

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 نيديرشمل 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 تالجت نييعت](#)

[داخال ا قمدخ مسانع ثجبل](#)

[Federation قمدخ مس او DoWithout Certificate](#)

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

[قلمص تاذا تامولعم](#)

قمدقمل

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

قيساسال تابلطتمل

تابلطتمل

هتبلاتل عيضاوملاب قفرعم كيدل نوكت نأب Cisco يصوصت:

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

نيوكتلا اذه كمزلي، ربتخمل هتبيثت ي ف SSO نيكمتل:

- Windows Server عم AD FS تبتتمل
- LDAP قنمازم نيوكت عم CUCM
- سيسايقلا CCM Super Users رود ديدحت عم هتاهن مدختسم

ةمدختسمل اتانوكملا

ةيلالات ةيداملا اتانوكملا اوجماربلا تارادصا اىل دننستسمل اذه يف ةدراولا تامولعمل دننست

- Windows Server م AD FS 2.0
- CUCM 10.5.2

ةصاخ ةيلعمل ةئيب يف ةدوجوملا ةزهجالا نم دننستسمل اذه يف ةدراولا تامولعمل عاشن اىل م تناك اذى. (يضا رتفا) حوسم نيوكتب دننستسمل اذه يف ةمدختسمل ةزهجالا عيمج اءب رما اىل لمحتحمل 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 عهتبيثتو AD FS 2.0 ليزنن

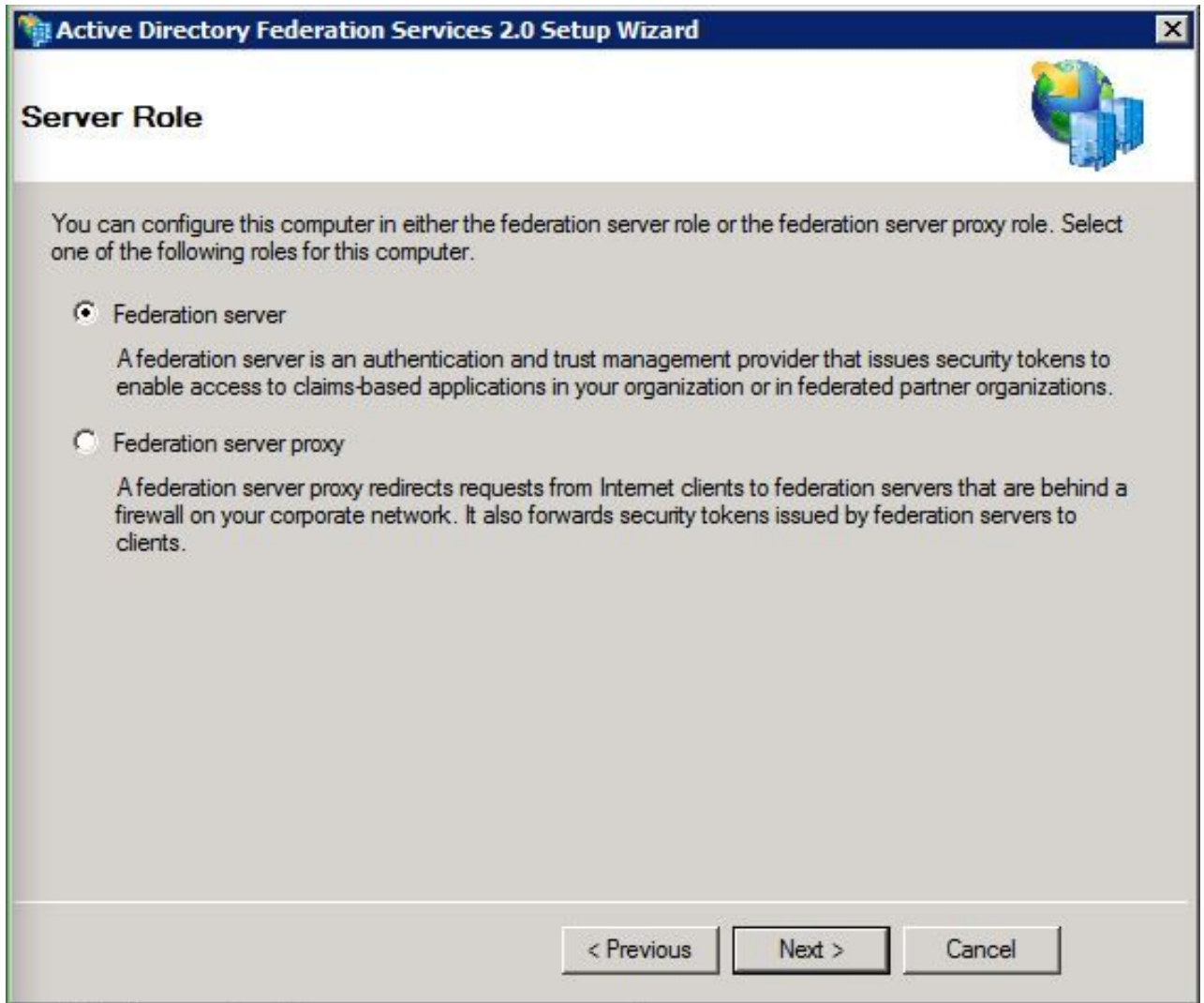
1. ةوطخلا [AD FS 2.0 ليزنن](#) اىل لقتنا .

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

Windows مءاخ اىل هل ليزنن مء اذى فلما لقتنا . 3. ةوطخلا

تبيثتلا ةعباتم . 4. ةوطخلا

Federation Server رءخا ، ةبلاطملا دنع . 5. ةوطخلا



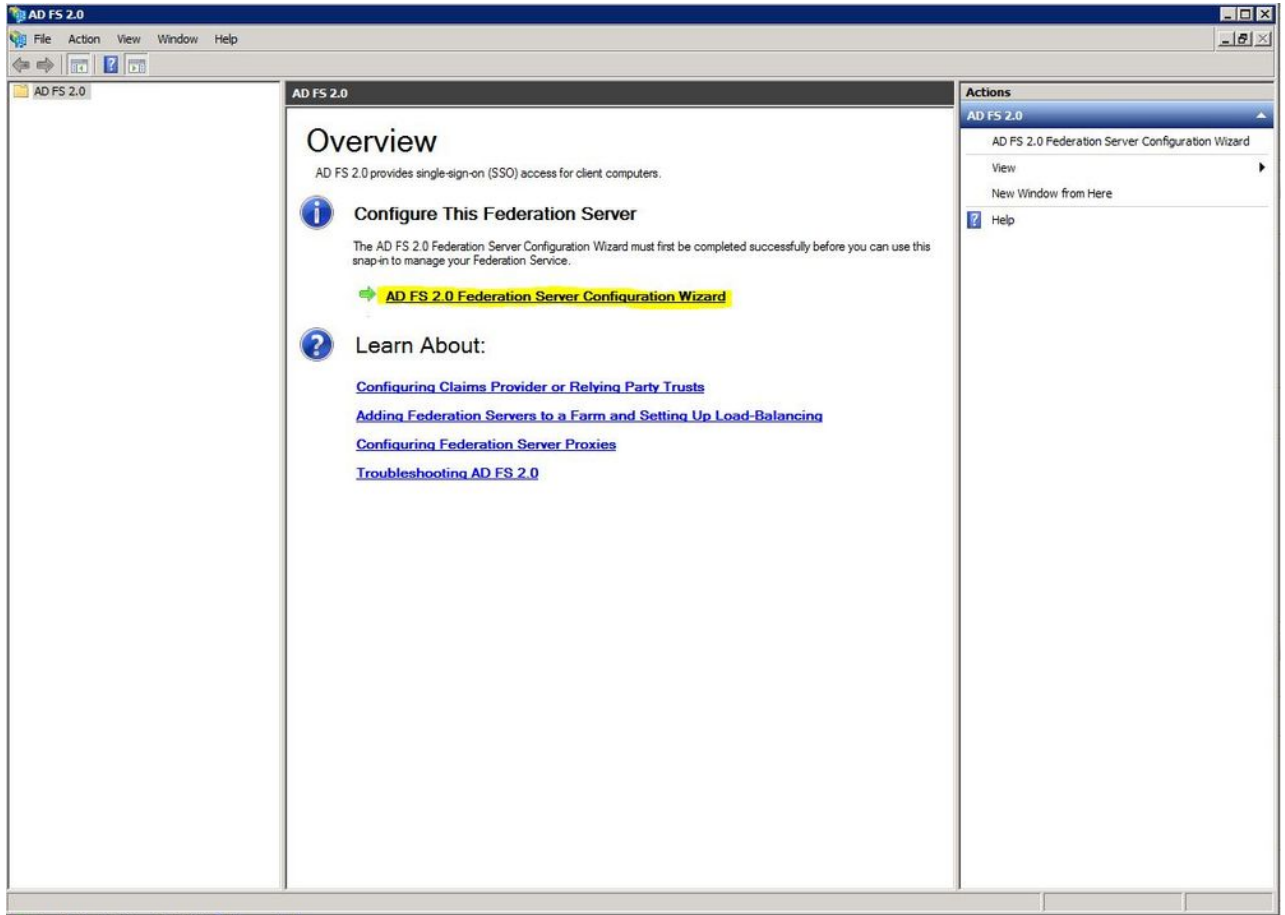
ءاهان قوف رونا ،كلذ متي نأ درجمب - ايئاقلت تايعبتلا ضعب تيبتت متي 6 ةوطخلا

ضعب ةفاضل لجاتحت ،كب صاخلا مداخل لىع اتبتم AD FS 2.0 كي دل حبصأ نأ دعب نأل الة.
ةئهل

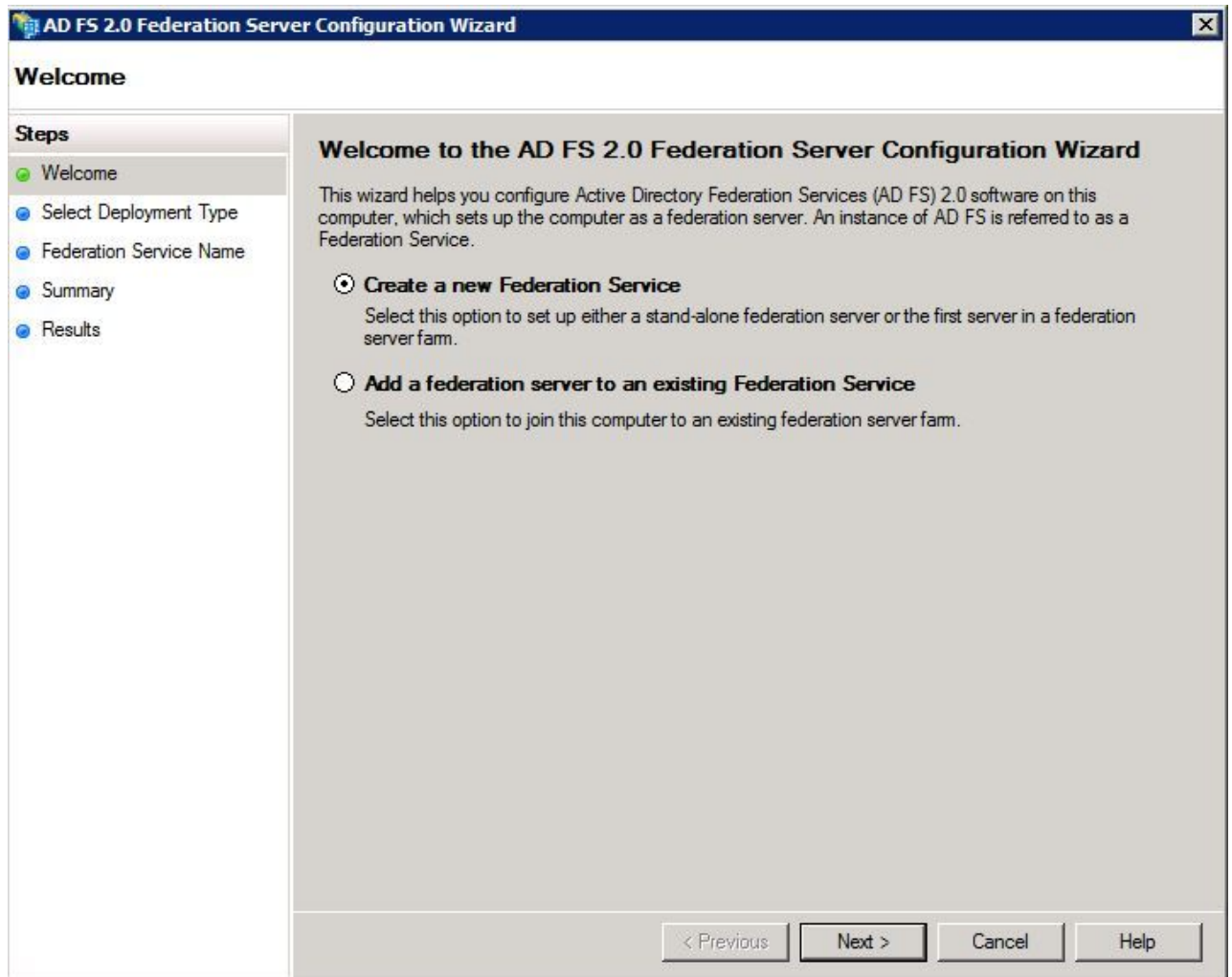
Windows مداخل لىع AD FS 2.0 نيوكت

دب قوف رونلا كنكمي ،تيبتتلا دعب ايئاقلت AD FS 2.0 ةذفان حتفت مل اذا 1. ةوطخلا
ايودي اهحتفل AD FS 2.0 ةرادا نع ثحبل او

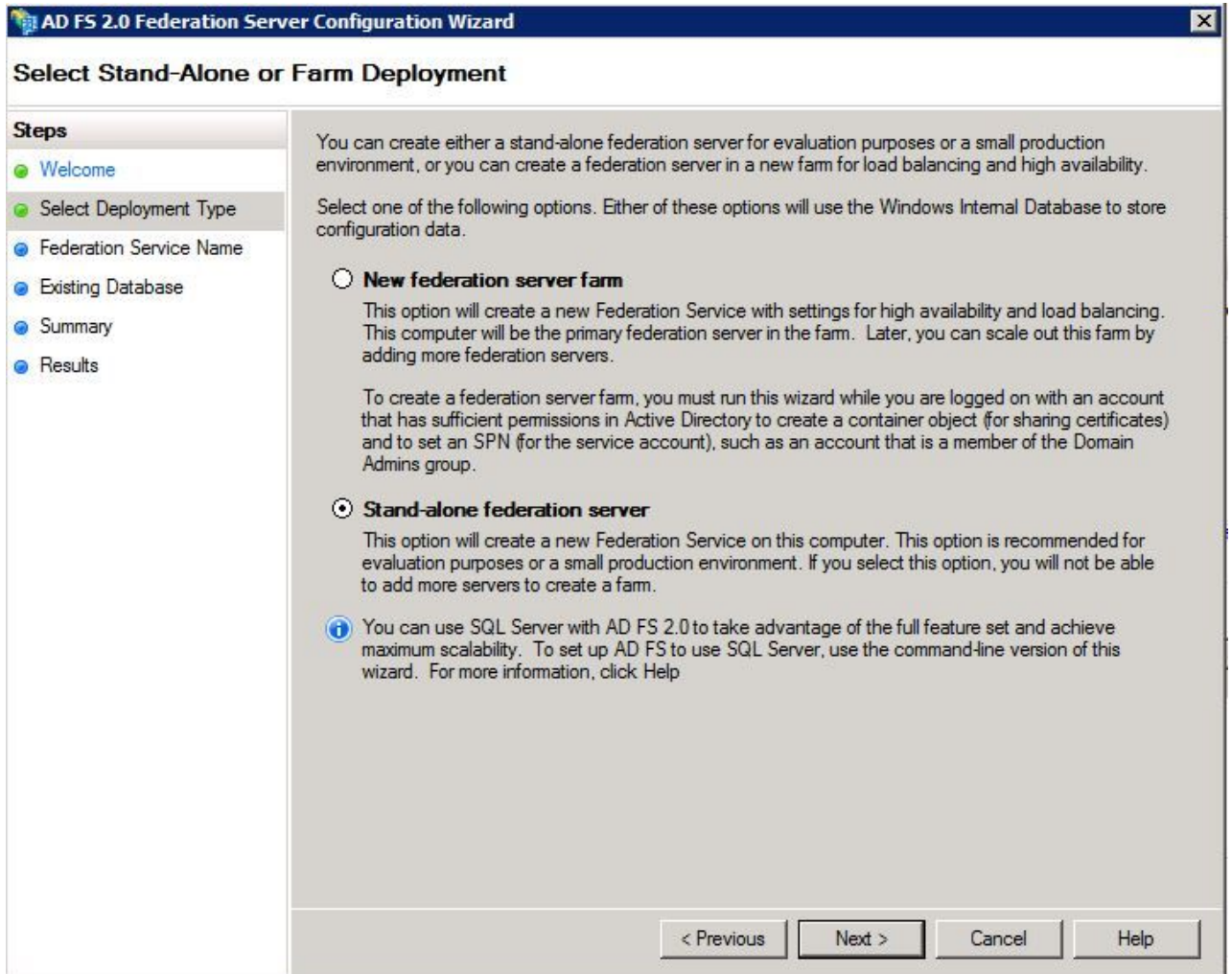
AD FS 2.0 داحتال مداخل نيوكت جلام رتخأ 2. ةوطخلا



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



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



يدلنا على الخطوات التي يجب اتخاذها عند إعداد خادم AD FS 2.0. يمكنك إما إنشاء خادم AD FS 2.0 منفردًا أو إنشاء خادم AD FS 2.0 في مزرعة. يمكنك إنشاء خادم AD FS 2.0 منفردًا لتجربة الغرض أو بيئة إنتاج صغيرة، أو يمكنك إنشاء خادم AD FS 2.0 في مزرعة لتوازن الحمل وتوافر عالٍ. سيستخدم أي من الخيارين التاليين قاعدة بيانات Windows Internal Database لتخزين بيانات التكوين.

مزرعة خادم خدمة اتحادية جديدة

سيؤدي هذا الخيار إلى إنشاء خدمة اتحادية جديدة مع إعدادات لتوافر عالٍ وتوازن حمل. ستكون هذه الحاسنة هي الخادم الرئيسي لخدمة اتحادية في المزرعة. لاحقًا، يمكنك توسيع نطاق هذه المزرعة عن طريق إضافة المزيد من خوادم خدمة اتحادية.

لإنشاء مزرعة خادم خدمة اتحادية، يجب تشغيل هذا السحر بينما أنت مسجل على حساب يتمتع بصلاحية كافية في Active Directory لإنشاء كائن حاوية (للمشاركة شهادات) ولإعداد SPN (لحساب الخدمة)، مثل حساب هو عضو في مجموعة Domain Admins.

خادم خدمة اتحادية منفرد

سيؤدي هذا الخيار إلى إنشاء خدمة اتحادية جديدة على هذه الحاسنة. يُنصح بهذا الخيار لتجربة الغرض أو بيئة إنتاج صغيرة. إذا قمت باختيار هذا الخيار، فلن تتمكن من إضافة المزيد من الخوادم لإنشاء مزرعة.

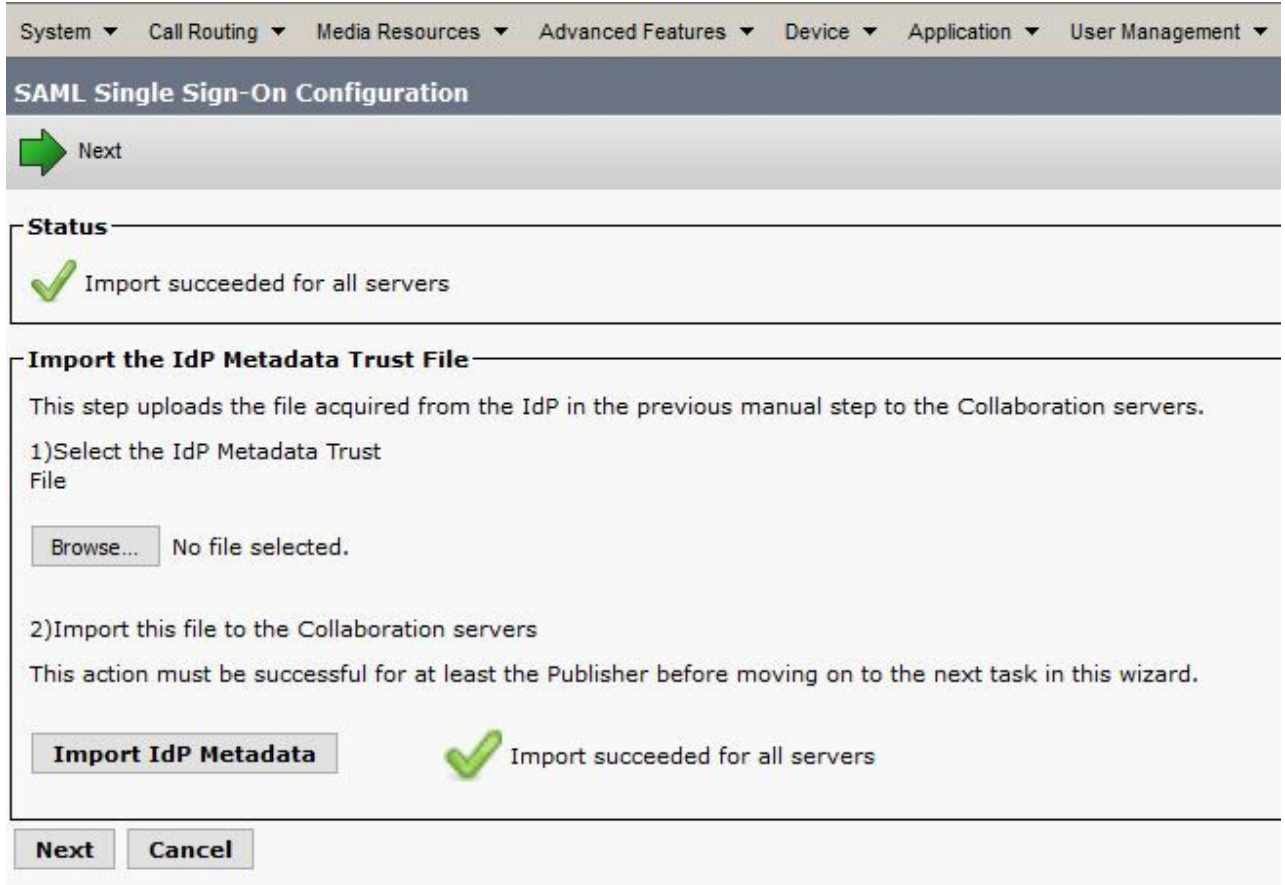
i يمكنك استخدام SQL Server مع AD FS 2.0 لتفادي الاستفادة من مجموعة الميزات الكاملة وتحقيق قابلية التوسع القصوى. لإعداد AD FS لاستخدام SQL Server، استخدم الإصدار من السحر. للمزيد من المعلومات، انقر فوق مساعدة.

< Previous Next > Cancel Help

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 ةدروتسمال IDp فيرعت تانايب لىل ةتلصح نأ دعب نآلا. 9 ةوطخلال لىل صاخال فرعمال لىل CUCM فيرعت تانايب داريتسا

ةقثلا فيرعت تانايب فلم ليزنت قوف رونا. 10 ةوطخلال

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

دلجم لىل تايوتحملال جرختساو Windows مداخل لىل zip. فلم لقنا. 12 ةوطخلال

ءاشنل و AD FS 2.0 مداخل لىل CUCM فيرعت تانايب داريتسا تابلالاطملا دعاوق

AD FS 2.0 ةرادل نع ثحبلالو ادب لىل رونا. 1 ةوطخلال

اهب قوثوم 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 اهءارءتسااب تمق ىتلا XML ءافلما ءارىتسا ىلإ جاتحت ،انه .4 ةوطخللا XML رءءاو ءلءملا ءافلما ىلإ ضرءتساو فلما نم لوعملا فرطلا لوء ءاناىب ءارىتسا ىلإ كرشانل

✎ هىلع SSO ماءءتسا ىءرت ءءوم نواعء مءاء ىلأ ةقباساللا ءاوطخللا مءءتسا :ةظحالم

The screenshot shows the 'Add Relying Party Trust Wizard' dialog box, specifically the 'Select Data Source' step. The wizard has a 'Steps' pane on the left with the following steps: Welcome, Select Data Source (current), Specify Display Name, Choose Issuance Authorization Rules, Ready to Add Trust, and Finish. The main area contains three radio button options for selecting data source information:

- Import data about the relying party published online or on a local network. Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata online or on a local network. Federation metadata address (host name or URL): [Text Box] Example: fs.contoso.com or https://www.contoso.com/app
- Import data about the relying party from a file. Use this option to import the necessary data and certificates from a relying party 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. Federation metadata file location: [Text Box: C:\Users\Administrator\Desktop\SPMetadata_1cucm1052.sckiewer.lab.xml] [Browse... Button]
- Enter data about the relying party manually. 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

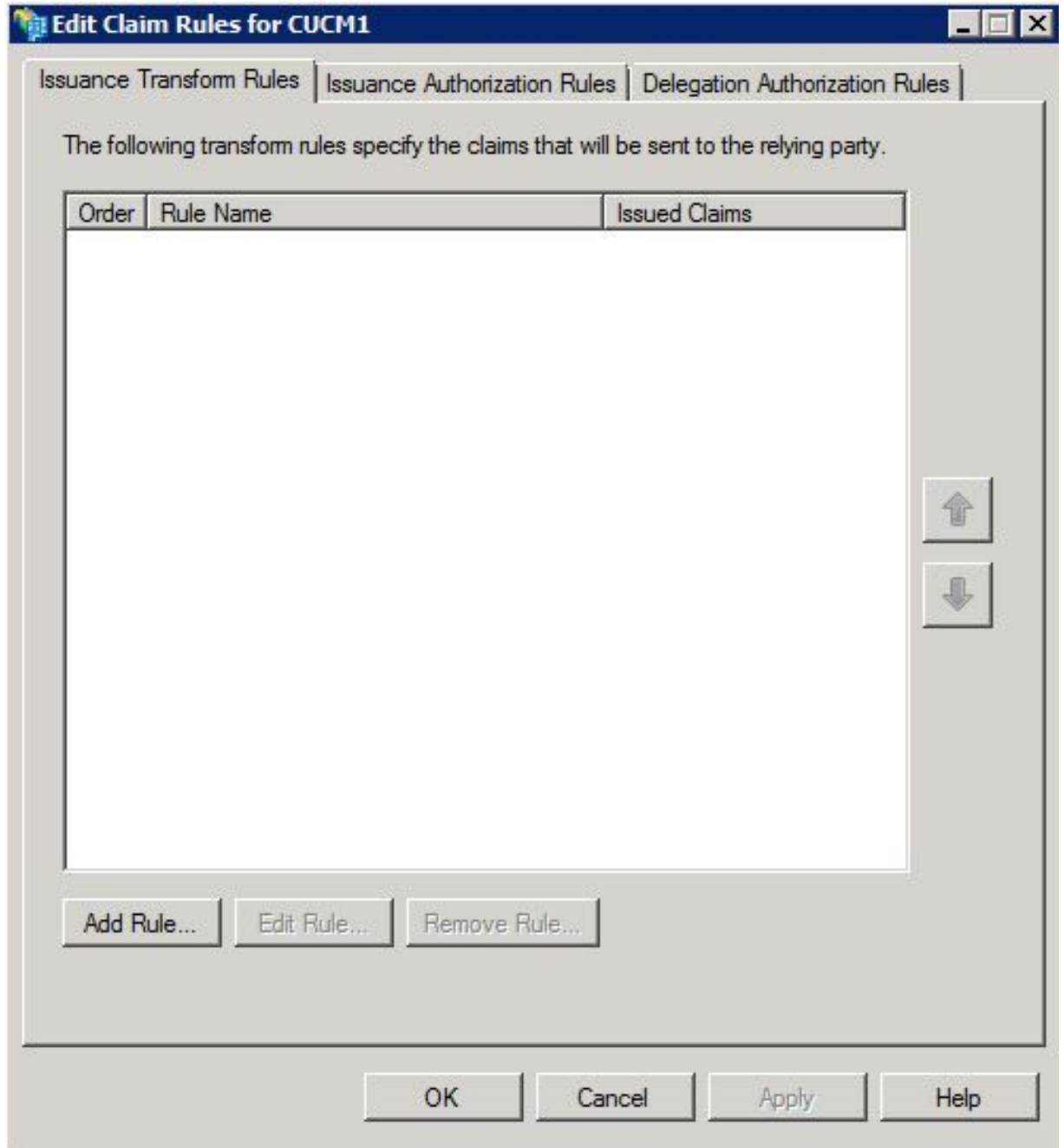
كلء ءءب رقناو ضرءلا مسا رء .6 ةوطخللا

قوف رقناو هءه ءامتعالا ةهء ىلإ لوصولاب نىمءءتسملل ءىمءل ءامساللا رءءأ .7 ةوطخللا ىللاءلا

ةىنءا ءلء ءءب ءقءقء .8 ةوطخللا

ءءاوق رىءءء "راوءلا ءبءم ءءءب تمق ءنأ نم ءءأء ،ءشاشللا هءه ىللع .9 ةوطخللا قالغإ قوف رقنا مءء ،قىقءءللل ءلاءملا قالغإ ءنع 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 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: ةظحال م

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

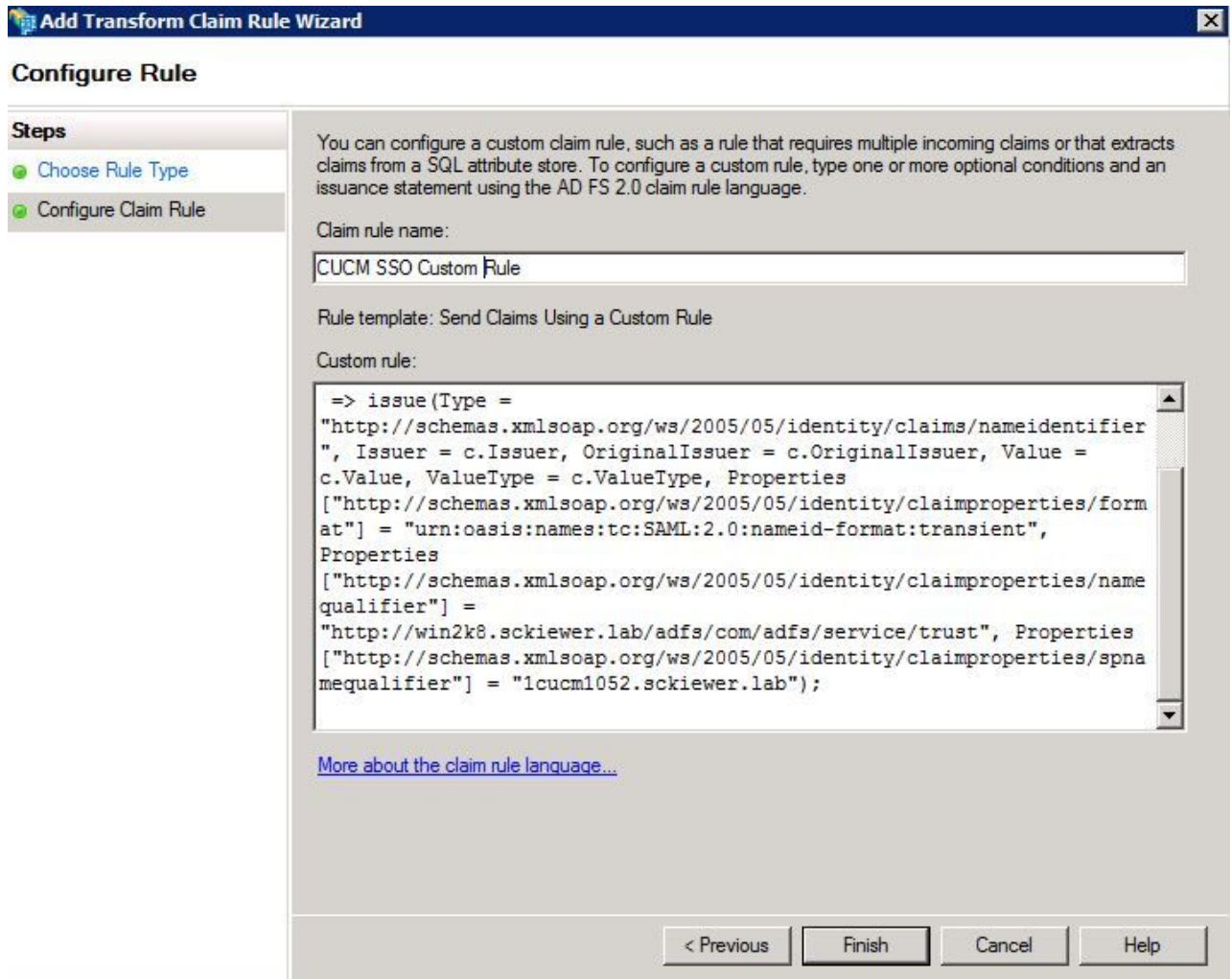
ةبلاطم ةدعاق مسا لخدأ 20 ةوطخل

صنلا اذه قصل، ةصصخملا ةدعاقلا لقح يف 21 ةوطخل

```
ج: [عونل] == http://schemas.microsoft.com/ws/2008/06/identity/ windowsAccountName]
=> رادصا [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

 روثلل تاوطلال عابتا كنكمي، AD FS ةمدخ مسا نم ادكأت م نكت مل اذا: ةطرحالم
فيرعت تانايب فلم يف لوألا رطسلا نم CUCM نايف فرعم بحس نكمي. هيلع
CUCM. اذك ودي فلملا نم لوألا رطسلا ىل 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 ةوطخلا

OK قوف رقناو 24 ةوطخلا

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

SSO رابتخا ليغشت و CUCM ىل سSO ني كمت ءاهن

CUCM ىل ءوجرلا 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 يذلي يئاهن لل مدخت سمل دح. 3 ة و ط خ ل ا
SSO... راب تخ ل يغ ش ت قوف

تانا ي ب ل خ د ا و ، ة ق ث ب ن م ل ا ت ا ر ا ط ا ل ا ب ح م س ي ك ب ص ا خ ل ا ض ر ع ت س م ل ا ن ا ن م د ك ا ت . 4 ة و ط خ ل ا
ر م ا ل ا ه ج و م ي ف ك ب ة ص ا خ ل ا د ا م ت ع ا ل ا



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 ل م ت ، ة ق ث ب ن م ل ا ة ذ ف ا ن ل ا ل ع ق ا ل ع ر ق ن ا . 5 ة و ط خ ل ا

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

اهحال صاوا ءاطخالا فاشك ت سا

ءاطخالا حيحصت يلا SSO تالجس نييغت

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

Cisco SSO وه تالجس لاء ءومجم مسا RTMT. نم SSO تالجس لي زنت نكمي

داحتالا ءمدخ مسا نع ثحبالا

AD FS 2.0 ءرادا نع ثحبالا ءدب قوف رقنا، داحتالا ءمدخ مسا يلع روثعلل

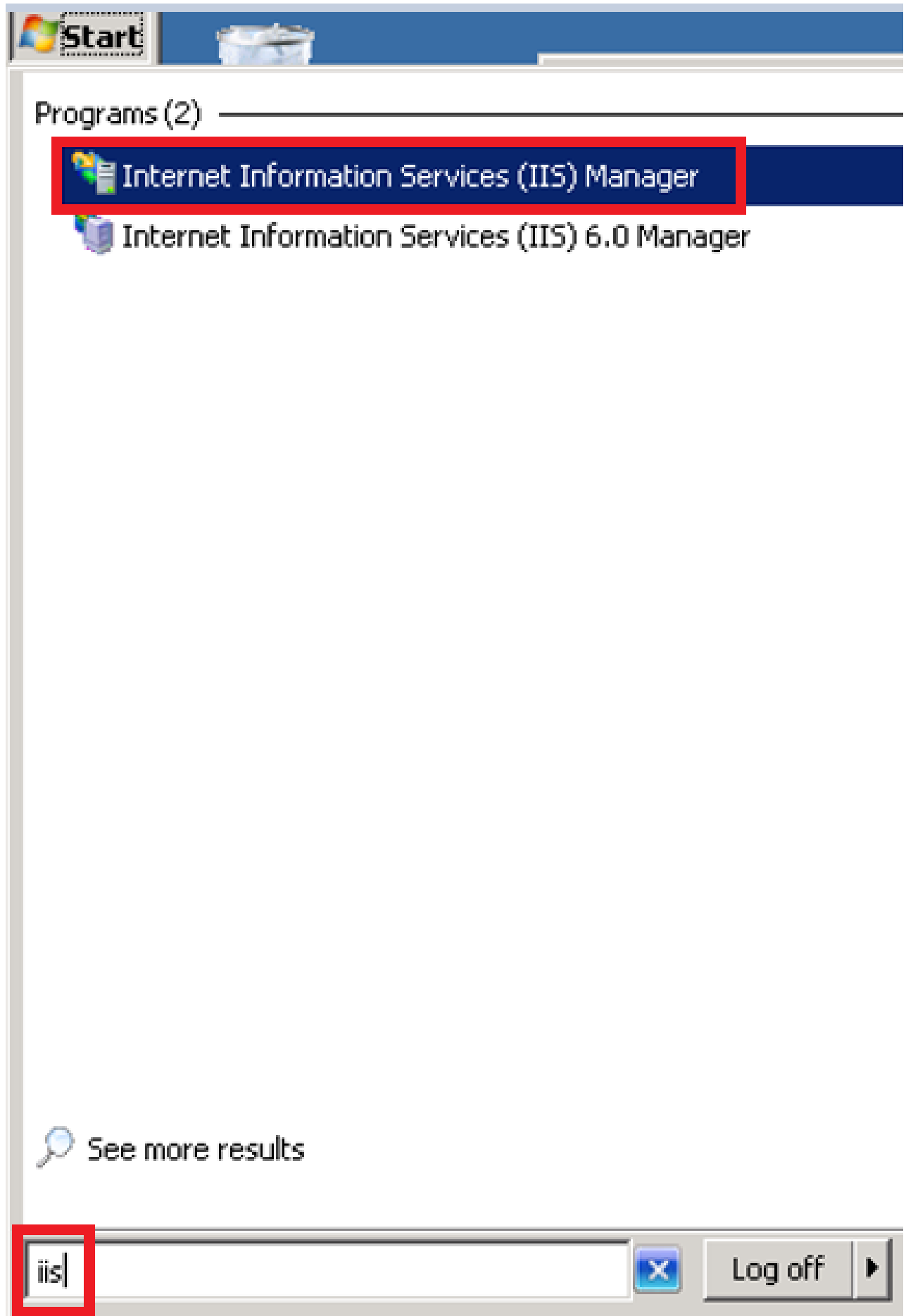
- داحتالا ءمدخ صئاصخ ريحت قوف رقنا
- Federation ءمدخ مسا نع ثحبالا، "ماع" بيوبتالا ءمالع يف كدوجو ءانثا

Federation ءمدخ مسا او DoWithout Certificate

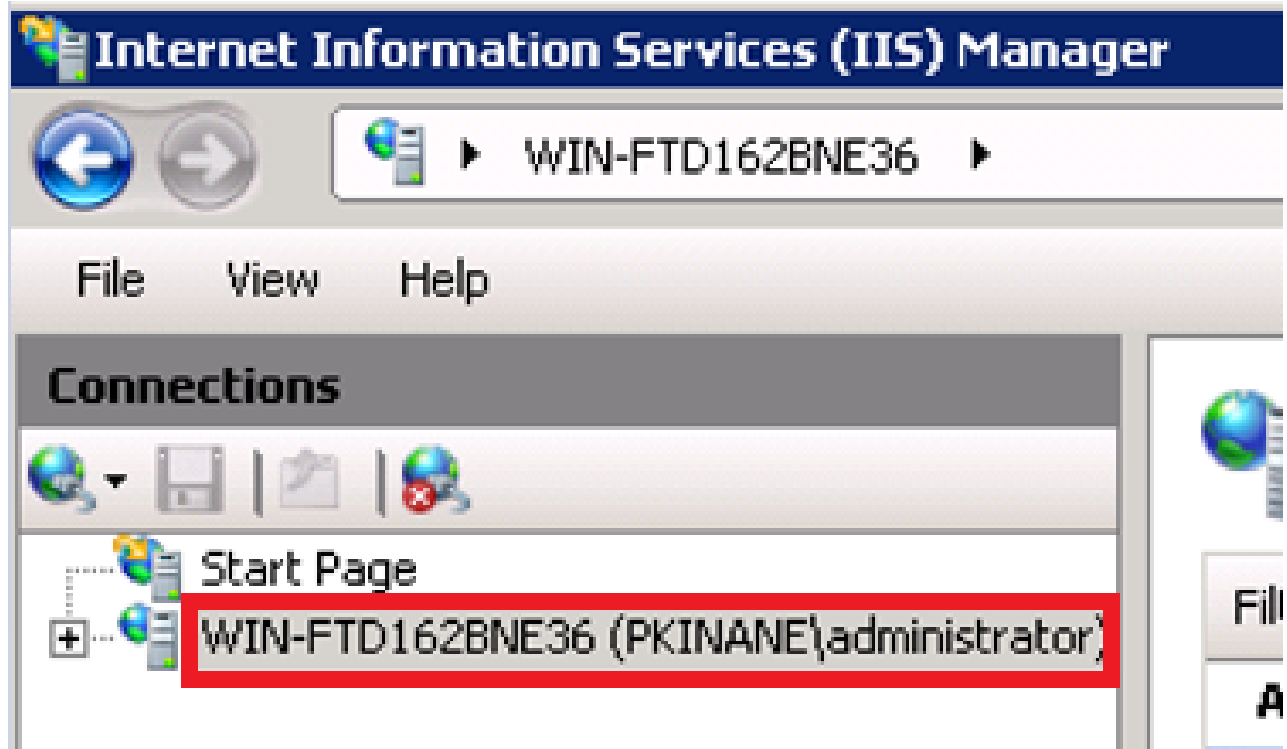
ءديج ءداهش ءاشنا يلا جاتحت كنإف، AD FS نيوكت جلاعم يف هذء اطخالا ءلاس رتملتسا اذا

مسا اهل ءدحمالا ءداهش لال نال داحتالا ءمدخ مسا ديحتل ءدحمالا ءداهش لال مادختسا رذعتي
يمسم) ءمالع ال ب ءوضوم مسا نودب يرخا ءداهش دح. (مسا ليري صق) ءمالع ال ب ءوضوم
يرخا ءرم لواح م، (يري صق

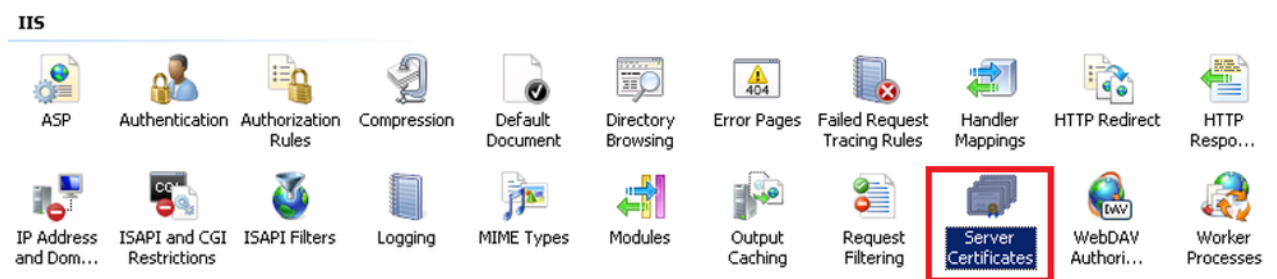
(IIS) "تنرتنالا تامولعم تامدخ ءرادا" حتفا م، IIS نع ثحبالا "ادبا" قوف رقنا 1. ءوطخلا



مداخل مساقوف رقنا 2 ةوطخا



مداخل تاداهش ىلع رقنا 3. ةوطخلا



ايتاذ ةعقوم ةداهش عاشن رقنا 4. ةوطخلا

Actions

Import...

Create Certificate Request...

Complete Certificate Request...

Create Domain Certificate...

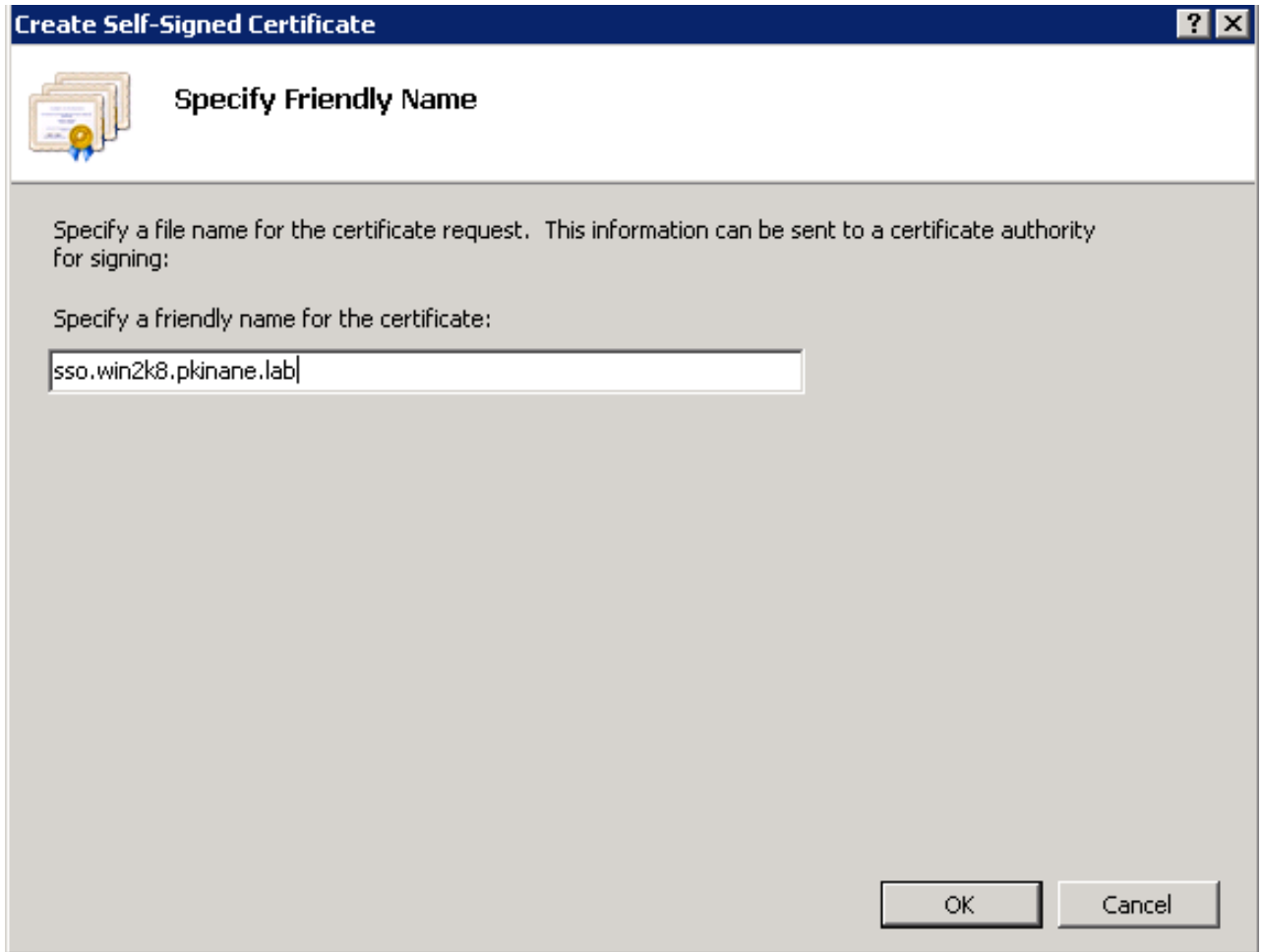
Create Self-Signed Certificate...



Help

Online Help

عداهشلل راعتسملال مسالال لخدأ. 5 ةوطخال



IDP و CUCM مداول ني ب نمازتم ريغ تقولا

Windows Server نيوكت يلا جاتحت، CUCM نم SSO رابتخا ليغشت دنع أطخ اذه تملتسا اذا IDP مداول و Cisco نم ةدحوملا تالاصتالا CUCM لثم NTP (مداول) مداول سفن مداخلتسال.

ريدم ني ب نمازتم ريغ تقولا نوكتي ام دنع اذه ثدحي دقو. ةحل اص ريغ SAML ةباجتسا مق. ني مداول الك يلع NTP نيوكت نم ققحتلا عاجرلا IDP مداول و Cisco نم ةدحوملا تالاصتالا هذه نم ققحتلل (CLI) رم اوألا رطس ةهجاو نم "NTP" ةكبشلا تقو لوكتورب ةلاح" ليغشتب Cisco Unified Communications Manager يلع ةلاحلا.

رابتخا عاجر يلا جاتحت، ةدحوملا ةحيصلا NTP مداول يلع Windows Server يوتحي نأ درجمب هويشت يوررضلا نم، تالاحلا ضعب يفو. ةرمتسم ةلكشملا تناك اذا ام ةفرعمو رخا SSO [انه](#) ةيلمعلا كلت لوح ليصافتلا نم ديزملا. ديكأتل ةحص ةرتف

ةلص تاذا تاملعم

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

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسمل اذ ه Cisco ت مچرت
ملاعلاء ن أ عي مچ ي ف ن ي م دخت سمل ل م عد ي و تح م مي دقت ل ة ي رش ب ل و
امك ة ق ي قد ن و ك ت ن ل ة ي ل أ ة مچرت ل ض ف أ ن أ ة ظ حال م ي ج ر ي . ة ص ا خ ل م ه ت غ ل ب
Cisco ي ل خ ت . ف ر ت ح م مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة مچرت ل ا ع م ل ا ح ل ا و ه
ي ل ا م ئ ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco
Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص أ ل ا ي ز ي ل ج ن إ ل ا دن تسمل ا