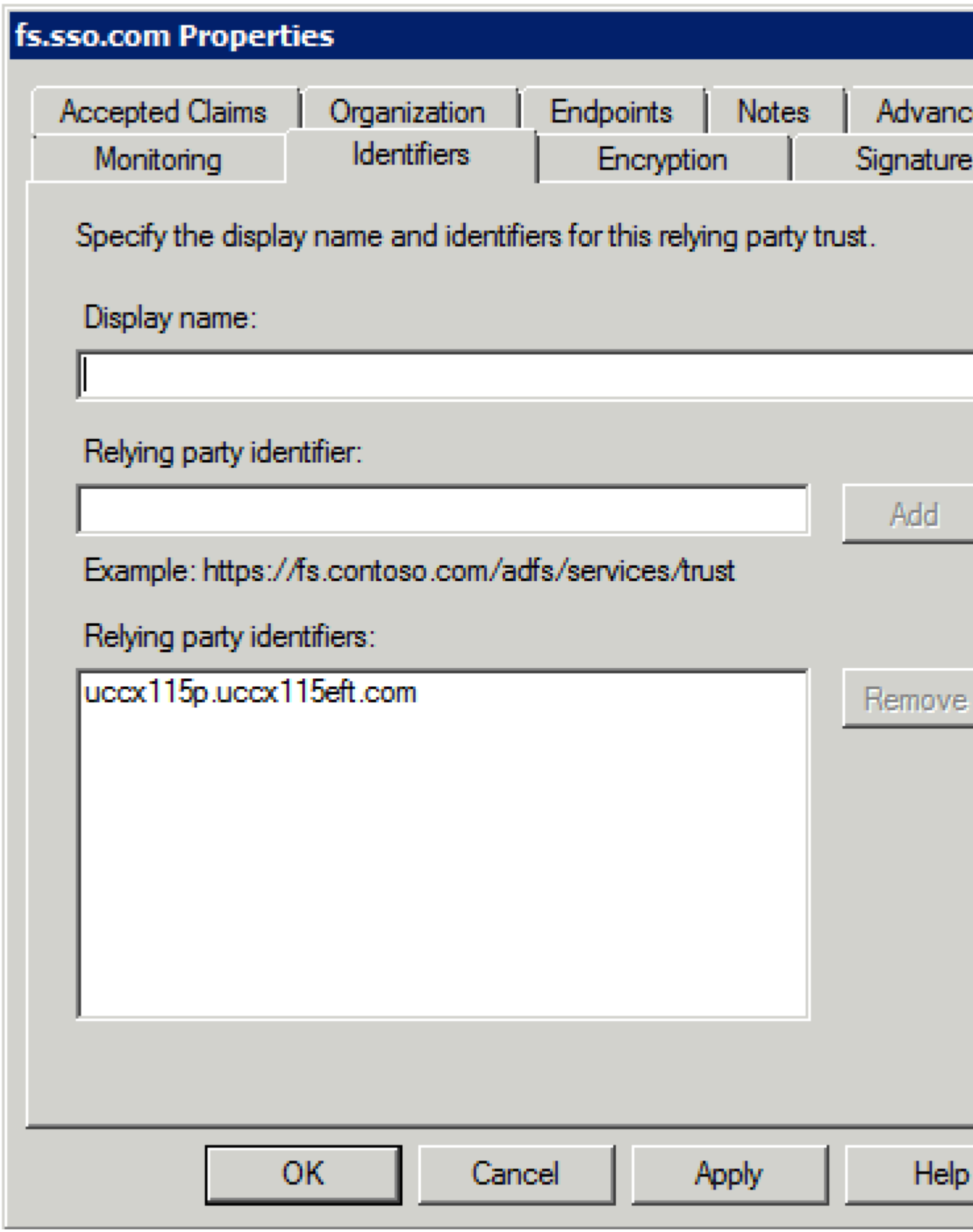


æ¥é©Ÿ4.å®Œæ˜¯ä¿¡è³´æ–¹ä¿¡ä»»çš„å»ºç«‹ã€‚



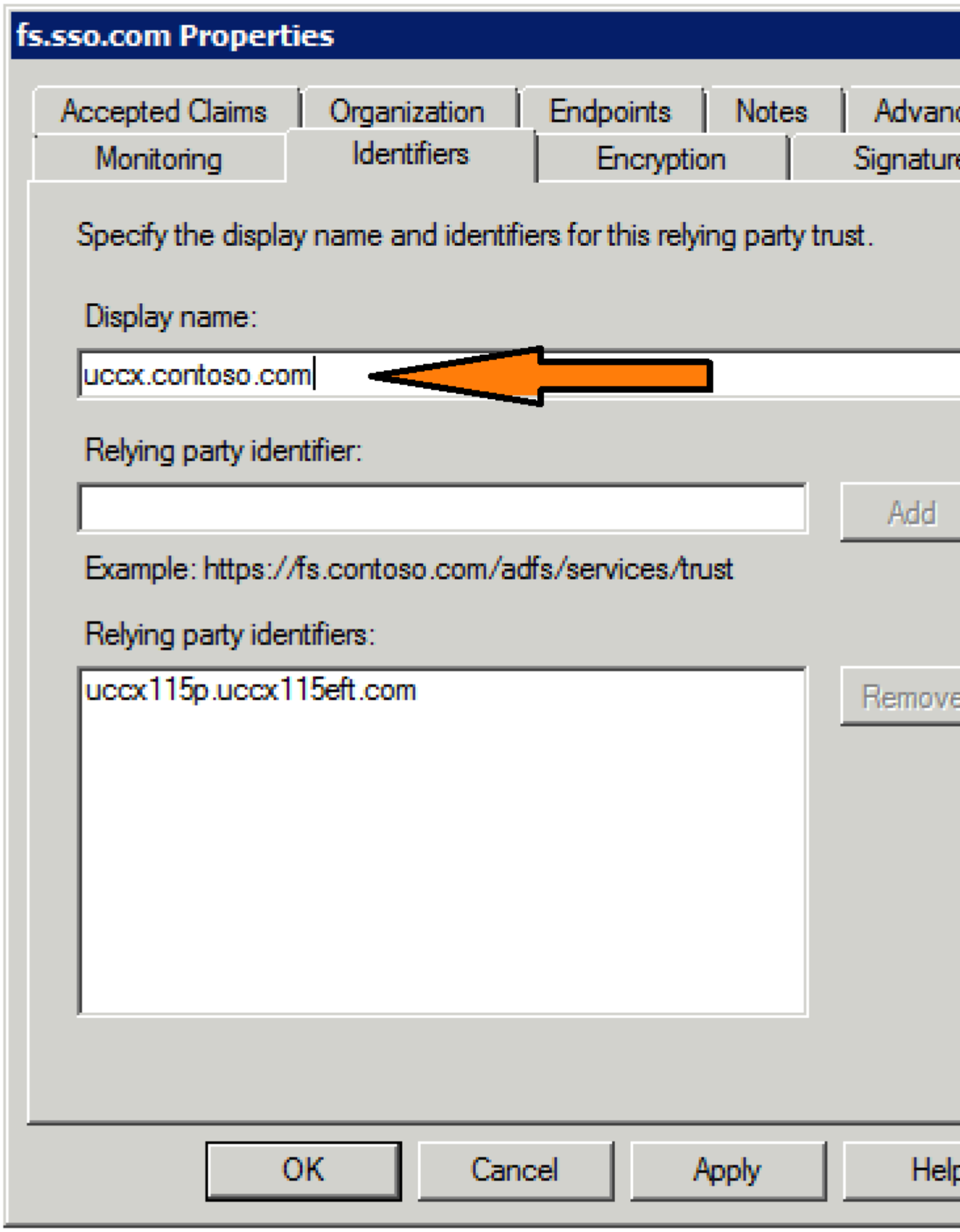
æ¥é©Ÿ5.åœ¨ä¿¡è³´æ–¹ä¿¡ä»»çš„å±¬æ€§ä¸¼Œé€‚æ“‡ Identifier é ç±¤ã€‚


Relying Party Trusts
Display Name
Enabled
Identifier
fs.
Yes
uccx115p.uccx115eft.com
Update from Federation Metadata...
Edit Claim Rules...
Disable
Properties
Delete
Help



æ¥é©Ÿ6.å°‡è¯å^¥ç¬¦è™Ÿè¨å®šç‚ºCisco Identity Serverçš„å®Œå…¨é™å®šä¸»æ©Ÿå��ï¼ŒCisco

Identity Serverå¯¾åžå…¶ç²²å¾— sp.xml å·²ä¸‹è¼‰ã€‚



æ¥é©Ÿ7.æŒ‰ä¸€ä¸‹å�³é�µä¿¡è³´æ–¹ä¿¡ä»»ï¼Œ¶å¾Œæ‰€ä¸‹ Edit Claim Rules.

å¿…é ˆæ–°å¢žå…©å€‹å‘Šè¦‹å‰ï¼Œå€‹æ˜¯åŒ¹é…LDAPï¼ˆè¼•åž‹ç›®éŒ„è¨ªå•�å�”å®šï¼‰

uid â€” æ‡‰ç”¨ç¨‹å¼�éœ€è¦�æ¤å±¬æ€§ä¥æ¨™è˜ç¶“é�Žèº«ä»½é©—è‰ç„¡ä½¿ç”¨è€…ã€,
user_principal - Cisco
Idéœ€è¦�æ¤å±¬æ€§ä¾†æ¨™è˜ç¶“é�Žèº«ä»½é©—è‰ç„¡ä½¿ç”¨è€…ç„é ˜ÿã€,

é ˜æ¬¾ç”³è«‹è¦�å‰1:

æŒ‰å��ç¨±æ–°å¢žè¦�å‰
NameID åž‹åˆ¥ï¼ˆåº‡LDAPå±¬æ€§çš„å€¼æ¯”è¼ƒï¼‰é€�ï¼‰š

- é�¸æ“‡å±¬æ€§å„²å˜ä½œç,ºActive Directory
- å°�æ˜ LDAPå±¬æ€§ User-Principal-Name æˆ�é•·è‡³ user_principal ï¼ˆå°�å¯«ï¼‰
- é�¸æ“‡å¿…é ˆç”¨ä½œçš„LDAPå±¬æ€§
  userId æ‡‰ç”¨ç¨‹å¼�ä½¿ç”¨è€…ï¼Œä¾¿æ¿¿ç™»å…¥ä¸¦å°‡å…¶å°¶å°° uid
  ï¼ˆå°�å¯«ï¼‰

é…�ç½®ç¤ºä¾‹ SamAccountName å°‡ç”¨ä½¿ç”¨è€…ID:

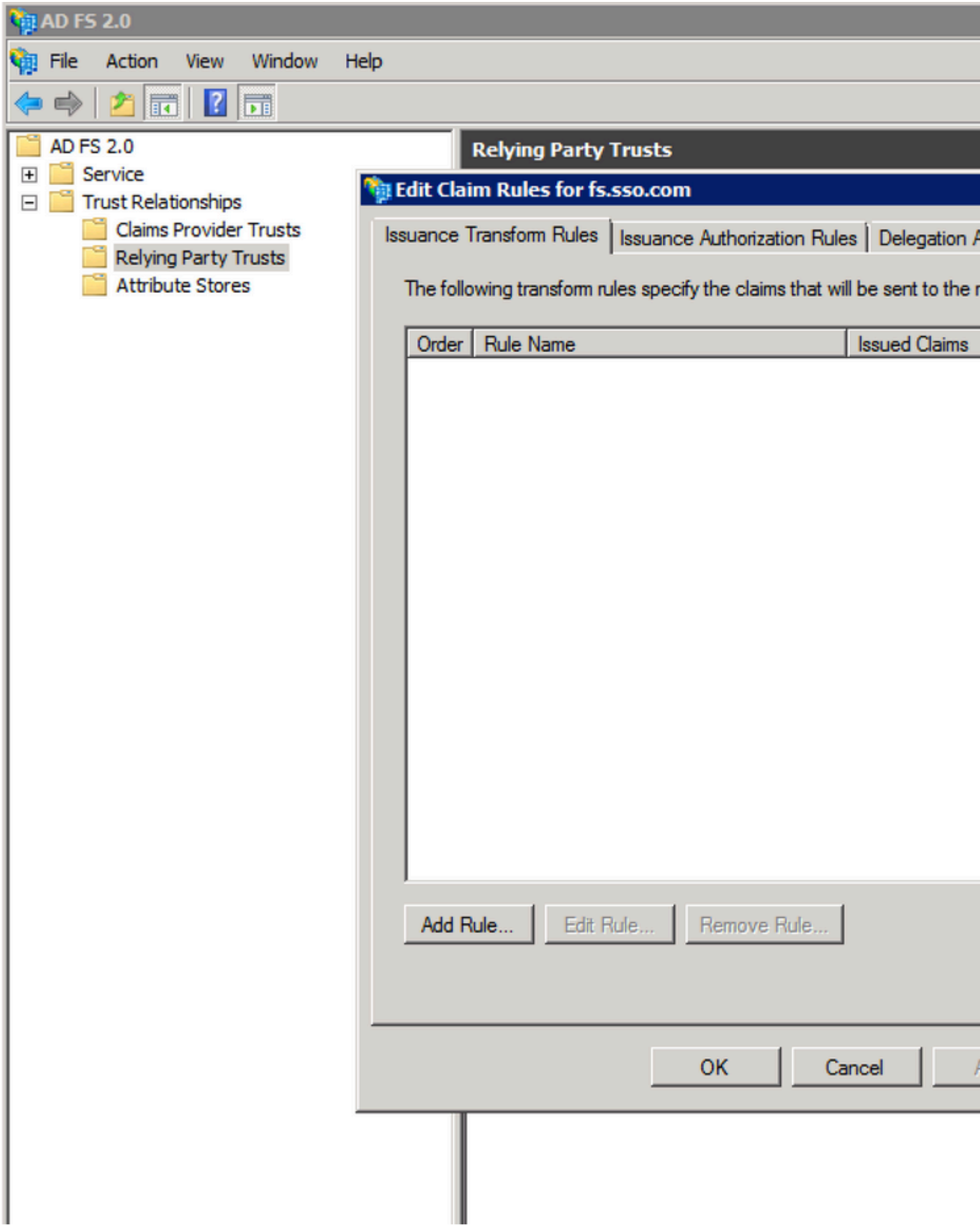
- å°�æ˜ LDAPå±¬æ€§ SamAccountName æˆ�é•·è‡³ uid.
- å°�æ˜ LDAPå±¬æ€§ User-Principal-Name æˆ�é•·è‡³ user_principal.

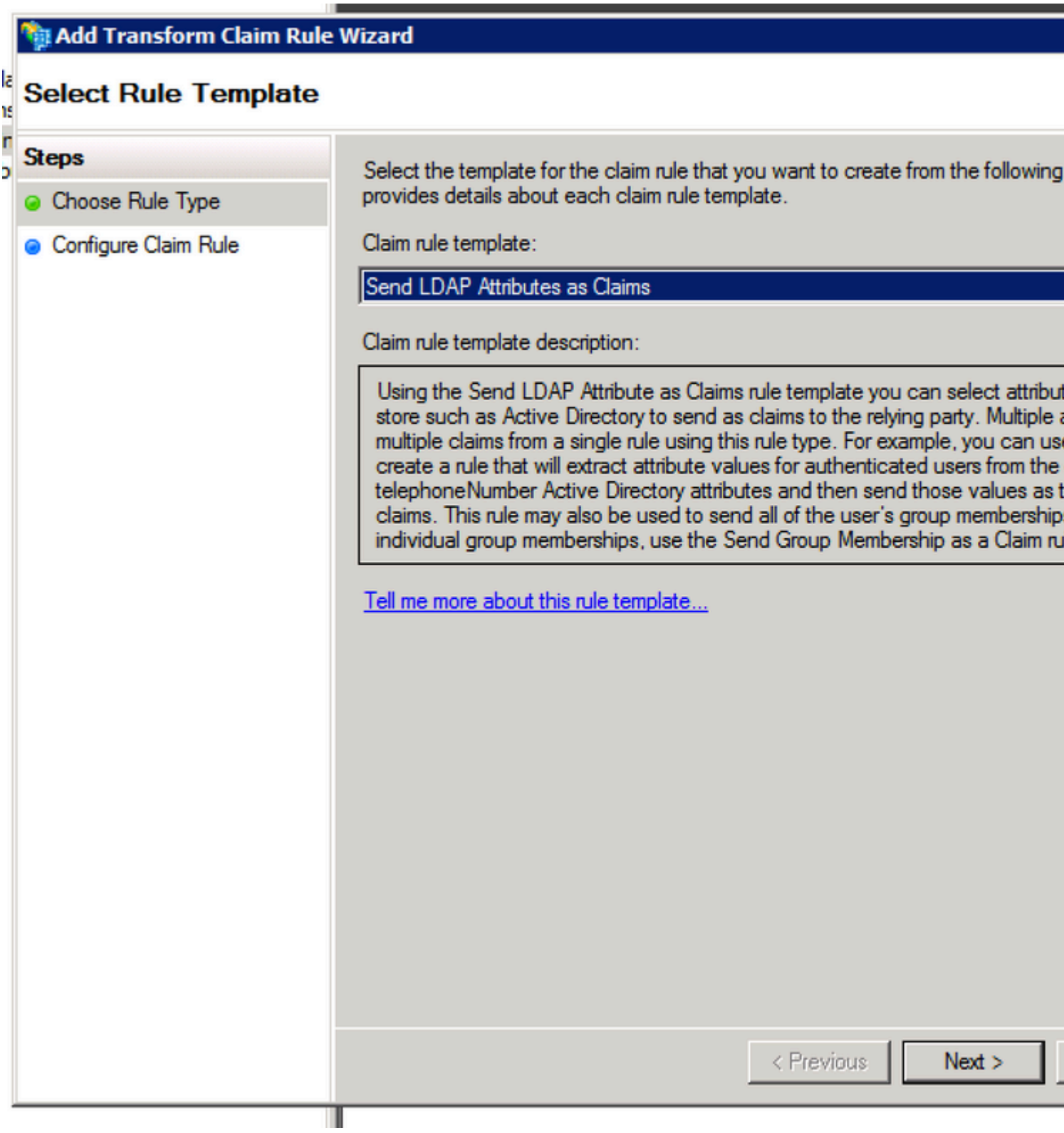
é…�ç½®ç¤ºä¾‹ UPN å¿…é ˆç”¨ä½œä½¿ç”¨è€…ID:

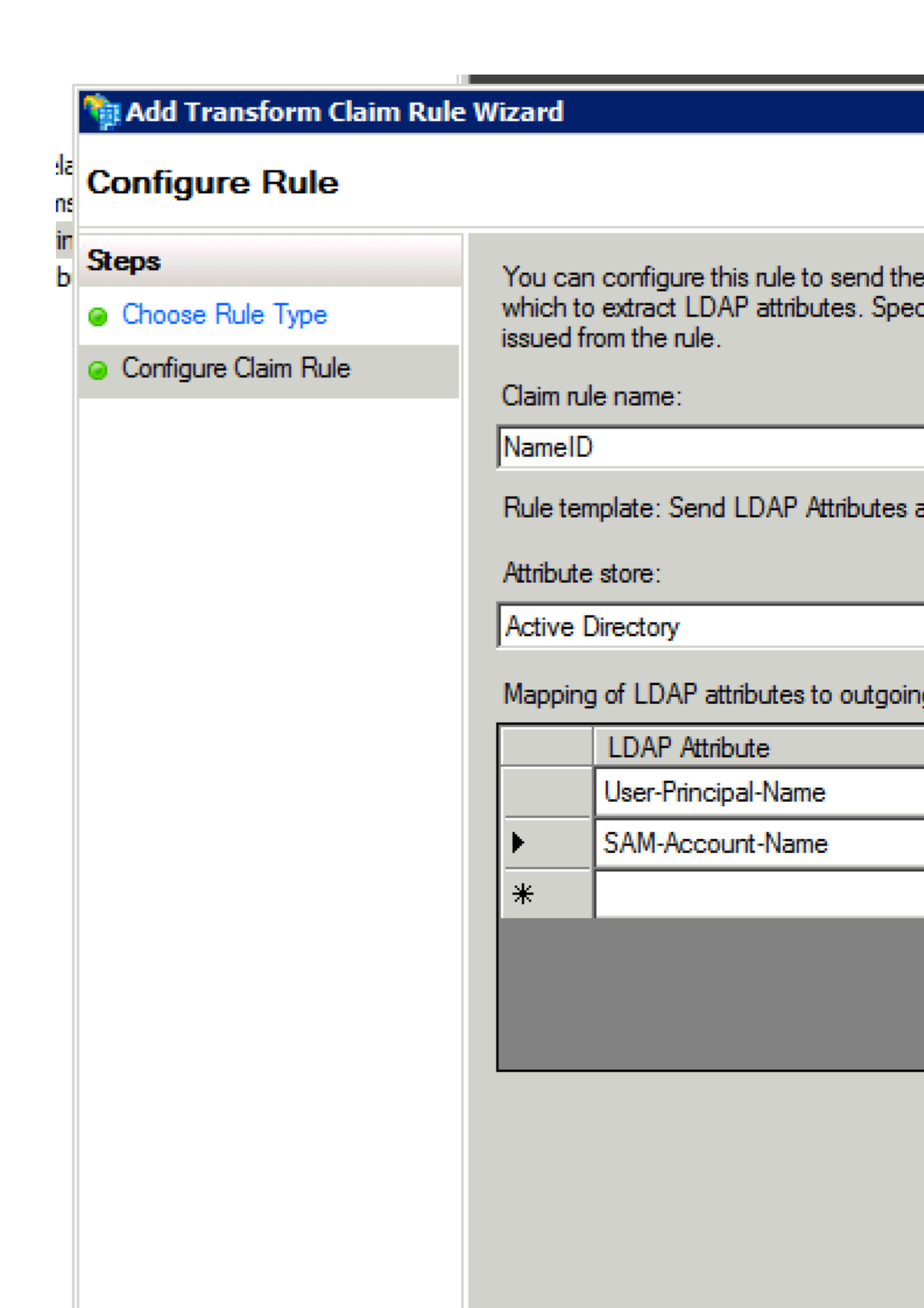
- å°�æ˜ LDAPå±¬æ€§ User-Principal-Name æˆ�é•·è‡³ uid.
- å°�æ˜ LDAPå±¬æ€§ User-Principal-Name æˆ�é•·è‡³ user_principal.

é…�ç½®ç¤ºä¾‹ PhoneNumber å¿…é ˆç”¨ä½œä½¿ç”¨è€…ID:

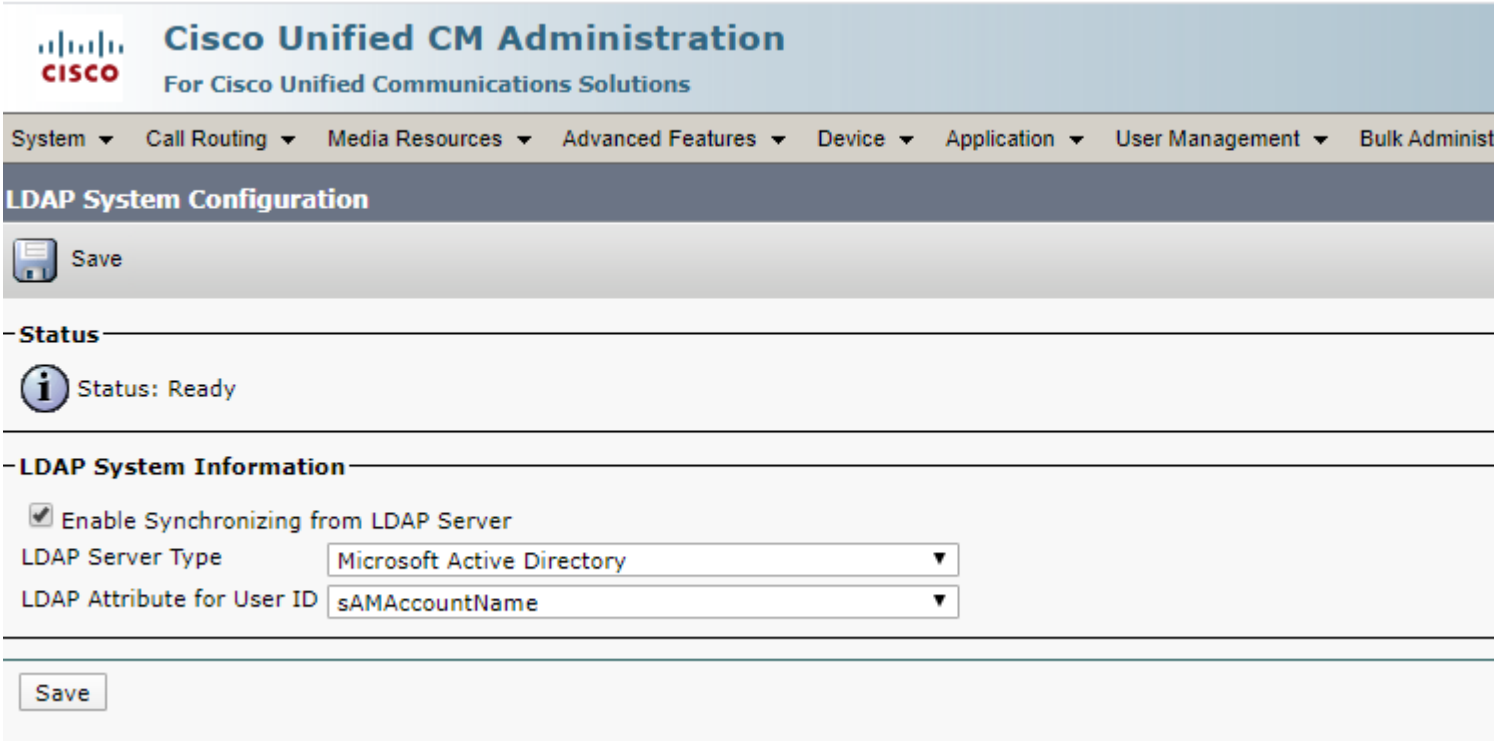
- å°‡LDAPå±¬æ€§telephoneNumber**å°�æ˜** å˚ uid .
- å°�æ˜ LDAPå±¬æ€§ User-Principal-Name æˆ�é•·è‡³ user_principal.


AD FS 2.0
File
Action
View
Window
Help
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


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
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 attribut
store such as Active Directory to send as claims to the relying party. Multiple
multiple claims from a single rule using this rule type. For example, you can us
create a rule that will extract attribute values for authenticated users from the
telephoneNumber Active Directory attributes and then send those values as
claims. This rule may also be used to send all of the user's group membership
individual group memberships, use the Send Group Membership as a Claim ru
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
which to extract LDAP attributes. Spec
issued from the rule.
Claim rule name:
NameID
Rule template: Send LDAP Attributes a
Attribute store:
Active Directory
Mapping of LDAP attributes to outgoin
LDAP Attribute
User-Principal-Name
SAM-Account-Name

ï¿½å‰ï¿½å¯¼èªŠçš„ç´„æ¢ä»¶ï¼Œé¡¯ç¤ºUCCXçš„å¯¼èªï¼NameIDã€‚å®(

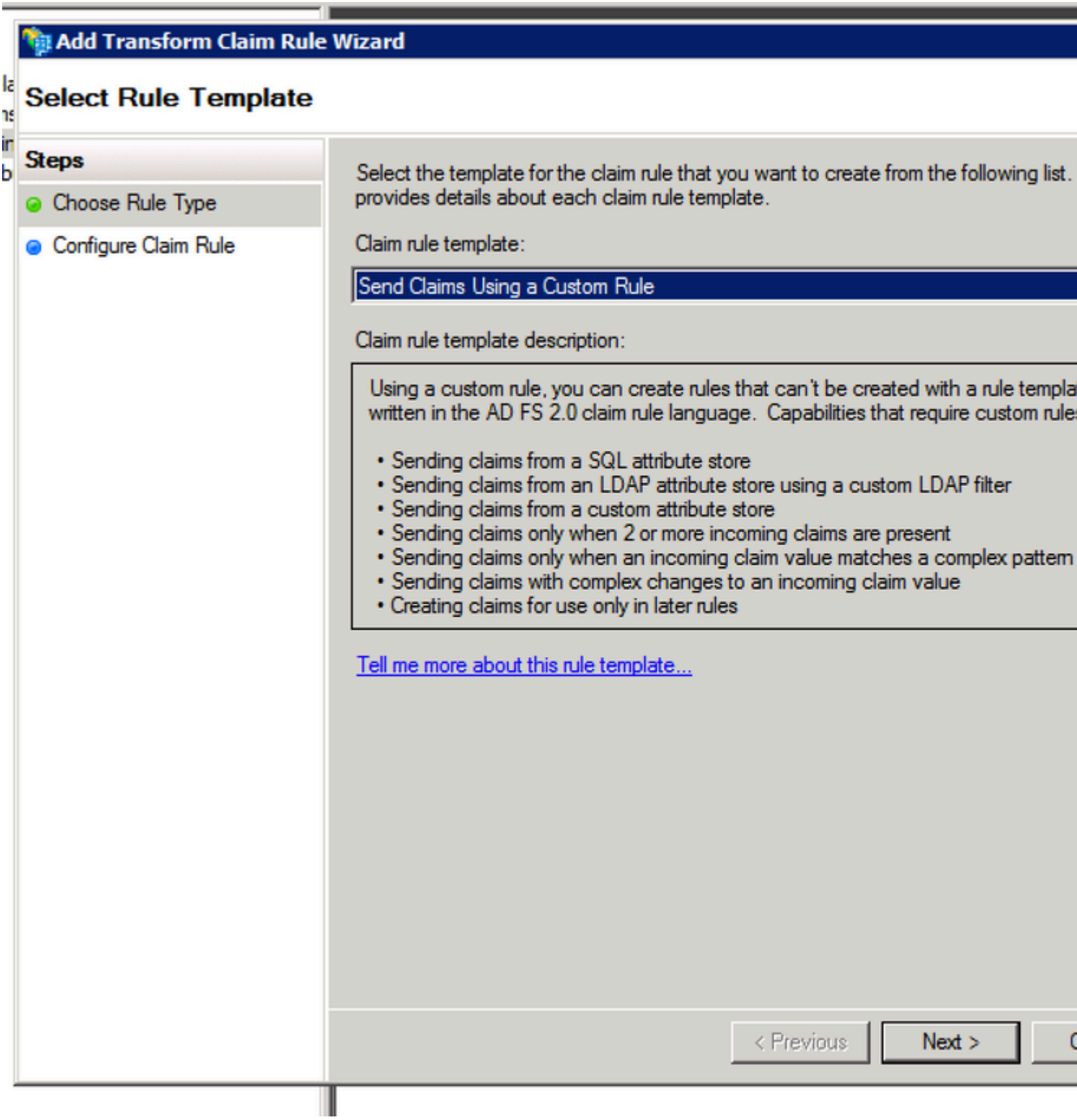


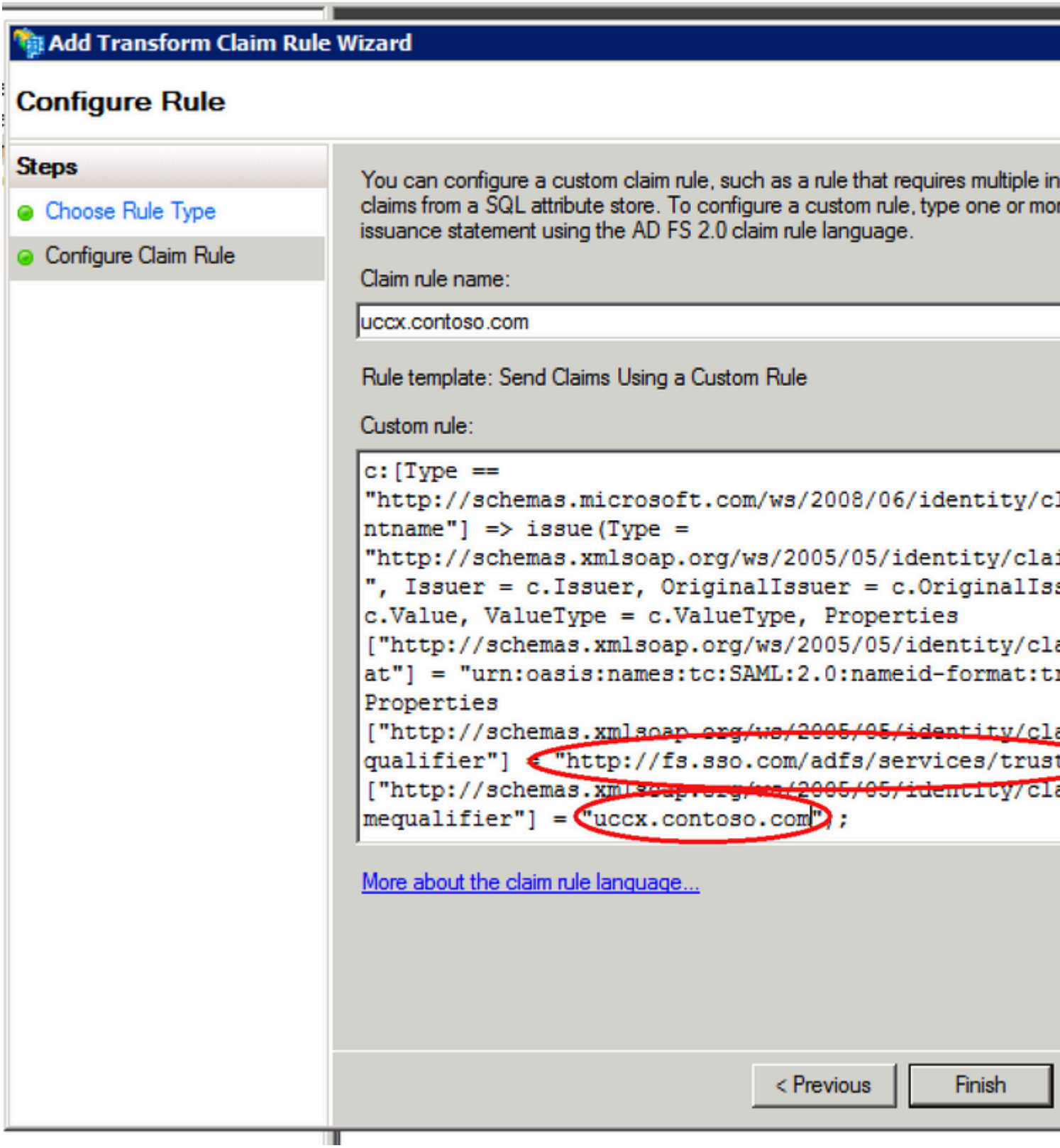
é ˜æ¬¾ç”³è«‹è¦ï¿½å‰2:

- æ–°å¢žï¿½ä¸€å€‹è‡ªå®šç¾©å®£å‘Šè¦ï¿½å‰åž‹å^¥çš„è¦ï¿½å‰ï¼Œè©²è¦ï¿½å‰çš„å¯¼èªæ–°çš„Identity Serverçš„å®Œå…¨é™ï¿½å®šä¸»æ©Ÿå¯¼èªï¼æ–°å¢žæ¤è¦ï¿½å‰æ–‡æœ¬ã€‚

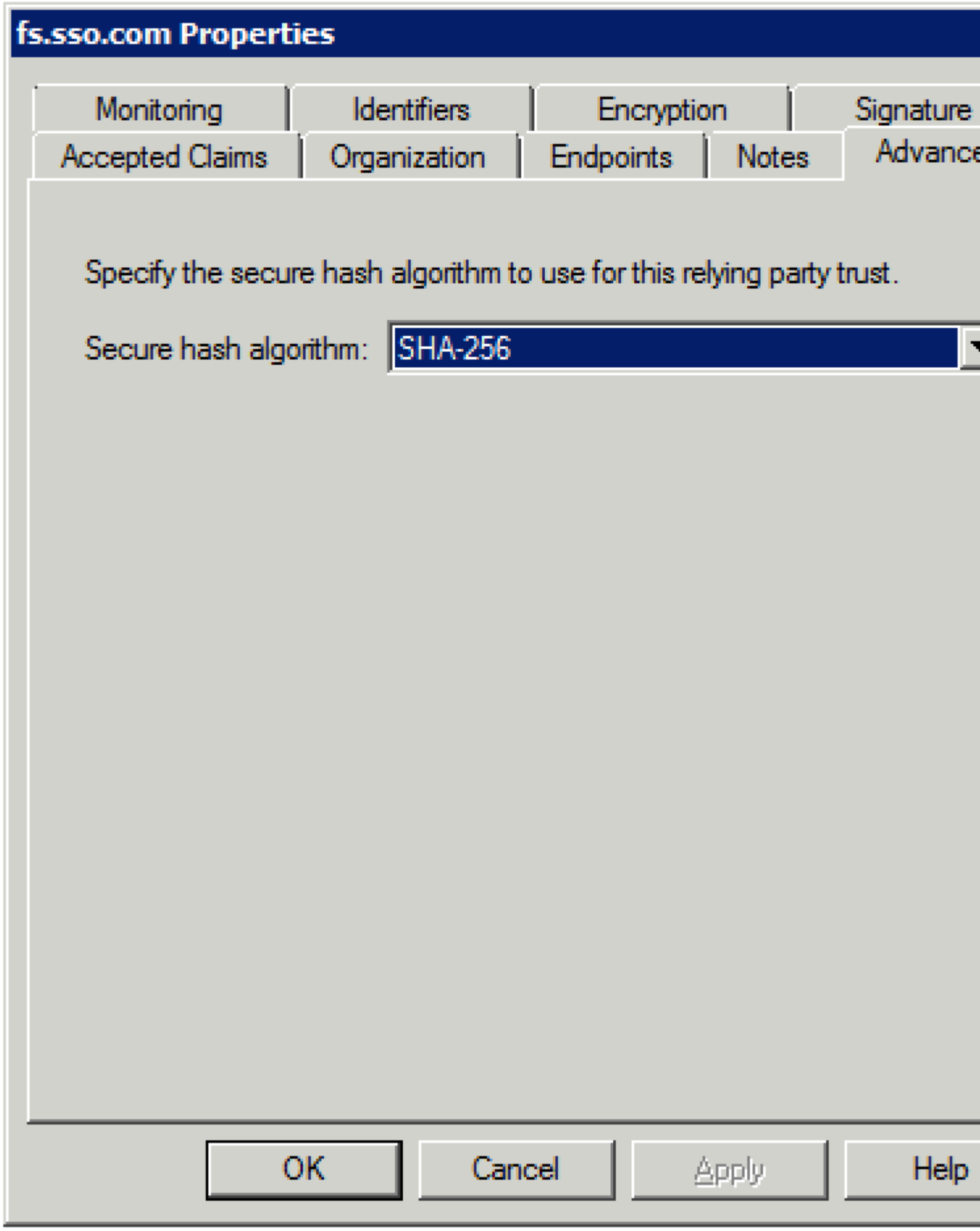
```
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"] => issue(
```

- åœ¨Cisco Identity Serverç¾¤é›†ä¸æ‰€æœ‰å®Œå…¨é™ï¿½å®šä¸»æ©Ÿå¯¼èªéƒ½æ˜¯Cisco Identity Serverä¸æœ€é«˜å±¤ç´šæœ¬åœ°ç¯€ä¸»æ©Ÿå¯¼èªçš„ä¸»æ©Ÿå¯¼èªã€‚
- <Cisco Identity Serverçš„å®Œå…¨é™ï¿½å®šä¸»æ©Ÿå¯¼>å¯¼èªå^†å¤§å°ï¿½å¯¯«ï¼Œæ¤å®ƒè^‡Cisco Identity Server FQDNå®Œå…¨åŒ¹é…ï¼^åŒ…æ‹¬å¤§å°ï¿½å¯¯«ï¼‰ã€‚
- <ADFSä¼°æœ¯å™¨FQDN>å¯¼èªå^†å¤§å°ï¿½å¯¯«ï¼Œæ¤å®ƒè^‡ADFS FQDNå®Œå…¨åŒ¹é…ï¼^åŒ…æ‹¬å¤§å°ï¿½å¯¯«ï¼‰ã€‚

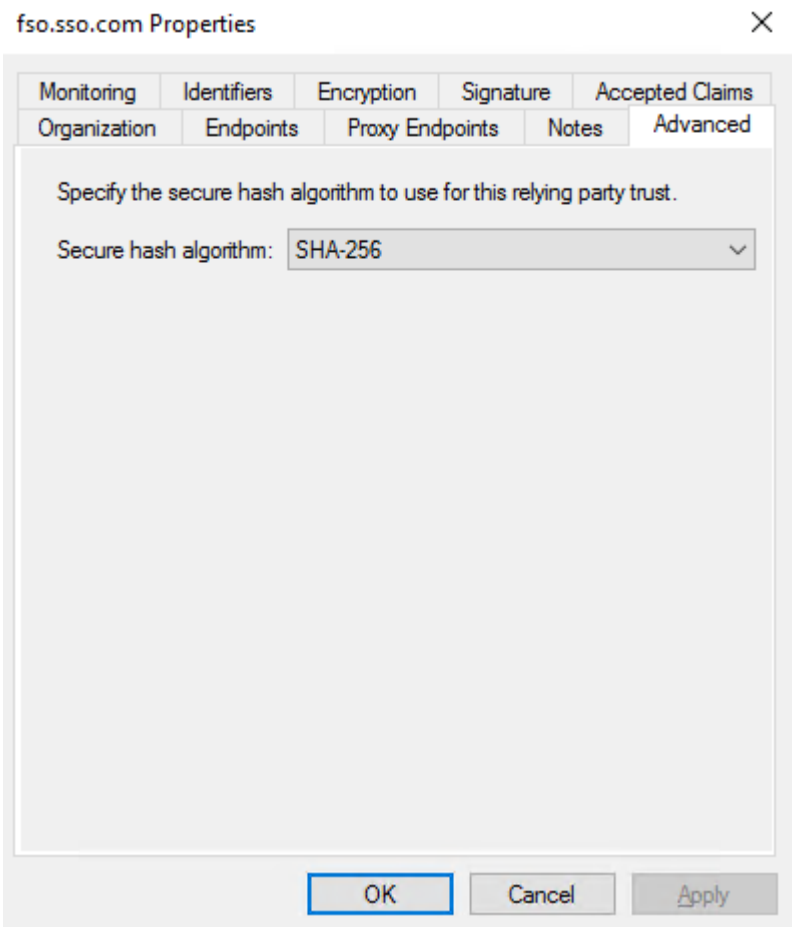

Add Transform Claim Rule Wizard
Select Rule Template
Steps
Choose Rule Type
Configure Claim Rule
Select the template for the claim rule that you want to create from the following list.
provides details about each claim rule template.
Claim rule template:
Send Claims Using a Custom Rule
Claim rule template description:
Using a custom rule, you can create rules that can't be created with a rule templa
written in the AD FS 2.0 claim rule language. Capabilities that require custom rule
• 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 >



æ¥é©Ÿ8.æŒ‰ä¸€ä¸‹å®³é®µä¿¡è³´æ–¹ä¿¡ä»»ï¼Œ¶å¾Œæ‰“ä¸‹ Properties ï¼Œ¶å¾Œé®¸æ“‡ã€Œad


fs.sso.com Properties
Monitoring
Identifiers
Encryption
Signature
Accepted Claims
Organization
Endpoints
Notes
Advance
Specify the secure hash algorithm to use for this relying party trust.
Secure hash algorithm:
SHA-256
OK
Cancel
Apply
Help

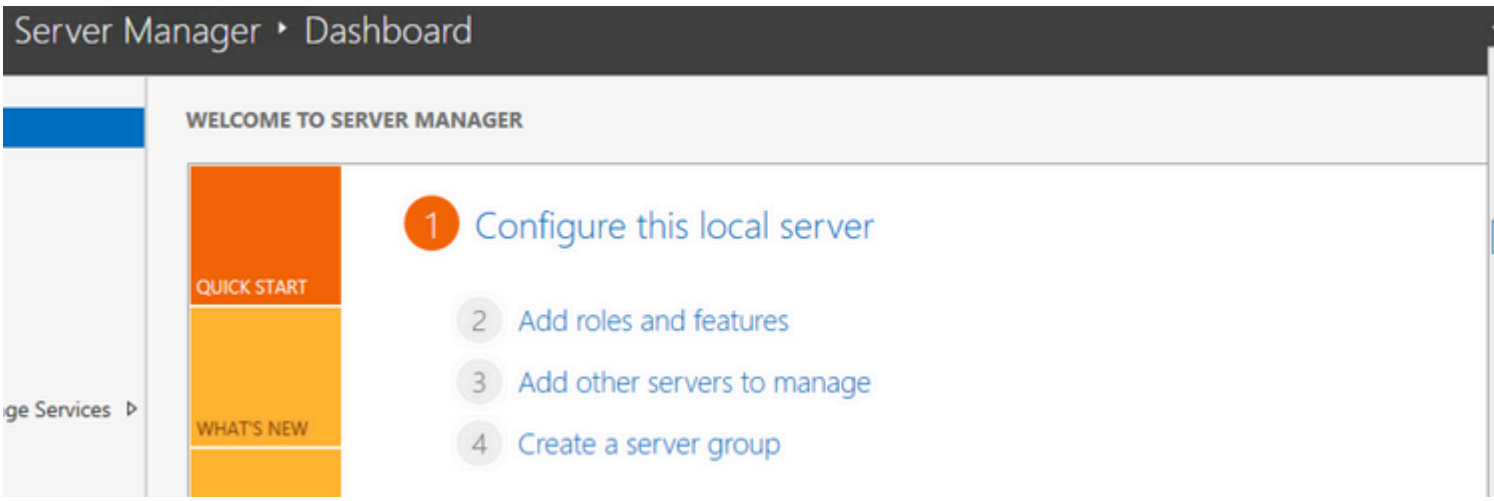
æ¥é©Ÿ9.å¦‚æ–¹€ç¤ºï¼Œé¸æ“‡Secure Hash Algorithm(SHA)ä½œç‚ºSHA-256ã€‚



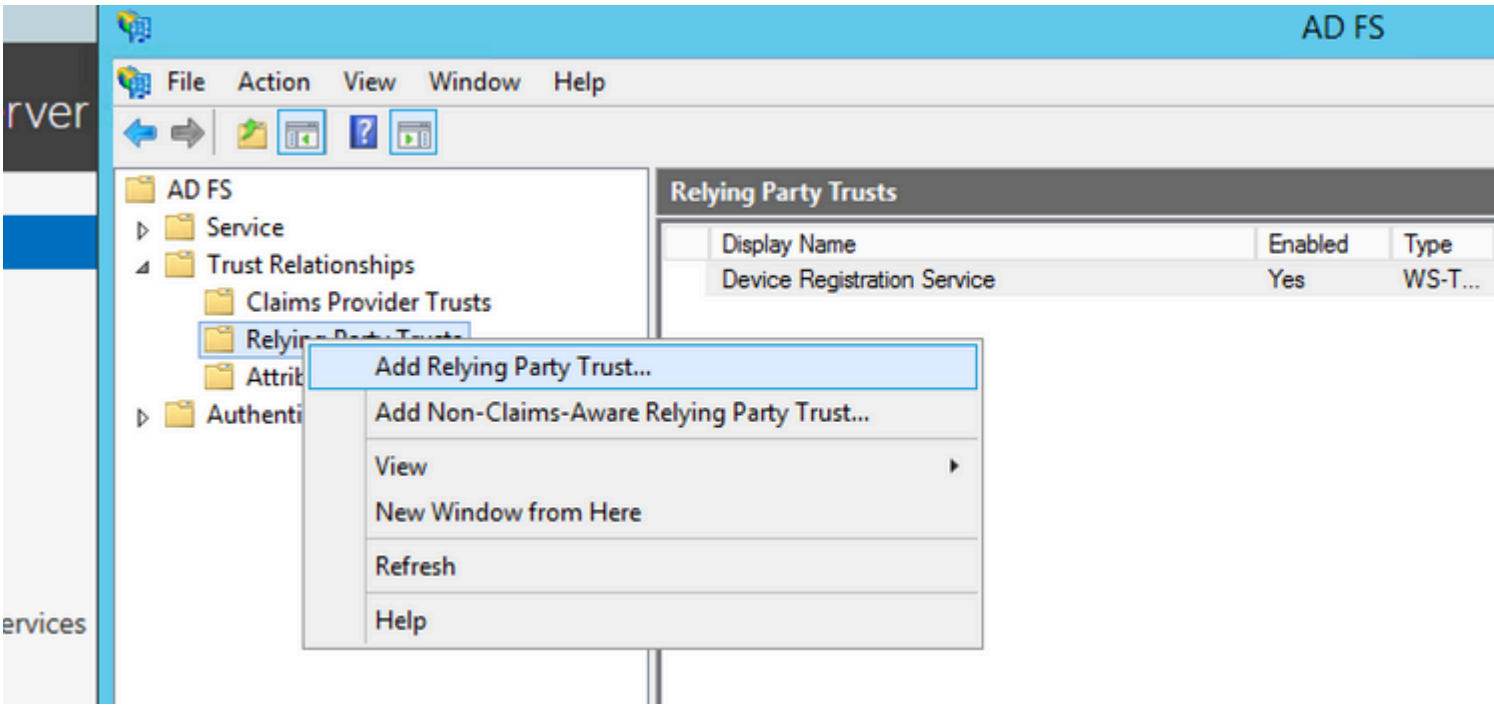
æ¥é©Ÿ10.æŒ‰ä¸€ä¸‹ OK.

ADFS 3.0

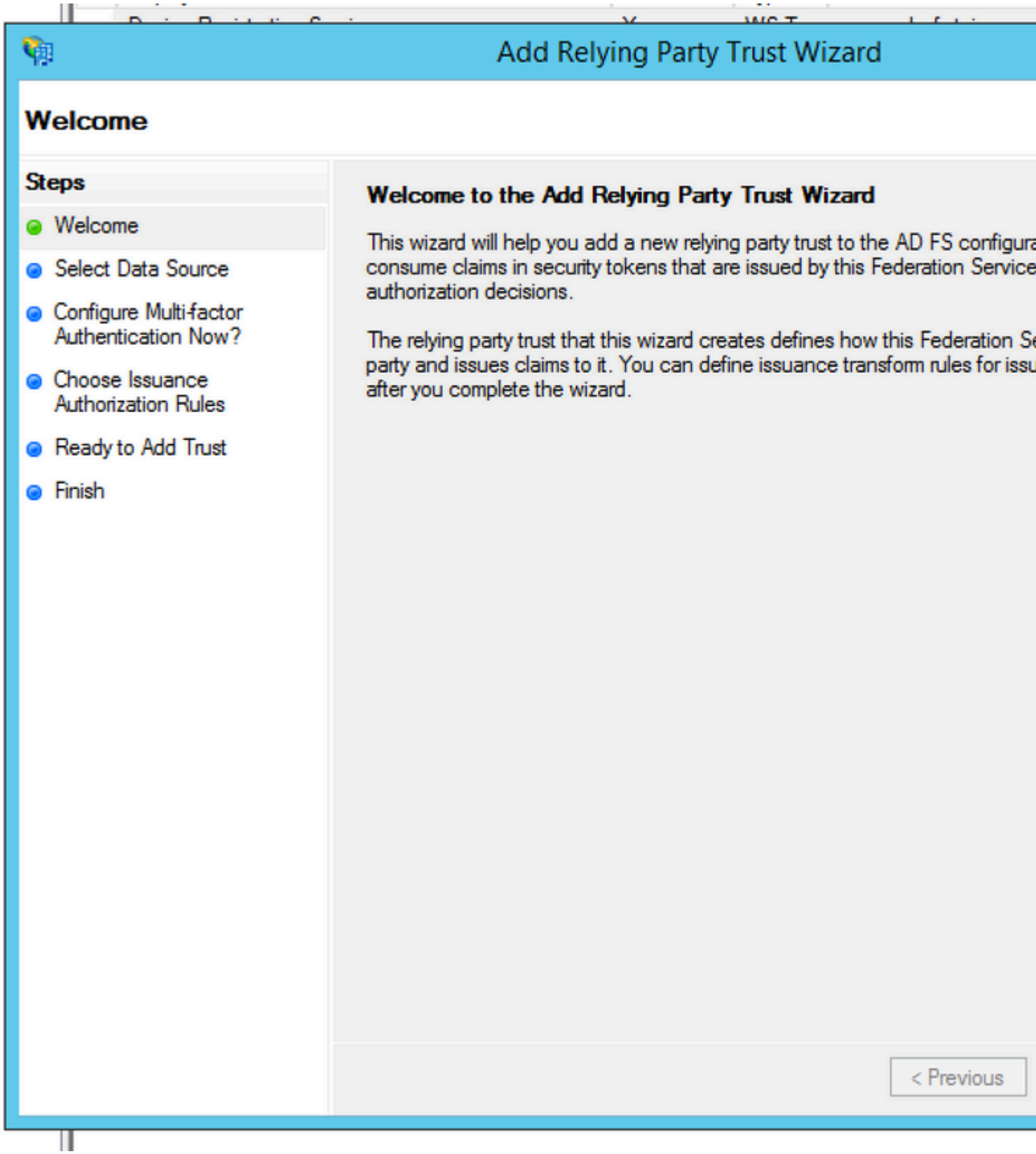
æ¥é©Ÿ1.åœ¨ADFSä¼ºæœ€å™¨ä¸Œå°Žèˆªè‡³ Server Manager > Tools > ADFS Management.

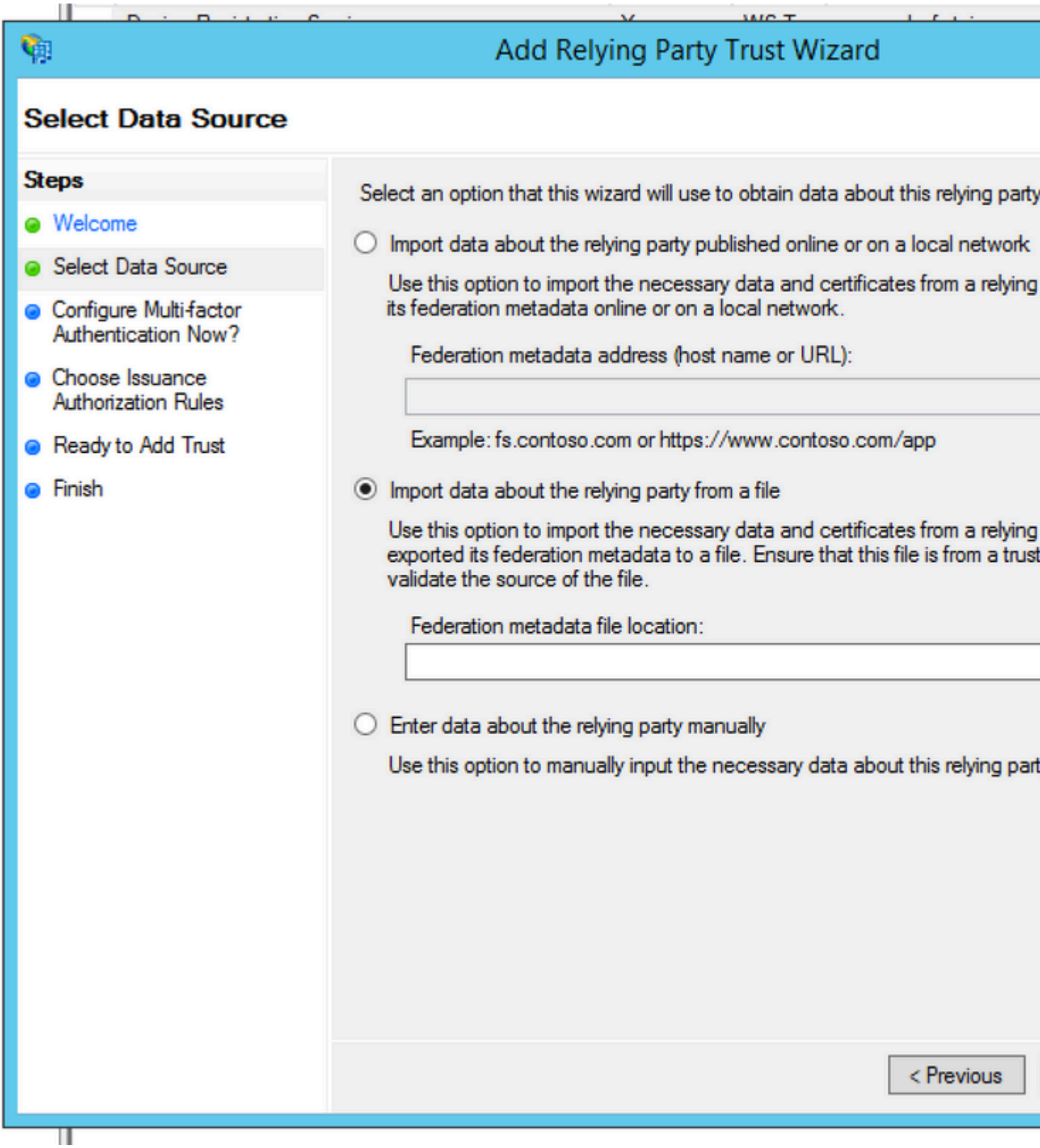


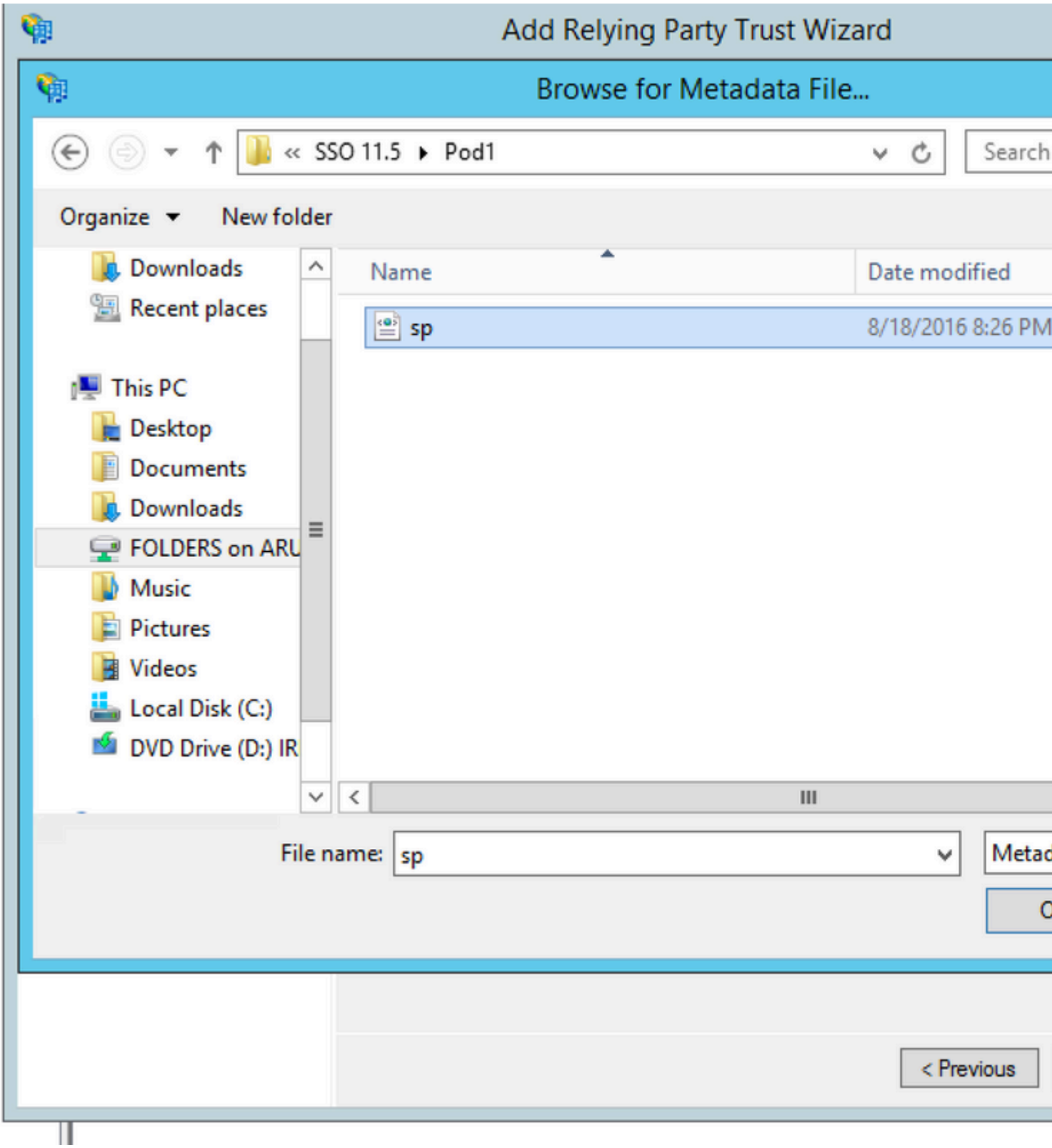
æ¥é©Ÿ2.å°Žèˆªè‡³ ADFS > Trust Relationship > Relying Party Trust.

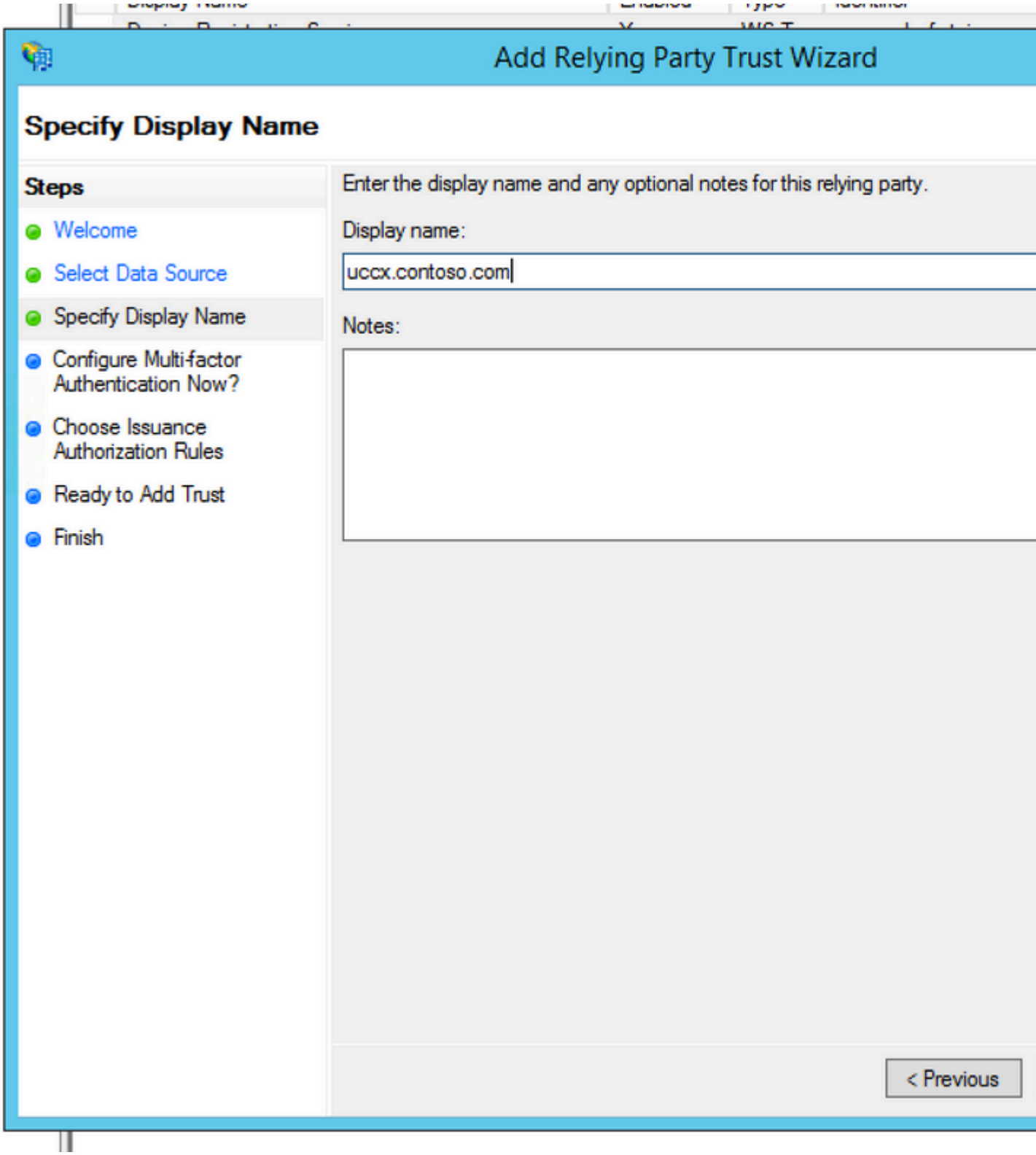


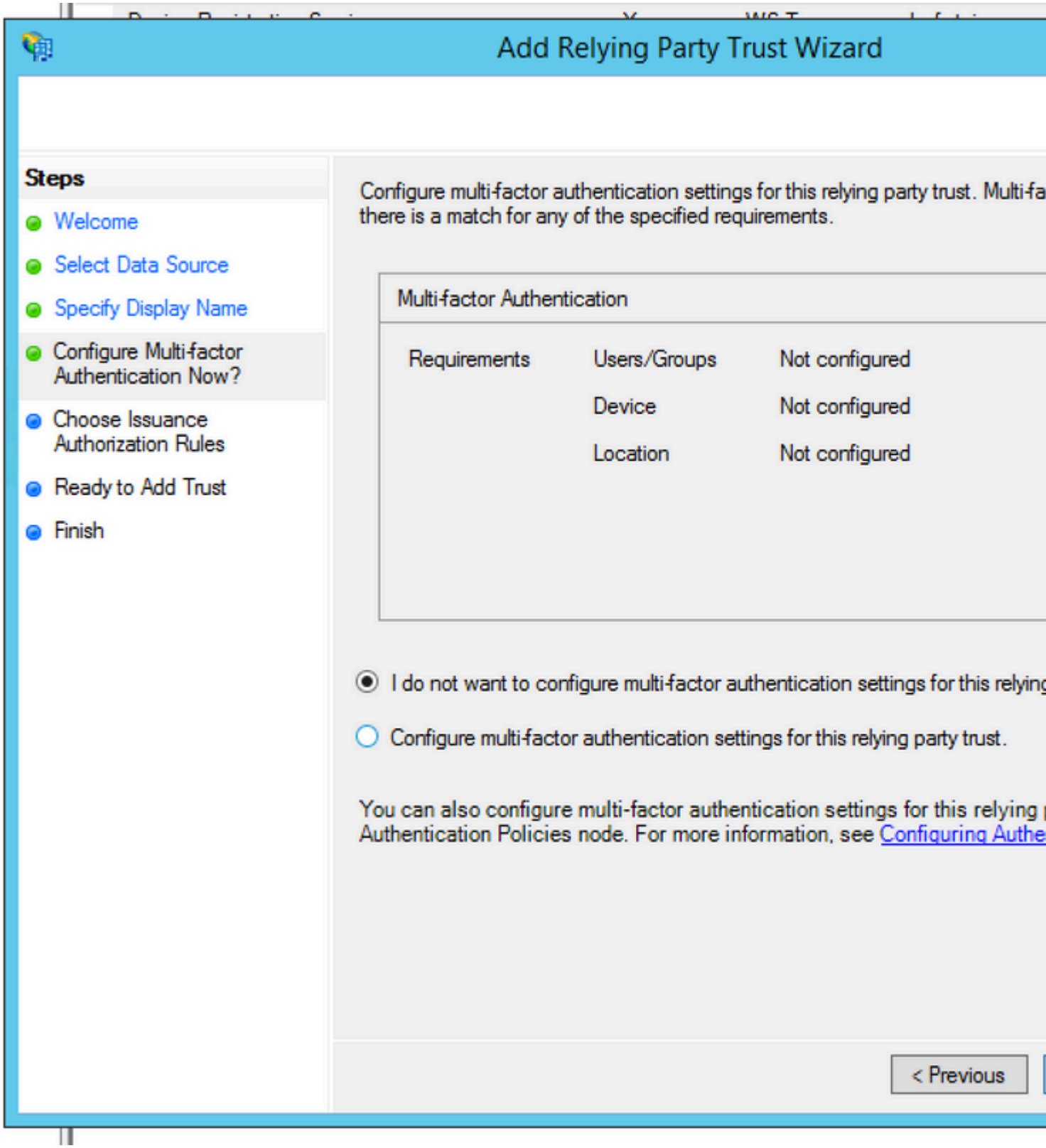
æ¥é©Ÿ3.é¸æ“‡é¸é … Import data about the relying party from a file.

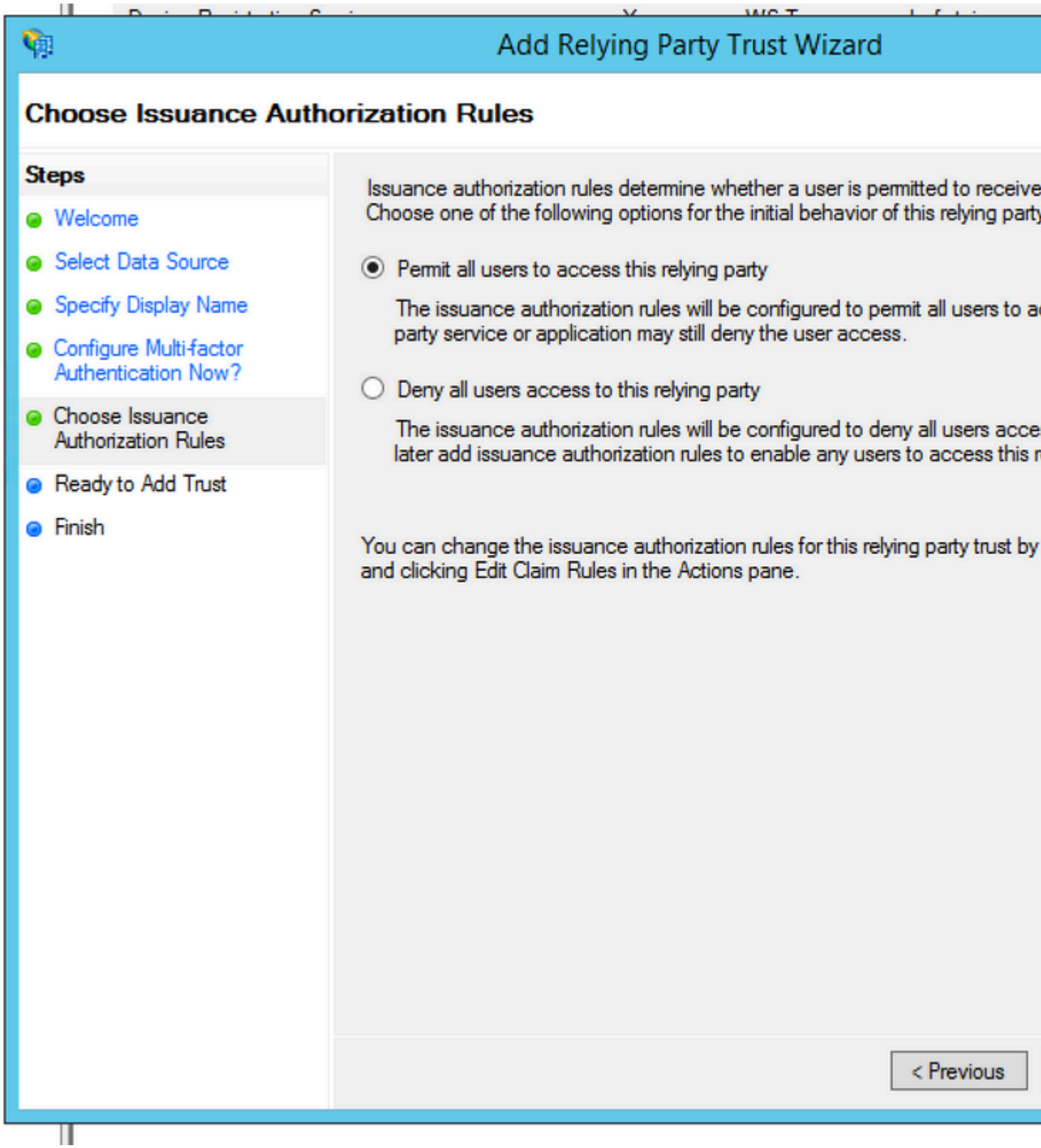

Add Relying Party Trust Wizard
Welcome
Steps
Welcome
Select Data Source
Configure Multi-factor Authentication Now?
Choose Issuance Authorization Rules
Ready to Add Trust
Finish
Welcome to the Add Relying Party Trust Wizard
This wizard will help you add a new relying party trust to the AD FS configura
consume claims in security tokens that are issued by this Federation Service
authorization decisions.
The relying party trust that this wizard creates defines how this Federation Se
party and issues claims to it. You can define issuance transform rules for issu
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
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
exported its federation metadata to a file. Ensure that this file is from a trust
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 part
< Previous

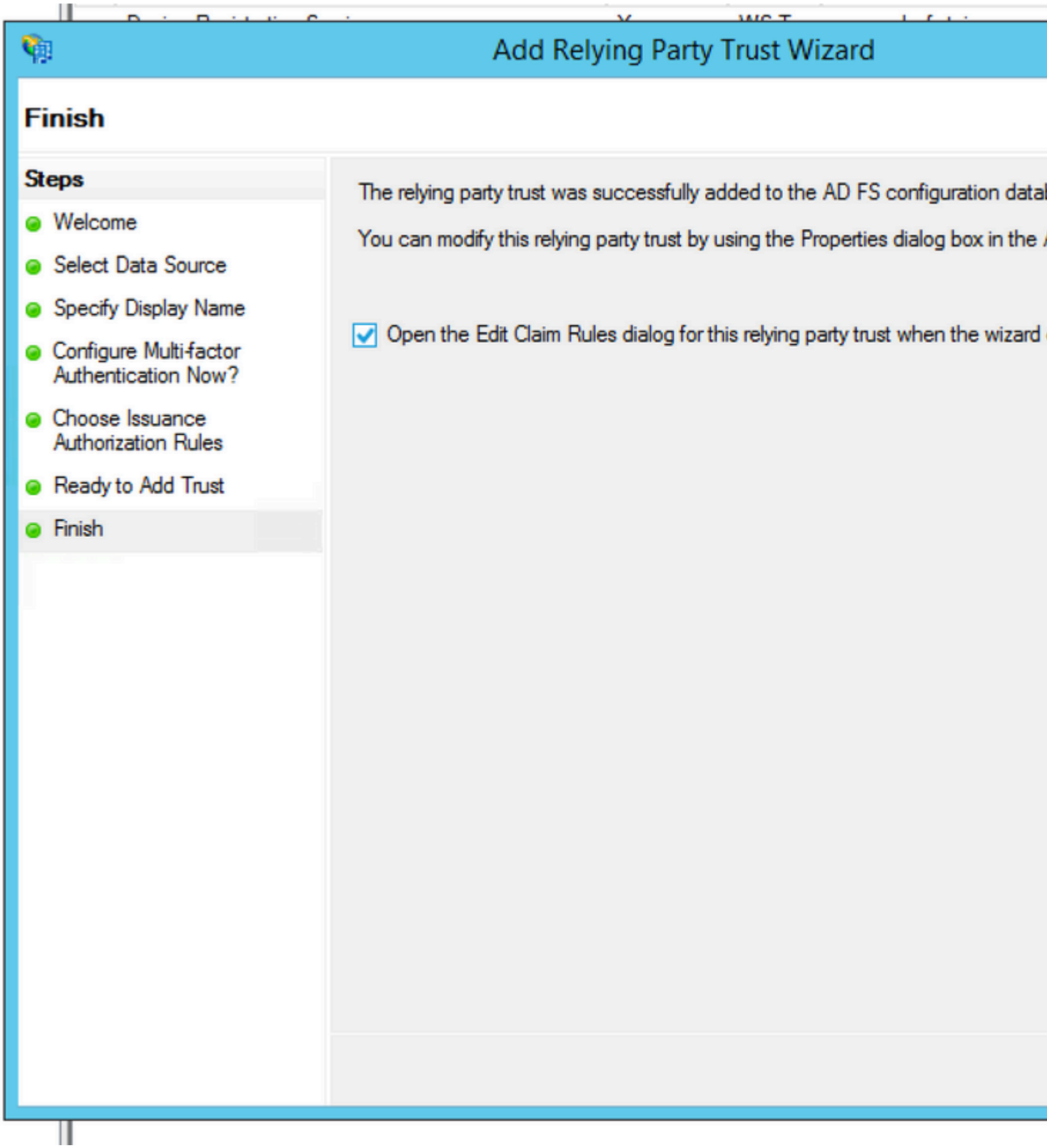

Add Relying Party Trust Wizard
Browse for Metadata File...
« SSO 11.5 ▸ Pod1
Search
Organize
New folder
Downloads
Recent places
This PC
Desktop
Documents
Downloads
FOLDERS on ARU
Music
Pictures
Videos
Local Disk (C:)
DVD Drive (D:) IR
Name
Date modified
sp
8/18/2016 8:26 PM
File name: sp
Metad
< Previous


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:
uccx.contoso.com
Notes:
< Previous

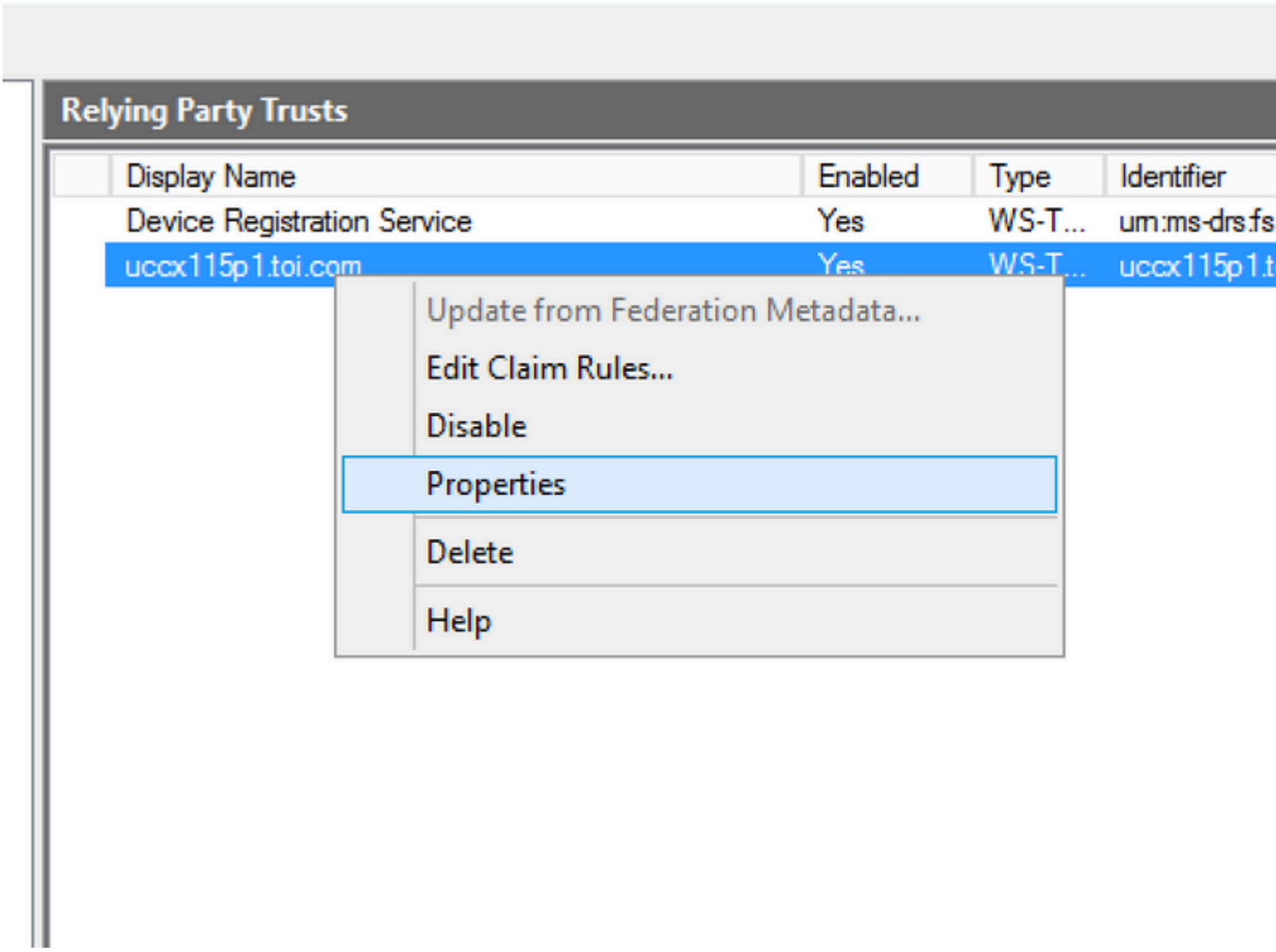

Add Relying Party Trust Wizard
Steps
Welcome
Select Data Source
Specify Display Name
Configure Multi-factor Authentication Now?
Choose Issuance Authorization Rules
Ready to Add Trust
Finish
Configure multi-factor authentication settings for this relying party trust. Multi-fa
there is a match for any 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
Configure multi-factor authentication settings for this relying party trust.
You can also configure multi-factor authentication settings for this relying
Authentication Policies node. For more information, see Configuring Authe
< Previous

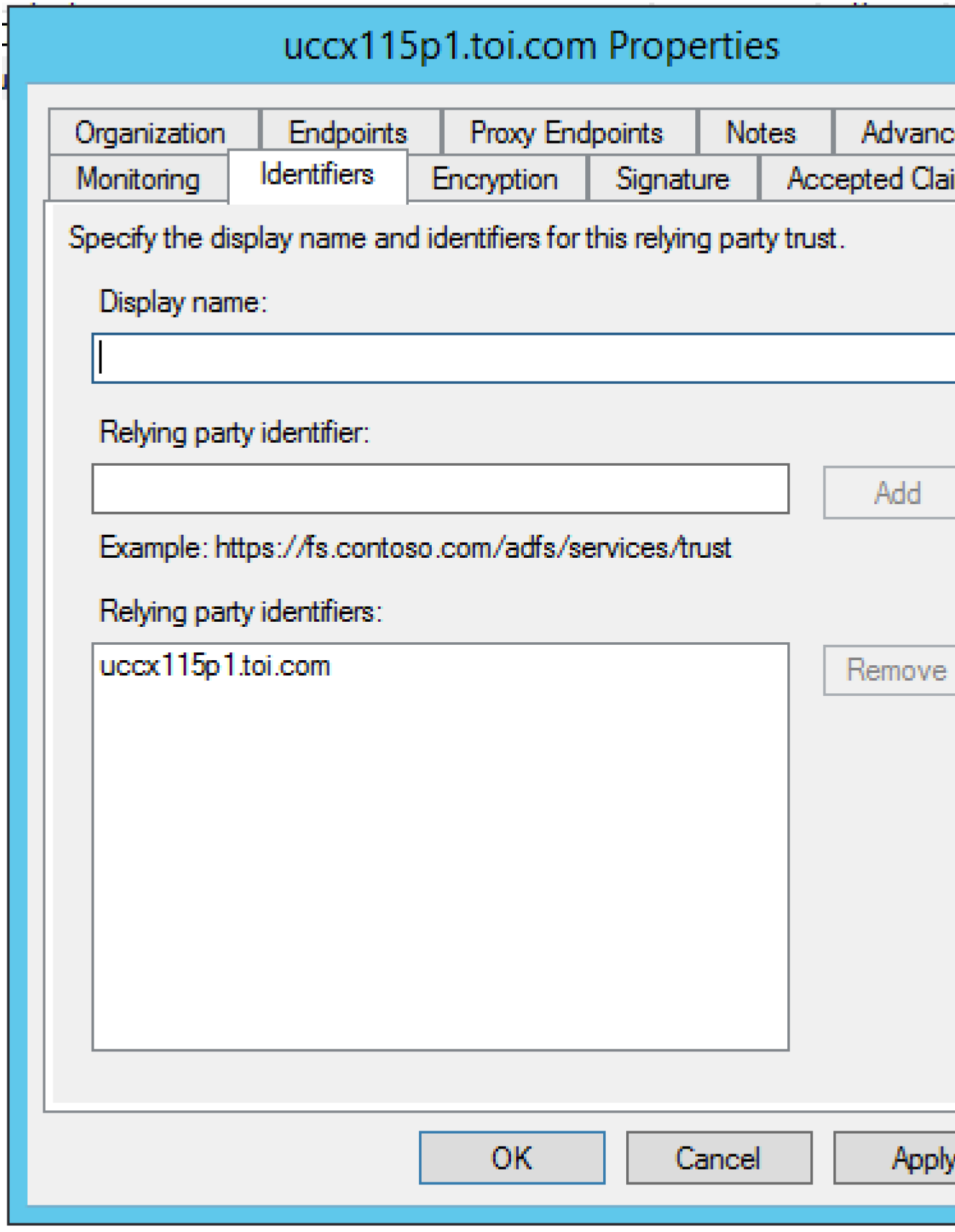


æ¥é©Ÿ4.å®Œæ˜¯ä¿¡è³´æ–¹ä¿¡ä»»çš„å»ºç«‹ã€‚

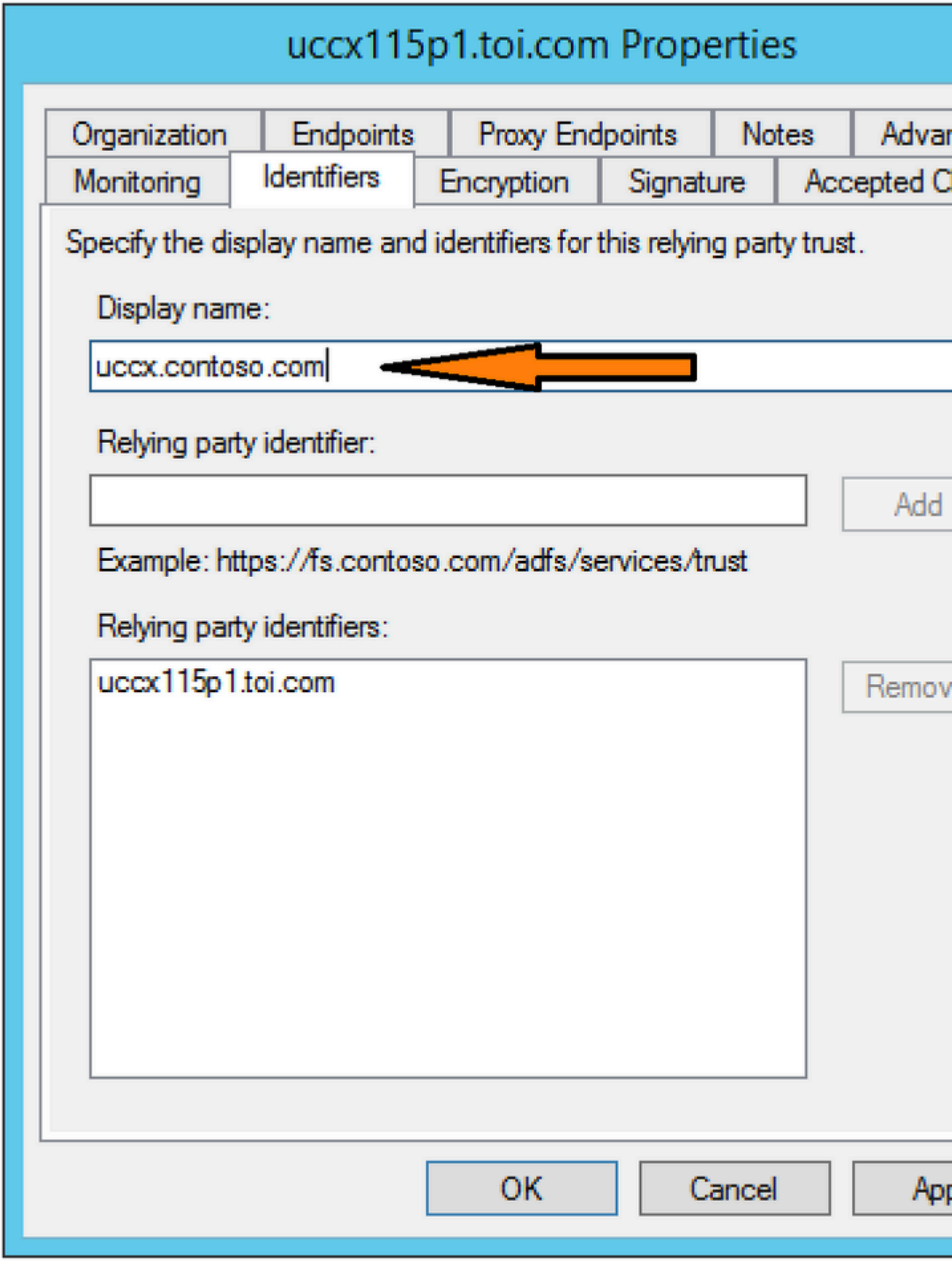


æ¥é©Ÿ5.åœ¨ä¿¡è³´æ–¹ä¿¡ä»»çš„å±¬æ€§ä¸¼Œé€‚æ“‡ Identifier é ç±¤ã€‚


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
Advanc
Monitoring
Identifiers
Encryption
Signature
Accepted Clai
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:
uccx115p1.toi.com
Remove
OK
Cancel
Apply

æ¥é©Ÿ6.å°‡è˜å^¥ç¬¦è™Ÿè¨®šç‚ºCisco Identity Serverçš„å®Œå…¨é™�å®šä¸»æ©Ÿå��ï¼Œæ–¼Cisco Identity Serverå¯¦ä¾žå…¶ç¢²å¾— sp.xml å·²ä¸‹è¼‰ã€‚



æ¥é©Ÿ7.æŒ‰ä¸€ä¸‹å•³é•µä¿¡è³´æ–¹ä¿¡ä»»ï¼Œ¶å¾Œæ‰€æŒ‰ä¸€ä¸‹ Edit Claim Rules.

uid â€” æ‡‰ç¨‹åº¼éœ€è¦æ¤å±¬æ€§ä¾†æ¨™è˜ç¶“é©—èˆçš„ä½¿ç”¨è€…å¸³æˆ·ã€‚
user_principal - Cisco
Idéœ€è¦æ¤å±¬æ€§ä¾†æ¨™è˜ç¶“é©—èˆçš„ä½¿ç”¨è€…å¸³æˆ·çš„ ˜åŸŸã€‚

é ˜æ¬¾ç”³è«‹è¦æ±‚1:

æŒ‰å••ç¨±æ–°å¢žè¦æ±‚
NameID åž‹å^¥ï¼^å°‡LDAPå±¬æ€§çš„å€¼ä½œç‚ºå®£å‘Šå‚³é€ï¼‰ï¼š

- é¸æ“‡å±¬æ€§å„²å˜ä½œç‚ºActive Directory
- å°æ˜ LDAPå±¬æ€§ User-Principal-Name æ^é••è‡³ user_principal ï¼^å°æ¯ï¼‰
- é¸æ“‡å¿…é ^ç”¨ä½œçš„LDAPå±¬æ€§
  userId ä¾›æ‡‰ç”¨ç¨‹å¼ä½¿ç”¨è€…ç™»å…¥ä¸¦å°‡å…¶ä°æ˜ å^° uidï¼^å°æ¯）

é…ç½®ç¤ºä¾‹ SamAccountName å°‡ç”¨æˆ·è¿›è€…ID:

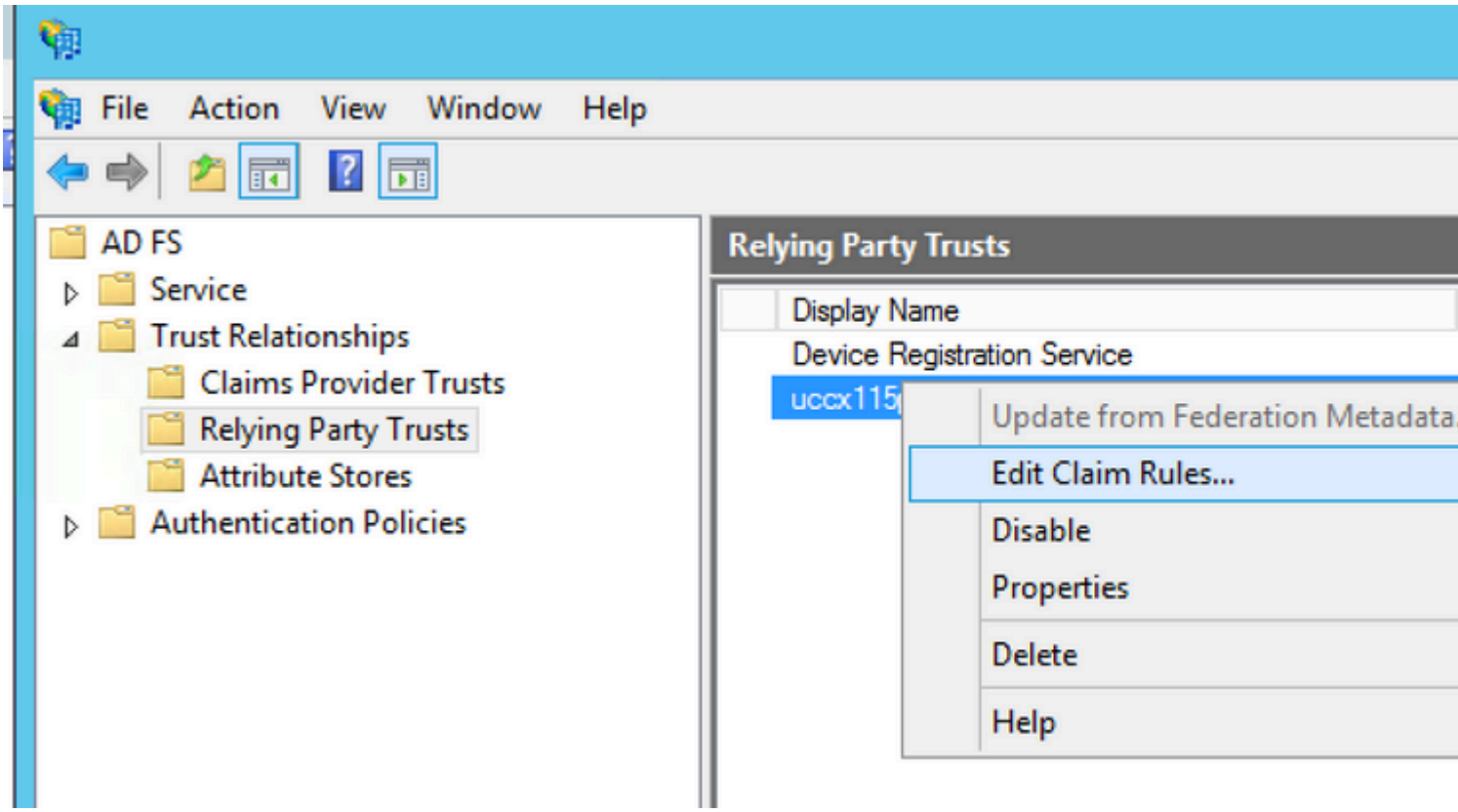
- å°æ˜ LDAPå±¬æ€§ SamAccountName æ^é••è‡³ uid.
- å°æ˜ LDAPå±¬æ€§ User-Principal-Name æ^é••è‡³ user_principal.

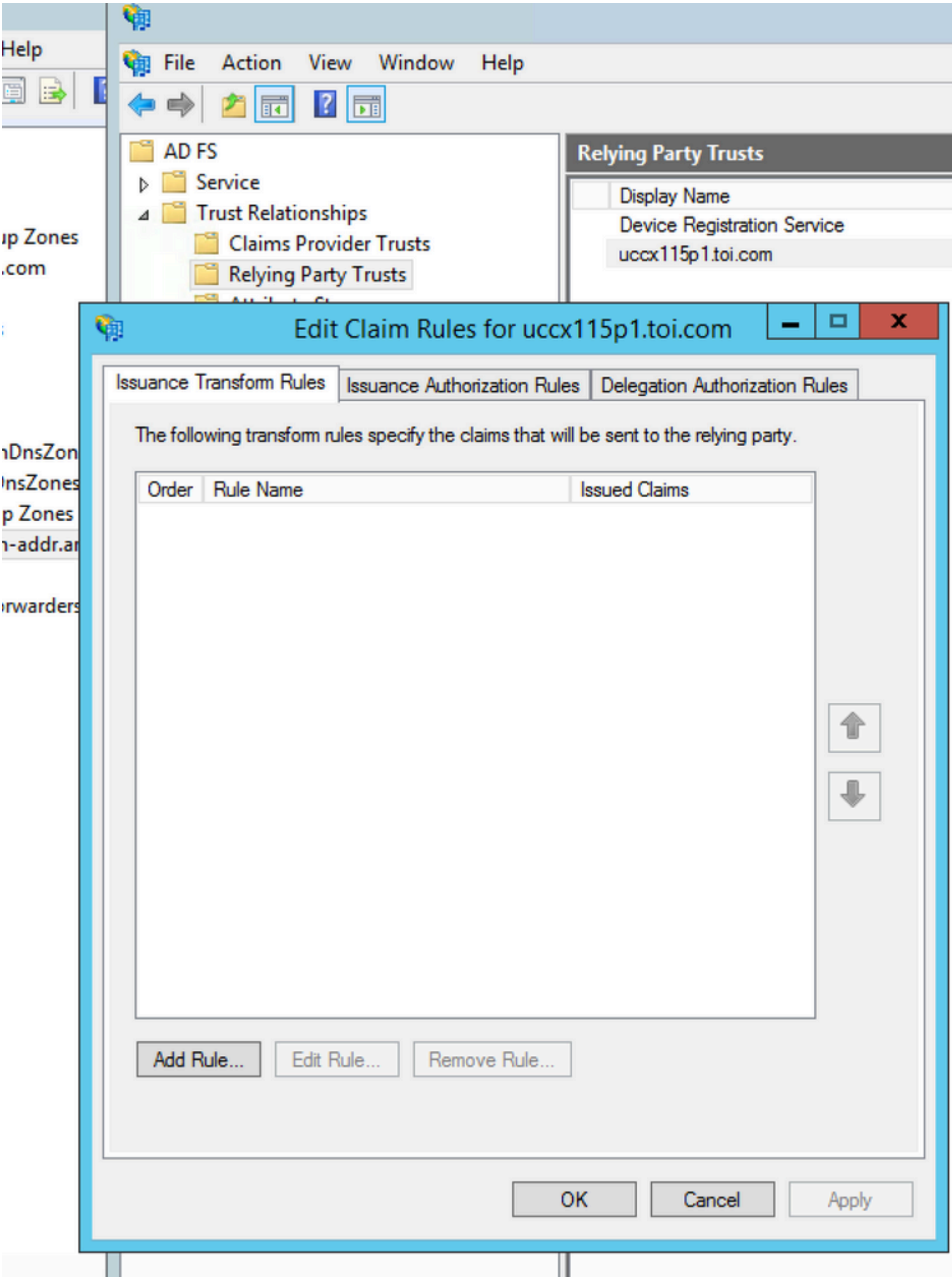
ç•¶UPNå¿…é ^ç”¨ä½œè¿›è€…IDæ™‚,é…ç½®ç¤ºä¾‹ï¼š

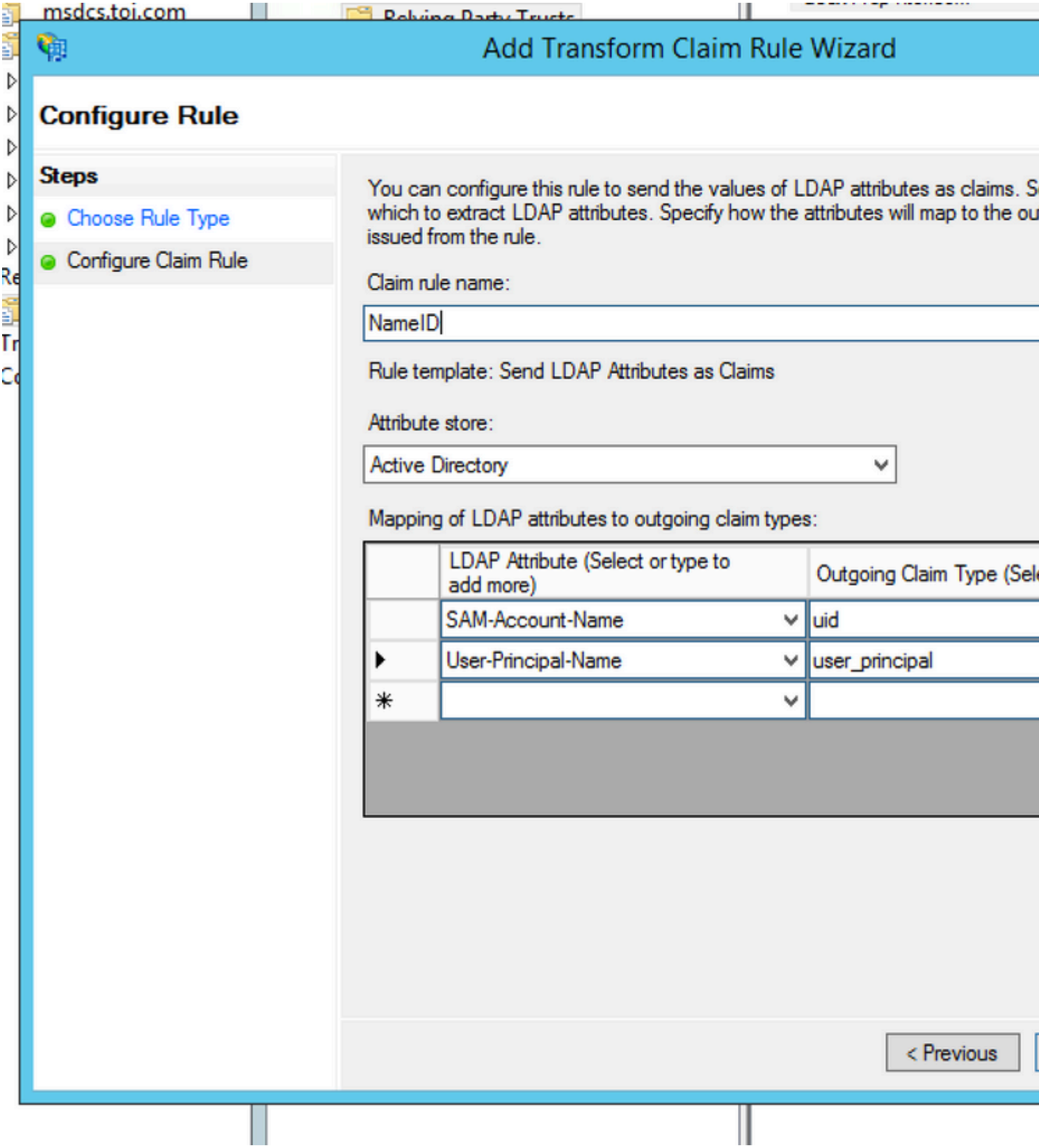
- å°æ˜ LDAPå±¬æ€§ User-Principal-Name æ^é••è‡³ uid.
- å°æ˜ LDAPå±¬æ€§ User-Principal-Name æ^é••è‡³ user_principal.

é…ç½®ç¤ºä¾‹ PhoneNumber å¿…é ^ç”¨ä½œè¿›è€…ID:

- å°æ˜ LDAPå±¬æ€§ telephoneNumber æ^é••è‡³ uid.
- å°æ˜ LDAPå±¬æ€§ User-Principal-Name æ^é••è‡³ user_principal.

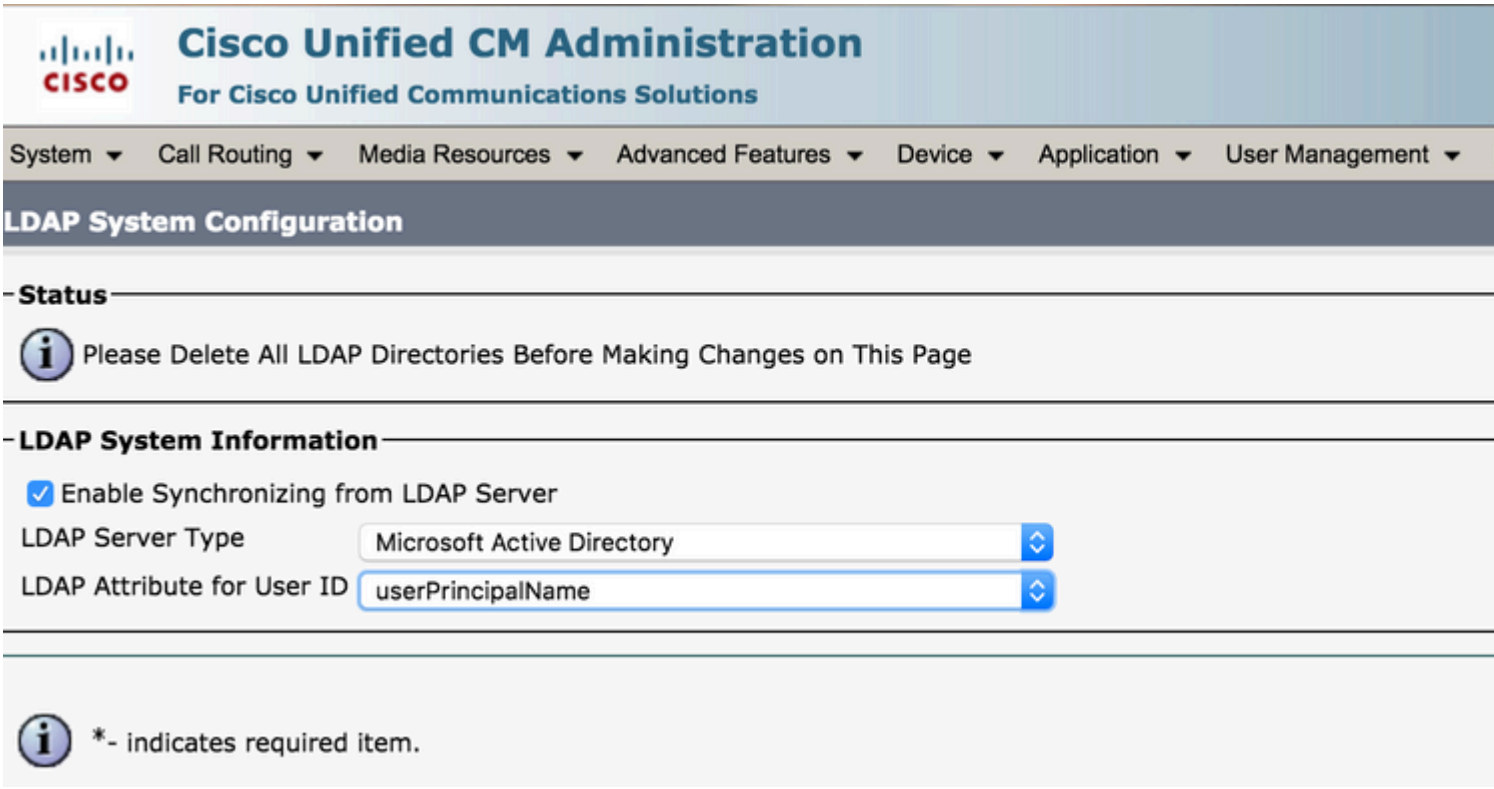

File
Action
View
Window
Help
AD FS
Service
Trust Relationships
Claims Provider Trusts
Relying Party Trusts
Attribute Stores
Authentication Policies
Relying Party Trusts
Display Name
Device Registration Service
uccx115
Update from Federation Metadata
Edit Claim Rules...
Disable
Properties
Delete
Help


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
Add Transform Claim Rule Wizard



æ³¨æ„ï¼šå¿…é ˆç¢ºä¿ç‚ºCUCM LDAPå®Œæ¥ä¸Šçš„ä½¿ç”¨è€…IDé…ç½®LDAPå±¬æ€§èˆ‡é…ç½®ç‚º uid åœ¨ADFSå®£å‘Šè¦å‰‡ä¸ä½¿ç¨±IDä¸ã€é€™æ˜¯ç‚ºCUICå’ŒFinesseç™»å…¥çš„æ£ç¢ºåŠŸèƒ

è¨»ï¼šæœ¬æ–‡æ”¼•ç”¨å®£å‘Šè¦�å‰‡å��ç¨±å’Œé¡¯ç¤ºå��ç¨±ï¼ˆå¦‚NameIDã€�UCCX

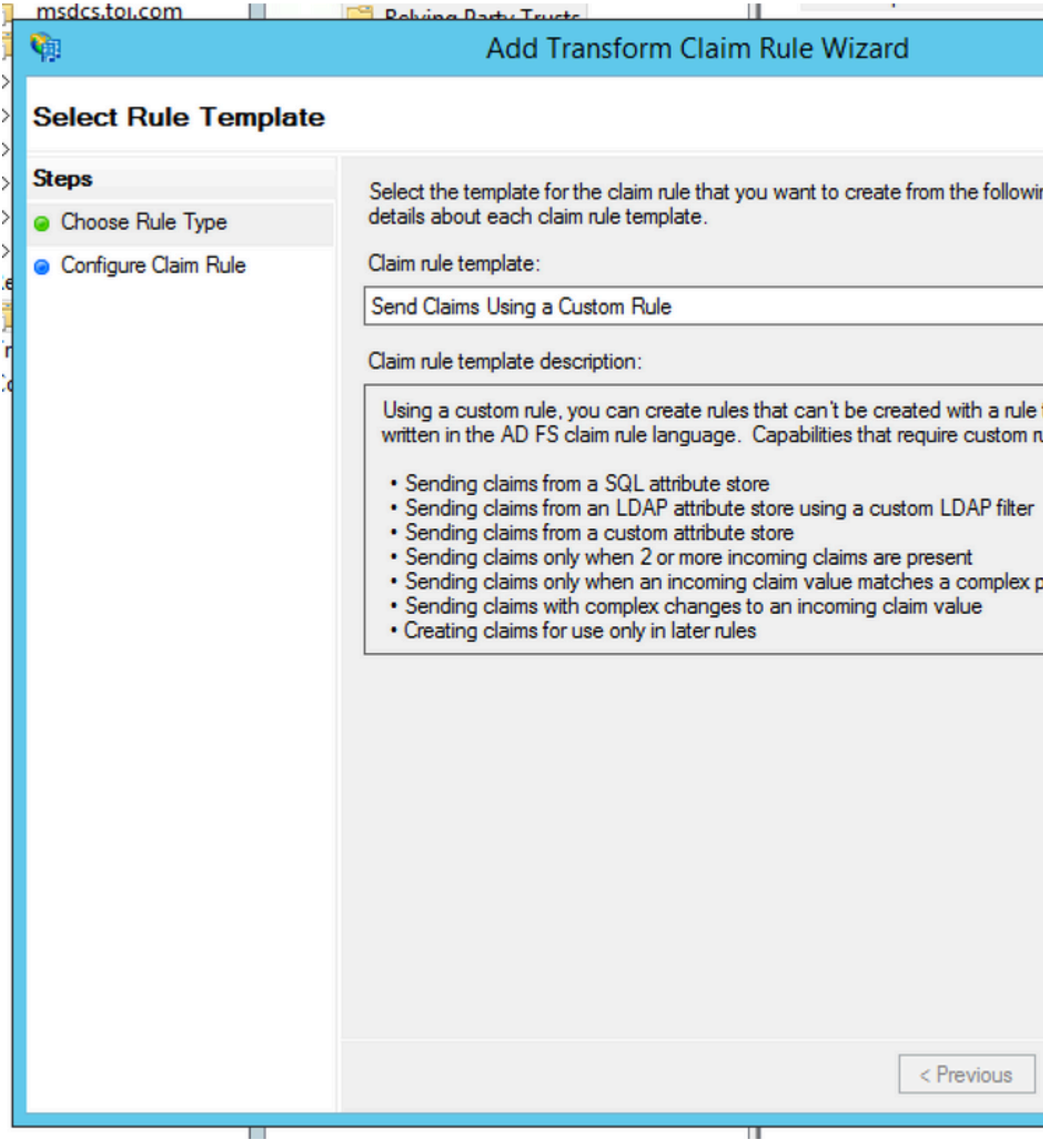


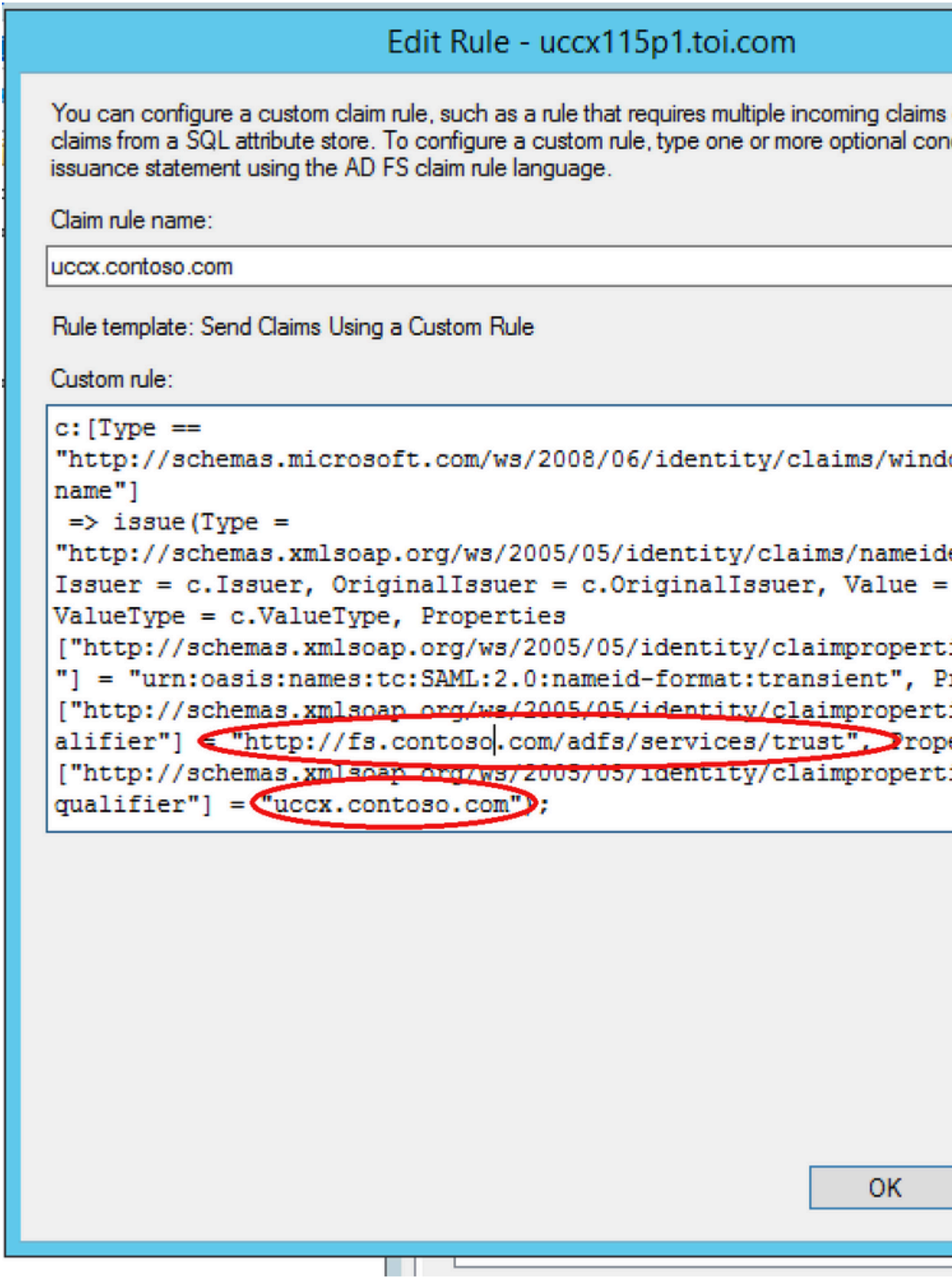
é ˜æ¬¾ç”³è«‹è¦�å‰‡2:

- æ–°å¢žå€‹è‡ªå®šç¾©å®£å‘Šè¦�å‰‡ï¼Œè¦‡è¦†ç¾„è¦‡è¦†çš„å��ç¨±æ
  Identity Serverçš„å®Œå…¨é™�å®šä¸»æ©Ÿå��ï¼Œæ–°å¢žæ¤è¦�å‰‡æ–‡æœ¬ã€‚

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

- åœ¨Cisco Identity Serverç¾¤é›†ä¸æ‰€æœ‰å®Œå…¨é™�å®šä¸»æ©Ÿå��éƒ½æ˜¯Cisco Identity Serverä¸å¯¦éš›ä½¿ç”¨è€…çš„ä¸»æ©Ÿå��ã€‚
- <Cisco Identity Serverçš„å®Œå…¨é™�å®šä¸»æ©Ÿå��>å�€åˆ†å¤§å°�å¯«ï¼Œæ¤å®ƒèˆ‡Cisco Identity Server FQDNå®Œå…¨åŒ¹é…ï¼ˆåŒ…æ‹¬å¤§å°�å¯«ï¼‰ã€‚
- <ADFSä¸»æœ�å™¨FQDN>å�€åˆ†å¤§å°�å¯«ï¼Œæ¤å®ƒèˆ‡ADFS FQDNå®Œå…¨åŒ¹é…ï¼ˆåŒ…æ‹¬å¤§å°�å¯«ï¼‰ã€‚


msdcs.tol.com
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 followi
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 r
• 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 p
• 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 con
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/windo
name"]
=> issue(Type =
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameide
Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value =
ValueType = c.ValueType, Properties
["http://schemas.xmlsoap.org/ws/2005/05/identity/claimpropert
"] = "urn:oasis:names:tc:SAML:2.0:nameid-format:transient", P
["http://schemas.xmlsoap.org/ws/2005/05/identity/claimpropert
alifier"] = "http://fs.contoso.com/adfs/services/trust",
["http://schemas.xmlsoap.org/ws/2005/05/identity/claimpropert
qualifier"] = "uccx.contoso.com";
OK

è¨»:

å€‹åˆ¥å¤§å°ï¼Œå› ç‚ºCmdLetå·²ç¶“ä½œç‚ºè§’è‰²å’ŒåŠŸèƒ½ä¿®æ–°å¢žçš„ä¸€éƒ¨åˆ†å®

è¨»:

å€‹åˆ¥å¤§å°ï¼Œå› ç‚ºæœƒèˆ‡è¿‘ã€Œä¿®å¾©ã€ä¸çš„ã€Œè¨å®šç¬¦

è¨»ï¼šåžUCCX 12.0ç‰ˆï¼ŒCisco IdSæ”¯æ´SHA-256ã€‚ä¿¡è³´æ–¹ä¿»ä½¿ç”¨SHA-256å°SAMLè«‹æ±‚é€²è¡Œç°½åï¼Œæœ‰å¤…ä¾†è‡ªADFSçš„éŸ¿æ‡‰ç›¸å®Œã€‚

ç”¨æ–¼è¯å¯ADFSçš„å¤šåŸŸé…ç½®

åœ¨ADFSä¸çš„è¯å¯æ…ã³¨ä‹ï¼Œç‰¹å®šADFSç‰¹å®šçš„ADFSç‚ºå…¶ä»––å·²é…ç½®åŸŸä¸çš„ä½¿ç”¨è€…...

åœ¨æœ¬ç¯€ä¸ï¼Œè¡¨ã€Œä¸»ãã€»ADFSã€€æ˜¯æŒ‡å¿…é ˆåœ¨IdSä¸ä½¿ç”¨çš„ADFSã€‚è¡¨ã€Œè¡¨ãè¯å¯ADFS

è¯å¯ADFSé…ç½®

åœ¨æ¯å€‹è¯å¯ADFSä¸ï¼Œå¿…é ˆç‚ºADFSå»ºç«‹ä¿¡ä»»ï¼Œä¸¦å¿…é ˆæŒ‡å®šIdSçš„ä¸»æ©Ÿåã€

ä»»ADFSé…ç½®

å°æ–¼ä»»ADFSï¼Œé™¤éžIdSçš„ä¿¡è³´æ–¼ä¿»å¤–ï¼Œéœ€è¦¢ä¿®æ”¹é…ç½®ã€‚

æ–°å¢ž Claim Provider Trust è¨å®šè¯å¯ç‚ºADFSã€‚

åœ¨å®£å‘Šæ¯¾ç¨‹å¼ä¿»ä¸ï¼Œç¡®ä¿¢ Pass through or Filter an Incoming Claim è¦å‰‡é…ç½®ç‚ºå‚³é žæ‰€æœ‰å®£å‘Šï¼Œé¸é …ï¼š

- å¿¯ç¨±ID
- å¾žä¸é¸æ“‡å¿¯ç¨±ID Incoming Claim Type æ”¶å˜ç®±
- é¸æ“‡ Transient ä½œç‚ºå‚³å…¥NameIDæ ¼å¼¯çš„é¸é …
- uidï¼šé€™æ˜¯ä¸€å€‹è‡ªå®šç¾©å®£å‘Šã€‚åœ¨CLIä¸è¼¸å…¥uid Incoming Claim Type æ”¶å˜ç®±
- user_principalï¼šé€™æ˜¯ä¸€å€‹è‡ªå®šç¾©å®£å‘Šã€‚åœ¨CLIä¸é¸µå…¥å€¼user_principal Incoming Claim Type æ”¶å˜ç®±

åœ¨IdSçš„ä¸»è¦ä¿»ä¸ï¼Œæ–°å¢ž Pass though or Filter an Incoming Claim ä»¥å‚³é žæ‰€æœ‰å®£å‘Šå€¼ä½œç‚ºé¸é …çš„è¦‰ä¸ã€‚

- å¿¯ç¨±IDFromSubdomain
- å¾žä¸é¸æ“‡å¿¯ç¨±ID Incoming Claim Type æ”¶å˜ç®±
- é¸æ“‡ Transient ä½œç‚ºå‚³å…¥NameIDæ ¼å¼¯çš„é¸é …
- uidï¼šé€™æ˜¯ä¸€å€‹è‡ªå®šç¾©å®£å‘Šã€‚åœ¨ä¸é¸µå…¥å€¼uid Incoming Claim Type æ”¶å˜ç®±
- user_principalï¼šé€™æ˜¯ä¸€å€‹è‡ªå®šç¾©å®£å‘Šã€‚åœ¨CLIä¸é¸µå…¥å€¼user_principal Incoming Claim Type æ”¶å˜ç®±

ADFSè‡ªå‹•æ›¸æ»¾å‹•æ›´æ–°

UCCX 11.6.1å€Šæ›´é«˜ç‰ˆæœ¬æ”¯æ€´è‡ªå‹•è‰²æ›¸¾å‹•æ›´æ–°ã€,(UCCX 11.6ä¸çš„Fedletåº«å€‡çˆ²å°ç‰ˆæœ¬14.0è§£æ±ºä¤†æ¤å•€é¡Œã€,)

Kerberosé©—è‰ï¼^æ•´å€^Windowsé©—è‰ï¼‰

æ•´å€^çš„Windowsèº«ä»½é©—è‰(IWA)ç‚ºä½¿ç”¨è€…æ€§èƒ½è¤‡é›œæ€§æ©Ÿå^¶ï¼Œä½†ä¸€

æ³¨æ„ï¼šå¦…å¾ž11.6å€Šæ›´é«˜ç‰ˆæœ¬æ”¯æ´Kerberosèº«ä»½é©—è‰ã€,

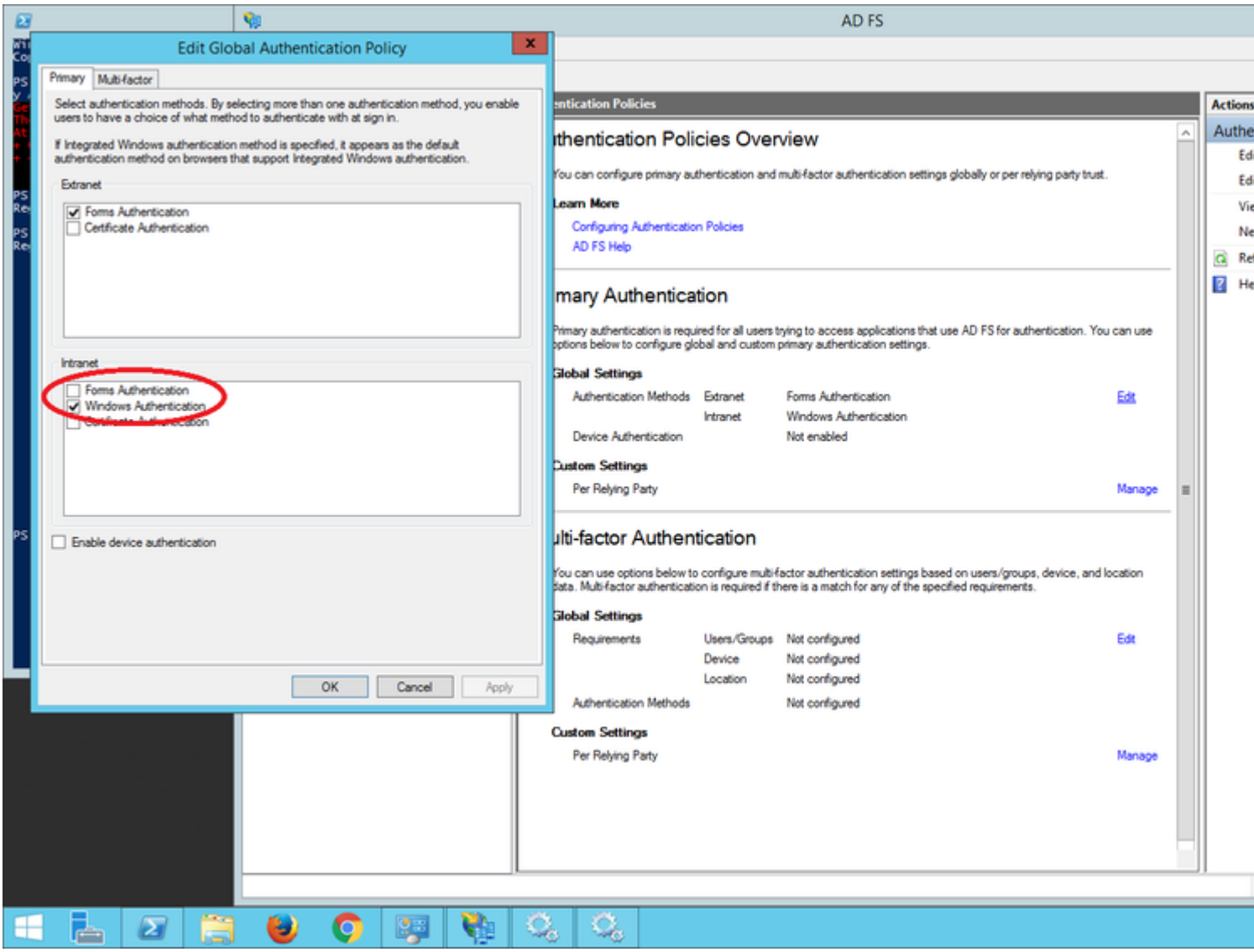
å·²ç™»å…¥å^°åŸŸæŽ§å^¶å™¨(DC)çš„åŸŸä½¿ç”¨è€…å€¯ç¨‹å¼ç™»å…¥å^°SSOå®¢æ^¶ç«¯ï¼Œè€Œç„¡éœ€3.0å®Œæ^�çš„ã€,

æ¥é©Ÿ1.é–‹å•ŸWindowså‘½ä»¤æ��ç¤ºç¬¦ä¸¦ä»¥ç®¡ç†å“¡ä½¿ç”¨è€…èº«ä»½é‚輸å…¥ä¾¿ä½¿ç”¨æŒ‡ **setspn -s http/**

\

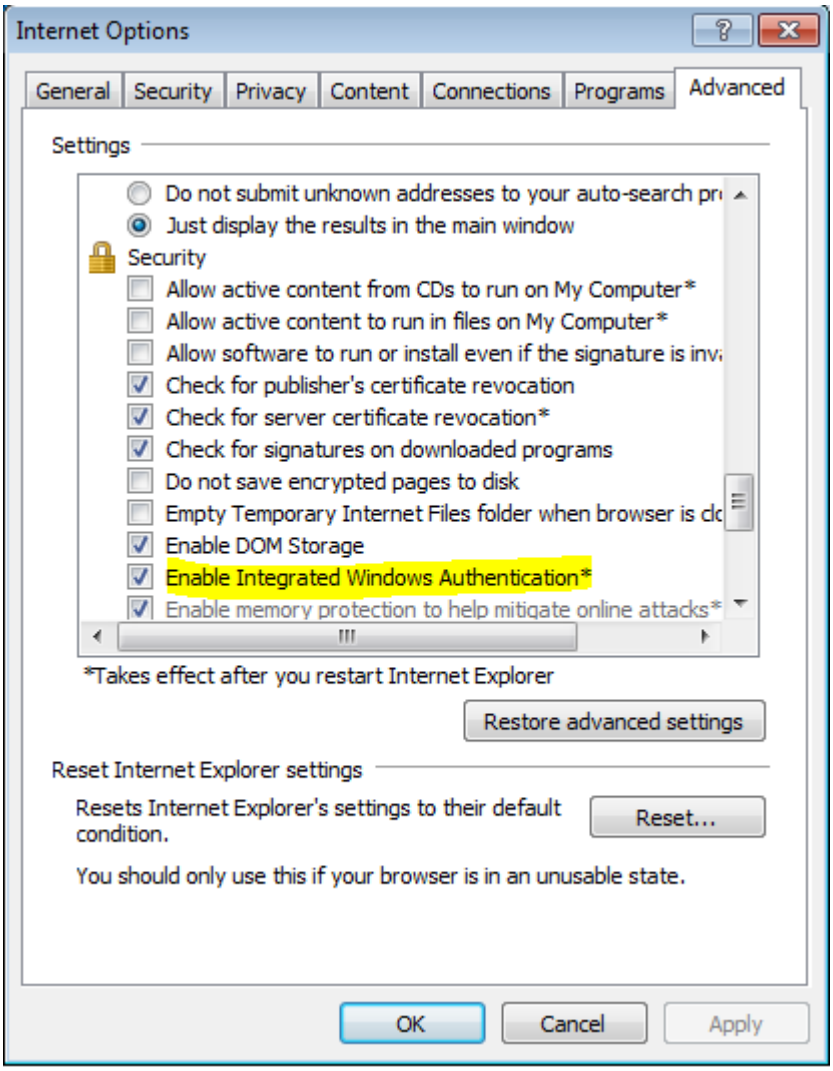
.

æ¥é©Ÿ2.ç¦�ç”¨ç—é”èº«ä»½é©—è‰ä¸¦ç‚ºIntranetç«™é»žå•Ÿç”¨Windowsèº«ä»½é©—è‰ã€,å°Žèˆªè
ADFS Management > Authentication Policies > Primary Authentication > Global Settings > Edit.åœ¨Intranetä¸‹ï¼Œç¢ºä¿ç¦�å�ªé¸ä¸Windowsèº«ä»½é©—è‰(å�–æ¶ˆé¸ä¸ã€Œè¡¨å–®èº«ä»½é©—è‰

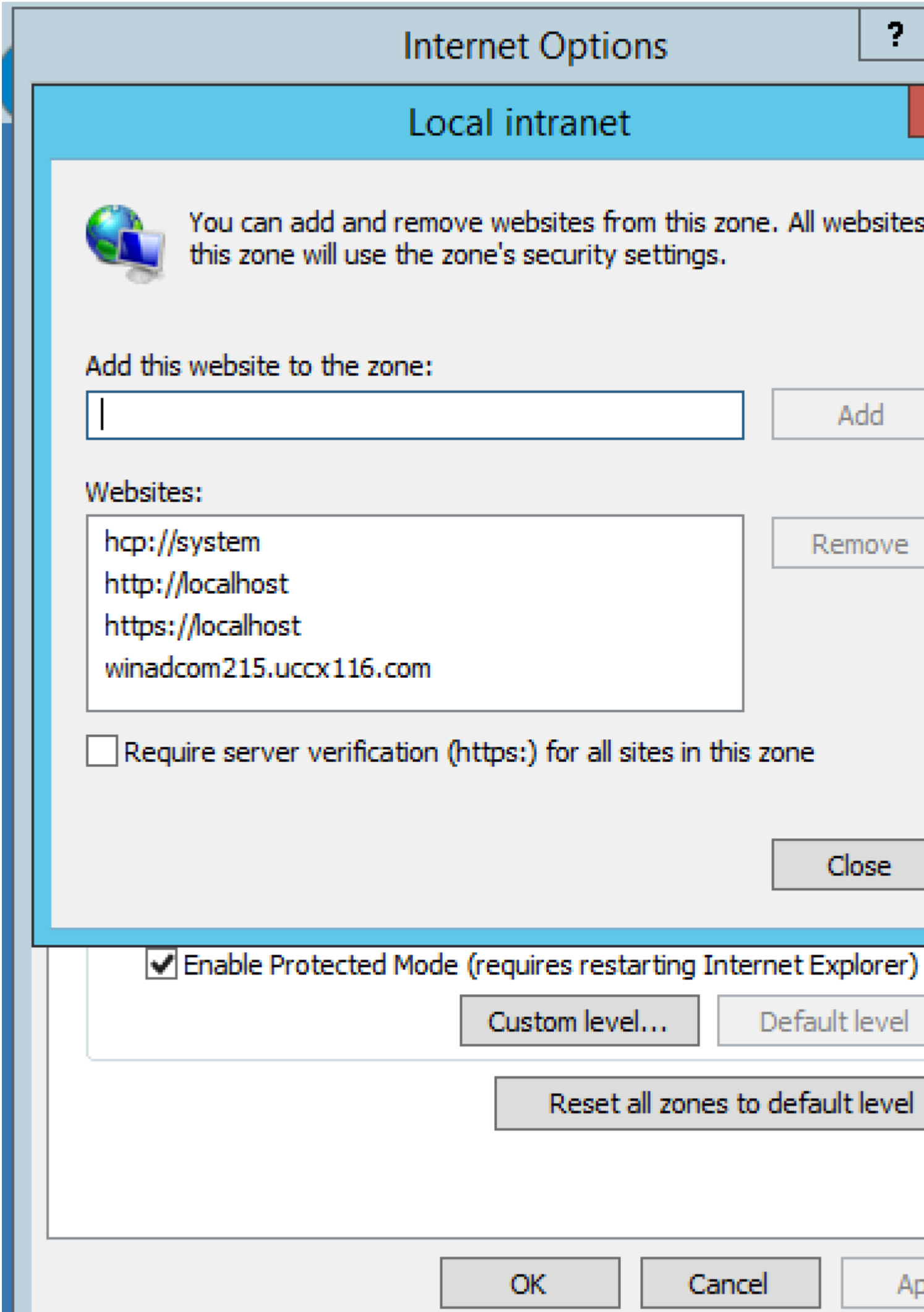


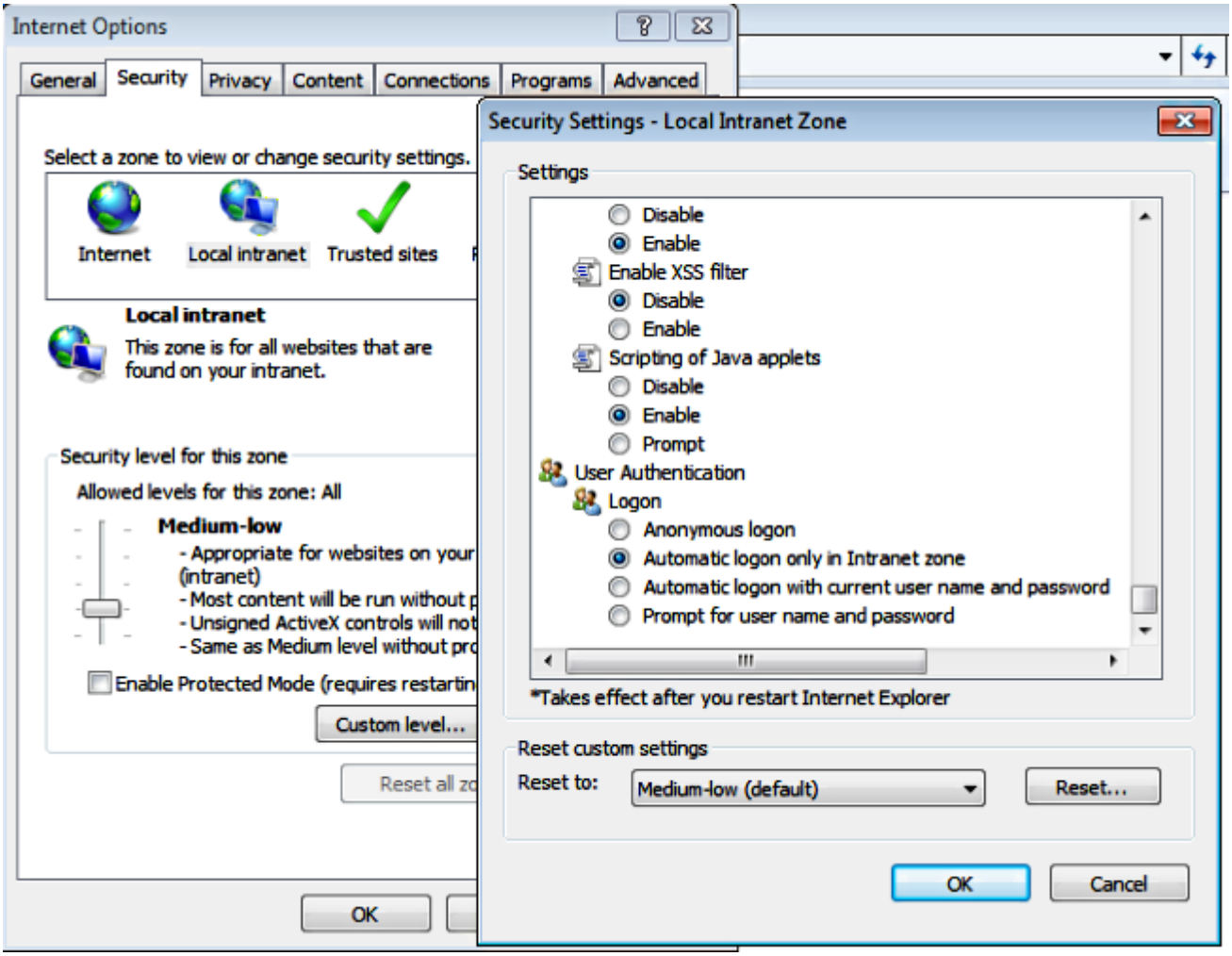
Microsoft Internet Explorer for IWAæ”¯æ´çš„é…ç½®

æ¥é©Ÿ1. ç¢ºä¿ Internet Explorer > Advanced > Enable Integrated Windows Authentication å·²é¸ä¸,



æ¥é©Ÿ2. å¿…é ˆå°‡ADFS URLæ–°å¢žå^° Security > Intranet zones > Sites (winadcom215.uccx116.com æ˜¯ADFS URL)ã€‚

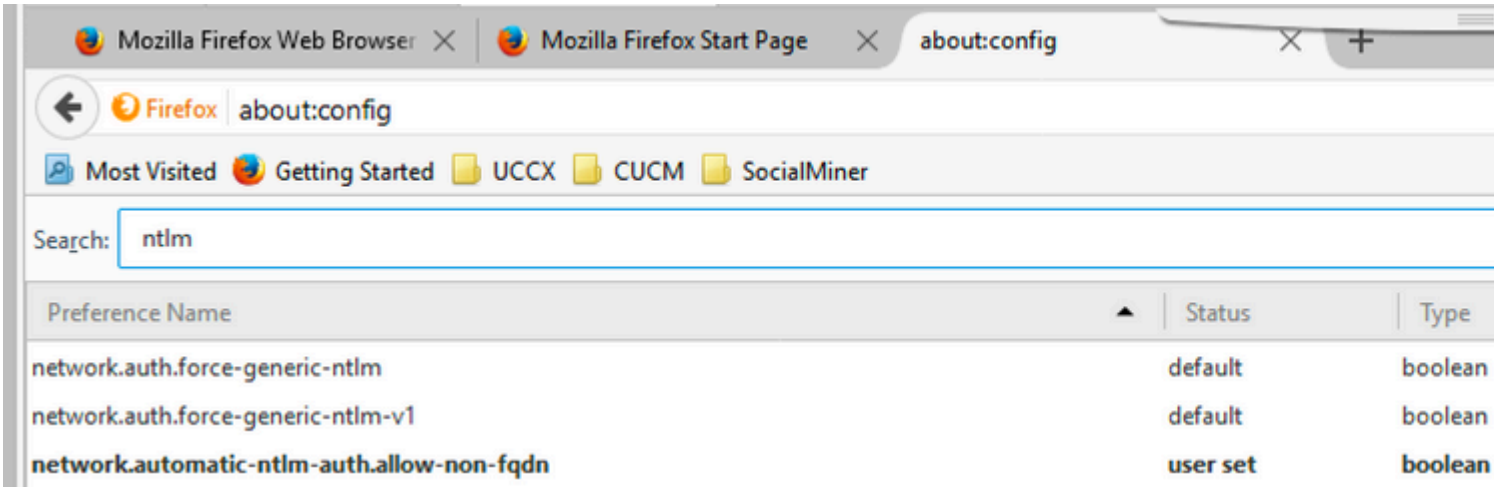

Internet Options
?
Local intranet
You can add and remove websites from this zone. All websites
this zone will use the zone's security settings.
Add this website to the zone:
Add
Websites:
hcp://system
http://localhost
https://localhost
winadcom215.uccx116.com
Remove
Require server verification (https:) 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



ç”¨æ–¼IWAæ”¯æ´ç„¡Mozilla Firefoxæ‰€éœ€çš„é…ç½®

æ¥é©Ÿ1.é€²å…¥Firefoxçš„é…ç½®æ¡¿å¼€ã€é–‹å•ŸFirefoxä¸¦è¼¸å…¥ about:config 作URLä¸ã€æŽ¥å—é¢¨éšªé™³è¿°ã€

æ¥é©Ÿ2.æ搜å°‹ ntlm ä¸¦å•Ÿç”¨ network.automatic-ntlm-auth.allow-non-fqdn 偏å…¶å®šç‚ºçœŸã€



æ¥é©Ÿ3.è¨å®š network.automatic-ntlm-auth.trusted-uris 仅ŸæˆÑé¡¯å¼ç„¡ADFS URLã€

ç”¨æ–¼IWAæ”¯æ´ç‚„Google Chromeæ‰€éœ€é…ç½®

Windowsä¸ç‚„Google Chromeä½¿ç”¨Internet Explorerè¨ç½®ï¼Œå› æ¤Internet Explorerä¸é€²è¡Œé…ç½® Tools > Internet Options å°�è©±æ–¹å¡Šï¼Œæ‰¾ä¸‹ä¸‹é•ç‚„ã€ŒæŽ§å¶¶é•¿æ•¿ã€ Internet Options åœ¨å•é¡žå¸¥å...§ Network and Internet.

SSOçš„é€²ä¸€æ¥é…ç½®

æœ¬æ–‡æª”å¾žSSOçš„IdPæ–¹é•¿æ••è¿°ä°†é...ç½®ï¼Œä»¥ä¾¿è¨‡æ€•ç‘IdSæ•´å•ˆã€,æœ‰é—œ

- UCCX
- UCCE
- PCCE

é©—è‰

æ¤é•Žç¨‹ç”¨æ–¼ç¢ºå®šæ˜¯å•¦åœ¨Cisco IdSå’ŒIDPä¹‹é–“æ£ç¢ºå»ºç«‹ä¿¡è³´æ–¹ä¿¡ä»»ã€,

- åœ¨ç€•è¦½å™¨ä¸è¼¸å…¥URL https://<ADFS_FQDN>/adfs/ls/IdpInitiatedSignOn.aspx?loginToRp=<IDS_FQDN>
- ADFSæ••ä¾›ç™»å...¥è¡¨å–®ã€,å¦,æžœä¸Šè¿°é...ç½®æ£ç¢ºï¼Œå‰¤æ¤é•¸å•¯ç”¨ã€,
- æˆ•åŠŸé©—è‰ï¼Œç€•è¦½å™¨å¿...é ‡é•å®šå•'è‡³https://<IDS_FQDN>:8553/ids/saml/res

---

è¨»ï¼šä½œç‚ºé©—è‰é•¸ä¸€éƒ¨å^†é¡¯ç¤ºçš„ã€Œæ¸å°•æ,...å–®ã€•é •ä¸•æ˜¯Œ¯

ç–‘é›£æŽ’è§£

å¦,éœ€ç–‘é›£æŽ’è§£ï¼Œè«‹å•fé–±https://www.cisco.com/c/en/us/support/docs/customer-collaboration/unified-contact-center-express/200662-ADFS-IdS-Troubleshooting-and-Common-Prob.htmlã€,

UCCX SSOç¹žé•Ž/æ•¢å¾©URL

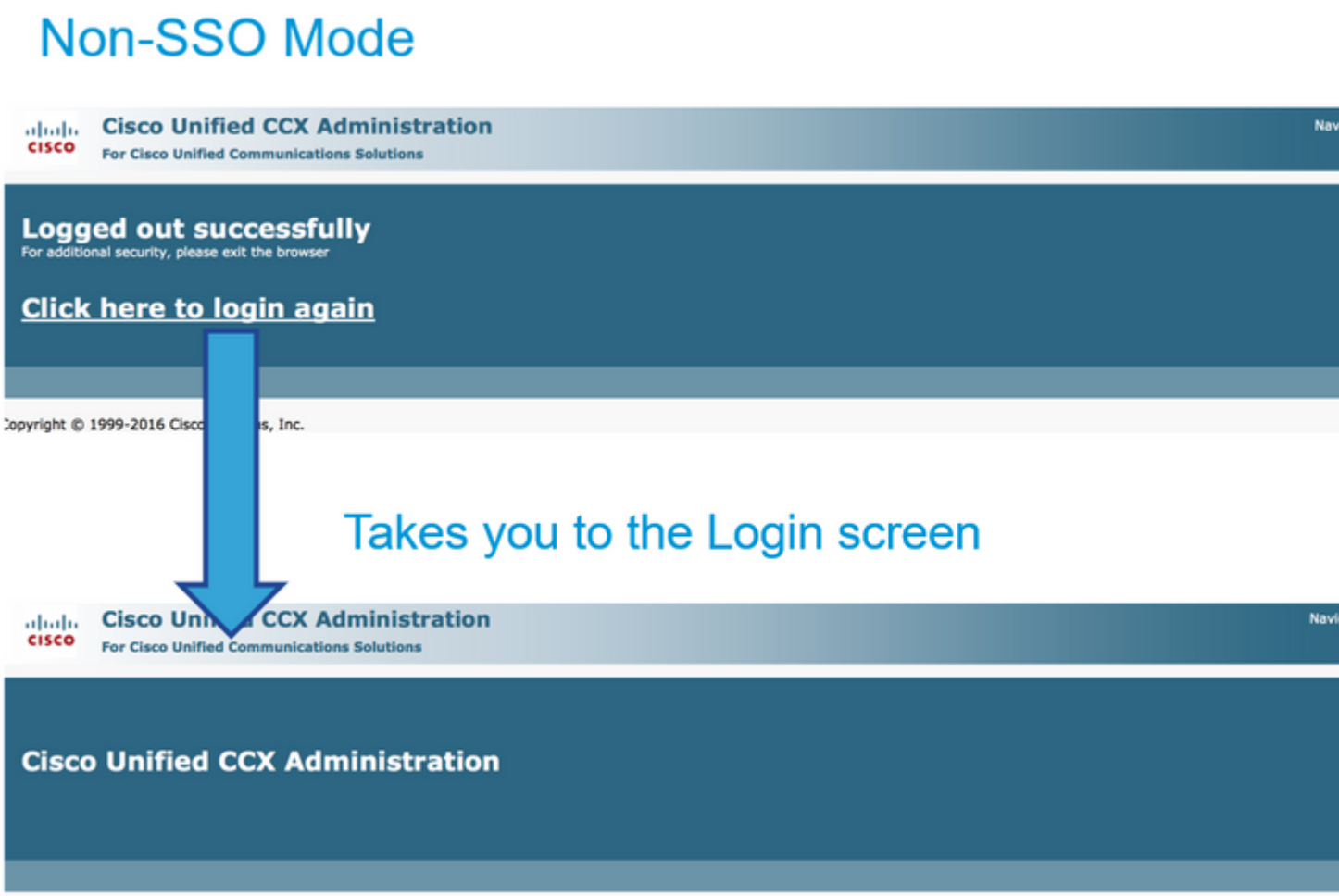
- Cisco Unified CCXç®¡ç•†
- Cisco Unified CCXå•¯ç¶è·æ€§

ç¦•ç”¨SSO

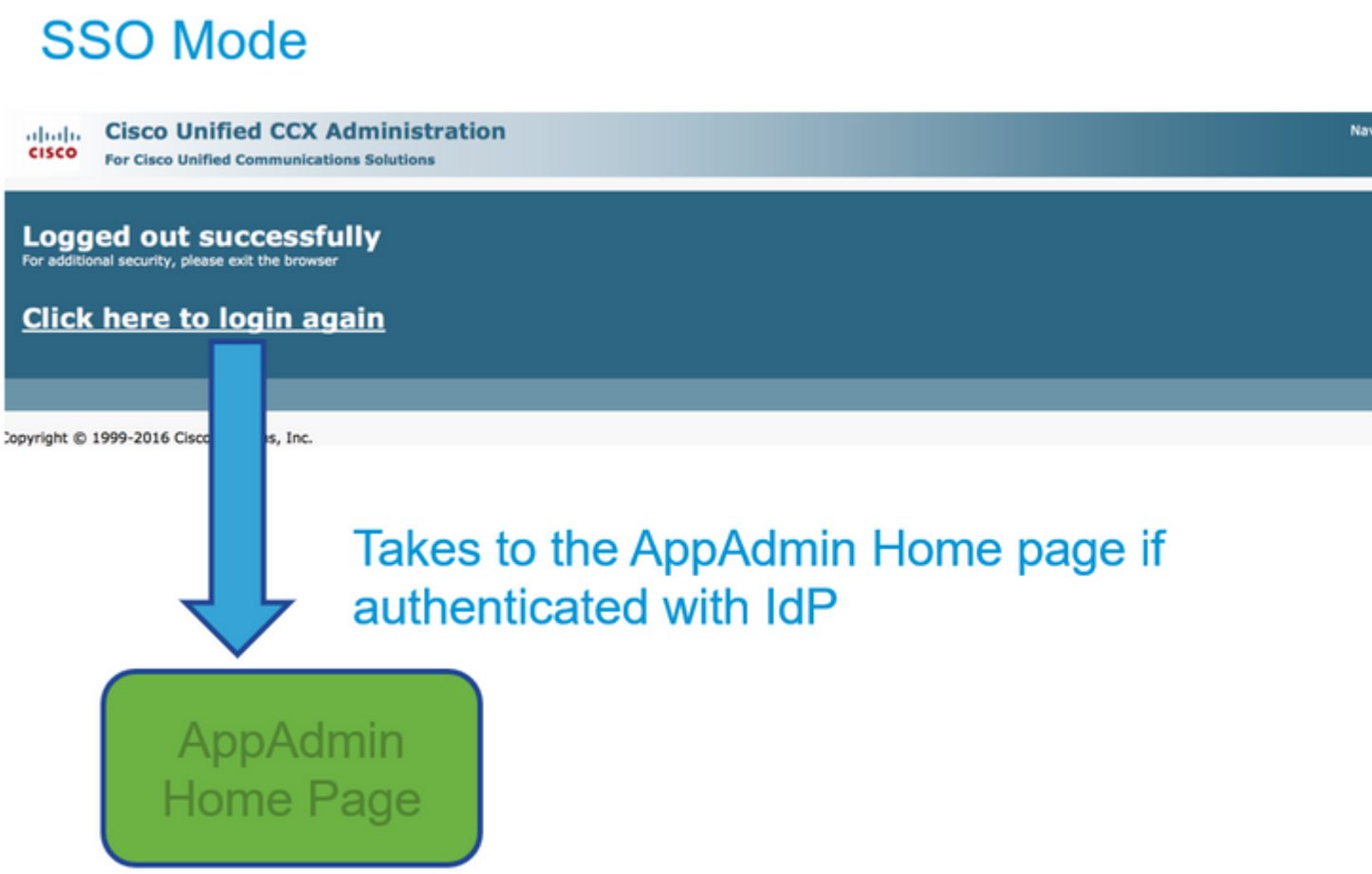
- GUIï¼šå°Žèˆªè‡³ CCX Administration > Single Sign-On (SSO) > Disable.
- CLI: set authmode non_sso (æ¤å‘½ä»¤å¿…é ˆå•Œæ™‚ç¦¯Pubå’ŒSubçš„SSO â€” å¦,æžœå‡ºç•«˜å•¯ç”¨æ€§(HA)ç¾¤é›†ï¼Œå‰‡å¾žUCCXç¯€é»žä¸Šçš„ä»»ä¸€ç¯€é»žåŸ·è¡

èž¢å¹•æˆªåœ–

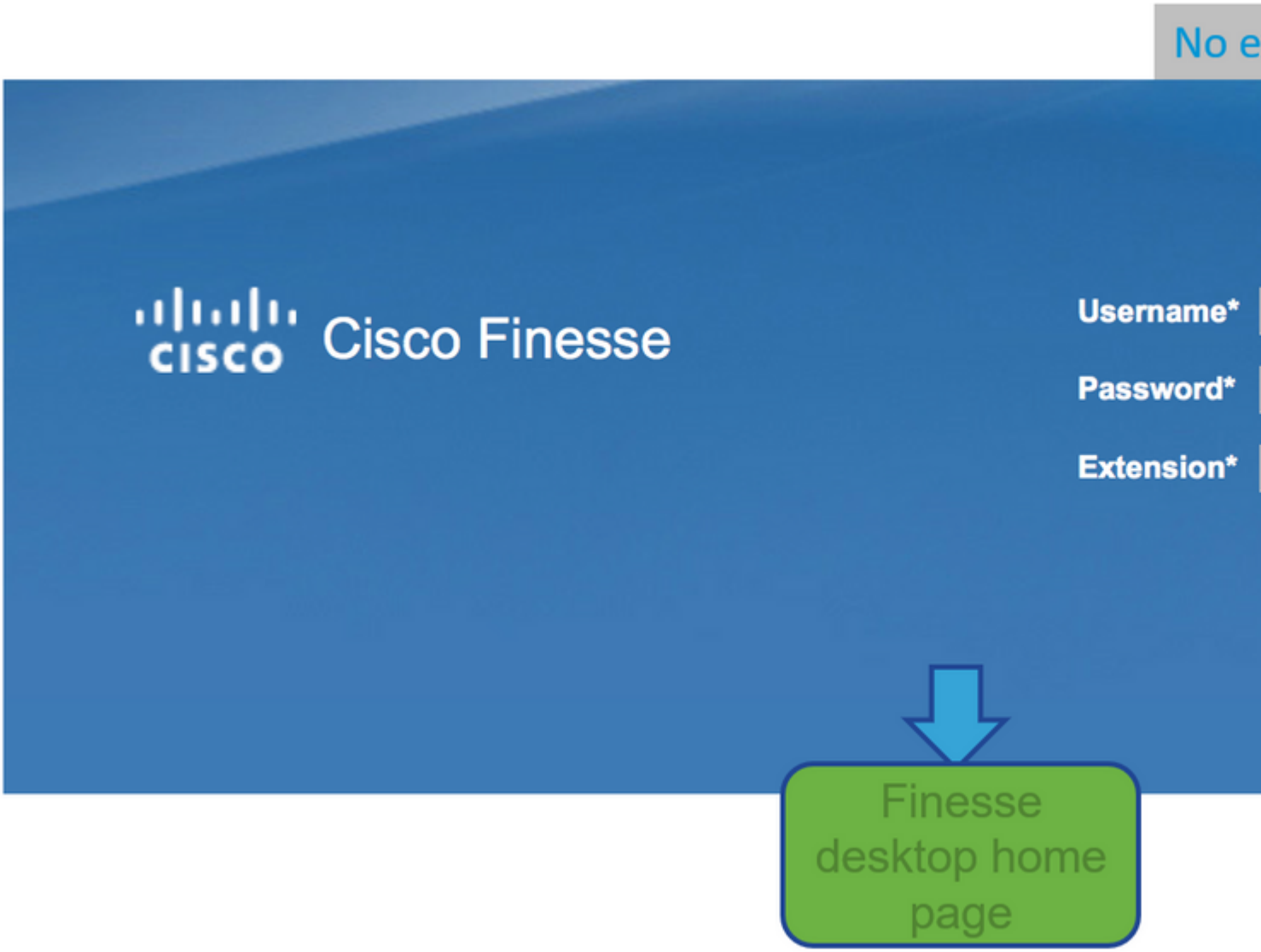
CCXç®¡ç�† â€” é�žSSO



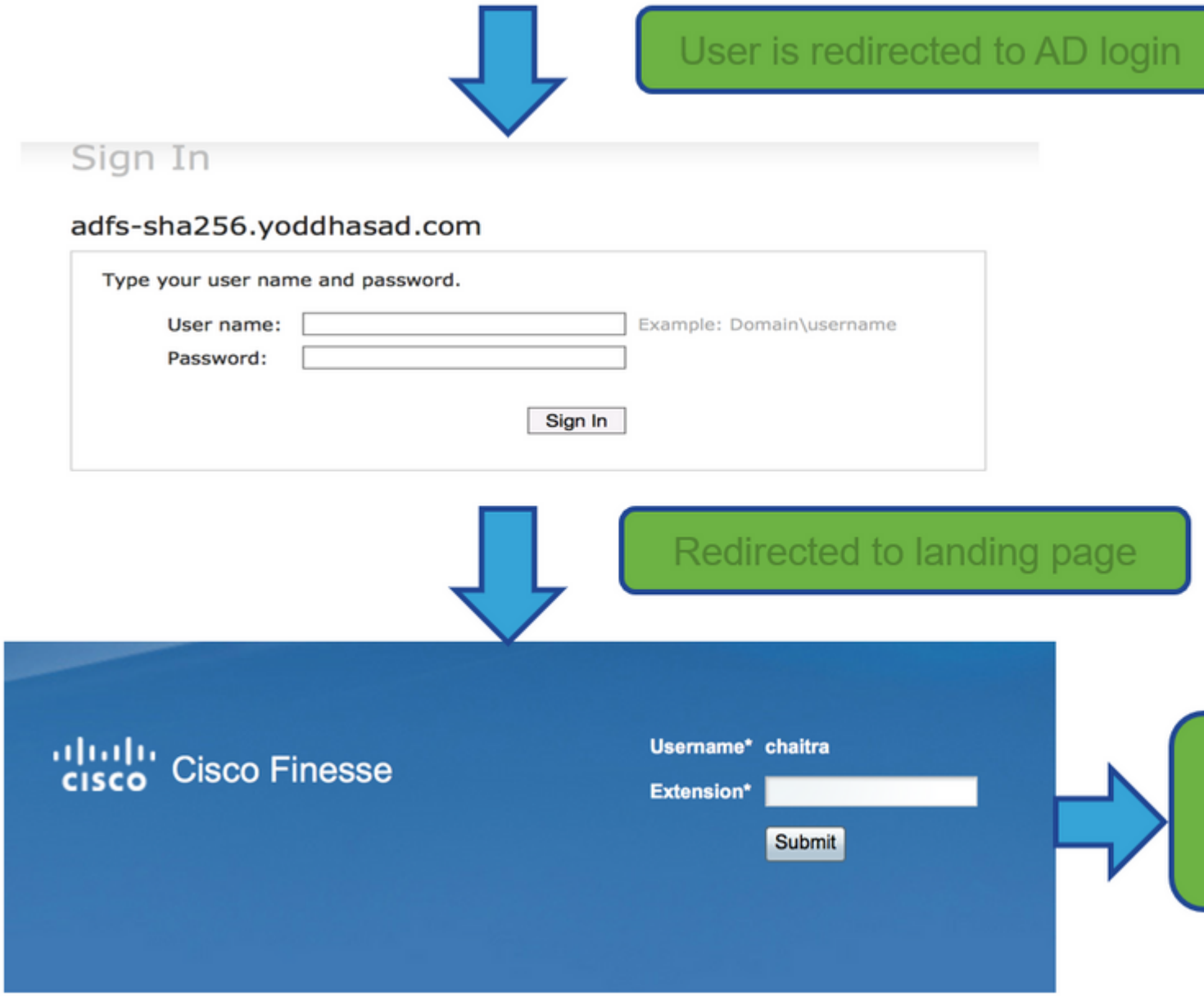
CCXç®¡ç�† â€” å•Ÿç”¨SSO



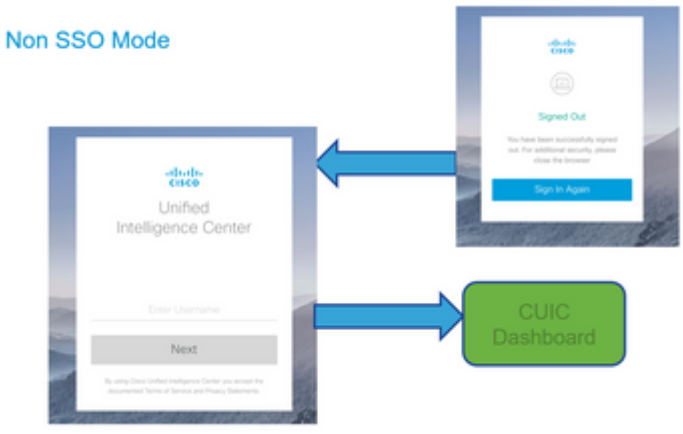
Finesseç™»å…¥ â€” é€šSSO



Finesseç™»å…¥ â€” å•Ÿç”¨SSO

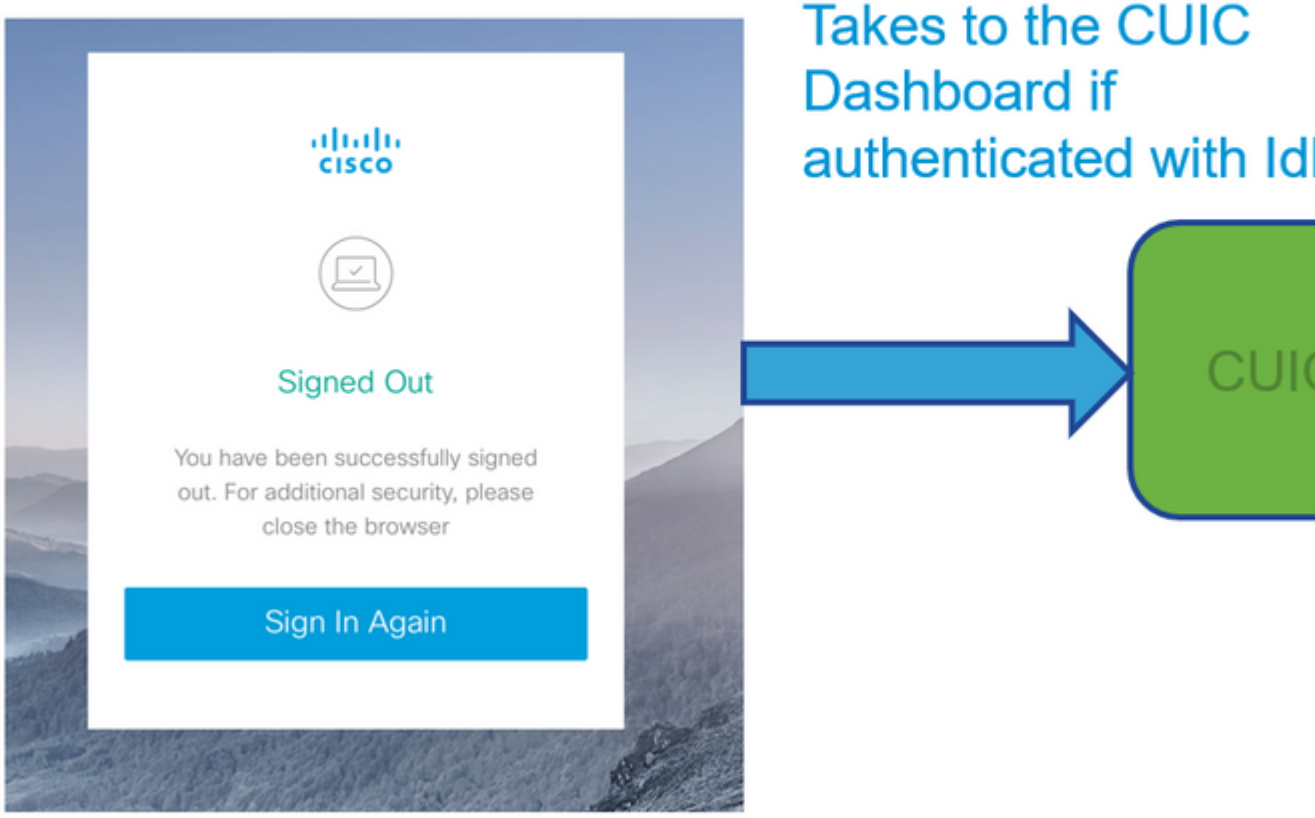


CUIC â€” é–žSSO



CUIC â€” å•Ÿç”¨SSO

SSO Mode


Takes to the CUIC Dashboard if authenticated with Id
cisco
Signed Out
You have been successfully signed out. For additional security, please close the browser
Sign In Again
CUI

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。