ä¸ºæ€�ç§‘è°«ä»½æœ�åŠ¡é…�ç½®è°«ä»½æ��

ç›®å½•

ç®€ä»‹
å…ˆå†³æ¡ä»¶
è¦�æ±‚
ä½¿ç”¨çš„ç»„ä»¶
èƒŒæ™¯ä¿¡æ¯
SSOæ¦‚è¿°
é…�ç½®æ¦‚è¿°
é…�ç½®
è°«ä»½éªŒè¯�ç±»åž‹
å»ºç«‹ä¿¡ä»»å…³ç³»
ADFS 2.0
ADFS 3.0
ä¸ºä¿¡èµ–æ–¹ä¿¡ä»»å��ç”¨å·²ç¾åŠ©çš„SAMLæ–è¨€ï¼ˆæ€�ç§‘Idï¼‰
ç”¨äºŽè�”å�ˆADFSçš„å¤šåŸŸé…�ç½®
è�”å�ˆADFSé…�ç½®
ä»»ADFSé…�ç½®
ADFSè‡ªåŠ¨è¯�ä¹¦æ»šåŠ¨æ›´æ–°
Kerberosè°«ä»½éªŒè¯�ï¼ˆé›†æˆ�Windowsè°«ä»½éªŒè¯�ï¼‰
Microsoft Internet Explorerçš„IWAæ”¯æŒ�é…�ç½®
ç”¨äºŽIWAæ”¯æŒ�çš„Mozilla Firefoxæ‰€éœ€çš„é…�ç½®
ç”¨äºŽIWAæ”¯æŒ�çš„Google Chromeæ‰€éœ€çš„é…�ç½®
SSOçš„è¿›ä¸€æ¥é…�ç½®
éªŒè¯�
æ•…éšœæŽ’é™¤
UCCX SSOæ—¥è·¯/æ�¢å¤�URL
ç¦�ç”¨SSO
å±•å¹•æ˜¾ç¤
CCXç®¡ç�† â€” é�žSSO
CCXç®¡ç�† â€” å¯ç”¨SSO
Finesseç™»å½• â€” é�žSSO
Finesseç™»å½• â€” å¯ç”¨SSO
CUIC â€” é�žSSO
CUIC â€” å¯ç”¨SSO

ç®€ä»‹

æœ¬æ–‡æ¡£ä¸ºæ€�ç§‘è°«ä»½æœ�åŠ¡(IdS)é…�ç½®è°«ä»½æ��ä¾›ç¨‹åº�(IdP)ä¸å¯¯ç

å…ˆå†³æ¡ä»¶

è¦�æ±‚

Cisco å»ºè®®æ‚¨äº†è§£ä»¥ä¸‹ä¸»é¢˜ï¼š

- 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�ˆèº«ä»½éªŒè¯�æœ�åŠ¡(ADFS)ç‰ˆæœ¬2.0/3.0

æ³¨æ„„ï¼šæœ¬æ–‡æ¡£å±•ç¤ºäº†UCCXï¼ŒUCCEå’ŒPCCEçš„é……ç½®ä¸IdS(UCCX/UCCE/PCCE)å’ŒIdPç±»ä¼¼ã€‚

ä½¿ç”¨ç„„ä»¶

æœ¬æ–‡æ¡£ä¸Žç‰¹å®šç„„è½¯ä»¶ç‰ˆæœ¬ä¸Žå…¶ä¸‹ï¼š

æœ¬æ–‡æ¡£ä¸Žç„„ä¿¡æ¯éƒ½åŸºäºŽç‰¹å®šå®žéªŒå®¤çŽ¯å¢ƒä¸çš„è®¾å¤‡ã€‚æœ¬æ–‡æ¡£ä¸ä½¿ç”¨çš„æ‰€æœ‰è®¾å¤‡å·²å¯ç”¨é»˜è®¤é…ç½®ã€‚å¦‚æžœæ‚¨çš„ç½‘ç»œå¤„äºŽå®žæ—¶ç”Ÿäº§ä¸ï¼Œè¯·ç¡®ä¿æ‚¨äº†è§£ä»»ä½•å‘½ä»¤çš„æ½œåœ¨å½±å“ã€‚

è¦ŒæŸ¥ä¿¡æ¯

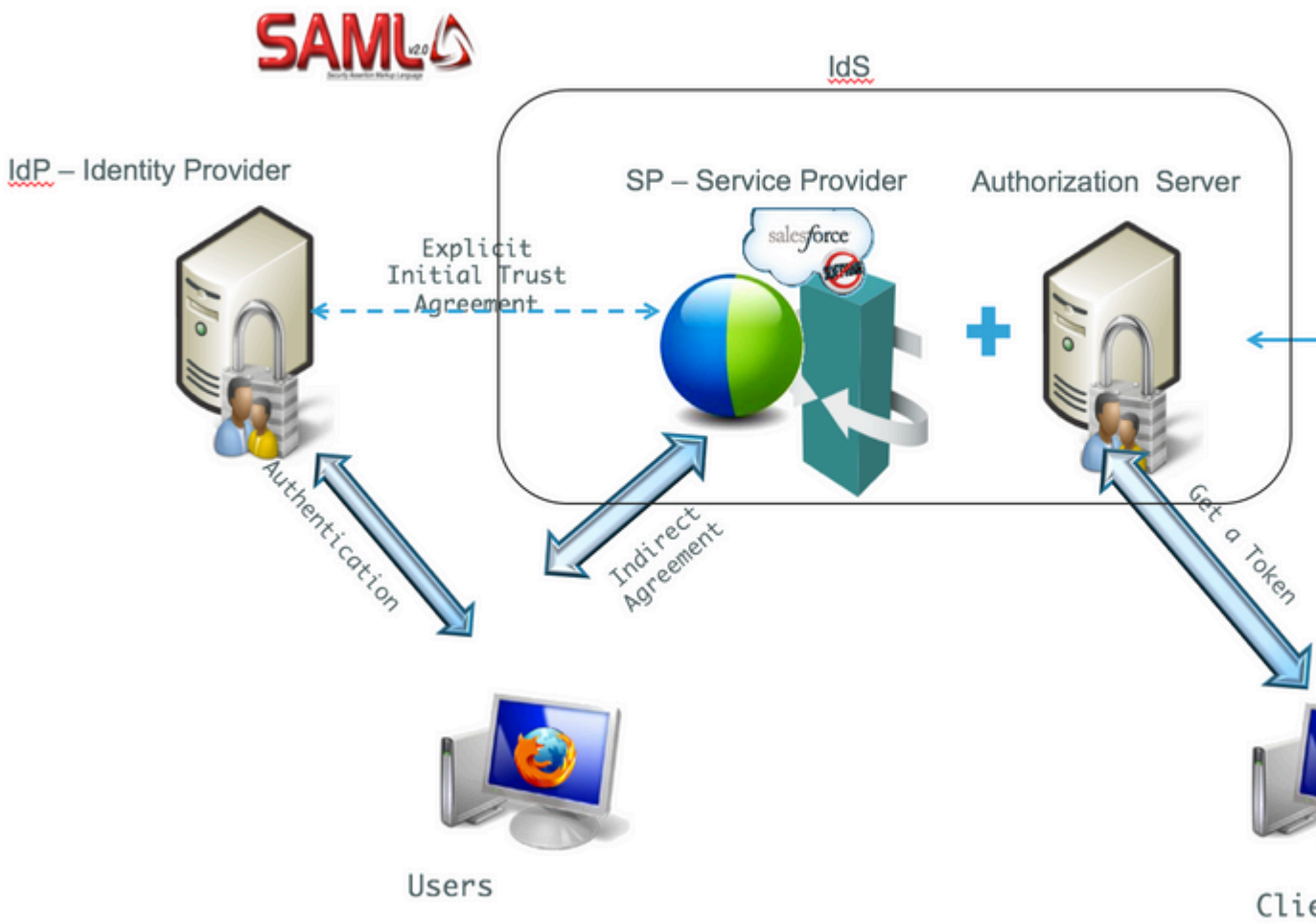
æ€»ç»“IdSéƒ¨ç½²æ¨¡å¼

äº§å“	éƒ¨ç½²
UCCX	å¹¶å˜
PCCE	ä¸ŽCUIC(Cisco Unified Intelligence Center)å’ŒLDï¼ˆå®žæ—¶•°æ�®ï¼‰å…±å˜
UCCE	ä¸ŽCUICå’ŒLDå…±å˜ï¼Œè¿›è¡Œ2000éƒ¨ç½²ã€‚ ç‹¬ç«‹å¼�ï¼Œé€‚ç”¨äºŽ4kå’Œ12kéƒ¨ç½²ã€‚

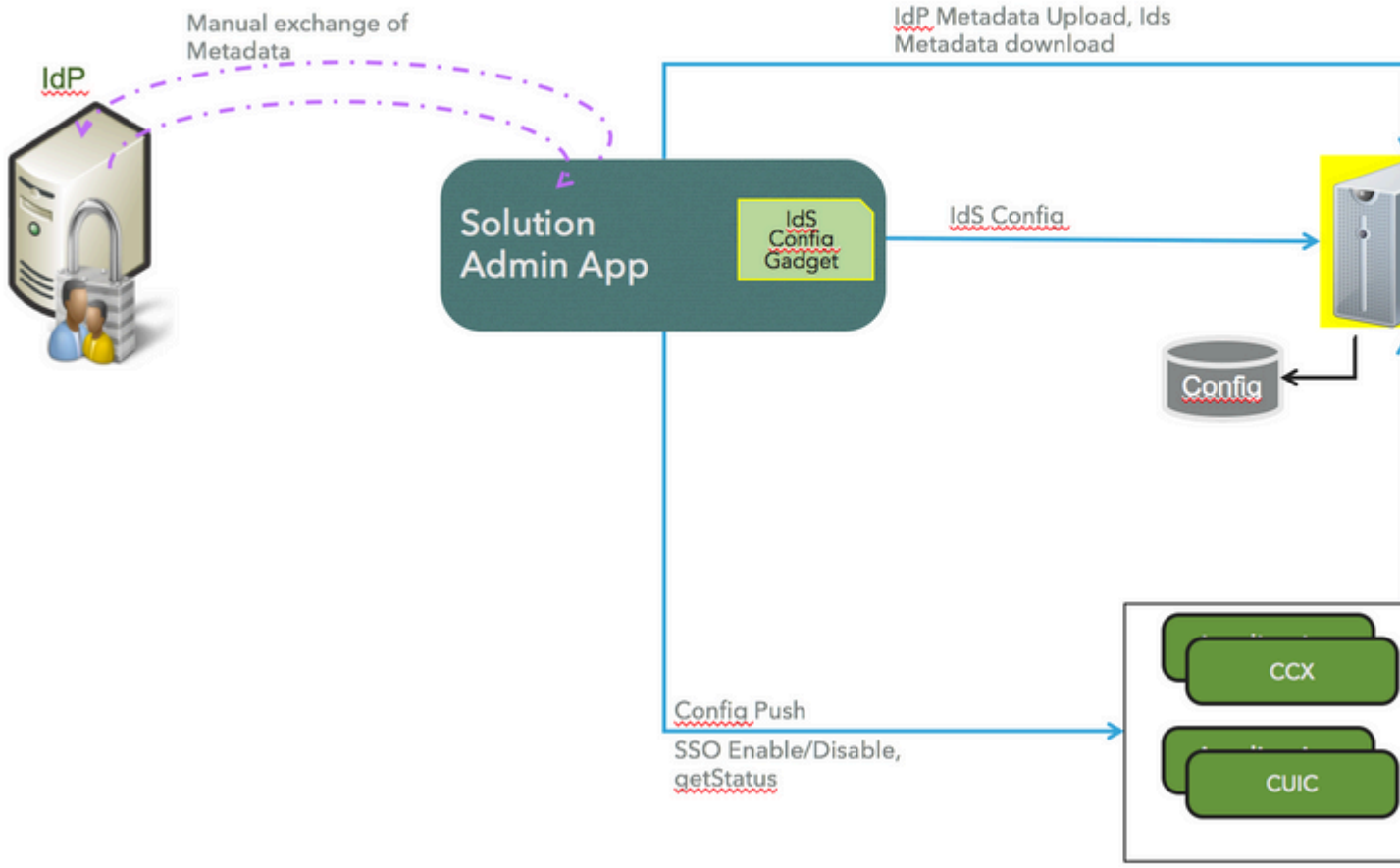
SSOæ¦‚è¿°

æ€»ç»“ä¸¤ä¸ªå…±å½¢å¼æ��ä¾›å¤šç§�æœ�åŠ¡ï¼Œä½¿äº‰æœ€ç»ˆç”¨æˆ·æ·¼ï¼Œæ¸å°ªé€

ä½¿ç”¨SAMLï¼ˆå®‰å…¨æ–‡æ¡£ æ‡®è¨€ï¼‰çš„SSOæ»¡è¶³è¦æ±‚ã€‚SAML/SSOä½¿ç”¨æˆ·èƒ½å¤Ÿé€šè¿‡11.5å…Šä¸€ä¸Šç‰ˆæœ¬ä¸å…¯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

é…ç½®æ¦‚è¿°



é…ç½®

èº«ä»½éªŒè¯ç±»åž‹

Cisco IdSä»…æ”¯æŒIdPçš„åŸºäºŽè¡¨å•çš„èº«ä»½éªŒè¯ã€‚

è¯·å‚é˜…è¿™äº›MSDNæ–‡ç« ä»¥äº†è§£å¦‚ä½•åœ¨ADFSä¸å¯¹è¡¨å•èº«ä»½éªŒè¯ã€‚

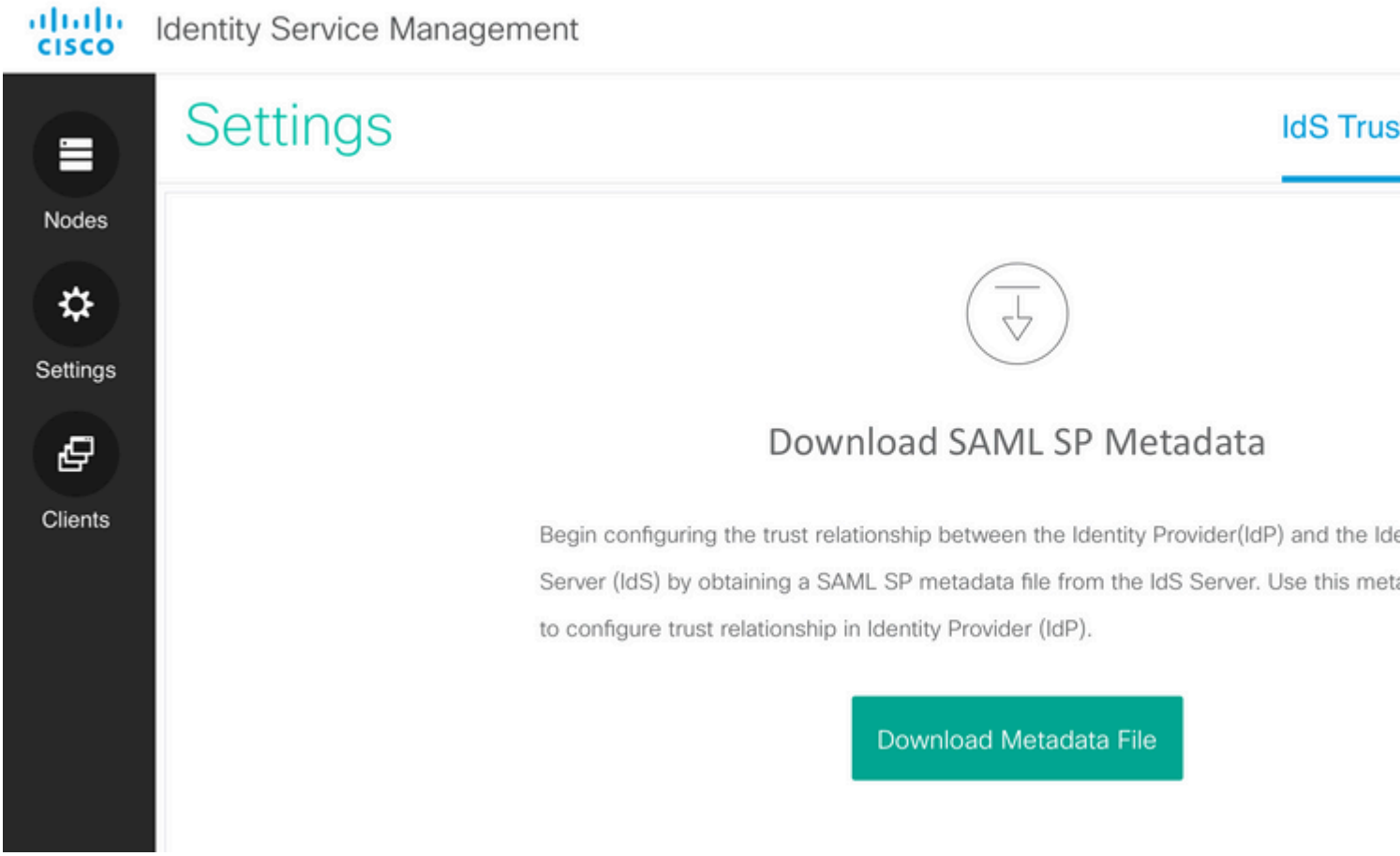
- æœ‰å…³ADFS 2.0çš„ä¿¡æ¯ï¼Œè¯·é˜…æ¤Microsoft TechNetæ–‡ç« ï¼Œ http://social.technet.microsoft.com/wiki/contents/articles/1600.ad-fs-2-0-how-to-change-the-local-authentication-type.aspxã€‚
- æœ‰å…³ADFS 3.0çš„ä¿¡æ¯ï¼Œè¯·é˜…æ¤Microsoft TechNetæ–‡ç« ï¼Œ https://learn.microsoft.com/en-us/archive/blogs/josrod/enabled-forms-based-authentication-in-adfs-3-0

æ³¨æ„:Cisco IdS 11.6å¯Šæ›´é«˜ç‰ˆæœ¬æ”¯æŒåŸºäºŽè¡¨å•çš„èº«ä»½éªŒè¯Œ

å»ºç«‹ä¿¡ä»»å…³ç³»

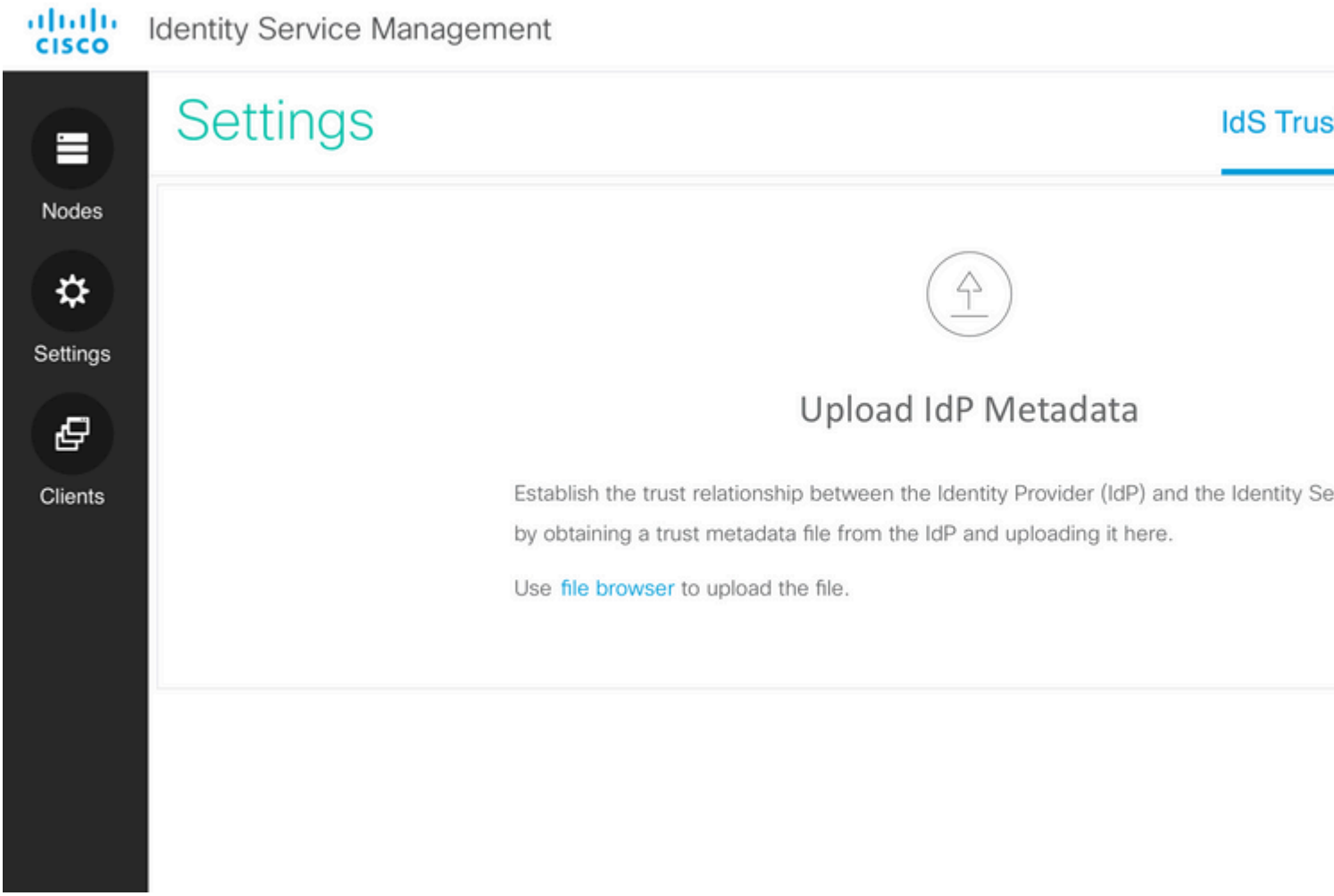
å¯¹äºŽè‡ªæ³¨å†Œï¼Œäº†ä½¿å”¯ç¨‹åº�èƒ½å¤Ÿä½¿ç”¨æ€�ç§'IDè¿›è¡ŒSSOï¼Œè¯·å¨IdSå'ŒIdPä¹‹é–

- ä¸‹è½½SAML SPå…ƒæ•°æ®æ–‡ä»¶ sp.xml.
- ä»Ž Settingsï¼Œå¯¼èˆªè‡³IdS Trust é€‰é¡¹å¡ã€‚



- ä»ŽURLçš„IdPä¸‹è½½IdPå…ƒæ•°æ®æ–‡ä»¶ï¼š https://<ADFSServer>/federationmetadata/2007-06/federationmetadata.xml

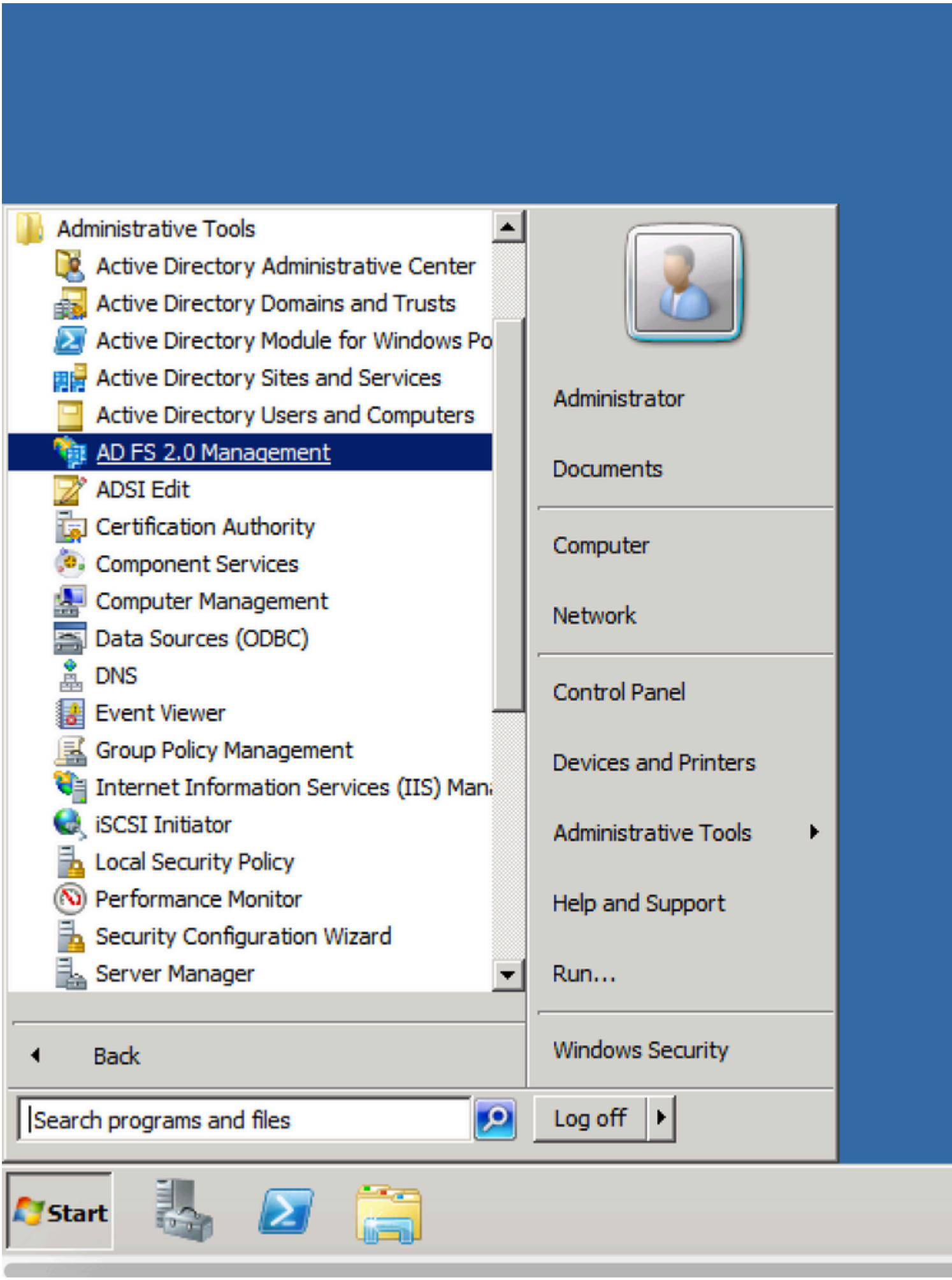
- åœ¨â€œIdSç®¡ç�†â€�(IdS Management)é¡µé�¢ä¸Šï¼Œä¸ä¼ €æ¥ä¸‹è½½çš„IdPå…ƒæ•°æ®æ–‡ä»¶ã€‚

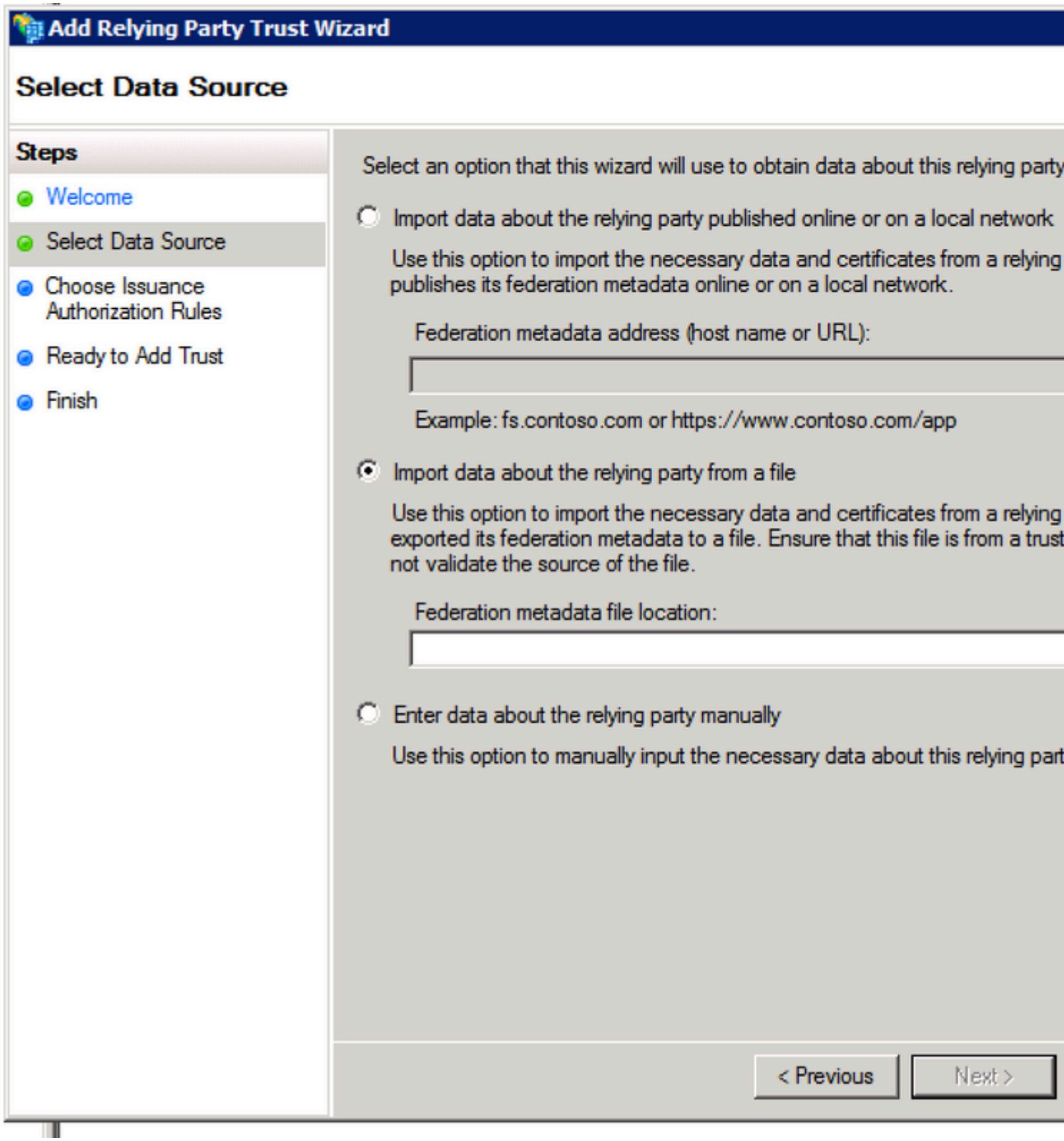


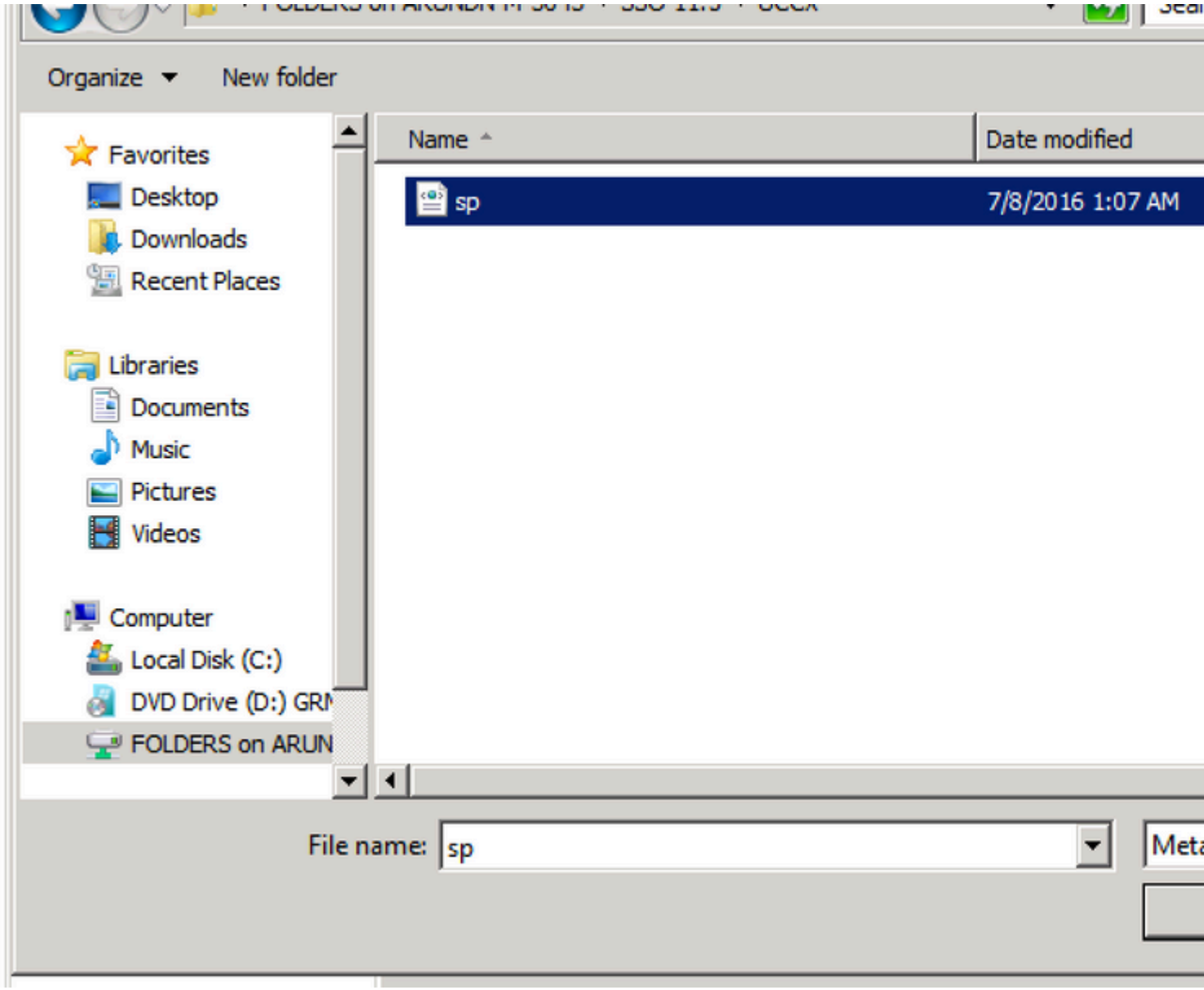
è¿™æ˜¯ä¸Šä¼ IdSå…ƒæ•°æ®åŒ…å£°æ˜Žæ–‡ä»¶çš„è¿‡ç¨‹ã€‚è¿™åœ¨ADFS 2.0å’Œ3.0ä¸è¿›è¡Œä¹Ÿæ¯”è¾ƒç›¸ä¼¼ã€‚

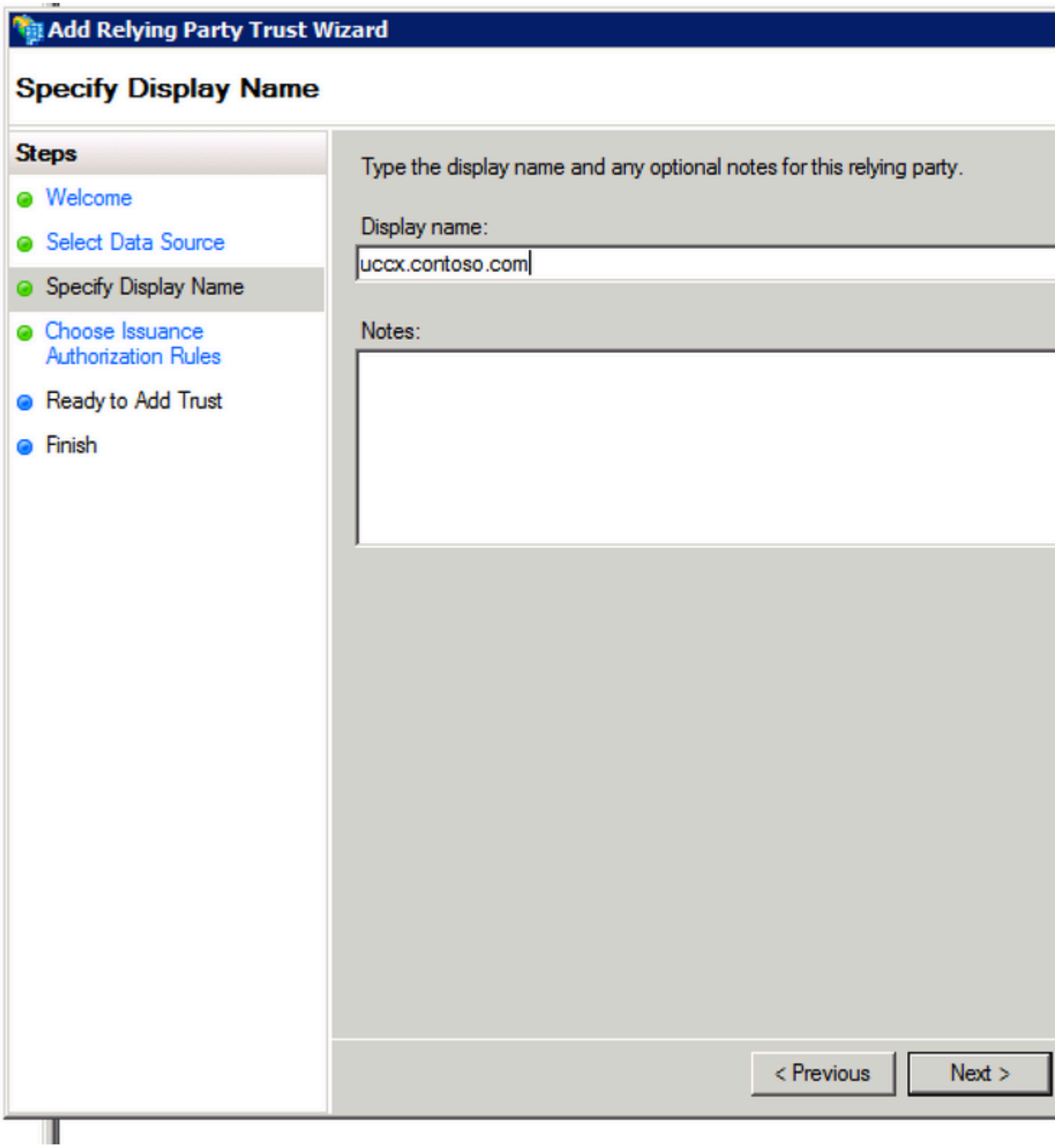
ADFS 2.0

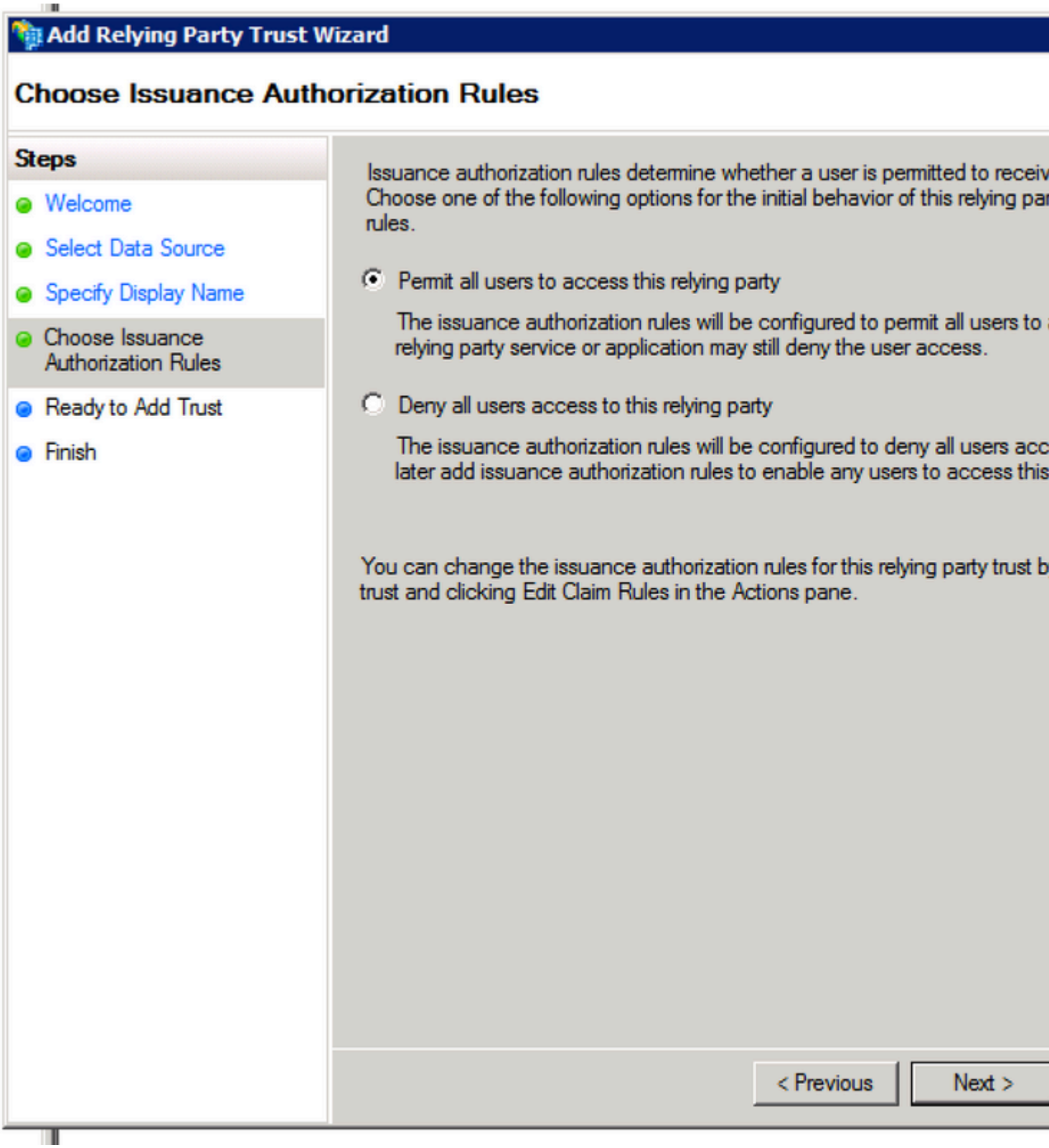
æ¥éª¤1:åœ¨ADFSæœ�åŠ¡â™¨ä¸ï¼Œå¯¼èˆªåˆ°ï¼Œ Start > All Programs > Administrative Tools > ADFS 2.0 Management,å¦‚å›¾æ‰€çº³:


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

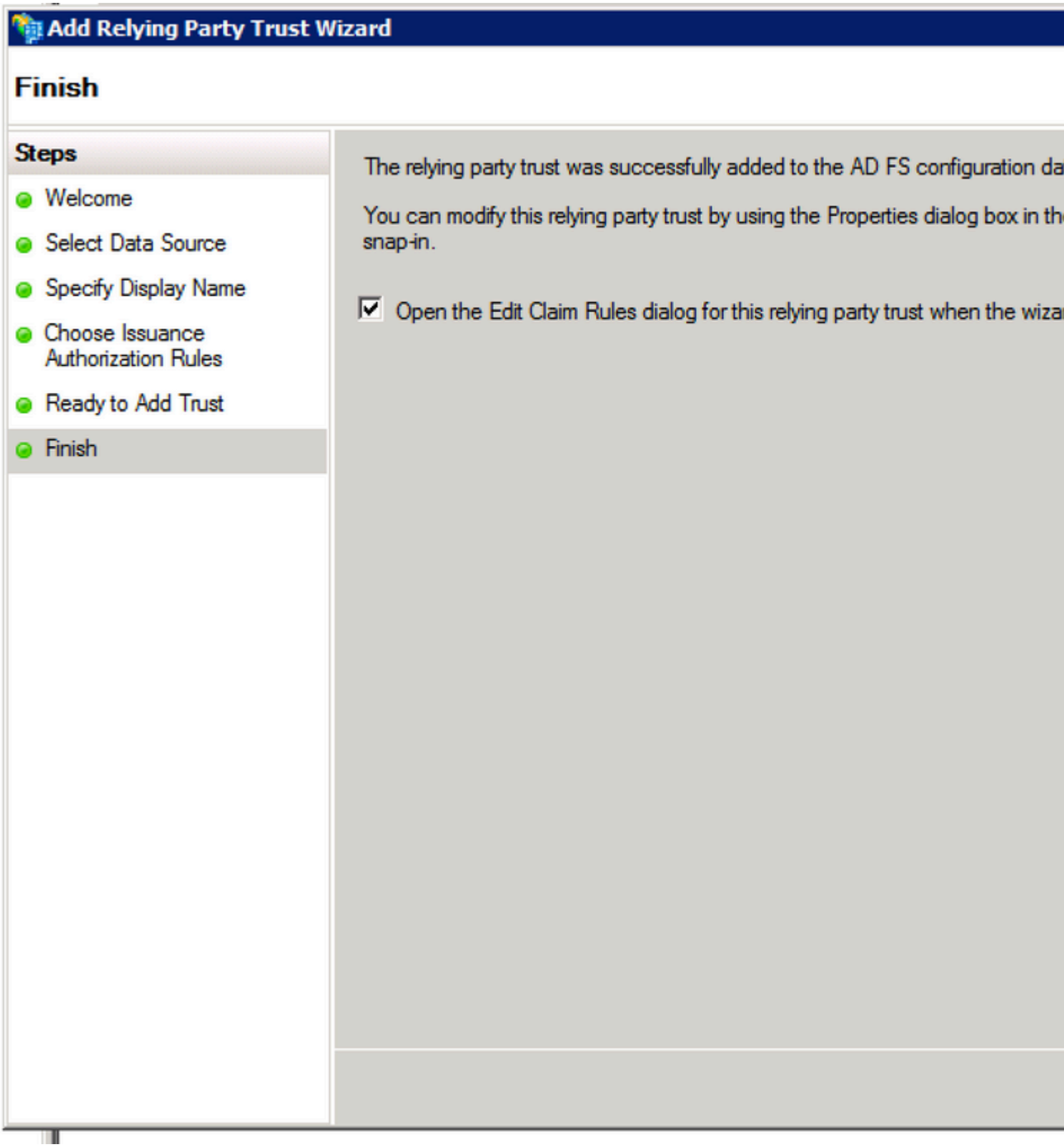

Add Relying Party Trust Wizard
Select Data Source
Steps
Welcome
Select Data Source
Choose Issuance Authorization Rules
Ready to Add Trust
Finish
Select an option that this wizard will use to obtain data about this relying party
Import data about the relying party published online or on a local network
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

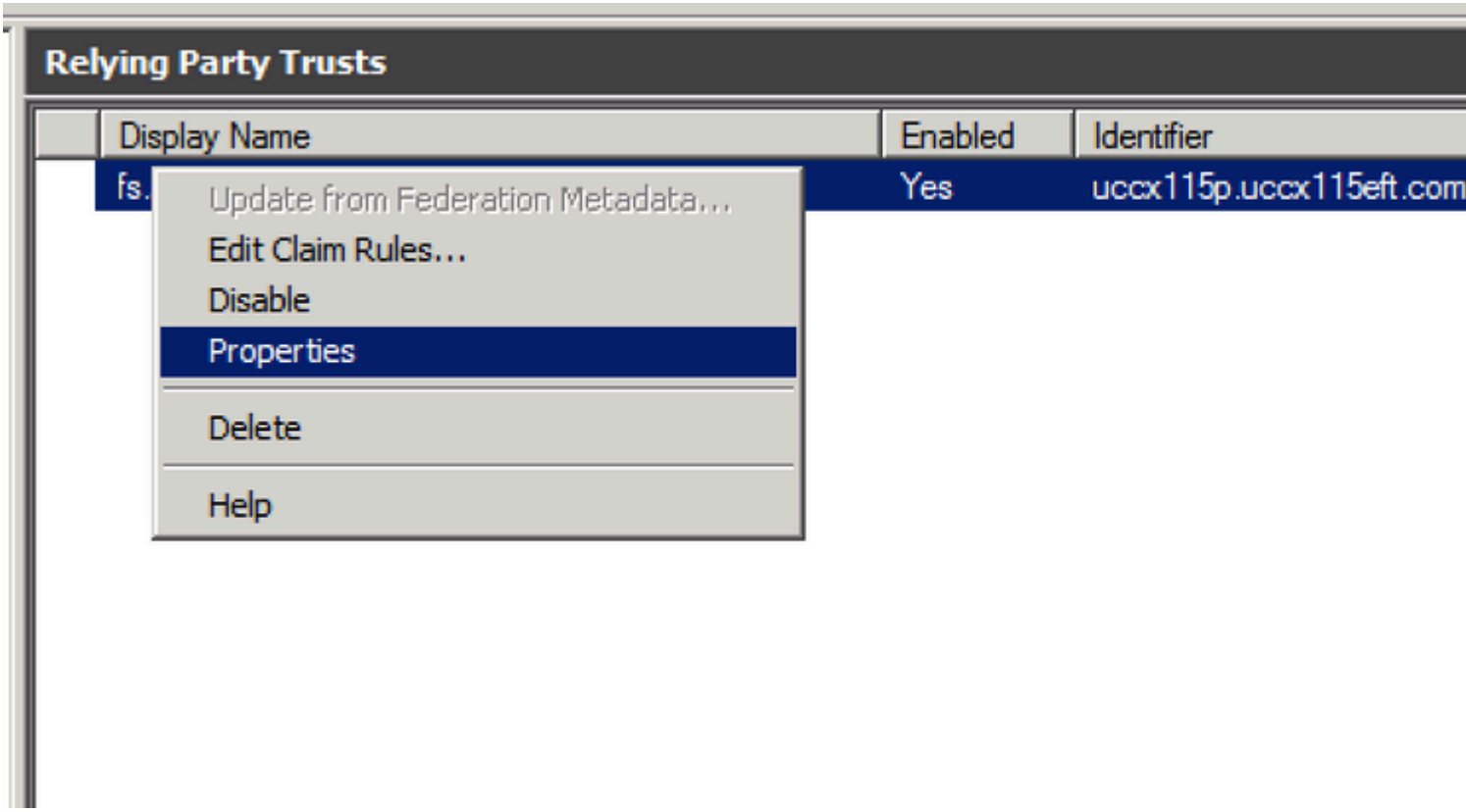

Add Relying Party Trust Wizard
Specify Display Name
Steps
Welcome
Select Data Source
Specify Display Name
Choose Issuance Authorization Rules
Ready to Add Trust
Finish
Type the display name and any optional notes for this relying party.
Display name:
uccx.contoso.com
Notes:
< Previous
Next >

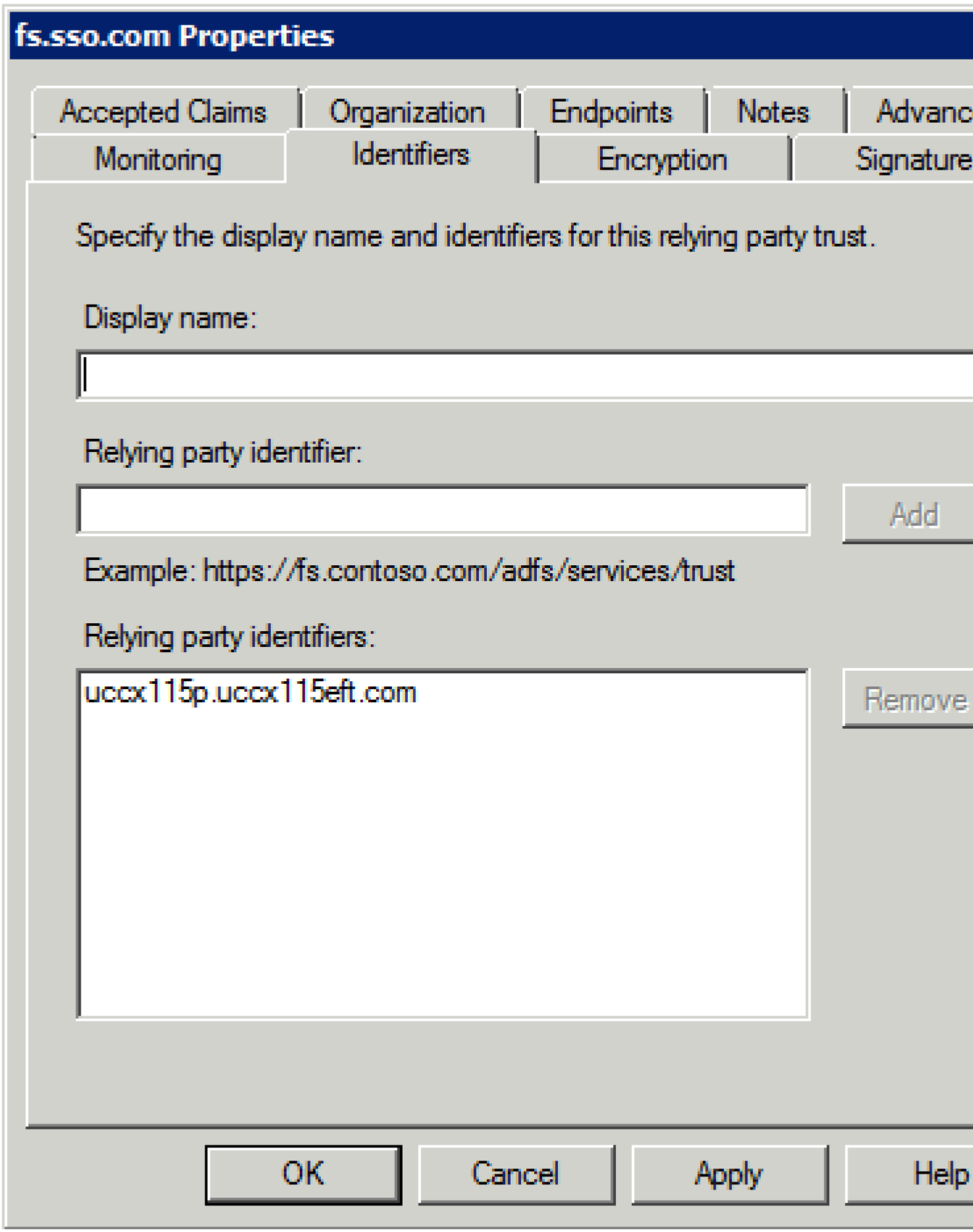


ç¬¬å››æ¥¼šå®Œæˆ�ä¿¡èµ–æ–¹ä¿¡ä»»çš„å»ºç«‹ã€‚



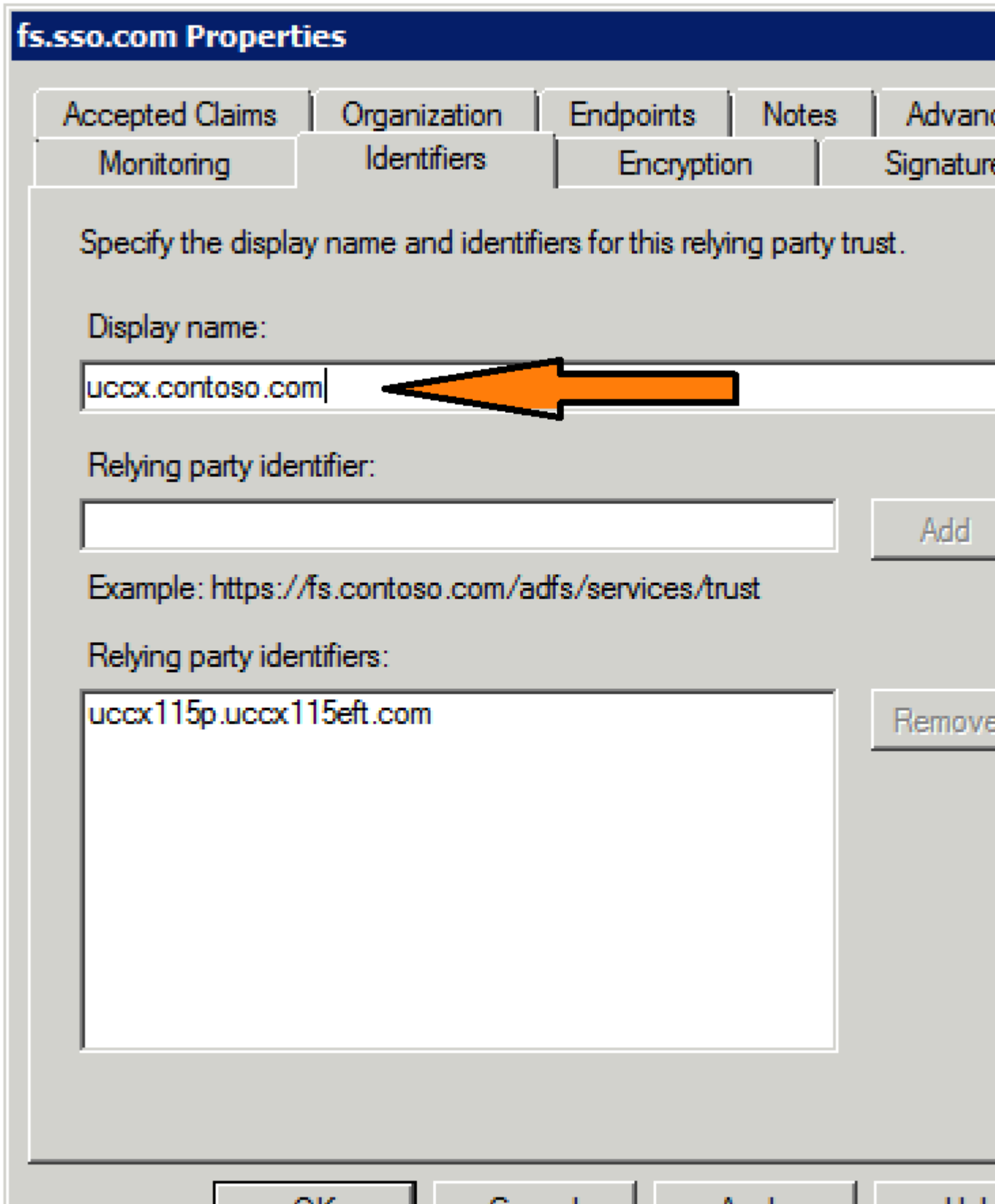
ç¬¬äº”æ¥ï¼šåœ¨ä¿¡èµæ–¹ä¿¡ä»»çš„å±žæ€§ä¸ŒéŒ€‰æ‹© Identifier é€‰é¡¹å�¡ã€‚


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



ç¬¬å…æ¥ï¼šå°†æ ‡è¯†ç¬¦è®¾ç½®ä¸ºCisco Identity

Serverçš„å®Œå…¨é™�å®šä¸»æœºå��ï¼ŒCisco Identity Serverå¯¯ä»Žå…¶èŽ·å¾—
sp.xml å·²ä¸‹è½½ã€‚


fs.sso.com Properties
Accepted Claims
Organization
Endpoints
Notes
Monitoring
Identifiers
Encryption
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:
uccx115p.uccx115eft.com
OK
Cancel
Apply

æ¥é¹¤

7.åé"®å•å‡»â€œä¿¡èµ–æ–¹ä¿¡ä»»â€ï¼Œ¶åŽå•å‡» Edit Claim Rules.

å¿…é¡»æ·»åŠ ä¸¤ä¸ªå£°æ˜Žè§„å™™ï¼Œä¸€ä¸ªæ˜¯åŒ¹é…LDAPï¼ˆè½»é‡ç§ç›®å½•è®¿é—®åè®®ï¼‰

uid â€" å°"ç"¨ç¨‹å°éœ€è¦æ¤å±žæ€§ä¥æ ‡è¯†ç»è¿‡è°«ä»½éªŒè¯çš„ç"¨æˆ·ã€‚
user_principal - Cisco
IDéœ€è¦æ¤å±žæ€§ä¥æ ‡è¯†ç»è¿‡è°«ä»½éªŒè¯çš„ç"¨æˆ·çš„é¢†åŸŸã€‚

é¢†æ¬¾ç"³è¯·è§„å™™1:

æŒ‰åç§°æ·»åŠ è§„å™™ NameID ç±»åž‹ï¼šå°†LDAPå±žæ€§çš„å€¼ä½œä¸ºå£°æ˜Žå'é€ï¼‰ï¼š

- é€‰æ‹©å±žæ€§å˜å,¨ä½œä¸ºActive Directory
- æ˜ å°„LDAPå±žæ€§ User-Principal-Name å˚ user_principal ï¼ˆå°å†™ï¼‰
- é€‰æ‹©å¿…é¡»ç"¨ä½œ userId ä»¥ä¾¿ç™»å½•å¹¶å°†å…¶æ˜ å„„å˚ uid ï¼ˆå°å†™ï¼‰

é…ç½®ç¤ºä¾‹ SamAccountName å°†ç"¨ä½œç"¨æˆ·ID:

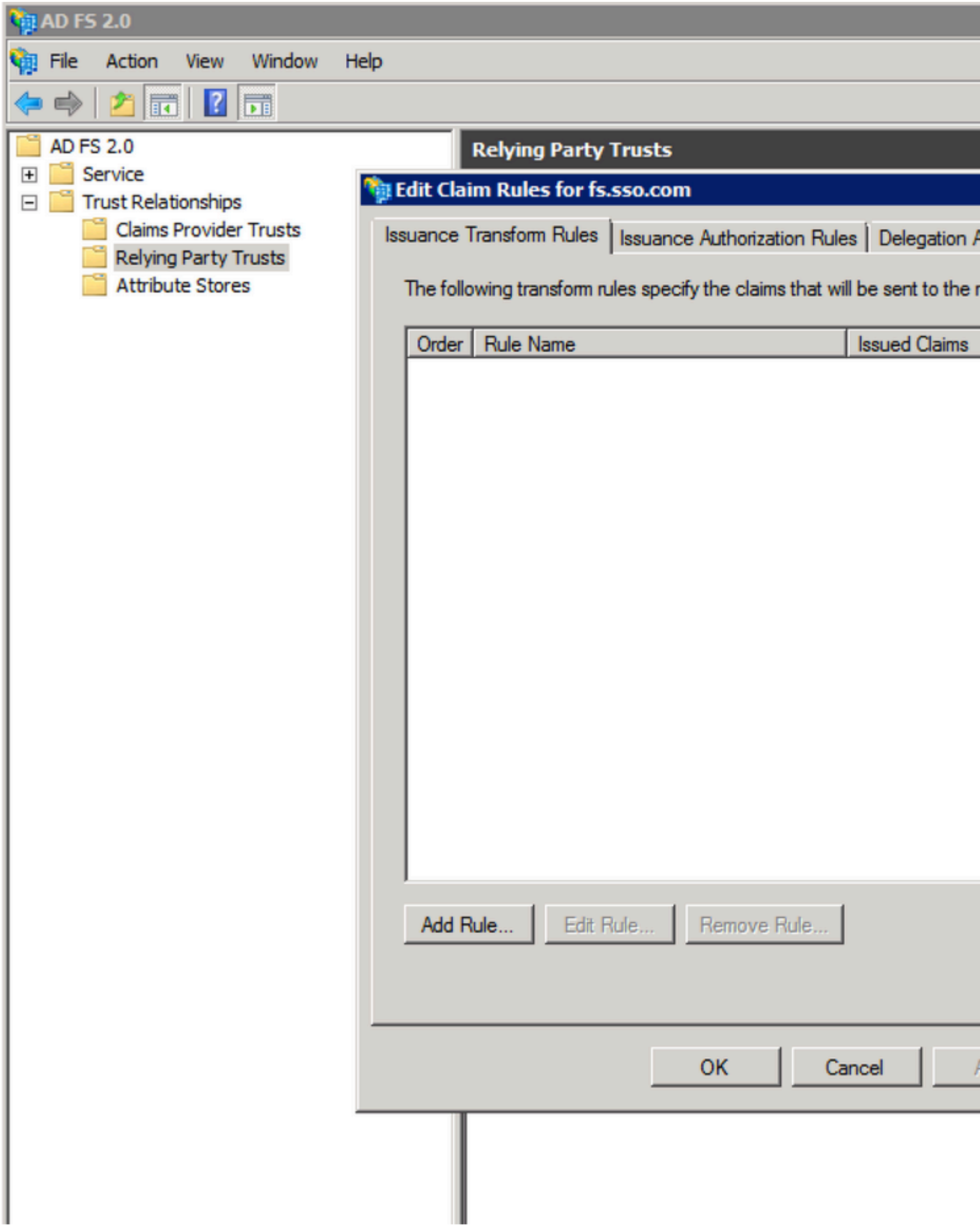
- æ˜ å°„LDAPå±žæ€§ SamAccountName å˚ uid.
- æ˜ å°„LDAPå±žæ€§ User-Principal-Name å˚ user_principal.

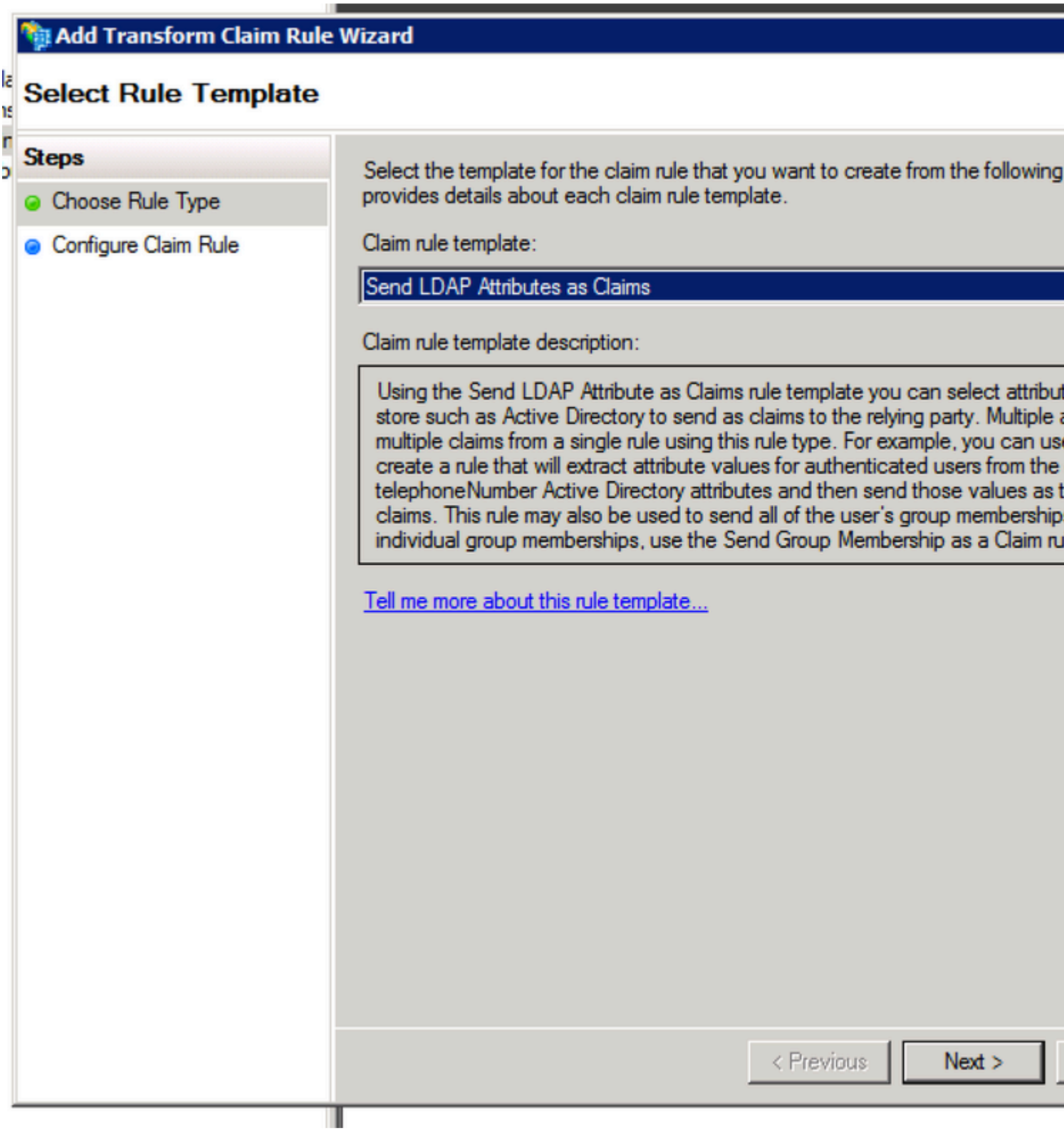
é…ç½®ç¤ºä¾‹ UPN å¿…é¡»ç"¨ä½œç"¨æˆ·ID:

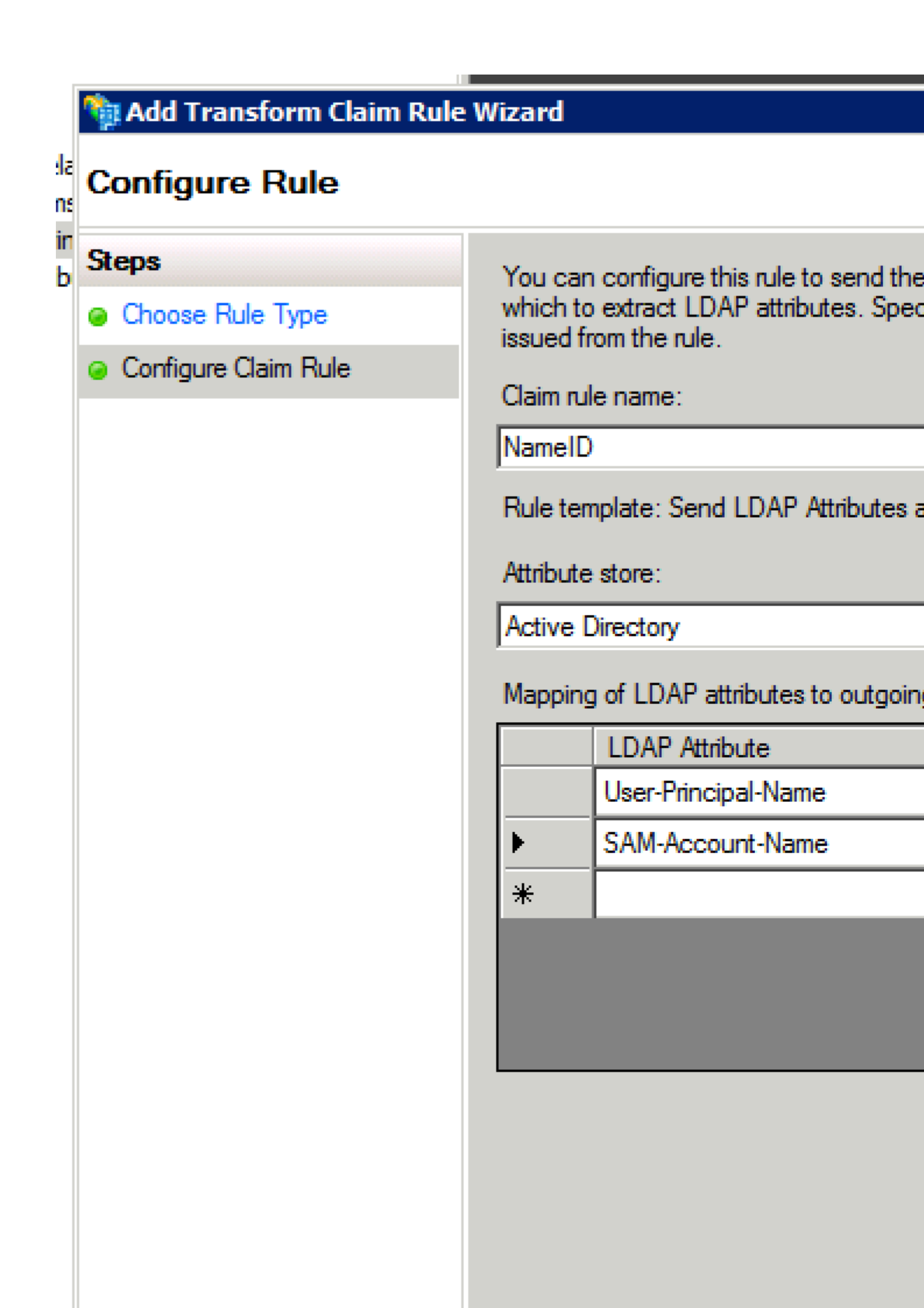
- æ˜ å°„LDAPå±žæ€§ User-Principal-Name å˚ uid.
- æ˜ å°„LDAPå±žæ€§ User-Principal-Name å˚ user_principal.

é…ç½®ç¤ºä¾‹ PhoneNumber å¿…é¡»ç"¨ä½œç"¨æˆ·ID:

- å°†LDAPå±žæ€§**telephoneNumber**æ˜ å°„å˚ uid .
- æ˜ å°„LDAPå±žæ€§ User-Principal-Name å˚ 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

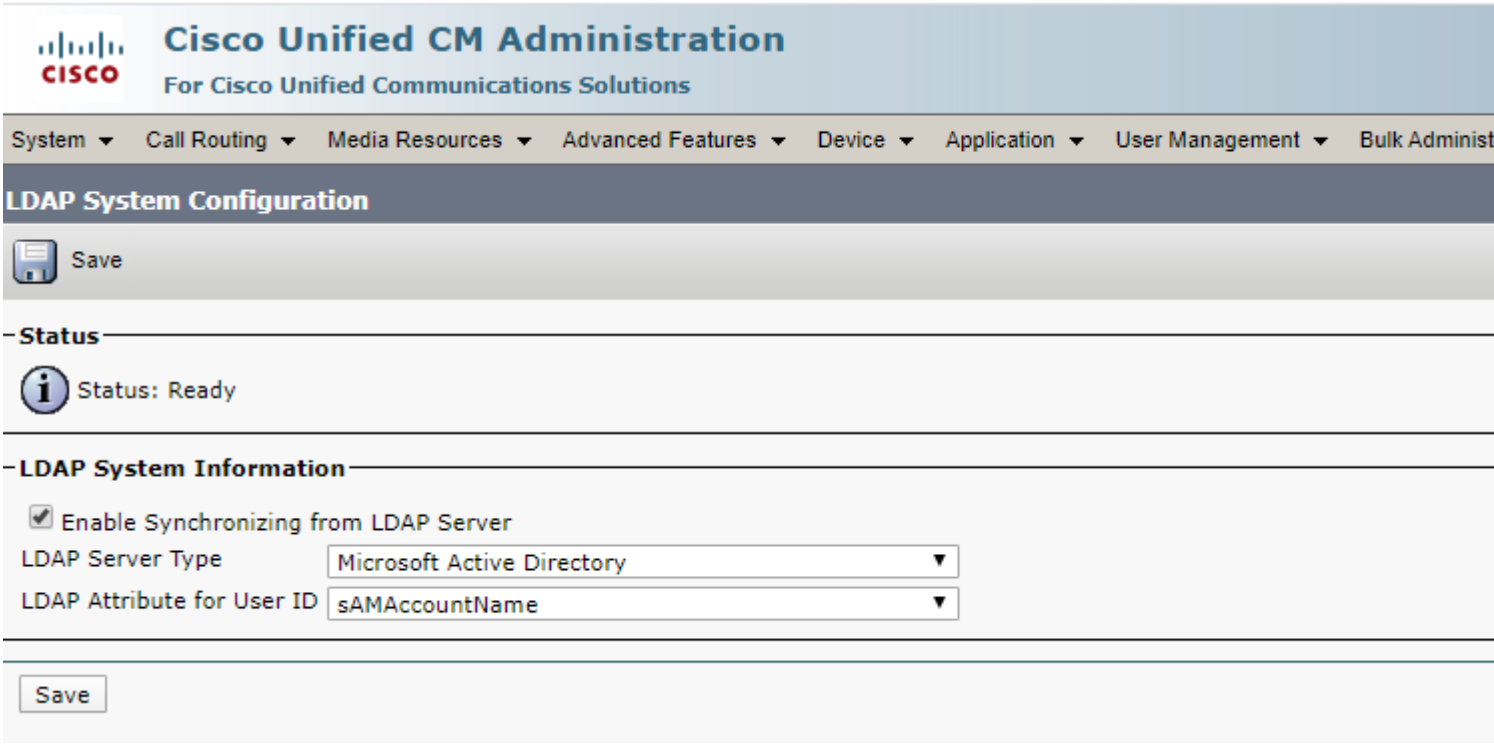

Add Transform Claim Rule Wizard
Select Rule Template
Steps
Choose Rule Type
Configure Claim Rule
Select the template for the claim rule that you want to create from the following
provides details about each claim rule template.
Claim rule template:
Send LDAP Attributes as Claims
Claim rule template description:
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¿½ä¸ºCUCM LDAPå¿Œæ¥ä¸Šçš„ç”¨æˆ·IDé…ï¿½ç½®çš„LDAPå±žæ€§ä¸Žé…ï¿½ç½®ä¸ºLDAPå±žæ€§çš„ uid åœ¨ADFSå£°æ˜Žè§„åˆ™ä¸ NameID.è¿™æ˜¯ä¸ºäº†ä½¿CUICå'ŒFinesseç™»å½•æ£å¸¸å·¥ä½œã€,

---

æ³¨æ„„ï¼šæœ¬æ–‡æ¡£å£°ç¨°å£°æ˜Žè§„åˆ™å••ç§°çš„é™¤åˆ¶æ¡ä»¶ï¼Œå¹¶ä¾ç¾¤ç»„ã

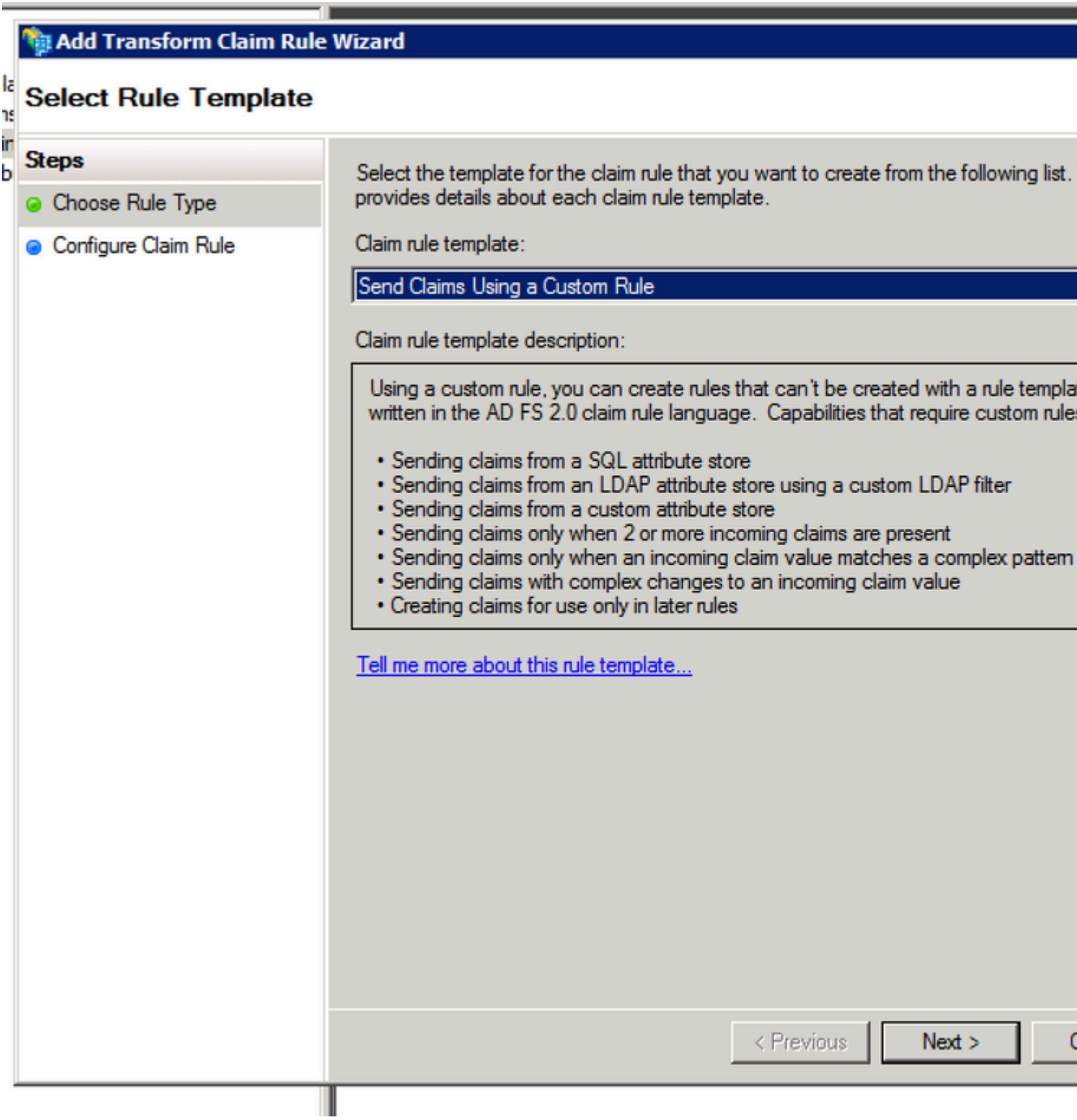


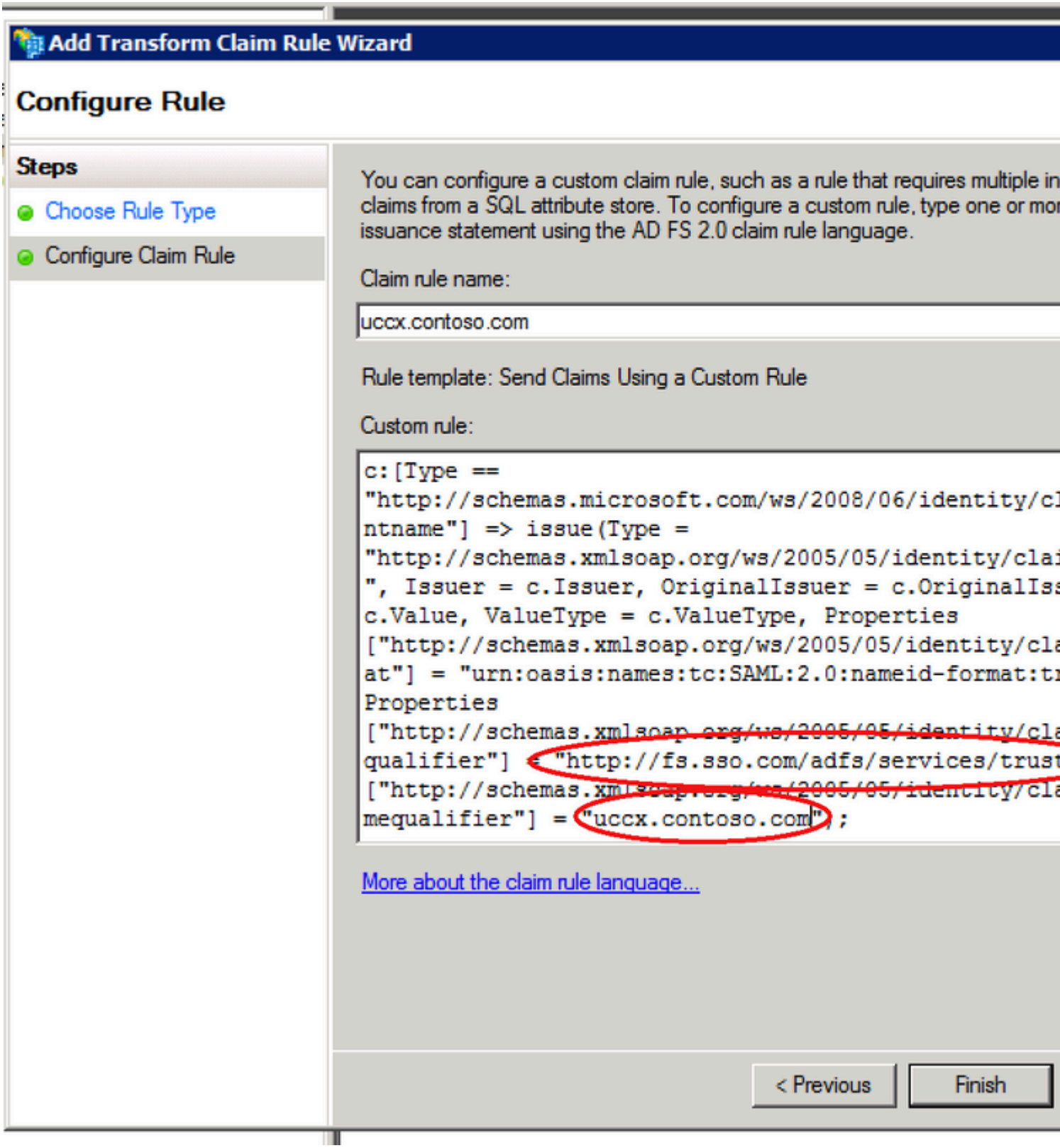
é¢†æ¬¾ç”³è¯·è§„åˆ™2:

- æ·»åŠ å¦¦ä¸€ä¸ªè‡ªå®šä¹‰å£°æ˜Žè§„åˆ™ç±»åž‹çš„è§„åˆ™ï¼Œè¯¥è§„åˆ™ç„¶å••ç§°Cisco Identity Serverçš„å®Œå…¨é™®å®šä¾›æœºå••ï¼Œå¹¶æ·»åŠ æ¤è§„åˆ™æ–‡æœ¬ã€,

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

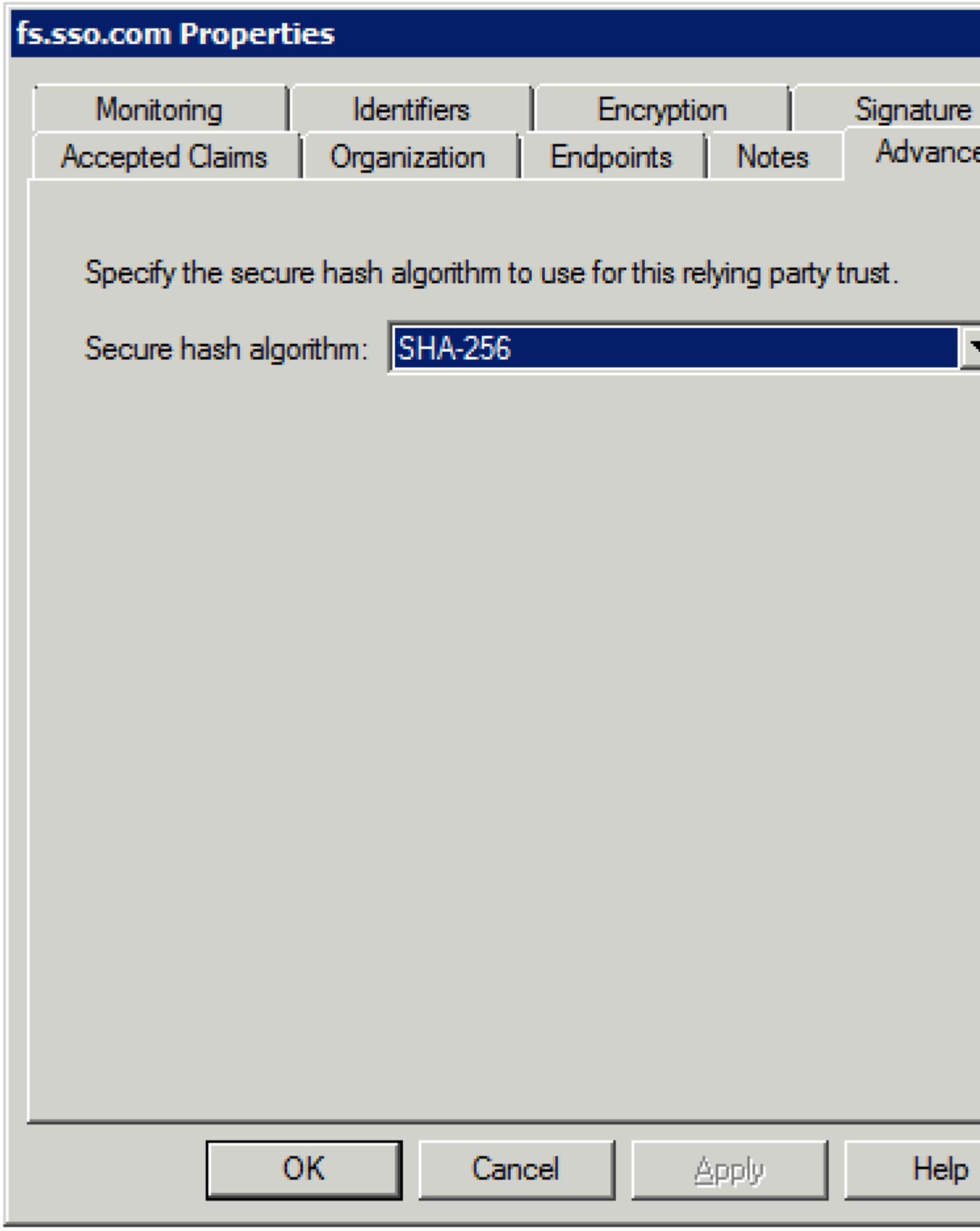
- åœ¨æ€ç§‘è°«ä»½æœ€åŽä¡å™¨é›¤ä¸ï¼Œæ‰€æœ‰å®Œå…¨é™®å®šä¾›æœºå••éƒ½æ˜¯
- <Fully qualified hostname of Cisco Identity Server>åŒºåˆ†å¤§å°•å†™ï¼Œæ¤å®ƒä¸Cisco Identity Server FQDNå®Œå…¨åŒ¹é…ï¼ˆåŒ…æ‹¬å¤§å°•å†™ï¼‰ã€,
- <ADFS Server FQDN>åŒºåˆ†å¤§å°•å†™ï¼Œæ¤å®ƒä¸ADFS FQDNå®Œå…¨åŒ¹é…ï¼ˆåŒ…æ‹¬å¤§å°•å†™ï¼‰ã€,


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 >

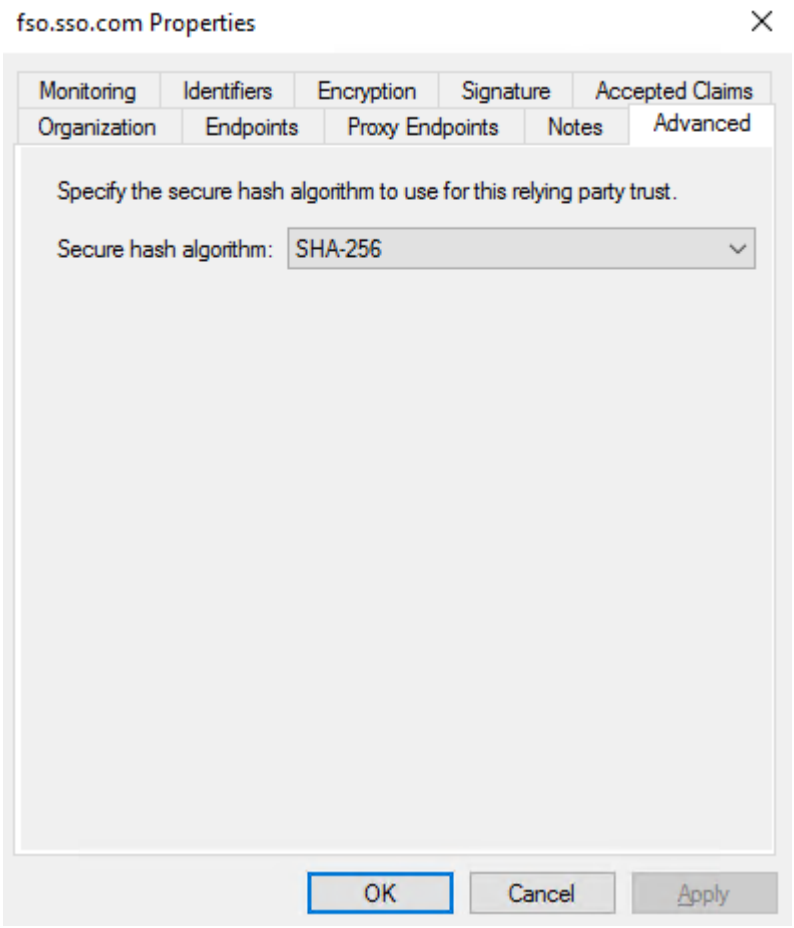


æ¥é³¤

8å€³é”®å€•å‡»â€œä¿¡èµ–æ–¹ä¿¡ä»»â€€ï¼Œç„¶å€Žå€•å‡» Properties å¹¶é€‰æ‹©â€œé«˜çº§â€€é€‰é¡¹


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

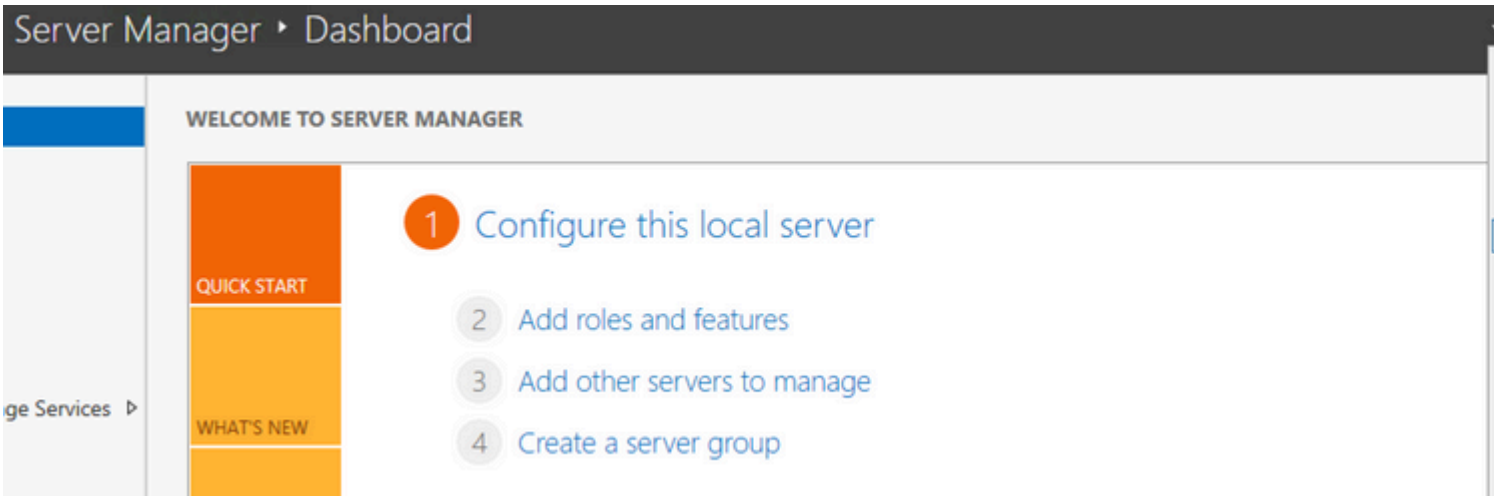
æ¥éª¤ 9å¦‚å›¾æ‰€ç¤ºï¼Œé€‰æ‹©Secure Hash Algorithm(SHA)ä½œä¸ºSHA-256ã€‚



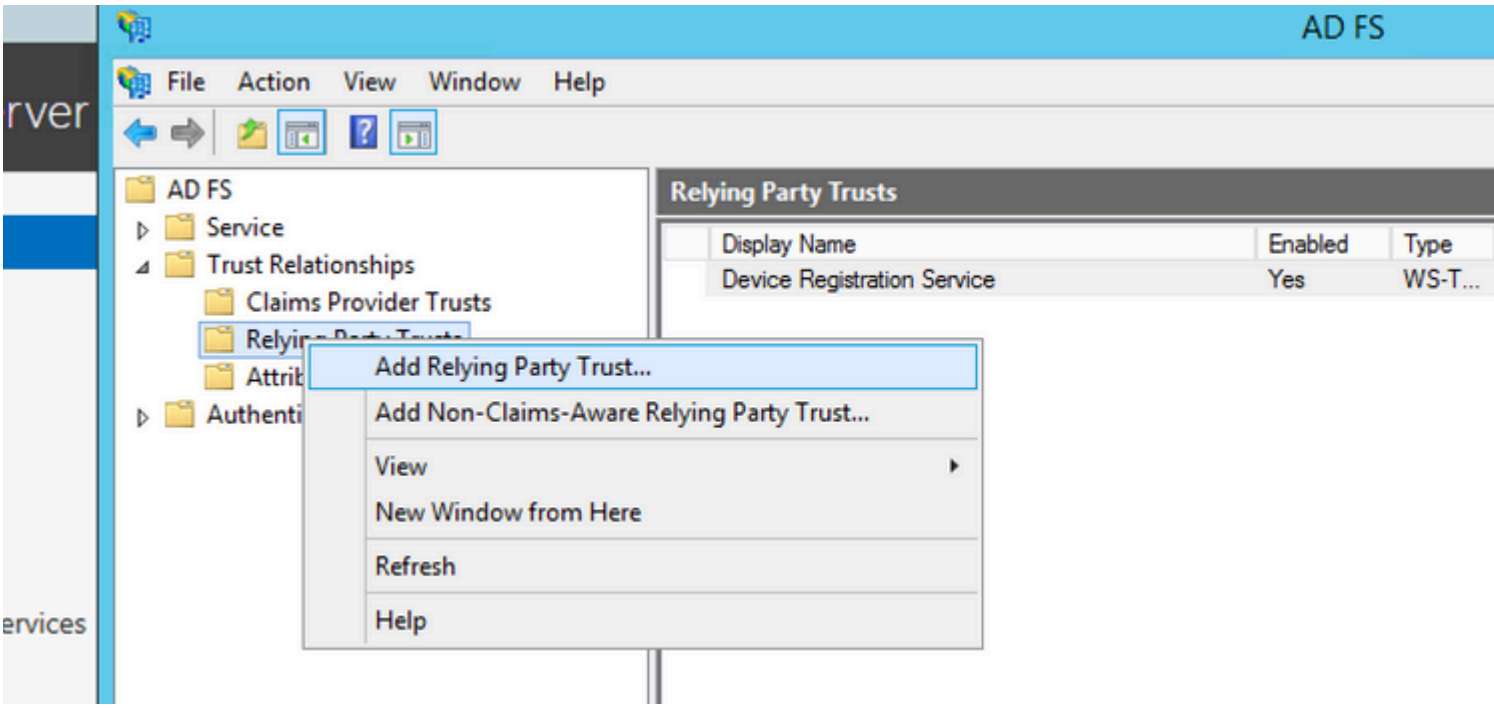
æ¥éª¤ 10ç‚¹å‡» OK.

ADFS 3.0

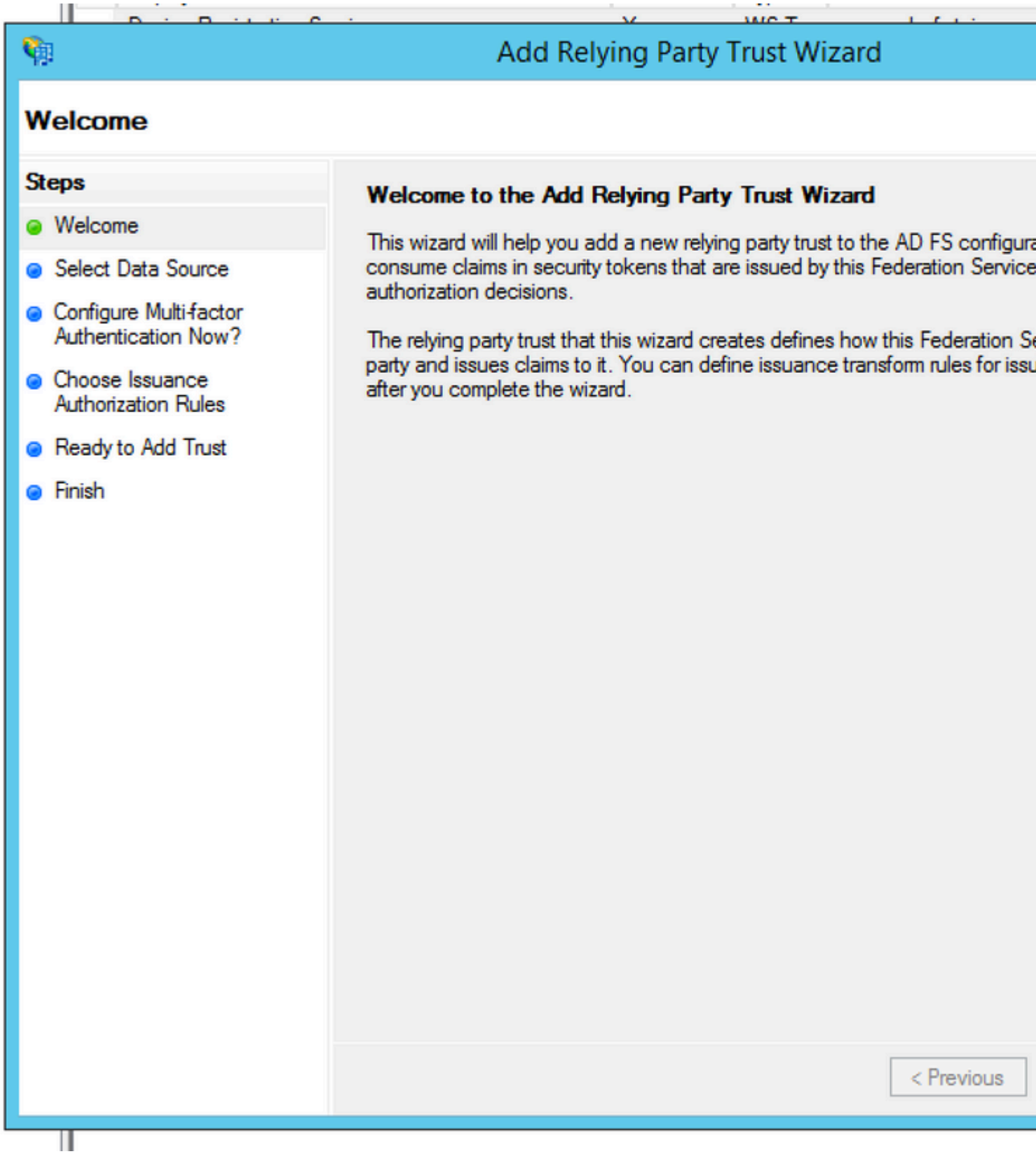
æ¥éª¤1:åœ¨ADFSæœ€åŠ¡å™¨ä¸Œå¯¼èˆªè‡³ Server Manager > Tools > ADFS Management.

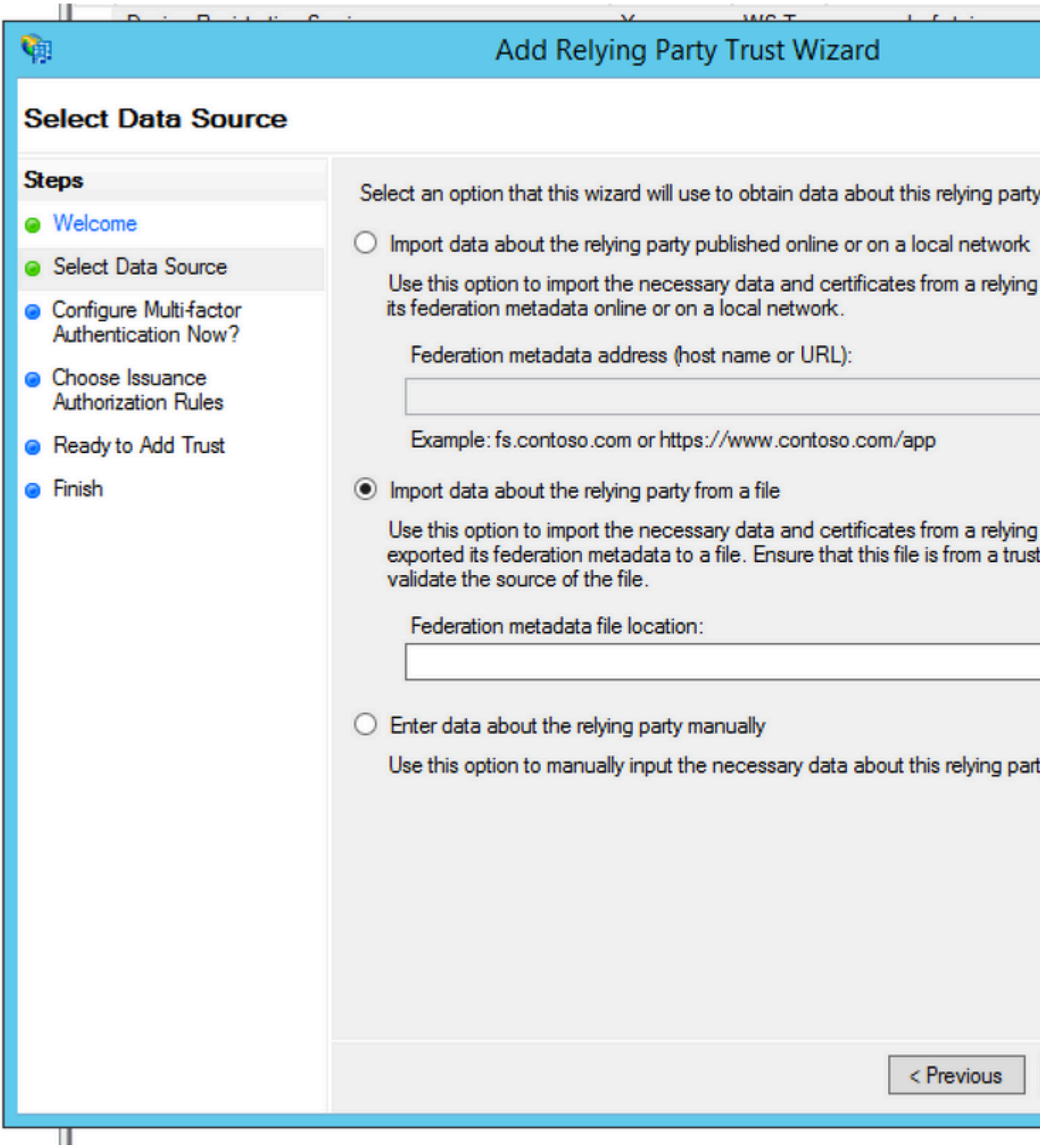


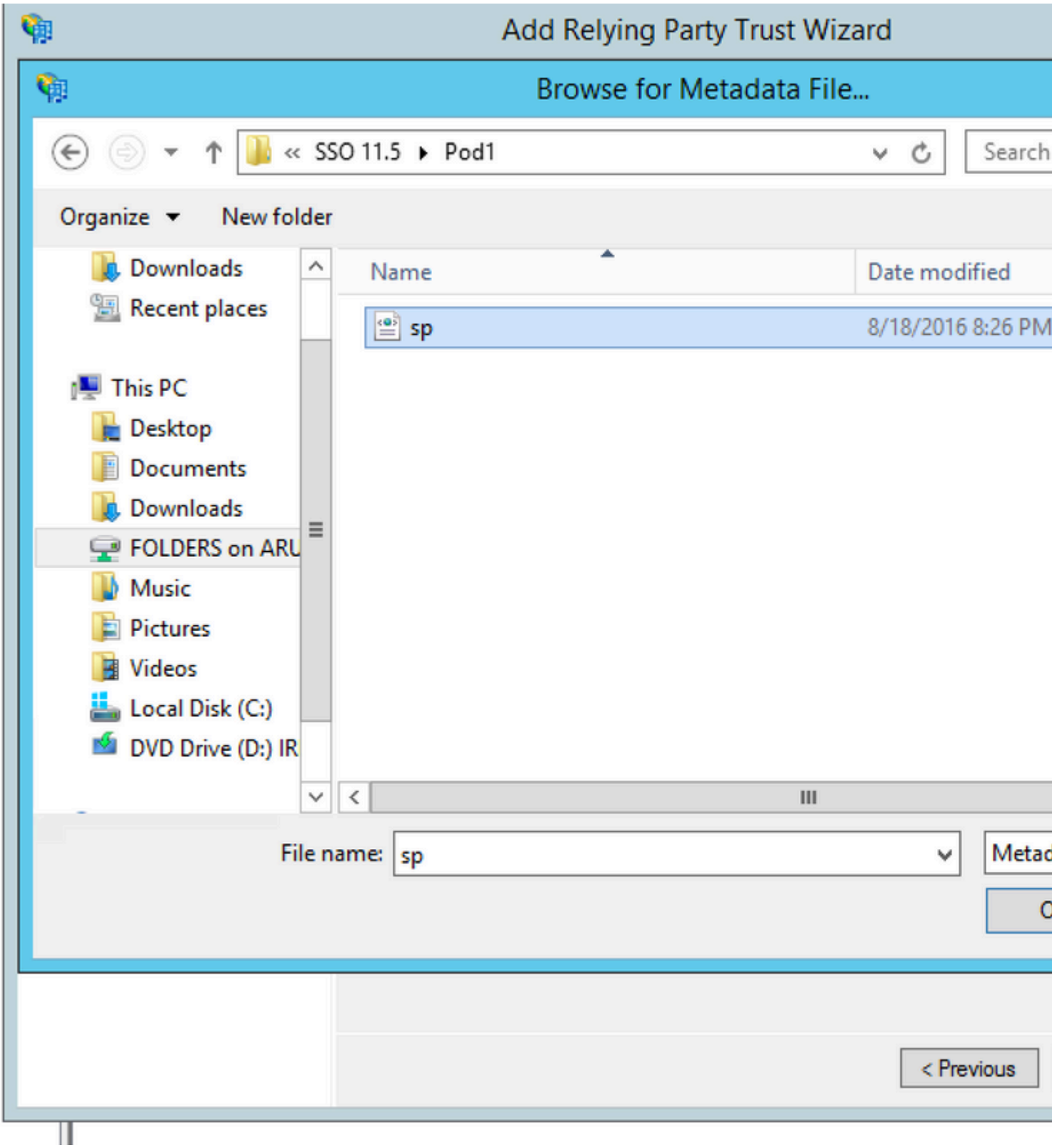
ç¬¬äºŒæ¥ï¼šå¯¼èˆªè‡³ ADFS > Trust Relationship > Relying Party Trust.

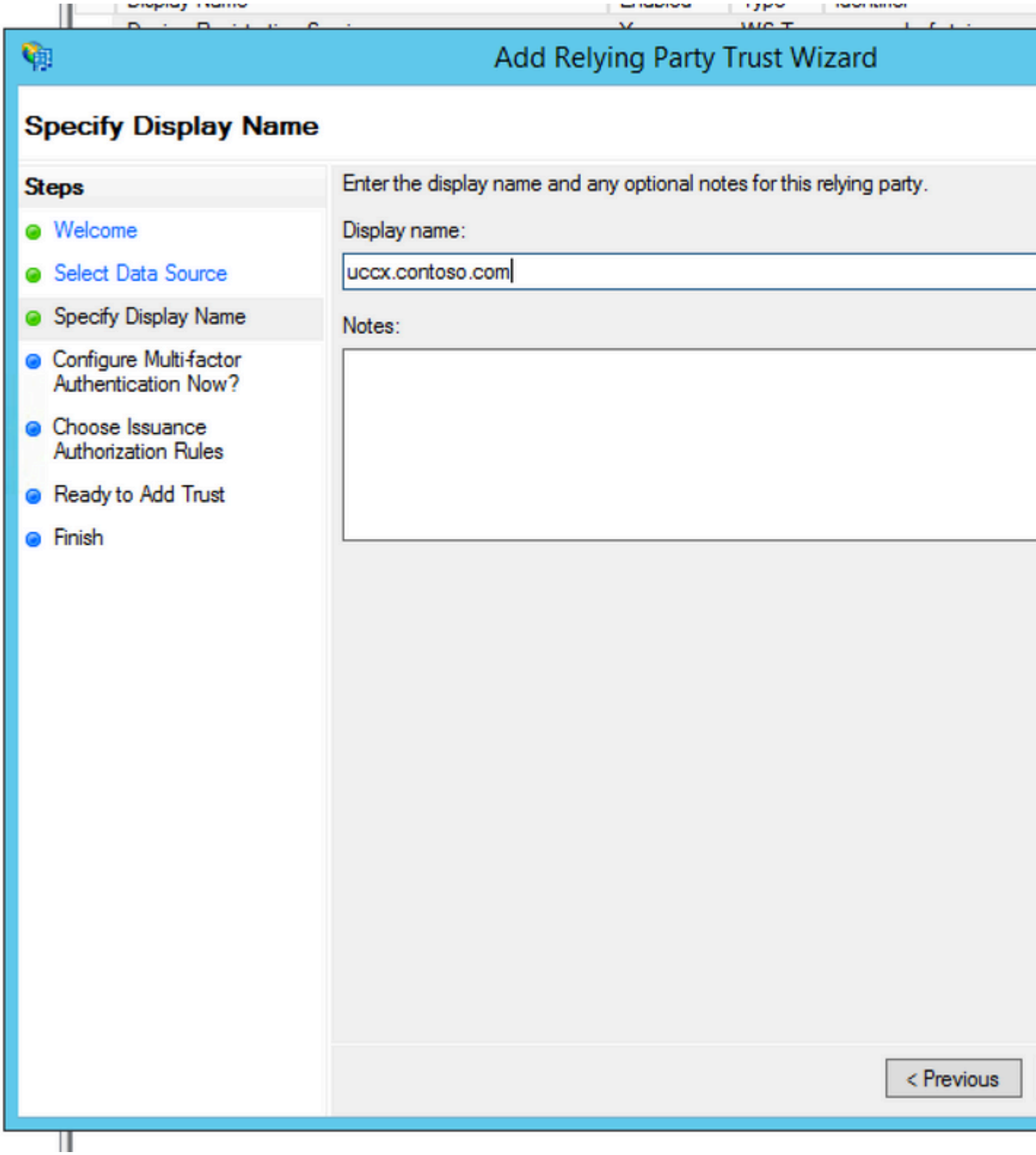


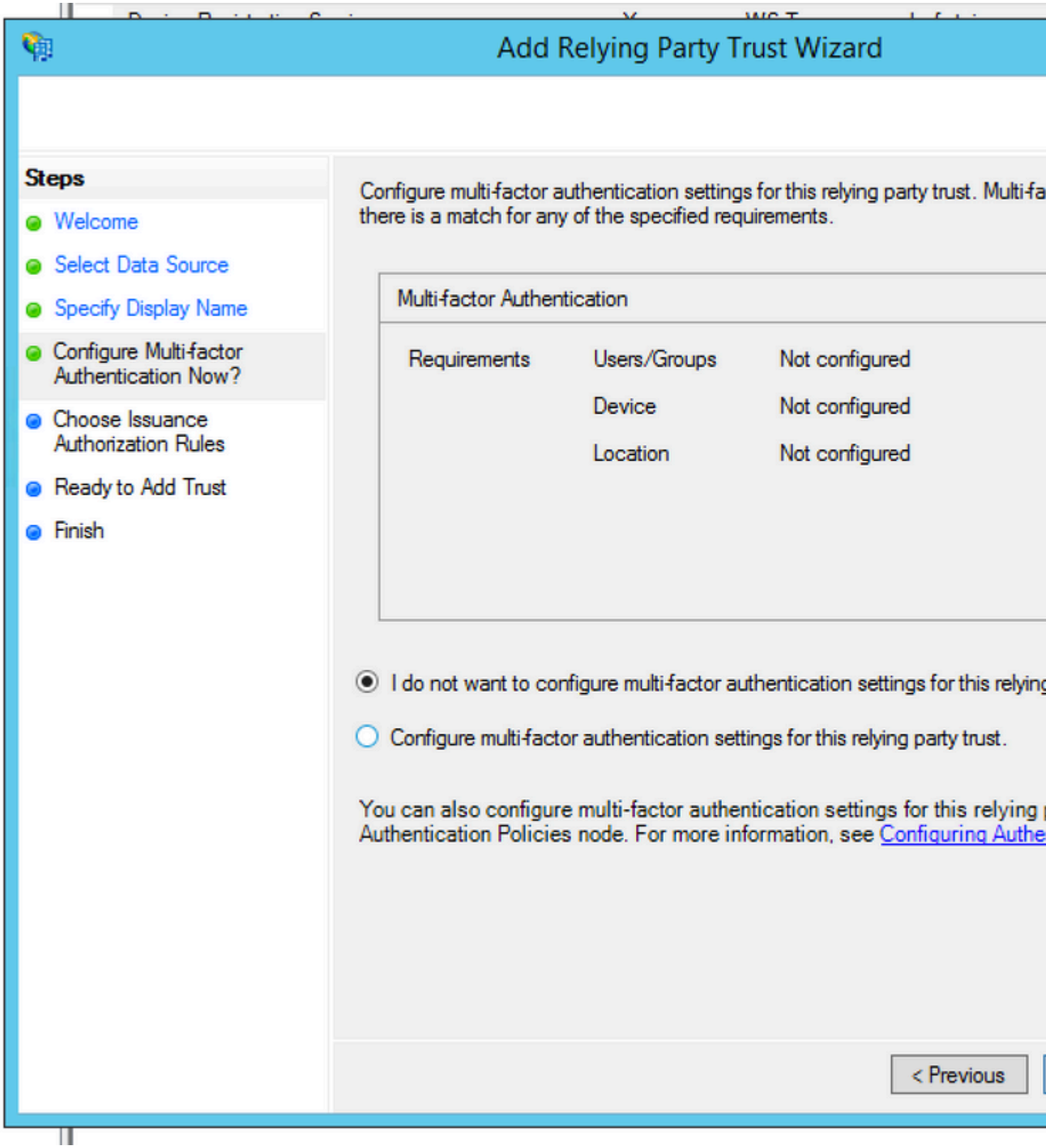
ç¬¬ä¸‰æ¥¼šé€‰æ‹©é€‰é¡¹ Import data about the relying party from a file.

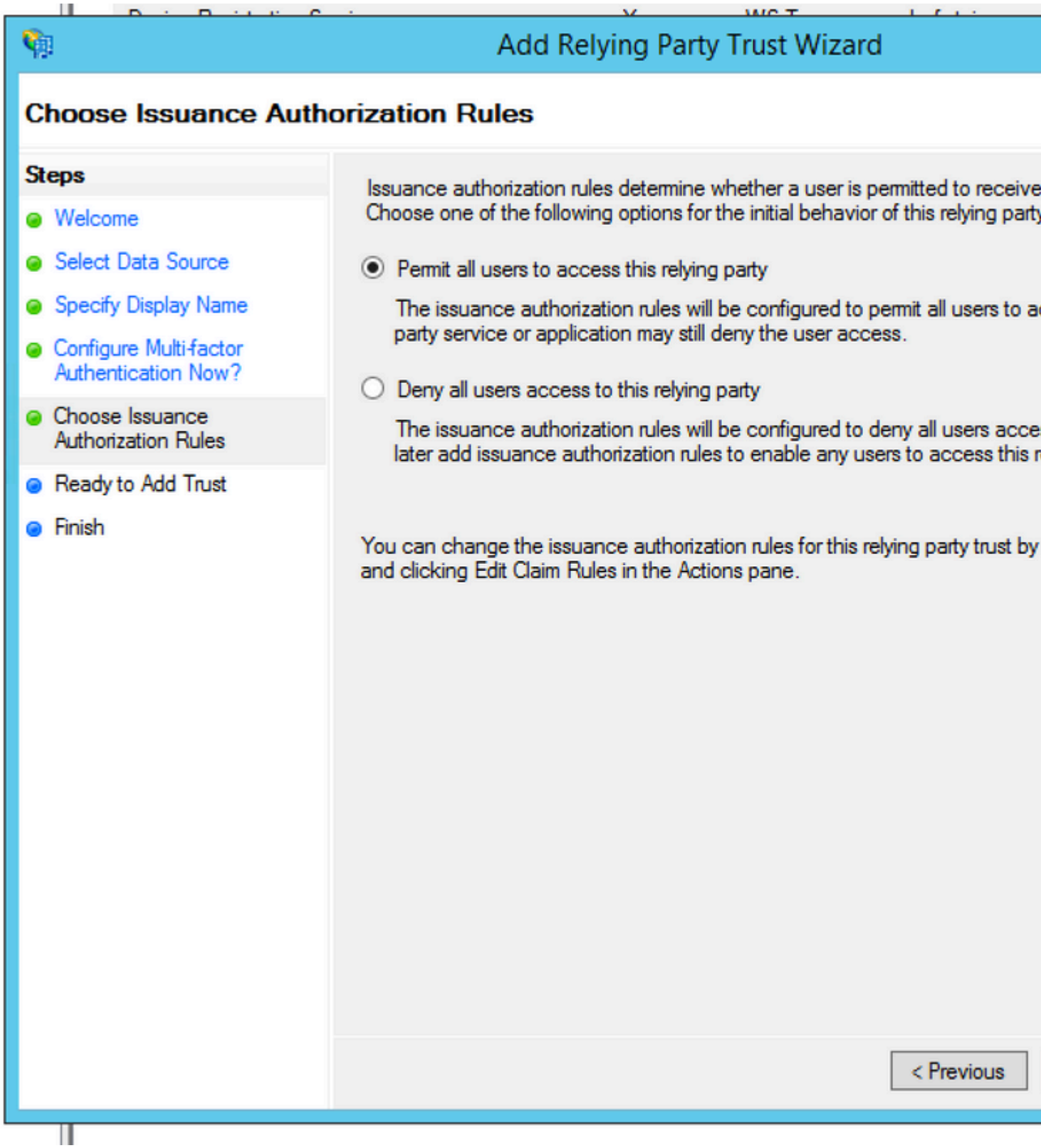

Add Relying Party Trust Wizard
Welcome
Steps
Welcome
Select Data Source
Configure Multi-factor Authentication Now?
Choose Issuance Authorization Rules
Ready to Add Trust
Finish
Welcome to the Add Relying Party Trust Wizard
This wizard will help you add a new relying party trust to the AD FS configura
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

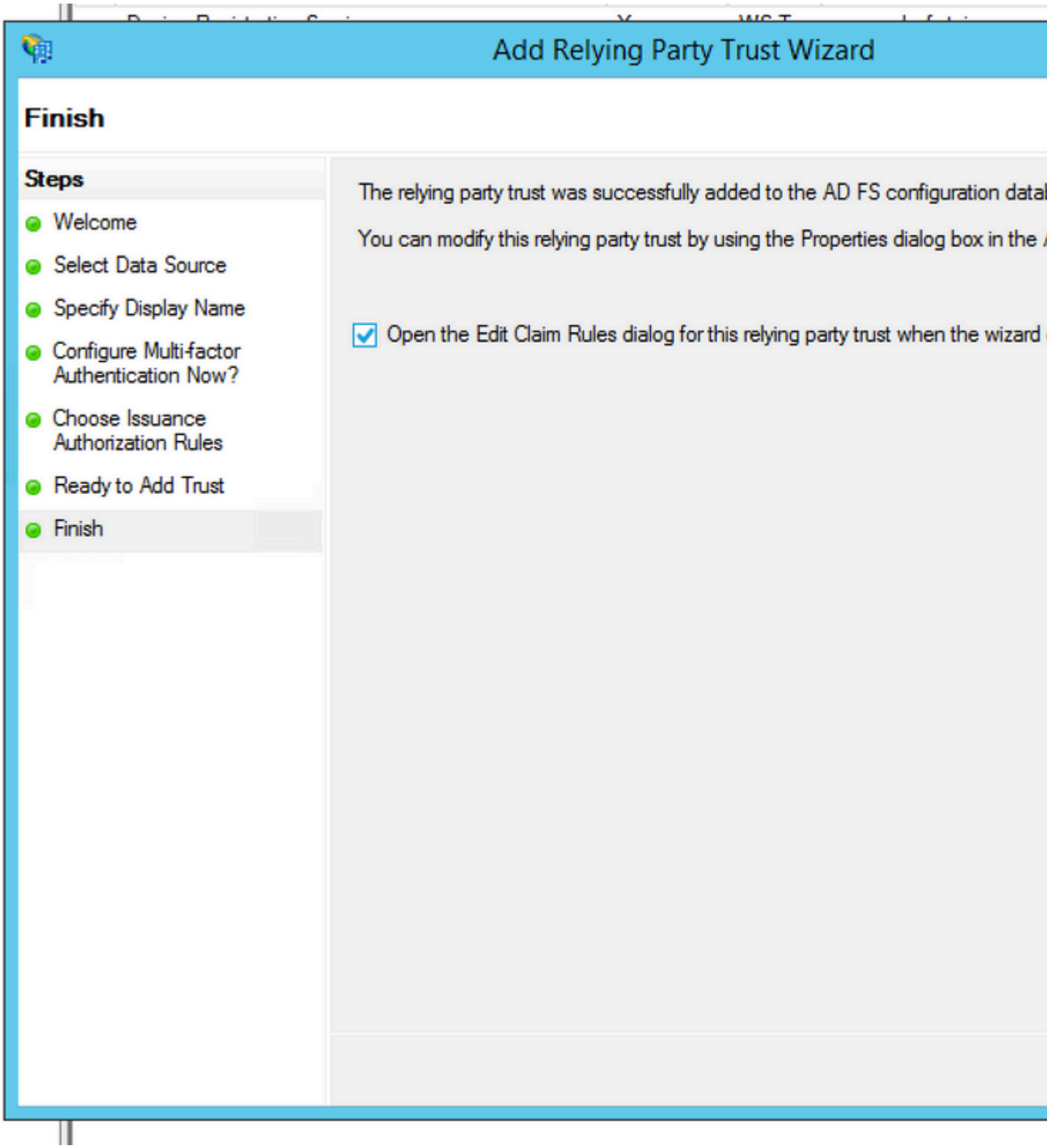

Add Relying Party Trust Wizard
Browse for Metadata File...
« SSO 11.5 ▸ Pod1
Search
Organize
New folder
Downloads
Recent places
This PC
Desktop
Documents
Downloads
FOLDERS on ARU
Music
Pictures
Videos
Local Disk (C:)
DVD Drive (D:) IR
Name
Date modified
sp
8/18/2016 8:26 PM
File name: sp
Metad
< Previous


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

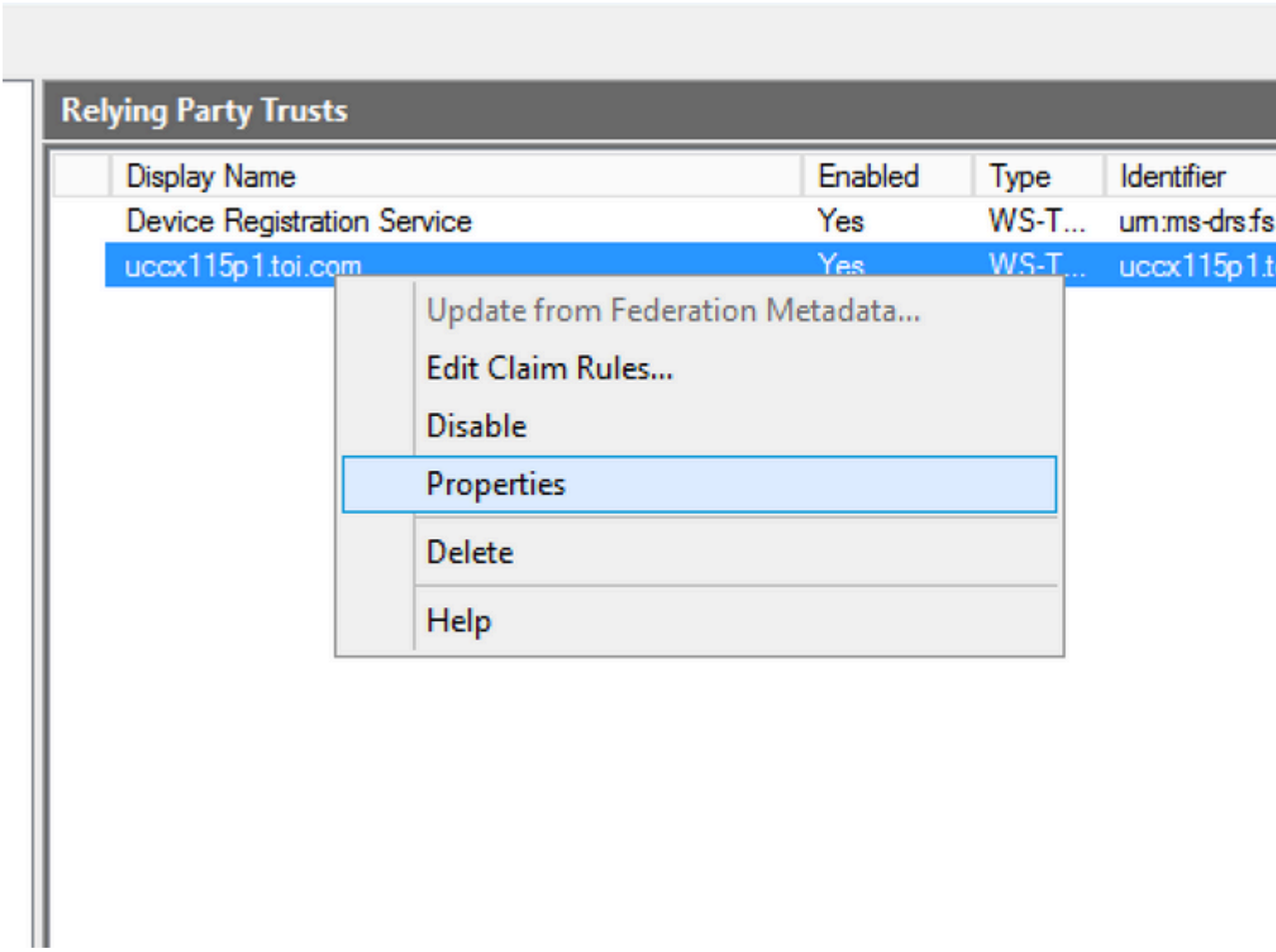

Add Relying Party Trust Wizard
Steps
Welcome
Select Data Source
Specify Display Name
Configure Multi-factor Authentication Now?
Choose Issuance Authorization Rules
Ready to Add Trust
Finish
Configure multi-factor authentication settings for this relying party trust. Multi-fa
there is a match for any 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

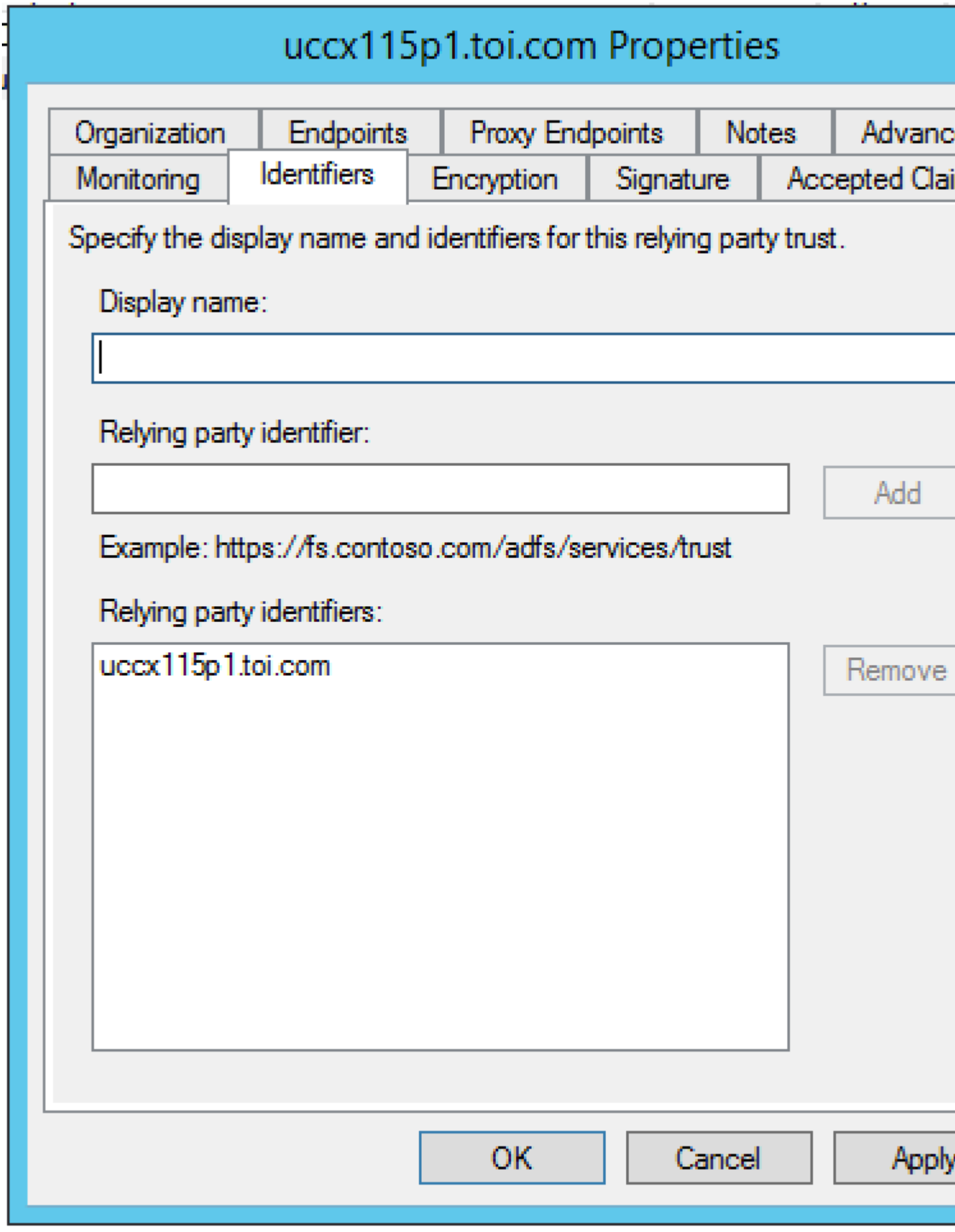


ç¬¬å››æ¥¼šå®Œæˆ�ä¿¡èµ–æ–¹ä¿¡ä»»çš„å»ºç«‹ã€‚

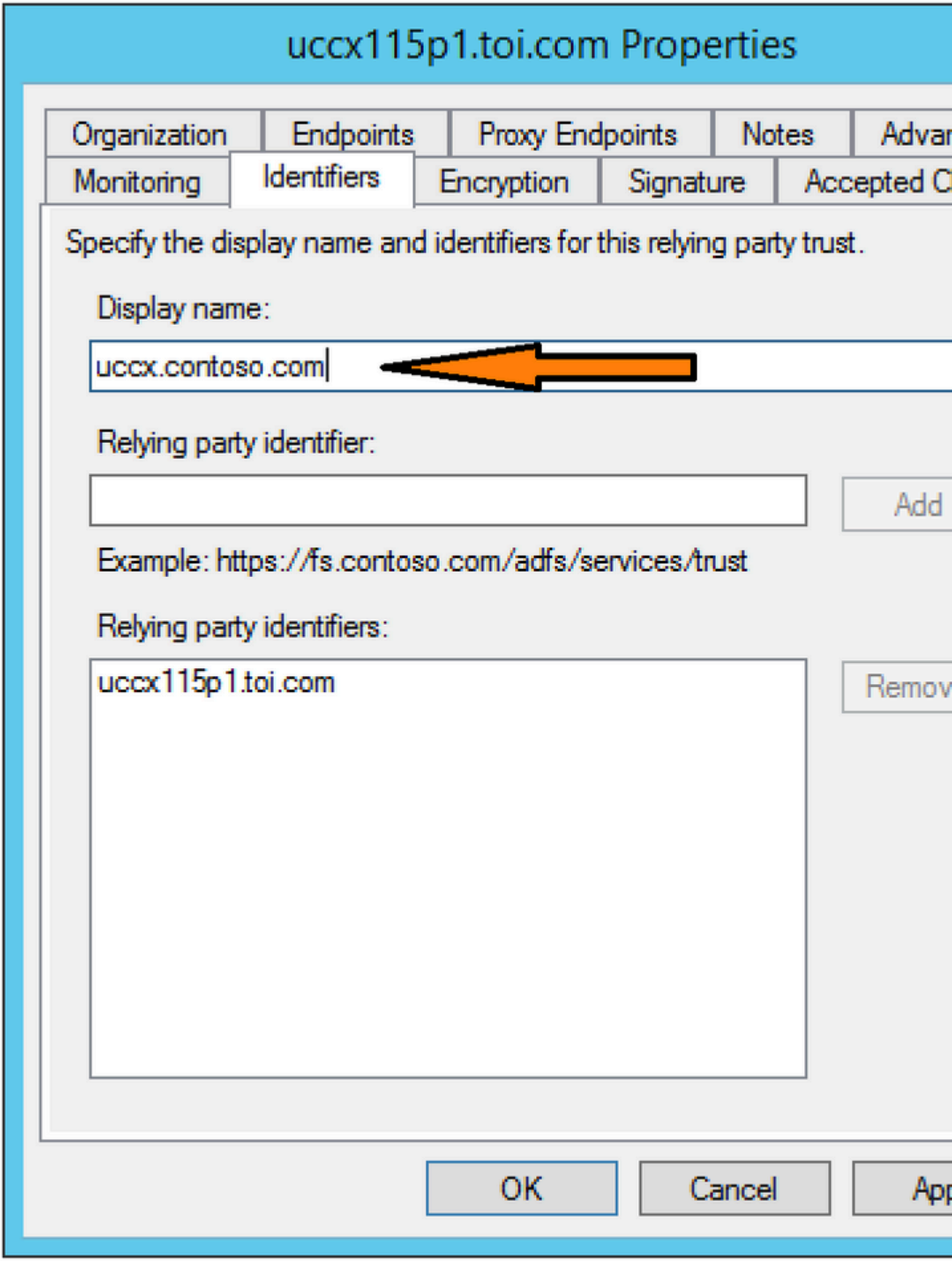


ç¬¬äº”æ¥ï¼šåœ¨ä¿¡èµæ–¹ä¿¡ä»»çš„å±žæ€§ä¸ŒéŒ€‰æ‹© Identifier é€‰é¡¹å�¡ã€‚


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

ç¬¬å…æ¥ï¼šå°†æ ‡è¯†ç¬¦è®¾ç½®ä¸ºCisco Identity Serverçš„å®Œå…¨é™å®šä¸»æœºå��ï¼ŒCisco Identity Serverå¯¯ä»Žå…¶è·å¾— sp.xml å·²ä¸‹è½½ã€‚



æ¥é¤ 7.å€³é”®å€•å‡»â€œä¿¡èµ–æ–¹ä¿¡ä»»â€ï¼Œç„¶åŽå€•å‡» Edit Claim Rules.

user_principal - Cisco
IDéœ€è¦�æ¤å±žæ€§ä»¥æ ‡è¯†ç»�è¿‡è°«ä»½éªŒè¯�çš„ç”¨æˆ·çš„é¢†åŸŸã€,

é¢†æ¬¾ç”³è¯·è§„å˜™1:

æŒ‰å��ç§°æ·»åŠ è§„å˜™ NameID ç±»åž‹ï¼å°†LDAPå±žæ€§çš„å€¼ä½œä¸°å£°æ˜Žå�'é€�ï¼‰ï¼š

- é€‰æ‹©å±žæ€§å˜ä¸ä½œä¸°Active Directory
- æ˜ å°„LDAPå±žæ€§ User-Principal-Name å˚ user_principal ï¼ˆå°å†™ï¼‰
- é€‰æ‹©å¿…é¡»ç”¨ userId ä»¥ä¾¿å°”ç”¨æˆ·ç™»å½•å¹¶å¹¶å…¶æ˜ å„å˚ uidï¼ˆå°å†™ï¼‰

é…�ç½®ä¾‹ SamAccountName å°†ç”¨æˆ·ID:

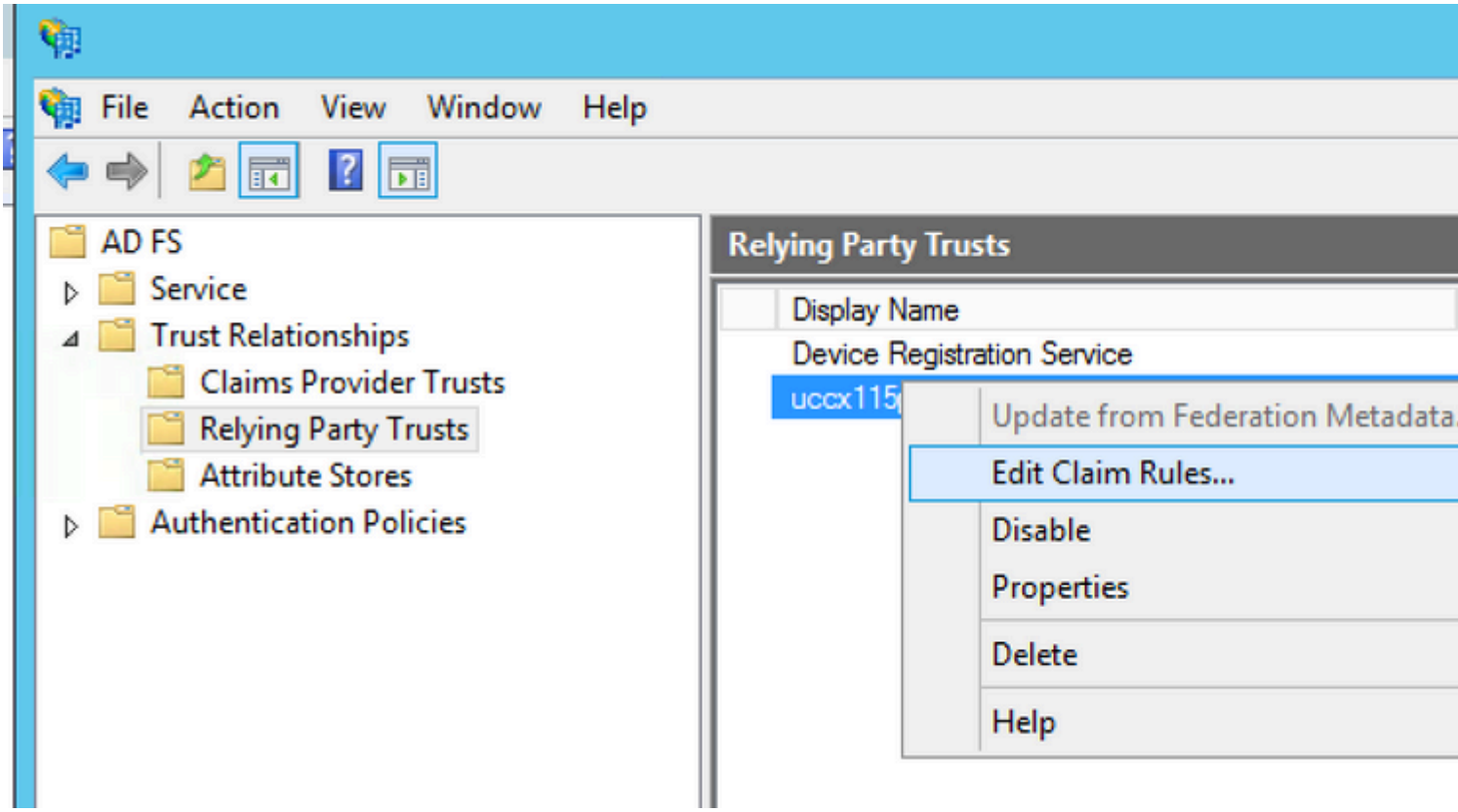
- æ˜ å°„LDAPå±žæ€§ SamAccountName å˚ uid.
- æ˜ å°„LDAPå±žæ€§ User-Principal-Name å˚ user_principal.

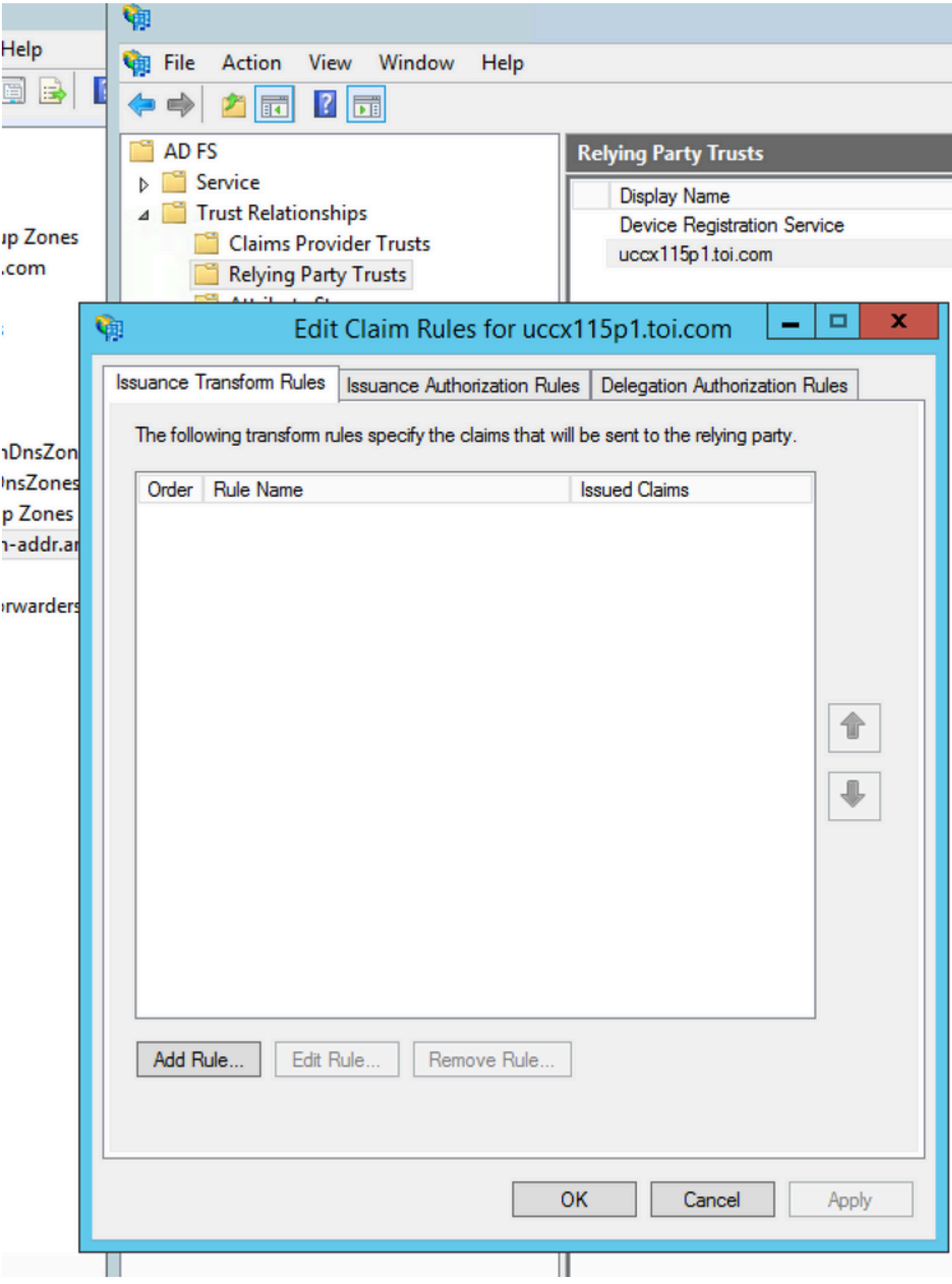
UPNå¿…é¡»ç”¨æˆ·IDæ—¶çš„é…�ç½®ä¾‹ï¼š

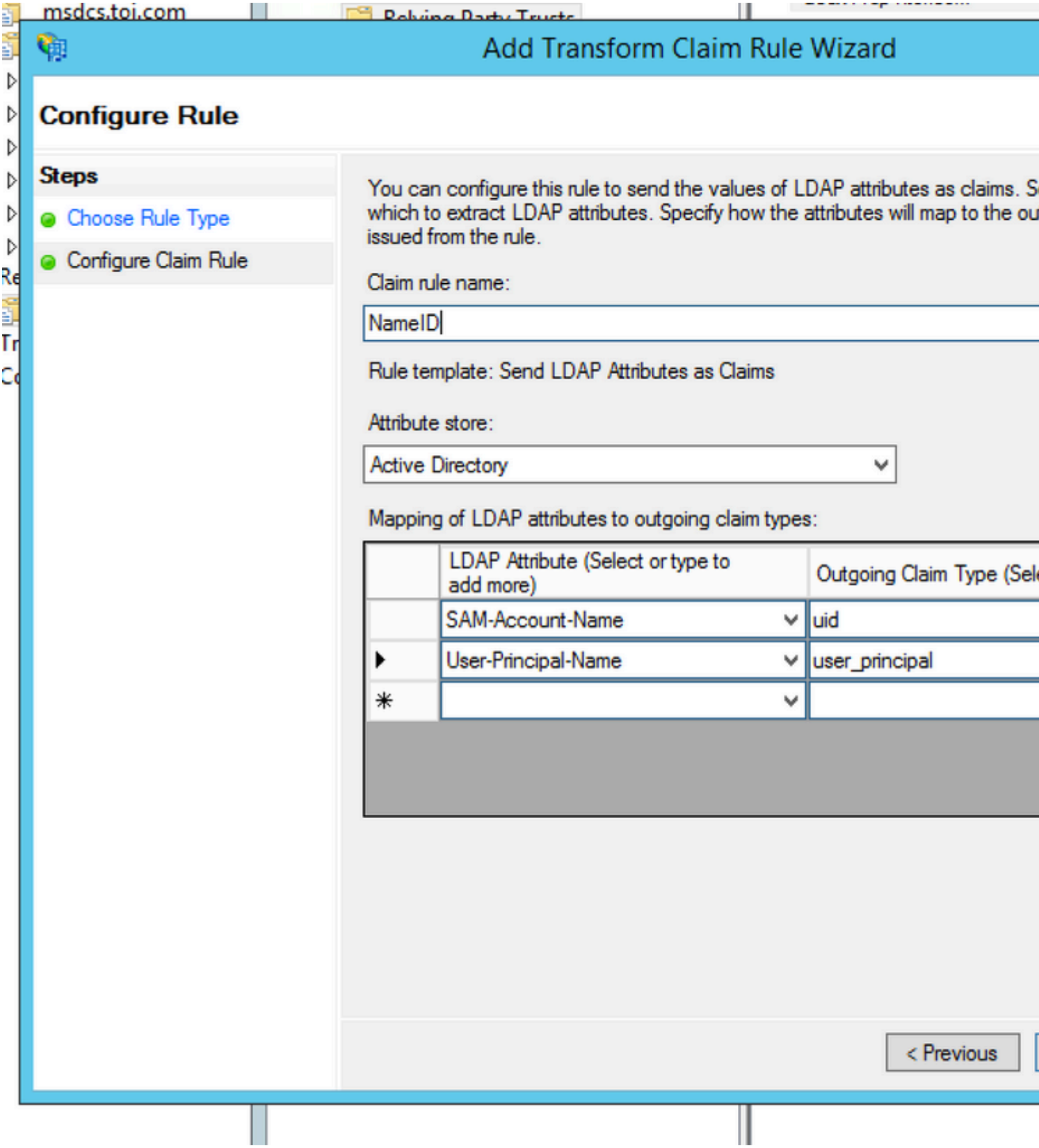
- æ˜ å°„LDAPå±žæ€§ User-Principal-Name å˚ uid.
- æ˜ å°„LDAPå±žæ€§ User-Principal-Name å˚ user_principal.

é…�ç½®ä¾‹ PhoneNumber å¿…é¡»ç”¨æˆ·ID:

- æ˜ å°„LDAPå±žæ€§ telephoneNumber å˚ uid.
- æ˜ å°„LDAPå±žæ€§ User-Principal-Name å˚ user_principal.

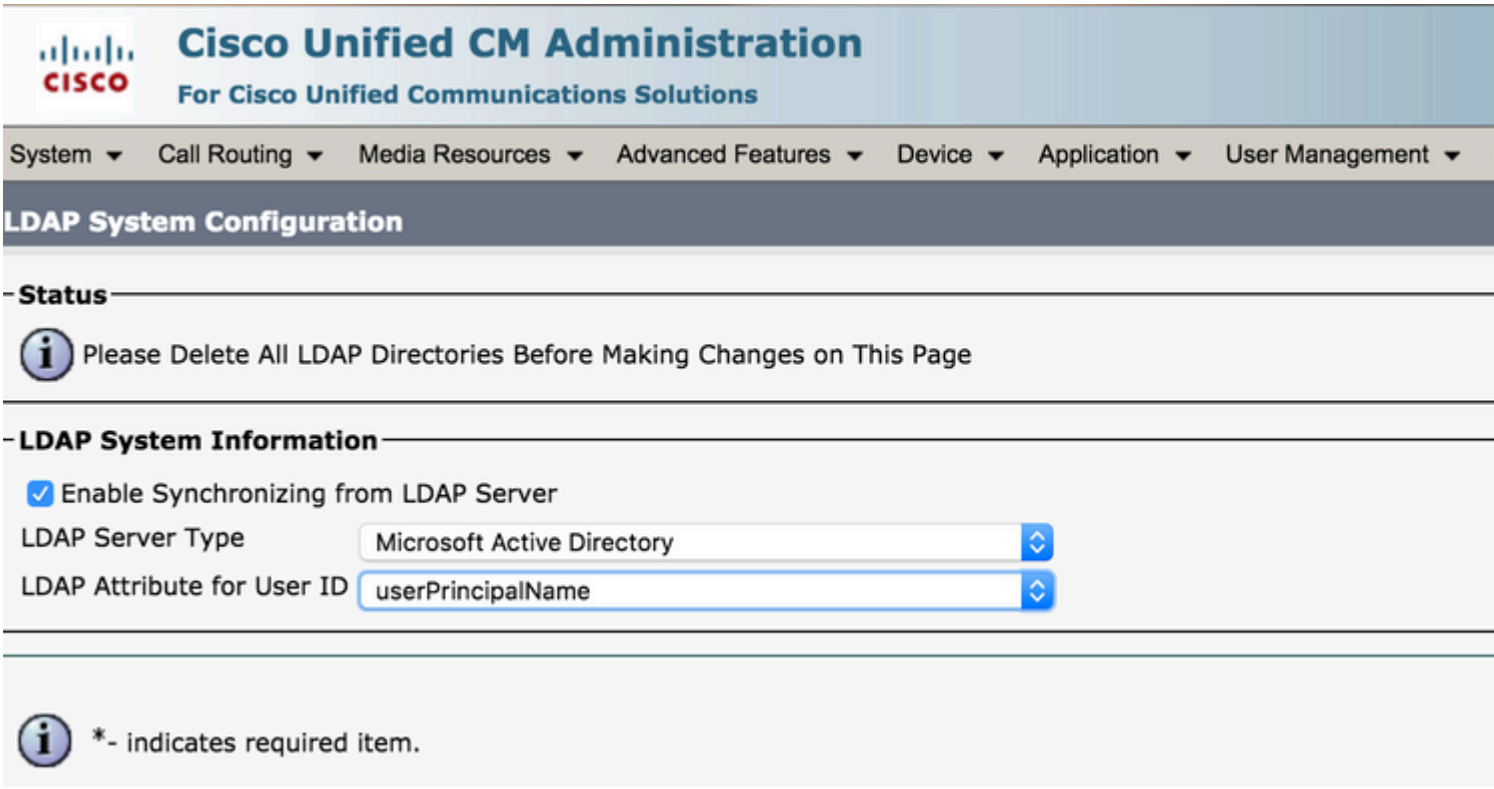



Help
File Action View Window Help
AD FS
Service
Trust Relationships
Claims Provider Trusts
Relying Party Trusts
Relying Party Trusts
Display Name
Device Registration Service
uccx115p1.toi.com
Edit Claim Rules for uccx115p1.toi.com
Issuance Transform Rules
Issuance Authorization Rules
Delegation Authorization 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
Add Transform Claim Rule Wizard



æ³¨ï¼šæ¸…å¿…é¡»ç¡®ä¿�ä¸ºCUCM LDAPå�Œæ¥ä¸Šçš„ç”¨æˆ·IDé…�ç½®çš„LDAPå±žæ€§ä¸Žé…�ç½®ä¸ºLDAPå±žæ€§çš„ uid åœ¨ADFSå£°æ˜Žè§„å˜™å��ç§°IDä¸ã€è¿™ç”¨äºŽCUICå’ŒFinesseç™»å½•çš„æ£ç¡®ÅŸÈƒ½ã

æ³¨ï¼šæœ¬æ–‡æ¡£ä¾†å£°æ˜Žè§„å^™å••ç§°å'Œæ˜¾ç¤ºå••ç§°ï¼^å¦‚NameIDã€•UC

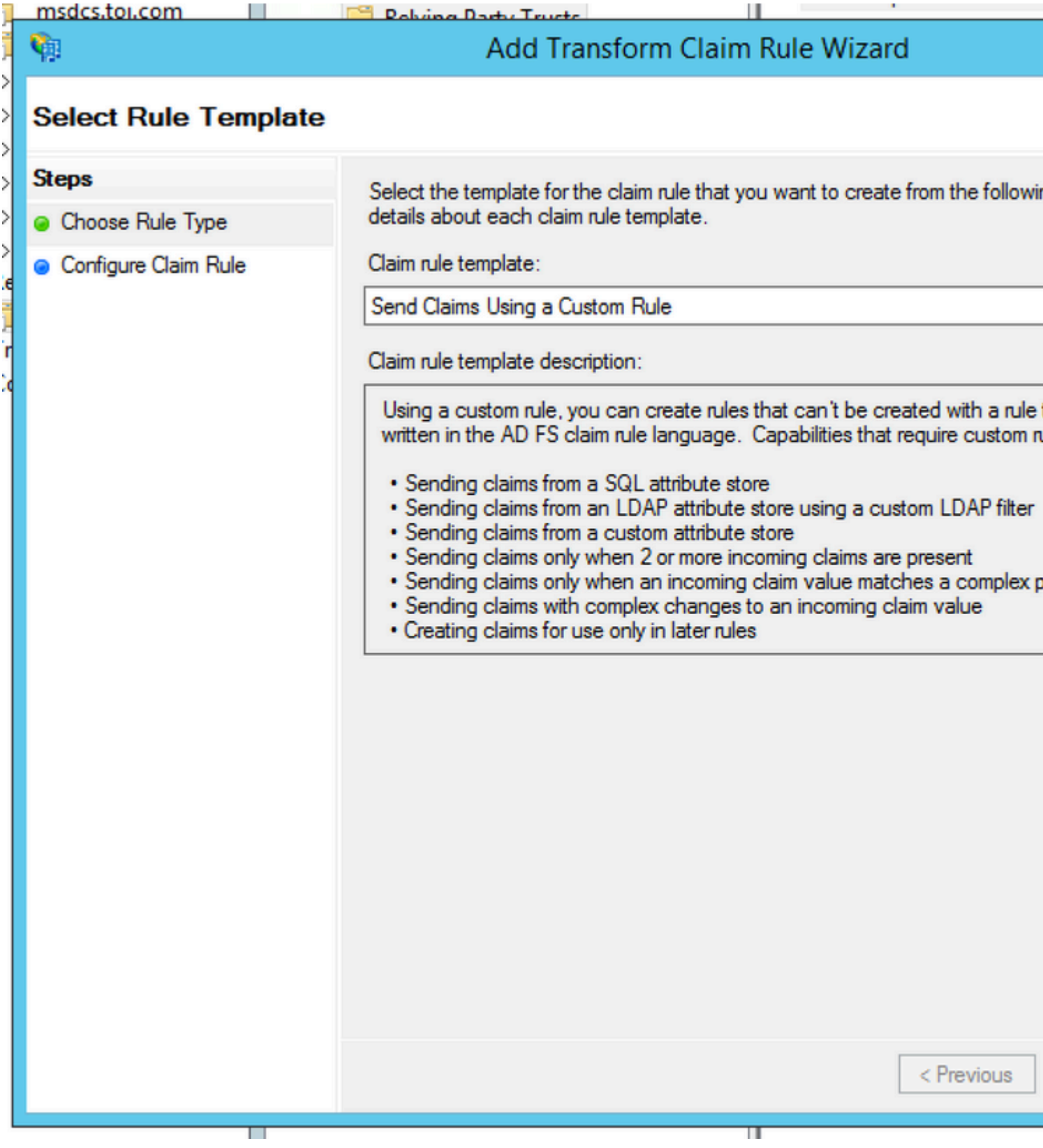


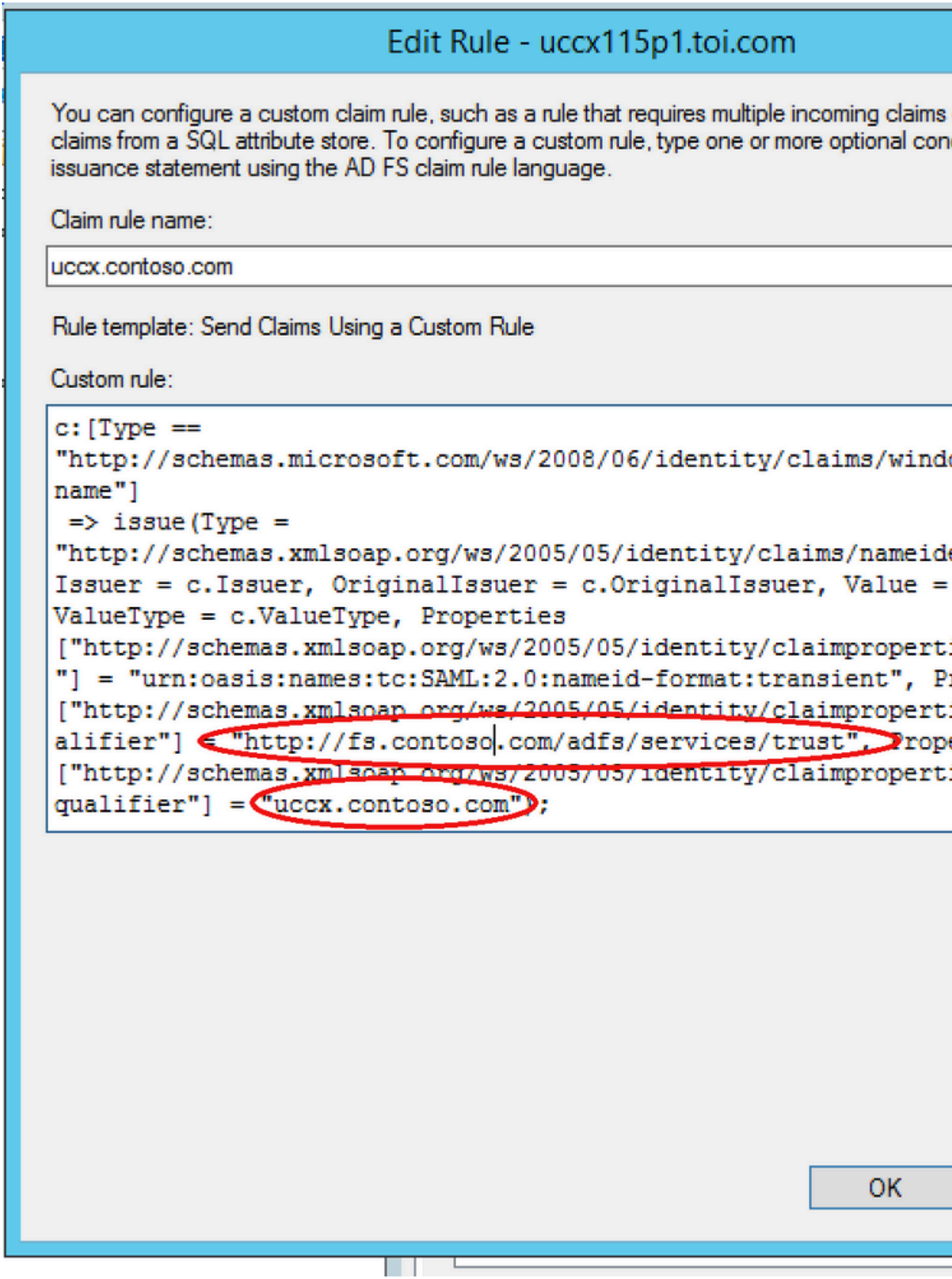
é¢†æ¬¾ç”³è¯·è§„å^™2:

- æ·»åŠ å••ä¸€ä¸ªè‡ªå®šä¹‰å£°æ˜Žè§„å^™ç±»åž‹çš„è§„å^™ï¼Œè¯¥è§„å^™çš„å••ç§°æ˜¯Cisco Identity Serverçš„å®Œå…¨é™••å®šä¸»æœºå••ï¼Œå¹¶æ·»åŠ æ¤è§„å^™æ–‡æœ¬ã€‚

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

- åœ¨ä€•ç§‘è°«ä»½æœ•åŠ¡å™¨é›†ç¾¤ä¸çš„æ‰€æœ‰å®Œå…¨é™••å®šä¸»æœºå••éƒ½æ˜¯
- <Fully qualified hostname of Cisco Identity Server>åŒºå^†å¤§å°•å†™ï¼Œæ¤å®Cisco Identity Server FQDNå®Œå…¨åŒ¹é…ï¼^åŒ…æ‹¬å¤§å°•å†™ï¼‰ã€‚
- <ADFS Server FQDN>åŒºå^†å¤§å°•å†™ï¼Œæ¤å®ADFS FQDNå®Œå…¨åŒ¹é…ï¼^åŒ…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

ï¼šå¦‚æžœä½¿ç”¨ADFS 3.0ï¼Œå˜åœ¨è¦æ¥éª¤2ã€‚å› ä¸ºCmdLetå·²ä½œä¸ºè§’è‰²åŠŸèƒ½æ·»åŠ çš„ä¸é

æ³¨:

åŒºåˆ†å¤§å°�å†™ï¼Œæ¤å®šâ€œä¿¡èµ–æ–¹ä¿¡ä»»â€�å±žæ€§çš„â€œæ ‡è¯†ç¬¦â€

**æ³¨ï¼šä»ŽUCCXç‰ˆæœ¬12.0å¼€å§‹ï¼ŒCisco IdSæ”¯æŒ SHA-256ã€‚ä¿¡èµ–æ–¹ä¿¡ä»»ä½¿ç”¨ SHA-256ç¾ç½²SAMLè¯·æ±‚ï¼¶æœŸæœ›ä»»ADFSèŽ·å¾—ç›¸å�Œçš„å“"å°"ã€‚

ç”¨äºŽè�”å�ˆADFSçš„å¤šåŸŸé…ç½®

åœ¨ADFSä¸çš„è�”å�ˆæƒ…å†µä¸ï¼Œç‰¹å®šåŸŸä¸çš„ADFSä¸°å…¶ä»–å·²é…ç½®åŸŸä¸çš„ç”¨æˆ·æ��

åœ¨æœ¬èŠ‚ä¸ï¼Œæœ¯è¯â€œæœ¬åœ°IdSâ€ADFSâ€œæ˜¯æŒ‡å¿…é¡»åœ¨IdSä½¿ç”¨çš„ç”¨æˆ·ä¸çš„ADFSã€‚æœ¯è¯â€œè¿œç¨‹ADFSâ€œæ˜¯æŒ‡ä¸Žæœ¬åœ°IdSè¿›è¡Œè”å¦

è”å¦ADFSé…ç½®

åœ¨æ¯ä¸ªè”å¦ADFSä¸ï¼Œå¿…é¡»ä¸ºè¦ä¸Žæœ¬åœ°IdSè¿›è¡Œè”å¦çš„æ‰€æœ‰è¿œç¨‹ADFSåˆ›ç´¢èµ„æ¥ä¿¡ä»»ã€‚

ä¸»ADFSé…ç½®

å¯¹äºŽä¸»ADFSï¼Œéœ€è¦æ–¹IdSçš„ä¿¡èµ–æ–¹ä»»åŠ¡ï¼Œä»¥å…è¿œç¨‹ADFSæ¥ä¿¡ä»»å®ƒã€‚

Addï¼šæ·»åŠ ï¼‰ Claim Provider Trust ADFSï¼Œè”å¦å¿…é¡»è®¾ç½®ä¸ºã€‚

åœ¨å£°æ˜Žæ��ä¾›ç¨‹åº�ä¿¡ä»»ä¸ï¼Œç¡®ä¿ Pass through or Filter an Incoming Claim å°†è§„å™™é…ç½®ä¸ºé€’æ‰€æœ‰å£°æ˜Žå€¼ä½œä¸ºé¡¹ï¼š

- å��ç§°ID
- ä»Žä¸é€‰æ‹©å��ç§°ID Incoming Claim Type æ”¶å˜ç®±
- é€‰æ‹© Transient ä½œä¸ºå…¥NameIDæ ¼å¼�çš„é€‰é¡¹
- uidï¼šè¿™æ˜¯è‡ªå®šä¹‰å£°æŽ,è¾“å…¥uid Incoming Claim Type æ”¶å˜ç®±
- user_principalï¼šè¿™æ˜¯ä¸€ä¸ªè‡ªå®šä¹‰å£°æŽ,åœ¨user_principalå—æ®µé¡®å…¥å€¼ Incoming Claim Type æ”¶å˜ç®±

åœ¨Idçš„ä¿¡èµ–æ–¹ä¸ï¼Œå¿…é¡» Pass though or Filter an Incoming Claim ä»¥ä¸€ç§æ–¹å£°æŽå€¼ä½œä¸ºé€‰é¡¹çš„è§„å™™ã€‚

- å��ç§°IDFromSubdomain
- ä»Žä¸é€‰æ‹©å��ç§°ID Incoming Claim Type æ”¶å˜ç®±
- é€‰æ‹© Transient ä½œä¸ºå…¥NameIDæ ¼å¼�çš„é€‰é¡¹
- uidï¼šè¿™æ˜¯è‡ªå®šä¹‰å£°æŽ,é¡®å…¥uid Incoming Claim Type æ”¶å˜ç®±
- user_principalï¼šè¿™æ˜¯ä¸€ä¸ªè‡ªå®šä¹‰å£°æŽ,åœ¨user_principalå—æ®µé¡®å…¥å€¼ Incoming Claim Type æ”¶å˜ç®±

ADFSè‡ªåŠ¨è¯ä¹¦æ»šåŠ¨æ›´æ–°

UCCX 11.6.1å•Šæ›´é«˜ç‰ˆæœ¬æ”¯æŒè‡ªåŠ¨è¯ä¹¦æ»šåŠ¨ã€‚(UCCX 11.6ä¸çš„Fedletå°“å•‡çº§å^°ç‰ˆæœ¬14.0è§£å†³ä°†æ¤é—®é¢˜ã€)

Kerberosè°«ä»½éªŒè¯ï¼ˆé›†æ^Windowsè°«ä»½éªŒè¯ï¼‰

é›†æ^çš„Windowsè°«ä»½éªŒè¯(IWA)ä¸ç”¨æ^·æ••ä¾›è°«ä»½éªŒè¯æœºå^¶ï¼Œä½†ä¸å…•è

æ³¨æ„ï¼šä»Ž11.6å•Šæ›´é«˜ç‰ˆæœ¬æ”¯æŒKerberosè°«ä»½éªŒè¯ã€‚

å·²ç™»å½•å^°åŸŸæŽ§å^¶å™¨(DC)çš„åŸŸç”¨æˆ·å•¯æ— ç¼«ç™»å½•å^°SSOå®¢æˆ·ç«¯ï¼Œè€Œæ— éœ€é 3.0æ‰§è¡Œçš„ã€‚

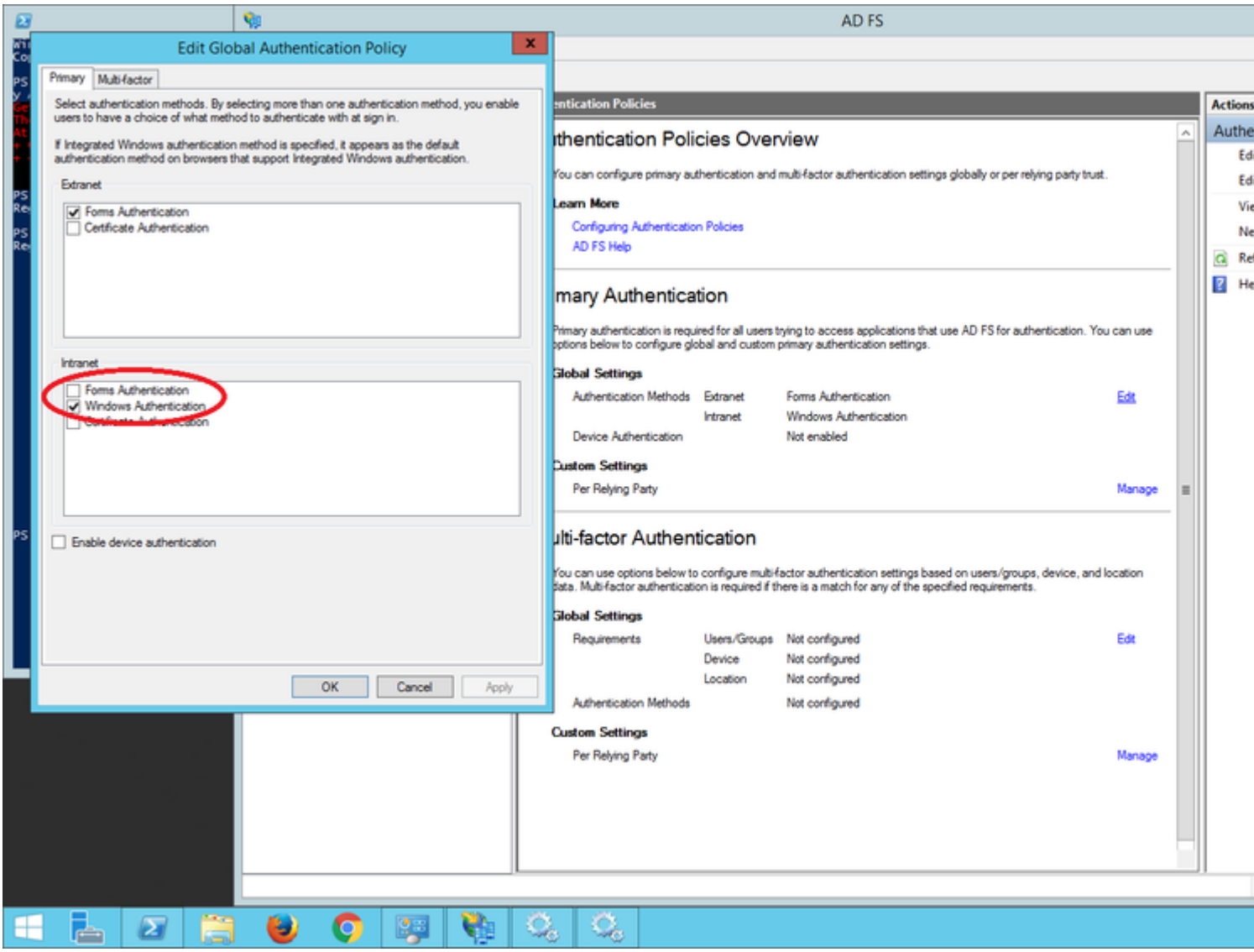
æ¥éª¤1:æ‰“å¼€Windowså‘½ä»¤æ••ç¤ºç¬¦å¹¶ä»¥ç®¡ç†å‘˜ç”¨æˆ·è««ä½¿è¡Œï¼Œä»¥ä¾¿å•‘æ³¨å†Œå‘½ä»¤ **setspn -s http/**

\

.

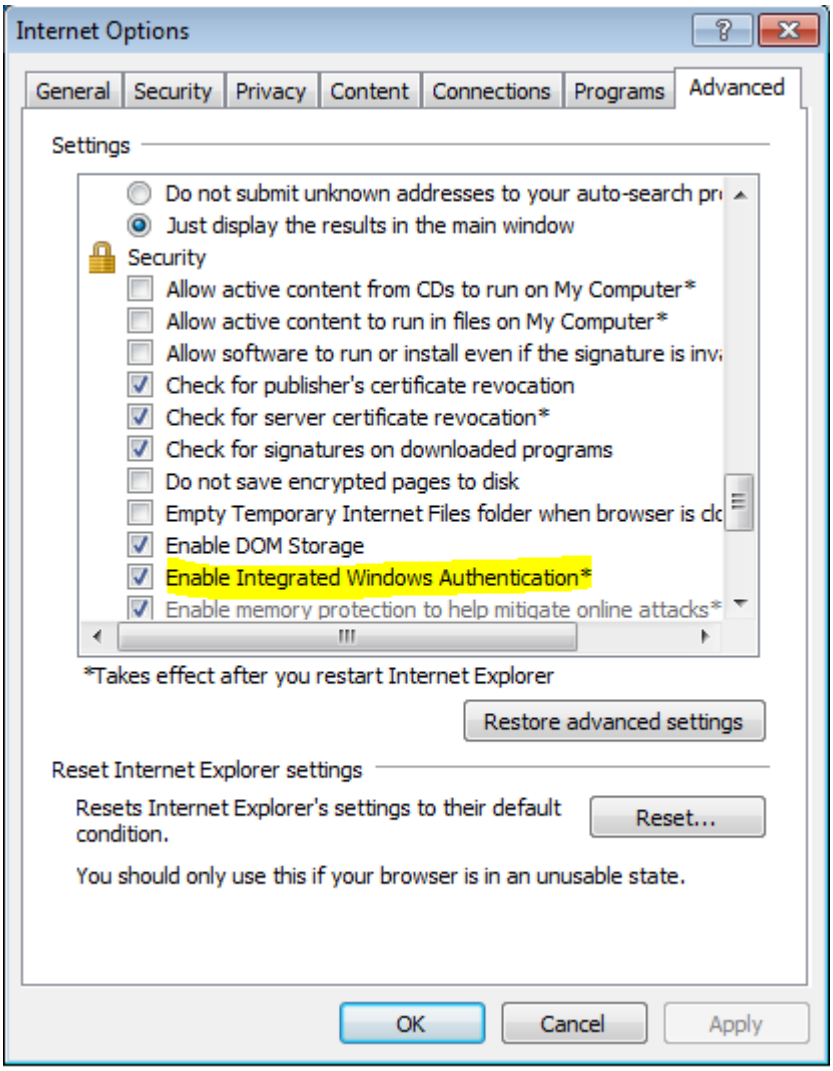
ç¬¬äºŒæ¥ï¼šç¡®ä¿¡æ•èº«ä»½éªŒè¯å¹¶å•¯ç”¨æ†…éƒ¨ç½‘ç«™,¹çš„Windowsè°«ä»½éªŒè¯ã€‚

ADFS Management > Authentication Policies > Primary Authentication > Global Settings > Edit.åœ¨Intranetä¸‹ï¼Œç¡®å•ªé€‰ä¸Windowsè°«ä»½éªŒè¯(å•–æ¶ˆé€‰ä¸Form Authentication)ã€‚

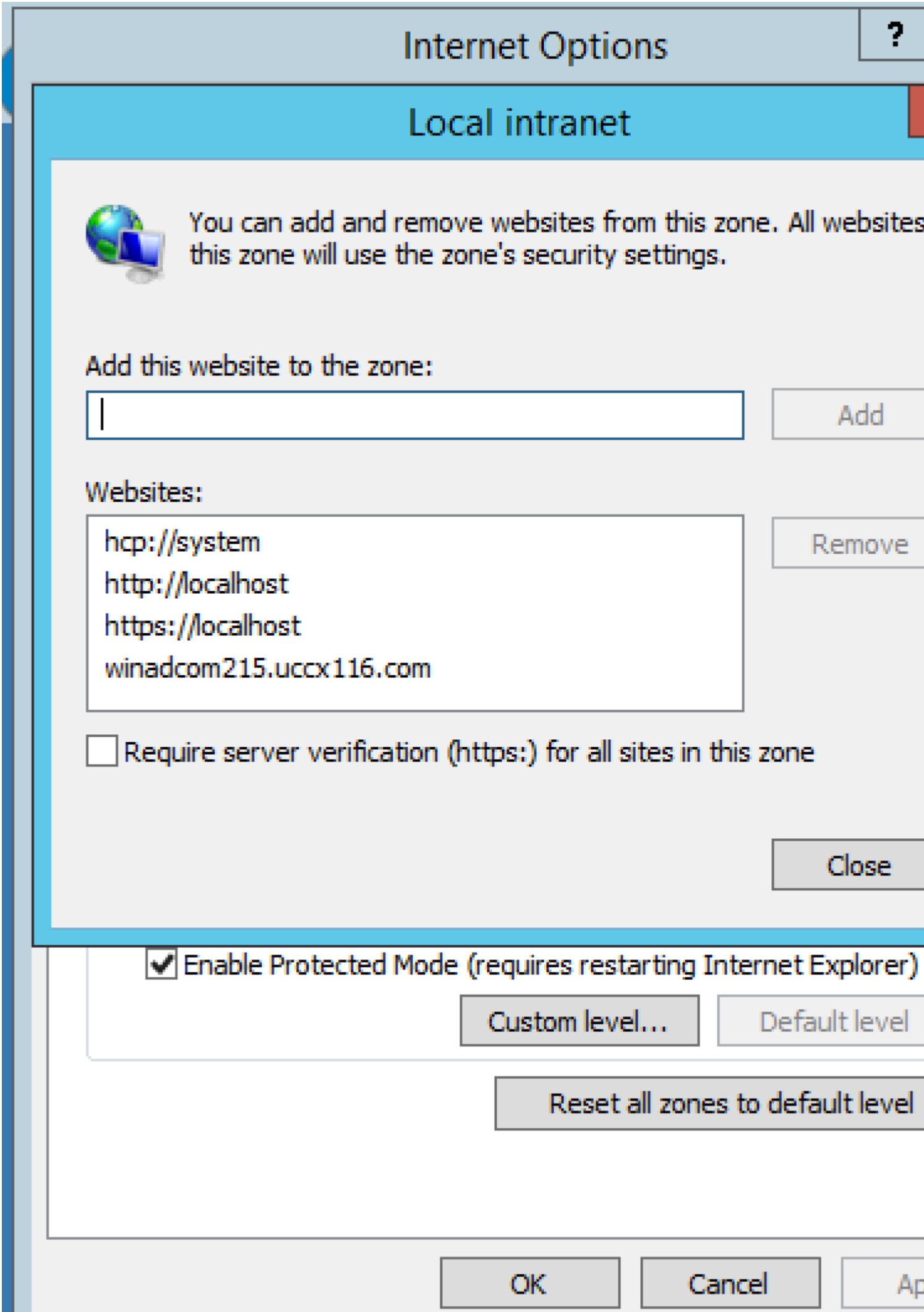


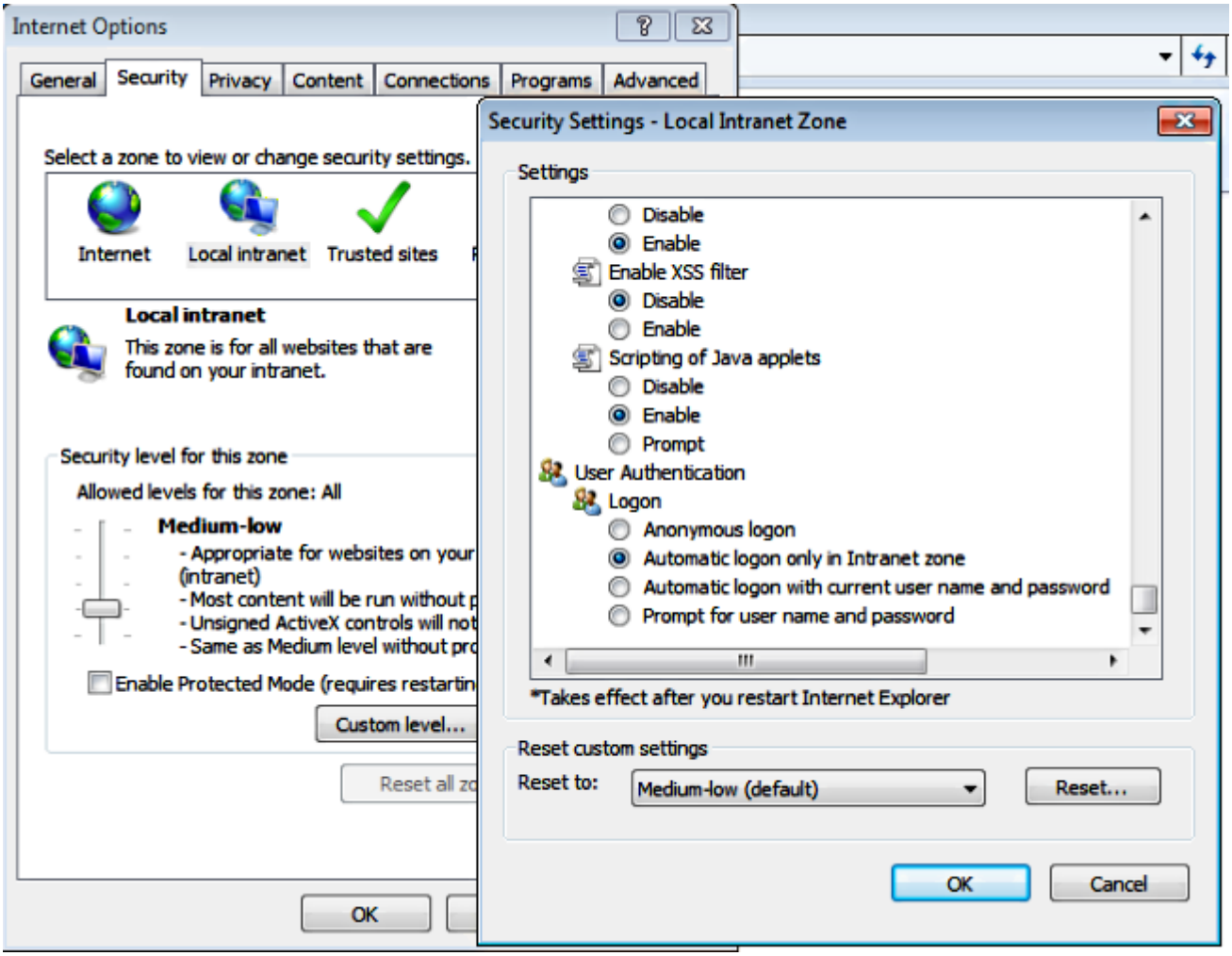
Microsoft Internet Explorerçš„IWAæ”¯æŒ©é...ç½®

æ¥éª¤1: ç¡®ä¿ Internet Explorer > Advanced > Enable Integrated Windows Authentication å·²é€‰ä¸,



ç¬¬äºŒæ¥¼š å¿…é¡»å°†ADFS URLæ·»åŠ å^° Security > Intranet zones > Sites (winadcom215.uccx116.com æ˜¯ADFS URL)ã€‚

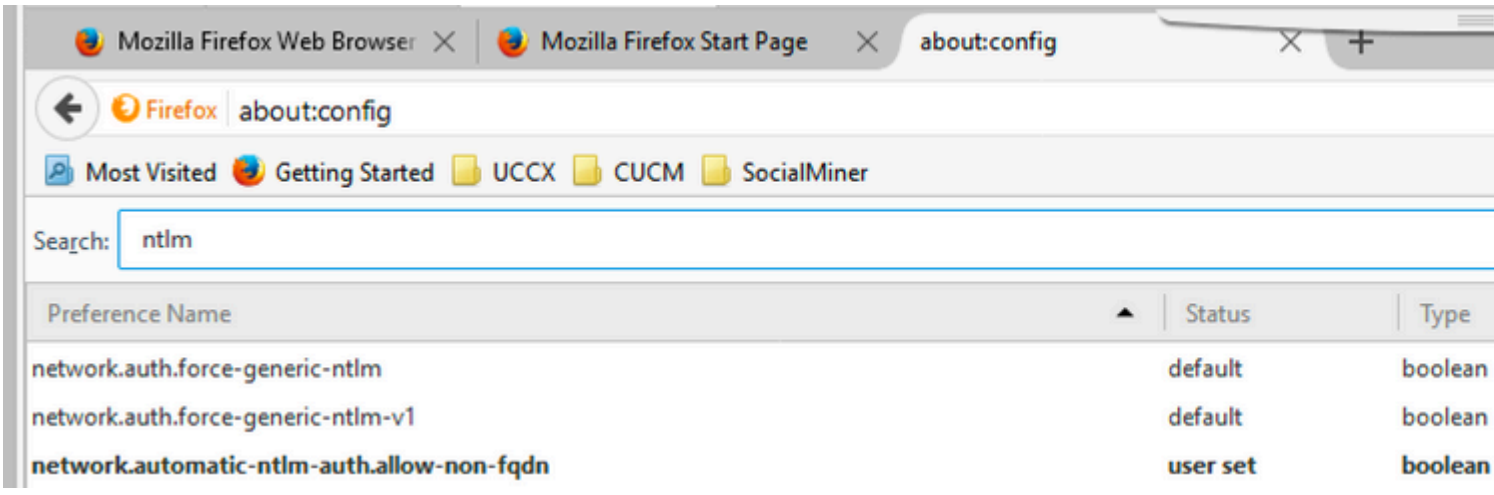

Internet Options
?
Local intranet
You can add and remove websites from this zone. All websites
this zone will use the zone's security settings.
Add this website to the zone:
Add
Websites:
hcp://system
http://localhost
https://localhost
winadcom215.uccx116.com
Remove
Require server verification (https:) 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”¨äºŽIWAæ”¯æŒ€çš„Mozilla Firefoxæ‰€éœ€çš„é…ç½®

æ¥éª¤1:è¿›å…¥Firefoxçš„é…ç½®æ¨¡å¼ã€‚æ‰“å¼€Firefoxå¹¶è¾“å…¥ about:config çš„URLã€‚æŽ¥å—é£Žé™©ç»§è¿›ã€‚

ç¬¬äºŒæ¥¤šæ¡ç´¢ ntlm å¹¶å¯¯ç”¨ network.automatic-ntlm-auth.allow-non-fqdn å¹¶å°†å…¶è®¾ç½®ä¸ºtrueã€‚



ç¬¬ä¸‰æ¥¤šè®¾ç½® network.automatic-ntlm-auth.trusted-uris æˆ–æ˜Žç¡®æŒ‡å®šADFS URLã€‚

ç”¨äºŽIWAæ”¯æŒ–çš„Google Chromeæ‰€éœ€çš„é…ç½®

Windowsä¸çš„Google Chromeä½¿ç”¨Internet Explorerè®¾ç½®ï¼Œæ¤åœ¨Internet Explorerä¸è¿›è¡Œé…ç½® Tools > Internet Options å¯¹è¯æ¡†ï¼Œæ^–ä»Žâ€œæŽ§å^¶é�¢æ¿â€�ä¸‹çš„ Internet Options åœ¨å¯±»å^«å†… Network and Internet.

SSOçš„è¿›ä¸€æ¥é…ç½®

æœ¬æ–‡æ¡£ä»£ŽSSOçš„IdPæ–¹é�¢æ��è¿°äºº ç”¨ä¸ŽCisco IdSé›†æ^�çš„é…ç½®ã€‚æœ‰å…³è¯¦ç»†ä¿¡æ¯ï¼Œè¯·å¯¼èˆªè‡³ä¸‹é¢—éƒ¨åˆ†ã€‚

- UCCX
- UCCE
- PCCE

éªŒè¯

æ¤è¿‡ç¨‹ä¸Ž ç®¡ç†å®šæ¯”å¦ Cisco IdSå’ŒIDPä¹‹é—´æ£ç®¡ç†å»ºç«‹ä¿¡èµ–æ–¹ä¿¡ä»»ã€‚

- ä»Žæ¡Œé¢§ˆå™¨è¾“å…¥URL https://<ADFS_FQDN>/adfs/ls/IdpInitiatedSignOn.aspx?loginToRp=<IDS_FQDN>
- ADFSæ��ä¾›ç™»å½•è¡¨å•€,å½“ä¸Šè¿°é…ç½®æ£ç®¡ç†å¯¼ç”¨å¯¯ã€‚
- æ^åŠŸè¿›è¡ŒéªŒè¯«ä»½éªŒè¯¯å¯¼å¼Ÿï¼Œæµ�è§ˆå™¨å¿…é¡»é‡å®šå‘è‡³https://<IDS_FQDN>:85

æ³¨ï¼šä½œä¸ºéªŒè¯æµ�ç¨‹çš„ä¸€éƒ¨åˆ†æ¾ç¤ºçš„â€œæ ¸å¯¯æ¸…å••â€éµéœ€ä¸æ˜¯

æ•…éšœæŽ’é™¤

æœ‰å…³éšœæŽ’é™¤ä¿¡æ¯ï¼Œè¯·å¯¼èˆªè‡³https://www.cisco.com/c/en/us/support/docs/customer-collaboration/unified-contact-center-express/200662-ADFS-IdS-Troubleshooting-and-Common-Prob.htmlã€‚

UCCX SSOæ—¶è·¯/æ¢å¤URL

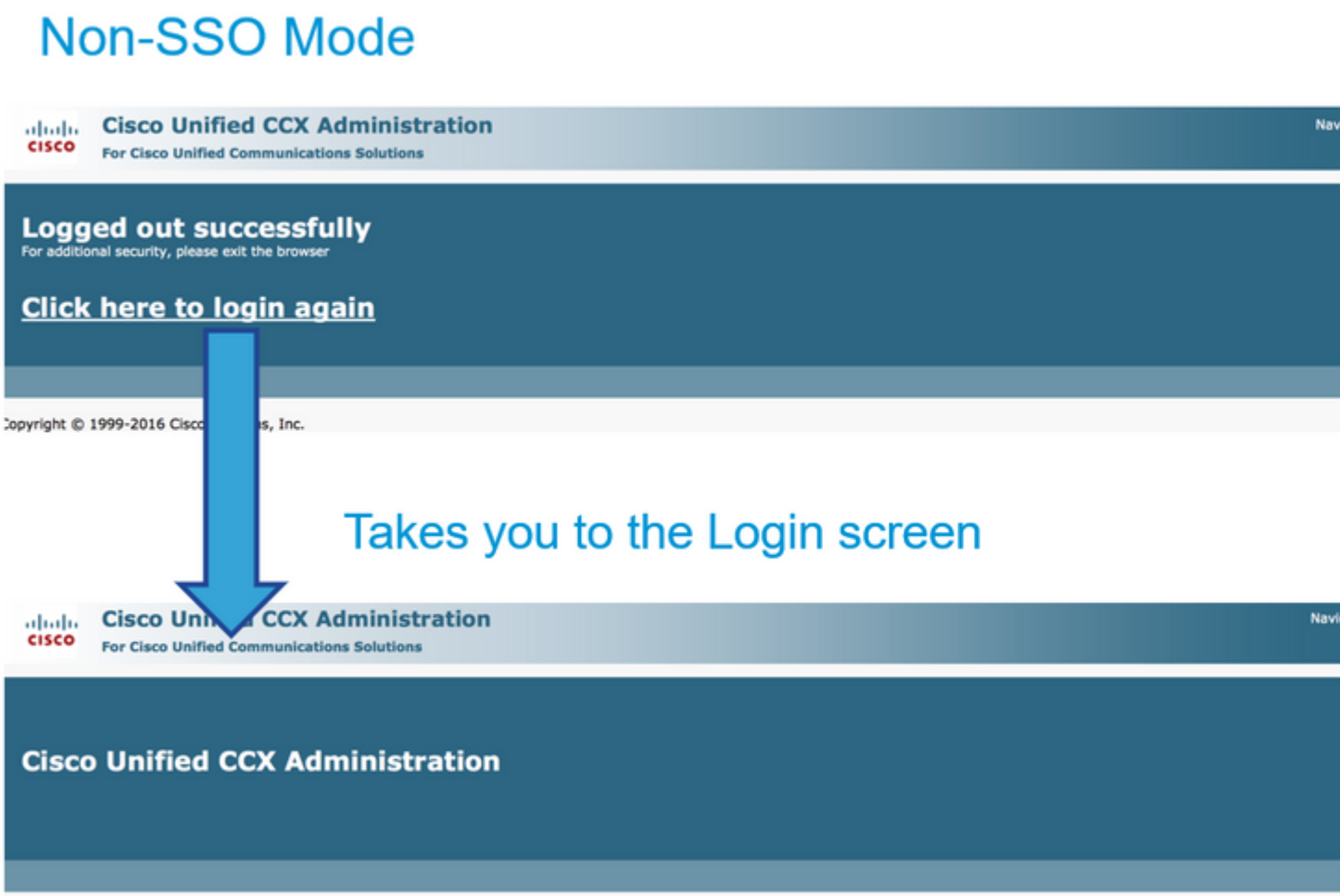
- Cisco Unified CCXç®¡ç†
- Cisco Unified CCXå¯¯ç»´æŠ¤æ€§

ç¦ç”¨SSO

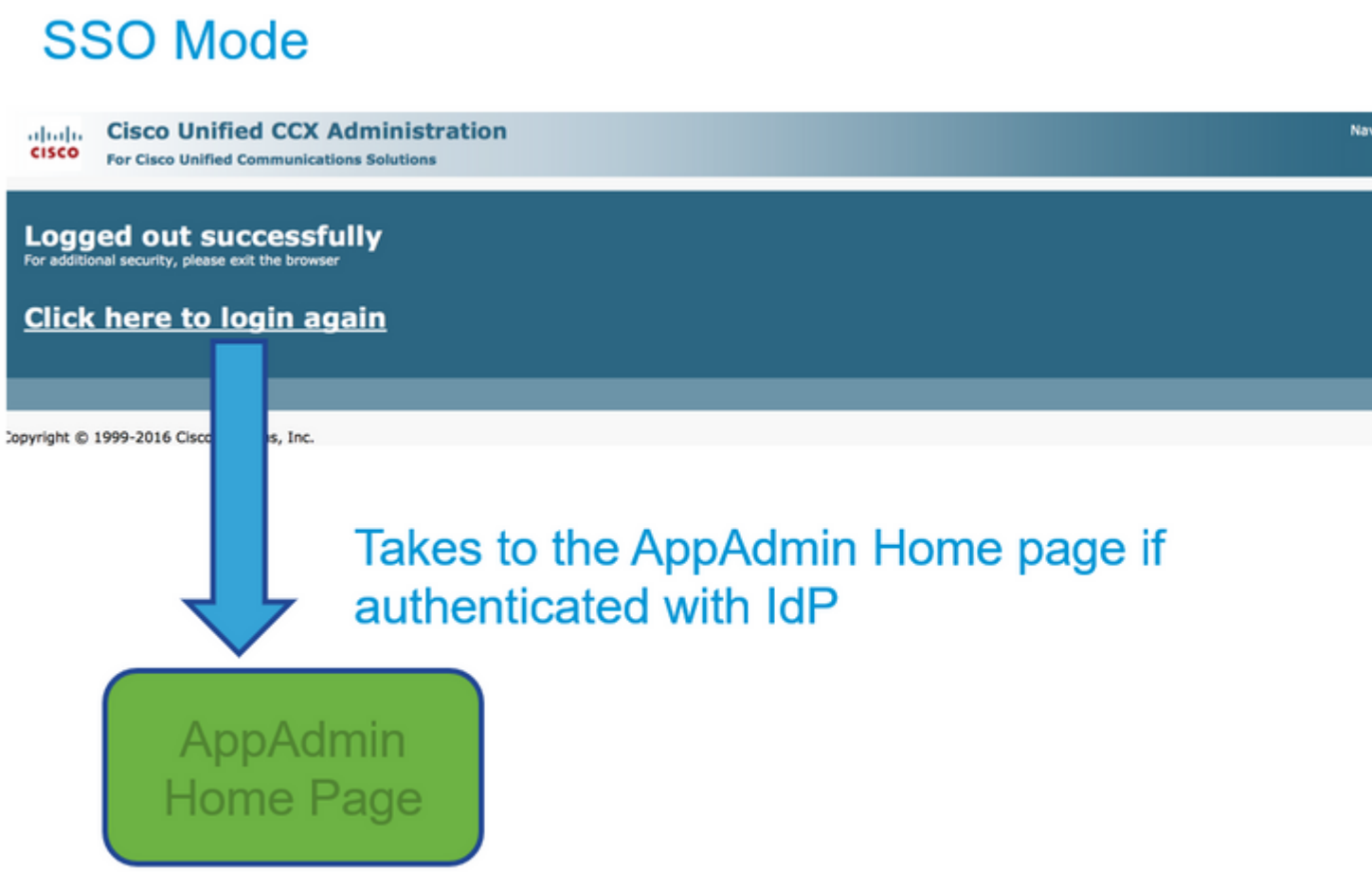
- GUIï¼šå¯¼èªªè‡³CCX Administration > Single Sign-On (SSO) > Disable.
- CLIï¼š set authmode non_sso (æ¤å‘½ä»¿…é¡»ç¦ç”¨Pubå’ŒSubçš„SSO â€”å¦,æžœå‡ºçŽ°é«˜å ¯ç”¨æ€§(HA)é›†ç¾¤ï¼Œå ¯ä»¥ŽUCCXèŠ‚ç‚¹ä¸Šçš„ä»»ä¸€èŠ‚ç‚¹æ‰§è¡Œæ¤å‘½ä»¤ã€‚

å±•å¹•æ˜¾ä¾›

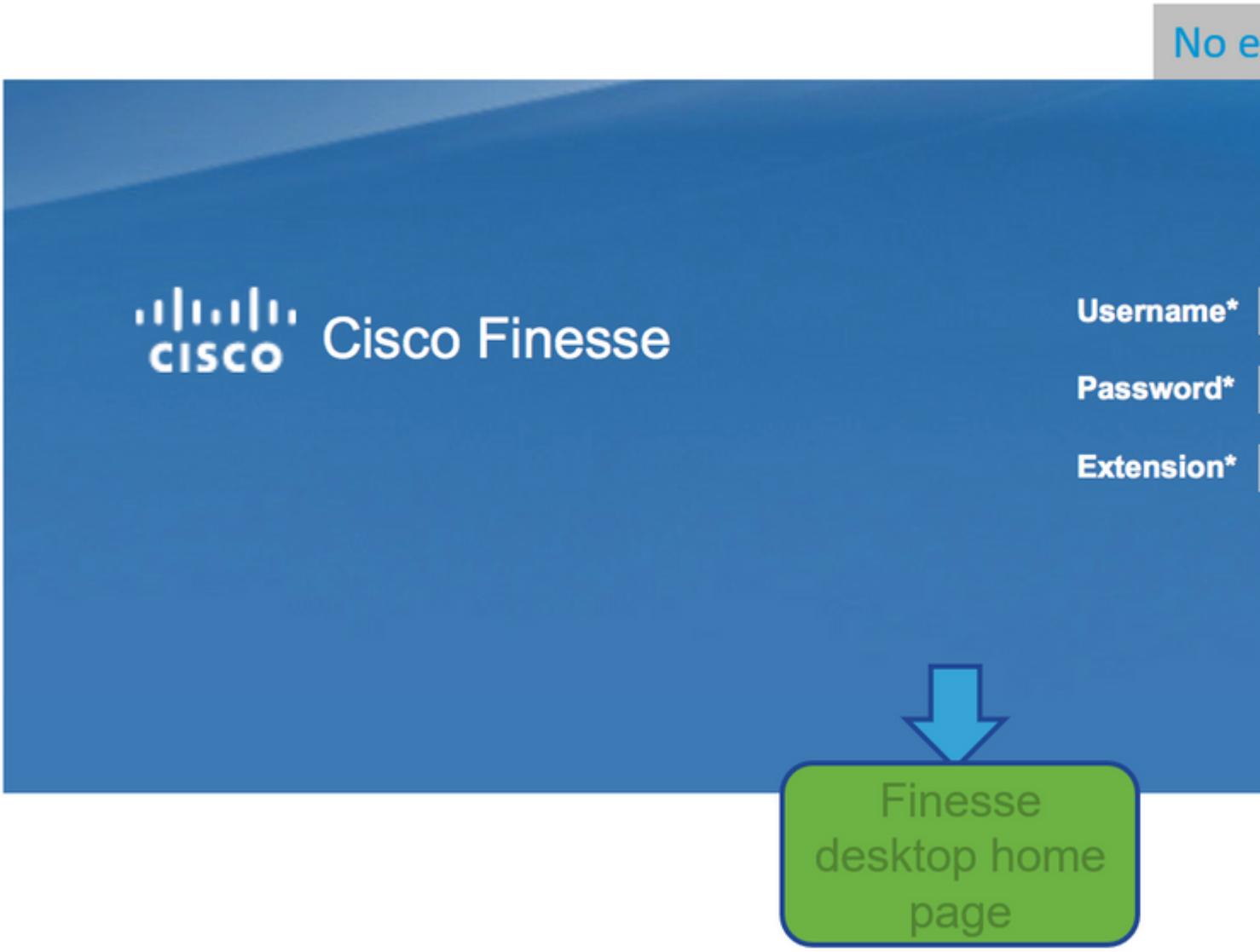
CCXç®¡ç†â€” é žSSO



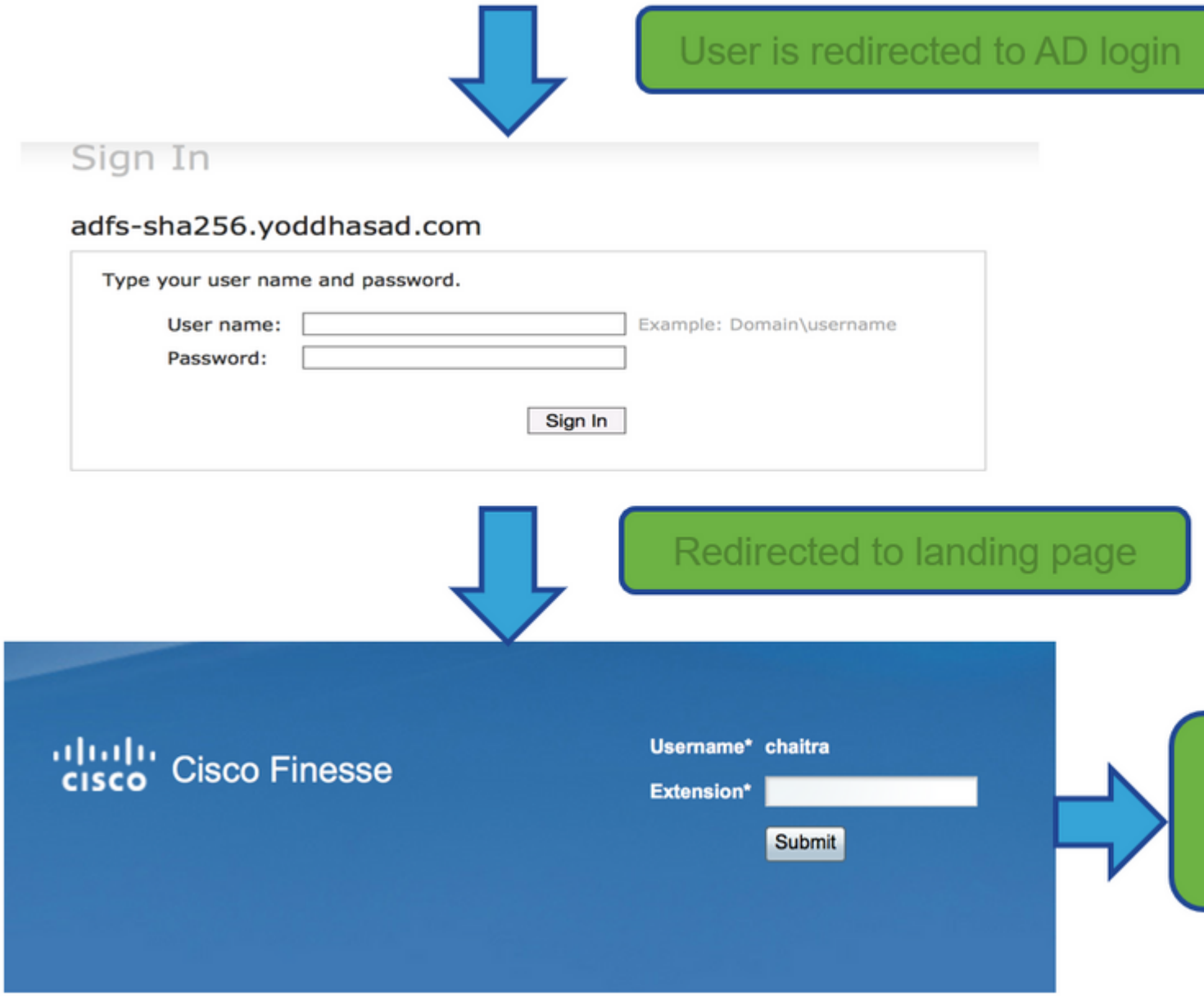
CCXç®¡ç†â€” å¯¯ç”¨SSO



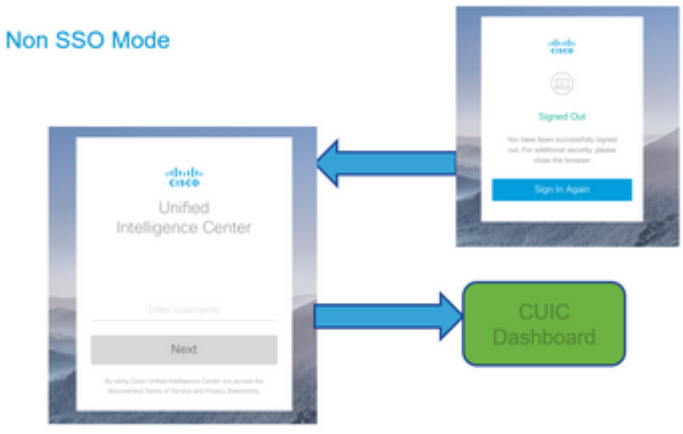
Finesseç™»å½• â€” é€šSSO



Finesseç™»å½• â€” å¯¯¨SSO

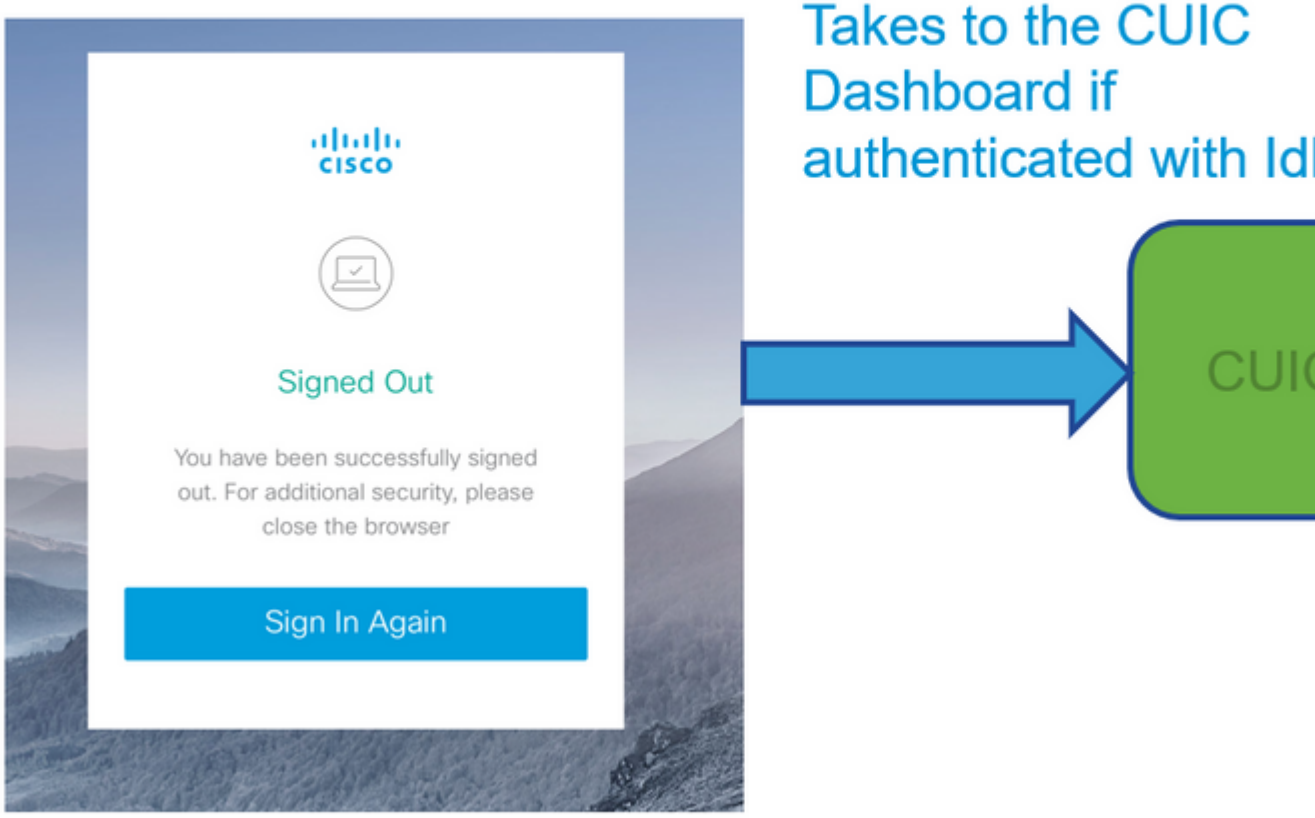


CUIC â€” é ž SSO



CUIC â€” å ¯ç ¨ 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

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。