

Configurare Single Sign-On con CUCM e AD FS 2.0

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Scaricare e installare AD FS 2.0 sul server Windows](#)

[Configurare AD FS 2.0 sul server Windows](#)

[Importare i metadati Idp in CUCM / Scaricare i metadati CUCM](#)

[Importa metadati CUCM nel server AD FS 2.0 e crea regole attestazione](#)

[Completare l'abilitazione di SSO su CUCM ed eseguire il test SSO](#)

[Risoluzione dei problemi](#)

[Imposta log SSO su debug](#)

[Trova Nome Servizio Federativo](#)

[Nome Servizio Federativo E Certificato Senza Punto](#)

[Tempo non sincronizzato tra i server CUCM e IDP](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come configurare Single Sign-On (SSO) su Cisco Unified Communications Manager e Active Directory Federation Service.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Unified Communications Manager (CUCM)
- Conoscenze di base di Active Directory Federation Service (ADFS)

Per abilitare l'SSO nell'ambiente di emulazione, è necessario disporre della seguente configurazione:

- Windows Server con ADFS installato.
- CUCM con sincronizzazione LDAP configurata.
- Utente finale con il ruolo Utenti privilegiati CCM standard selezionato.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Windows Server con AD FS 2.0
- CUCM 10.5.2

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico

ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Viene fornita la procedura per ADFS 2.0 con Windows Server 2008 R2. Questi passaggi funzionano anche per AD FS 3.0 in Windows Server 2016.

Scaricare e installare AD FS 2.0 sul server Windows

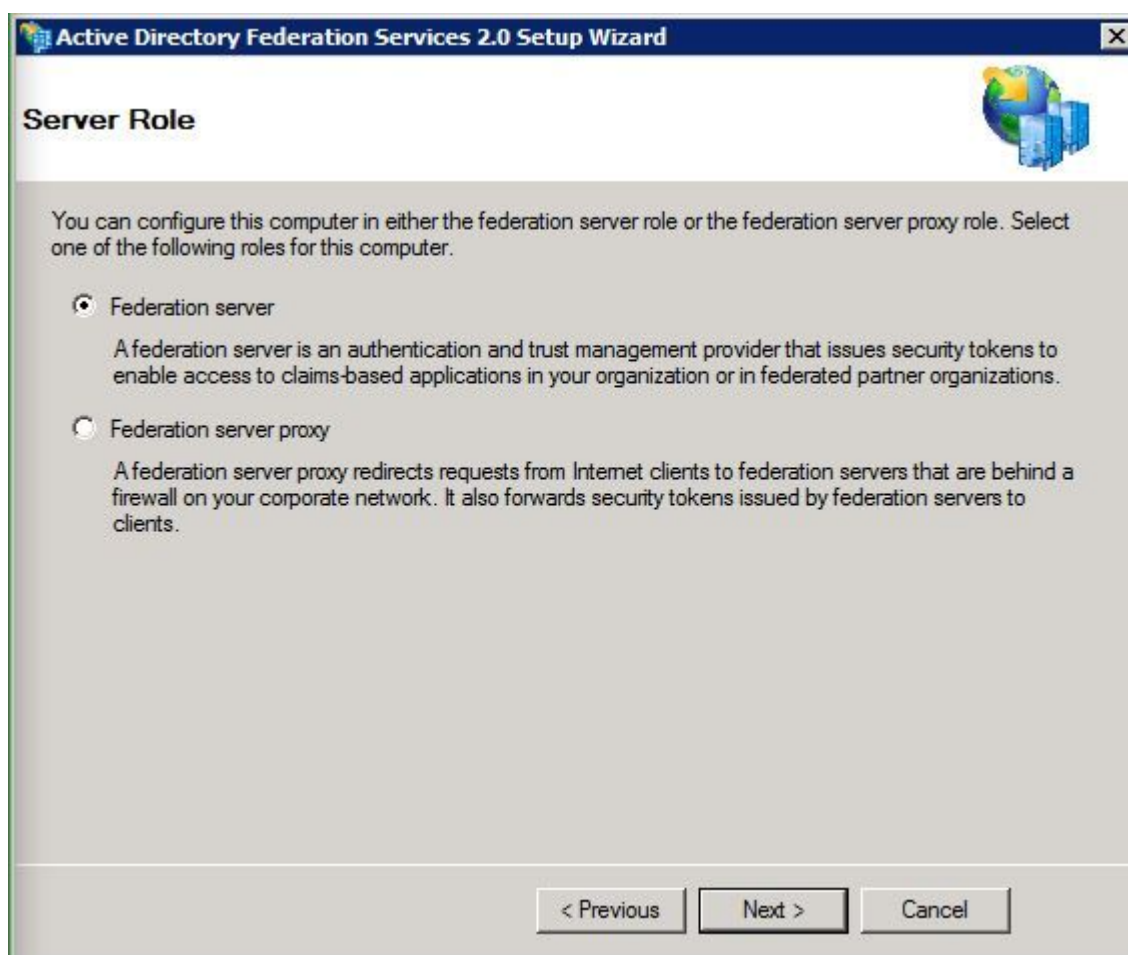
Passaggio 1. Passare a [Scarica ADFS 2.0](#).

Passaggio 2. Assicurarsi di selezionare il download appropriato in base al server Windows in uso.

Passaggio 3. **Spostare** il file scaricato sul server Windows.

Passaggio 4. Procedere con l'installazione:

Passaggio 5. Quando richiesto, scegliere **Server federativo**:



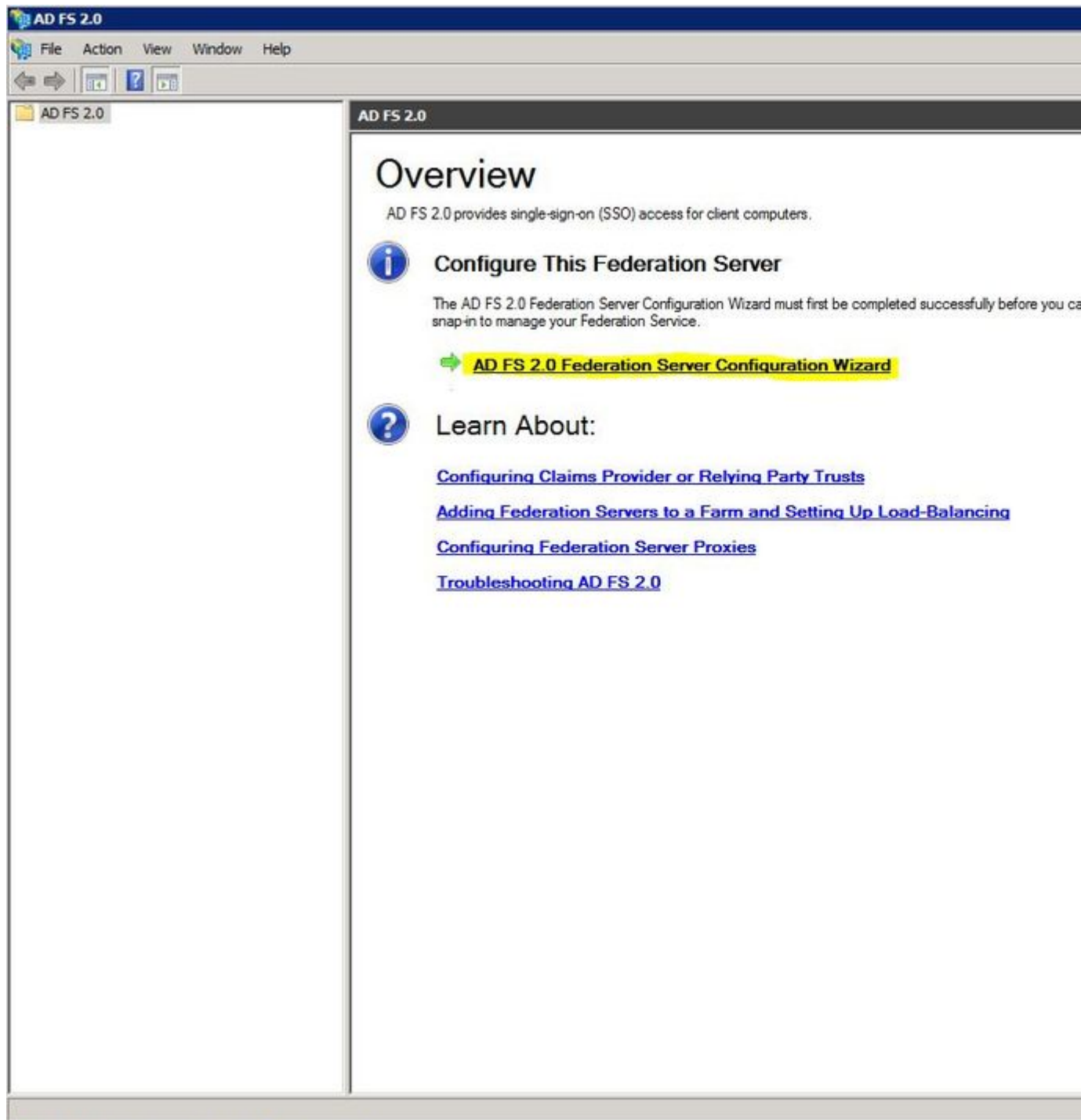
Passaggio 6. Alcune dipendenze vengono installate automaticamente. Al termine, fare clic su **Fine**.

Dopo avere installato ADFS 2.0 nel server, è necessario aggiungere alcune configurazioni.

Configurare AD FS 2.0 sul server Windows

Passaggio 1. Se dopo l'installazione la finestra di AD FS 2.0 non viene aperta automaticamente, è possibile fare clic su **Start** e cercare Gestione AD FS 2.0 per aprirla manualmente.

Passaggio 2. Scegliere **Configurazione guidata server federativo ADFS 2.0**.



Passaggio 3. Fare quindi clic su **Crea nuovo servizio federativo**.

Welcome

Steps

- Welcome
- Select Deployment Type
- Federation Service Name
- Summary
- Results

Welcome to the AD FS 2.0 Federation Server Configuration Wizard

This wizard helps you configure Active Directory Federation Services (AD FS) 2.0 software on this computer, which sets up the computer as a federation server. An instance of AD FS is referred to as a Federation Service.

Create a new Federation Service

Select this option to set up either a stand-alone federation server or the first server in a federation server farm.

Add a federation server to an existing Federation Service

Select this option to join this computer to an existing federation server farm.

< Previous

Next >

Cancel

Help

Passaggio 4. Per la maggior parte degli ambienti è sufficiente il **server federativo autonomo**.

Select Stand-Alone or Farm Deployment

Steps

- Welcome
- Select Deployment Type
- Federation Service Name
- Existing Database
- Summary
- Results

You can create either a stand-alone federation server for evaluation purposes or a small production environment, or you can create a federation server in a new farm for load balancing and high availability.

Select one of the following options. Either of these options will use the Windows Internal Database to store configuration data.

 New federation server farm

This option will create a new Federation Service with settings for high availability and load balancing. This computer will be the primary federation server in the farm. Later, you can scale out this farm by adding more federation servers.

To create a federation server farm, you must run this wizard while you are logged on with an account that has sufficient permissions in Active Directory to create a container object (for sharing certificates) and to set an SPN (for the service account), such as an account that is a member of the Domain Admins group.

 Stand-alone federation server

This option will create a new Federation Service on this computer. This option is recommended for evaluation purposes or a small production environment. If you select this option, you will not be able to add more servers to create a farm.

i You can use SQL Server with AD FS 2.0 to take advantage of the full feature set and achieve maximum scalability. To set up AD FS to use SQL Server, use the command-line version of this wizard. For more information, click Help

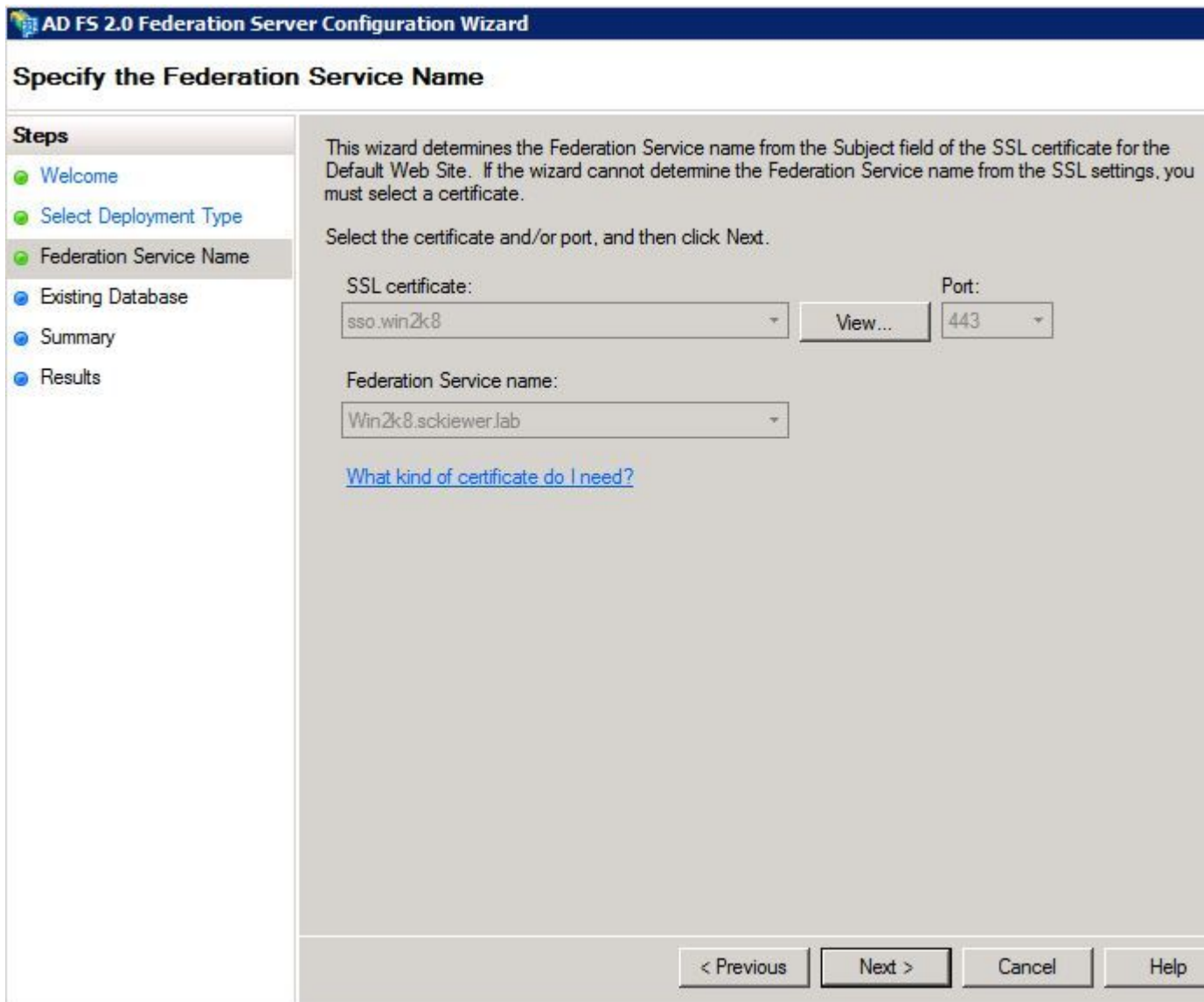
< Previous

Next >

Cancel

Help

Passaggio 5. Successivamente, verrà richiesto di scegliere un certificato. Questo campo viene compilato automaticamente se il server dispone di un certificato.



Passaggio 6. Se nel server è già presente un database ADFS, è necessario rimuoverlo per continuare.

Passaggio 7. Viene infine visualizzata una schermata di riepilogo in cui è possibile fare clic su **Avanti**.

Importare i metadati Idp in CUCM / Scaricare i metadati CUCM

Passaggio 1. Aggiornare l'URL con il nome host/FQDN del server Windows e scaricare i metadati dal server AD FS - <https://hostname/federationmetadata/2007-06/federationmetadata.xml>

Passaggio 2. Passare a **Cisco Unified CM Administration > System > SAML Single Sign-On** (Amministrazione Cisco Unified CM > Sistema > SAML Single Sign-On).

Passaggio 3. Fare clic su **Abilita SSO SAML**.

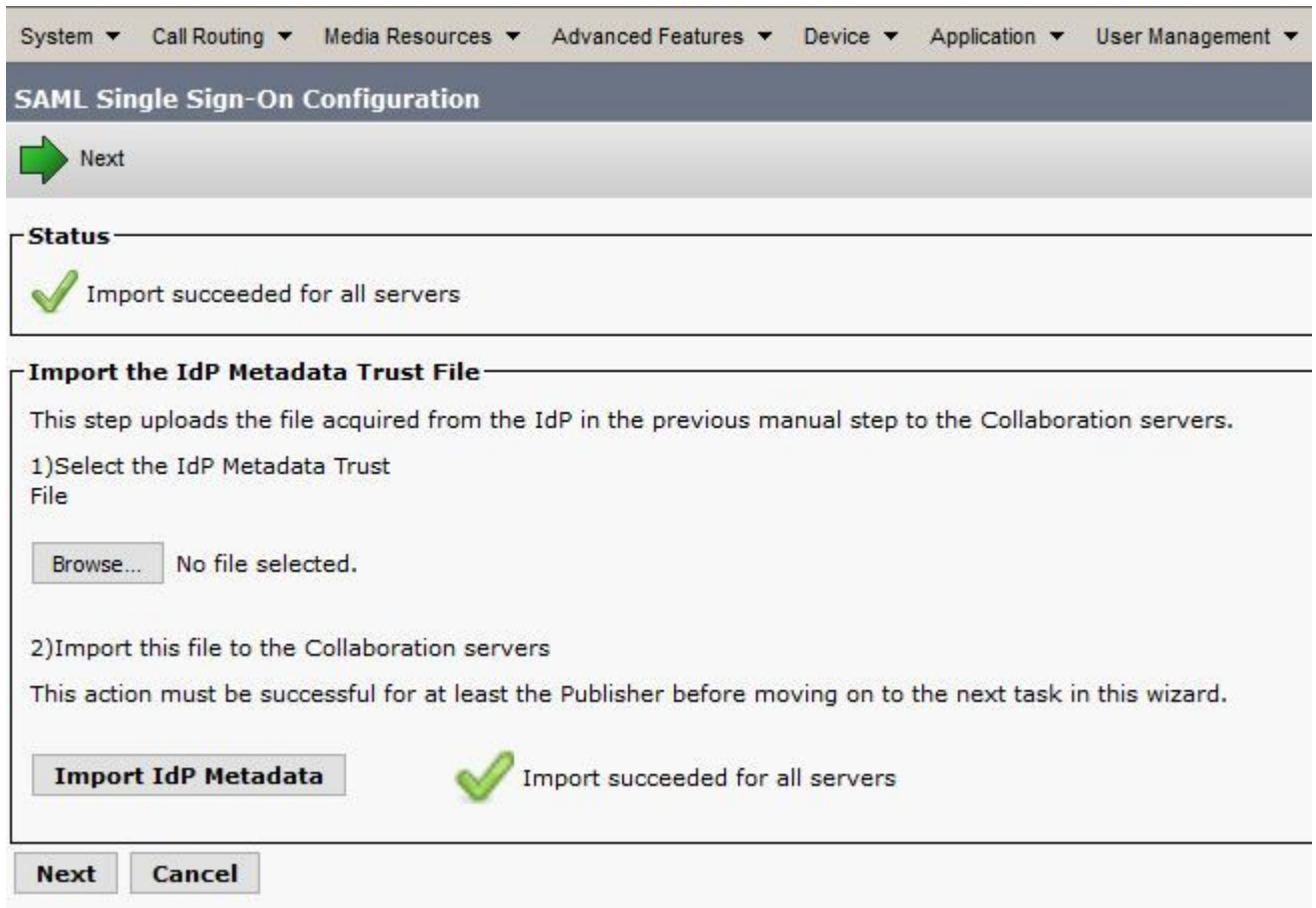
Passaggio 4. Se viene visualizzato un avviso relativo alle connessioni al server Web, fare clic su **Continua**.

Passaggio 5. Successivamente, CUCM richiede di scaricare il file di metadati dal proprio IdP. In questo scenario, il server AD FS è l'IdP e i metadati sono stati scaricati nel passaggio 1, quindi fare clic su

Avanti.

Passaggio 6. Fate clic su **Sfoggia (Browse) > Seleziona il file .xml dal passo 1 > Fate clic su Importa metadati IdP (Import IdP Metadata).**

Passaggio 7. Un messaggio indica che l'importazione è stata completata:



Passaggio 8. Fare clic su Next (Avanti).

Passaggio 9. Ora che i metadati IdP sono stati importati in CUCM, è necessario importare i metadati di CUCM nel proprio IdP.

Passaggio 10. Fare clic su **Scarica file metadati attendibili.**

Passaggio 11. Fare clic su Next (Avanti).

Passaggio 12. Spostare il file .zip sul server Windows ed estrarre il contenuto in una cartella.

Importa metadati CUCM nel server AD FS 2.0 e crea regole attestazione

Passaggio 1. Fare clic su **Start** e cercare **Gestione AD FS 2.0.**

Passaggio 2. Fare clic su **Obbligatorio: aggiungere un componente attendibile.**

Nota: se questa opzione non è visualizzata, è necessario chiudere la finestra ed aprirla di nuovo.

Passaggio 3. Dopo aver aperto **Aggiunta guidata attendibilità componente**, fare clic su **Avvia**.

Passaggio 4. È necessario importare i file XML estratti nel passaggio 12. Selezionare **Importa i dati relativi al componente da un file** e selezionare i file della cartella e scegliere il codice XML per l'editore.

Nota: utilizzare i passaggi precedenti per qualsiasi server Unified Collaboration su cui si intende utilizzare SSO.

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, a 'Steps' pane lists: Welcome, Select Data Source (highlighted), Specify Display Name, Choose Issuance Authorization Rules, Ready to Add Trust, and Finish. The main area contains three radio button options:

- 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 with path 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 right, there are four buttons: '< Previous', 'Next >', 'Cancel', and 'Help'.

Passaggio 5. Fare clic su Next (Avanti).

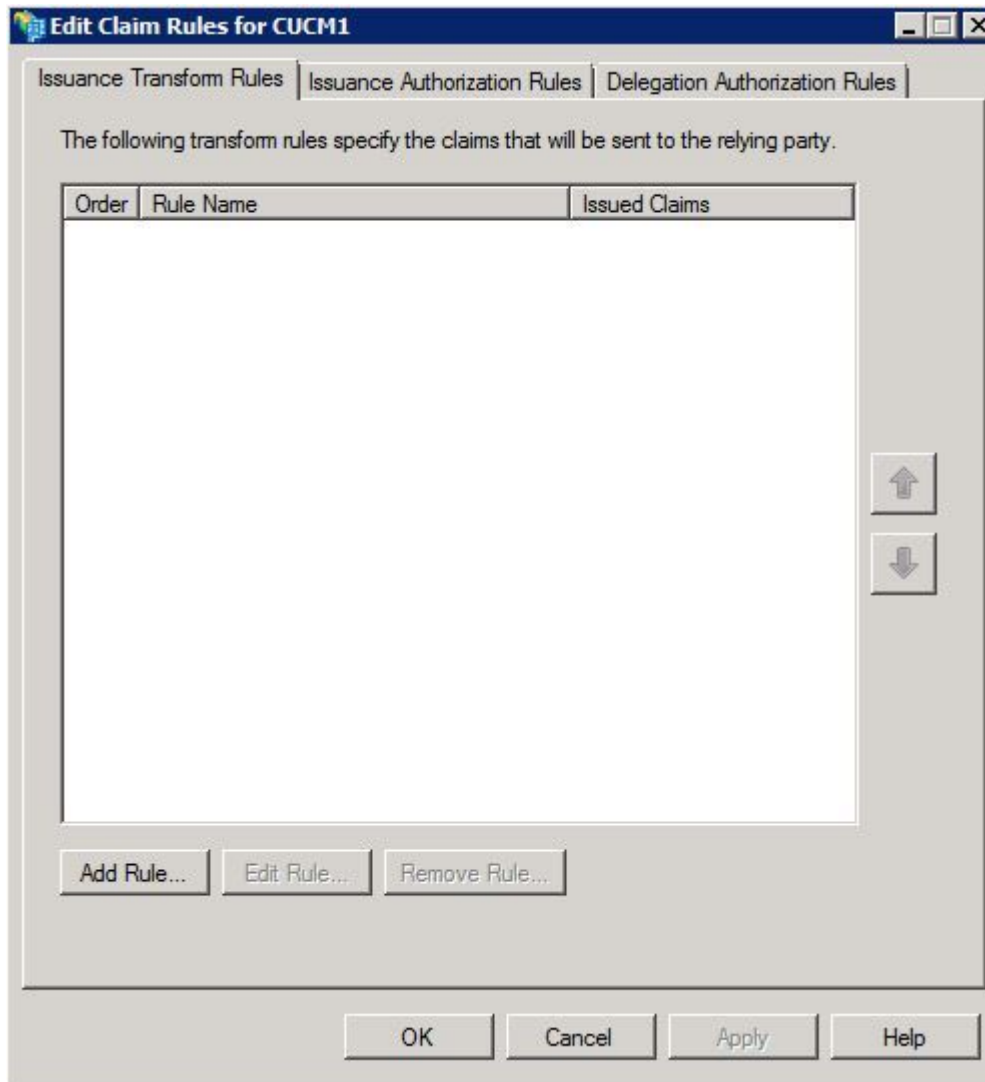
Passaggio 6. Modificare il **nome visualizzato** e fare clic su **Avanti**.

Passaggio 7. Scegliere **Consenti a tutti gli utenti di accedere a questo componente** e fare clic su **Avanti**.

Passaggio 8. Fare di nuovo clic su **Avanti**.

Passaggio 9. In questa schermata assicurarsi di avere **aperto la finestra di dialogo Modifica regole attestazione per l'attendibilità del componente quando la procedura guidata viene selezionata** e quindi fare clic su **Chiudi**.

Passaggio 10. Viene visualizzata la finestra Modifica regole attestazione.



Passaggio 11. In questa finestra fare clic su **Aggiungi regola**.

Passaggio 12. Per il **modello di regola attestazione**, scegliere **Invia attributi LDAP come attestazioni** e fare clic su **Avanti**.

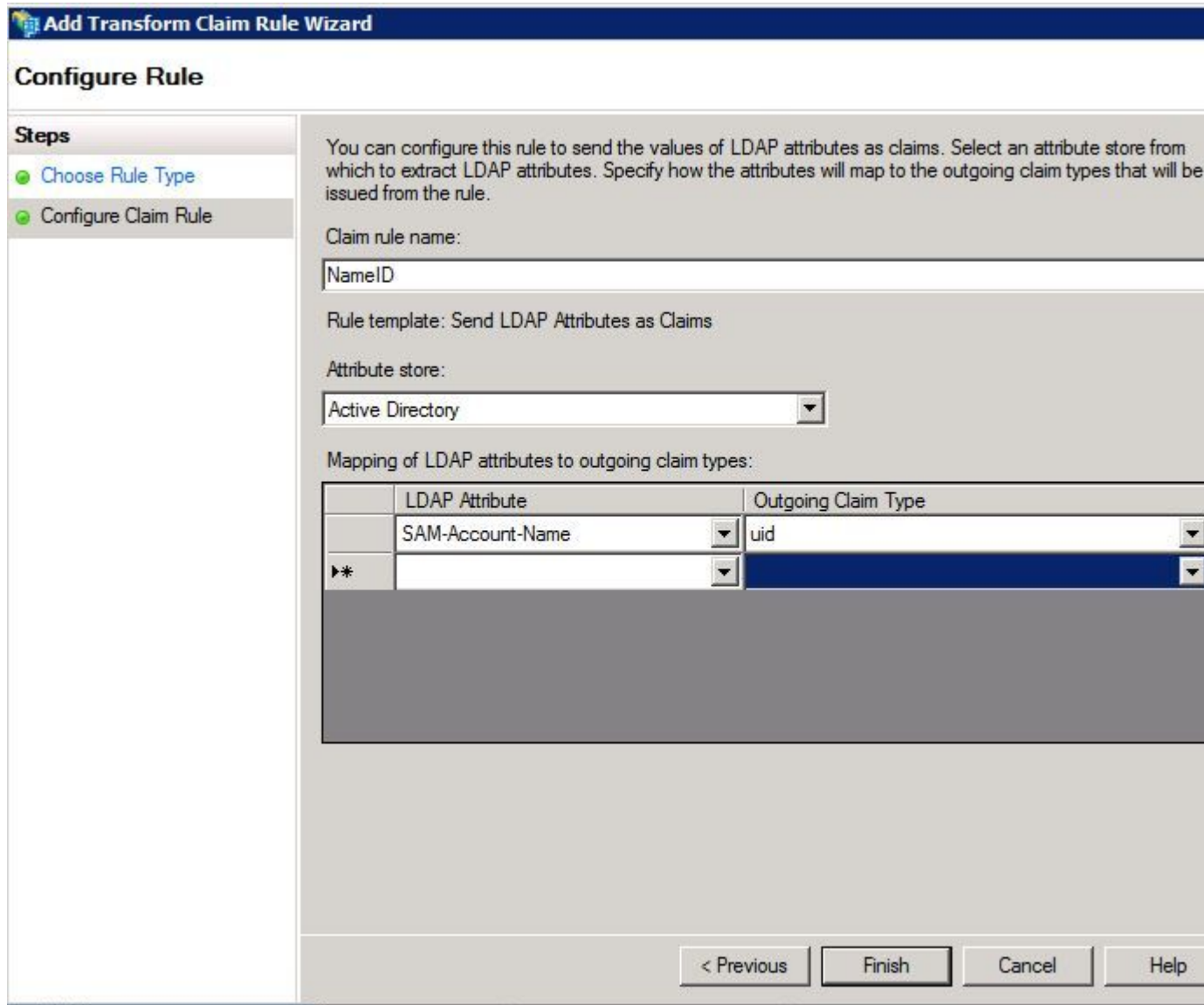
Passaggio 13. Nella pagina successiva immettere **NameID** per il **nome della regola di attestazione**.

Passaggio 14. Scegliere **Active Directory** per l'**archivio attributi**.

Passaggio 15. Scegliere **SAM-Account-Name** per l'**attributo LDAP**.

Passaggio 16. Immettere **uid** per il **tipo di attestazione in uscita**.

Nota: l'UID non è un'opzione dell'elenco a discesa, ma deve essere immesso manualmente.



Passaggio 17. Fare clic su Finish (Fine).

Passaggio 18. La prima regola è stata completata. Fare nuovamente clic su **Aggiungi regola**.

Passaggio 19. Scegliere **Invia attestazioni utilizzando una regola personalizzata**.

Passaggio 20. Immettere il **nome** di una **regola di attestazione**.

Passaggio 21. Nel campo **Regola personalizzata** incollare il testo seguente:

```
c:[Tipo == "http://schemas.microsoft.com/ws/2008/06/identity/claim/nomecontabile"]
=> problema(Tipo = "http://schemas.xmlsoap.org/ws/2005/05/identity/claim/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",Proprietà["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/namequalifier"] =
"http://ADFS\_FEDERATION\_SERVICE\_NAME/com/adfs/service/trust",
Proprietà["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier"] =
"CUCM_ENTITY_ID");
```

Passaggio 22. Assicurarsi di modificare AD_FS_SERVICE_NAME e CUCM_ENTITY_ID in base ai valori appropriati.

Nota: se non si è certi del nome del servizio ADFS, è possibile eseguire la procedura per individuarlo. È possibile estrarre l'ID entità CUCM dalla prima riga del file di metadati CUCM. Nella prima riga del file è presente un elemento entityID simile al seguente, entityID=1cucm1052.sckiewer.lab,. È necessario immettere il valore sottolineato nella sezione appropriata della regola attestazione.

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/namequalifier"] = "http://win2k8.sckiewer.lab/adfs/com/adfs/service/trust", Properties ["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier"] = "1cucm1052.sckiewer.lab");
```

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

< Previous Finish Cancel Help

Passaggio 23. Fare clic su Finish (Fine).

Passaggio 24. Fare clic su OK.


Nota: le regole di attestazione sono necessarie per qualsiasi server Unified Collaboration su cui si intende utilizzare SSO.

Completare l'abilitazione di SSO su CUCM ed eseguire il test SSO


Passaggio 1. Una volta completata la configurazione del server AD FS, è possibile tornare a CUCM.

Passaggio 2. Nella pagina di configurazione finale è stato visualizzato il messaggio:

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

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 administrative access.

Valid administrator Usernames

sckiewer

2) Launch SSO test page

Passaggio 3. Selezionare l'utente finale con il ruolo **Utenti privilegiati CCM standard** selezionato e fare clic su **Esegui test SSO...**

Passaggio 4. Verificare che il browser consenta i popup e immettere le credenziali nella richiesta.

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

Passaggio 5. Fare clic su **Close** (Chiudi) nella finestra popup, quindi su **Finish** (Fine).

Passaggio 6. Dopo un breve riavvio delle applicazioni Web, l'SSO viene attivato.

Risoluzione dei problemi

Imposta log SSO su debug

Per impostare i log SSO su debug, eseguire questo comando nella CLI di CUCM: **set samltrace level debug**

I log SSO possono essere scaricati da RTMT. Il nome del set di registri è **Cisco SSO**.

Trova Nome Servizio Federativo

Per trovare il nome del servizio federativo, fare clic su **Start** e cercare **Gestione AD FS 2.0**.

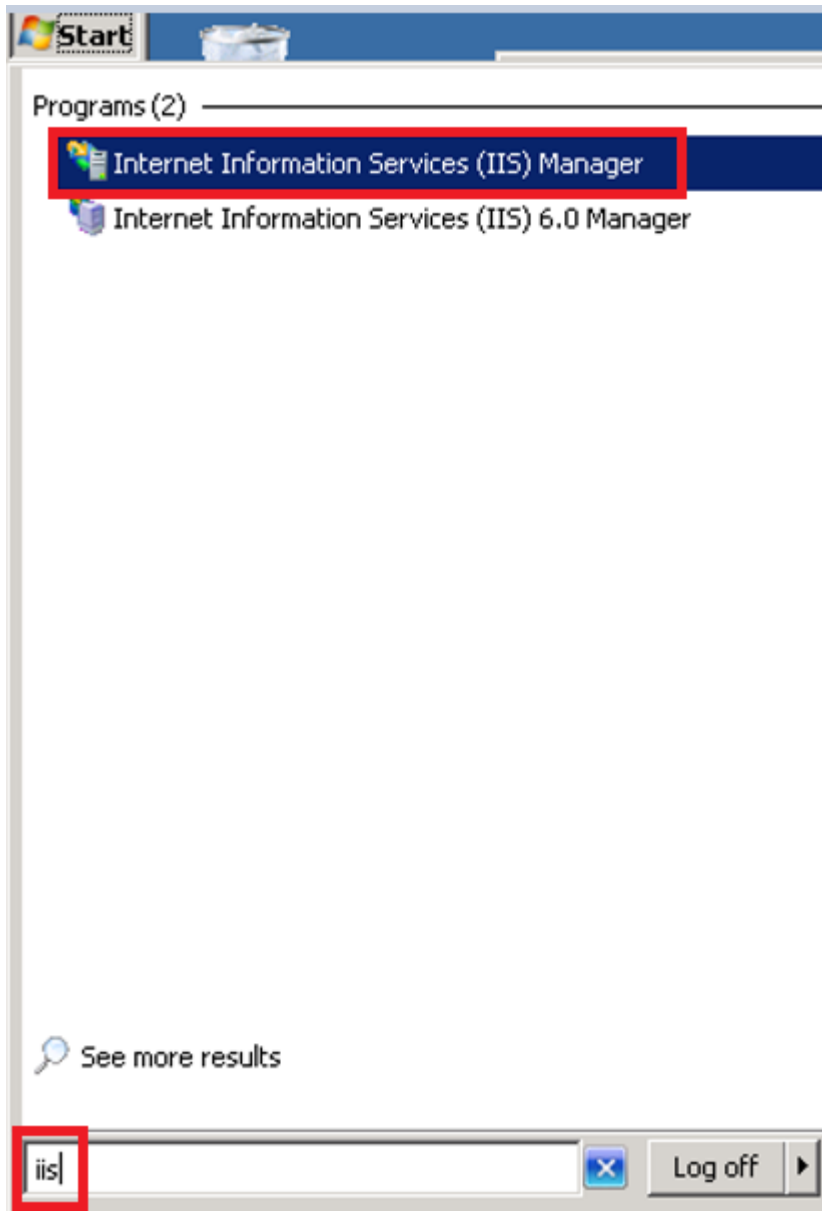
- Fare clic su Modifica **proprietà servizio federativo...**
- Nella scheda Generale cercare **nome servizio federativo**

Nome Servizio Federativo E Certificato Senza Punto

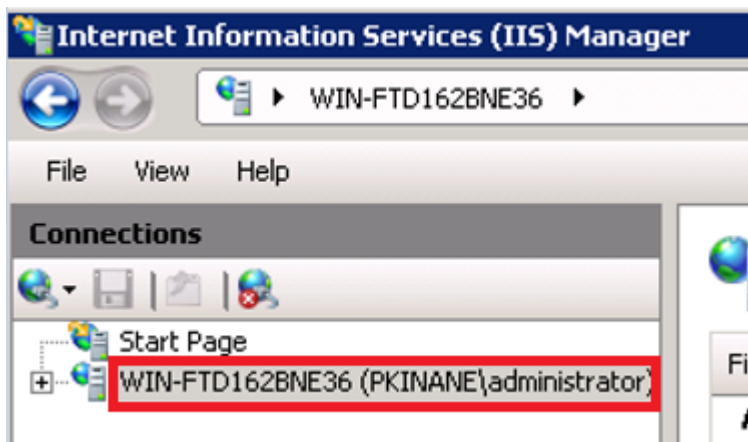
Se viene visualizzato questo messaggio di errore nella configurazione guidata di AD FS, è necessario creare un nuovo certificato.

Impossibile utilizzare il certificato selezionato per determinare il nome del servizio federativo. Il nome del soggetto del certificato selezionato è senza punti (nome breve). Selezionare un altro certificato senza un nome soggetto (nome breve) senza punti, quindi riprovare.

Passaggio 1. Fare clic sul pulsante Start e cercare iis, quindi aprire Gestione Internet Information Services (IIS)

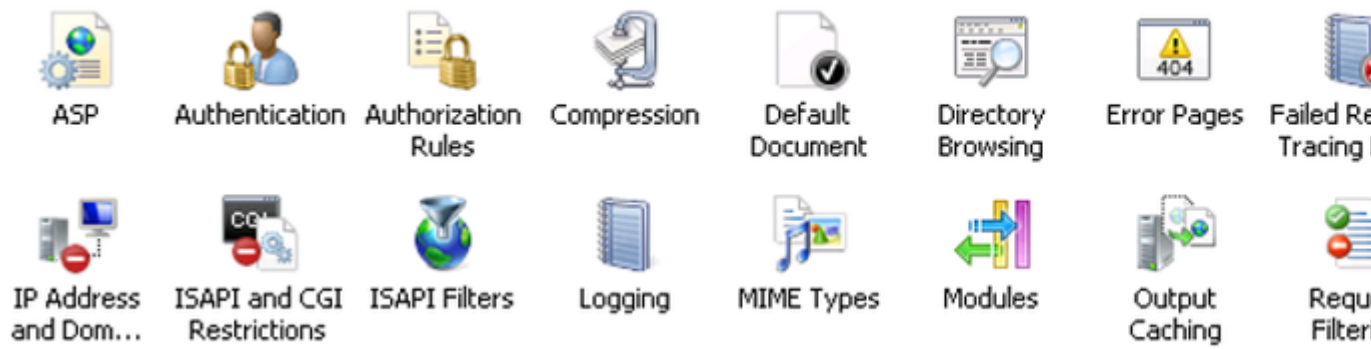


Passaggio 2. Fare clic sul nome del server.

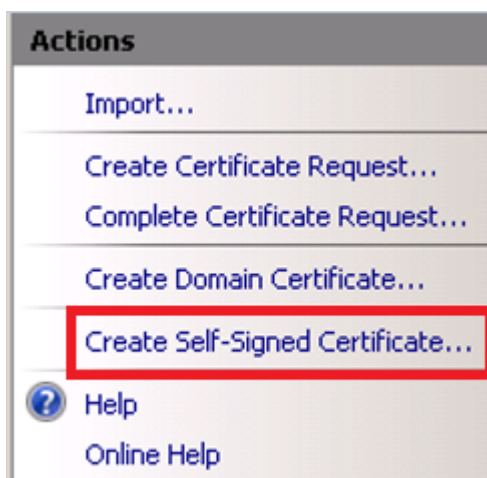


Passaggio 3. Fare clic su Certificati server.

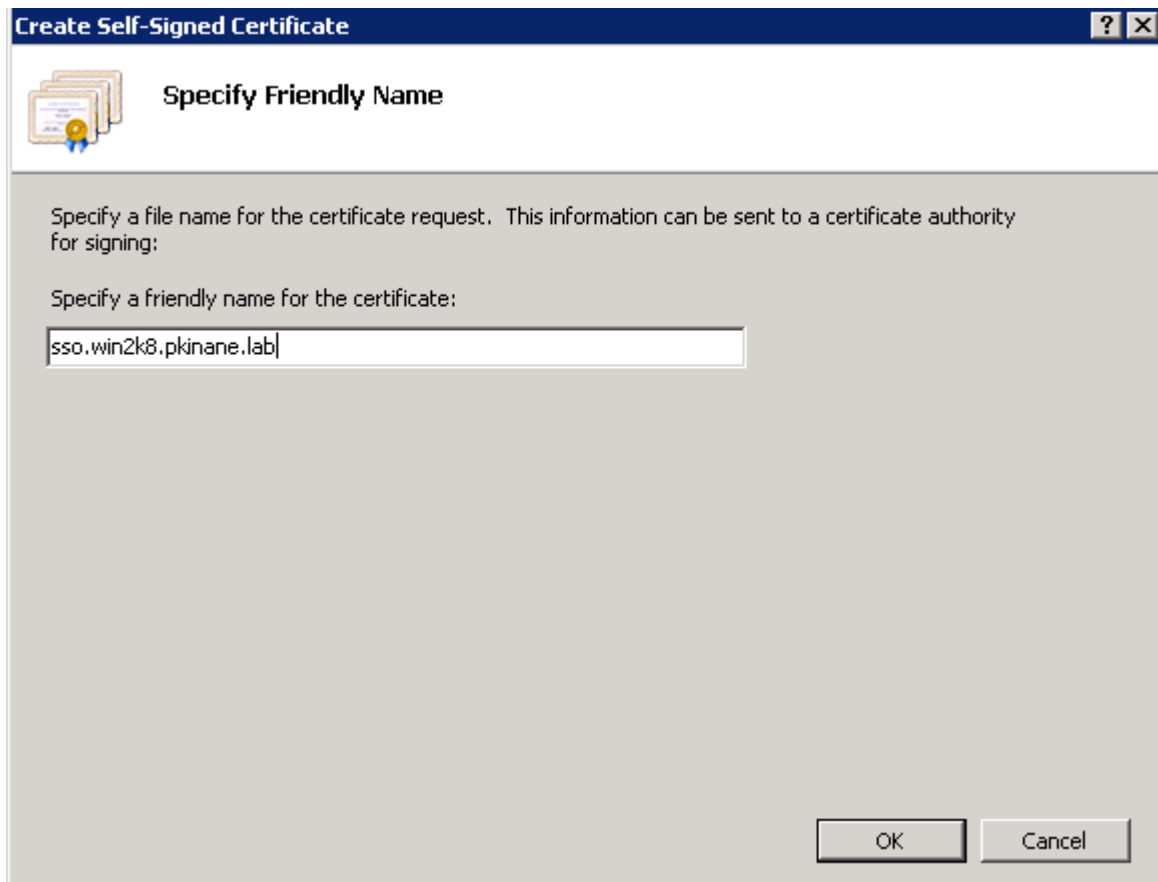
IIS



Passaggio 4. Scegliere Crea certificato autofirmato.



Passaggio 5. Immettere il nome desiderato per l'alias del certificato.



Tempo non sincronizzato tra i server CUCM e IDP

Se questo errore si verifica quando si esegue il test SSO da CUCM, è necessario configurare Windows Server in modo che utilizzi gli stessi server NTP di CUCM.

Risposta SAML non valida. Questa situazione può verificarsi quando il tempo non è sincronizzato tra Cisco Unified Communications Manager e i server IDP. Verificare la configurazione NTP su entrambi i server. Eseguire "utils ntp status" dalla CLI per verificare questo stato su Cisco Unified Communications Manager.

Dopo aver specificato i server NTP corretti per Windows Server, è necessario eseguire un altro test SSO e verificare se il problema persiste. In alcuni casi, è necessario distorcere il periodo di validità dell'asserzione. [Qui](#) maggiori dettagli su questo processo.

Informazioni correlate

- [Documentazione e supporto tecnico â€“ Cisco Systems](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).