

Unity Connection versie 10.5 SAML SPA-configuratievoorbeeld

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 Unity Connection (UCXN).

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. Zie 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.

Active Directory Federation Service (AD FS) versie 2.0 moet worden geïnstalleerd en geconfigureerd om SAML-verzoeken te kunnen behandelen.

Gebruikte componenten

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

- AD FS versie 2.0 als IDP
- UCXN als serviceproviders
- Microsoft Internet Explorer versie 1.0

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 XML-gebaseerd, open-standaard gegevensformaat voor gegevensuitwisseling. Het is een authenticatieprotocol dat door serviceproviders wordt gebruikt om een gebruiker te authenticeren. De informatie over de veiligheidscontrole wordt tussen een IDP en de serviceprovider doorgegeven.

SAML is een open standaard die klanten in staat stelt om tegen elke SAML-enabled samenwerking (of Unified Communications)-service ongeacht het clientplatform te authenticeren.

Alle Cisco Unified Communications web interfaces, zoals Cisco Unified Communications Manager (CUCM) of UCXN, gebruiken het protocol van SAML versie 2.0 in de SAML SSO-functie. Om de Lichtgewicht Directory Access Protocol (LDAP) gebruiker echt te maken, delegeert UCXN een verificatieaanvraag aan de IDP. Dit door de UCXN gegenereerde verificatieverzoek is een SAML-aanvraag. De IDP authentiek en keert een SAML aanname terug. De SAML-test toont ja (geauthentiseerd) of nee (authenticatie mislukt).

Met SAML SSO kan een LDAP-gebruiker inloggen op clienttoepassingen met een gebruikersnaam en wachtwoord dat op de IDP voor authentiek is. Een inloggen van een gebruiker op een van de ondersteunde webtoepassingen voor Unified Communications-producten, nadat u de SAML SSO-functie hebt ingeschakeld, krijgt u ook toegang tot deze webtoepassingen op UCXN (behalve CUCM en CUCM IM and Presence):

Unity Connection-gebruikers

LDAP-gebruikers met rechten voor beheerders

LDAP-gebruikers zonder rechten voor beheerders

Webtoepassingen

- UCXN-toediening
- Cisco UCXN-servicemodule
- Cisco Unified Services
- Cisco Mobile Communications Assistant
- Web inbox
- Mini Web Inbox (desktopversie)
- Cisco Mobile Communications Assistant
- Web inbox
- Mini Web Inbox (desktopversie)
- Cisco Jabber-clients

Configureren

Netwerkdigram

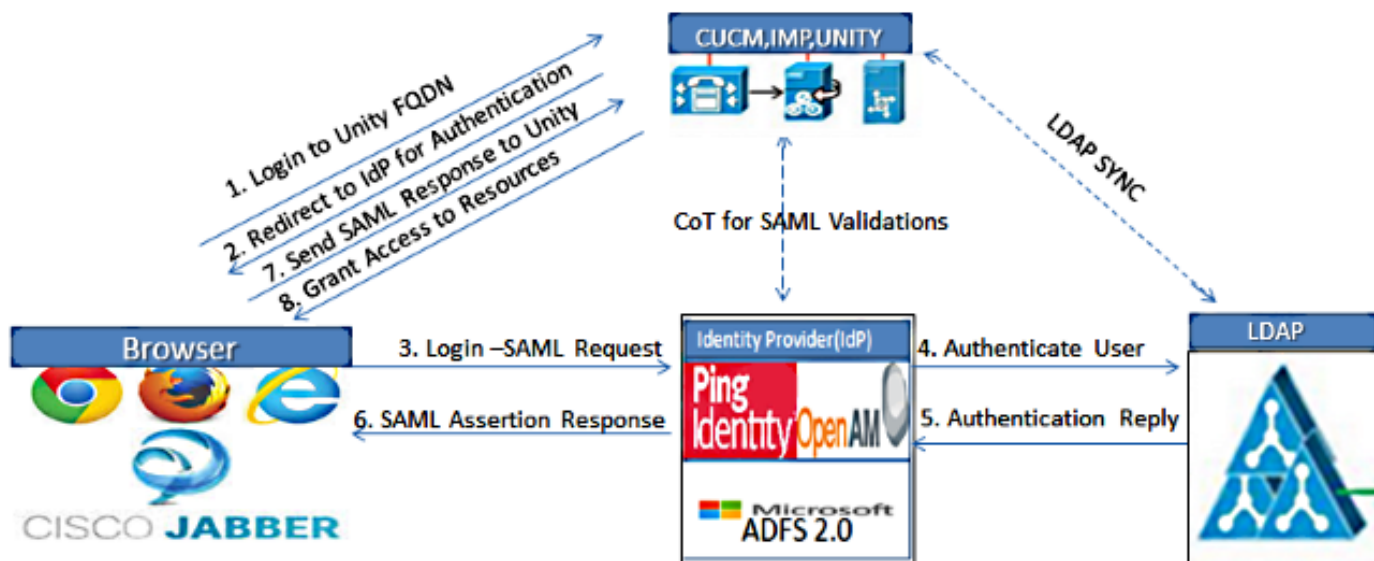


Figure :SAML Single sign SSO Call Flow for Collaboration Servers

Instellen map

1. Teken in de UCXN-beheerpagina en selecteer **LDAP** en klik op **LDAP Setup**.
2. Controleer **synchronisatie vanaf LDAP Server inschakelen** en klik op **Opslaan**.

The screenshot shows the "LDAP System Configuration" interface. It includes a "Save" button at the top left. The "Status" section shows "Status: Ready". The "LDAP System Information" section has a checked checkbox for "Enable Synchronizing from LDAP Server". Below this, there are two dropdown menus: "LDAP Server Type" set to "Microsoft Active Directory" and "LDAP Attribute for User ID" set to "sAMAccountName". A "Save" button is located at the bottom left of the configuration area.

3. Klik op **LDAP**.

4. Klik op **LDAP-adresconfiguratie**.

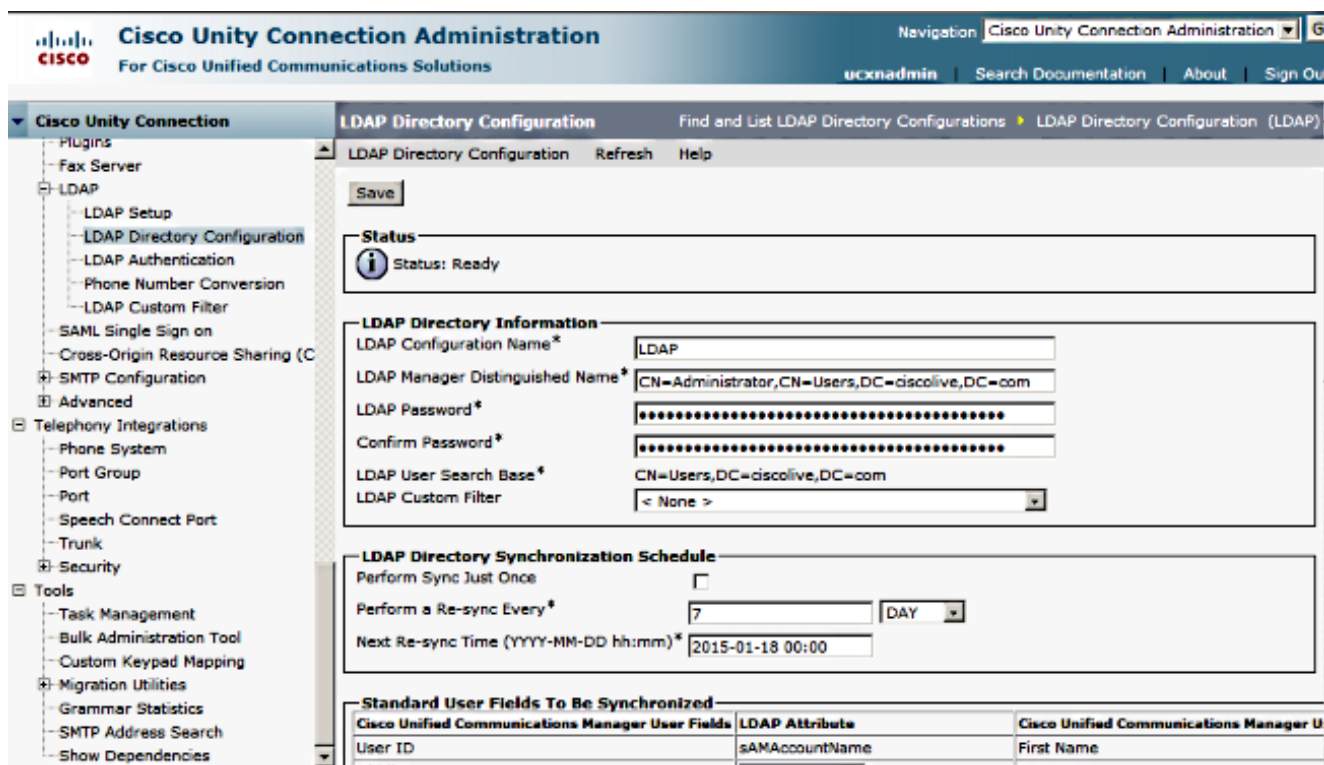
5. Klik op **Nieuw toevoegen**.

6. Deze items configureren:

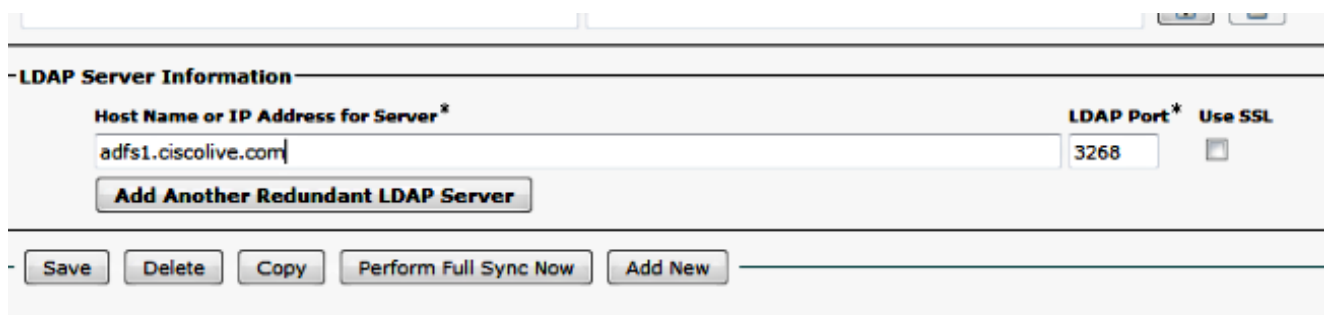
Instellingen voor live-directoryTe synchroniseren
gebruikerseigenschapsynchronisatieschemaHost-name of IP-adres en poortnummer van
de LDAP-server

7. Controleer **SSL gebruiken** als u Secure Socket Layer (SSL) wilt gebruiken om te communiceren met de LDAP folder.

Tip: Als u LDAP via SSL instelt, uploadt u het LDAP folder certificaat naar CUCM. Raadpleeg de LDAP-directory-inhoud in de [Cisco Unified Communications Manager SRND](#) voor informatie over het accountsynchronisatiemechanisme voor specifieke LBP-producten en algemene beste praktijken voor de synchronisatie van LDAP.



8. Klik op **Nu volledige sync uitvoeren**.



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

9. **Gebruikers** uitvouwen en selecteer **Gebruikers van importeren**.

10. Selecteer in de lijst **Eindgebruikers van Unified Communications Manager** zoeken de optie **LDAP-map**.

11. Als u slechts een deelgroep van de gebruikers in de LDAP-map wilt importeren waarmee u UCXN hebt geïntegreerd, voert u de toepasselijke specificaties in de zoekvelden in.

12. Selecteer **Zoeken**.

13. Selecteer in de op Sjabloonlijst gebaseerde lijst de **Administrator-sjabloon** die u wilt gebruiken als u de geselecteerde gebruikers wilt maken.

Voorzichtig: Als u een beheerdersjabloon specificeert, hebben de gebruikers geen postvakjes.

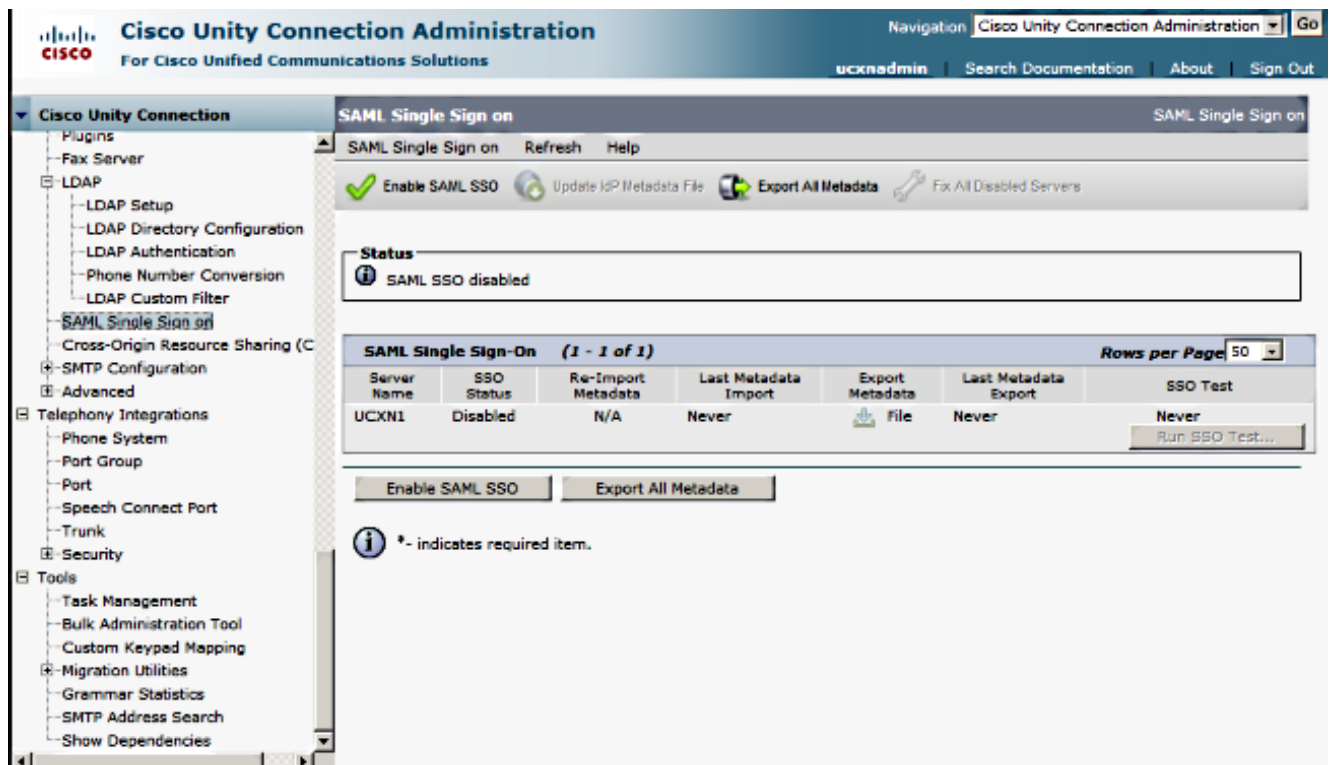
14. Controleer de aanvinkjes voor de gebruikers van LDAP voor wie u UCXN gebruikers wilt maken en klik op **Geselecteerd importeren**.

The screenshot shows the Cisco Unity Connection Administration interface. The left sidebar contains a tree view with categories like Users, Class of Service, Templates, Contacts, Distribution Lists, Call Management, and Message Storage. The main content area is titled 'Import Users' and includes a search bar, a 'Find' section with dropdowns for 'Find End Users In' (set to 'LDAP Directory') and 'Where' (set to 'Alias'), and an 'Import With' section with a dropdown for 'Based on Template' (set to 'administratortemplate'). Below these is a 'Directory Search Results' section with a table showing search results. The table has columns for 'Alias', 'First Name', 'Last Name', 'Phone Number', and 'Extension'. A single row is visible with 'sso' in the Alias column, 'Saml' in the First Name column, and 'SSO' in the Last Name column. There are 'Import Selected' and 'Import All' buttons above and below the table.

SAML SSO inschakelen

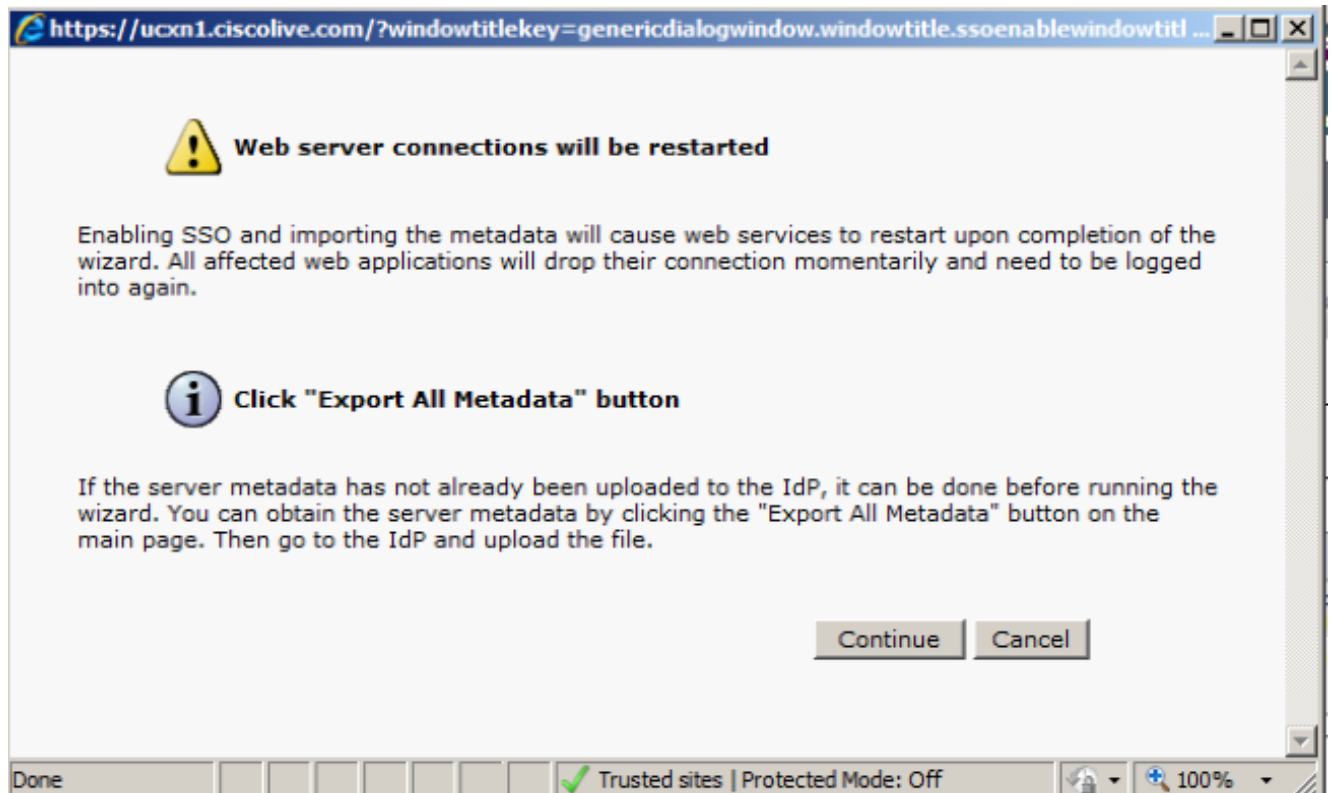
1. Log in op de UCXN-gebruikersinterface.

2. Kies **Systeem > SAML single-aanmelding** en het venster voor SAML SETL Configuration verschijnt.

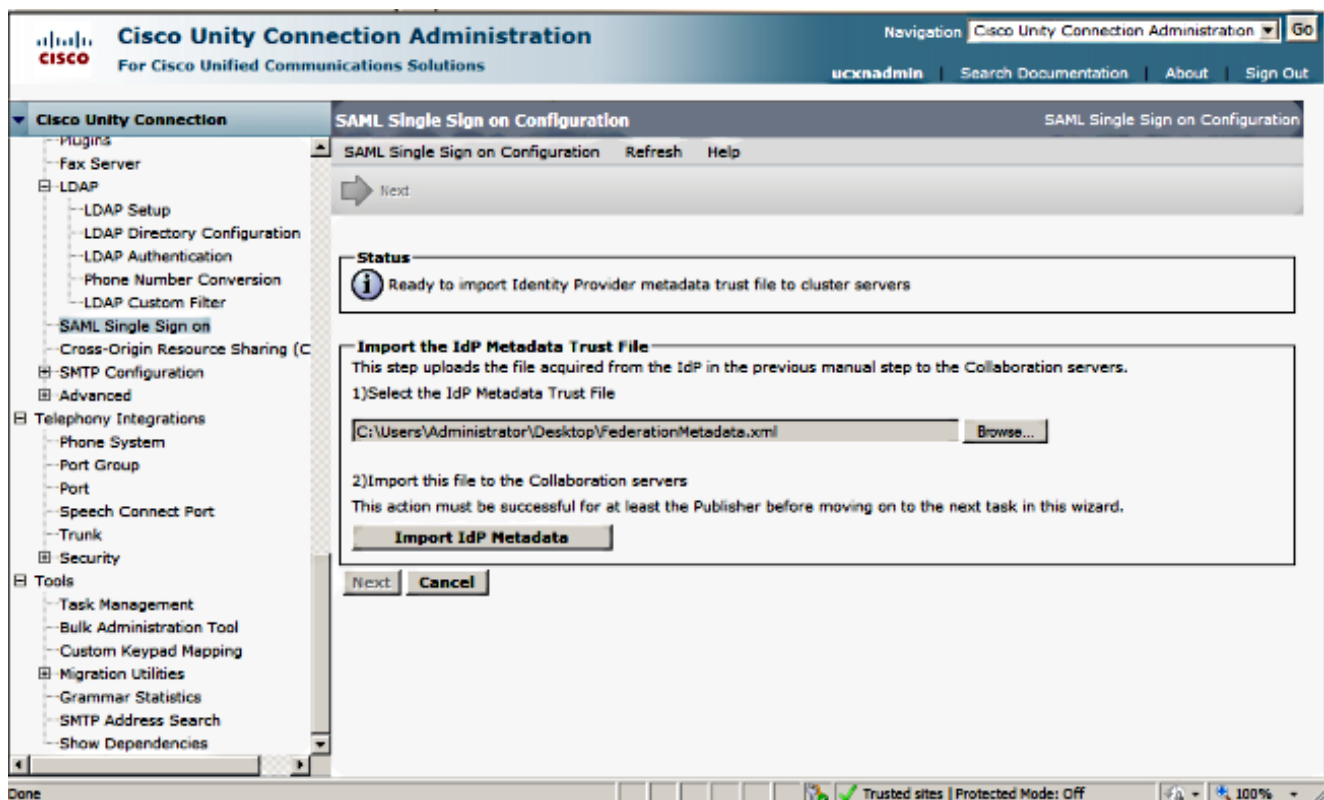


3. Klik om SAML SSO op het cluster in te schakelen op **SAML SSO**.

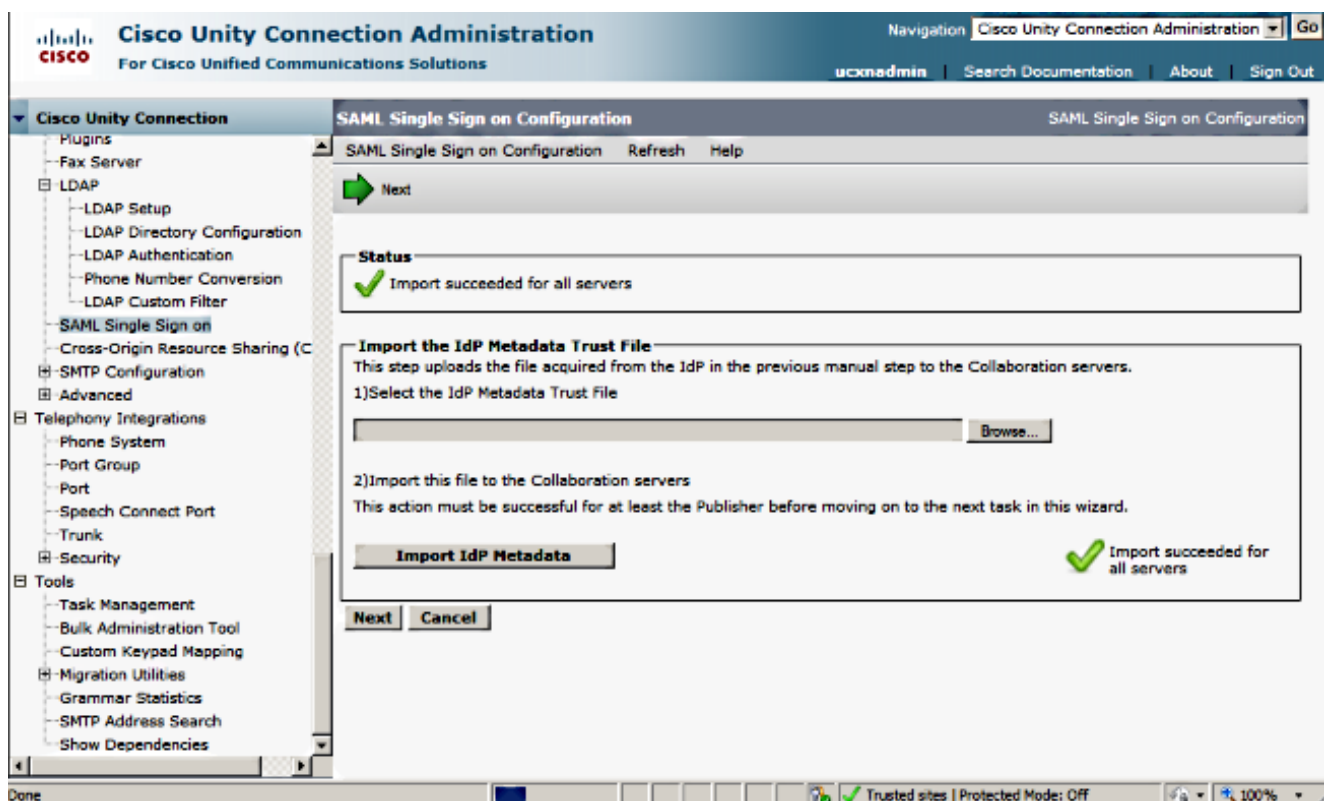
4. Klik in het venster Waarschuwing opnieuw instellen op **Doorgaan**.



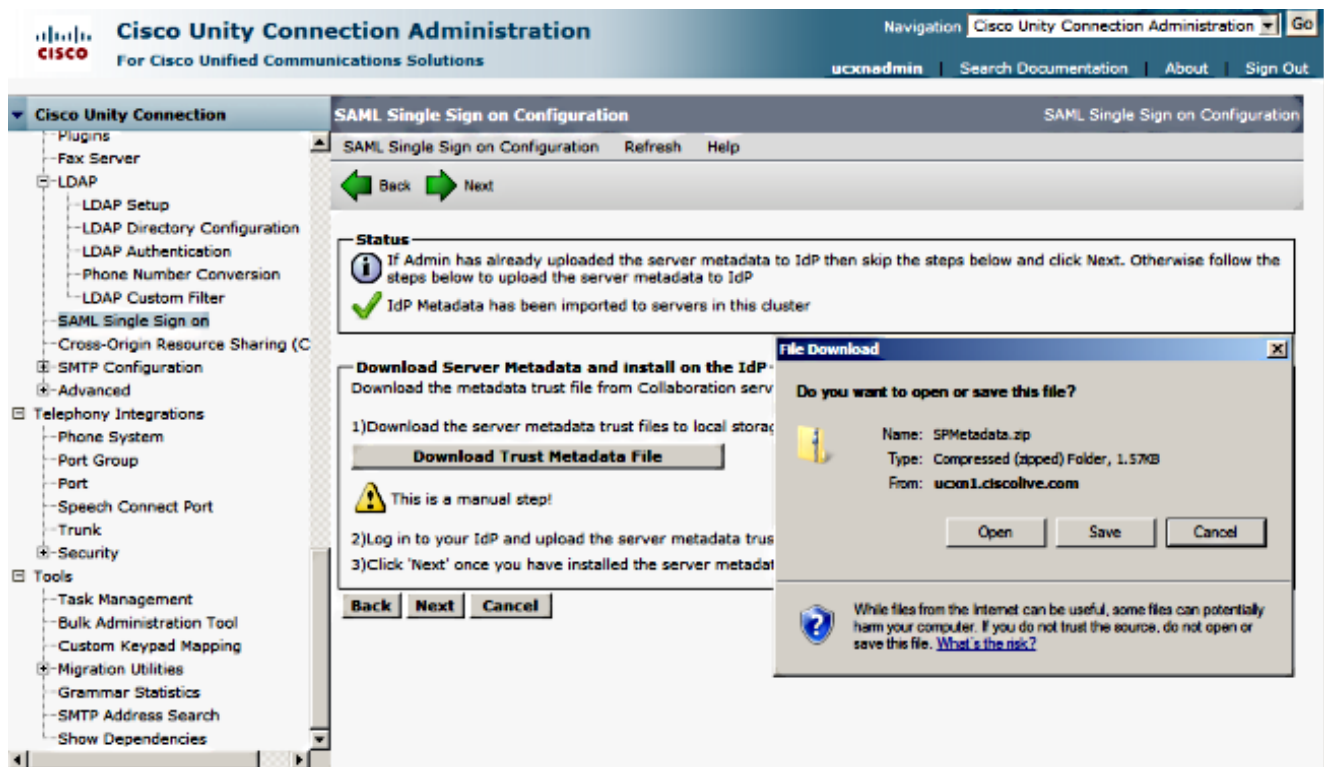
5. Klik op het SSO-scherm op **Bladeren** om het XML-bestand met metagegevens over **FederatieMetagegevens.xml** te importeren met de stap IP-metagegevens.



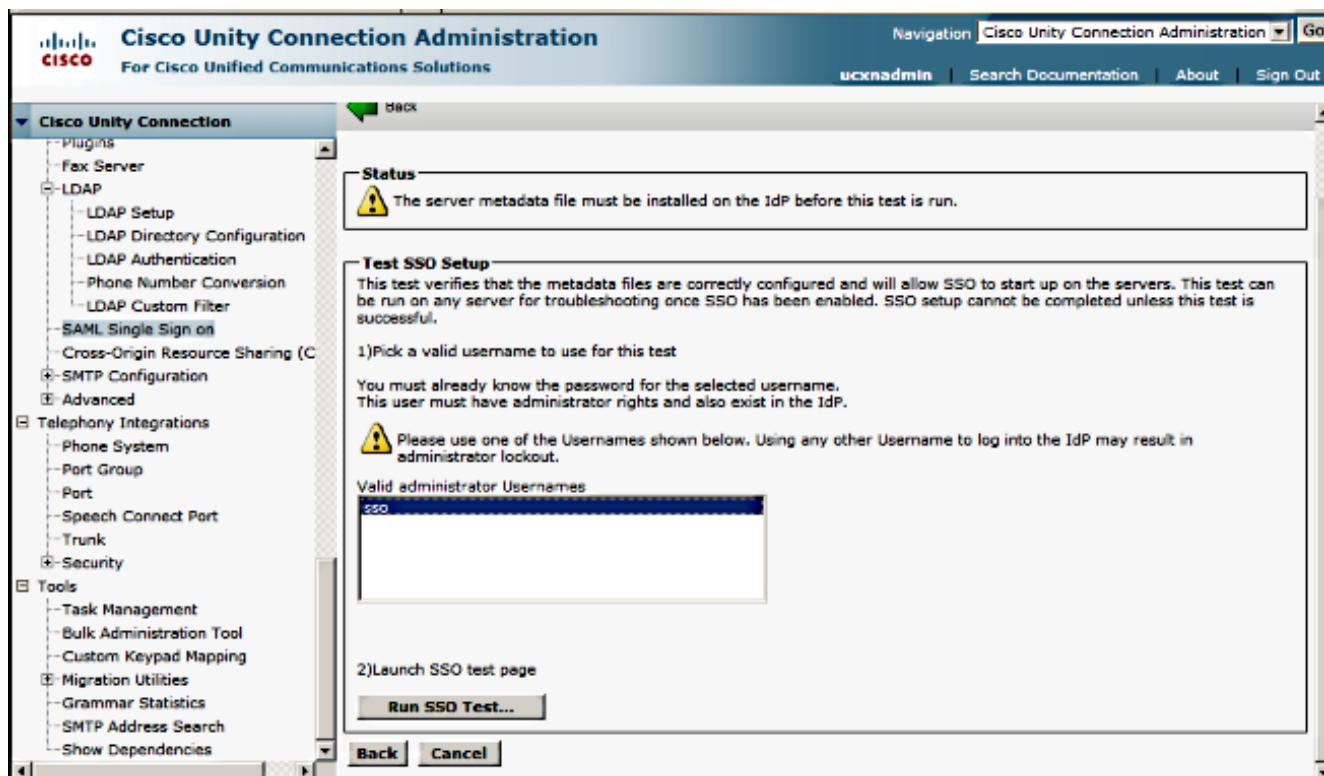
6. Klik na het uploaden van het metagegevensbestand op **Importeren van IDP-metagegevens** om de IDP-informatie naar UCXN te importeren. Bevestig dat de invoer succesvol was en klik op **Volgende** om verder te gaan.



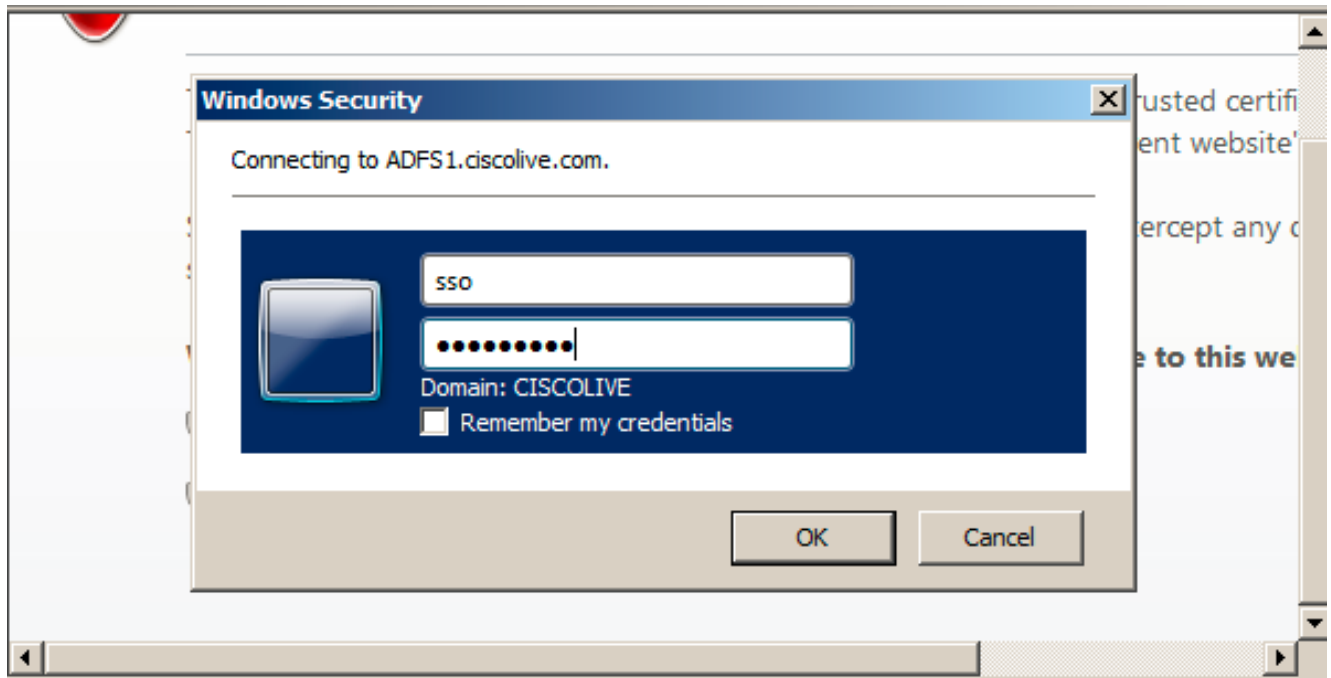
7. Klik op **Download Trust Metadata File** (doe dit alleen als u al geen ADFS met UCXN Metagegevens hebt ingesteld) om de UCXN metagegevens in een lokale map op te slaan en [UCXN als Relaying Party Trust](#) toe te [voegen](#). Ga verder naar stap 8 zodra de configuratie van de AD FS is voltooid.



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

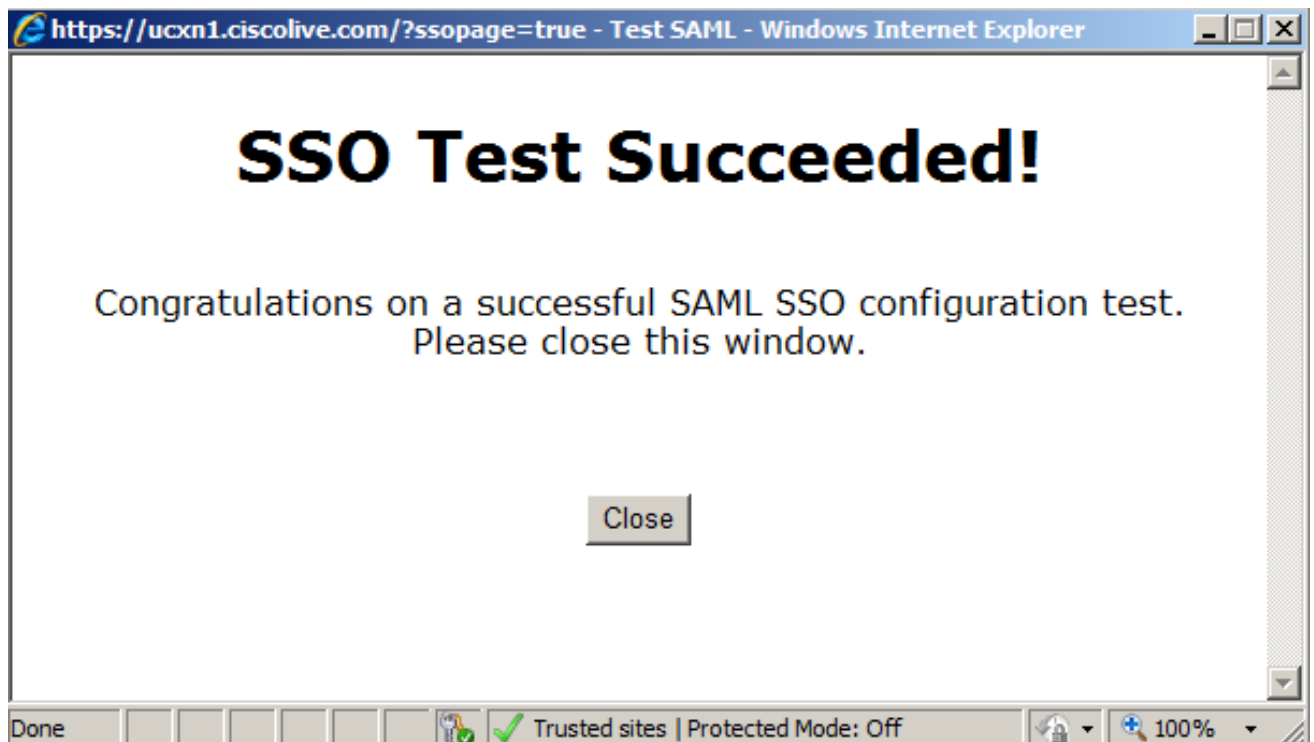


9. certificaatwaarschuwingen negeren en verder gaan. Wanneer u wordt gevraagd om inzendingen, voert u de gebruikersnaam en het wachtwoord van de SSO in en klikt u op OK.



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

10. Nadat alle stappen zijn voltooid, ontvangt u de "SSO Test Success"! bericht. Klik op **Sluiten** en **Voltooien** om verder te gaan.



U hebt nu de configuratietaken voltooid om SSO op UCXN met AD FS in te schakelen.

Verplicht. Opmerking: Start de SSO-test voor UCXN Subscriber als dit een cluster is, om SAML SSO in te schakelen. AD FS moet worden geconfigureerd voor alle knooppunten van

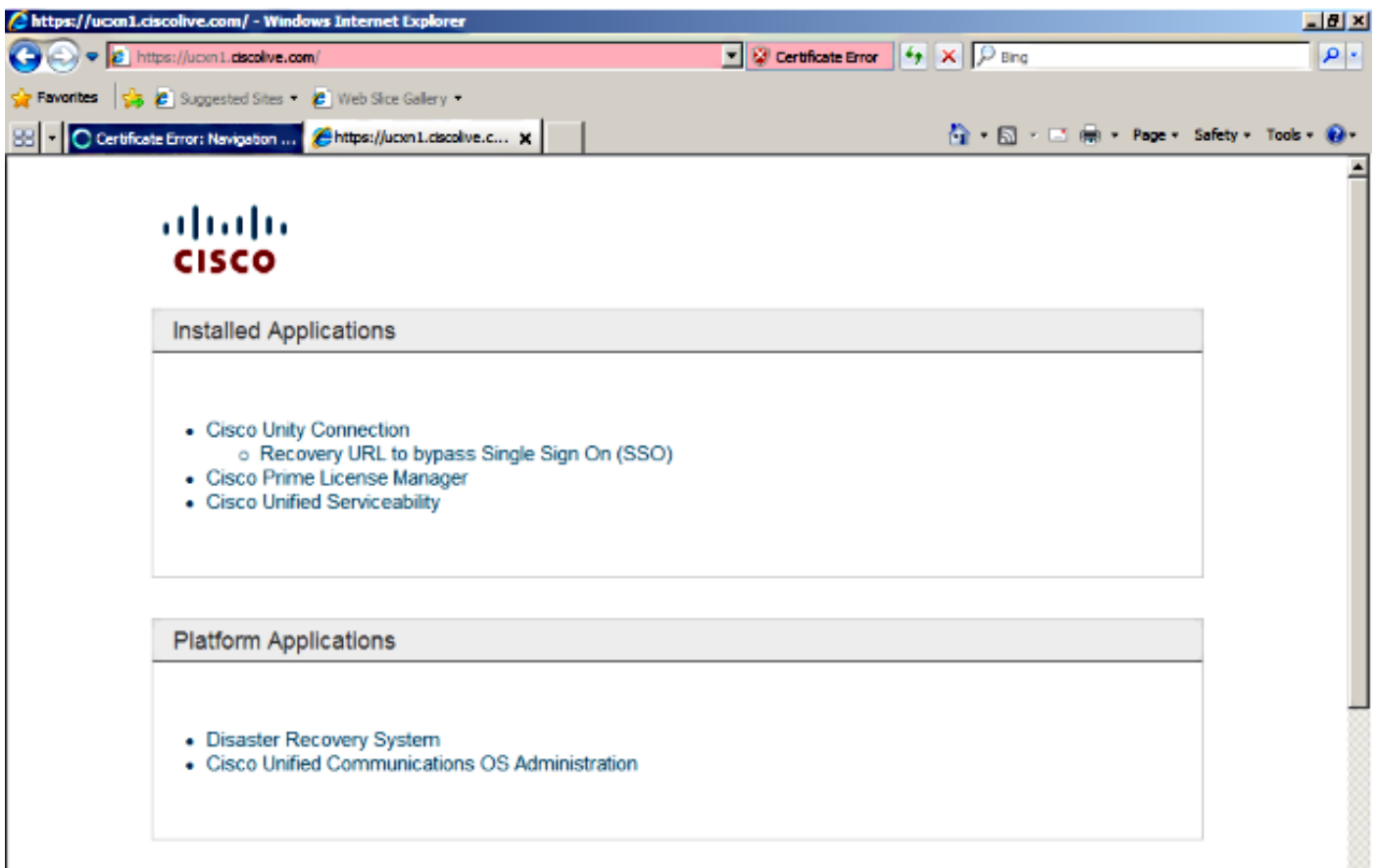
UCXN in een cluster.

Tip: Als u de XML-bestanden van alle knooppunten op IDP configureren en de SSO-bewerking op één knooppunt start, dan is SAML SSO automatisch ingeschakeld op alle knooppunten in de cluster.

U kunt ook CUCM en CUCM IM and Presence voor SAML SSO configureren als u SAML SSO wilt gebruiken voor Cisco Jabber Clients en een echte SSO-ervaring aan eindgebruikers geven.

Verifiëren

Open een webbrowser en voer de FQDN van UCXN in en u ziet een nieuwe optie onder Geïnstalleerde toepassingen met de naam **Terugwinning URL om Single aanmelding (SSO) te omzeilen**. Zodra u op de link **Cisco Unity Connection** klikt, wordt u gevraagd om aanmeldingsgegevens in het ADSL-bestand. Nadat u de aanmeldingsgegevens van SSO's van gebruikers hebt ingevoerd, wordt u aangemeld bij Unity Management-pagina, Unified Serviceability-pagina.



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

- Licentiebeheer voor Prime
- OS-beheer
- Noodherstelsysteem

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.

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