

Unified Communications Manager 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 Unified Communications Manager (CUCM) 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.

Bei zeitlicher Abweichung zwischen CUCM und IdP wird folgender Fehler angezeigt: "Ungültige SAML-Antwort." Dieser Fehler kann auftreten, wenn die Zeit zwischen den CUCM- und IDP-Servern nicht synchronisiert ist. Damit SAML SSO funktioniert, müssen Sie die richtige NTP-Konfiguration installieren und sicherstellen, dass die Zeitdifferenz zwischen der 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.

Verwendete Komponenten

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

- Active Directory Federation Service (AD FS) Version 2.0 als IDP
- CUCM-Version 10.5 als Service Provider
- Microsoft Internet Explorer 10

Vorsicht: Dieses Dokument basiert auf einem neu installierten CUCM. Wenn Sie SAML SSO auf einem bereits in der Produktion befindlichen Server konfigurieren, müssen Sie möglicherweise einige der Schritte entsprechend überspringen. Wenn Sie die Schritte auf dem Produktionsserver durchführen, müssen Sie auch die Auswirkungen auf den Dienst verstehen. Es wird empfohlen, dieses Verfahren außerhalb der Geschäftszeiten durchzuführen.

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, auf offenen Standards basierendes Datenformat, das Administratoren den nahtlosen Zugriff auf bestimmte Cisco Collaboration-Anwendungen ermöglicht, nachdem sie sich bei einer dieser Anwendungen angemeldet haben. SAML SSO erstellt beim Austausch von Metadaten im Rahmen des Bereitstellungsprozesses zwischen dem IdP und dem Service Provider einen Circle of Trust (CoT). Der Service Provider vertraut den Benutzerinformationen der ID, um den Zugriff auf die verschiedenen Dienste oder Anwendungen zu ermöglichen.

Hinweis: Service Provider sind nicht mehr an der Authentifizierung beteiligt. SAML Version 2.0 delegiert die Authentifizierung von den Service Providern und den IdPs. Der Client authentifiziert sich anhand der IdP, und der IdP gewährt dem Client eine Assertion. Der Client stellt dem Dienstleister die Assertion dar. Da ein CoT eingerichtet ist, vertraut der Service Provider der Assertion und gewährt dem Client Zugriff.

Konfigurieren

Netzwerkdiagramm

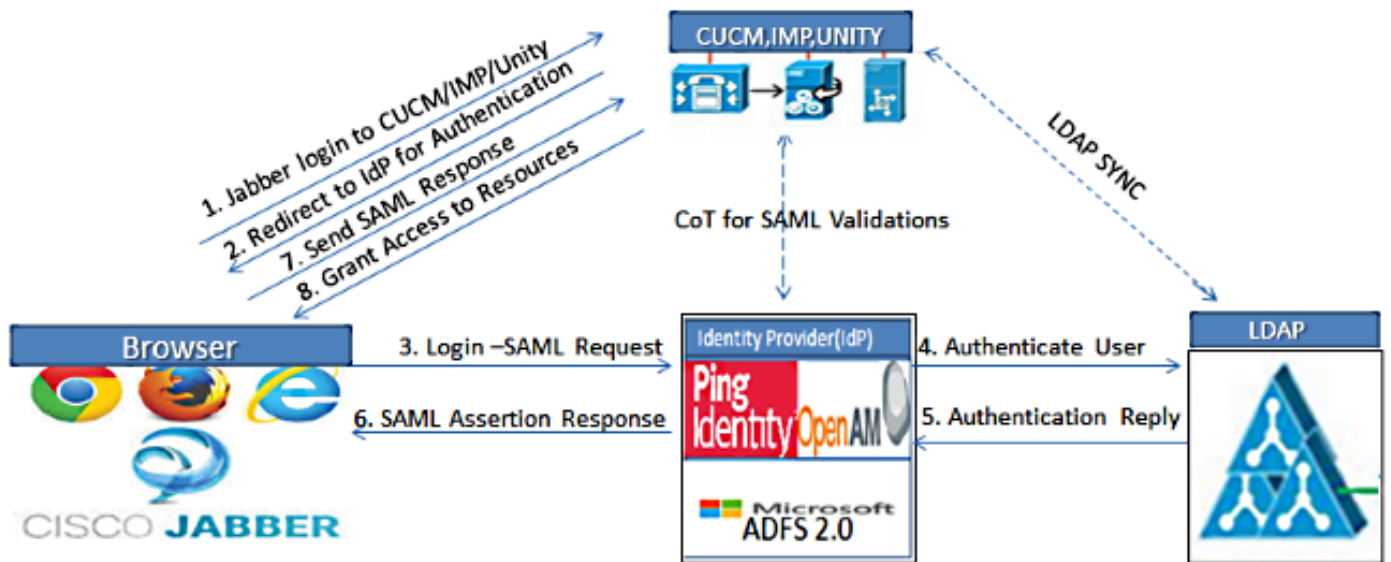
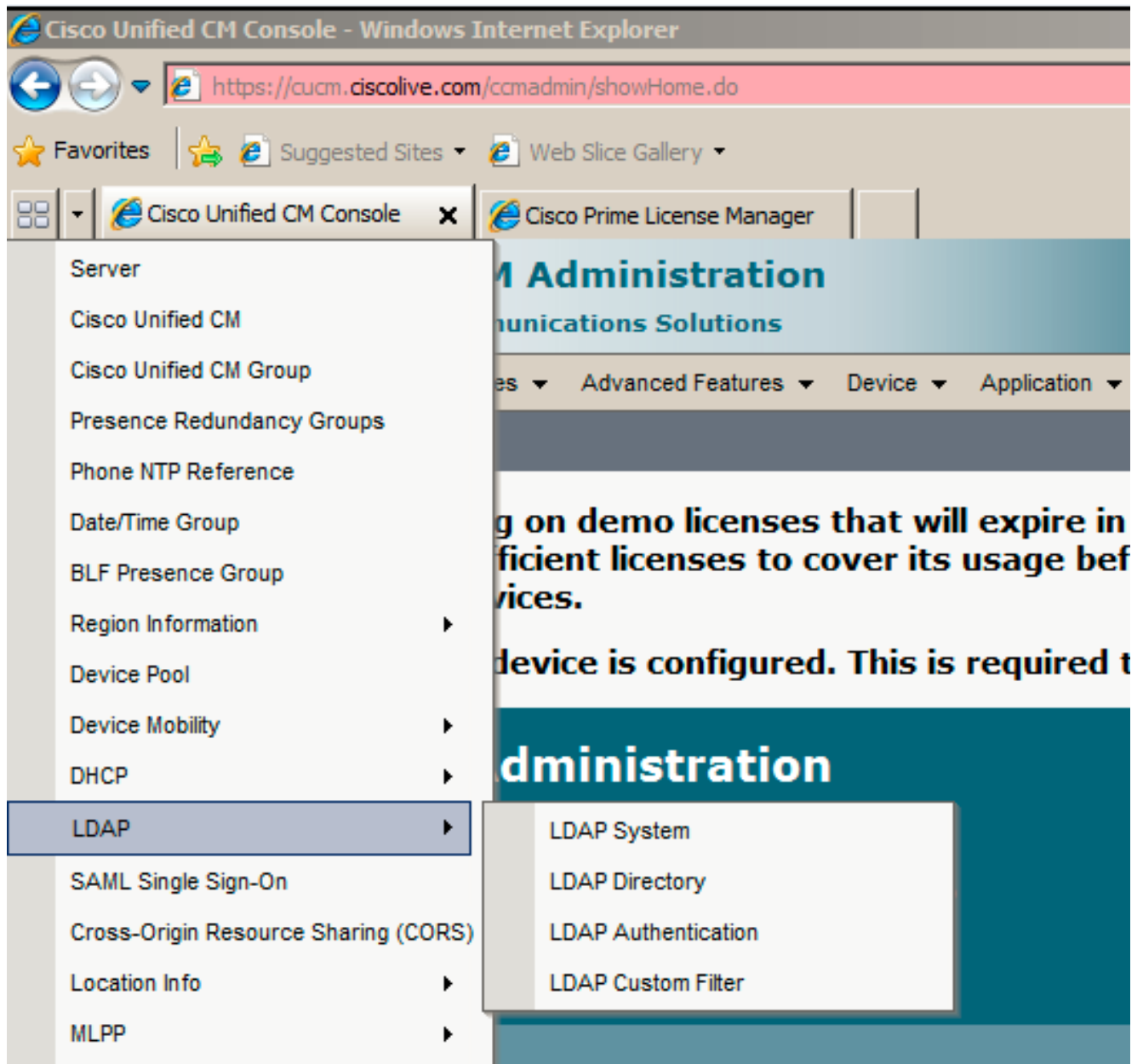


Figure :SAML Single sign SSO Call Flow for Collaboration Servers


Verzeichniseinrichtung

1. Wählen Sie Cisco Unified CM Administration > System > LDAP > LDAP System aus.




2. Klicken Sie auf **Neu hinzufügen**.
3. Servertyp und -attribut für das Lightweight Directory Access Protocol (LDAP) konfiguriert.
4. Wählen Sie **Synchronisierung vom LDAP-Server aktivieren** aus.

LDAP System Configuration

 Save

Status

 Status: Ready

LDAP System Information

Enable Synchronizing from LDAP Server

LDAP Server Type






LDAP Attribute for User ID

5. Wählen Sie **Cisco Unified CM Administration > System > LDAP > LDAP Directory** aus.


6. Konfigurieren Sie diese Elemente:

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

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

Tipp: Wenn Sie LDAP über SSL konfigurieren möchten, laden Sie das LDAP-Verzeichniszertifikat auf CUCM hoch. Informationen zum Synchronisierungsmechanismus für

bestimmte LDAP-Produkte und allgemeine Best Practices für die LDAP-Synchronisierung finden Sie im LDAP-Verzeichnisinhalt in [Cisco Unified Communications Manager SRND](#).

8. Klicken Sie auf **Speichern** und **führen Sie die vollständige Synchronisierung jetzt aus**. **Hinweis:** Vergewissern Sie sich, dass der **Cisco DirSync-Dienst** auf der Webseite Serviceability aktiviert ist, bevor Sie auf Save (Speichern) klicken.

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*:** adfs1.ciscolive.com
- LDAP Port*:** 3268
- Use SSL:**
- Buttons:** Add Another Redundant LDAP Server, Save, Delete, Copy, Perform Full Sync Now, Add New

9. Navigieren Sie zu **Benutzerverwaltung > Endbenutzer**, und wählen Sie einen Benutzer aus, dem Sie die CUCM-Verwaltungsrolle zuweisen möchten (in diesem Beispiel wird **SSO** für Benutzer ausgewählt).

The screenshot shows the 'Find and List Users' interface. It includes a navigation menu at the top, a search bar, and a table of users.

Status: 3 records found

User ID	First Name	Last Name	Department	Directory URI	User Status
ss0	Saml	SSO			Active LDAP Synchronized User
user2	User	2			Active LDAP Synchronized User

10. Blättern Sie nach unten zu den Berechtigungsinformationen, und klicken Sie auf **Zu Zugriffskontrollgruppe hinzufügen**. Wählen Sie **Standard CCM Super Users** aus, klicken Sie auf **Auswahl hinzufügen**, und klicken Sie auf **Speichern**.

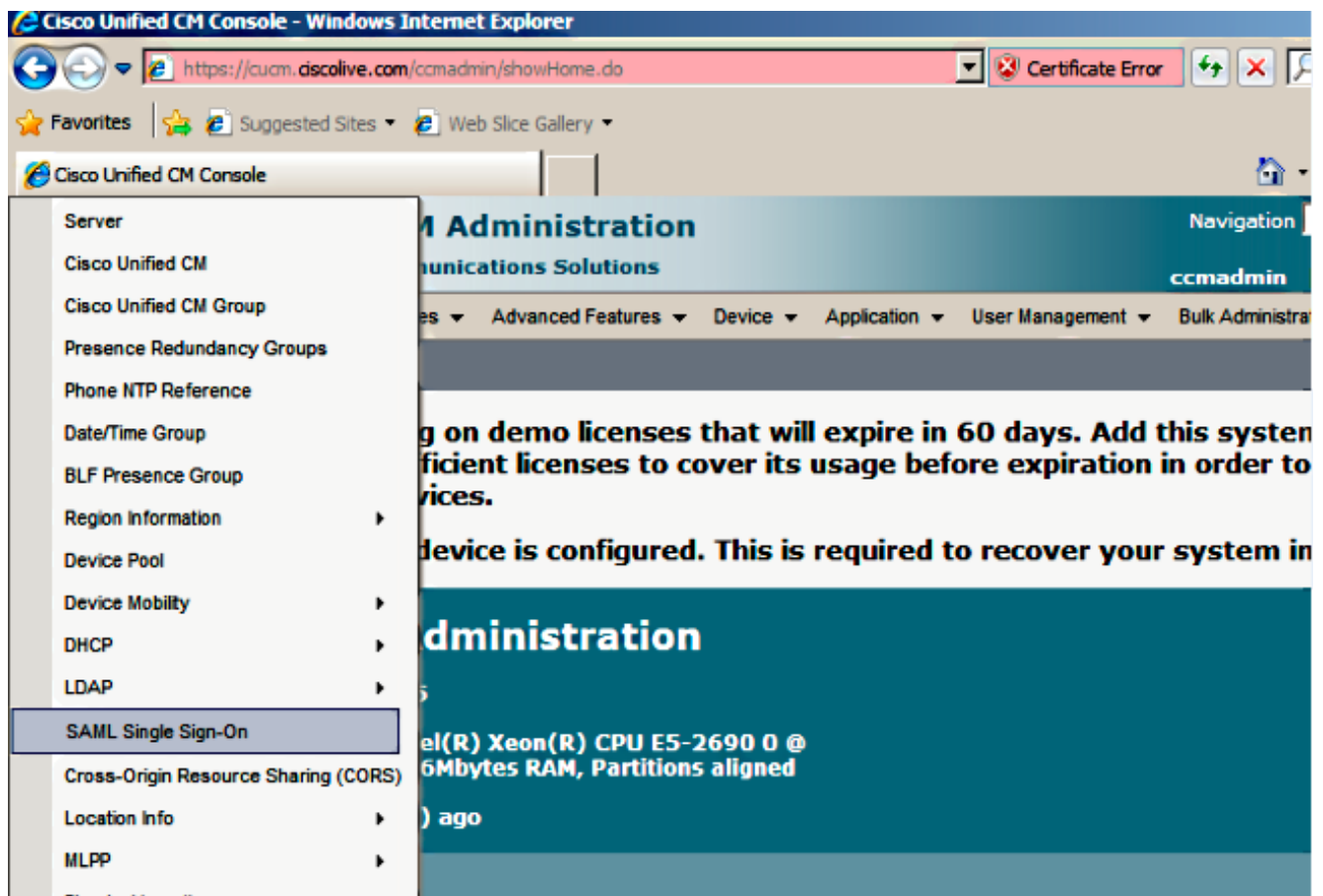
The screenshot shows the 'Permissions Information' configuration page. It includes the following elements:

- Groups:** Standard CCM Super Users
- Roles:** Standard AXL API Access, Standard Admin Rep Tool Admin, Standard CCM Admin Users, Standard CCMADMIN Administration, Standard CUReporting
- Buttons:** Add to Access Control Group, Remove from Access Control Group, View Details (for Groups and Roles), Save, Delete, Add New

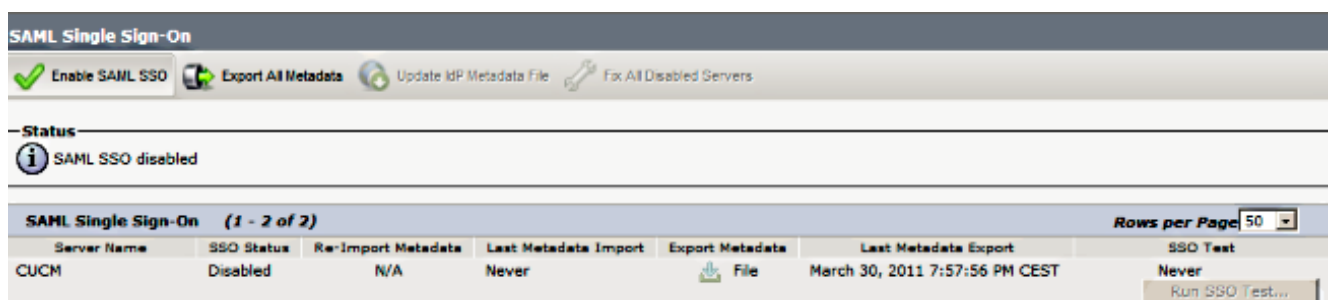
SAML SSO aktivieren

1. Melden Sie sich bei der Benutzeroberfläche der CUCM-Verwaltung an.

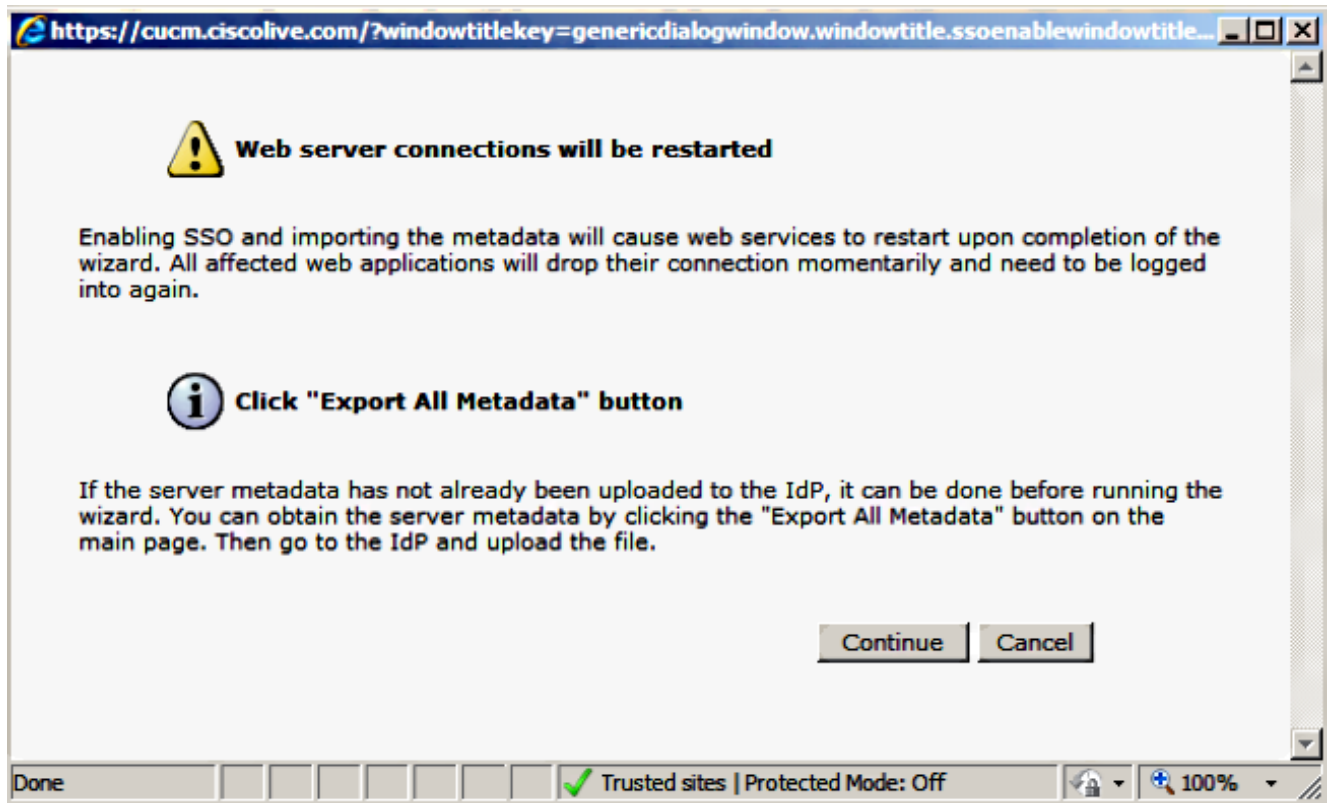
2. Wählen Sie **System > SAML Single Sign-On**, und das Fenster SAML Single Sign-On Configuration wird geöffnet.



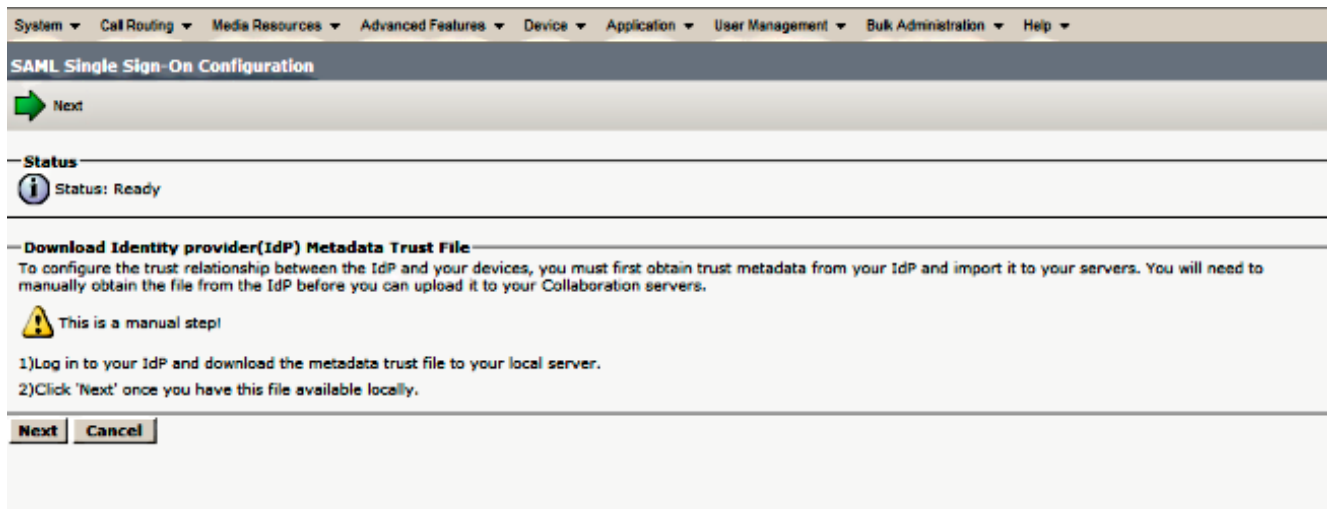
3. Um die SAML-SSO für den Cluster zu aktivieren, klicken Sie auf **SAML-SSO aktivieren**.



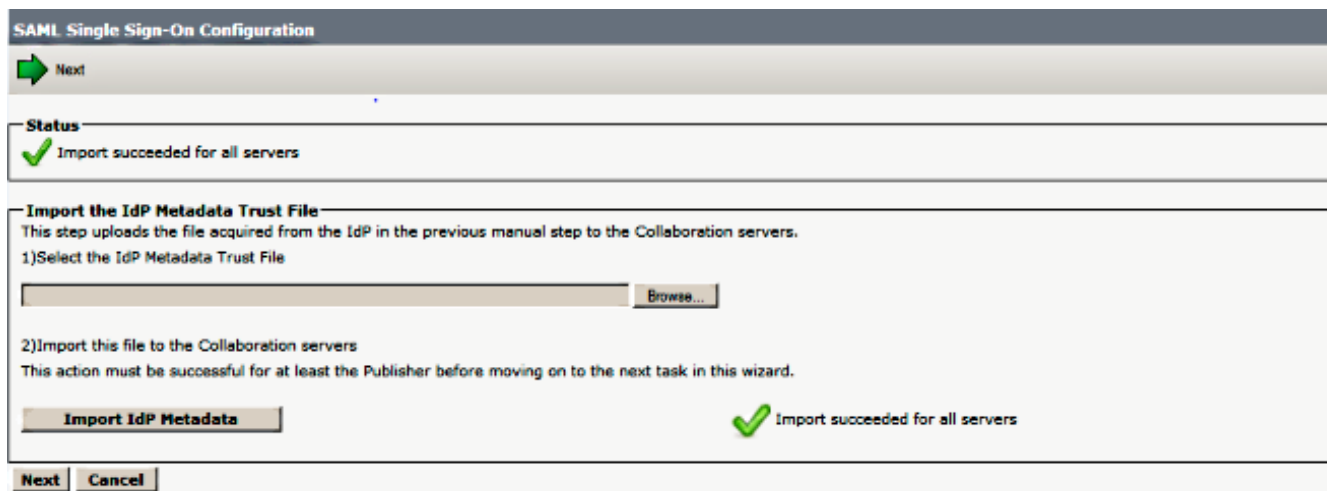
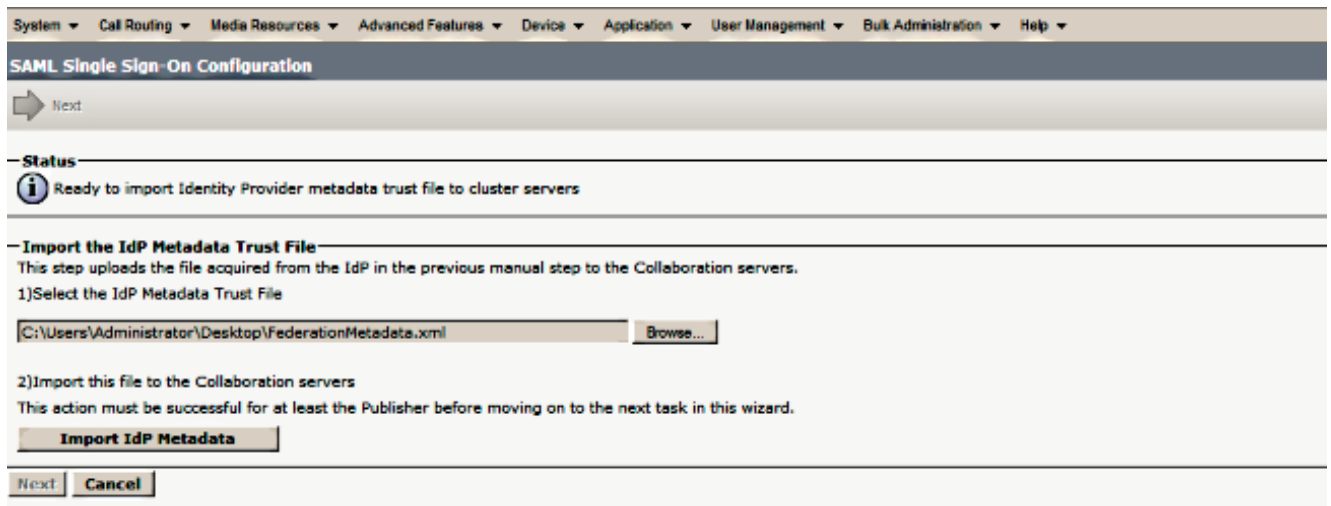
4. Klicken Sie im Fenster Warnung zurücksetzen auf **Weiter**.



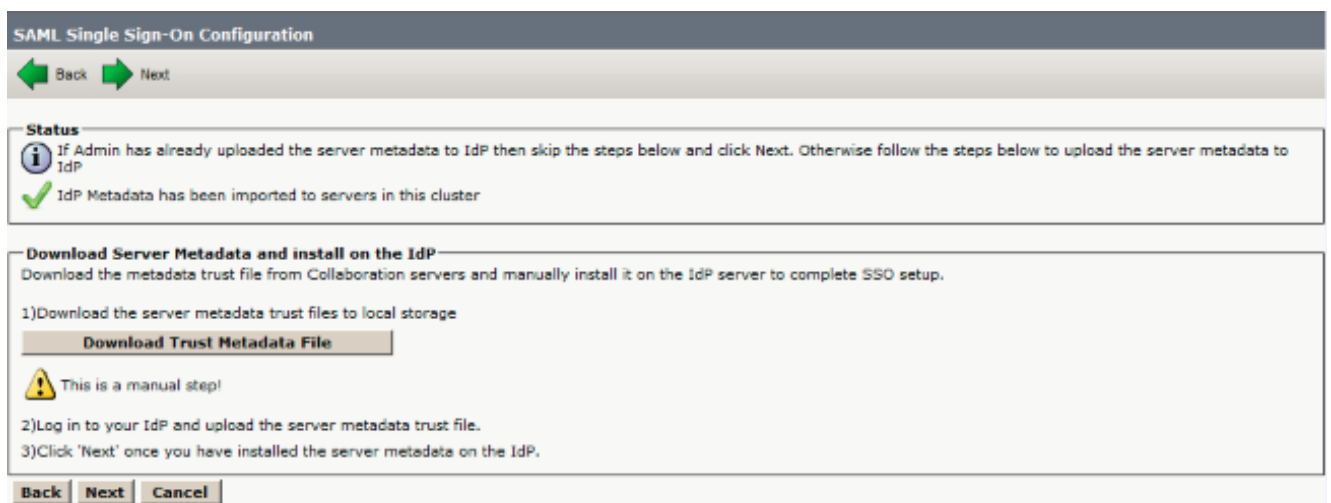
5. Klicken Sie auf dem SSO-Bildschirm auf **Durchsuchen**, um die XML-Datei IDP (**FederationMetadata.xml**)-Metadaten mit dem Schritt **IdP-Metadaten** zu importieren.



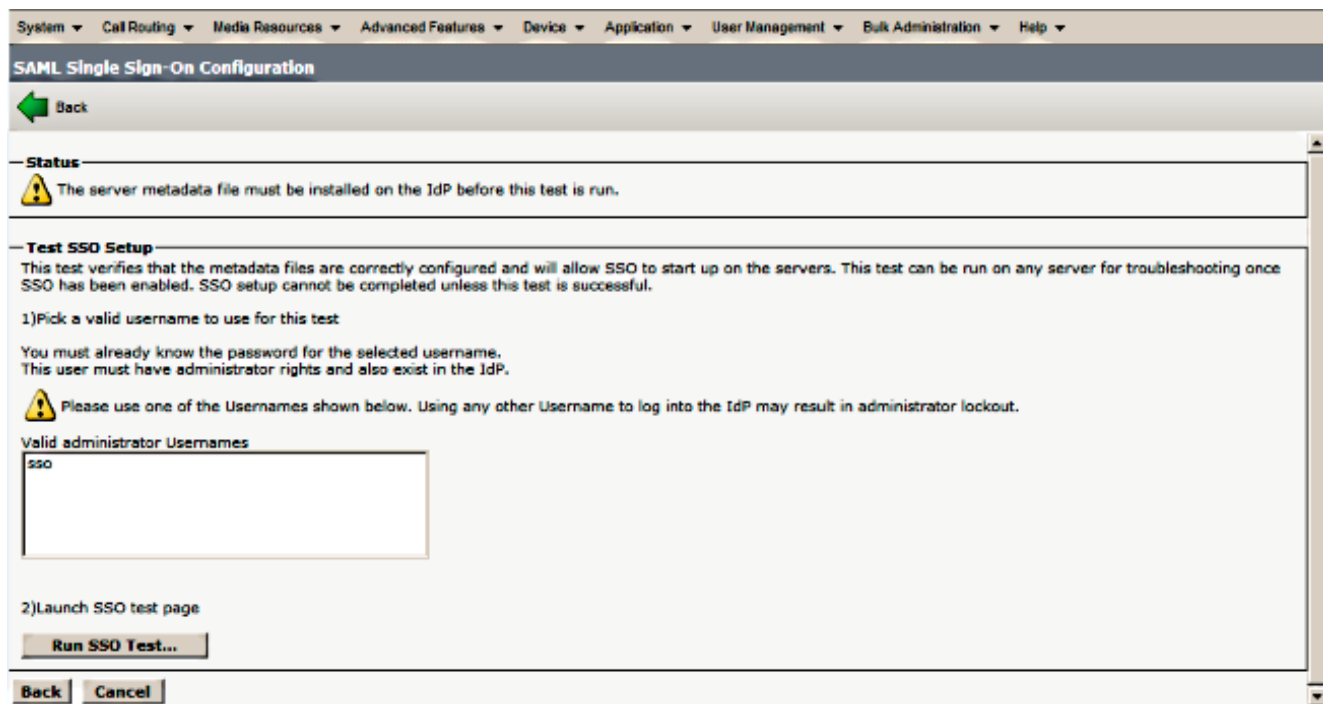
6. Klicken Sie nach dem Hochladen der Metadattendatei auf **IDP-Metadaten importieren**, um die IDP-Informationen in CUCM zu importieren. Bestätigen Sie, dass der Import erfolgreich war, und klicken Sie auf **Weiter**, um fortzufahren.



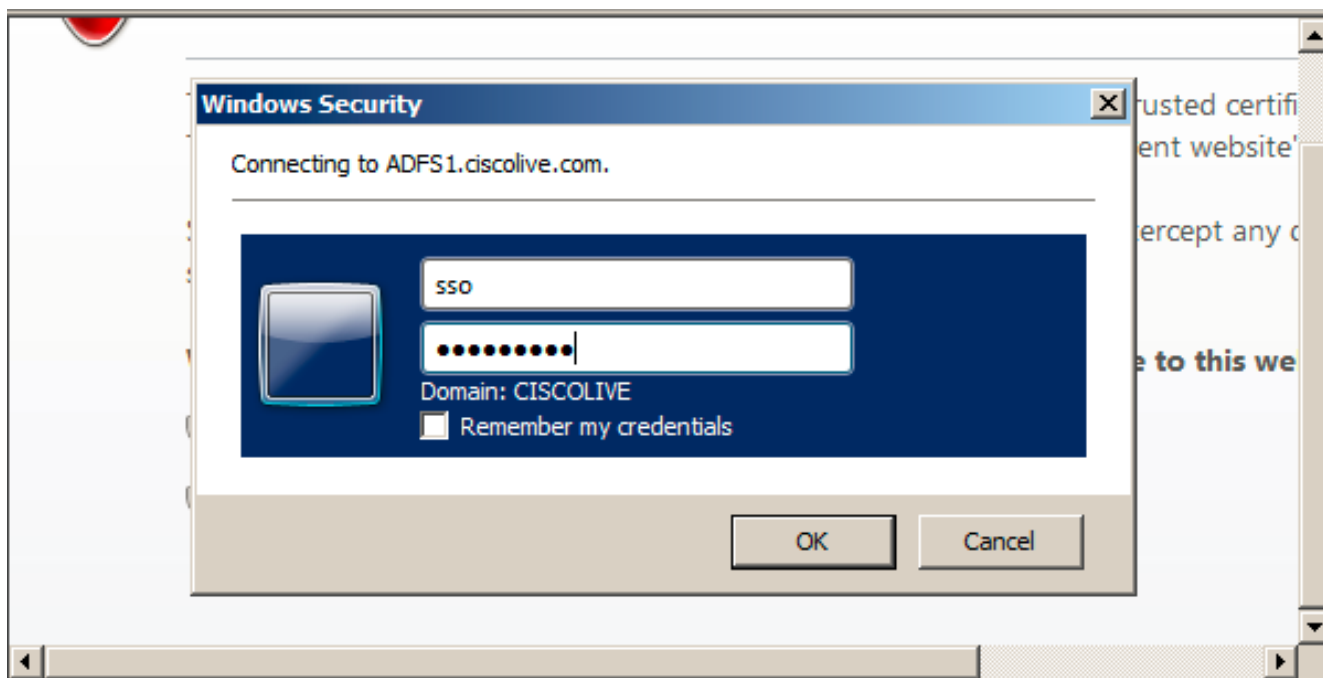
7. Klicken Sie auf **Trust Metadata File herunterladen** (optional), um die CUCM- und CUCM IM- und Presence-Metadaten in einem lokalen Ordner zu speichern, und gehen Sie zu [Add CUCM as Relying Party Trust](#). Wenn die AD FS-Konfiguration abgeschlossen ist, fahren Sie mit Schritt 8 fort.



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

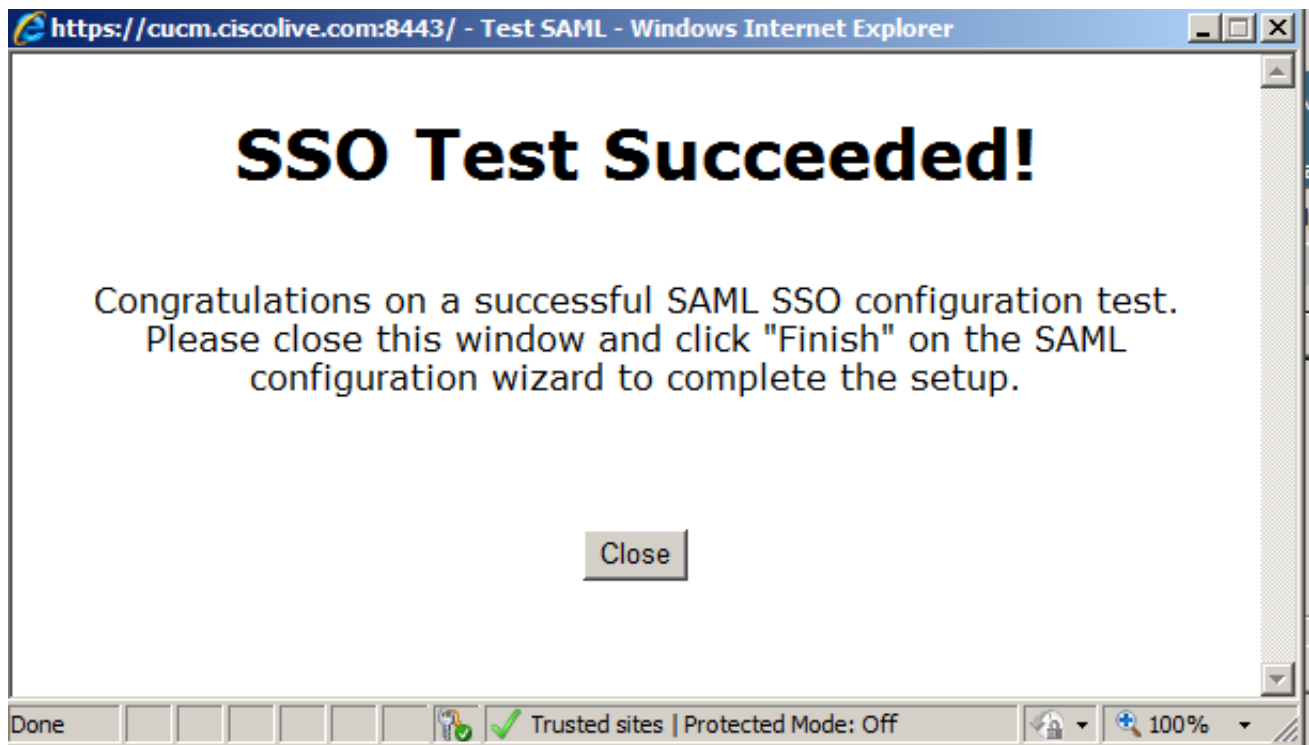


9. Zertifikatswarnungen ignorieren und weiter fortfahren Wenn Sie zur Eingabe der Anmeldeinformationen aufgefordert werden, geben Sie den Benutzernamen und das Kennwort für die Benutzer-SSO ein und klicken Sie auf OK.



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

10. Nach Abschluss aller Schritte wurde der SSO-Test erfolgreich durchgeführt. wird angezeigt. Klicken Sie auf **Schließen** und **Beenden**, um fortzufahren. Sie haben nun die Konfigurationsaufgaben erfolgreich abgeschlossen, um SSO auf CUCM mit AD FS zu aktivieren.



11. Da CUCM IM und Presence wie der CUCM-Subscriber agieren, müssen Sie [CUCM IM und Presence als Relying Party Trust](#) konfigurieren und anschließend **SSO-Test ausführen**, um SAML SSO von der CUCM SAML-SSO-Seite selbst zu aktivieren.

Hinweis: Wenn Sie alle XML-Metadaten-Dateien aller Knoten auf IdP konfigurieren und die SSO-Operation auf einem Knoten aktivieren, ist die SAML SSO auf allen Knoten im Cluster aktiviert.

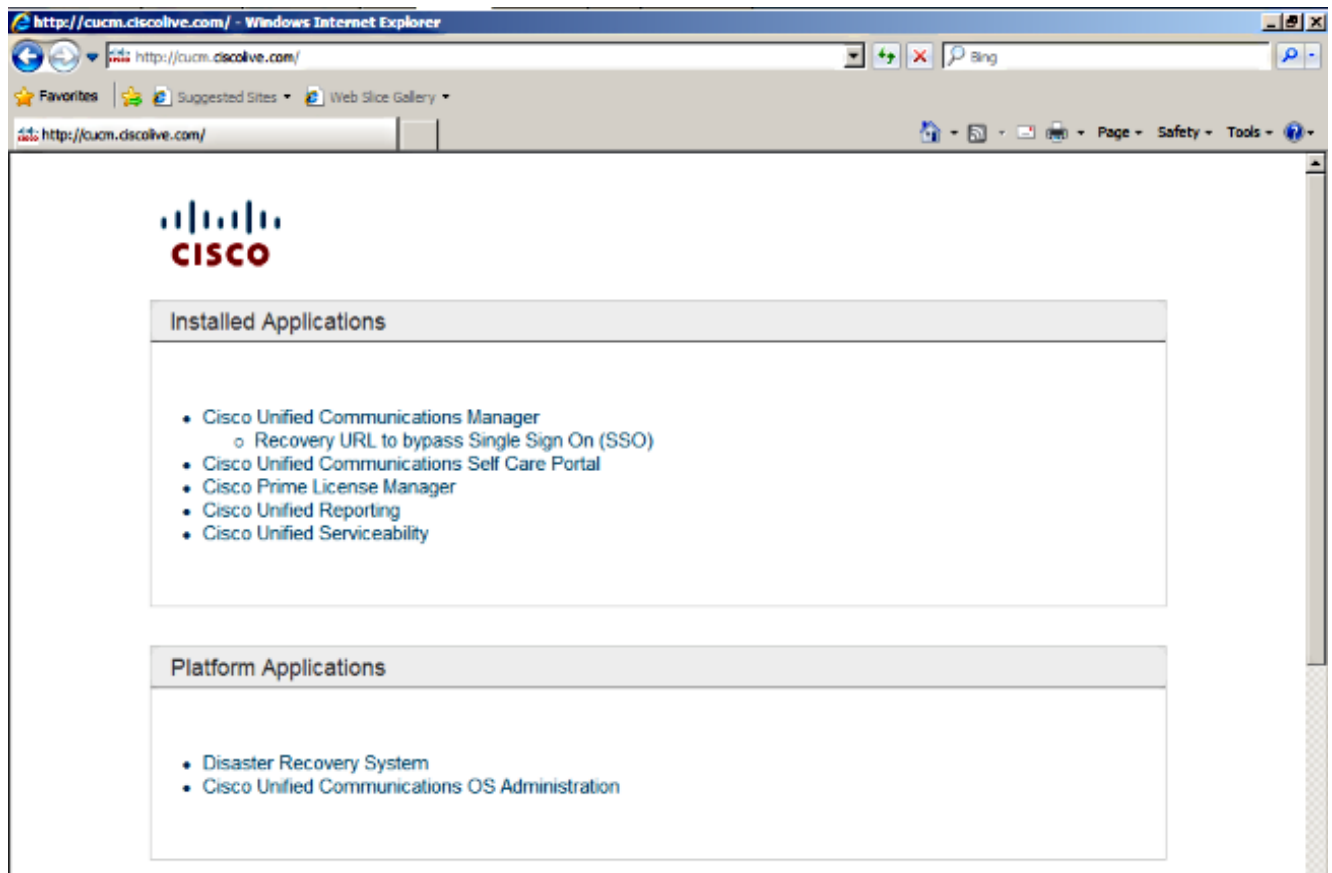
AD FS muss für alle Knoten von CUCM und CUCM IM und Presence in einem Cluster als Relay Party (Weiterleitungsgruppe) konfiguriert werden.

Tipp: Sie sollten auch Cisco Unity Connection und CUCM IM and Presence für SAML SSO konfigurieren, wenn Sie die SAML SSO-Erfahrung für Cisco Jabber-Clients verwenden möchten.

Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

1. Öffnen Sie einen Webbrowser, und geben Sie den FQDN für CUCM ein.
2. Klicken Sie auf **Cisco Unified Communications Manager**.
3. Wählen Sie die Webanwendung (**CM Administration/Unified Serviceability/Cisco Unified Reporting**) aus, und drücken Sie **Go**, um vom AD FS zur Eingabe der Anmeldeinformationen aufgefordert zu werden. Sobald Sie die Anmeldeinformationen des Benutzers **SSO** eingegeben haben, werden Sie erfolgreich bei der ausgewählten Webanwendung angemeldet (**CM Administration-Seite, Unified Serviceability-Seite, Cisco Unified Reporting**).



Hinweis: SAML SSO ermöglicht keinen Zugriff auf folgende Seiten:

- Prime Licensing Manager
- Betriebssystemverwaltung
- Disaster Recovery System

Fehlerbehebung

Wenn Sie SAML nicht aktivieren können und sich nicht anmelden können, verwenden Sie die neue Option unter Installierte Anwendungen mit dem Namen **Recovery URL, um Single Sign-on (SSO)** zu umgehen, die verwendet werden kann, um sich mit den Anmeldeinformationen anzumelden, die während der Installation erstellt wurden, oder mit lokal erstellten CUCM Administrative Benutzern.

Cisco Unified CM Console - Windows Internet Explorer

https://cuom.dscolive.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

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.

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