

Настройте Единую точку входа с помощью CUCM и AD FS 2.0 (Windows Server 2008 R2)

Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Загрузка и AD FS 2.0 Установки на вашем Windows Server](#)

[Настройте AD FS 2.0 на своем Windows Server](#)

[Импортируйте Метаданные Idp к CUCM / Загружают Метаданные CUCM](#)

[Импортируйте CUCM Metatdata к серверу AD FS 2.0 и создайте правила требования](#)

[Закончите Включать SSO на CUCM и запустите Тест SSO](#)

[Устранение неисправностей](#)

[SSO набора регистрирует для отладки](#)

[Обнаружение имени сервиса федерации](#)

[Сертификат Dotless, когда Specifing Имя сервиса Федерации](#)

[Время вне синхронизования между CUCM и серверами IDP](#)

Введение

Этот документ описывает, как настроить Единую точку входа с помощью Объединенных коммуникаций Cisco управляют (CUCM) и Сервиса Федерации Active Directory (AD FS) 2.0 (Windows Server 2008 R2).

Внесенный Скоттом Кивертом, специалистом службы технической поддержки Cisco.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Cisco Unified Communication Manager
- Знание Basic ADFS 2.0

Для включения SSO в лабораторной среде вам нужна эта конфигурация

- Windows Server с установленным AD FS 2.0
- CUCM с настроенным синхронизованием LDAP.
- Конечный пользователь с Стандартная роль Привилегированных пользователей CCM выбрана.

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Windows Server с AD FS 2.0
- CUCM

Внутренняя информация Cisco

Загрузка и AD FS 2.0 Установки на вашем Windows Server

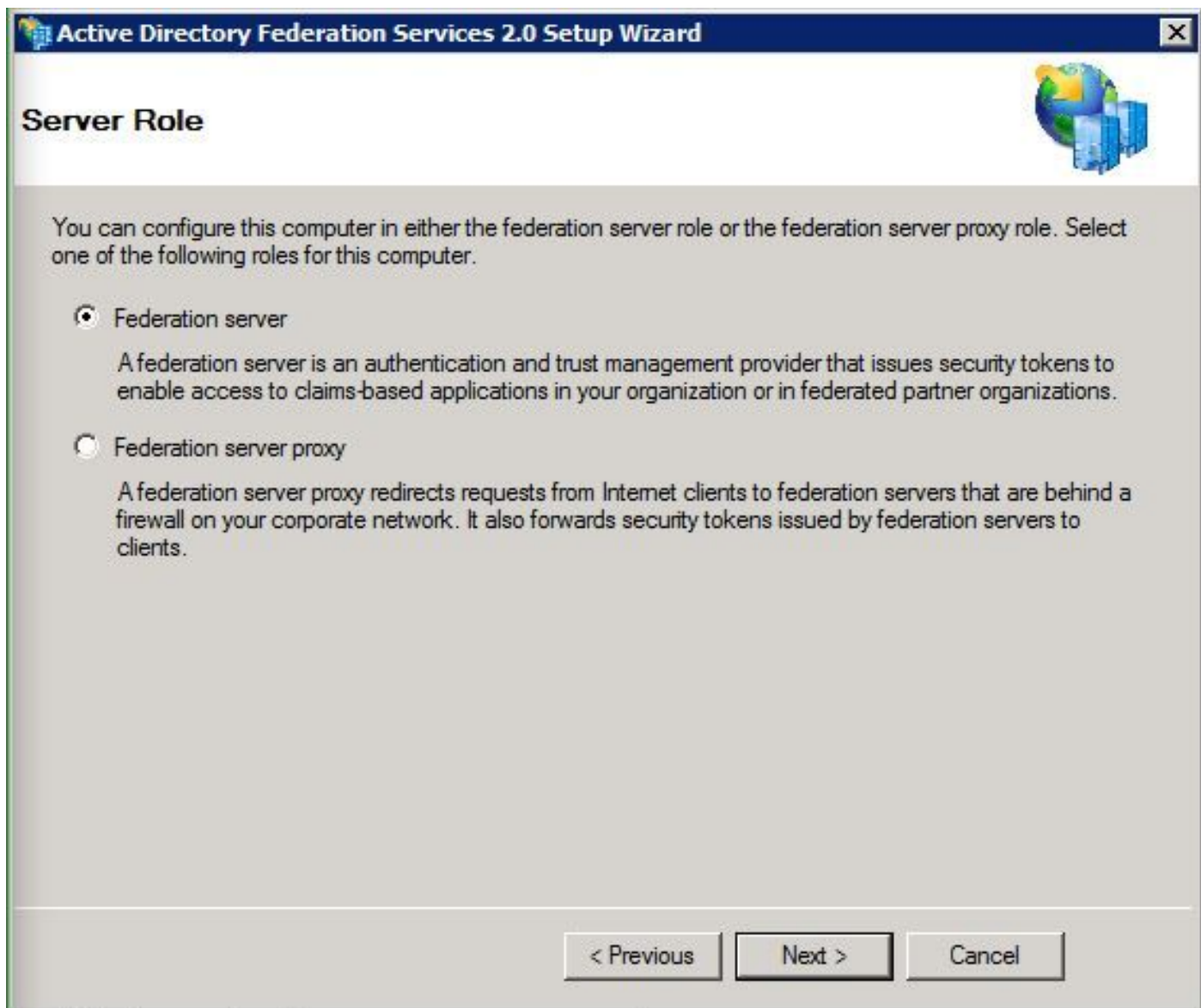
Шаг 1. Перейти к <https://www.microsoft.com/en-us/download/details.aspx?id=10909> и нажимают Continue.

Шаг 2. Во всплывающем окне удостоверьтесь, что вы выбираете соответствующую загрузку на основе своего Windows Server.

Шаг 3. Переместите загружаемый файл в своего Windows Server.

Шаг 4. . Продолжите установку:

Шаг 5. . Когда предложено, выберите **Federation Server**:



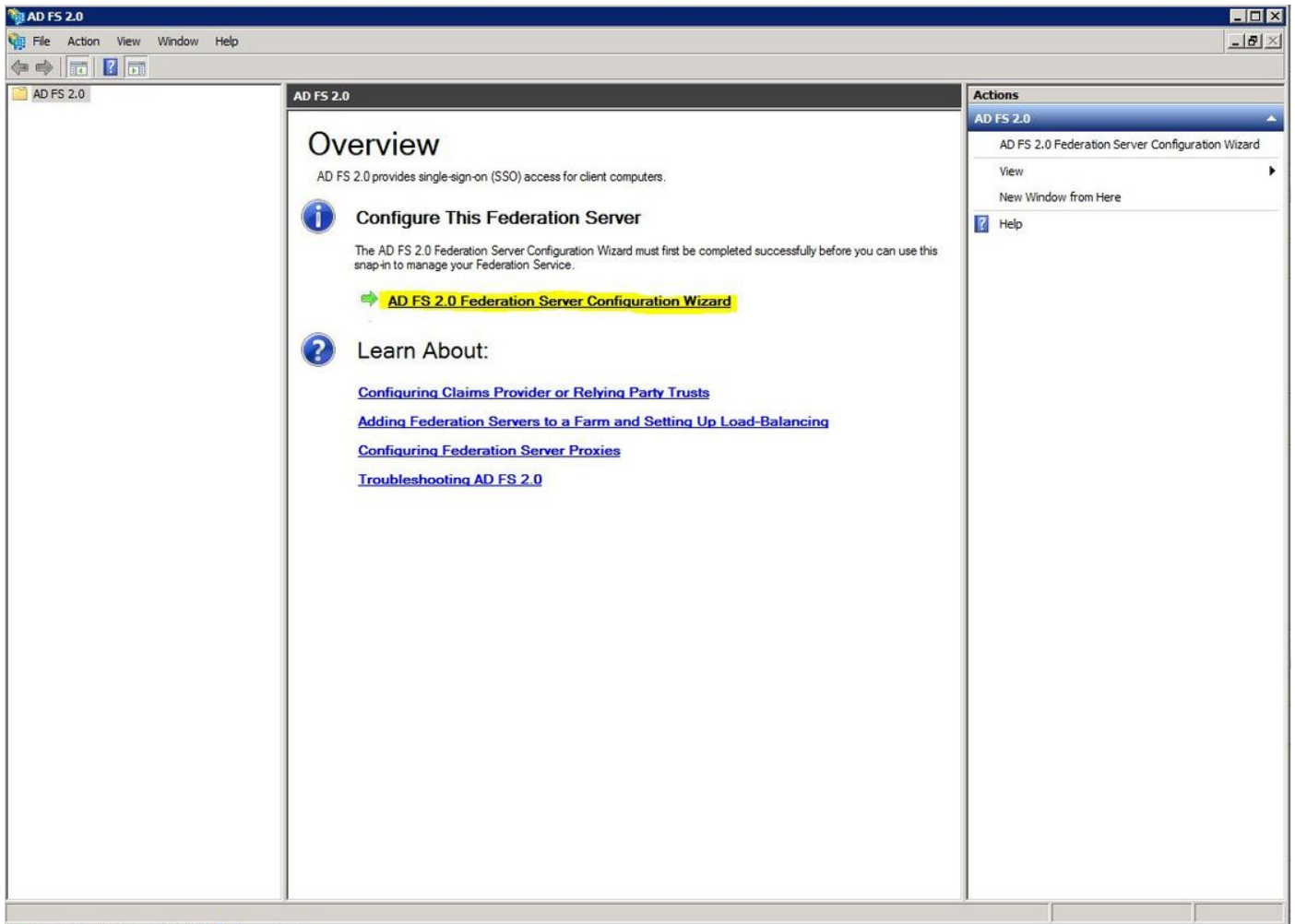
Шаг 6. Некоторые зависимости могут быть установлены автоматически, и вам предлагают нажать **Finish**.

Теперь, когда вам установили AD FS 2.0 на вашем сервере, необходимо добавить некоторую конфигурацию.

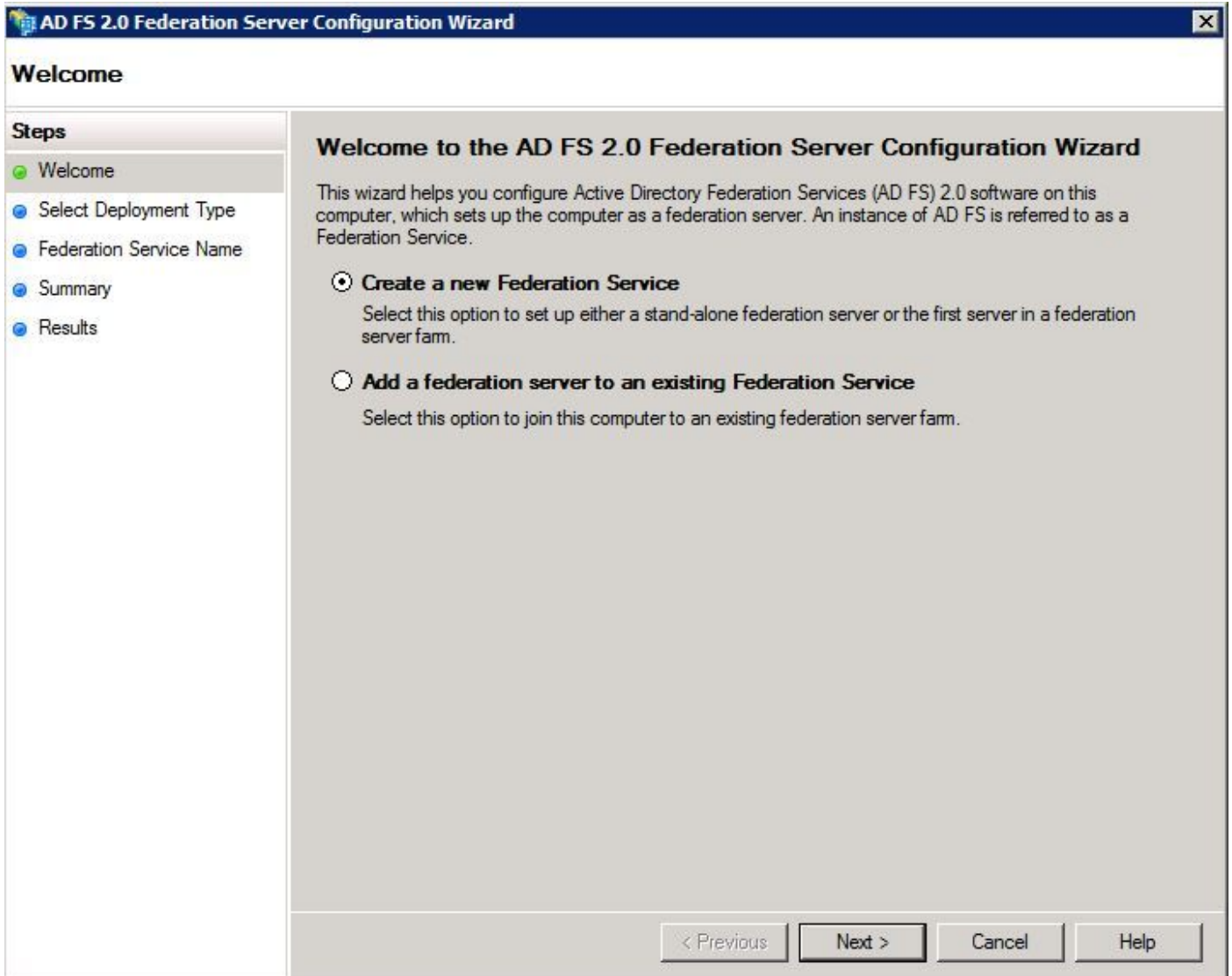
Настройте AD FS 2.0 на своем Windows Server

Шаг 1. Окно AD FS 2.0 должно было открыться после установки, однако, можно найти его путем нажатия **Start** и поиска менеджмента AD FS 2.0.

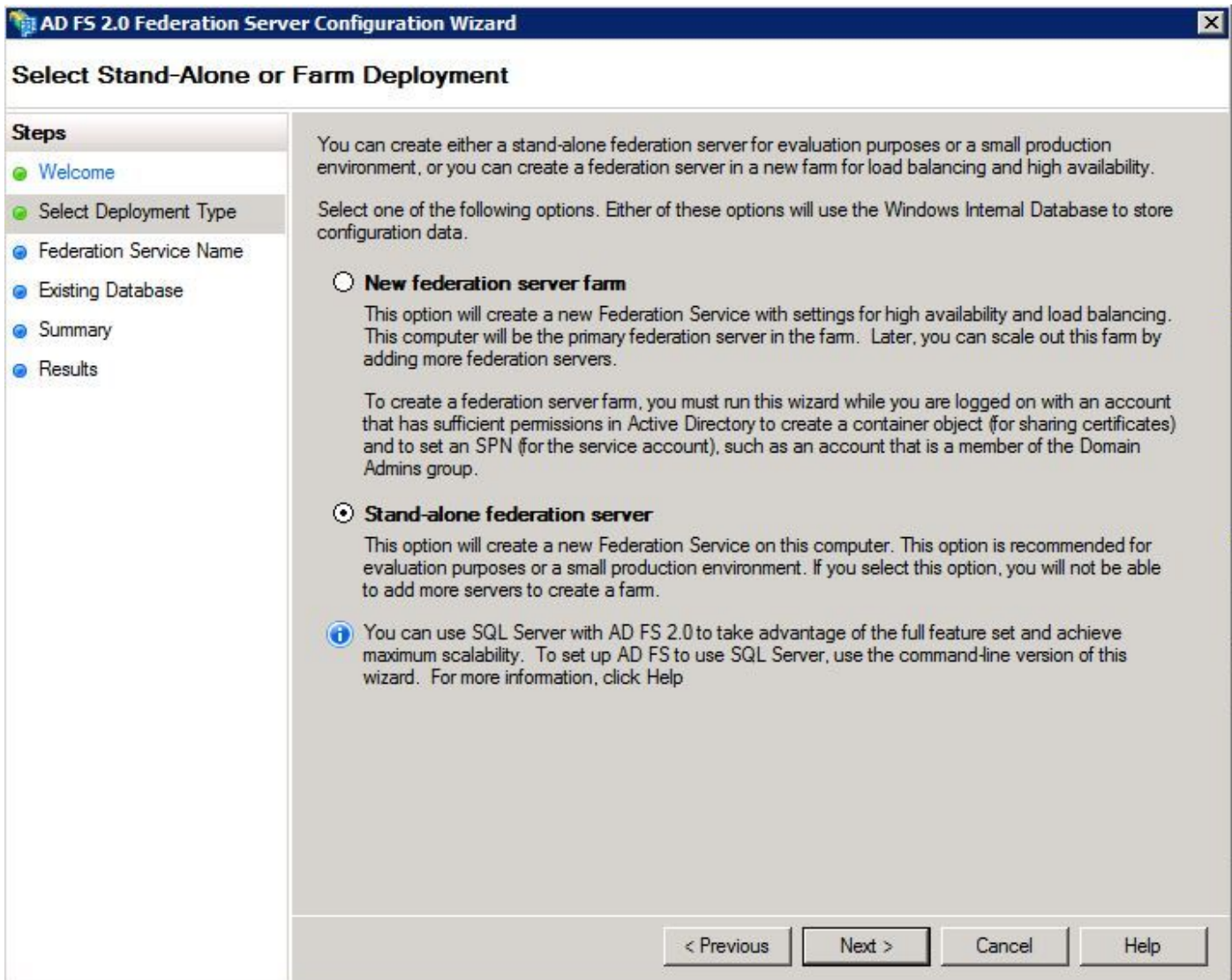
Шаг 2.. Как только у вас есть открытое окно AD FS, выберите **AD FS 2.0 Мастера настройки Федеративного сервера**.



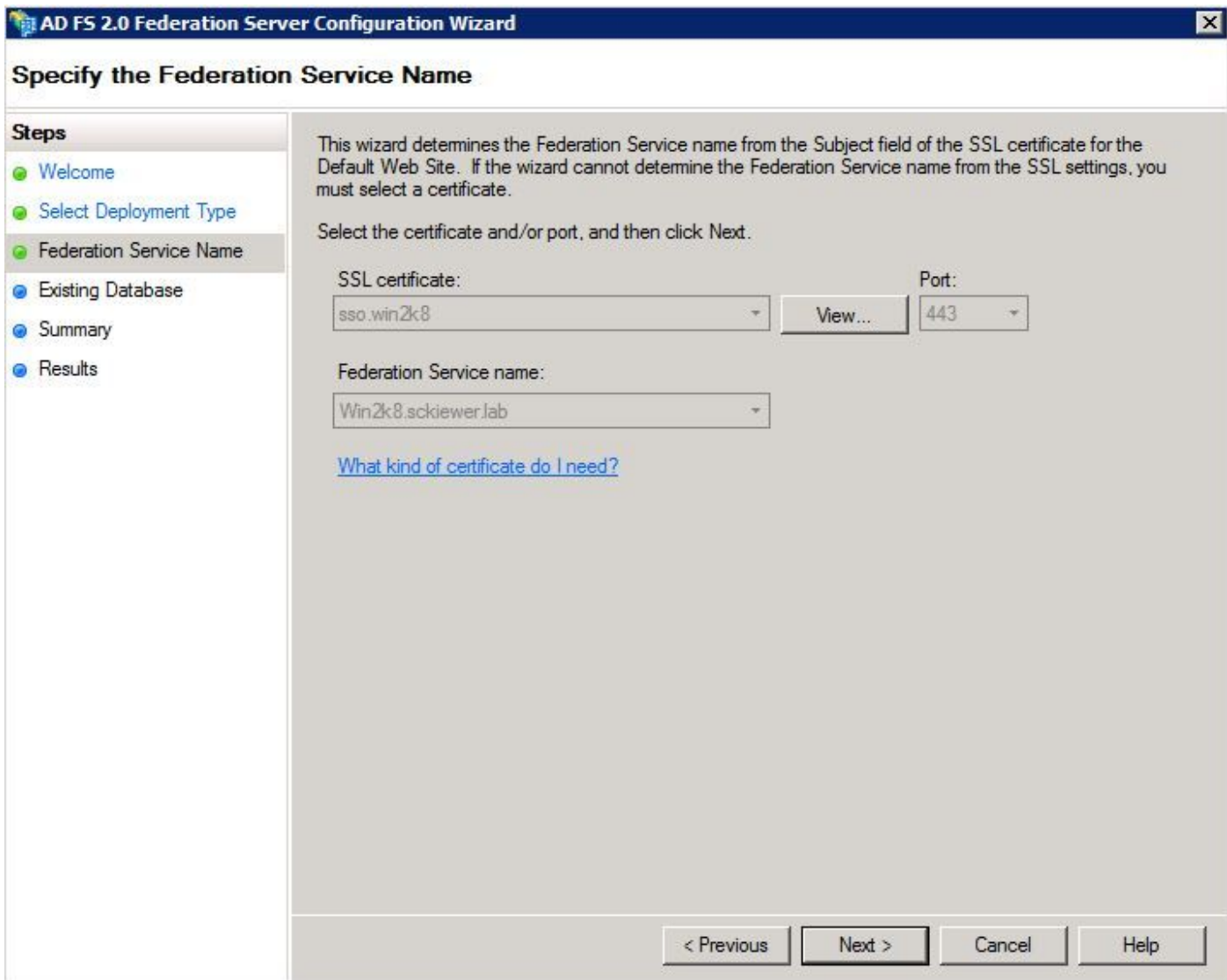
Шаг 3. Затем, нажмите **Create** новый Сервис Федерации.



Шаг 4. . Для лабораторной среды **Автономный федеративный сервер** достаточен.



Шаг 5. . Затем, вас просят выбрать сертификат, который использует сервер. Это должно автоматический заполнять, пока сервер уже имеет сертификат.



Шаг 6. Если у вас есть существующая AD база данных FS по серверу, необходимо удалить его для продолжения.

Шаг 7. Наконец, вы находитесь на итоговом экране, где можно просто нажать **Next**.

Импортируйте Метаданные Idp к CUCM / Загружают Метаданные CUCM

Шаг 1. Загрузите метаданные от своего AD сервера FS путем навигации к следующему URL: <https://hostname/federationmetadata/2007-06/federationmetadata.xml>

Шаг 2. Переместитесь к Cisco по Унифицированному администрированию CM> Система> Единая точка входа SAML

Шаг 3. Нажмите **Enable SAML SSO**

Шаг 4. . Можно получить предупреждение о Соединениях Web-сервера, бывших должных быть перезагруженными, просто пораженными , **Продолжаются**

Шаг 5. . Затем, CUCM дает вам команду загружать файл метаданных от своего IdP. В этом сценарии вашим AD сервером FS является IdP, и мы загрузили метаданные в **Шаге 1** выше, поэтому нажмите **Next**.

Шаг 6. Вас просят импортировать файл.

Шаг 7. Нажмите **Browse> Select, .xml от Шага 1> Нажимает Import IdP Metadata**.

Шаг 8. Необходимо получить сообщение, что импорт был успешен:

System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾ User Management ▾

SAML Single Sign-On Configuration

Next

Status

Import succeeded for all servers

Import the IdP Metadata Trust File

This step uploads the file acquired from the IdP in the previous manual step to the Collaboration servers.

1) Select the IdP Metadata Trust File

No file selected.

2) Import this file to the Collaboration servers

This action must be successful for at least the Publisher before moving on to the next task in this wizard.

Import succeeded for all servers

Шаг 9 Нажмите кнопку Next

Шаг 10. Теперь, когда вам импортировали метаданные IdP в CUCM, необходимо импортировать метаданные CUCM в IdP.

Шаг 11. Нажмите **Download Trust Metadata File**

Шаг 12 Нажмите кнопку Next (Далее)

Шаг 13. Переместите файл .zip, который был загружен в **Шаге 12** в вашего Windows Server, и извлеките содержание к папке.

Импортируйте CUCM Metadata к серверу AD FS 2.0 и создайте правила требования

Шаг 1. На этом этапе вернитесь к своему AD серверу FS и откройте окно управления AD FS 2.0 путем нажатия **Start** и поиска **менеджмента AD FS 2.0**.

Шаг 2. Нажмите **Required: Добавьте доверяемую полагающуюся сторону** (примечание: если вы не видите это, вы, возможно, должны закрыть окно и открыть его, выполняют резервное копирование. Эта опция не обнаружится, если окно оставили открытым, так как **Мастер Федеративного сервера** завершил).

Шаг 3. Как только у вас есть **Добавить Полагающийся Партийный Тростовый** открытый **Мастер**, нажмите **Start**.

Шаг 4. . Здесь, необходимо импортировать файлы .xml, которые вы извлекли в **Шаге 13**, поэтому выберите **данные Import о полагающейся стороне от файла** и перейдите к папке, содержащей файлы, выберите .xml для своего издателя.

Примечание: Выполните те же действия выше для любого Унифицированного Сервера совместной работы, на котором вы хотите использовать SSO.

The screenshot shows the 'Add Relying Party Trust Wizard' window. The title bar reads 'Add Relying Party Trust Wizard'. The main window title is 'Select Data Source'. On the left, a 'Steps' pane shows a progress list: 'Welcome', 'Select Data Source' (current step), '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 containing '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'.

Шаг 5. . Нажмите кнопку **Next**

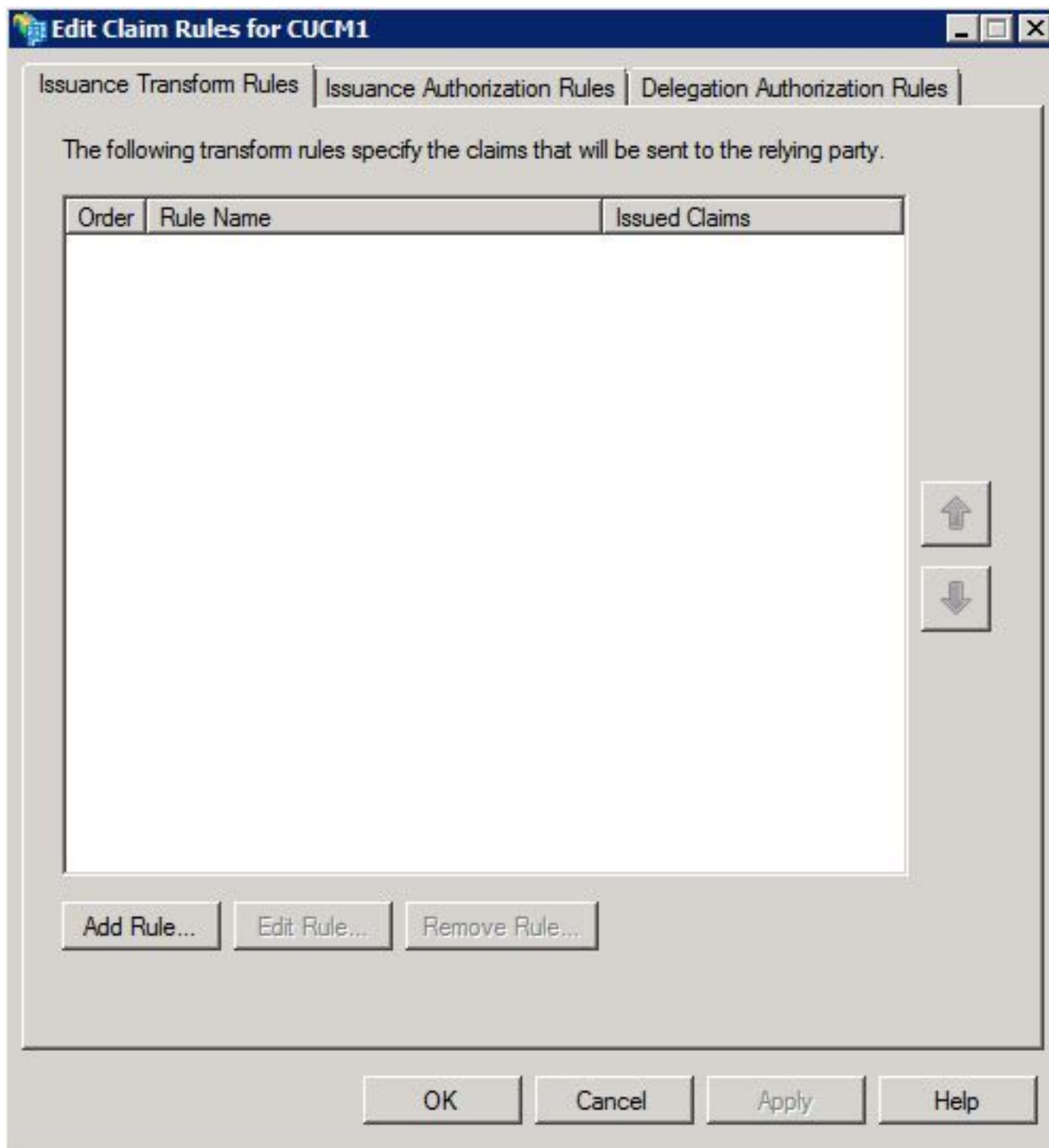
Шаг 6. Отредактируйте **Название Показа** к тому, что вы хотели бы, тогда нажимают **Next**.

Шаг 7. Выберите **Permit все пользователи, чтобы обратиться к этой полагающейся стороне** и нажать **Next**

Шаг 8. Нажмите **Next** еще раз

Шаг 9. На этом экране удостоверьтесь, что вы имеете **Открытый диалоговое окно Правил Заявления о Редактировании для этого полагающегося партийного доверия когда проверенные завершения мастера**, затем нажимаете **Close**

Шаг 10. Вы должны теперь быть принесены к окну, которое похоже на это:



Шаг 11. В этом окне **нажмите Add Правило**.

Шаг 12. Для **шаблона правила Требования** выберите **Send LDAP Attributes** как **Требования** и нажмите **Next**.

Шаг 13. На следующей странице введите **NameID** для имени правила **Требования**

Шаг 14. Выберите **Active Directory** для хранилища **Атрибута**

Шаг 15. Выберите **SAM-Account-Name** для атрибута **LDAP**

Шаг 16. Введите **uid** для **Исходящего Типа Требования**

Примечание: **uid** не является опцией, которая автозаполнится или обнаружится в

выпадающем списке

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

Шаг 17. Нажмите кнопку **Finish**

Шаг 18. Необходимо теперь видеть правило, однако, мы должны будем добавить другое правило, так **нажмите Add Правило** снова.

Шаг 19. Выберите **Send Claims Using a Custom Rule**

Шаг 20. Введите имя правила **Требования** (это может быть чем-либо),

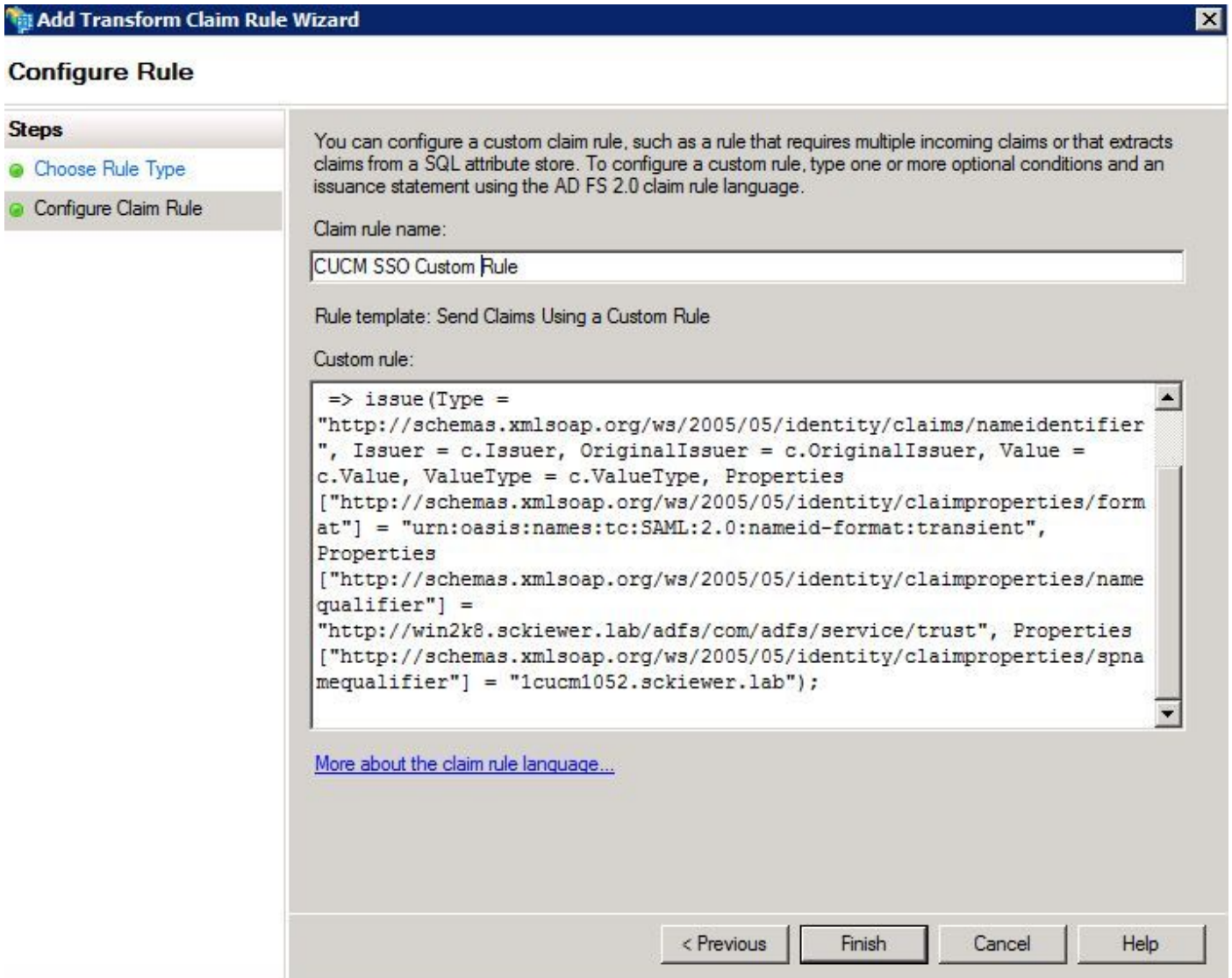
Шаг 21. В поле **Пользовательского правила** вставьте следующий текст:

```
с : [Введите == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"  
=> проблема (Тип = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier", Отправитель = с. Отправитель,  
OriginalIssuer = с. OriginalIssuer, Значение = с. Значение, ValueType = с. ValueType, Свойства  
["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"] = "urn:oasis:names:tc:SAML:2.0:nameid-format:transient",  
Свойства ["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/namequalifier"] =  
"http://<AD\_FS\_SERVICE\_NAME>/adfs/com/adfs/service/trust", Свойства  
["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier"] = "<CUCM\_FQDN>");
```

Шаг 22. Удостоверьтесь, что вы модифицируете два блока синего текста с соответствующими значениями.

Примечание: Если вы не уверены в **AD Имени сервиса FS**, переходите к комментариям

этого документа, чтобы учиться как identify AD Имя сервиса FS.



Шаг 23. Нажмите кнопку Finish

Шаг 24. Нажмите кнопку OK

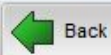
Примечание: Правила требования необходимы для любого Унифицированного Сервера совместной работы, на котором вы хотите использовать SSO.

Закончите Включать SSO на CUCM и запустите Тест SSO

Шаг 1. Теперь, когда AD сервер FS полностью настроен, можно вернуться к CUCM.

Шаг 2. Необходимо находиться на странице, которая похожа на это:

SAML Single Sign-On Configuration



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

2) Launch SSO test page

Run SSO Test...

Back

Cancel

Шаг 3. Разрешение и выбирает вашего Конечного пользователя, который имеет **Стандартную** выбранную роль **Привилегированных пользователей CCM** , и нажмите **Run SSO Test...**

Шаг 4. . Всплывающее окно должно появиться, который может занять приблизительно 30 секунд для загрузки, но в конечном счете вам нужно предоставить проблему войти.

Шаг 5. . Введите пароль, который вы настроили на Сервере LDAP для выбранного пользователя, и необходимо тогда видеть:

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

Шаг 6. Нажмите **Close** на всплывающем окне и затем **Конце**.

SSO теперь настроен в вашей лабораторной работе.

Устранение неисправностей

SSO набора регистрирует для отладки

Чтобы заставить журналы SSO отлаживать вас должны выполнить эту команду в CLI CUCM:
набор `samltrace` отладка уровня

Журналы SSO могут быть загружены от RTMT. Название регистрационного набора является **SSO Cisco**.

Обнаружение имени сервиса федерации

Можно подтвердить имя сервиса федерации путем нажатия **Start** и поиска и вводного менеджмента **AD FS 2.0**.

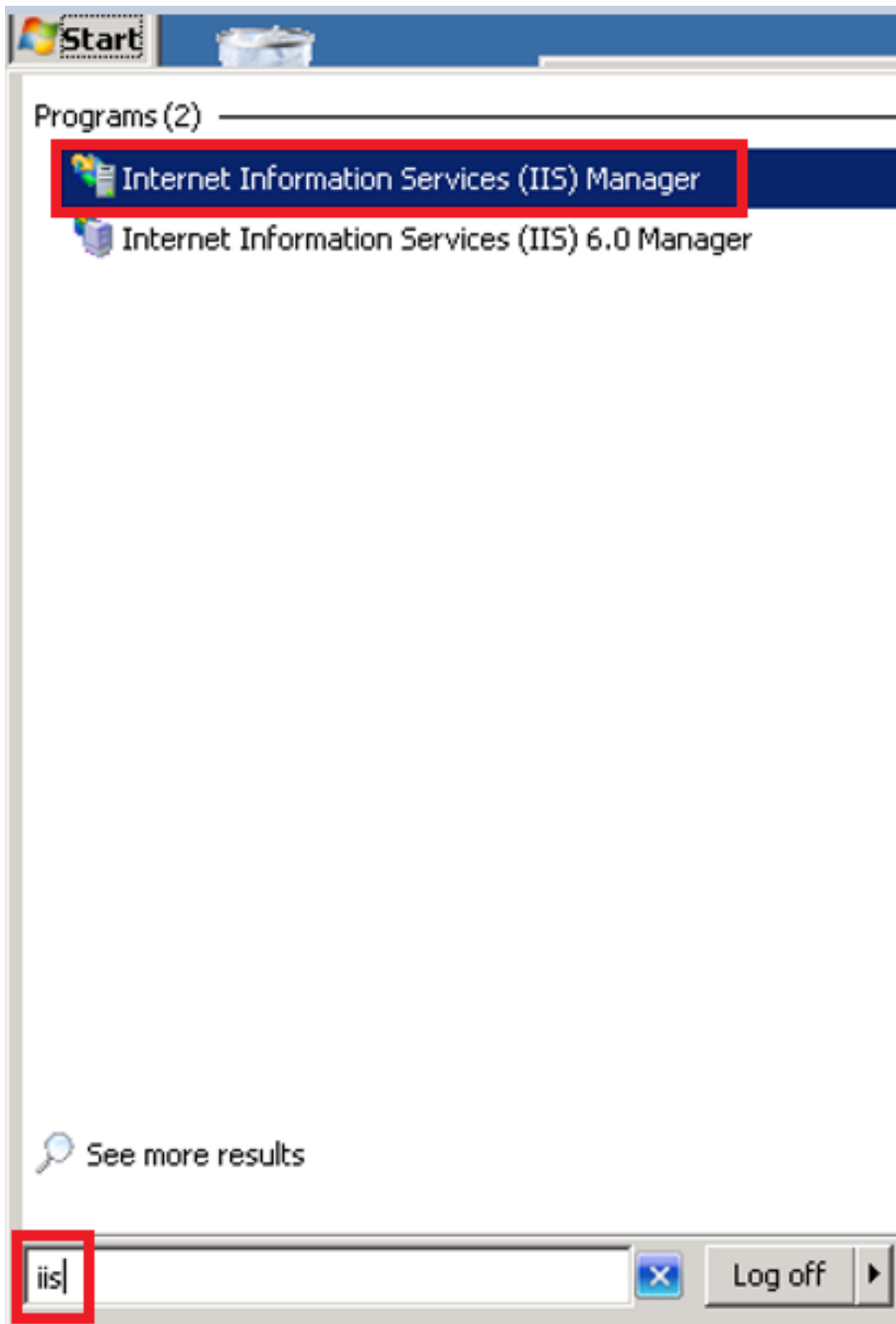
- Щелкните по **Edit Federation Service Properties ...**
- В то время как на Вкладке Общие ищут **Имя сервиса Федерации**

Сертификат Dotless, когда Specifying Имя сервиса Федерации

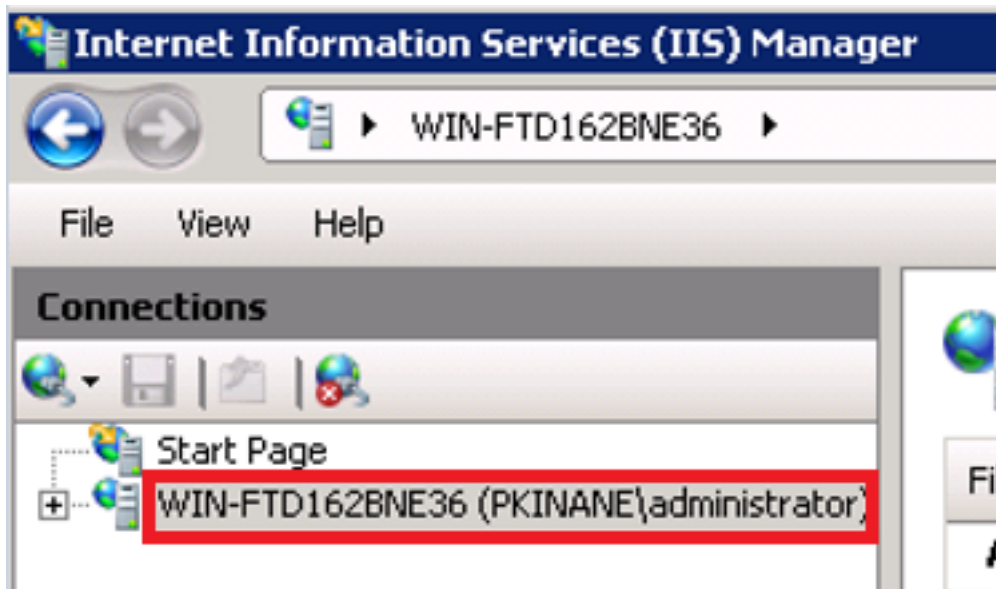
При получении следующего сообщения об ошибке при прохождении через AD мастера настройки FS необходимо будет создать новый сертификат.

"Выбранный сертификат не может использоваться, чтобы решить, что Имя сервиса Федерации because выбранный сертификат имеет dotless (названный) Именем субъекта (например, fabrikam). Выберите другой сертификат без dotless (названного) Именем субъекта (например, fs.fabrikam.com), и затем попробуйте еще раз".

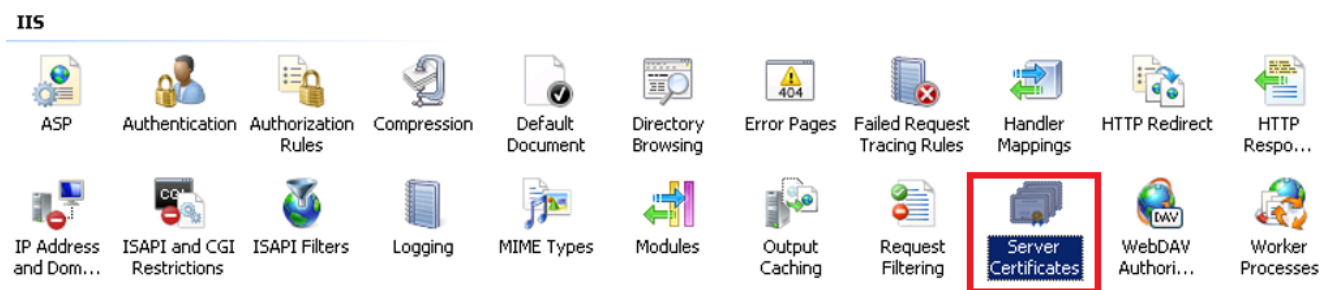
Нажмите Start и ищите iis, тогда открывают Менеджера информационных сервисов интернета (IIS)



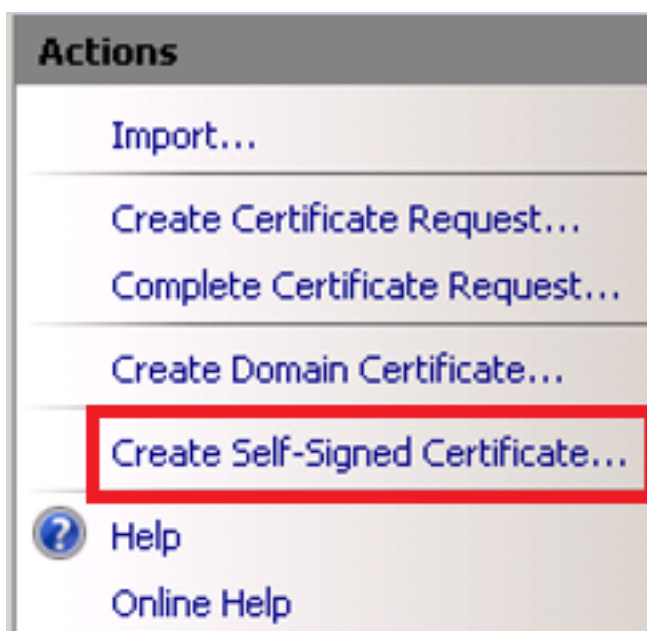
Щелкните по названию своего сервера



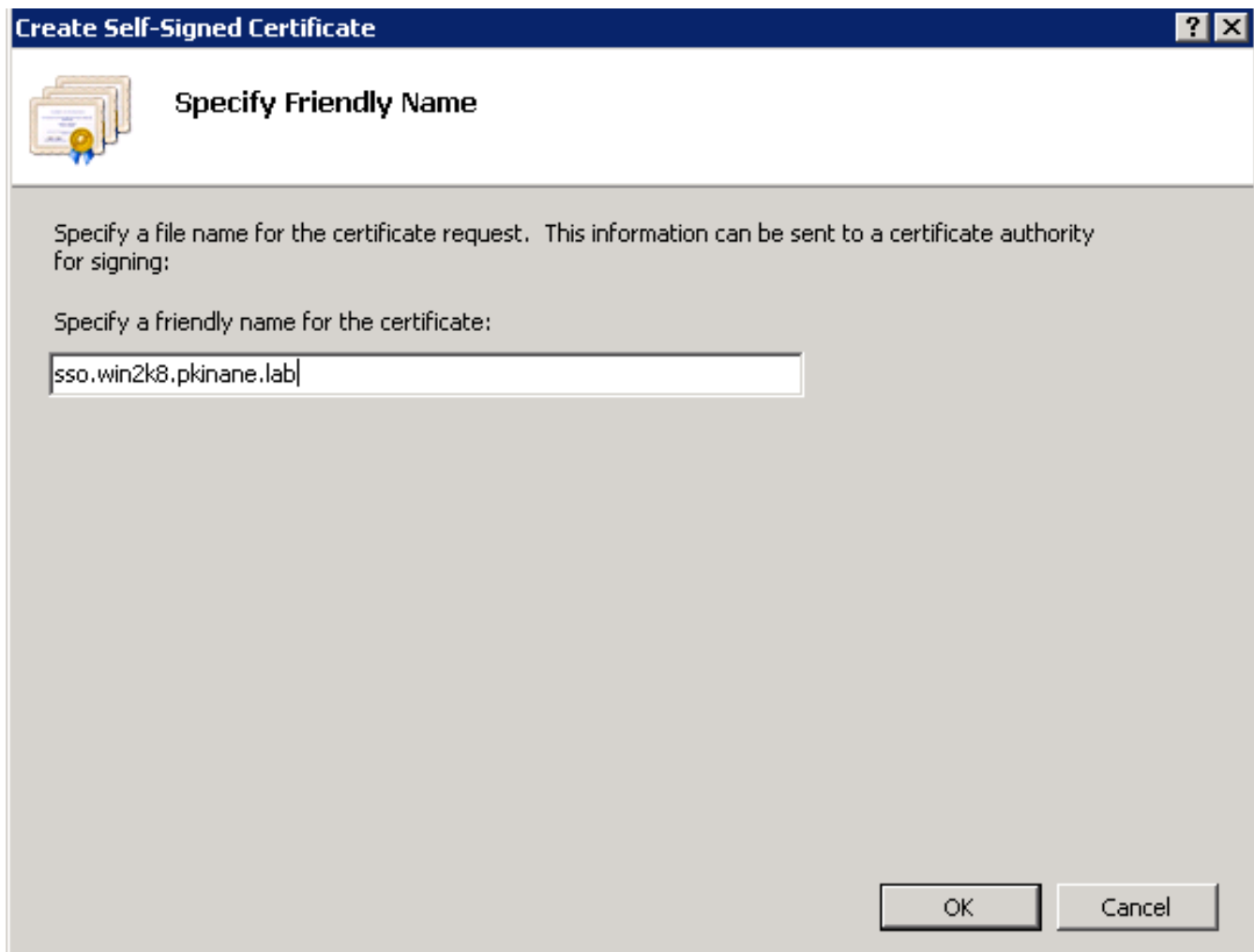
Щелкните по Server Certificates



Щелкните по Create Self-Signed Certificate



Введите имя, которое вы хотите для псевдонима вашего сертификата



Время вне синхронизования между CUCM и серверами IDP

При получении ошибки, упомянутой ниже при попытке запустить тест SSO от CUCM вы, возможно, должны настроить Windows Server для использования тех же серверов NTP в качестве CUCM. Процесс, чтобы сделать это охвачено в комментариях.

"Недопустимый ответ SAML. Когда время вне синхронизования между Cisco Unified Communications Manager и серверами IDP, это может быть вызвано. Проверьте конфигурацию NTP на обоих серверах. Выполните "статус ntp utils" от CLI для проверки этого статуса на Cisco Unified Communications Manager".

Как только Windows Server задали серверы NTP, необходимо получить метаданные от Idp снова и загрузить его к CUCM. Затем пойдите непосредственно в SSO, тестируют и видят, получаете ли вы все еще ту же ошибку.