

Configuratievoorbeeld van Unified Communications Manager, versie 10.5 SAML

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Network Time Protocol \(NTP\) instellen](#)

[Domain Name Server \(DNS\)-instelling](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Configureren](#)

[Netwerkdigram](#)

[Instellen map](#)

[SAML SSO inschakelen](#)

[Verifiëren](#)

[Problemen oplossen](#)

Inleiding

Dit document beschrijft hoe u de Security Association Markup Language (SAML) single aanmelding (SSO) kunt configureren en controleren voor Cisco Unified Communications Manager (CUCM).

Voorwaarden

Vereisten

Network Time Protocol (NTP) instellen

Om te kunnen SAML SSO's kunnen werken, moet u de juiste NTP-instellingen installeren en ervoor zorgen dat het tijdsverschil tussen de Identity Provider (IDP) en de Unified Communications-toepassingen niet meer dan drie seconden bedraagt.

Als er een time-mismatch is tussen CUCM en IDP, ontvangt u deze fout: "Ongeldige SAML respons." Deze fout kan worden veroorzaakt wanneer de tijd niet is afgestemd op de CUCM- en IDP-servers. Om te kunnen SAML SSO's werken, moet u de juiste NTP-instellingen installeren en ervoor zorgen dat het tijdsverschil tussen de IDP en de Unified Communications-toepassingen niet meer dan drie seconden bedraagt.

Raadpleeg het gedeelte NTP-instellingen in de [Cisco Unified Communications Operating System Management Guide](#) voor informatie over het [synchroniseren van](#) klokken.

Domain Name Server (DNS)-instelling

Unified Communications-toepassingen kunnen DNS gebruiken om FQDN-namen (Full Qualified Domain Names) (FQDN's) op IP-adressen op te lossen. De serviceproviders en de IDP kunnen door de browser worden opgelost.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Active Directory Federation Service (AD FS) versie 2.0 als IDP
- CUCM versie 10.5 als serviceproviders
- Microsoft Internet Explorer 1.0

Voorzichtig: Dit document is gebaseerd op een nieuw geïnstalleerd CUCM. Als u SAML SSO op een reeds in productie server vormt, kunt u een aantal stappen dienovereenkomstig moeten overslaan. U moet ook de impact van de service begrijpen als u de stappen op de productieserver uitvoert. Aanbevolen wordt deze procedure tijdens niet-openingstijden uit te voeren.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Achtergrondinformatie

SAML is een op XML gebaseerd, open-standaard gegevensformaat dat beheerders in staat stelt om tot een bepaalde reeks Cisco samenwerkingstoepassingen naadloos toegang te hebben nadat zij in één van die toepassingen tekenen. SAML SSO stelt een Cirkel van het Vertrouwen (CoT) in wanneer het metagegevens uitwisselt als onderdeel van het leveringsproces tussen de IDP en de serviceprovider. De serviceprovider vertrouwt op de gebruikersinformatie van de ID om toegang tot de verschillende services of toepassingen te bieden.

Opmerking: Serviceprovider is niet langer betrokken bij authenticatie. SAML versie 2.0 delegeert verificatie niet aan de serviceproviders en de IDs. De client authenticceert de IDP en de IDP verleent een waarschuwing aan de klant. De client presenteert de verklaring aan de serviceprovider. Aangezien er een CoT is opgericht, vertrouwt de dienstverlener de Assertion en verleent hij toegang tot de cliënt.

Configureren

Netwerkdigram

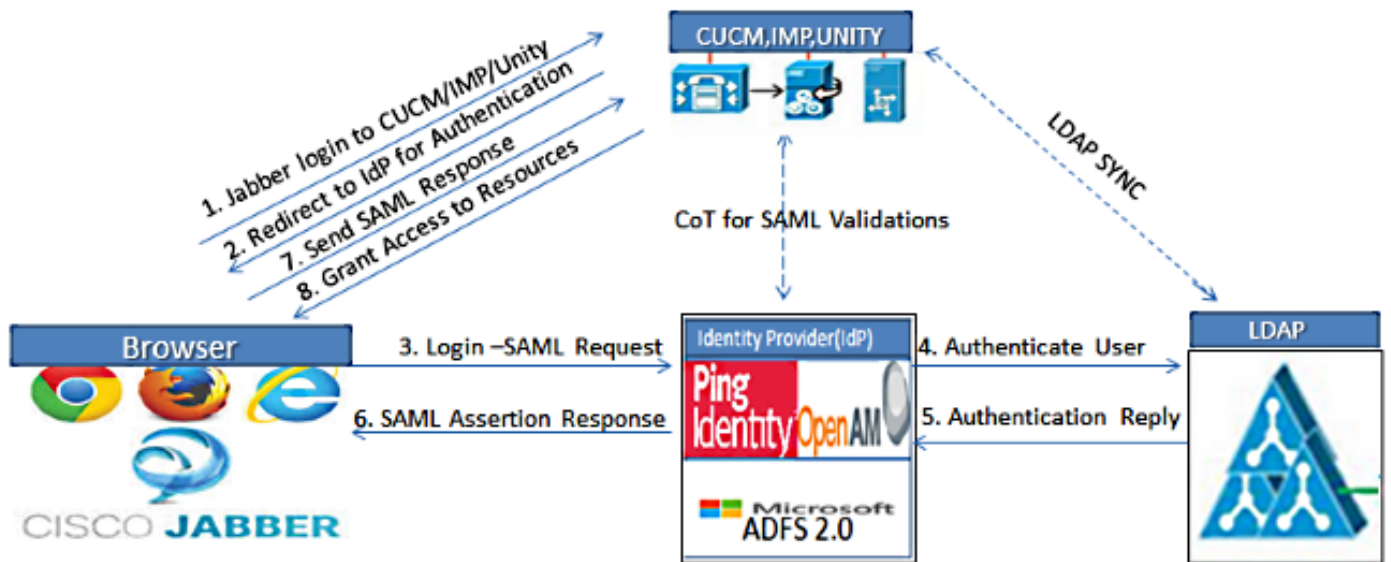
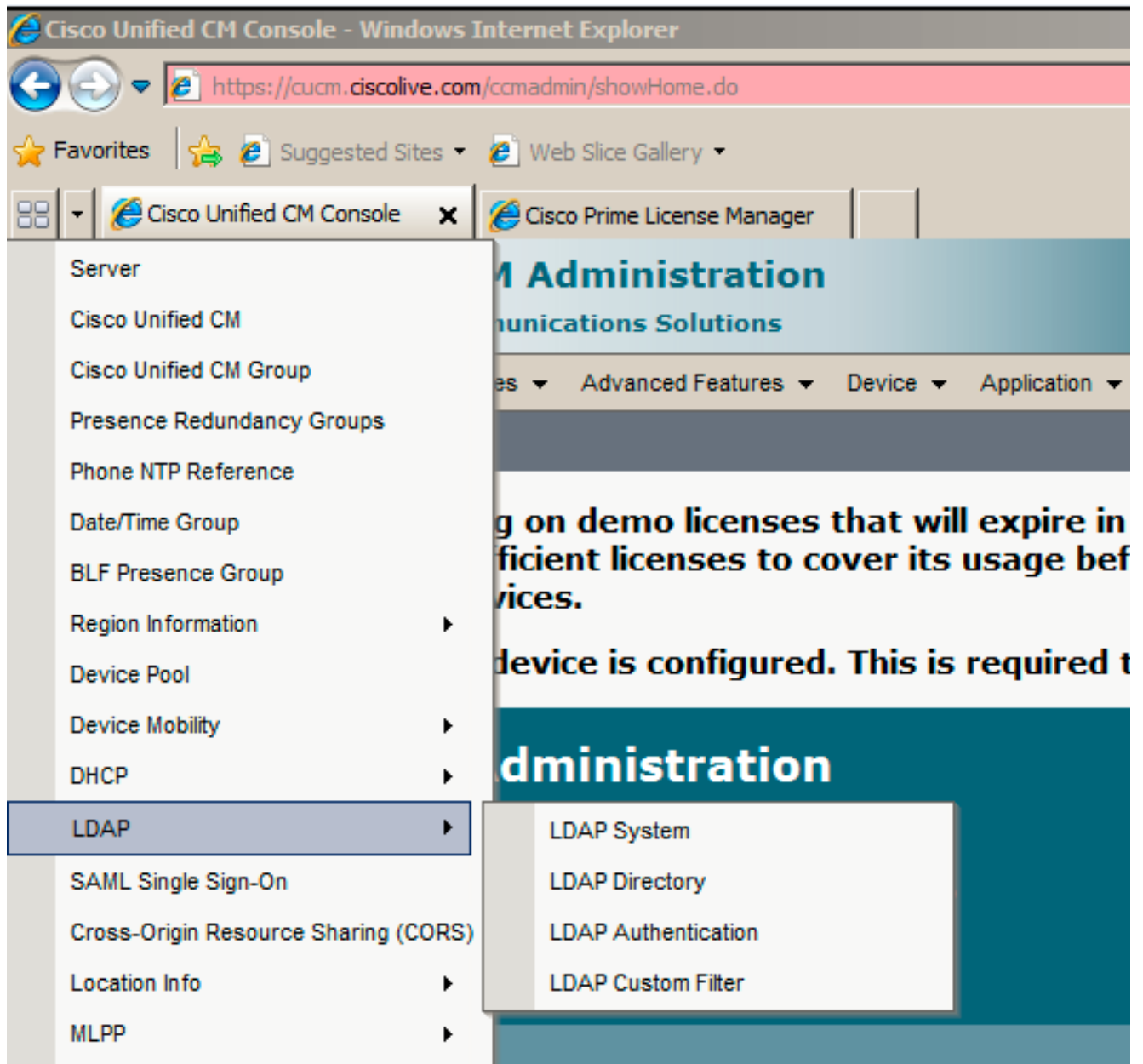


Figure :SAML Single sign SSO Call Flow for Collaboration Servers


Instellen map

1. Kies Cisco Unified CM Management > System > LDAP > LDAP-systemem.




2. Klik op **Nieuw toevoegen**.
3. Configureer het type en de eigenschap van de lichtgewicht Directory Access Protocol (LDAP).
4. Kies **synchroniseren vanaf LDAP Server inschakelen**.

LDAP System Configuration

 Save

Status

 Status: Ready

LDAP System Information

Enable Synchronizing from LDAP Server

LDAP Server Type






LDAP Attribute for User ID

5. Kies Cisco Unified CM-beheer > Systeem > LDAP > LDAP-map.


6. Deze items configureren:

Instellingen voor lire-directoryTe synchroniseren
gebruikerseigenschappenynchronisatieschemaLDAP server hostname of IP-adres en poortnummer

LDAP Directory

 Save  Delete  Copy  Perform Full Sync Now  Add New

Status

 Status: Ready

LDAP Directory Information

LDAP Configuration Name*

LDAP Manager Distinguished Name*

LDAP Password*

Confirm Password*

LDAP User Search Base*

LDAP Custom Filter

7. Schakel **gebruik SSL uit** als u geen Secure Socket Layer (SSL) wilt gebruiken om met de LDAP-map te communiceren.

Tip: Als u LDAP via SSL wilt configureren, uploadt u het LDAP folder certificaat naar CUCM. Zie de LDAP-directory inhoud in [Cisco Unified Communications Manager SRND](#) voor

informatie over het accountsynchronisatiemechanisme voor specifieke LDAP-producten en algemene beste praktijken voor de synchronisatie van LDAP.

8. Klik op **Opslaan** en voer vervolgens **de volledige sync nu uit**.

Opmerking: Zorg ervoor dat **Cisco DirSync** service is ingeschakeld in de webpagina voor serviceproviders voordat u op Opslaan klikt.

The screenshot shows the 'LDAP Server Information' configuration page. It includes a form with the following fields and controls:

- Host Name or IP Address for Server ***: Text input containing 'adfs1.ciscolive.com'.
- LDAP Port ***: Text input containing '3268'.
- Use SSL**: A checkbox that is currently unchecked.
- Add Another Redundant LDAP Server**: A button below the form.
- Save**, **Delete**, **Copy**, **Perform Full Sync Now**, and **Add New**: A row of buttons at the bottom of the configuration area.

9. Navigeer naar **gebruikersbeheer > Eindgebruiker** en selecteer een gebruiker aan wie u de administratieve rol van CUCM wilt geven (dit voorbeeld selecteert gebruiker **SSO**).

The screenshot shows the 'Find and List Users' interface. It includes the following elements:

- System** navigation menu: Call Routing, Media Resources, Advanced Features, Device, Application, User Management, Bulk Administration, Help.
- Find and List Users** header.
- Buttons: **Add New**, **Select All**, **Clear All**, **Delete Selected**.
- Status** section: **3 records found**.
- User (1 - 3 of 3)** section with a search bar and filters.
- Table of users:**

<input type="checkbox"/>	User ID ^	First Name	Last Name	Department	Directory URI	User Status
<input type="checkbox"/>	880	Saml	SSO			Active LDAP Synchronized User
<input type="checkbox"/>	user2	User	2			Active LDAP Synchronized User

10. Blader naar de informatie over toegangsrechten en klik op **Toevoegen aan de groep toegangscontrole**. Selecteer **Standaard CCM-gebruikers**, klik op **Geselecteerd toevoegen** en klik op **Opslaan**.

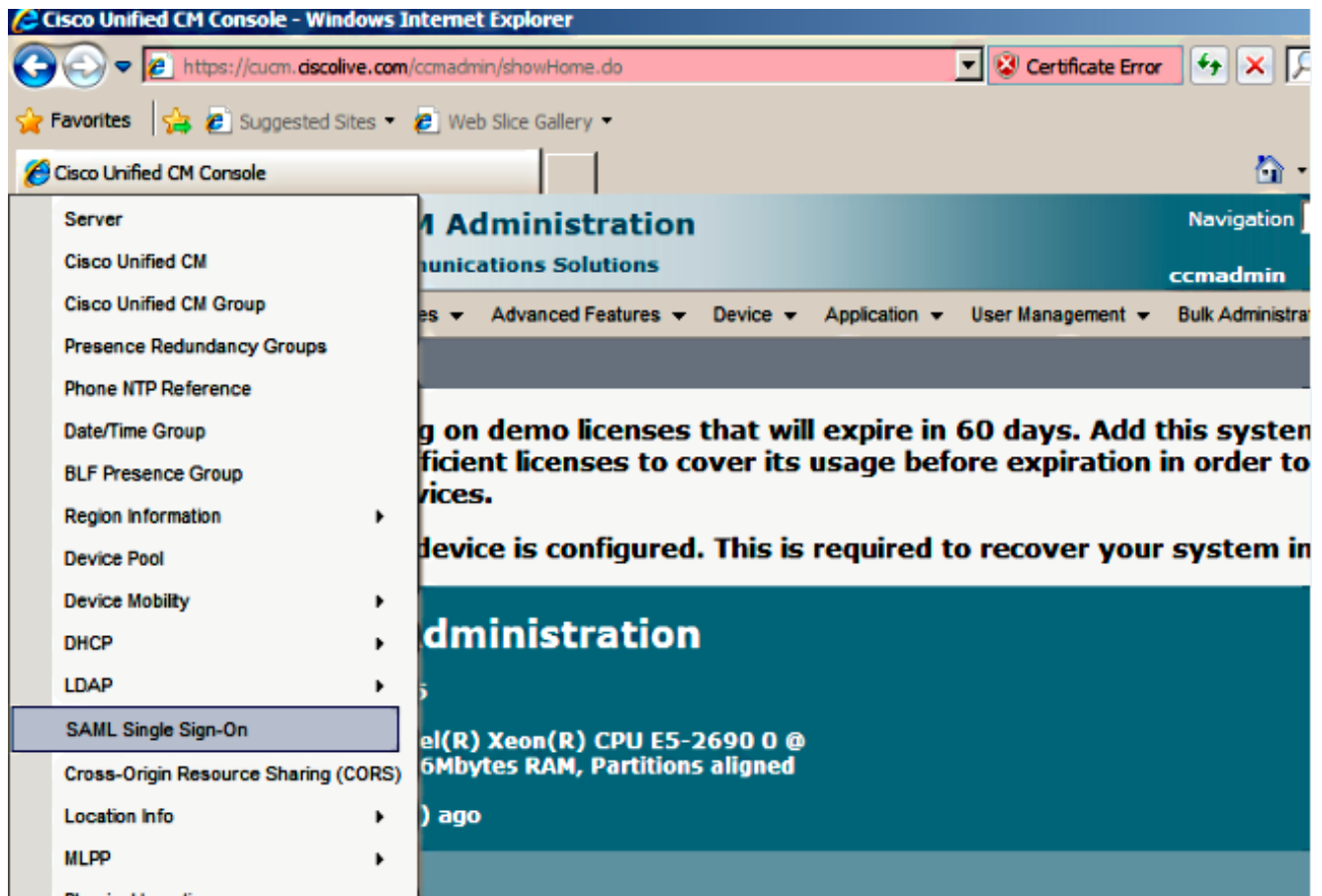
The screenshot shows the 'Permissions Information' configuration page. It includes the following elements:

- Groups** list: Standard CCM Super Users.
- Roles** list: Standard AXL API Access, Standard Admin Rep Tool Admin, Standard CCM Admin Users, Standard CCMADMIN Administration, Standard CUREporting.
- Add to Access Control Group** and **Remove from Access Control Group** buttons.
- View Details** links for both Groups and Roles.
- Save**, **Delete**, and **Add New** buttons at the bottom.

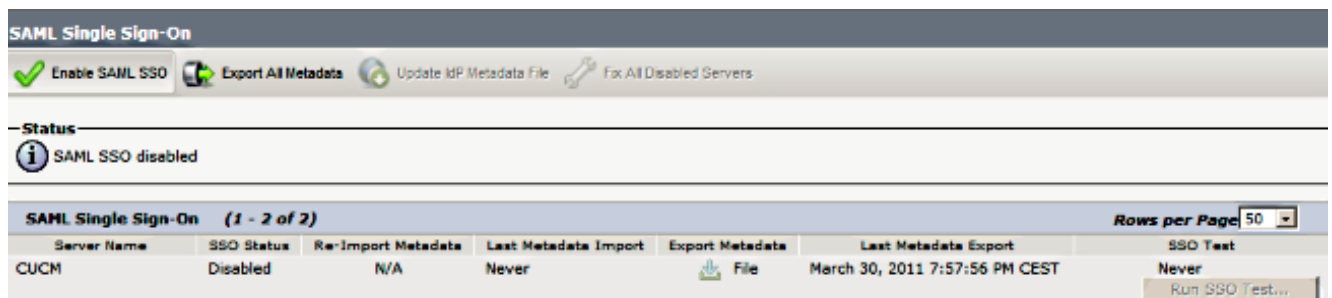
SAML SSO inschakelen

1. Log in op de CUCM-gebruikersinterface.

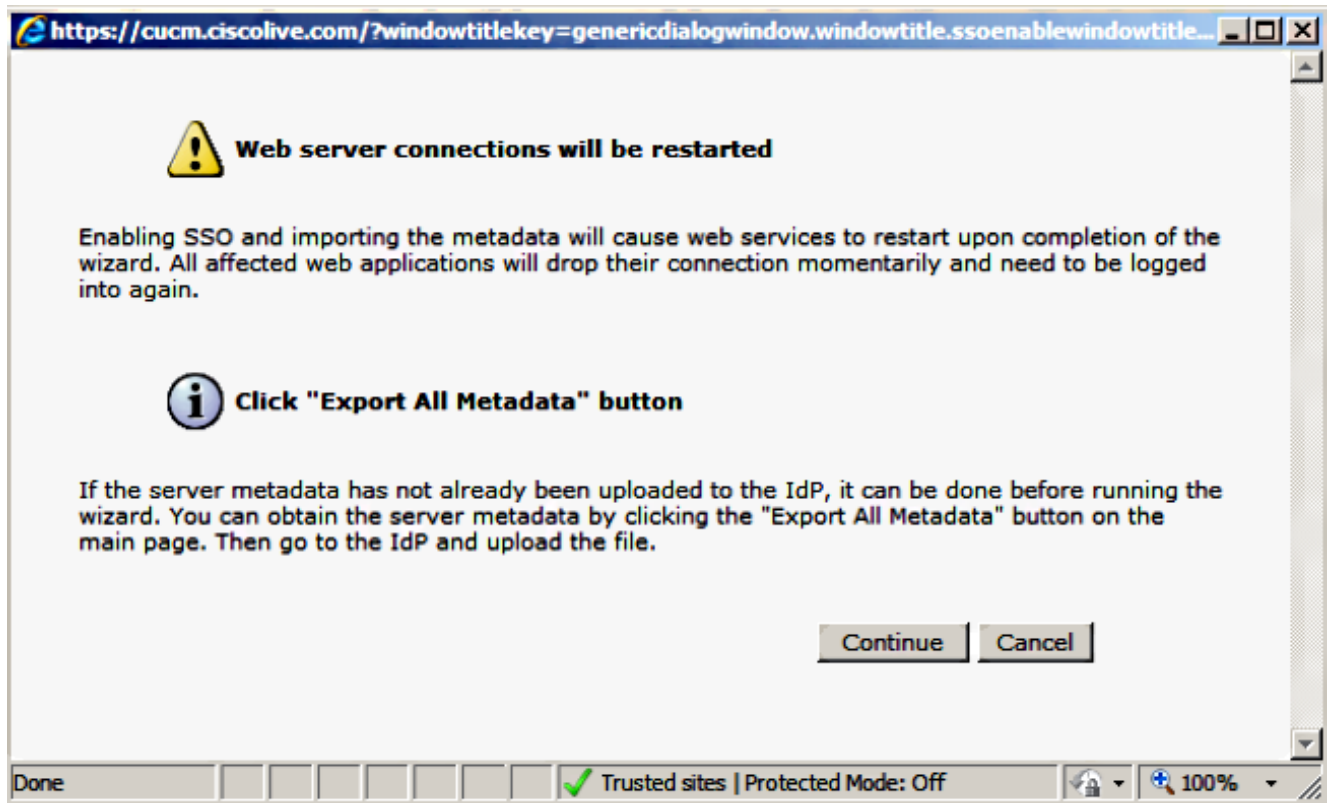
2. Kies **Systeem > SAML single-aanmelding** en het venster SAML Single aanmelding/configuratie wordt geopend.



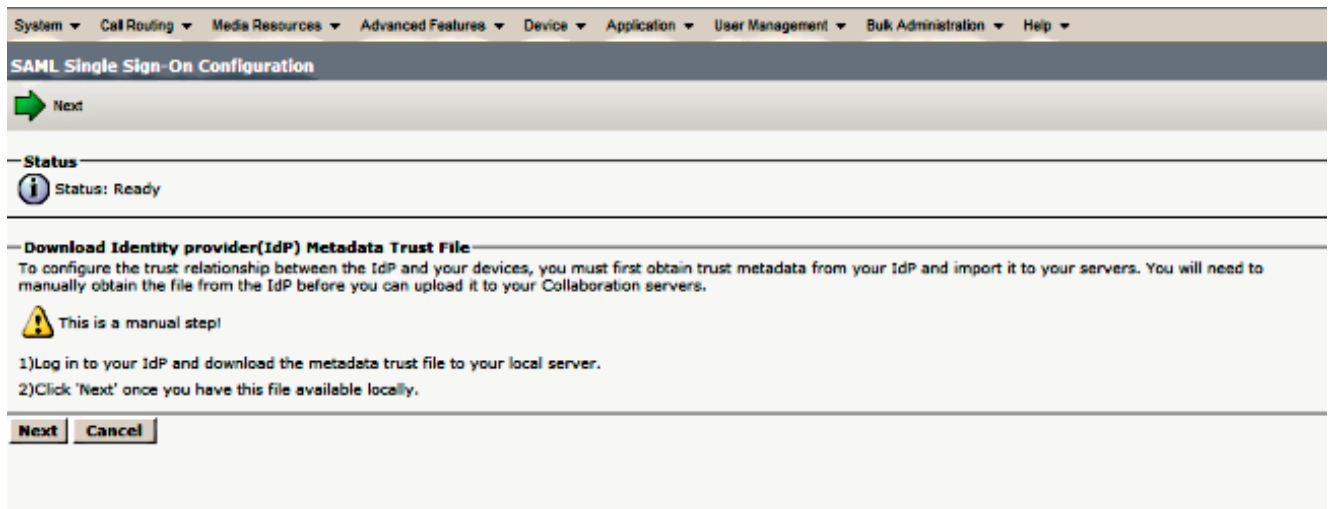
3. Klik om SAML SSO op het cluster in te schakelen op **SAML SSO**.



4. Klik in het venster Waarschuwing opnieuw instellen op **Doorgaan**.



5. Klik op het SSO-scherm op **Bladeren** om het XML-bestand met de stap **IDP-metagegevens** te importeren van de IDP-metagegevens (**FederationMetagegevens.xml**).




6. Klik na het uploaden van het metagegevensbestand op **Importeren van IDP-metagegevens** om de IDP-informatie naar CUCM te importeren. Bevestig dat de invoer succesvol was en klik op **Volgende** om verder te gaan.

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

SAML Single Sign-On Configuration

Next

Status
 Ready to import Identity Provider metadata trust file to cluster 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

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.

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



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

7. Klik op **Download Trust Metadata File** (optioneel) om de CUCM en de CUCM IM and Presence metadata in een lokale map op te slaan en [CUCM toe te voegen als vertrouwen van de vertrouwende partij](#). Ga verder naar stap 8 zodra de configuratie van de AD FS is voltooid.


SAML Single Sign-On Configuration

Back Next

Status
 If Admin has already uploaded the server metadata to IdP then skip the steps below and click Next. Otherwise follow the steps below to upload the server metadata to IdP
 IdP Metadata has been imported to servers in this cluster

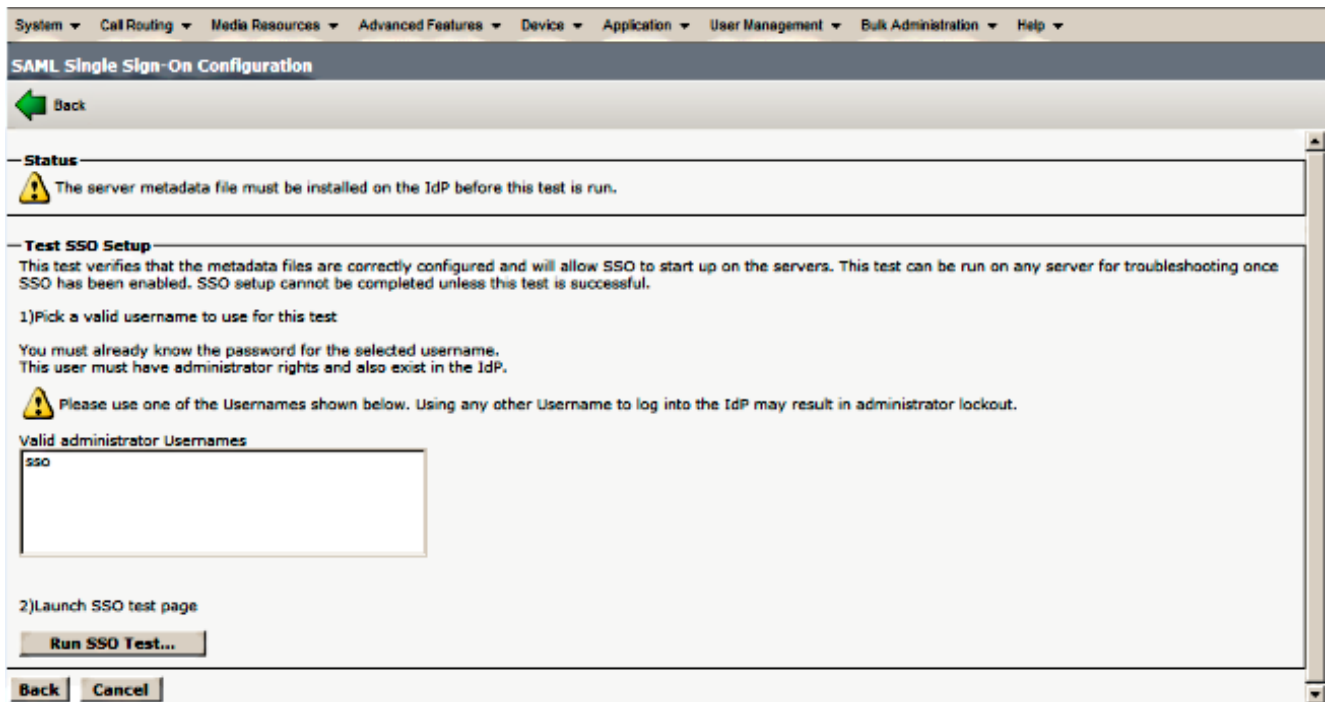
Download Server Metadata and install on the IdP
 Download the metadata trust file from Collaboration servers and manually install it on the IdP server to complete SSO setup.

1) Download the server metadata trust files to local storage

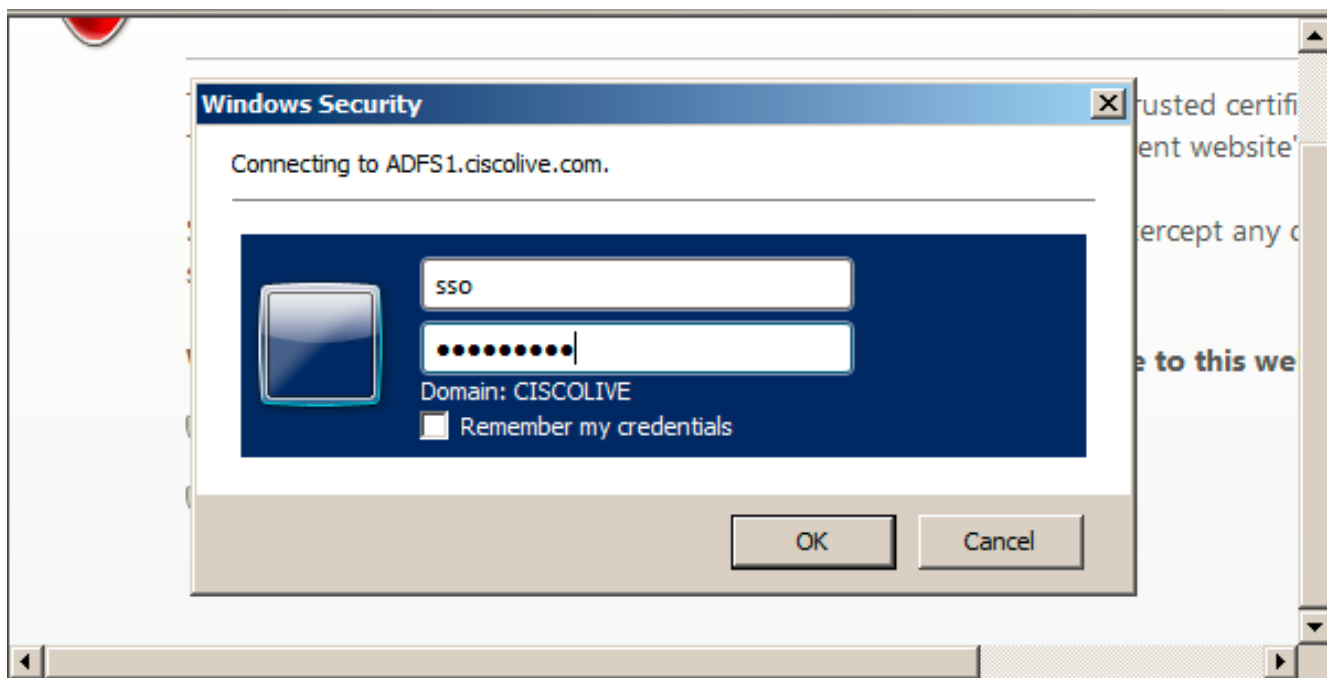
 This is a manual step!

2) Log in to your IdP and upload the server metadata trust file.
 3) Click 'Next' once you have installed the server metadata on the IdP.

8. Selecteer **SSO** als de beheergebruiker en klik op **Test uitvoeren**.

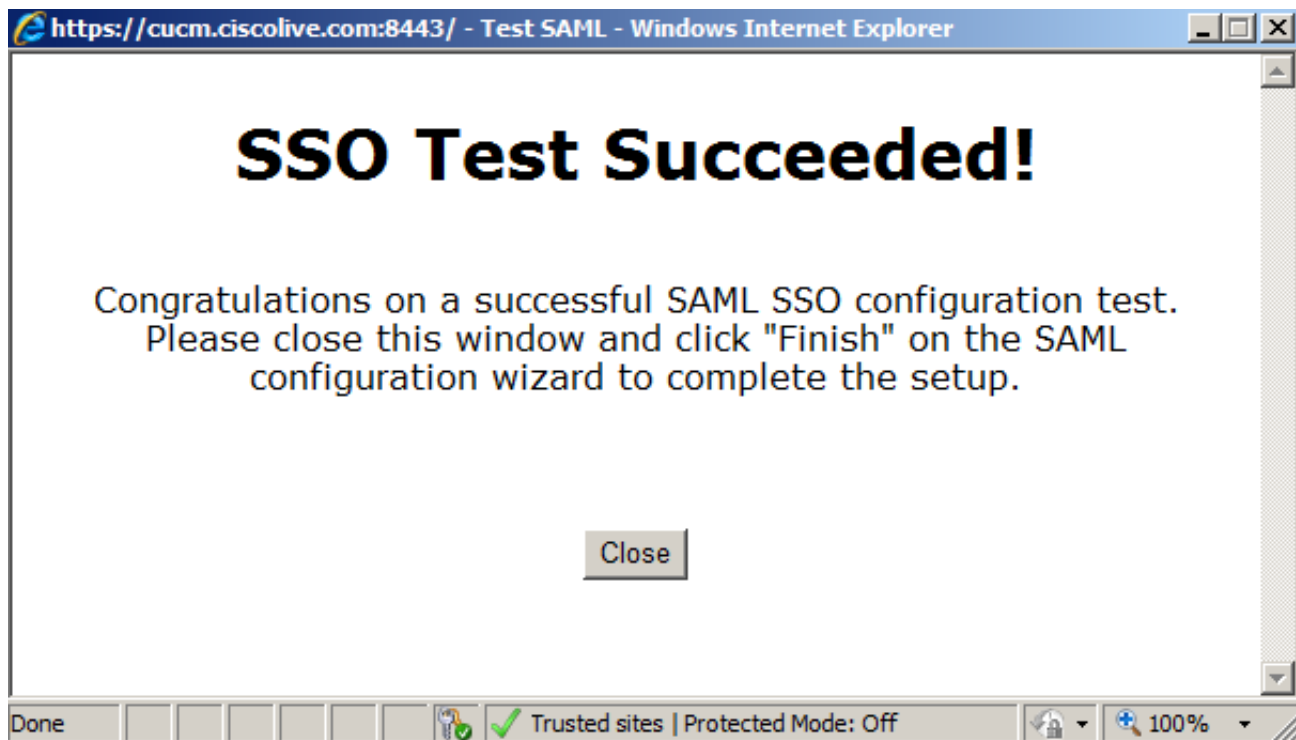


9. Herhaal de waarschuwing van het certificaat en ga verder. Wanneer u om geloofsbrieven wordt gevraagd, voer de gebruikersnaam en het wachtwoord voor gebruiker **SSO** in en klik op **OK**.



Opmerking: Dit configuratievoorbeeld is gebaseerd op zelfondertekende CUCM- en AD FS-certificaten. Indien u certificaten van de certificaatautoriteit (CA) gebruikt, moeten de juiste certificaten op zowel AD FS als CUCM worden geïnstalleerd. Raadpleeg [certificaatbeheer en -validatie](#) voor meer informatie.

10. Nadat alle stappen zijn voltooid, is de "SSO-test voltooid!" bericht wordt weergegeven. Klik op **Sluiten** en **Voltooien** om verder te gaan. U hebt nu de configuratietaken voltooid om de SSO op CUCM met AD FS in te schakelen.



11. Aangezien CUCM IM and Presence net als CUCM Subscriber werkt, moet u [Add CUCM IM and Presence](#) configureren [als Relying Party Trust](#) en **SSO Test uitvoeren** om SAML SSO vanuit de CUCM SAML SSO-pagina zelf in te schakelen.

Opmerking: Als u de XML-bestanden van alle knooppunten op IDP configureren en u SSO-handeling op één knooppunt activeert, dan is SAML SSO ingeschakeld op alle knooppunten in de cluster.

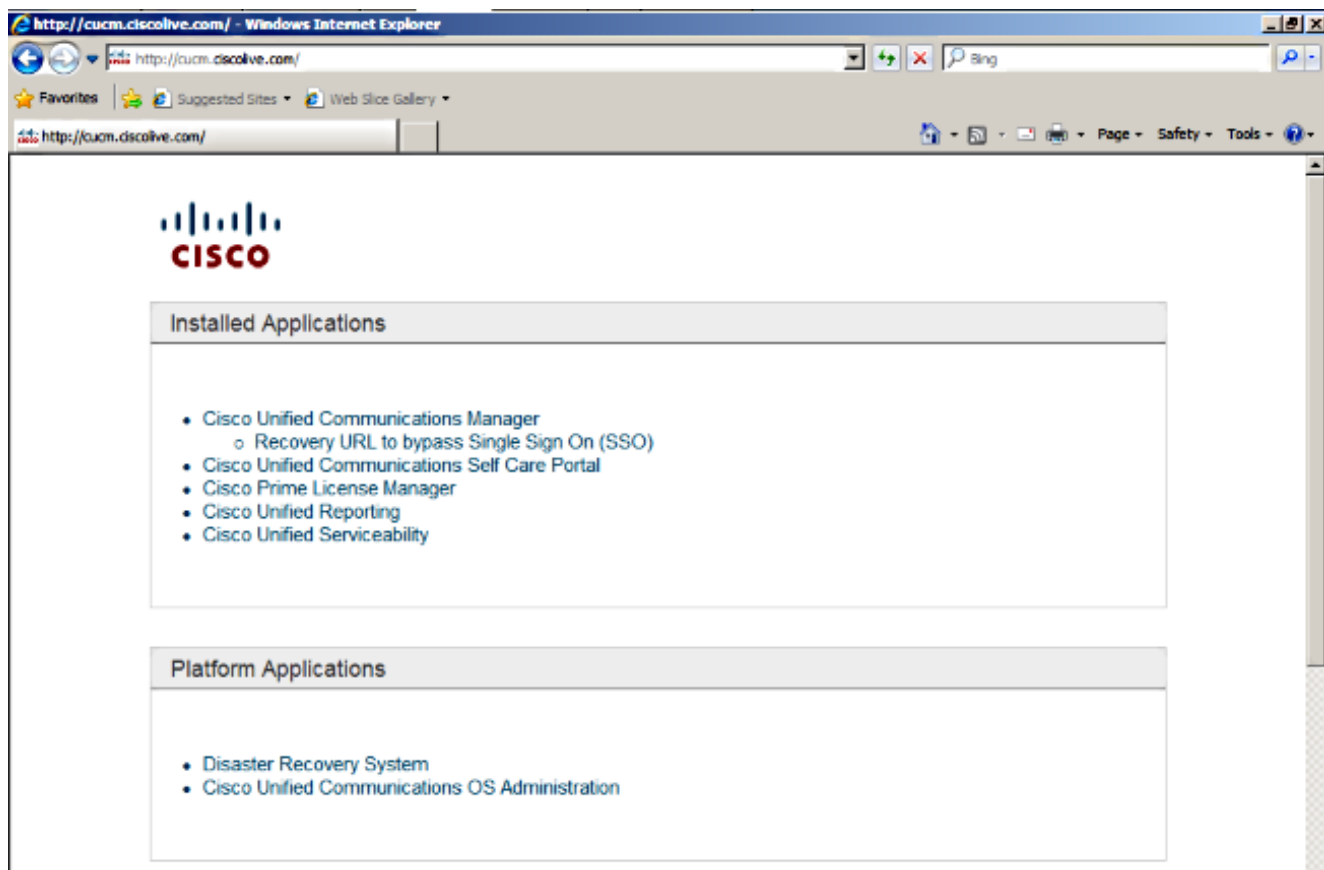
AD FS moet worden geconfigureerd voor alle knooppunten van CUCM en CUCM IM and Presence in een cluster als Relay Party.

Tip: U dient Cisco Unity Connection en CUCM IM and Presence voor SAML SBBM ook te configureren als u de SAML SLIM-ervaring wilt gebruiken voor Cisco Jabber Clients.

Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

1. Open een webbrowser en voer de FQDN voor CUCM in.
2. Klik op **Cisco Unified Communications Manager**.
3. Selecteer de webapp (**CM-beheer/Unified Services/Cisco Unified Reporting**) en druk op **Go**, dan dient u te worden gevraagd naar aanmeldingsgegevens door de AD-FS. Nadat u de aanmeldingsgegevens van **de** gebruiker **SSO** hebt ingevoerd, bent u met succes aangemeld op de geselecteerde webapp (**CM-beheerpagina, Unified Service-pagina, Cisco Unified Reporting**).



Opmerking: SAML SSO biedt geen toegang tot deze pagina's:

- Licentiebeheer voor Prime
- OS-beheer
- Noodherstelsysteem

Problemen oplossen

Als u geen SAML kunt inschakelen en u niet kunt inloggen, gebruikt u de nieuwe optie onder Geïnstalleerde toepassingen met de naam **Terugwinning URL** om de **Single aanmelding (SSO)** te omzeilen. Deze optie kan worden gebruikt om in te loggen met de aanmeldingsgegevens die tijdens de installatie of door lokaal gemaakte CUCM-gebruikers zijn gemaakt.

Cisco Unified CM Console - Windows Internet Explorer

https://cuom.dscoolve.com/ccadmin/showRecovery.do Certificate Error Bing

Cisco Unified CM Console

Cisco Single Sign On Recovery Administration

For Cisco Unified Communications Solutions

Cisco Single Sign On Recovery Administration

This page will validate credentials locally, allowing access only to applications that are running on this server, and will not leverage SAML SSO authentication.

This page can be disabled through the CLI.

Username: ccadmin
Password: [REDACTED]
Login Reset

Copyright © 1999 - 2015 Cisco Systems, Inc.
All rights reserved.

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at our [Export Compliance Product Report](#) web site.

For information about Cisco Unified Communications Manager please visit our [Unified Communications System Documentation](#) web site.

For Cisco Technical Support please visit our [Technical Support](#) web site.

Raadpleeg voor meer informatie over probleemoplossing [SAML SSP voor Collaboration Products 10.x](#).