

# مادختساب يداخال لوخدلا ليجست نيوكت AD FS 2.0 و CUCM

## تايوتحمل

---

[قمدقمل](#)

[قيساسال تابلطتمل](#)

[تابلطتمل](#)

[قمدختسمل تانوكمل](#)

[قيساسا تامولعم](#)

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

[Windows مدخال يلع AD FS 2.0 نيوكت](#)

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

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

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

[اهخالص او عاخال افاشكتسا](#)

[عاخال احيصت يلل SSO تالجتس نييعت](#)

[داخال ا 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 كملزلي، ربتخمل هتبيثت ي SSO نيكمتل:

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

## ةمدختسمل اتانوكملا

ةيلالات ةيداملا اتانوكملا او جماربلا تارادصا اىل دن تسملا اذه يف ةدراولا تامولعمل دن تست

- Windows Server م AD FS 2.0
- CUCM 10.5.2

ةصاخ ةيلعمل ةئيب يف ةدوجوملا ةزهجالا نم دن تسملا اذه يف ةدراولا تامولعمل عاشن ا م تناك اذ ا . (يضا رتفا) حوسم نيوكتب دن تسملا اذه يف ةمدختسمل ةزهجالا عيمج اءب رما اىل لم تحملا ريثا لىل كمهف نم دكا ف ، ليغشتلا دي ق ك تكبش

## ةيساسا تامولعمل

اضيا تاوطخلا هذه لمعت . Windows Server 2008 R2 م AD FS 2.0 ب صاخلا اءرالا ريفوت م تي م Windows Server 2016 اىل م AD FS 3.0 م

## Windows مءاخ اىل عهت يثبت و AD FS 2.0 ليزنن

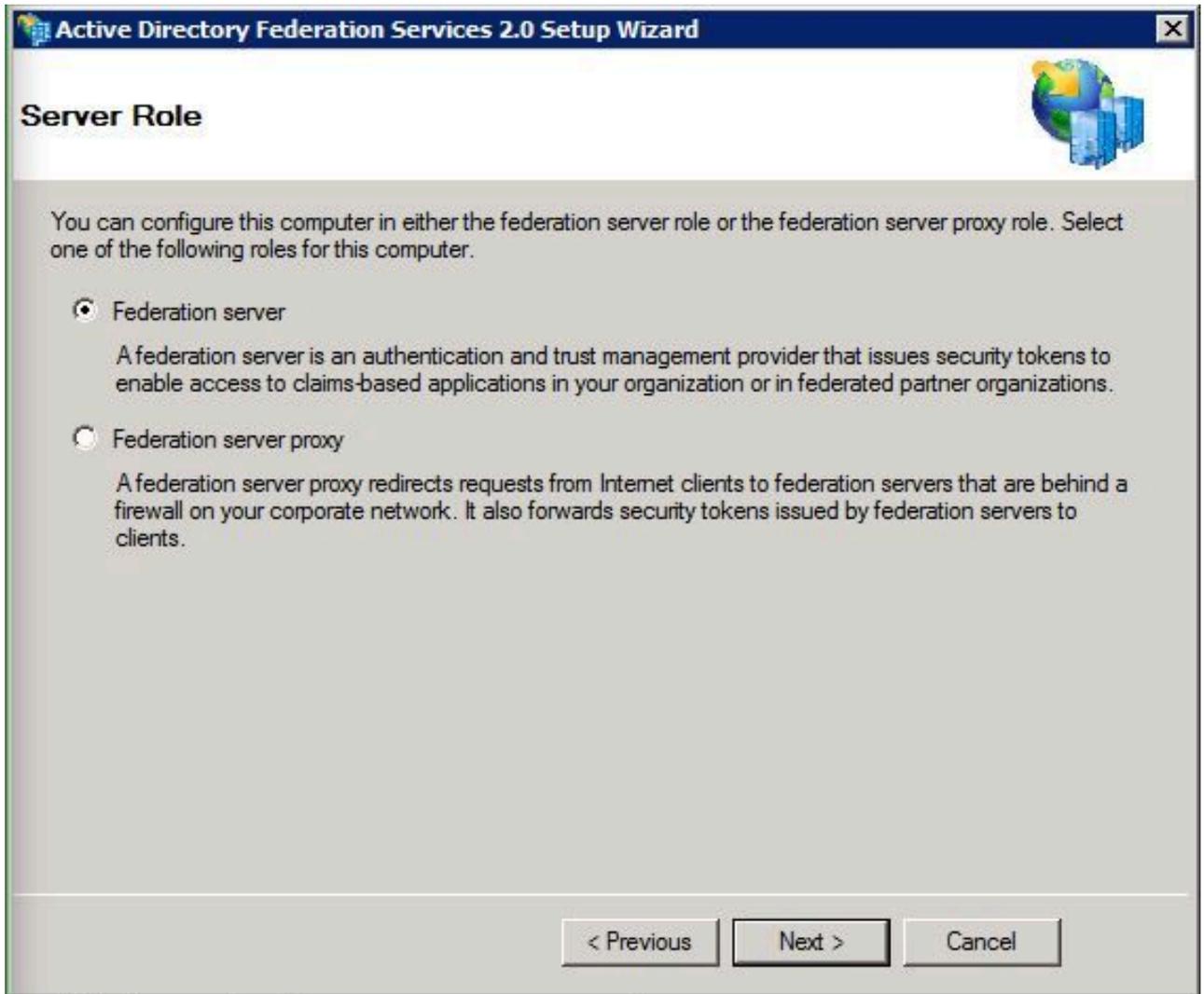
1. ةوطخلا [AD FS 2.0 ليزنن](#) اىل لقتنا .

Windows مءاخ اىل اءانتسا بسانملا ليزننلا ديحت نم دكا . 2. ةوطخلا

Windows مءاخ اىل هل ليزنن مء يذلا فلملا لقتنا . 3. ةوطخلا

ت يثبتلا ةعباتم . 4. ةوطخلا

Federation Server رءخا ، ةبلاطملا دن ع . 5. ةوطخلا



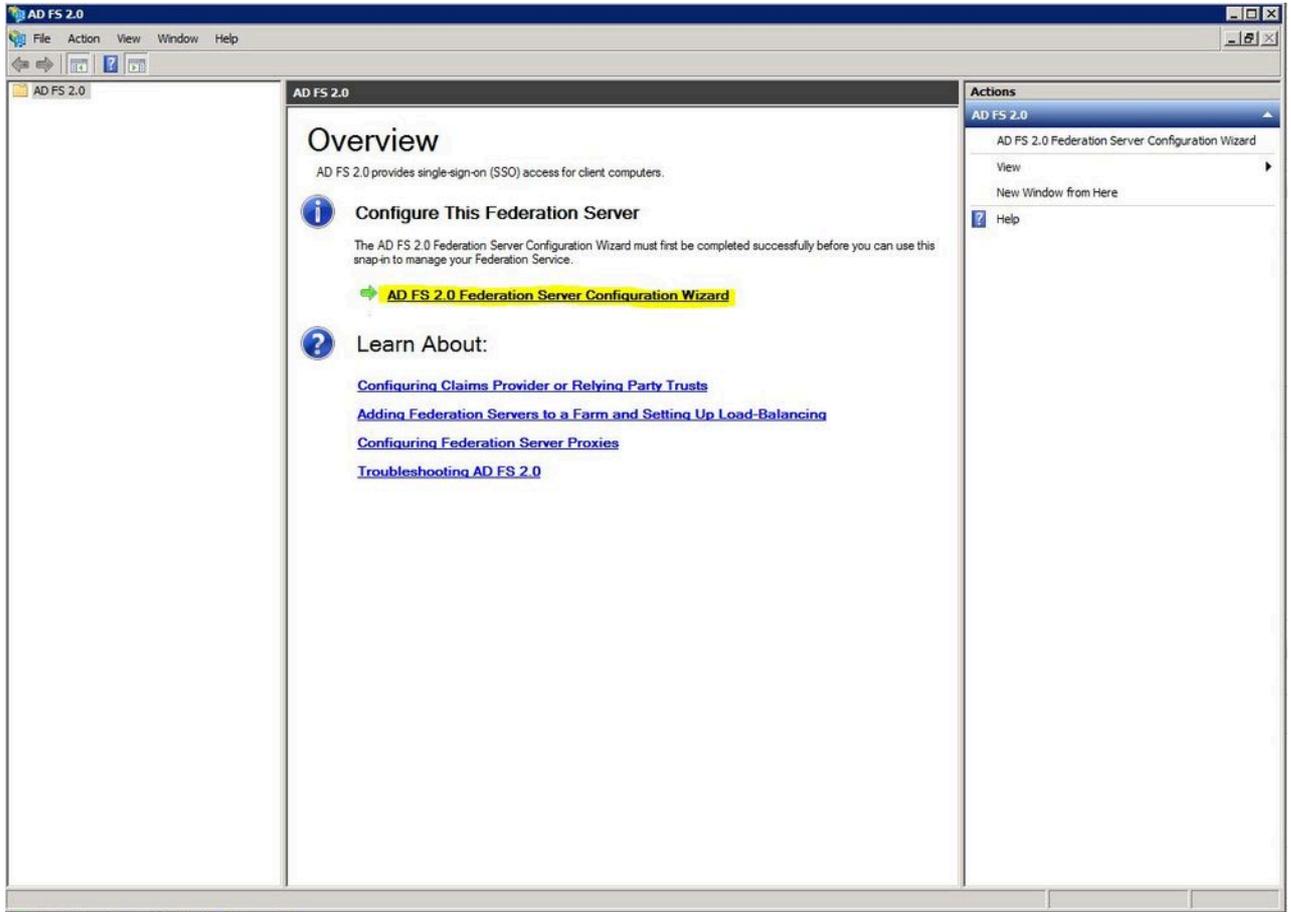
ءاهن ا قوف رقنا ،كلذ متي نأ درجم ب .ايئاقلت تايعبتلا ضع ب تيبثت متي 6 ةوطخلا

ضع ب ةفاضل ا ل اجاتحت ،كب صاخلا مداخل ا ل ع اتبثم AD FS 2.0 كيدي دل حبصأ نأ دع ب نألا ةئيهتلا

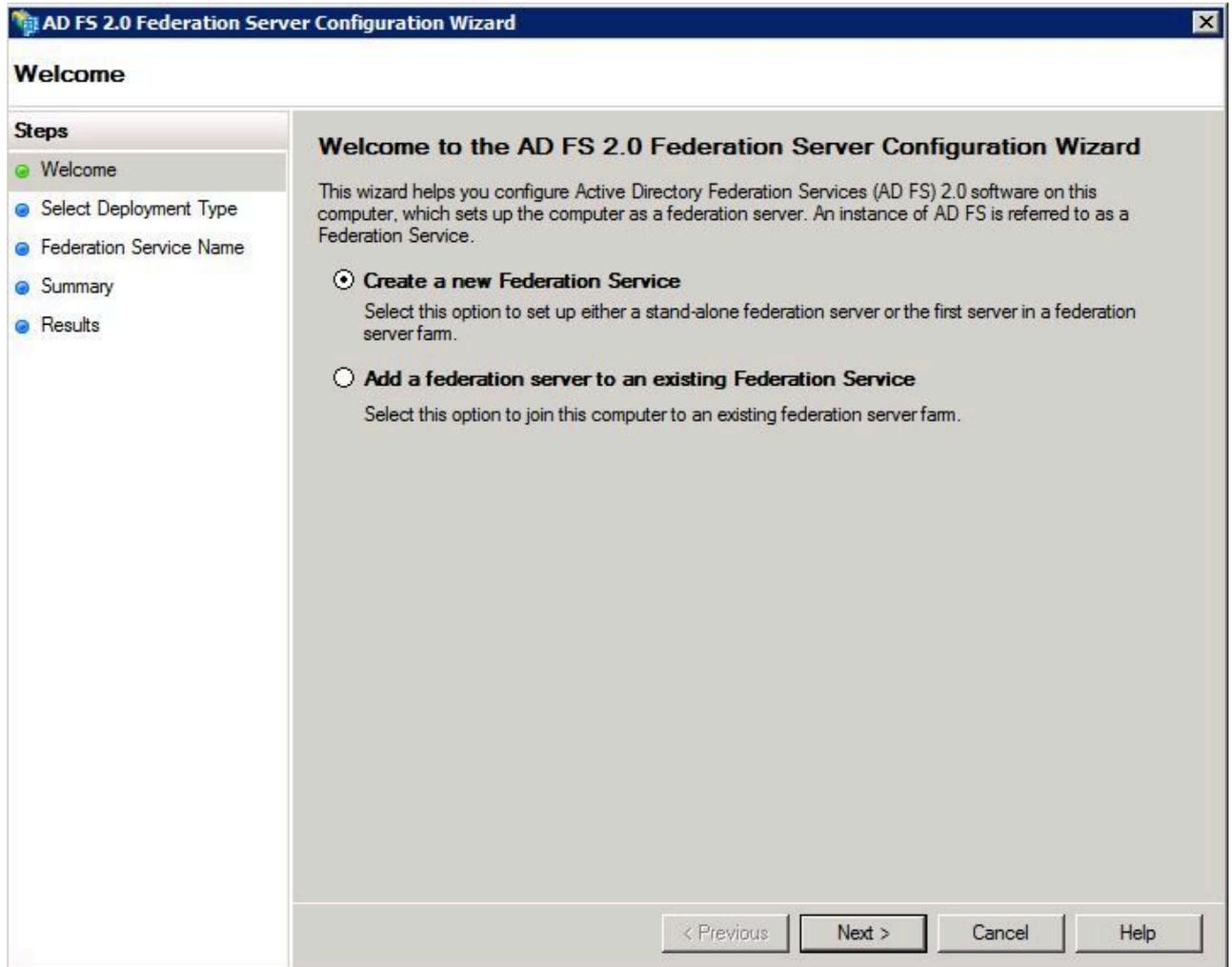
## Windows مداخل ا ل ع AD FS 2.0 نيوكت

شحبلاو عب ا ل ع رقنا ،تيبثتلا دع ب ايئاقلت AD FS 2.0 ةذفان حتفت مل اذا 1. ةوطخلا ايودي اهحتفل AD FS 2.0 ةراد ا نع

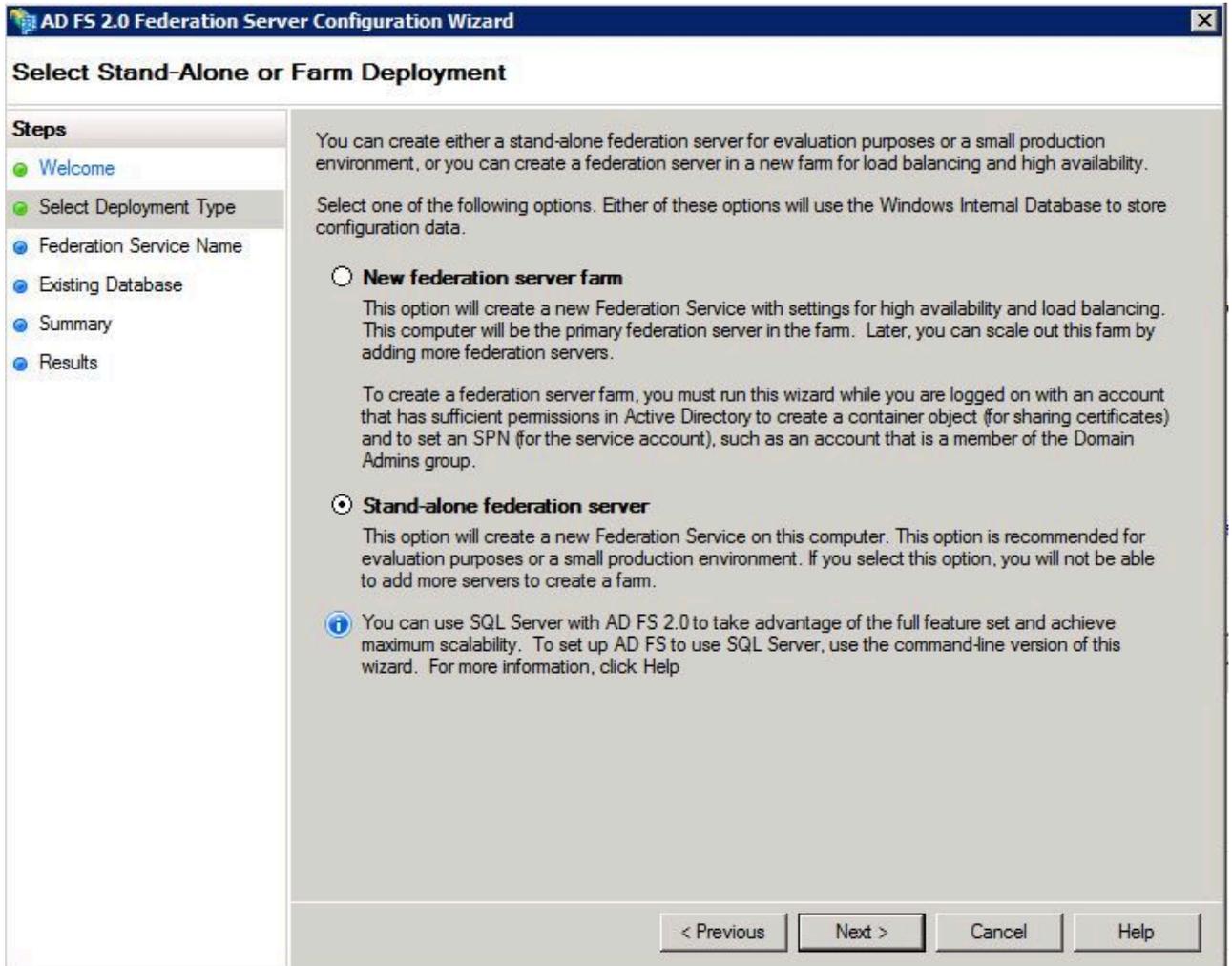
AD FS 2.0 داحتالا مداخل نيوكت جلاع م رتخأ 2. ةوطخلا



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



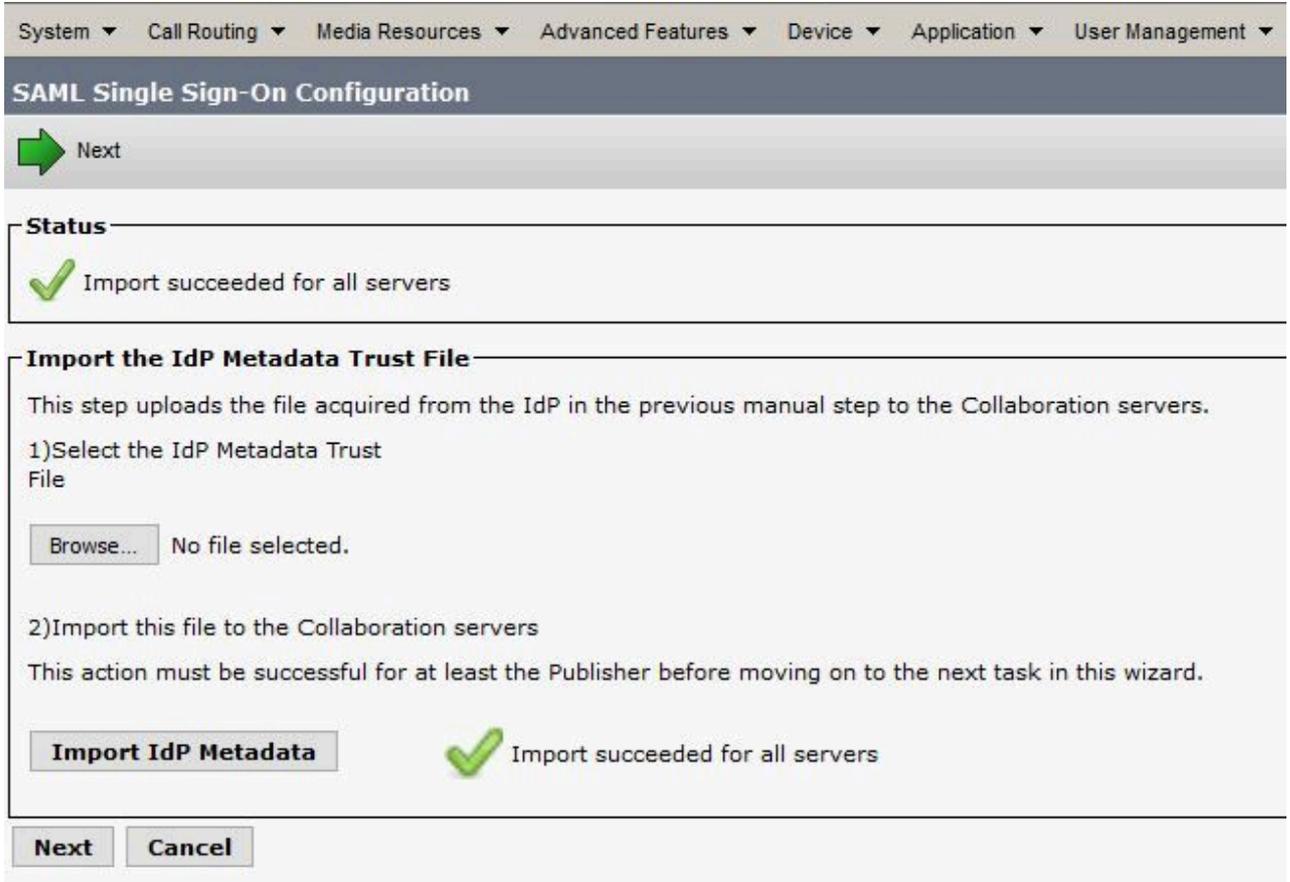
يدلنا على الخطوات التي يجب اتخاذها عند إعداد خادم AD FS 2.0. يمكنك إما إنشاء خادم AD FS 2.0 منفردًا، أو يمكنك إنشاء خادم AD FS 2.0 في مزرعة لتوزيع الحمل وتحقيق توافر عالٍ.



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 تايوتحملال جرختساو Windows مداخ لىل zip. فلم لقنا. 12 ةوطخلال

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

AD FS 2.0 ةرادل نع ثحبلال و ادب لىل رونا. 1 ةوطخلال

اهب قووثوم 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 ةهء ةقث ةفاضا جلاءم حتف متى نأ ءرءمب 3. ةوطخللا

ءءء 12. ةوطخللا ىف اهءارءتسا ب تمق ىتلا XML ءافلما ءارىتسا ىلإ جاتحت ،انه 4. ةوطخللا XML رءءاو ءلءملا ءافلما ىلإ ضرءتسا وءلم نم لوءءملا فرءلال لوء ءاناىب ءارىتسا ىلإ ءرءانل

✎ هىلء SSO مءءءتسا ءىرت ءءوم نواعء مءاء ىلأ ةقبا سلال ءاوطخللا مءءءتسا :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

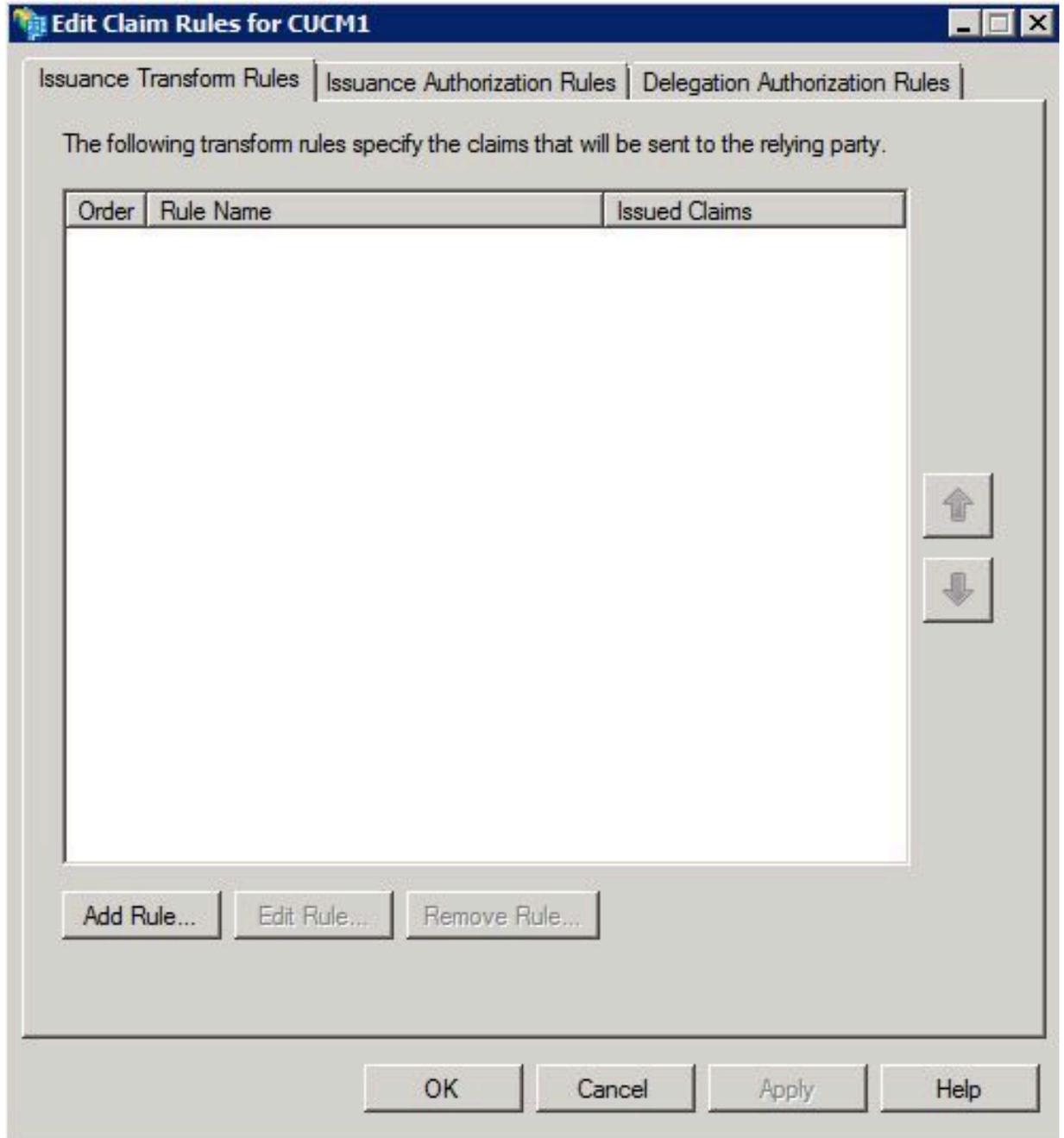
ءلء ءءب رقنا وءرءللا مسا رءء 6. ةوطخللا

قوف رقنا وءه ءامتعالا ةهء ىلإ لوءولاب نىمءءءتسا مءل ءىءءل ءامسا رءءأ 7. ةوطخللا ىللاءلا

ءىءناء ءلء ءءب ءقءقء 8. ةوطخللا

ءءاوق رىءءء "راءءللا ءءءفب تمق ءنأ نم ءءأءء ،ءشاشللا هءه ىلء 9. ةوطخللا قالغإ قوف رقنا مءء ،قىقءءللا ءلءءملا قالغإ ءنء هءه لوءءملا فرءلال ةقءل "ءبءللاءملا

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 اطمك 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 ترتخأ . 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: [عونل] == http://schemas.microsoft.com/ws/2008/06/identity/ windowsAccountName] => رادصلا [عونل] = http://schemas.xmlsoap.org/ws/2005/05/identity/cltarget/nameIdentifier",  
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 ىل AD\_FS\_SERVICE\_NAME و CUCM\_ENTITY\_ID ريغت نم دكأت 22 ةوطخلا  
ةبسانملا

روثعلل تاوطخلا 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  
اذهك ودبي فلملا نم لوألا رطسلا ىلع نايف فرعم دجوي CUCM.  
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/form  
at"] = "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 ةوطخلا

OK قوف رقناو 24 ةوطخلا

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

## SSO رابتخا ليغشت و CUCM ىلع SSO نيكمت ءاهن

CUCM ىل عوجرلا كنكمي، لماك لكشب AD FS مداخ ةئيهت دعب نآلا 1 ةوطخلا

بيءاهنلا نيوكتل ءحفص يف تفقوت دقل 2 ةوطخلا

**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 ةوطخل  
SSO... راب تخ ل يغشت قوف

تاناي ب لخدأو، ةقثب نمل تاراط ل اب حم سي كب صاخل ضرعت سمل نأ نم دكأت. 4 ةوطخل  
رمأل هجوم يف كب ةصاخل 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، ةقثب نمل ةذفان لل يلع قوالغ رقن. 5 ةوطخل

SSO نيكمت متي، بيولا تاقي بطلت ليري صق ليغشت اداعا دعب 6. ةوطخلا

## اهحال صاوا ءاطخالا فاشك ت سا

ءاطخالا حيحصت ىلإ SSO تالجس نييعت

ب صاخلا CLI يف رمالا اذه ليغشت كي لع بجي، ءاطخالا حيحصت ىلإ SSO تالجس نييعت ل  
CUCM: set samltrace level debug

Cisco SSO وه تالجس لاة وومجم مسا RTMT. نم SSO تالجس لي زنت نكمي

داحتالا ةمدخ مسا نع شحبالا

AD FS 2.0 ةرادا نع شحبالا و ادب قوف رقنا، داحتالا ةمدخ مسا ىلع روثعلل

- ...داحتالا ةمدخ صئاصخ ريرحت قوف رقنا
- Federation ةمدخ مسا نع شحبالا، "ماع" بيوبتالا ةمالع يف كدوج وءانثا

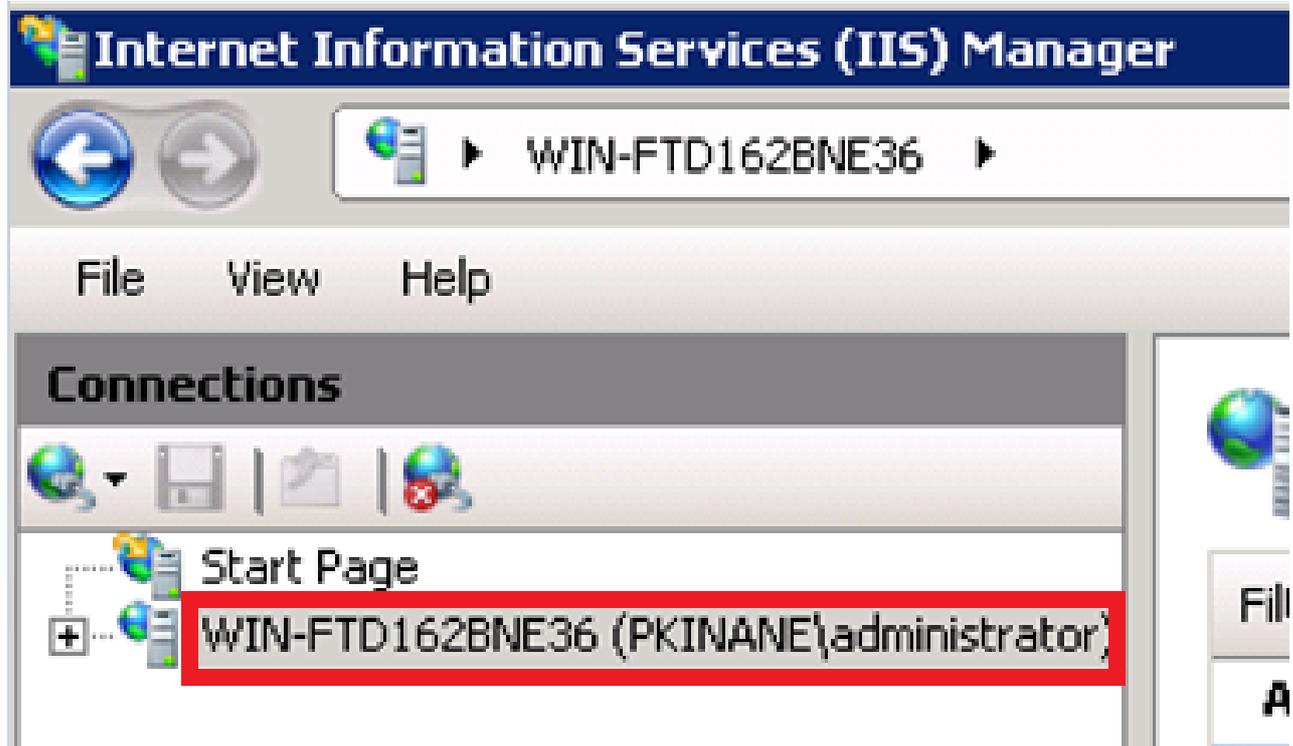
Federation ةمدخ مسا او DoWithout Certificate

ةديج ةداهش ءاشنا ىلإ جاتحت كنإف، AD FS نيوكت جلاعم يف هذء اطخالا ةلاس ر تملتسا إذا

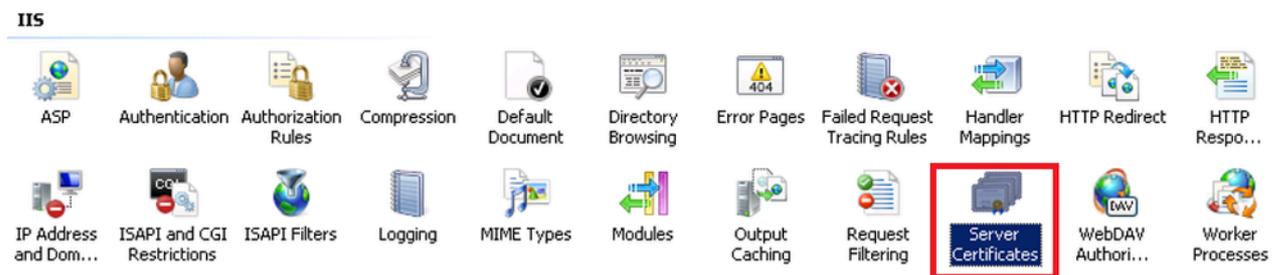
مسا اهل ةددحمل ةداهش ل نأل داحتالا ةمدخ مسا دي دحتل ةددحمل ةداهش ل مادختسا رذعتي  
ىمس (م) ةمالع ال ب عوضوم مسا نودب ىرخأ ةداهش ددح. (مسا ليري صق) ةمالع ال ب عوضوم  
ىرخأ ةرم لواح م، (يرى صق)

(IIS) ت نرتنإلا تامولعم تامدخ ةرادا حتفا م، IIS نع شحبالا و ادب قوف رقنا 1. ةوطخلا





مداخل تاداهش ىلع رقنا 3. ةوطخلا



ايتاذ ةعقوم ةداهش عاشن رقنا 4. ةوطخلا

## Actions

Import...

Create Certificate Request...

Complete Certificate Request...

Create Domain Certificate...

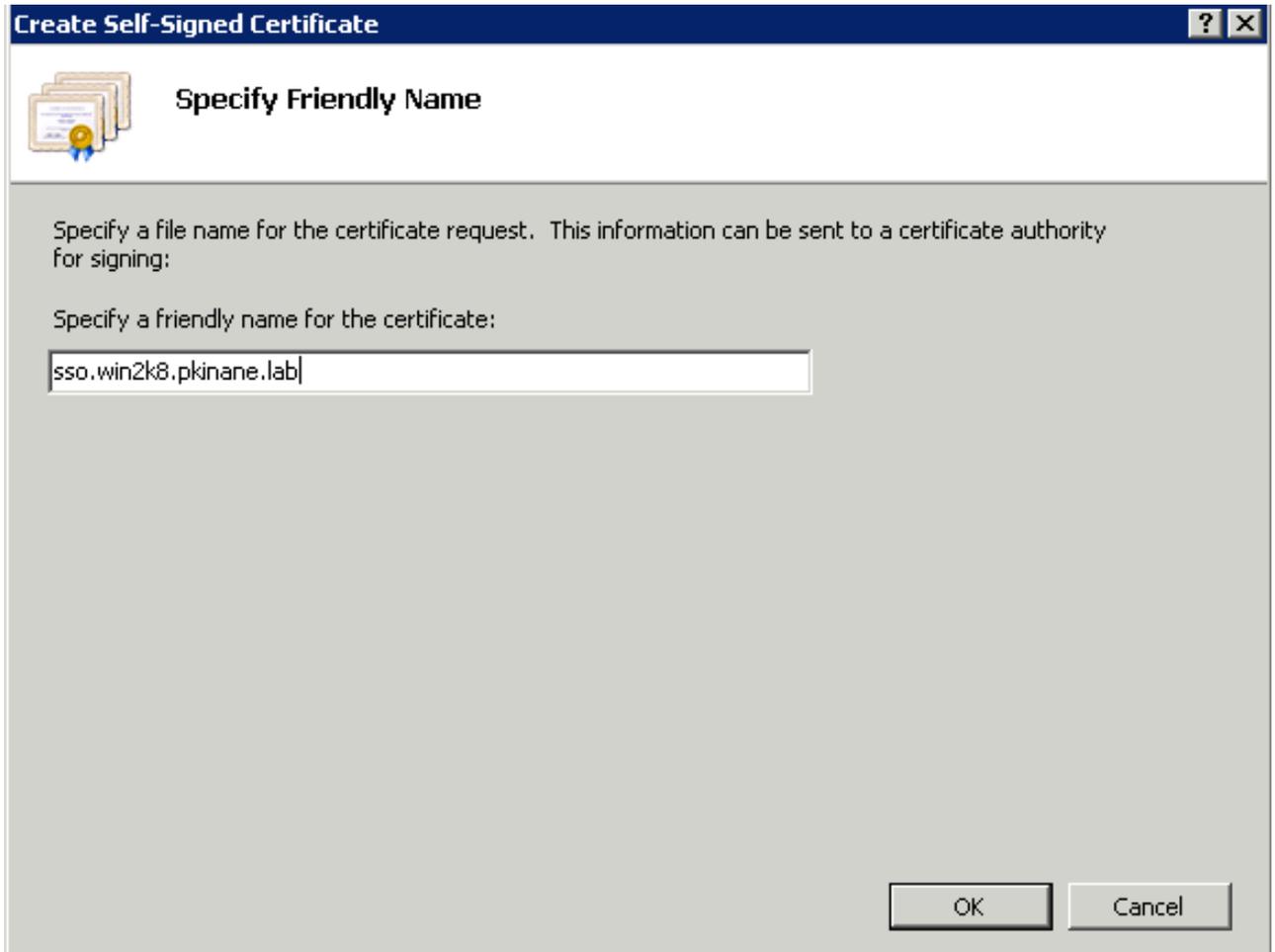
Create Self-Signed Certificate...



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 س فن م ادختسال.

ريدم نيب نم ازتم ريغ تقولا نوكتي ام دنع اذه ثدحي دقو. ةحل اص ريغ SAML ةب اجاتسا  
مق. نيم داخلا الك ىل ع NTP نيوكت نم ققحتل اءا رل. IDP مداوخ و Cisco نم ةدحومل تالاصتالا  
هذه نم ققحتلل (CLI) رم اوألا رطس ةه جاو نم "NTP) ةك بشل تقو لوكتورب ةلاح" ليغشت ب  
Cisco Unified Communications Manager ىل ع ةلاحلا.

رابتخا اءا رل اجاتحت، ةدحومل ةح يحيصل NTP مداوخ ىل ع Windows Server يوتحي نأ درجم ب  
هيوشت يوررضلا نم، تالاحل ضعب ي فو. ةرمتسم ةلكشملا تناك اذا ام ةفرعمو رخأ SSO  
[انه](#) ةيلمعلا كلت لوح ليصافتلا نم ديزملا. ديكأتل ةحص ةرتف

## ةلص تاذا تامولعم

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

ةمچرتل هذه لوح

ةللأل تاينقتل نم ةومچم مادختساب دن تسمل اذہ Cisco تچرت  
ملاعلاء انء مچي في نيمدختسمل معدى وتحم مي دقتل ةيرشبل او  
امك ةقيقد نوك ت نل ةللأل ةمچرت لصف أن ةظحال مچرئي. ةصاخل مه تلبل  
Cisco يخلت. فرتحم مچرت مامدقي يتل ةي فارتحال ةمچرتل عم لاخل او  
ىل إامءاد ةوچرلاب ي صؤتو تامچرتل هذه ةقد نع اهتيل وئسم Cisco  
Systems (رفوتم طبارل) ي لصلأل يزي لچن إل دن تسمل