

# مادختساب يداخال لوخدلا ليجست نيوكت AD FS 2.0 و CUCM

## تايوتحمل

---

[قمدقمل](#)

[قيساسال تابلطتمل](#)

[تابلطتمل](#)

[قمدختسمل تانوكمل](#)

[قيساسا تامولعم](#)

[Windows مداخ يلع هتبيثت و AD FS 2.0 ليزنت](#)

[Windows مداخ يلع AD FS 2.0 نيوكت](#)

[CUCM فيرعت تانايب ليزنت / CUCM يلل IDP فيرعت تانايب داريتسا](#)

[تابلطتمل دعاوق عاشن و AD FS 2.0 مداخ يلل CUCM فيرعت تانايب داريتسا](#)

[SSO رابتخال ليغشت و CUCM يلع SSO نيكمت اهان](#)

[اهجالص او عاطخال افاشكتسا](#)

[عاطخال جيحصت يلل SSO تالجتس نييعت](#)

[داخال قمدخ مسانع ثجبل](#)

[Federation قمدخ مسان و DoWithout Certificate](#)

[IDP و CUCM مداوخ نيي نمازتم ريغ تقولا](#)

[قلمص تاذا تامولعم](#)

---

## قمدقمل

Cisco Unified (SSO) يداخال لوخدلا ليجست نيوكت هتبيثت دنتمسمل اذه فصوي  
Active Directory داخال قمدخ و Cisco Unified Communications Manager.

## قيساسال تابلطتمل

### تابلطتمل

هتبلاتل عيضاوملاب هفرعم كيدل نوكت نأب Cisco يصوصت:

- Cisco Unified Communications Manager (CUCM) جم انرب
- Active Directory (AD FS) داخال قمدخ هتبيثت هفرعم

نيوكتلا اذه كملزي، ربتخمل هتبيثت ي ف SSO نيكمتل:

- Windows Server عم AD FS تبتتمل
- LDAP هتبيثت عم CUCM
- سيسايقلا CCM Super Users رود ديدحت عم هتبيثت سمل

## ةمدختسمل اتانوكملا

ةيلالاتل ةيدامل اتانوكملا وجماربل اتارادصلإ لىل دننستسمل اذه يف ةدراول تامولعمل دننست

- Windows Server م AD FS 2.0
- CUCM 10.5.2

ةصاخ ةيلعمل ةئيبل يف ةدوجوملا ةزهجال نم دننستسمل اذه يف ةدراول تامولعمل عاشنإ م تناك اذإ. (يضارتفا) حوسم نيوكتبل دننستسمل اذه يف ةمدختسمل ةزهجال عيمج تادب رمل لمتحمل ريثاتلل كمهف نم دكاتف، ليغشتل دي قكتكبش

## ةيساسأ تامولعمل

اضيأ تاوطخل اذه لمعت. Windows Server 2008 R2 م AD FS 2.0 ب صاخل اءارجل ري فوت م تي م Windows Server 2016 لىل AD FS 3.0 م

## Windows مداخل لىل ةتبيثتو AD FS 2.0 ليزنت

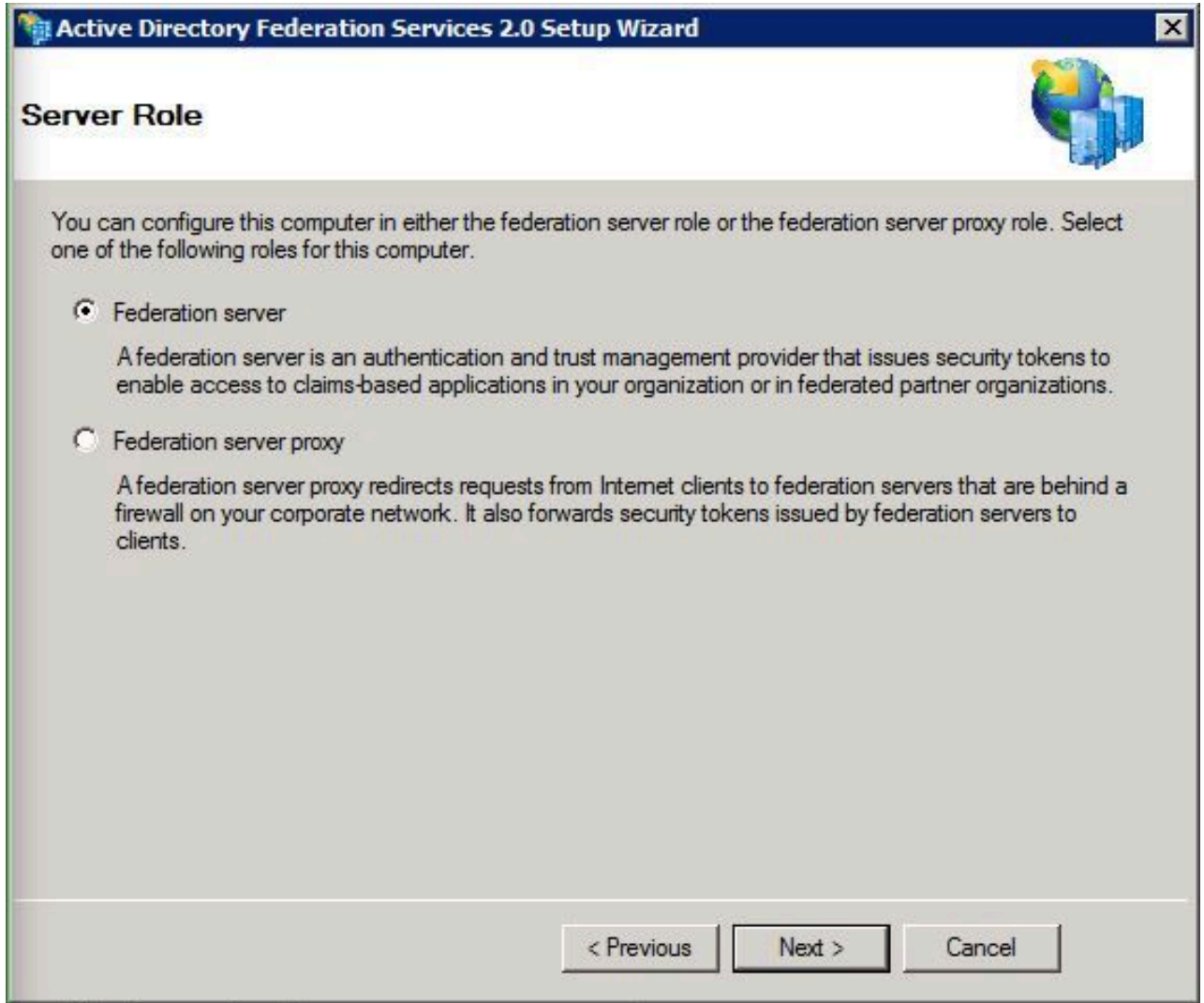
1. ةوطخل [AD FS 2.0 ليزنت](#) لىل لقتنا.

Windows مداخل لىل اءانتسا بسانملا ليزنتل ديحت نم دكات. 2. ةوطخل

Windows مداخل لىل هل ليزنت م ت يذل فللمل لقتنا. 3. ةوطخل

تتبيثتلا ةعباتم. 4. ةوطخل

Federation Server رتخأ، ةبلاطملا دنع. 5. ةوطخل



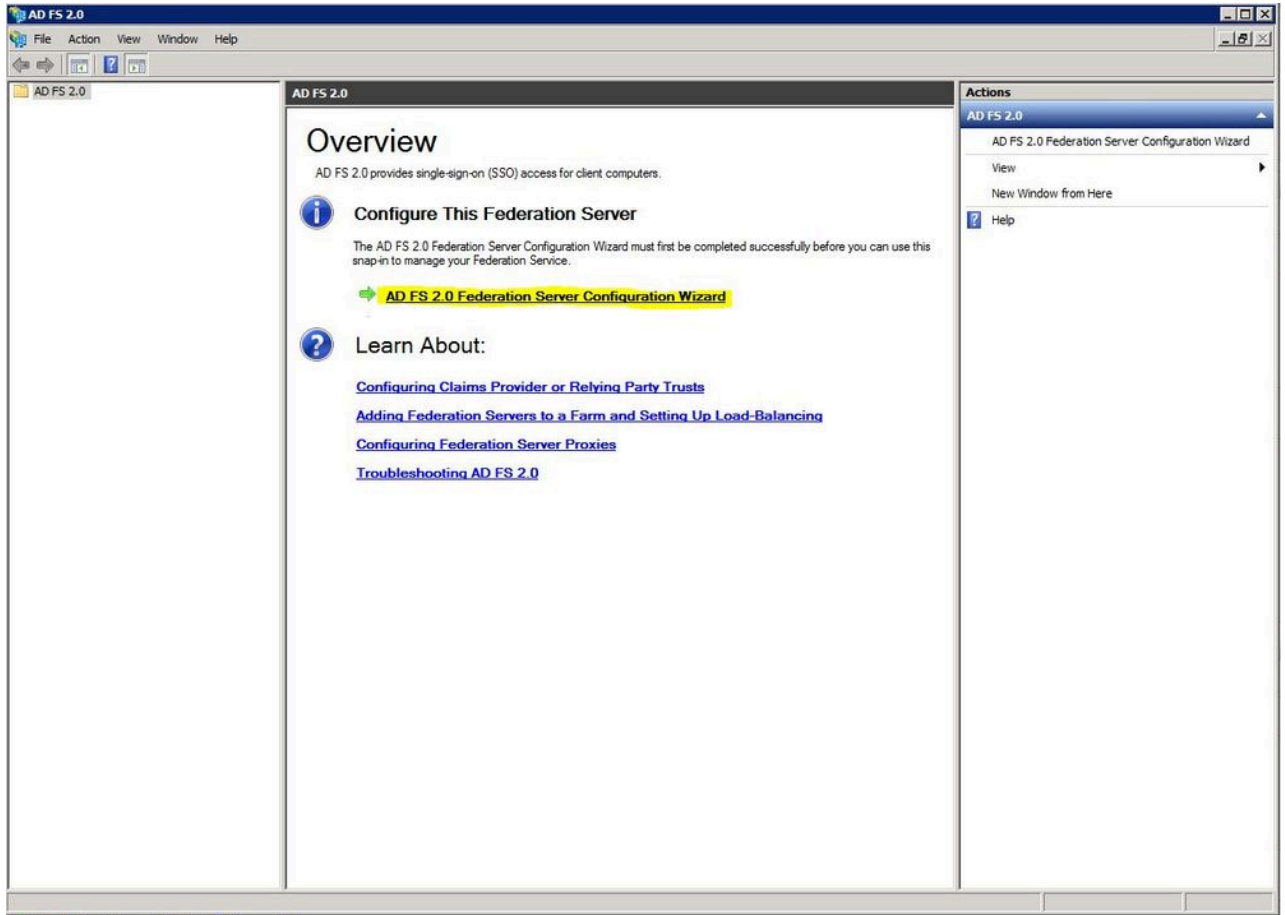
ءاهن ا قوف رقنا ،كلذ متي نأ درجمب .ايئاقولت تايعبتللا ضع ب تيبثت متي .6 ةوطخللا

ضع ب ةفاضل ا ل اجاتحت ،كب صاخلا مداخللا لىل ع اتبثم AD FS 2.0 كيدي دل حبصأ نأ دعب نأللا ةئيهتللا

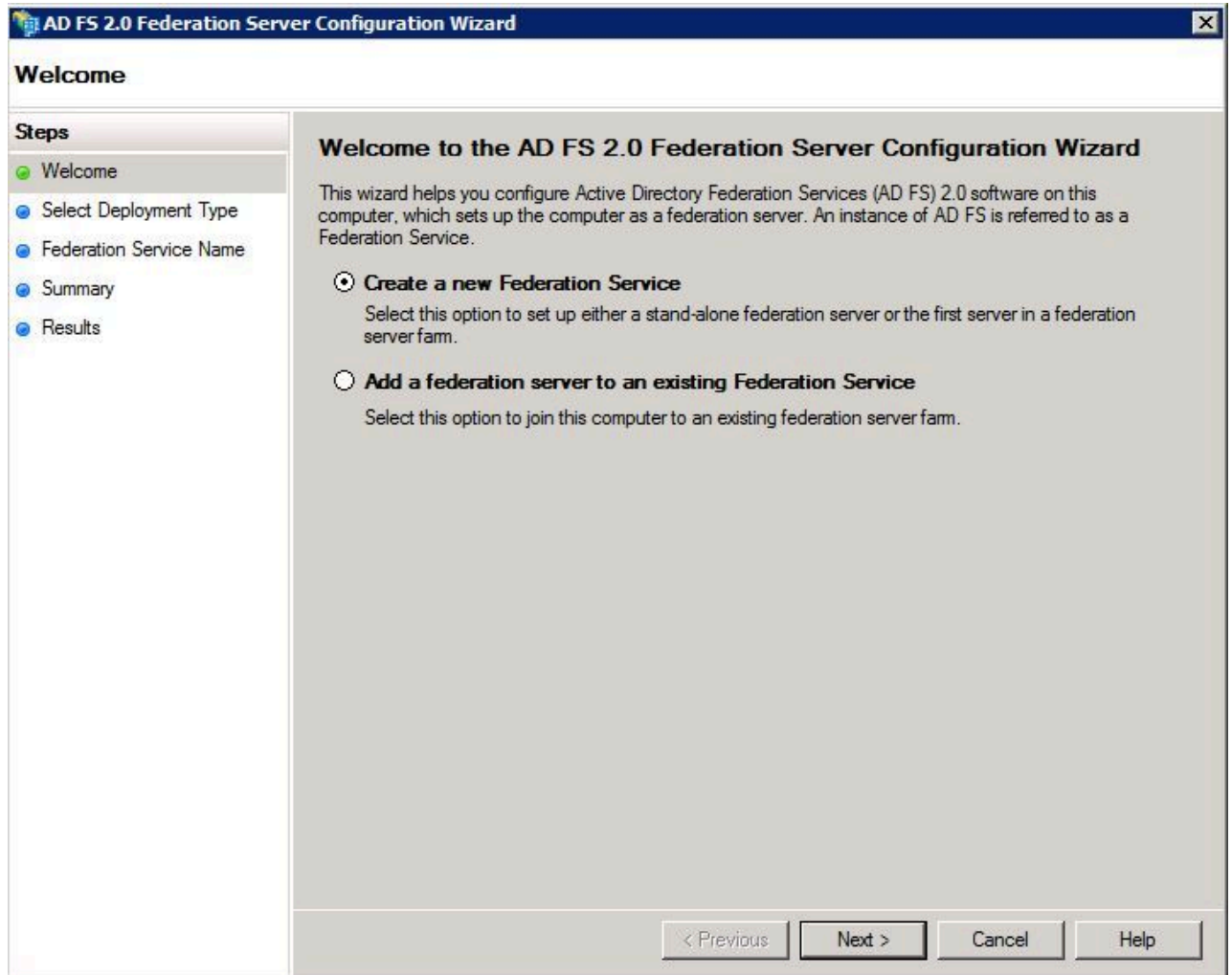
## Windows مداخل لىل ع AD FS 2.0 نيوكت

شحبلاو ادب لىل ع رقنا ،تيبثتلا دعب ايئاقولت AD FS 2.0 ةذفان حتفت مل اذا .1 ةوطخللا ايودي اهحتفل AD FS 2.0 ةرادل نع

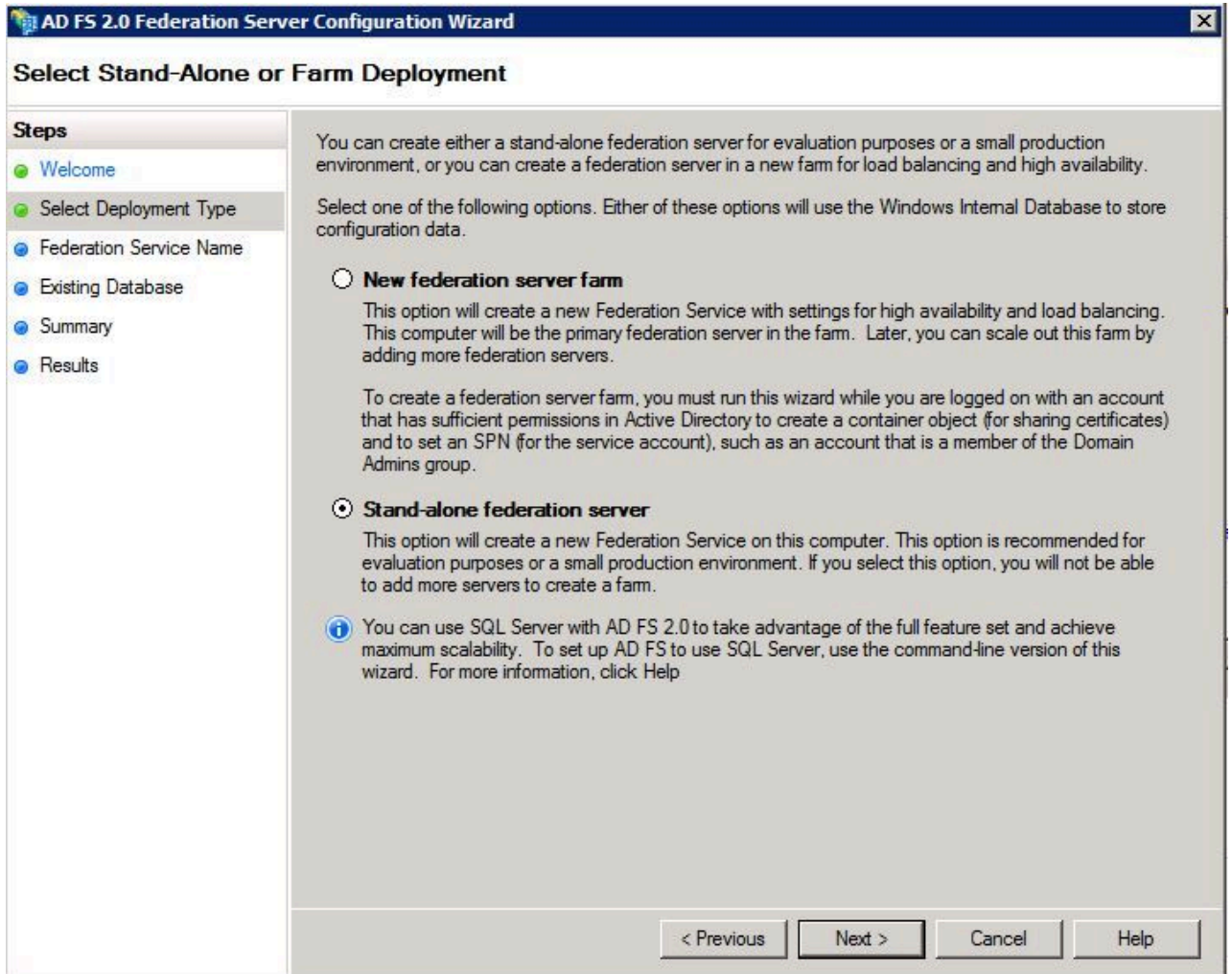
AD FS 2.0 داحتاللا مداخل نيوكت جلاع م رتخأ .2 ةوطخللا



ةديج داحتإ ةمدخ ءاشنإ قوف رقنا ،كلذ دع ب .3 ةوطخلا



اي فاك لقتسمل دا حتال م داخ نو كي ، تائيب ل م طعم ي ف . 4 ة و ط خ ل ا



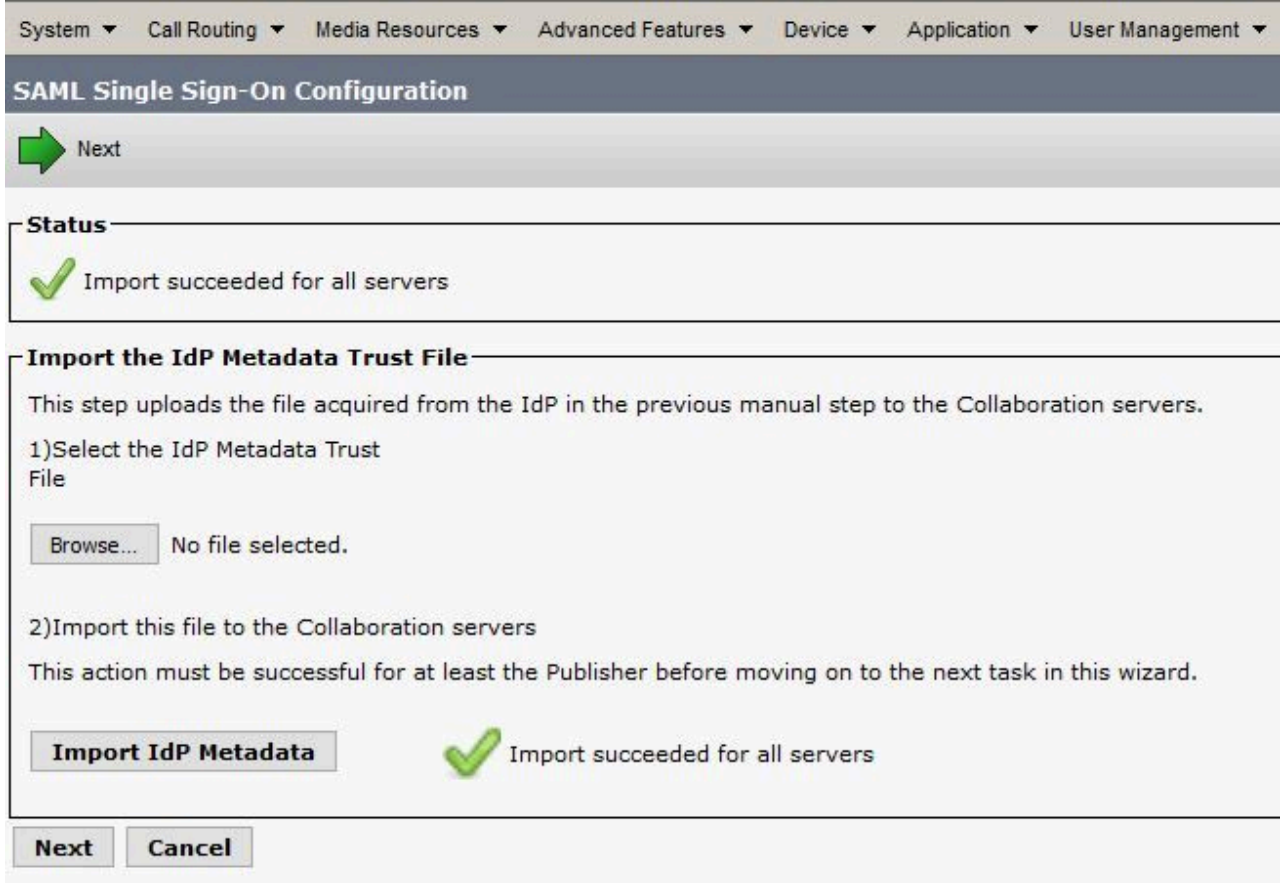
يدلنا على الخطوات التي يجب اتخاذها عند إعداد خادم AD FS 2.0. يمكنك إما إعداد خادم AD FS 2.0 كخادم مستقل، أو إعداد خادم AD FS 2.0 كخادم في مزرعة. يمكنك أيضًا إعداد خادم AD FS 2.0 باستخدام SQL Server. للحصول على مزيد من المعلومات، انقر فوق مساعدة.



ي.لالتا قوف رونا كلذل، 1 ةوطخلال في فيرعتالتا تانايب

تانايب داريتسا قوف رونا > 1 ةوطخلال نم xml. ديحت > ضارعتسا قوف رونا. 6 ةوطخلال  
فيرعت IdP.

ةحجان تناك داريتسالال ةيلمع نأ لىل ةلاس رر شت. 7 ةوطخلال



ي.لالتا (ال) Next قوف رونا. 8 ةوطخلال

لىل جاتحت، CUCM لىل ةدروتسم ال IDp فيرعت تانايب لىل ةتلصح نأ دعب نآل. 9 ةوطخلال  
كب صاخال فرعلم لىل CUCM فيرعت تانايب داريتسا

ةقثال فيرعت تانايب فلم ليزنت قوف رونا. 10 ةوطخلال

ي.لالتا (ال) Next قوف رونا. 11 ةوطخلال

دلجم لىل تايوتحمل جرختساو Windows مداخ لىل zip. فلم لقنا. 12 ةوطخلال

## ءاشن و AD FS 2.0 مداخ لىل CUCM فيرعت تانايب داريتسا تابلالاطم ال دعاوق

AD FS 2.0 ةراد نع ثحبل او ءب لىل رونا. 1 ةوطخلال

اهب قوٹوم دامتعا ةهجة فاضا: بولطم قوف رونا. 2 ةوطخلال



✎ ىرخأ ةرم اهحتفو ةذفانللا قالغإ ىلإ جاتحت ،راىخللا اذه ىرت مل اذا :ةظحالم

ءءب قوف رقنا ،ءامتعالا ةهج ةقث ةفاضل جلاءم حتف متى نأ ءرءمب 3. ةوطخللا

ءءء 12. ةوطخللا ىف اهءارءتساب تمق ىتلا XML ءافلما ءارىتسإ ىلإ جاتحت ،انه 4. ةوطخللا XML رءءاو ءلءملا ءافلما ىلإ ضرءتساو فلما نم لوعملا فرطلا لوء ءاناىب ءارىتسإ كءرشانل

✎ هىلع SSO ماءءتسإ ءىرت ءءوم نواعء مءاء ىلأ ةقءباسللا ءاوطخللا مءءتسأ :ةظحالم

The screenshot shows the 'Add Relying Party Trust Wizard' dialog box, specifically the 'Select Data Source' step. The title bar reads 'Add Relying Party Trust Wizard'. On the left, there is a 'Steps' pane with the following items: 'Welcome', 'Select Data Source' (highlighted), 'Specify Display Name', 'Choose Issuance Authorization Rules', 'Ready to Add Trust', and 'Finish'. The main area contains the following text: 'Select an option that this wizard will use to obtain data about this relying party:'. There are three radio button options: 1. 'Import data about the relying party published online or on a local network'. Below this is the text: 'Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata online or on a local network.' and a text box for 'Federation metadata address (host name or URL):' with an example: 'Example: fs.contoso.com or https://www.contoso.com/app'. 2. 'Import data about the relying party from a file'. Below this is the text: 'Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file.' and a text box for 'Federation metadata file location:' containing the path 'C:\Users\Administrator\Desktop\SPMetadata\_1cucm1052.sckiewer.lab.xml' and a 'Browse...' button. 3. 'Enter data about the relying party manually'. Below this is the text: 'Use this option to manually input the necessary data about this relying party organization.' At the bottom, there are four buttons: '< Previous', 'Next >', 'Cancel', and 'Help'.

(ىللاءلا) Next قوف رقنا 5. ةوطخللا

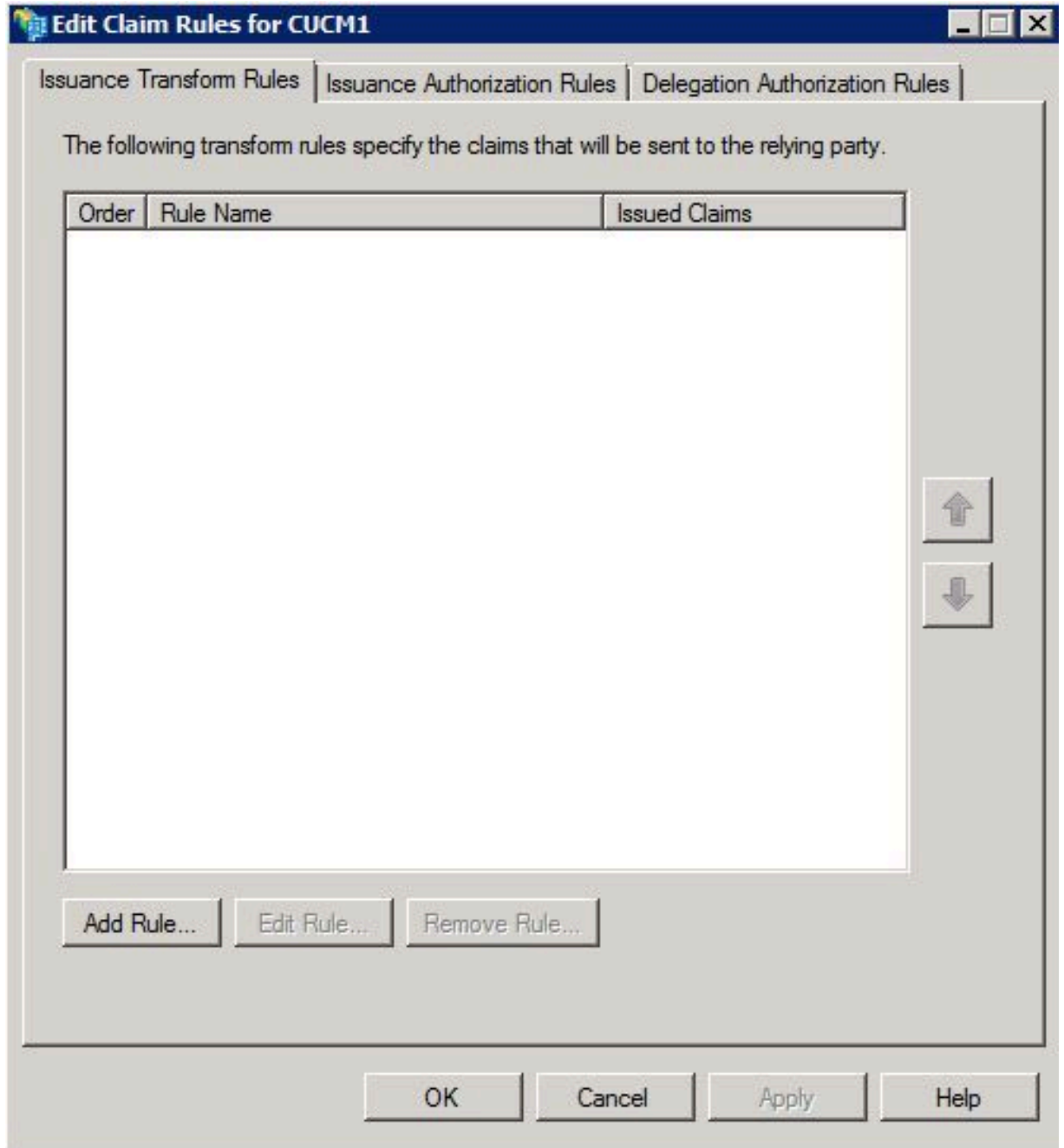
كءلء ءعب رقناو ضرءللا مسا رءء 6. ةوطخللا

قوف رقناو هءه ءامتعالا ةهج ىلإ لوصولاب نىمءءتسمللا عىمءل ءامسللا رءءأ 7. ةوطخللا ىللاءلا

ةىنءا ءلءل ءعب ءقءقء 8. ةوطخللا

ءءاوق رىءءء "راوءللا عءرم ءءفءب تمق كءنأ نم ءكأء ،ءشاشللا هءه ىلع 9. ةوطخللا قالغإ قوف رقنا مءء ،قىقءءلل جلاءملا قالغإ ءنء هءه لوعملا فرطلا ةقءل "ءبلاءملا

تابل اطملا دعاق ريرحت راطل ا حت ف متي .10 ةوطخل



ةدعاق ةفاضل قوف رقنا ، راطل ا اذ ف .11 ةوطخل

قوف رقنا و تابل اطملا LDAP تامس لاسرا رتخأ ، ةبلاطملا ةدعاق بلاق ل .12 ةوطخل  
يلال

ةبلاطملا ةدعاق مسال NameID لخدأ ، ةيلال ةحفصل ف .13 ةوطخل

تامسل نل نل Active Directory رتخأ .14 ةوطخل

ةمس LDAP ل ل SAM-account-name رتخأ .15 ةوطخل

ةرداصل ةبلاطملا عون ل id لخدأ .16 ةوطخل

ايودي هلاخدا بجي - ةلدسنملا ةمئاقلا يف ارايخ سي ل ديرفلا فرعمال: ةظحالم

**Add Transform Claim Rule Wizard**

**Configure Rule**

**Steps**

- Choose Rule Type
- Configure Claim Rule

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

Claim rule name: NameID

Rule template: Send LDAP Attributes as Claims

Attribute store: Active Directory

Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute	Outgoing Claim Type
	SAM-Account-Name	uid
▶*		

< Previous Finish Cancel Help

ءاهن إ قوف رقنا 17. ةوطخل

ىرخأ ةرم ةدعاق ةفاضل قوف رقنا .نآلا ىل وءالا ةدعاقلا تهتنا 18. ةوطخل

ةصصخم ةدعاق مادختساب تابللاطملا لاسرا رتخأ 19. ةوطخل

ةبلاطم ةدعاق مسا لخدأ 20. ةوطخل

صنلا اذه قصل، ةصصخملا ةدعاقلا لقح يف 21. ةوطخل

```
ج: [عونلا] == http://schemas.microsoft.com/ws/2008/06/identity/windowsAccountName]
=> رادصلا = http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/nameid
ردصم = c.Issuer, OriginalIssuer = c.OriginalIssuer, ةمقلا = c.Value, ValueType =
c.ValueType, Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/nameid-
format:transient, خاصئاصخ["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/namequalifier"
= http://ADFS_FEDERATION_SERVICE_NAME/com/adfs/service/trust",
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier"] =
"CUCM_ENTITY_ID");
```

ميرقلا لىل CUCM\_ENTITY\_ID و AD\_FS\_SERVICE\_NAME ريغت نم دكأت 22 ةوطخل  
ةبسانملا

روثعلل تاوطخلل عابتا كنكمي، AD FS ةمدخ مسا نم ادكأت م نكت مل اذا: ةظحالم  
فيرعت تانايب فلم يف لوألا رطسلا نم CUCM نايف فرعم بحس نكمي. هيلع  
CUCM. اذك ودي فلملا نم لوألا رطسلا لىل نايف فرعم دجوي  
نم بسانملا مسقلا يف ةرطسما ةميرقلا لاخدا بجي. entityID=1cucm1052.sckiewer.lab.  
ةبلاطملا ةدعاق

**Add Transform Claim Rule Wizard**

**Configure Rule**

**Steps**

- Choose Rule Type
- Configure Claim Rule

You can configure a custom claim rule, such as a rule that requires multiple incoming claims or that extracts 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 2.0 claim rule language.

Claim rule name: CUCM SSO Custom Rule

Rule template: Send Claims Using a Custom Rule

Custom rule:

```
=> issue (Type =  
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier",  
Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value =  
c.Value, ValueType = c.ValueType, Properties  
["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"] =  
"urn:oasis:names:tc:SAML:2.0:nameid-format:transient",  
Properties  
["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/name  
qualifier"] =  
"http://win2k8.sckiewer.lab/adfs/com/adfs/service/trust", Properties  
["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spna  
mequalifier"] = "1cucm1052.sckiewer.lab");
```

[More about the claim rule language...](#)

< Previous Finish Cancel Help

ءاهن قوف رقنا 23 ةوطخل

OK قوف رقناو 24 ةوطخل

هيلع SSO مادختسا يونت دحوم نواعت مداخ يأل تابلاطملا دعاوق رفوت مزلي: ةظحالم

## SSO رابتخا ليغشت و CUCM لىل SSO نيكمت ءاهن


CUCM لىل عوجرلا كنكمي، لماك لكشب AD FS مداخ ةئيهت دعب نآلا 1 ةوطخل

بيءاهنلا نيوكتلل ءحفص يف تفقوت دقل 2 ةوطخل

**SAML Single Sign-On Configuration**

[Back](#)

**Status**


 The server metadata file must be installed on the IdP before this test is run.

**Test SSO Setup**

This test verifies that the metadata files are correctly configured and will allow SSO to start up on the servers. This test can be run on a

1) Pick a valid username to use for this test

You must already know the password for the selected username.  
This user must have administrator rights and also exist in the IdP.

 Please use one of the Usernames shown below. Using any other Username to log into the IdP may result in administrator lockout.

Valid administrator Usernames

sckiewer

2) Launch SSO test page

[Run SSO Test...](#)

[Back](#) [Cancel](#)

رقن او يسايق لل CCM Super Users رود دي دحت مت يذلا يئاهن لل مدخت سمل دح. 3 ةوطخ لل SSO... راب تخ ل يغشت قوف

تاناي ب لخدأو، ةقث ب نمل تاراط ل اب حم سي كب صاخ لل ضرعت سمل نأ نم دكأت. 4 ةوطخ لل رمال هجوم يف كب ةصاخ لل دامتعالا

Test SAML - Firefox Developer Edition

<https://1cucm1052.sckiewer.lab:8443/ssosp/pages/TestSSO.jsp>

## SSO Test Succeeded!

Congratulations on a successful SAML SSO configuration test. Please close this window and click "Finish" on the SAML configuration wizard to complete the setup.

[Close](#)

ءاهن مت، ةقث ب نمل ةذفان لل لعل قالغ رقن. 5 ةوطخ لل

SSO نيكمت متي، بيولا تاقىب طتل ةريصق لىغشت ةداعإ دعب 6. ةوطخل

## اهحال صإو ءاطخال افاشك ت سا

ءاطخال احيصت ىلإ SSO تالجس نييعت

ب صاخلا CLI يف رمالا اذه لىغشت كىل ع بجي، ءاطخال احيصت ىلإ SSO تالجس نييعت ل  
CUCM: set samltrace level debug

Cisco SSO وه تالجس ل ءومجم مسا RTMT. ن سSO تالجس لىزنن نكمي

داحتالا ءمدخ مسا نع شحبلا

AD FS 2.0 ءرادإ نع شحبلا ءدب قوف رقنا، داحتالا ءمدخ مسا ىل ع روثلل

- داحتالا ءمدخ صئاصخ رىرت قوف رقنا
- Federation ءمدخ مسا نع شحبا، "ماع" بىوبتلا ءمالع يف كدوج وءانثأ

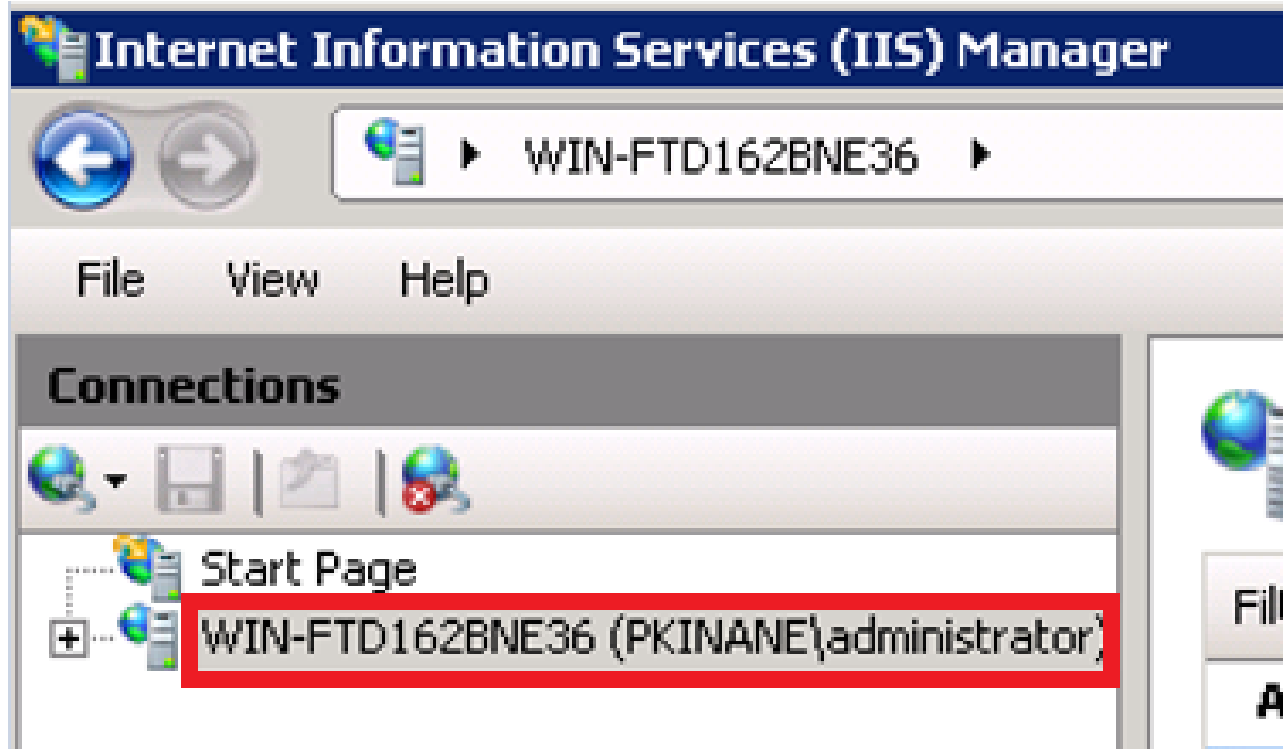
Federation ءمدخ مسا او DoWithout Certificate

ءديج ءداهش ءاشنإ ىلإ جاتحت كنإف، AD FS نىوكت جلاعم يف هءه أطلال ءلاس ر تملتسا إذا

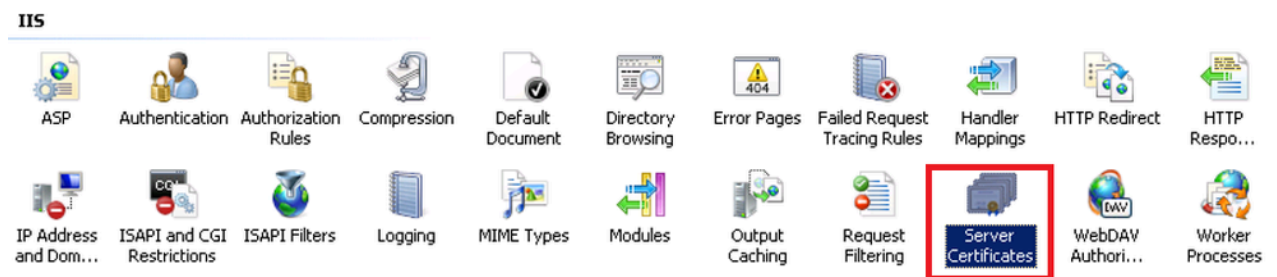
مسا اهل ءدحمل ءداهش ل نأل داحتالا ءمدخ مسا دىدحتل ءدحمل ءداهش ل مادختسا رذعتي  
ىمس (ءمالع الب ءوضوم مسا نوب ىرخأ ءداهش دح). (مسا لىصق) ءمالع الب ءوضوم  
ىرخأ ءرم لواح م، (رىصق

(IIS) ت نرتنإل ءاملعم ءمدخ ءرادإ حتفا م، IIS نع شحبلا ءدب قوف رقنا 1. ةوطخل





مداخل تاداهش ىلع رقنا 3. ةوطخلا



ايتاذ ةعقوم ةداهش عاشن رقنا 4. ةوطخلا



## Actions

Import...

Create Certificate Request...

Complete Certificate Request...

Create Domain Certificate...

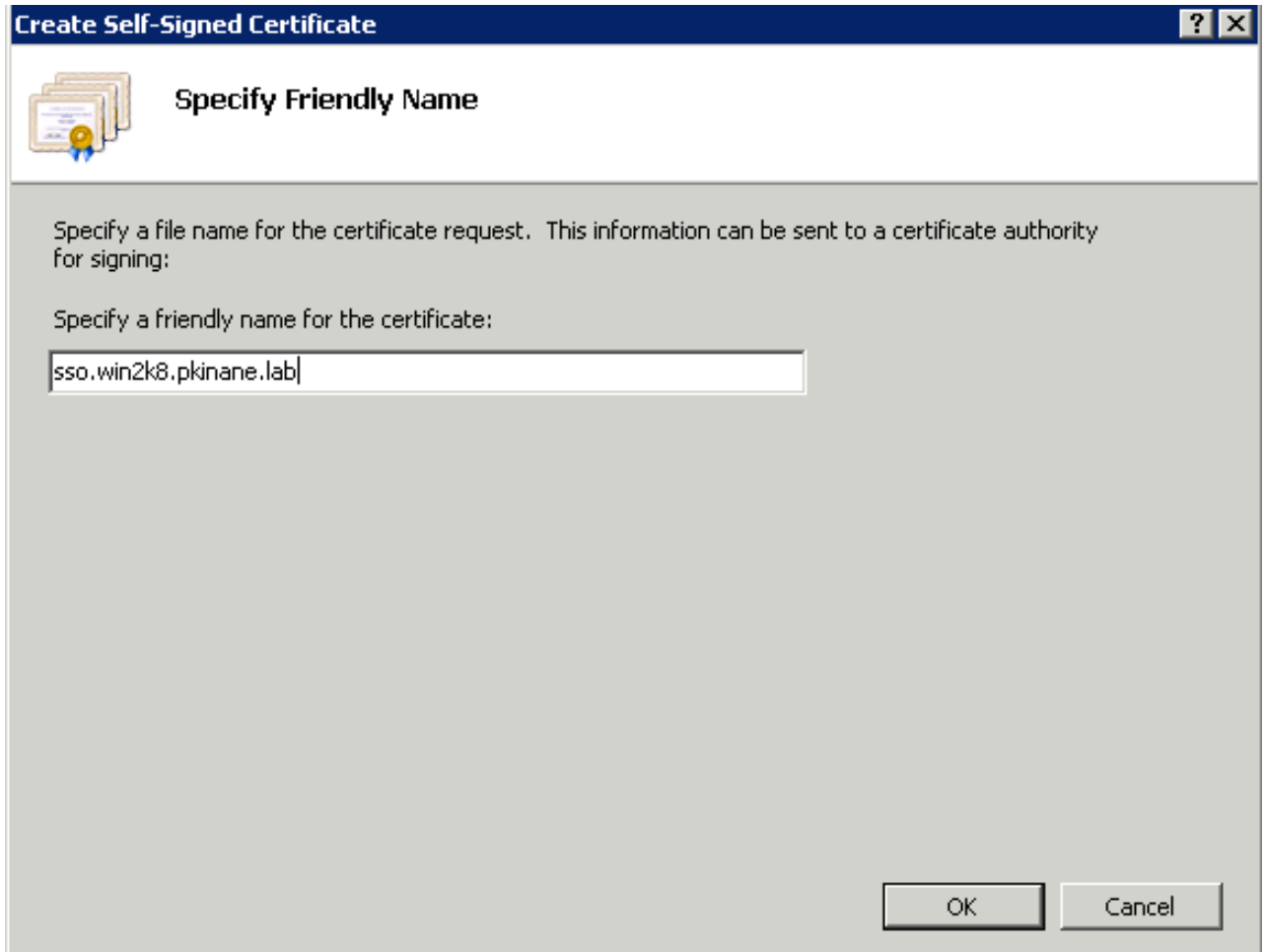
Create Self-Signed Certificate...



Help

Online Help

ةداهش لل راعتسمال مسالا لخدأ. 5 ةوطخال



## IDP و CUCM مداوخ نيب نم ازتم ريغ تقولا

Windows Server نيوكت ىل اجاتحت، CUCM نم SSO رابتخا ليغشت دنع أطخ اذه تملتسا اذا CUCM لثم NTP (مداوخ) مداخ سفن مادختسال.

ريدم نيب نم ازتم ريغ تقولا نوكتي ام دنع اذه ثدحي دقو. ةحل اص ريغ SAML ةباجتسا مق. نيم داخلا الك ىل ع NTP نيوكت نم ققحتلا اءارلا IDP مداوخ و Cisco نم ةدحوملا تالاصتالا هذه نم ققحتلل (CLI) رم اوألا رطس ةهجاو نم "NTP) ةكبشلا تقو لوكتورب ةلاح" ليغشتب Cisco Unified Communications Manager ىل ةلاحلا.

رابتخا اءارلا ىل اجاتحت، ةدحوملا ةححصلا NTP مداوخ ىل ع Windows Server يوتحي نأ درجمب هيوشت يوررضلا نم، تالاحلا ضعب ي فو. ةرمتسم ةلكشملا تناك اذا ام ةفرعمو رخا SSO [انه](#) ةيلمعلا كلت لوح ليصافتلا نم ديزملا. ديكأتل ةحص ةرتف

## ةلص تاذا تامولعم

- [Cisco Systems - تادنتس مل او ينقتلا معدلا](#)

