

Unity Connection-Version 10.5 SAML SSO-Konfigurationsbeispiel

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Network Time Protocol \(NTP\)-Einrichtung](#)

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

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[Netzwerkdigramm](#)

[Verzeichniseinrichtung](#)

[SAML SSO aktivieren](#)

[Überprüfen](#)

[Fehlerbehebung](#)

Einführung

In diesem Dokument wird beschrieben, wie die SAML (Security Assertion Markup Language) Single Sign-On (SSO) für Cisco Unity Connection (UCXN) konfiguriert und verifiziert wird.

Voraussetzungen

Anforderungen

Network Time Protocol (NTP)-Einrichtung

Damit SAML SSO funktioniert, müssen Sie die richtige NTP-Konfiguration installieren und sicherstellen, dass die Zeitdifferenz zwischen dem Identity Provider (IdP) und den Unified Communications-Anwendungen drei Sekunden nicht überschreitet. Weitere Informationen zur Synchronisierung von Uhren finden Sie im Abschnitt "NTP Settings" (NTP-Einstellungen) im [Administratorleitfaden für das Cisco Unified Communications-Betriebssystem](#).

DNS-Einrichtung (Domain Name Server)

Unified Communications-Anwendungen können DNS verwenden, um vollständig qualifizierte Domännennamen (FQDNs) in IP-Adressen aufzulösen. Die Service Provider und die IdP müssen vom Browser auflösbar sein.

Active Directory Federation Service (AD FS) Version 2.0 muss installiert und konfiguriert werden, um SAML-Anfragen zu bearbeiten.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- AD FS Version 2.0 als IdP
- UCXN als Service Provider
- Microsoft Internet Explorer Version 10

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

SAML ist ein XML-basiertes, offenes Datenformat für den Datenaustausch. Es ist ein Authentifizierungsprotokoll, das von Service Providern zur Authentifizierung eines Benutzers verwendet wird. Die Informationen zur Sicherheitsauthentifizierung werden zwischen einem IdP und dem Service Provider weitergegeben.

SAML ist ein offener Standard, der es Clients ermöglicht, sich gegen jeden SAML-fähigen Collaboration- (oder Unified Communication-) Service zu authentifizieren, unabhängig von der Client-Plattform.

Alle Cisco Unified Communication-Webschnittstellen, wie z. B. Cisco Unified Communications Manager (CUCM) oder UCXN, verwenden das SAML Version 2.0-Protokoll in der SAML SSO-Funktion. Um den LDAP-Benutzer (Lightweight Directory Access Protocol) zu authentifizieren, delegiert UCXN eine Authentifizierungsanforderung an die IDP. Diese vom UCXN generierte Authentifizierungsanfrage ist eine SAML-Anforderung. Die IDP authentifiziert und gibt eine SAML-Assertion zurück. Die SAML-Assertion zeigt entweder Yes (authentifiziert) oder No (Authentifizierung fehlgeschlagen) an.

Mit SAML SSO kann sich ein LDAP-Benutzer mit einem Benutzernamen und einem Kennwort, die sich auf dem IdP authentifizieren, bei Client-Anwendungen anmelden. Wenn Sie die SAML SSO-Funktion aktiviert haben, erhalten Benutzer, die sich bei einer der unterstützten Webanwendungen für Unified Communication-Produkte anmelden, auch Zugriff auf diese Webanwendungen auf UCXN (außer CUCM und CUCM IM und Presence):

Unity Connection-Benutzer

Webanwendungen

LDAP-Benutzer mit Administratorrechten

- UCXN-Administration
- Cisco UCXN-Benutzerfreundlichkeit
- Cisco Unified Serviceability
- Cisco Personal Communications Assistant
- Web-Posteingang
- Mini-Web-Posteingang (Desktop-Version)
- Cisco Personal Communications Assistant
- Web-Posteingang

LDAP-Benutzer ohne Administratorrechte

- Mini-Web-Posteingang (Desktop-Version)
- Cisco Jabber-Clients

Konfigurieren

Netzwerkdiagramm

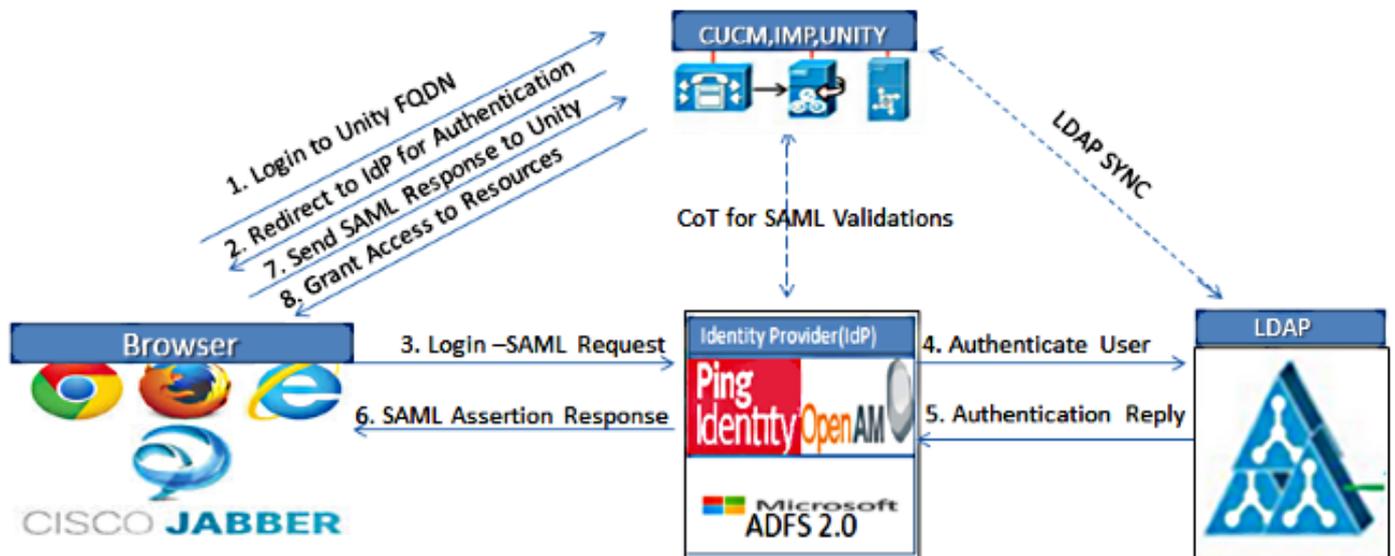
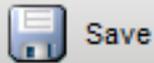


Figure :SAML Single sign SSO Call Flow for Collaboration Servers

Verzeichniseinrichtung

1. Melden Sie sich bei der UCXN-Administrationsseite an, wählen Sie **LDAP aus**, und klicken Sie auf **LDAP Setup**.
2. Aktivieren Sie die Option **Synchronisierung vom LDAP-Server aktivieren**, und klicken Sie auf **Speichern**.

LDAP System Configuration



Save

Status



Status: Ready

LDAP System Information

Enable Synchronizing from LDAP Server

LDAP Server Type

LDAP Attribute for User ID

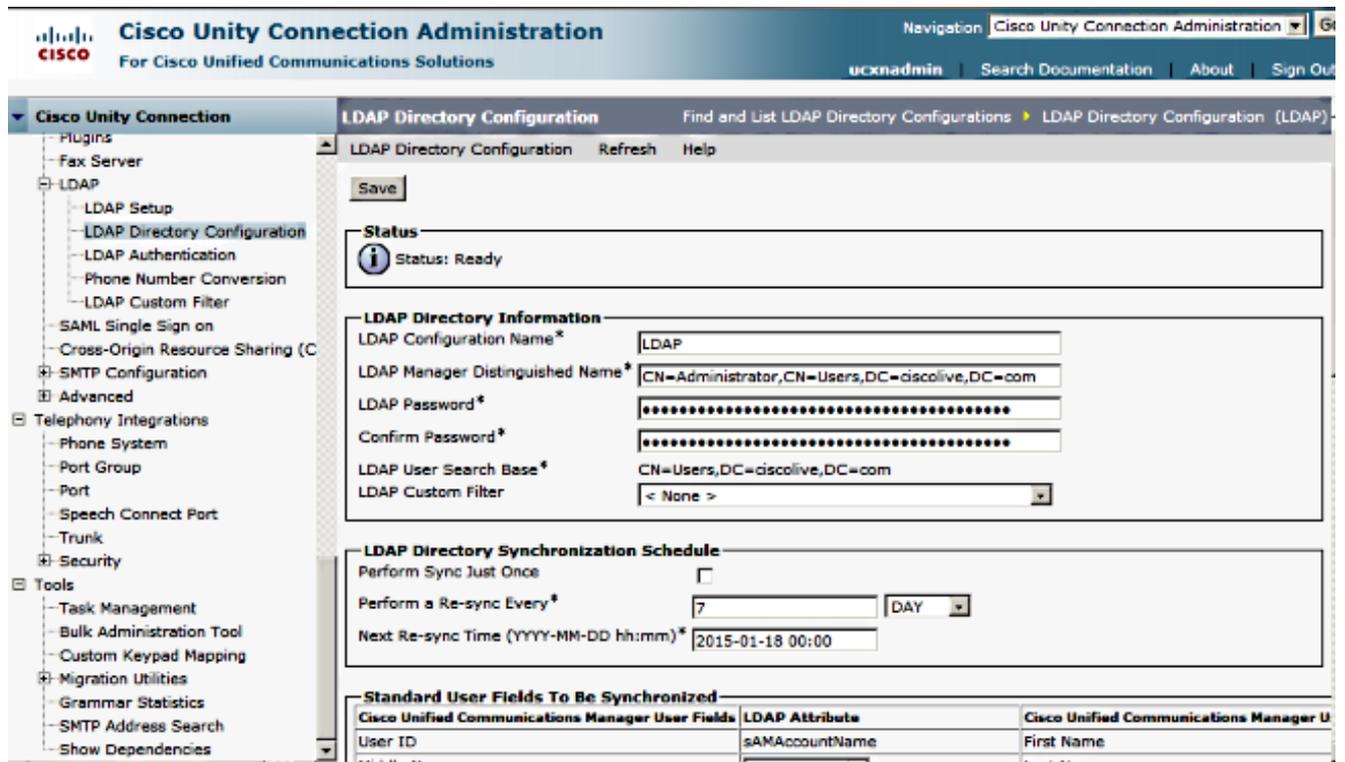
Save

3. Klicken Sie auf **LDAP**.
4. Klicken Sie auf **LDAP-Verzeichniskonfiguration**.
5. Klicken Sie auf **Neu hinzufügen**.
6. Konfigurieren Sie diese Elemente:

Kontoeinstellungen für LDAP-Verzeichnisse
Zu synchronisierende Benutzerattribute
Synchronisierungsplan
Hostname oder IP-Adresse des LDAP-Servers und Portnummer

7. Aktivieren Sie **SSL verwenden**, wenn Sie Secure Socket Layer (SSL) verwenden möchten, um mit dem LDAP-Verzeichnis zu kommunizieren.

Tipp: Wenn Sie LDAP über SSL konfigurieren, laden Sie das LDAP-Verzeichniszertifikat auf den CUCM hoch. Informationen zum Synchronisierungsmechanismus für bestimmte LDAP-Produkte und allgemeine Best Practices für die LDAP-Synchronisierung finden Sie im LDAP-Verzeichnisinhalt im [Cisco Unified Communications Manager SRND](#).



8. Klicken Sie auf **Vollständige Synchronisierung jetzt durchführen**.



Hinweis: Vergewissern Sie sich, dass der **Cisco DirSync**-Dienst auf der Webseite Serviceability aktiviert ist, bevor Sie auf Save (Speichern) klicken.

9. Erweitern Sie **Benutzer**, und wählen Sie **Benutzer importieren aus**.

10. Wählen Sie in der Liste **Endbenutzer für Unified Communications Manager suchen** die Option **LDAP-Verzeichnis** aus.

11. Wenn Sie nur eine Teilmenge der Benutzer im LDAP-Verzeichnis importieren möchten, mit dem Sie UCXN integriert haben, geben Sie die entsprechenden Spezifikationen in die Suchfelder ein.

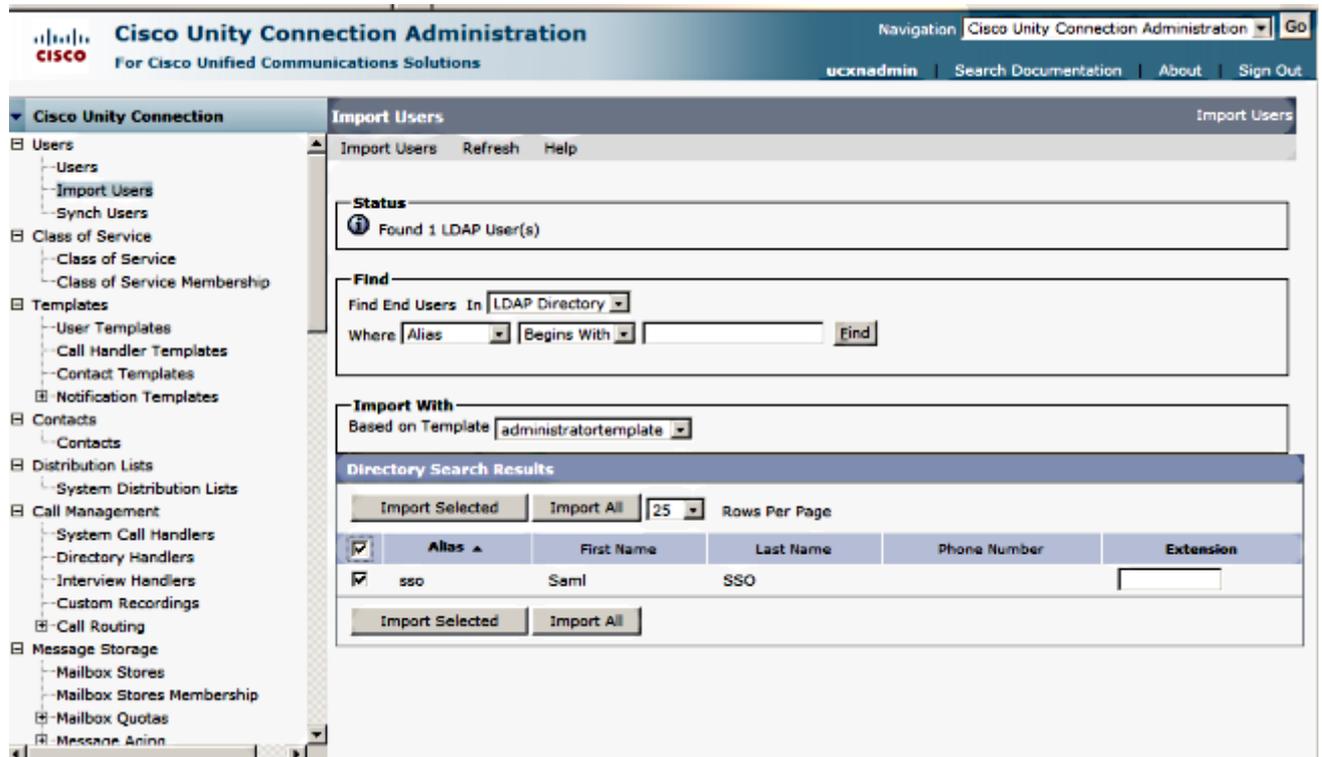
12. Wählen Sie **Suchen** aus.

13. Wählen Sie in der Liste Basierend auf Vorlage die **Administratorvorlage** aus, die UCXN bei der Erstellung der ausgewählten Benutzer verwenden soll.

Vorsicht: Wenn Sie eine Administratorvorlage angeben, verfügen die Benutzer nicht über

Mailboxen.

14. Aktivieren Sie die Kontrollkästchen für die LDAP-Benutzer, für die Sie UCXN-Benutzer erstellen möchten, und klicken Sie auf **Import Selected (Ausgewählt importieren)**.



SAML SSO aktivieren

1. Melden Sie sich bei der UCXN Administration-Benutzeroberfläche an.
2. Wählen Sie **System > SAML Single Sign-on**, und das Fenster SAML SSO Configuration (SSO-Konfiguration für SAML) wird geöffnet.

Cisco Unity Connection Administration
For Cisco Unified Communications Solutions

Navigation: Cisco Unity Connection Administration | Go
ucxnadmin | Search Documentation | About | Sign Out

SAML Single Sign on

Enable SAML SSO | Update IdP Metadata File | Export All Metadata | Fix All Disabled Servers

Status
SAML SSO disabled

Server Name	SSO Status	Re-Import Metadata	Last Metadata Import	Export Metadata	Last Metadata Export	SSO Test
UCXN1	Disabled	N/A	Never	File	Never	Never Run SSO Test...

Enable SAML SSO | Export All Metadata

* - indicates required item.

3. Um die SAML-SSO für den Cluster zu aktivieren, klicken Sie auf **SAML-SSO aktivieren**.

4. Klicken Sie im Fenster Warnung zurücksetzen auf **Weiter**.

Web server connections will be restarted

Enabling SSO and importing the metadata will cause web services to restart upon completion of the wizard. All affected web applications will drop their connection momentarily and need to be logged into again.

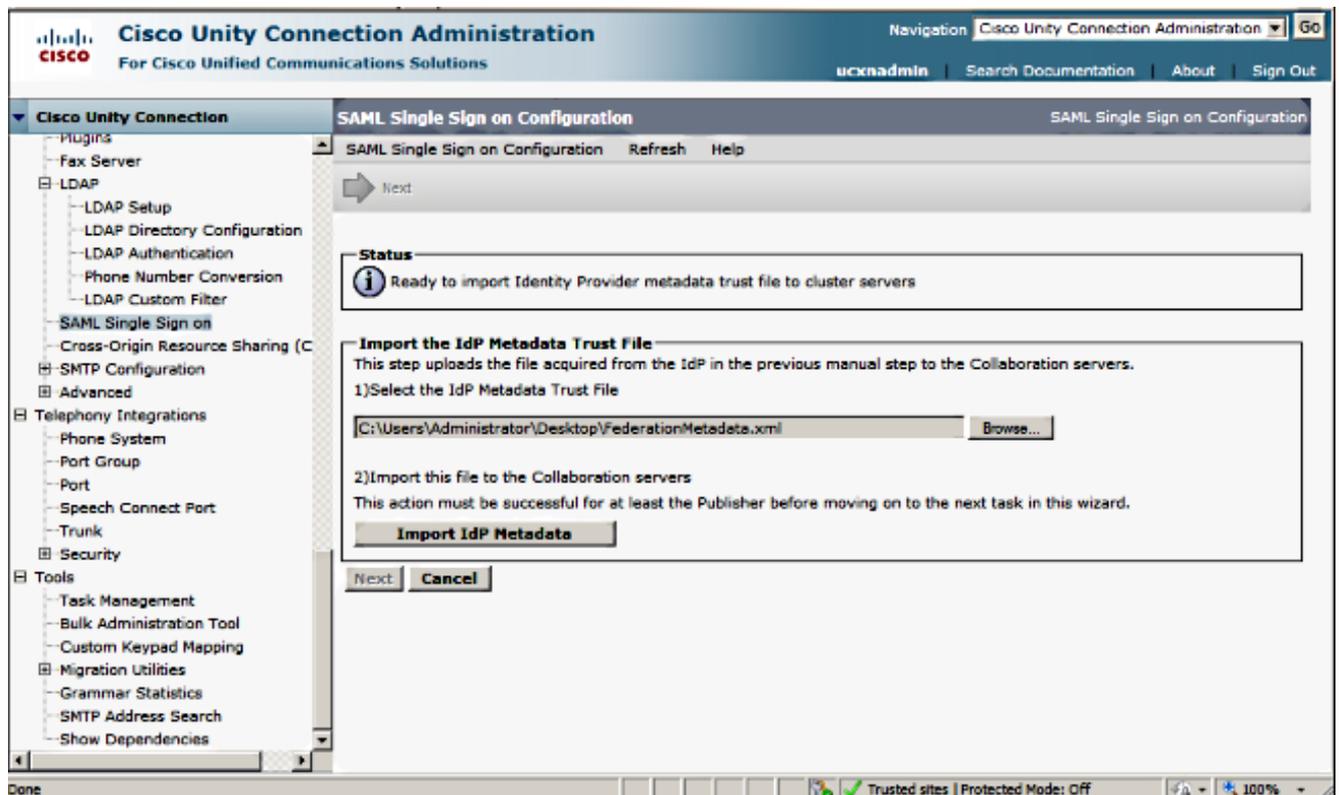
Click "Export All Metadata" button

If the server metadata has not already been uploaded to the IdP, it can be done before running the wizard. You can obtain the server metadata by clicking the "Export All Metadata" button on the main page. Then go to the IdP and upload the file.

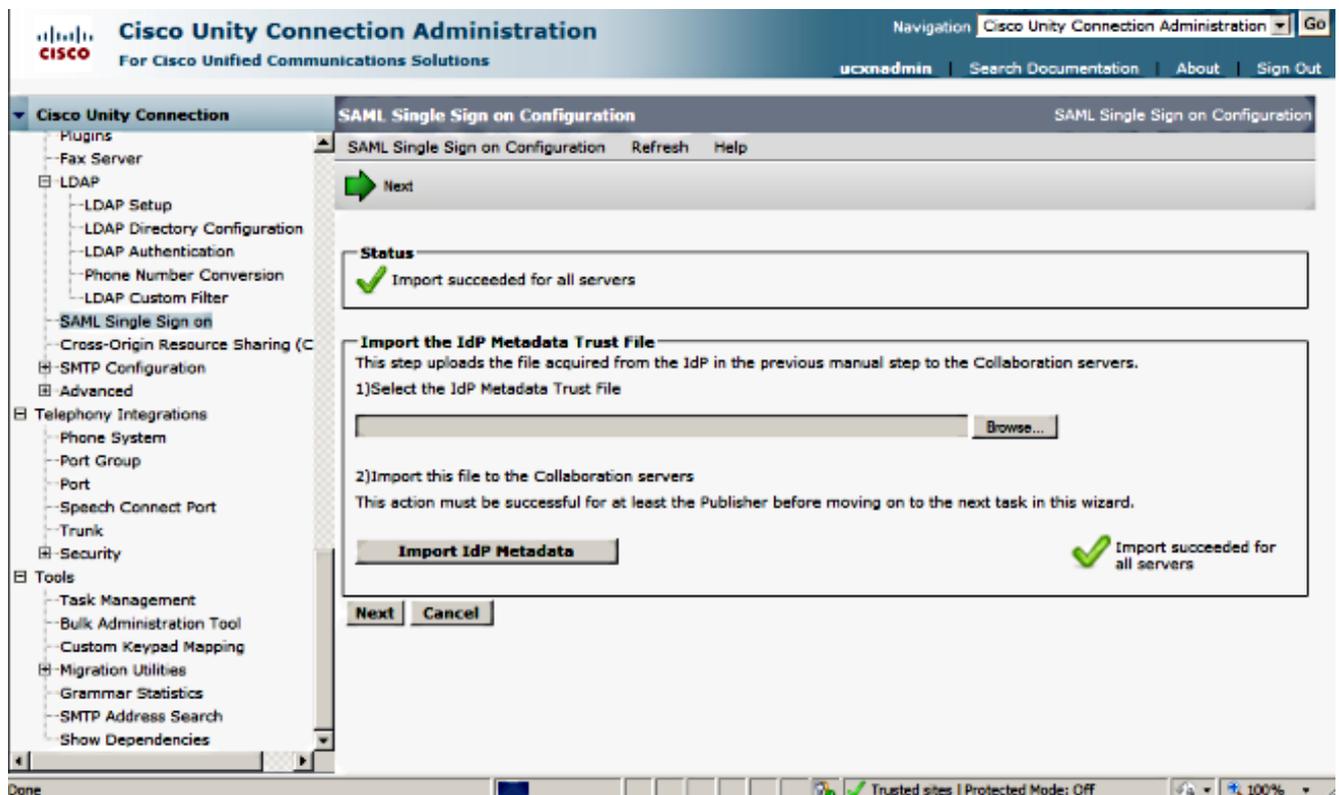
Continue | Cancel

Done | Trusted sites | Protected Mode: Off | 100%

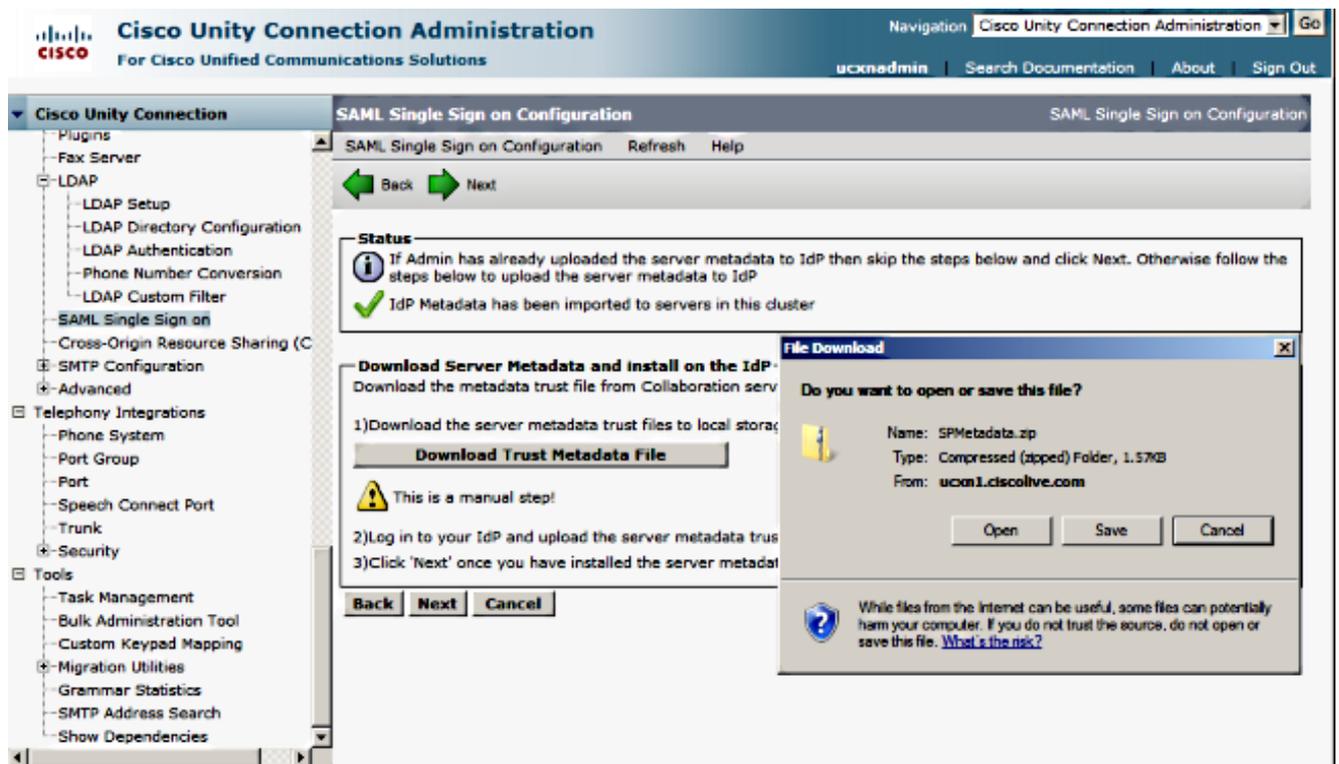
5. Klicken Sie auf dem SSO-Bildschirm auf **Durchsuchen**, um die XML-Datei **FederationMetadata.xml** Metadata mit dem Schritt **Idp Metadata** herunterladen zu importieren.



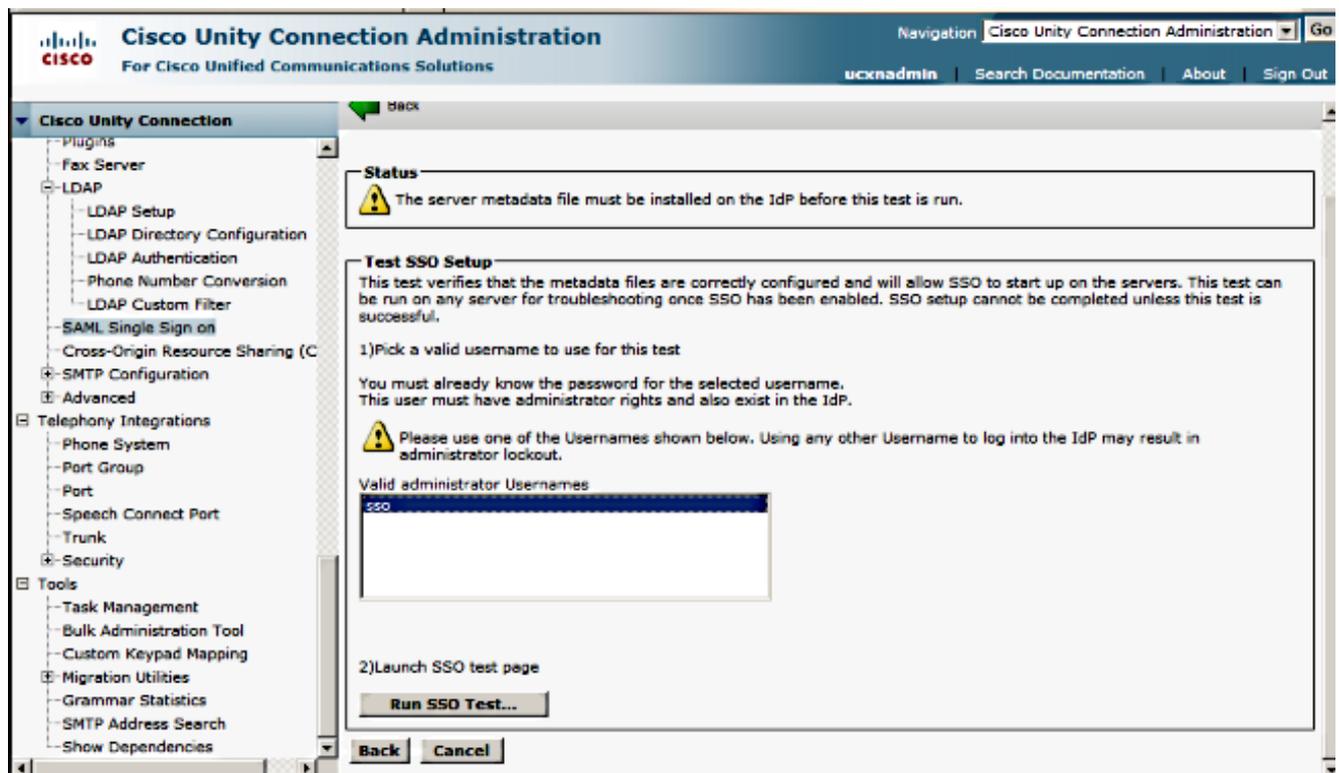
6. Klicken Sie nach dem Hochladen der Metadatenfile auf **IDP-Metadaten importieren**, um die IDP-Informationen in UCXN zu importieren. Bestätigen Sie, dass der Import erfolgreich war, und klicken Sie auf **Weiter**, um fortzufahren.



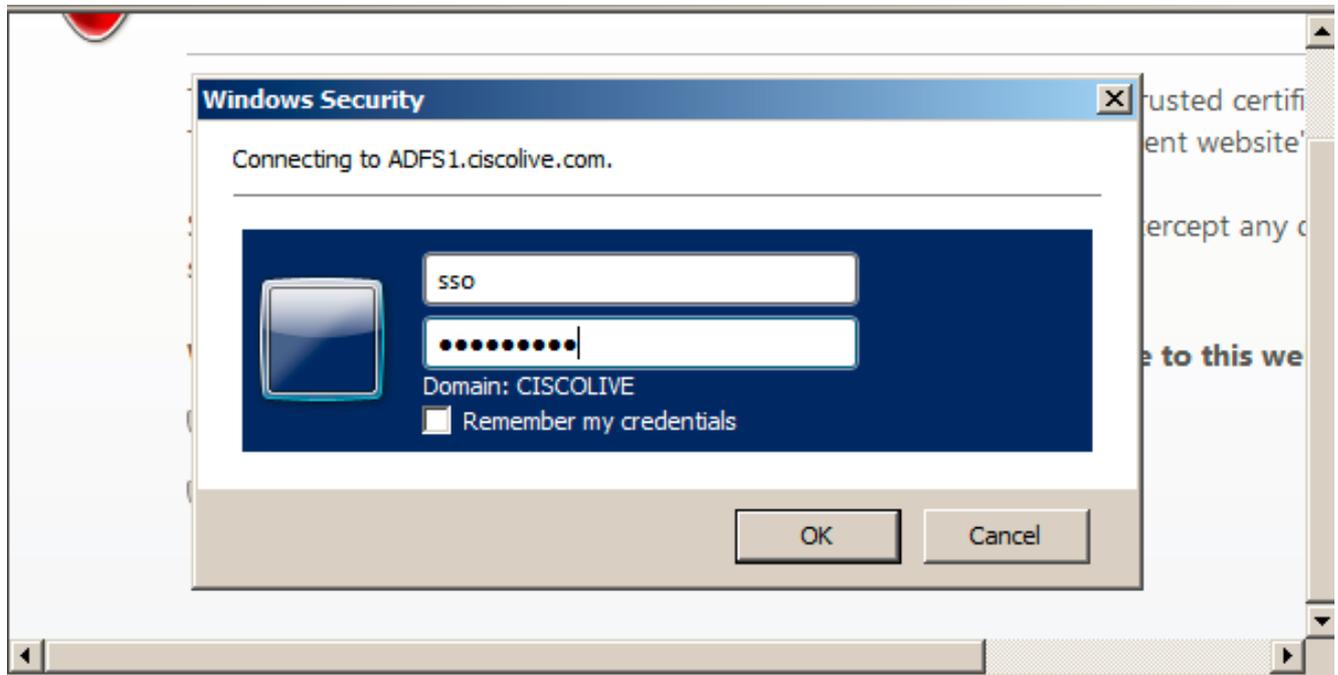
7. Klicken Sie auf **Trust Metadata Fileset herunterladen** (nur wenn Sie ADFS noch nicht mit UCXN Metadata konfiguriert haben), um die UCXN-Metadaten in einem lokalen Ordner zu speichern, und gehen Sie zum [Hinzufügen von UCXN als Relay Party Trust](#). Wenn die AD FS-Konfiguration abgeschlossen ist, fahren Sie mit Schritt 8 fort.



8. Wählen Sie **SSO** als Administrator aus, und klicken Sie auf **SSO-Test ausführen**.

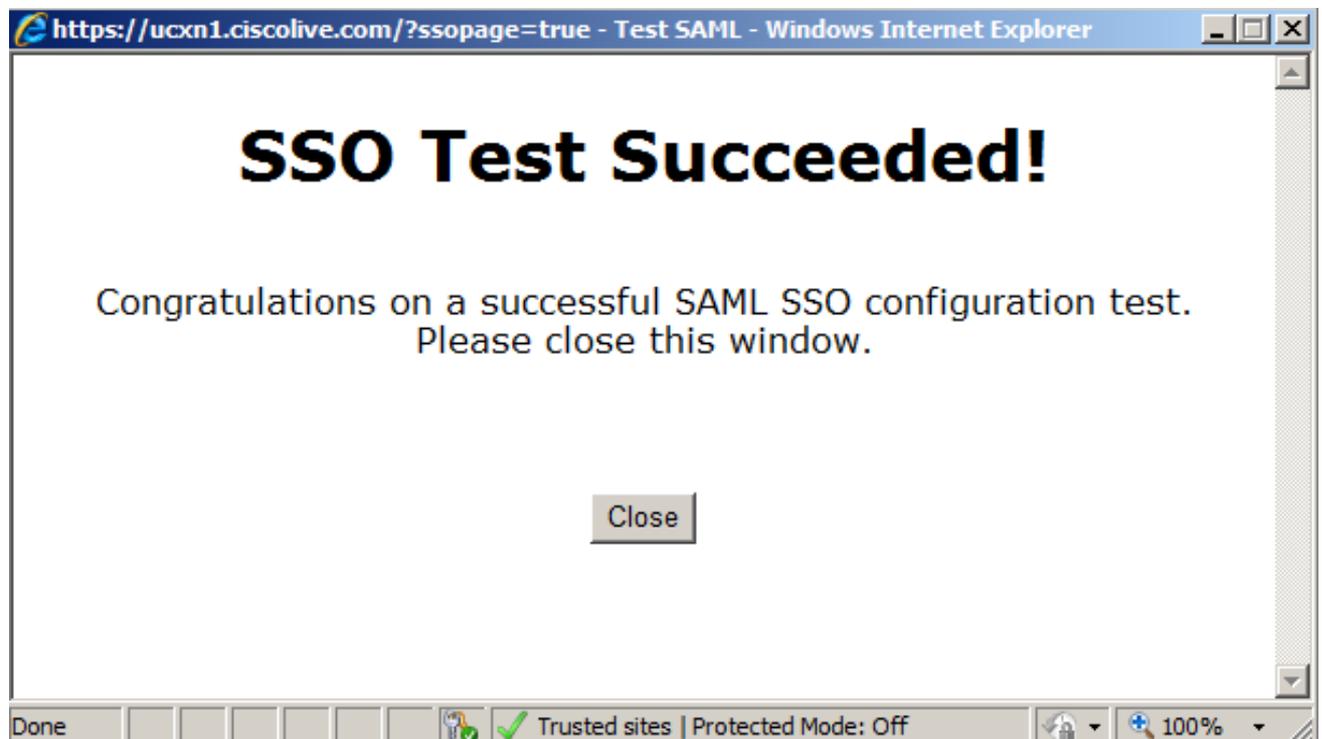


9. Zertifikatswarnungen ignorieren und weiter fortfahren Wenn Sie zur Eingabe der Anmeldeinformationen aufgefordert werden, geben Sie den Benutzernamen und das Kennwort der Benutzer-SSO ein, und klicken Sie auf **OK**.



Hinweis: Dieses Konfigurationsbeispiel basiert auf selbstsignierten UCXN- und AD FS-Zertifikaten. Falls Sie Zertifikate der Zertifizierungsstelle (Certificate Authority, CA) verwenden, müssen entsprechende Zertifikate sowohl auf AD FS als auch auf UCXN installiert sein. Weitere Informationen finden Sie unter [Zertifikatsverwaltung und -validierung](#).

10. Nachdem alle Schritte abgeschlossen sind, erhalten Sie den "SSO-Test erfolgreich durchgeführt". Nachricht. Klicken Sie auf **Schließen** und **Beenden**, um fortzufahren.



Sie haben nun die Konfigurationsaufgaben erfolgreich abgeschlossen, um SSO auf UCXN mit AD FS zu aktivieren.

Obligatorische Anmerkung: Führen Sie den SSO-Test für UCXN-Teilnehmer aus, wenn es

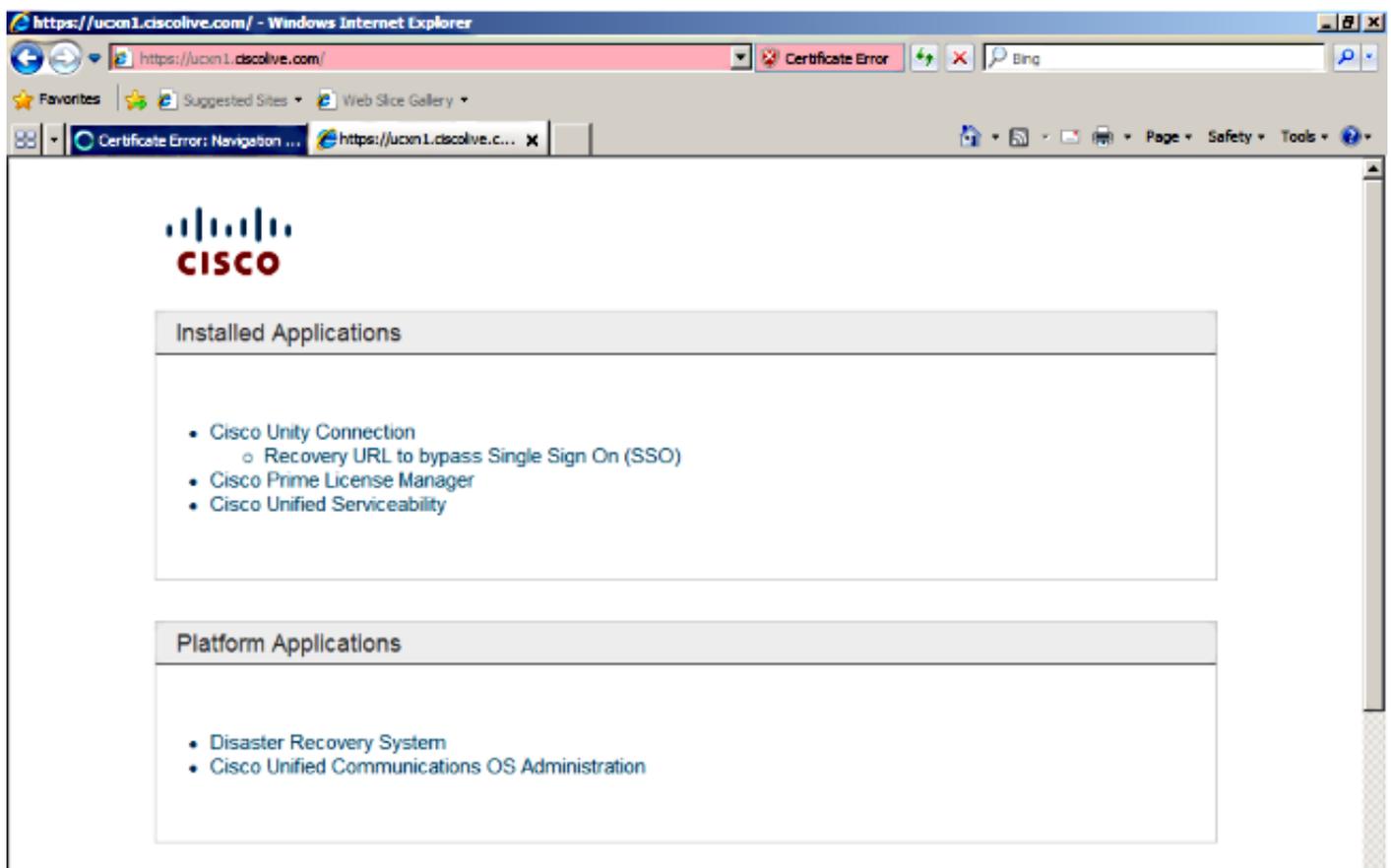
sich um ein Cluster zur Aktivierung von SAML SSO handelt. AD FS muss für alle UCXN-Knoten in einem Cluster konfiguriert werden.

Tipp: Wenn Sie die XML-Metadaten aller Knoten auf IDs konfigurieren und die SSO-Operation auf einem Knoten aktivieren, wird die SAML SSO auf allen Knoten im Cluster automatisch aktiviert.

Sie können CUCM und CUCM IM and Presence für SAML SSO auch konfigurieren, wenn Sie SAML SSO für Cisco Jabber-Clients verwenden und Endbenutzern eine echte SSO-Erfahrung bieten möchten.

Überprüfen

Öffnen Sie einen Webbrowser, und geben Sie den FQDN von UCXN ein. Unter Installierte Anwendungen sehen Sie eine neue Option namens **Recovery URL, um Single Sign-on (SSO) zu umgehen**. Wenn Sie auf den Link **Cisco Unity Connection** klicken, werden Sie vom AD FS zur Eingabe der Anmeldeinformationen aufgefordert. Nachdem Sie die Anmeldeinformationen des Benutzer-SSO eingegeben haben, werden Sie erfolgreich bei der Seite Unity Administration (Unity-Administration), Unified Serviceability (Unified Serviceability), angemeldet.



Hinweis: SAML SSO ermöglicht keinen Zugriff auf folgende Seiten:

- Prime Licensing Manager
- Betriebssystemverwaltung
- Disaster Recovery System

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Weitere Informationen finden Sie unter [Problembehandlung bei SAML SSO für Collaboration-Produkte 10.x](#).