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 Basick 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

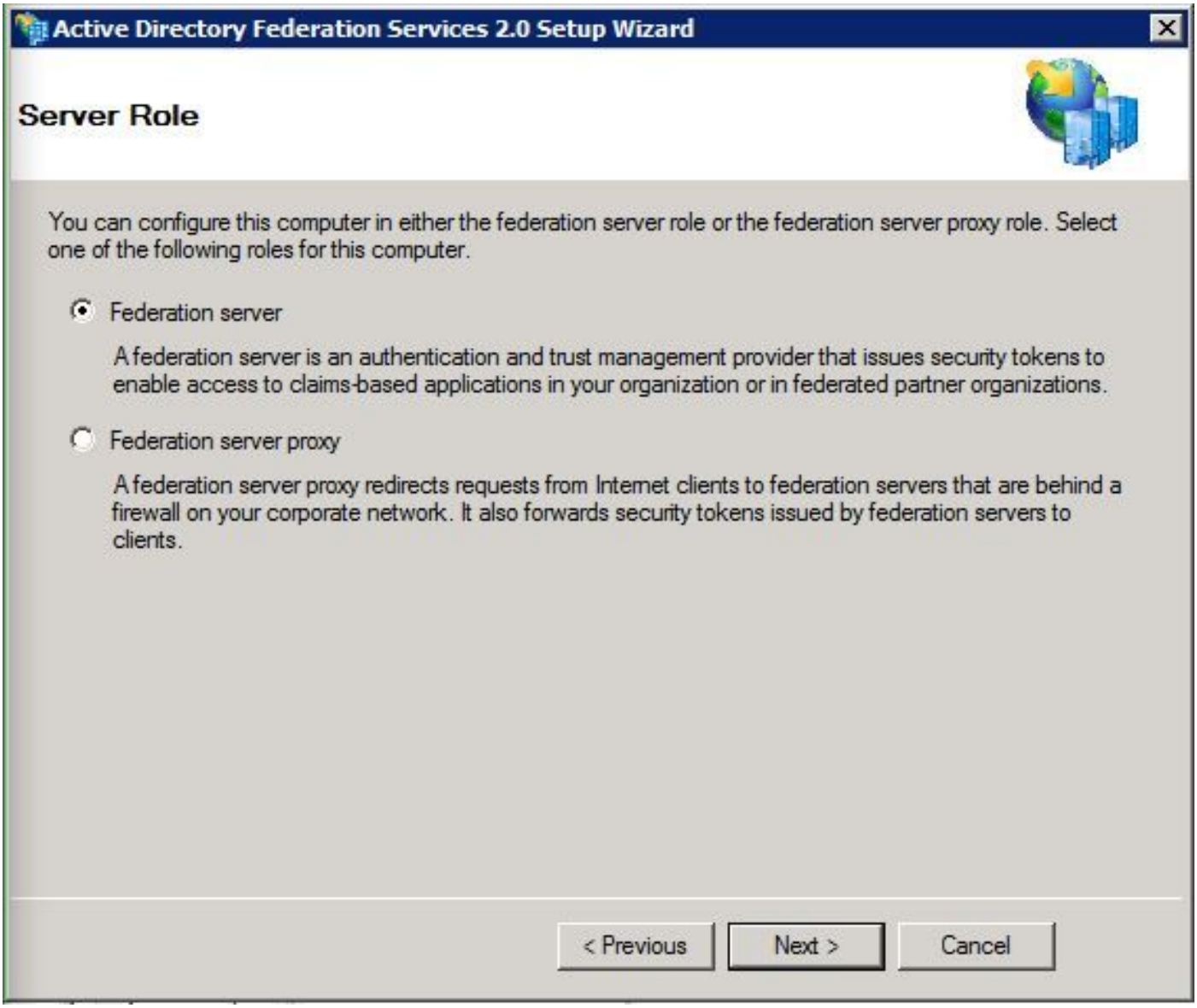
Шаг 1. Перейти к https://www.microsoft.com/en-us/download/details.aspx? id=10909 и нажимают Continue.

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**:



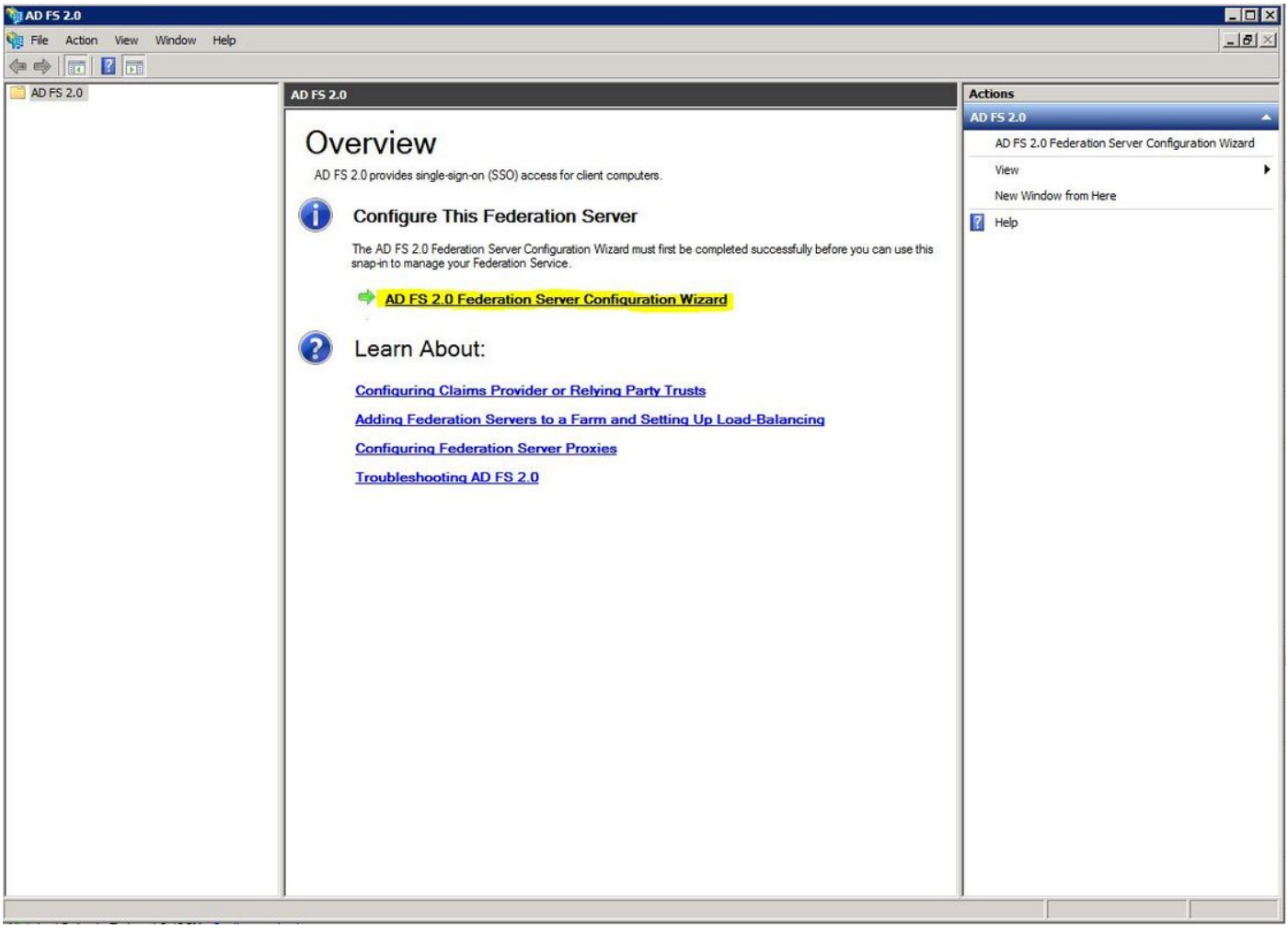
Шаг 6. Некоторые зависимости могут быть установлены автоматически, и вам предлагают нажать **Finish**.

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

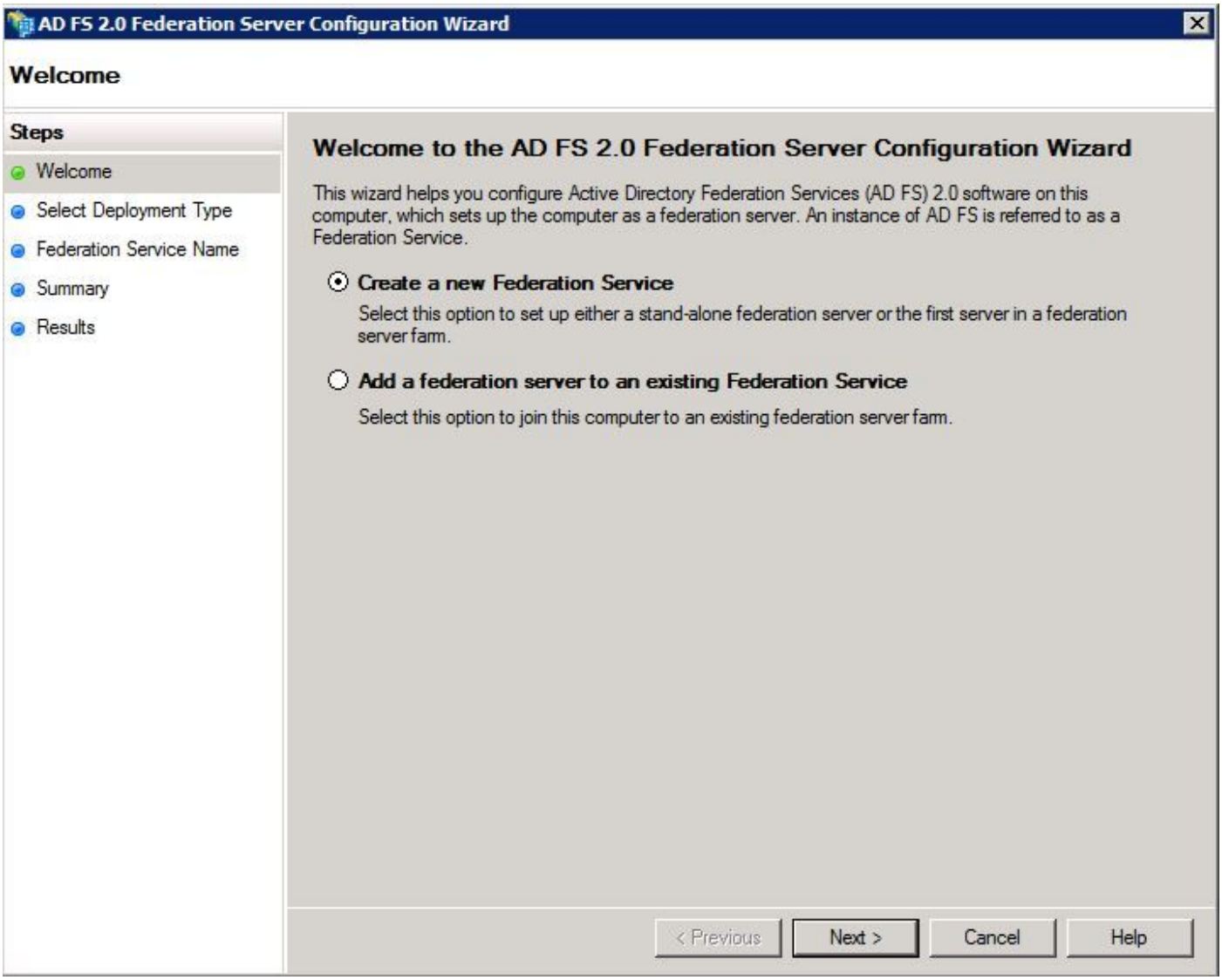
Настройте AD FS 2.0 на своем Windows Server

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.

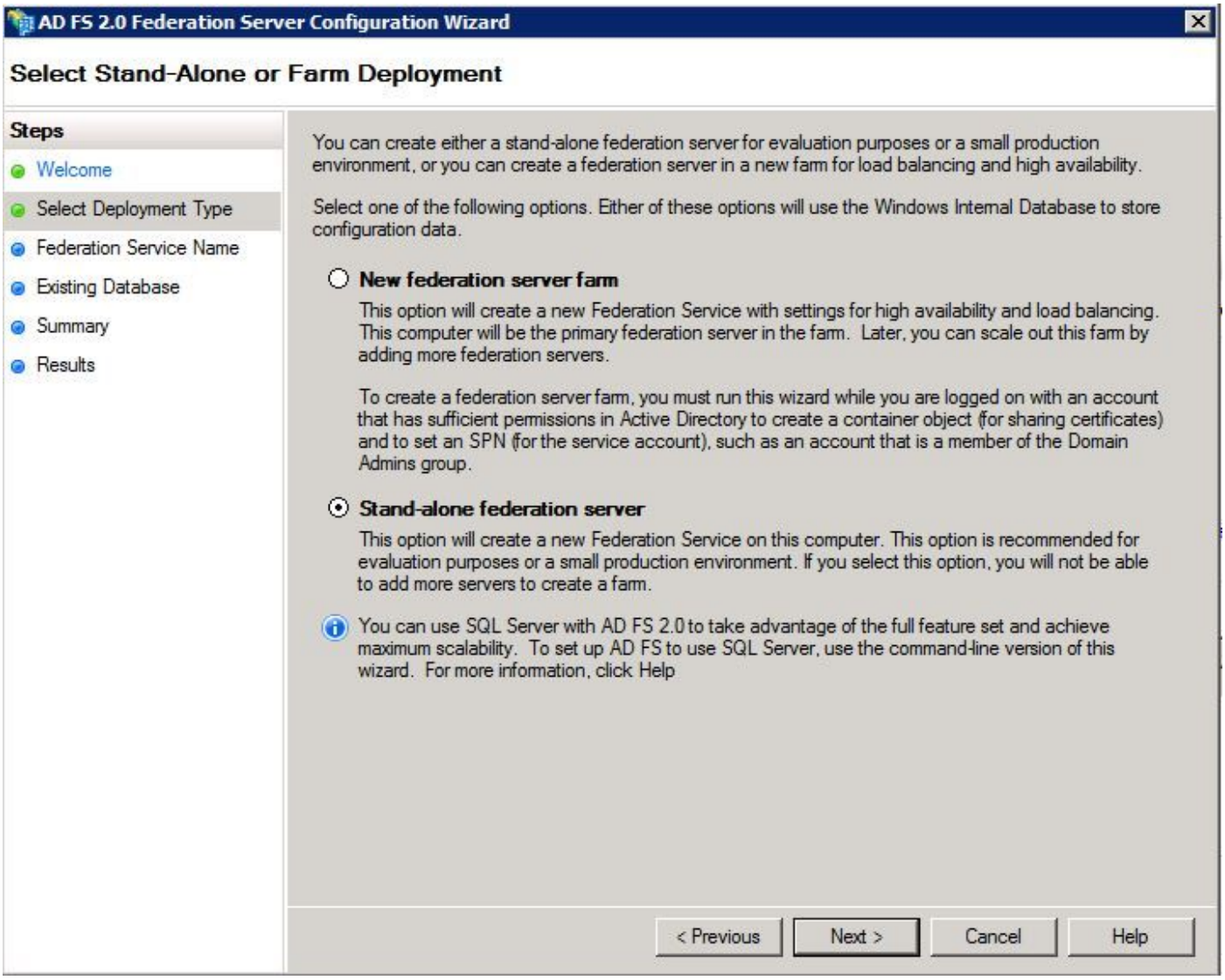
Шаг 2.. Как только у вас есть открытое окно AD FS, выберите **AD FS 2.0 Мастера настройки Федеративного сервера.**



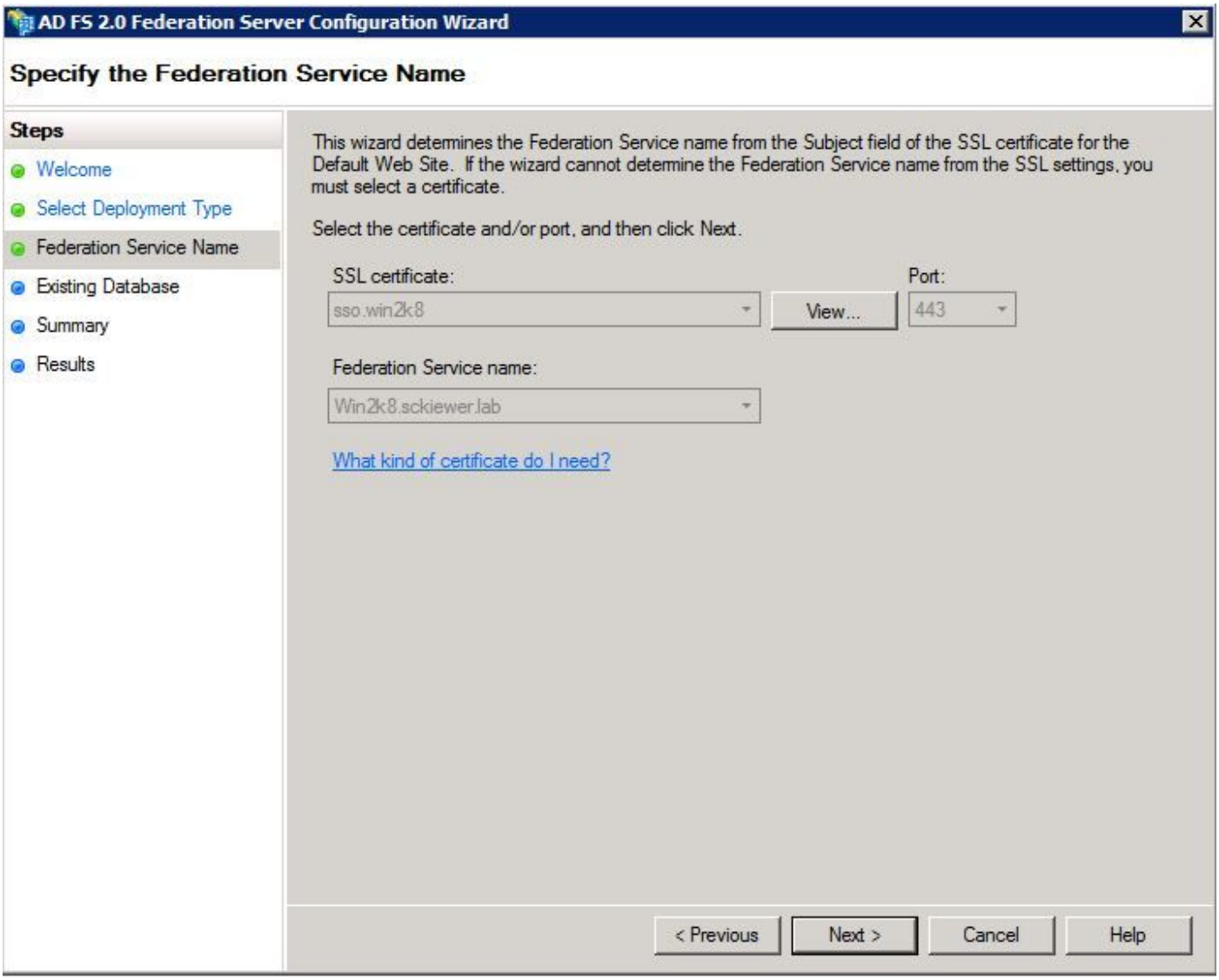
Шаг 3. Затем, нажмите **Create новый Сервис Федерации.**



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**

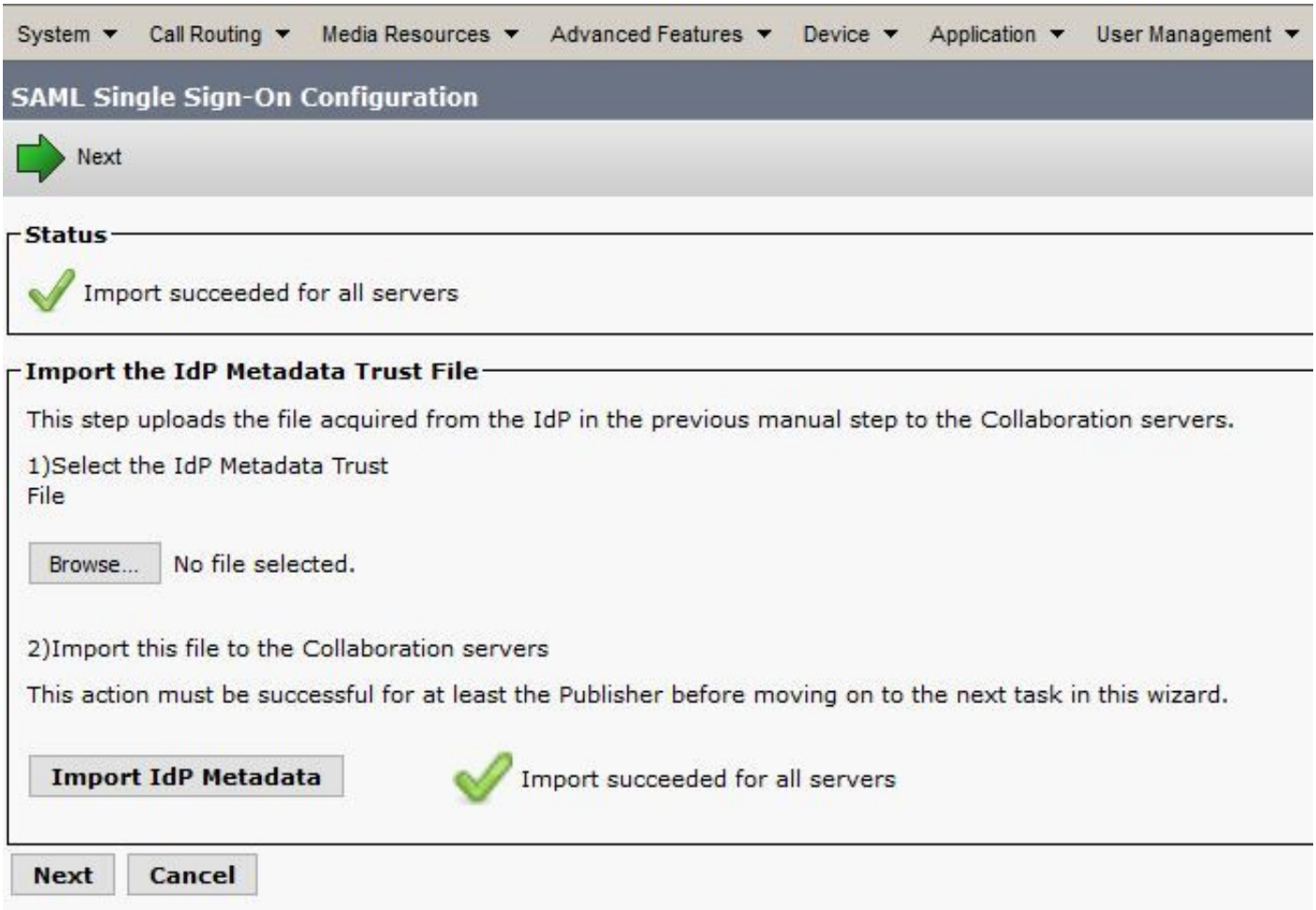
Шаг 4. . Можно получить предупреждение о Соединениях Web-сервера, бывших должных быть перезагруженными, просто пораженными **, Продолжаются**

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:



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 Metatdata к серверу AD FS 2.0 и создайте правила требования

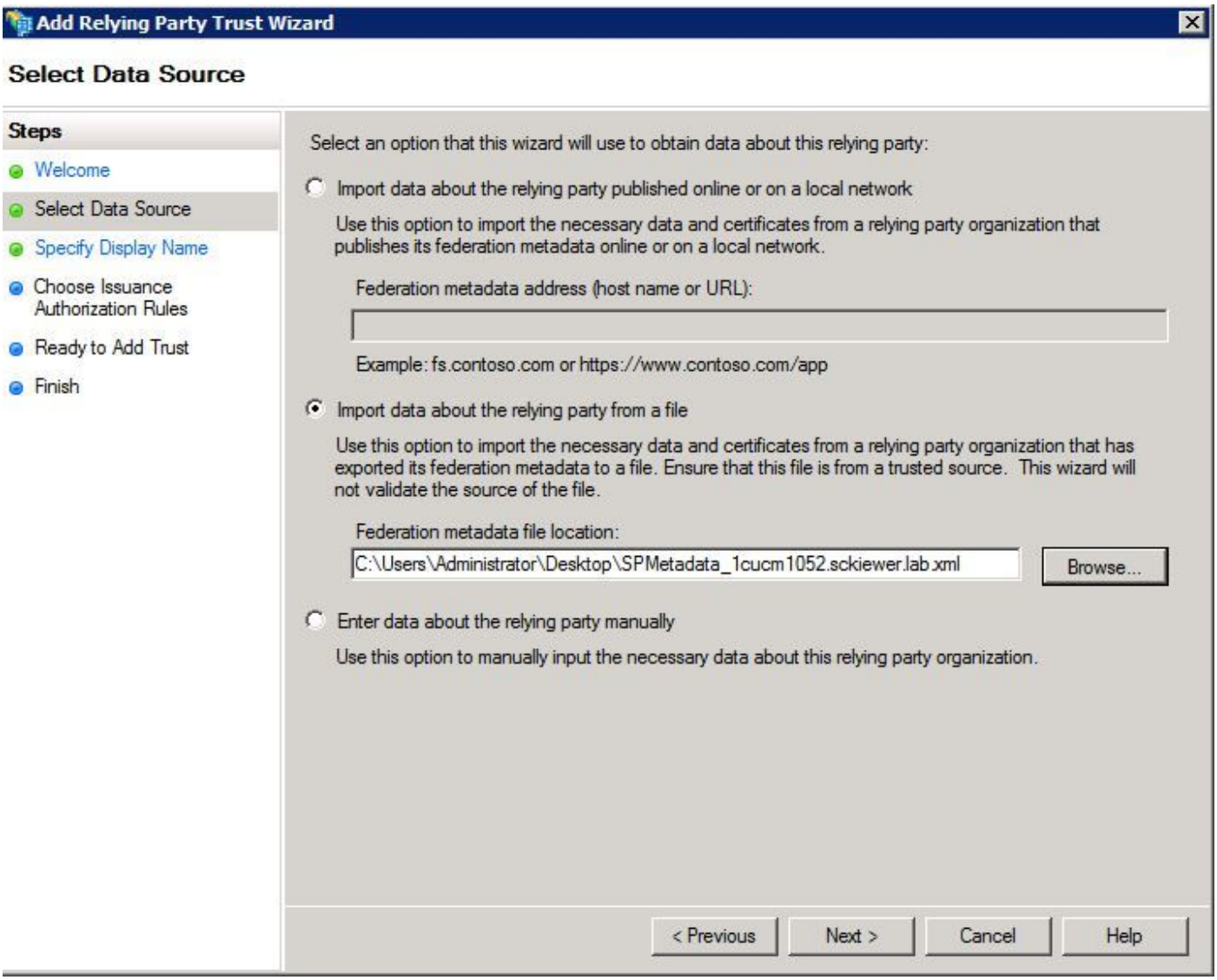
Шаг 1. На этом этапе вернитесь к своему AD серверу FS и откройте окно управления AD FS 2.0 путем нажатия **Start** и поиска **менеджмента AD FS 2.0.**

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 Трастовый** 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.



Шаг 5. . **Нажмите кнопку Next**

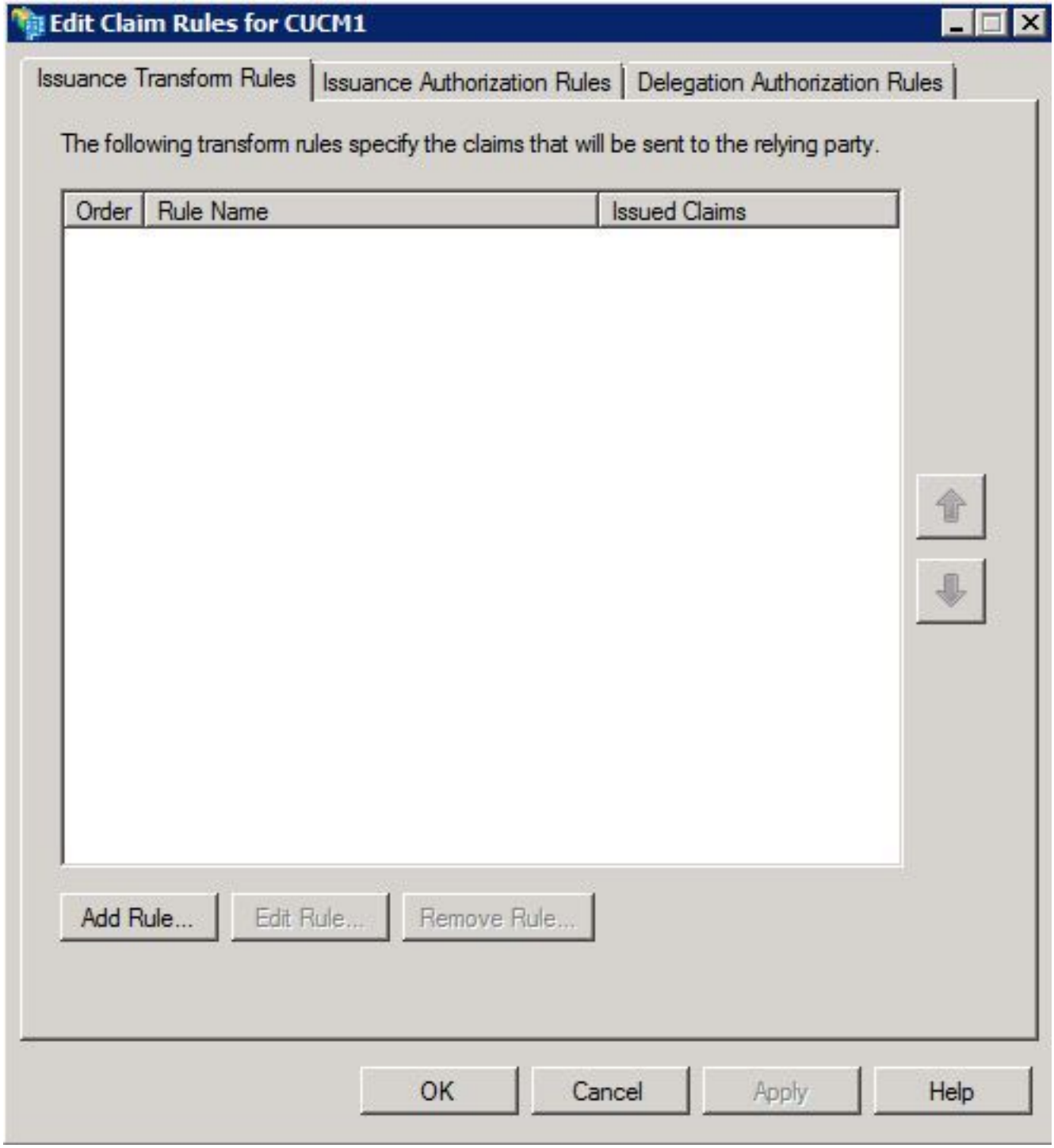
Шаг 6. Отредактируйте **Название Показа** к тому, что вы хотели бы, тогда нажимают **Next.**

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**

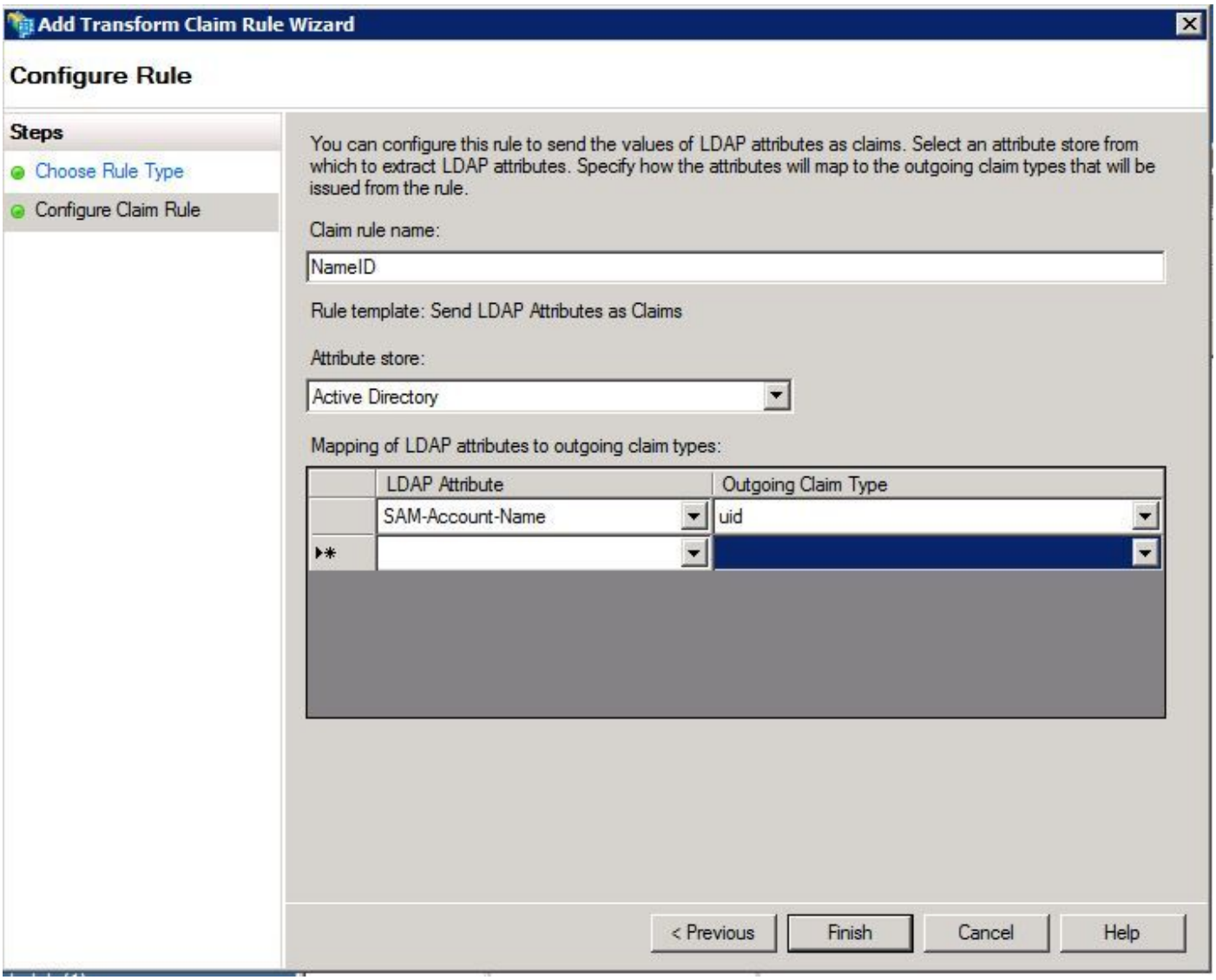
Шаг 14. Выберите **Active Directory** для **хранилища Атрибута**

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



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),

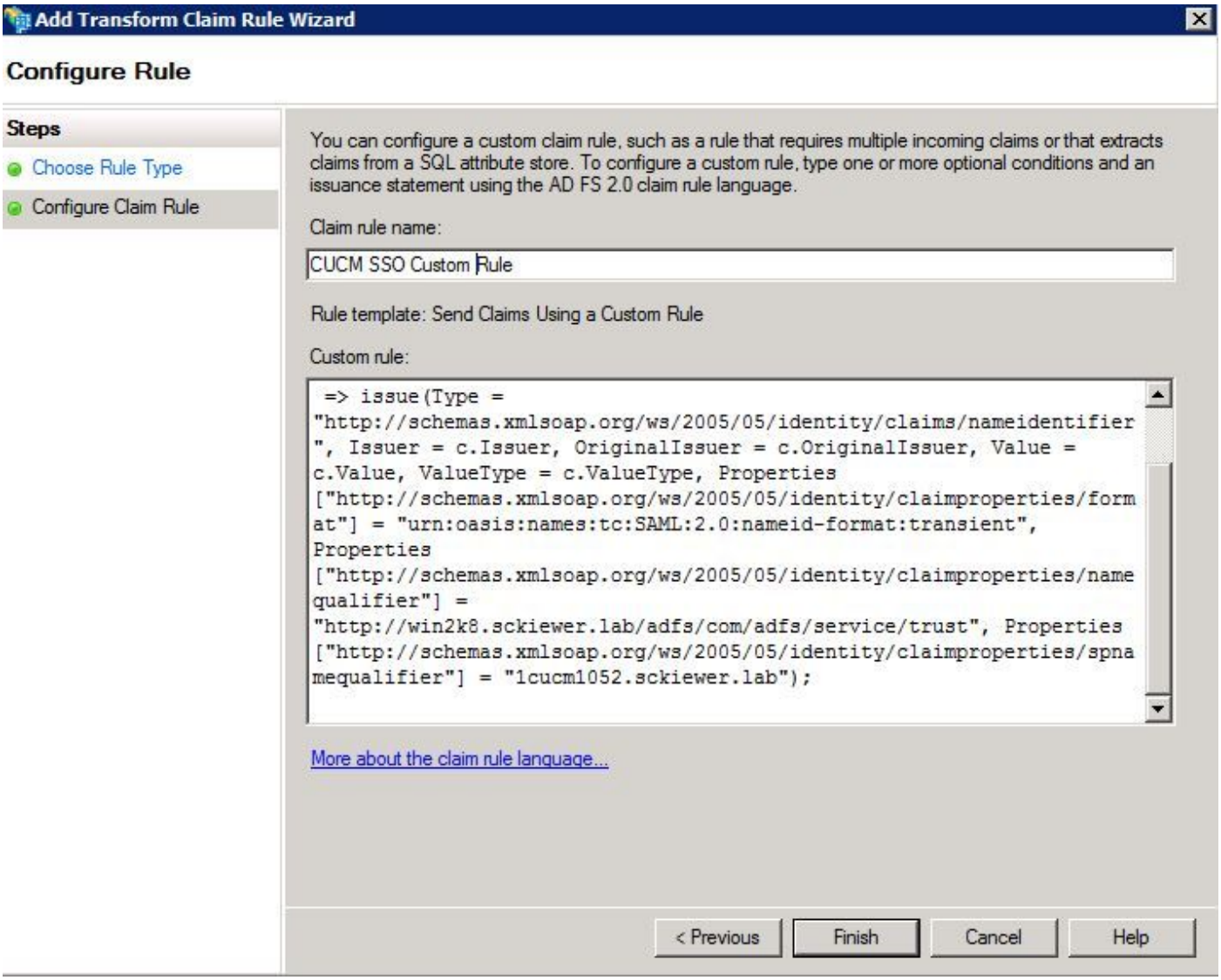
Шаг 21. В поле **Пользовательского правила** вставьте следующий текст:

```
c : [Введите == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"]
 => проблема (Тип = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier", Отправитель = c. Отправитель,
OriginalIssuer = c. OriginalIssuer, Значение = c. Значение, ValueType = c. 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 idendtify **AD Имя сервиса FS.**



Шаг 23. **Нажмите кнопку Finish**

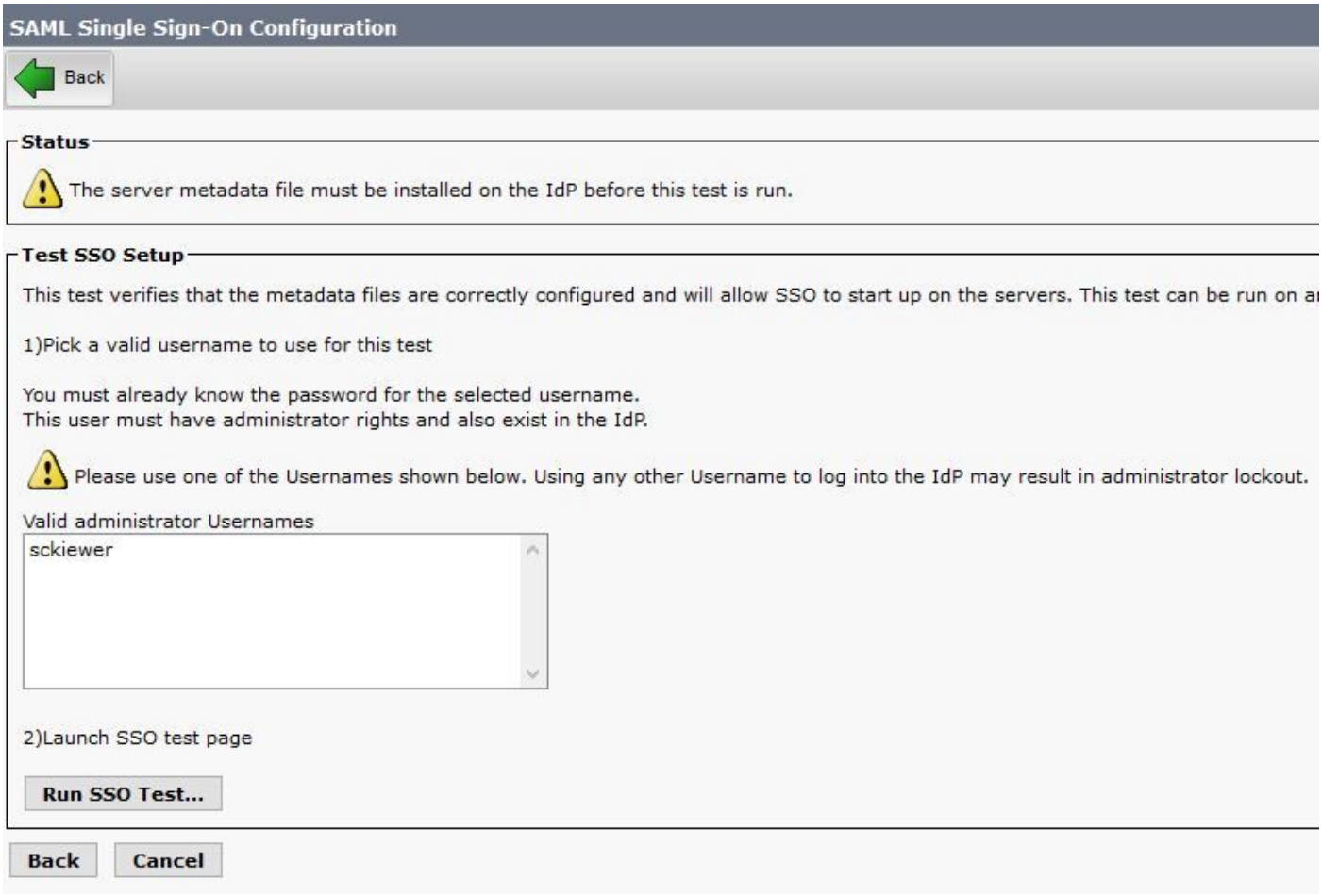
Шаг 24. **Нажмите кнопку OK**

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:



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:

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**.

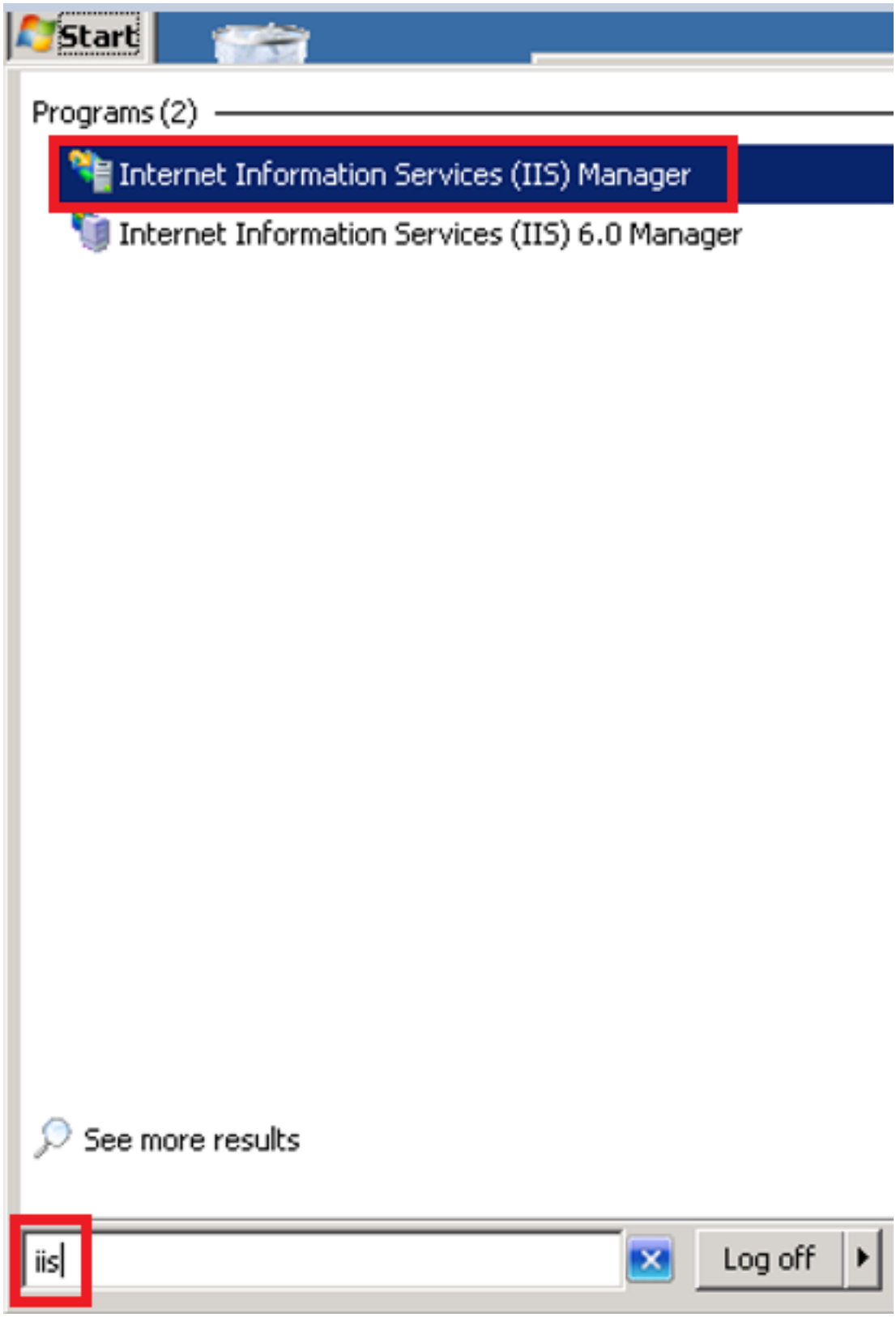
• Щелкните **по Edit Federation Service Properties …**
• В то время как на Вкладке Общие ищут **Имя сервиса Федерации**

Сертификат Dotless, когда Specifing Имя сервиса Федерации

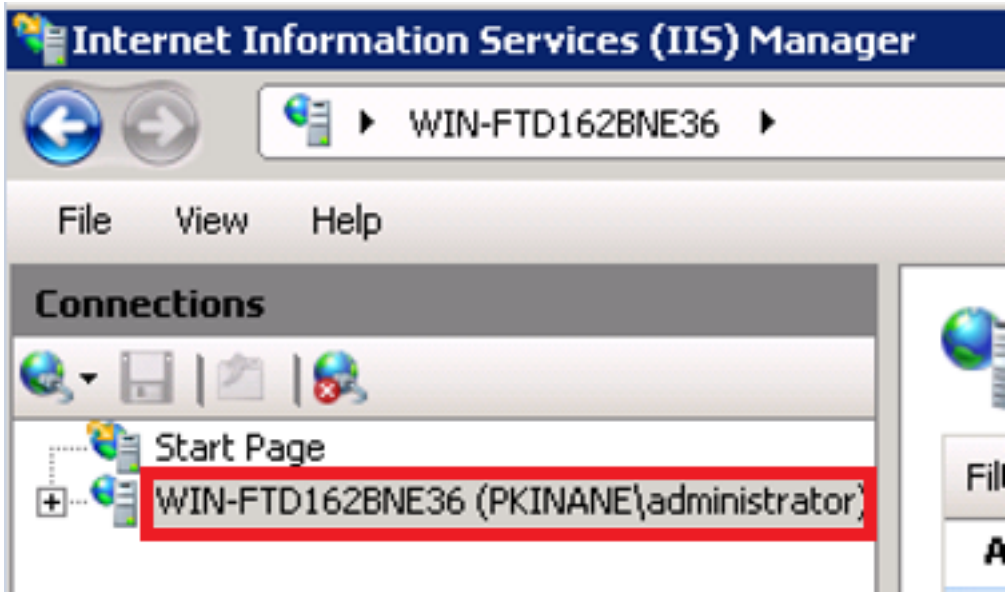
При получении следующего сообщения об ошибке при прохождении через AD мастера настройки FS необходимо будет создать новый сертификат.

"Выбранный сертификат не может использоваться, чтобы решить, что Имя сервиса Федерации becuase 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".

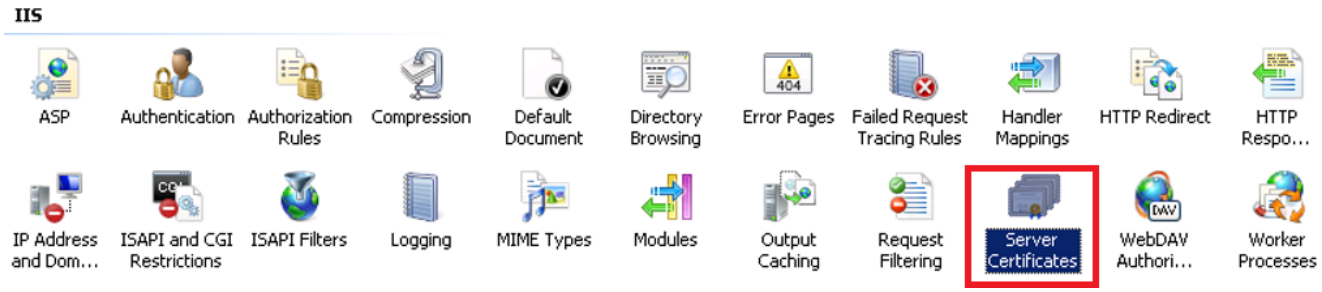
Нажмите Start и ищите iis, тогда открывают Менеджера информационных сервисов интернета (IIS)



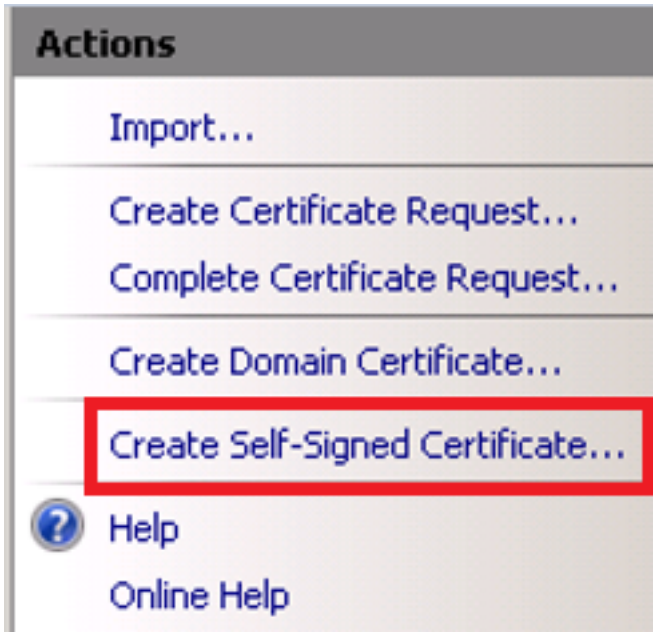
Щелкните по названию своего сервера



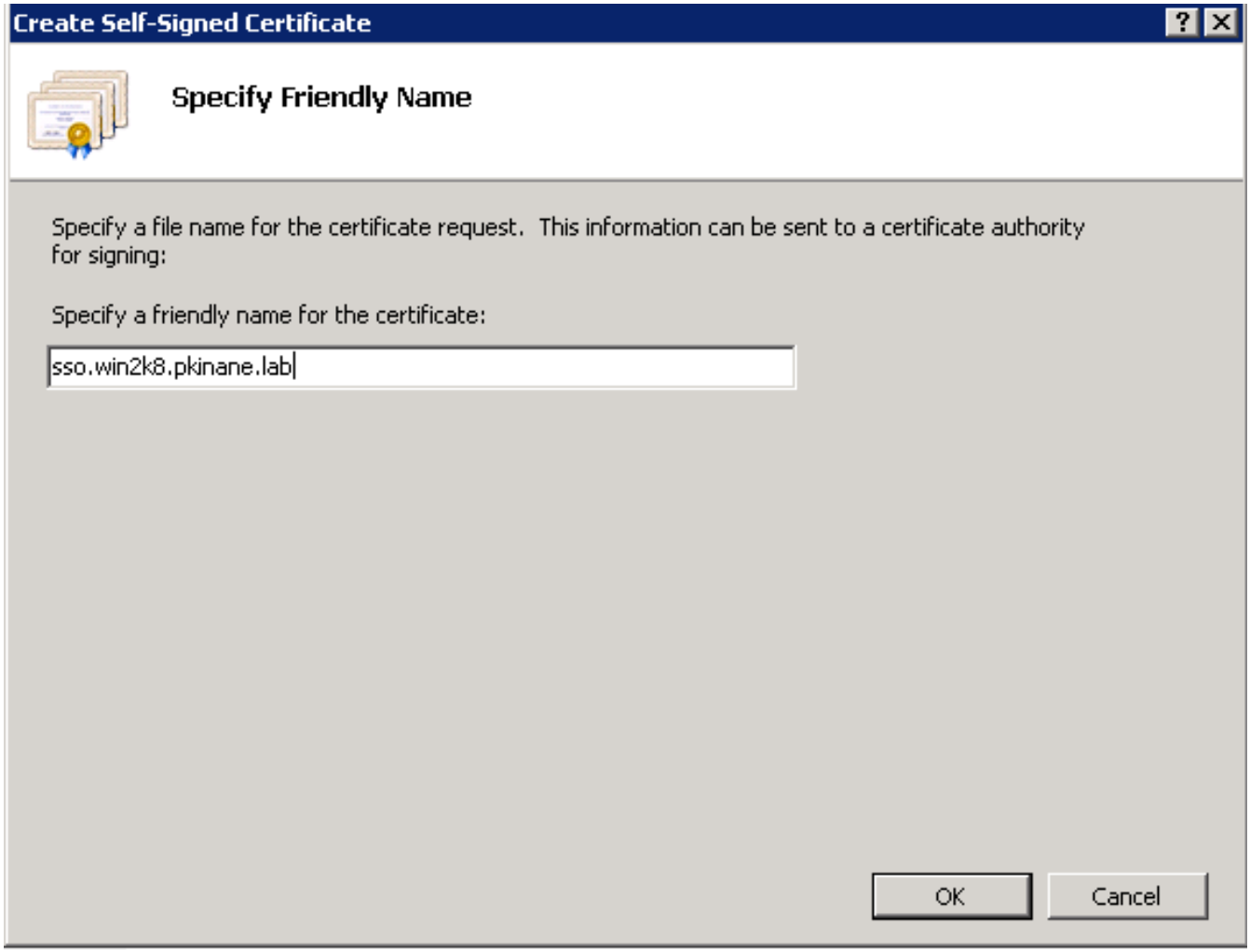
Щелкните по Server Certificates



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.