

統一通訊管理器10.5版SAML SSO配置示例

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[網路時間協定\(NTP\)設定](#)

[域名伺服器\(DNS\)安裝程式](#)

[採用元件](#)

[背景資訊](#)

[設定](#)

[網路圖表](#)

[目錄設定](#)

[啟用SAML SSO](#)

[驗證](#)

[疑難排解](#)

簡介

本檔案介紹如何設定和驗證思科整合通訊管理員(CUCM)的安全宣告標籤語言(SAML)單一登入(SSO)。

必要條件

需求

網路時間協定(NTP)設定

要使SAML SSO正常工作，必須安裝正確的NTP設定，並確保身份提供程式(IdP)和統一通訊應用程式之間的時間差不超過三秒。

如果CUCM和IdP之間存在時間不匹配，您將收到以下錯誤："無效SAML響應。" 當CUCM和IdP伺服器之間的時間不同步時，可能導致此錯誤。要使SAML SSO正常工作，必須安裝正確的NTP設定，並確保IdP和統一通訊應用程式之間的時間差不超過三秒。

有關如何同步時鐘的資訊，請參閱[Cisco Unified Communications作業系統管理指南](#)中的NTP設定部分。

域名伺服器(DNS)安裝程式

統一通訊應用程式可以使用DNS將完全限定域名(FQDN)解析為IP地址。服務提供商和IdP必須由瀏覽器解析。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 作為IdP的Active Directory聯合身份驗證服務(AD FS)版本2.0
- 作為服務提供商的CUCM 10.5版
- Microsoft Internet Explorer 10

注意：本文檔基於新安裝的CUCM。如果在已投入生產的伺服器上配置SAML SSO，則可能必須相應地跳過某些步驟。在生產伺服器上執行這些步驟時，還必須瞭解服務影響。建議在非工作時間執行此過程。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

背景資訊

SAML是基於XML的開放式標準資料格式，使管理員能夠在登入到其中某個應用後，無縫訪問一組已定義的思科合作應用。SAML SSO在作為IdP與服務提供商之間的調配過程的一部分交換後設資料時建立信任圈(CoT)。服務提供商信任IdP的使用者資訊以提供對各種服務或應用的訪問。

附註：服務提供商不再參與身份驗證。SAML 2.0版將身份驗證從服務提供商處委託給IdP。客戶端根據IdP進行身份驗證，IdP向客戶端授予斷言。客戶端向服務提供商顯示斷言。由於已建立CoT，因此服務提供商信任宣告並授予對客戶端的訪問許可權。

設定

網路圖表

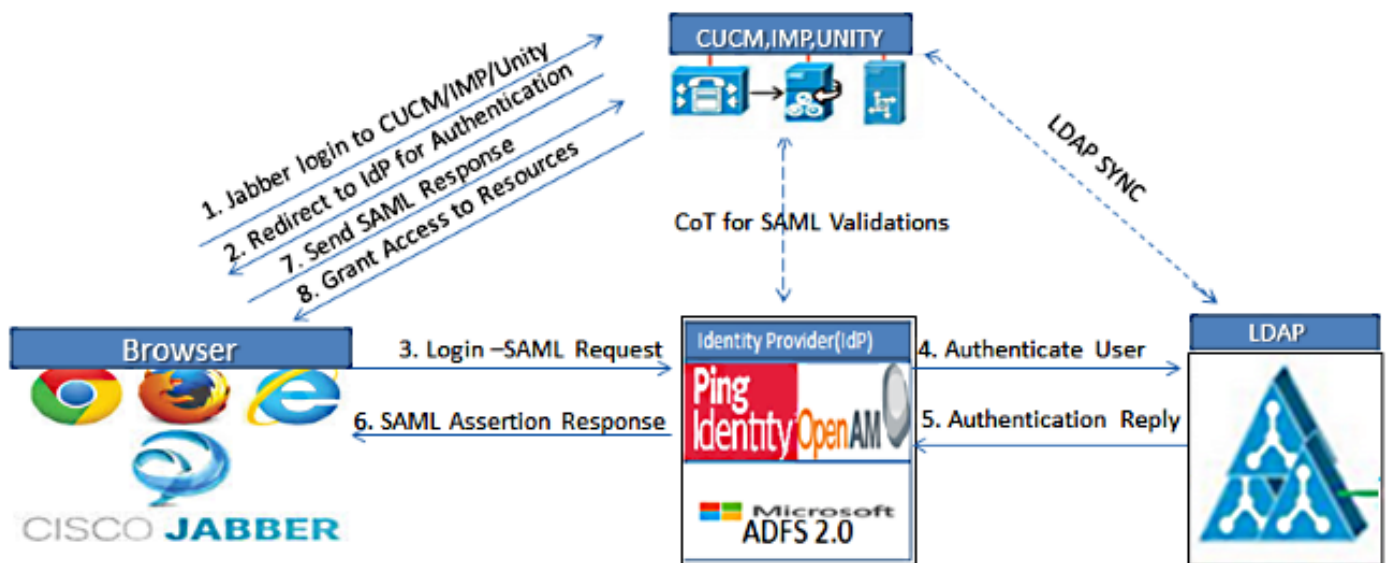
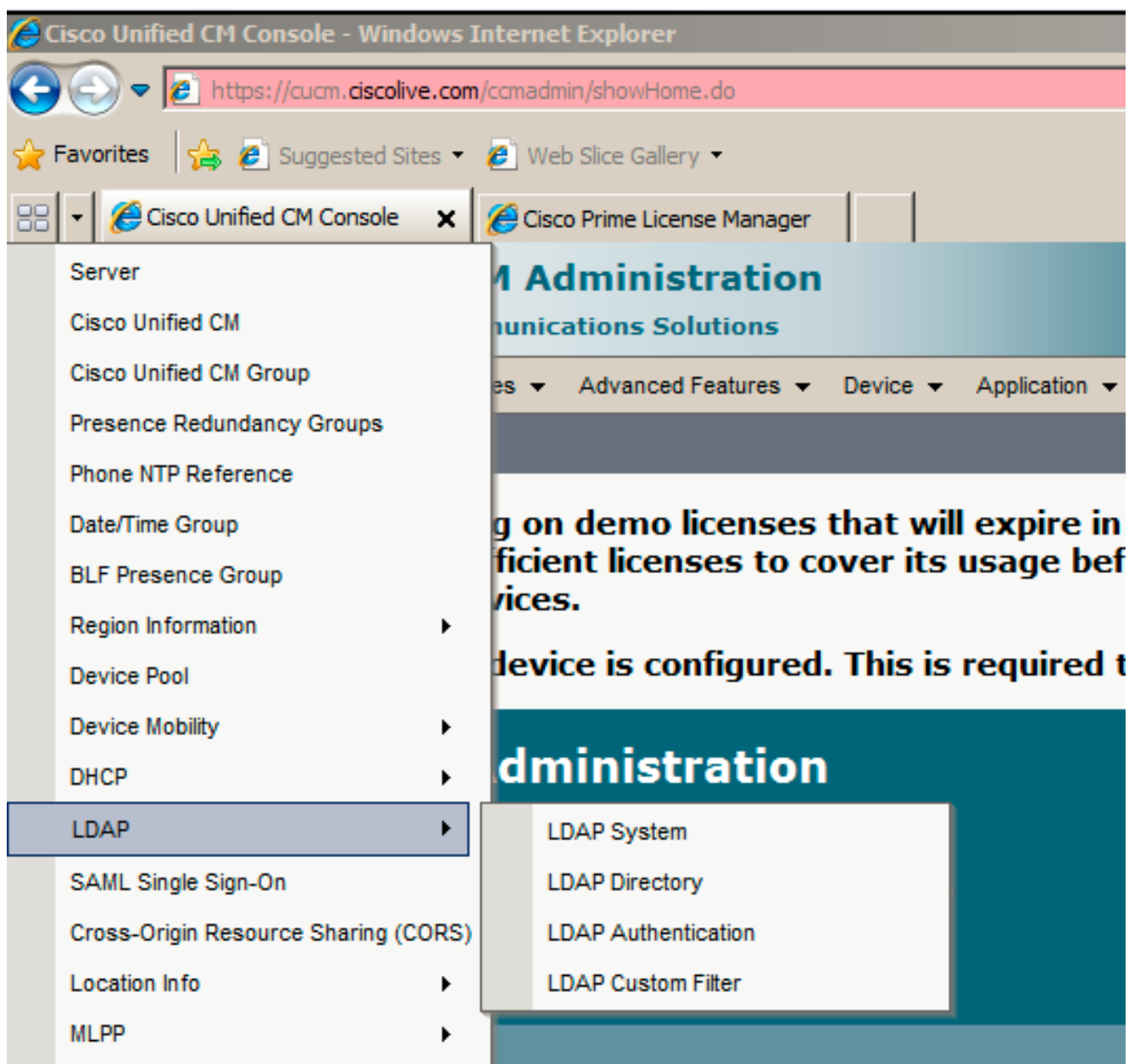


Figure :SAML Single sign SSO Call Flow for Collaboration Servers


目錄設定

1. 選擇Cisco Unified CM Administration > System > LDAP > LDAP System。




2. 按一下「Add New」。
3. 配置輕量型目錄訪問協定(LDAP)伺服器型別和屬性。
4. 選擇Enable Synchronizing from LDAP Server。

LDAP System Configuration

 Save

Status

 Status: Ready

LDAP System Information

Enable Synchronizing from LDAP Server

LDAP Server Type






LDAP Attribute for User ID

5. 選擇Cisco Unified CM Administration > System > LDAP > LDAP Directory。


6. 配置以下專案：

LDAP目錄帳戶設定要同步的使用者屬性同步計畫LDAP伺服器主機名或IP地址和埠號

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*

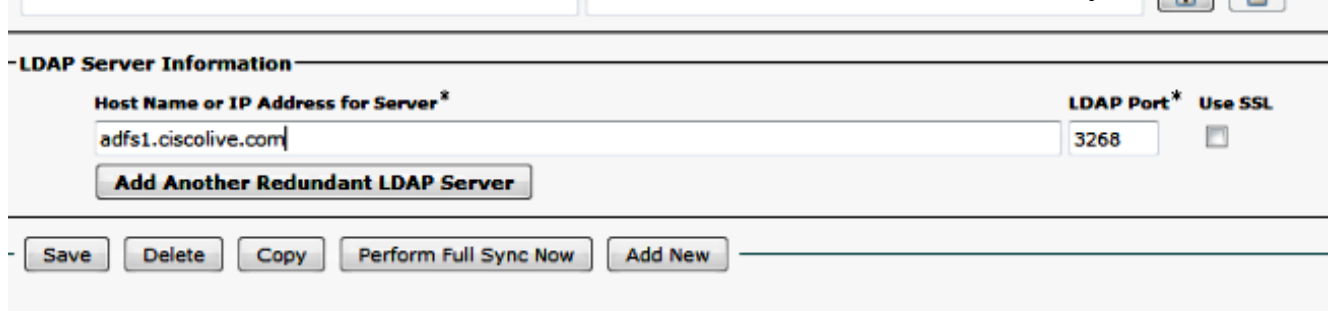
LDAP Custom Filter

7. 如果不想使用安全套接字層(SSL)與LDAP目錄通訊，請取消選中**使用SSL**。

提示：如果要通過SSL配置LDAP，請將LDAP目錄證書上傳到CUCM。有關特定LDAP產品的帳戶同步機制和LDAP同步的一般最佳實踐的資訊，請參閱[Cisco Unified Communications Manager SRND](#)中的LDAP目錄內容。

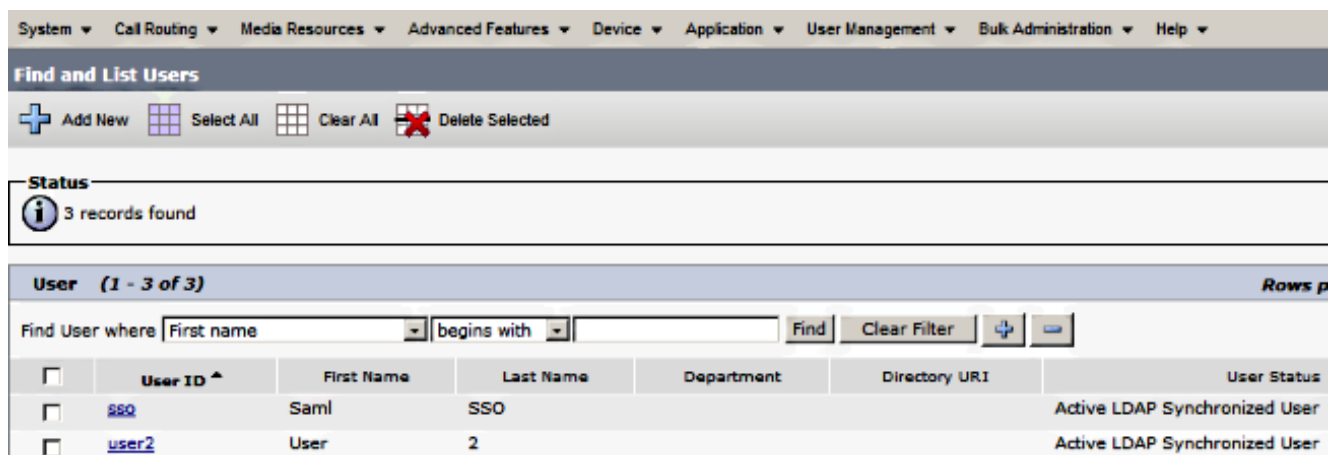
8. 按一下**Save**，然後按一下**Perform Full Sync Now**。

附註：按一下「儲存」之前，請確保在「可服務性」網頁中啟用了Cisco DirSync服務。



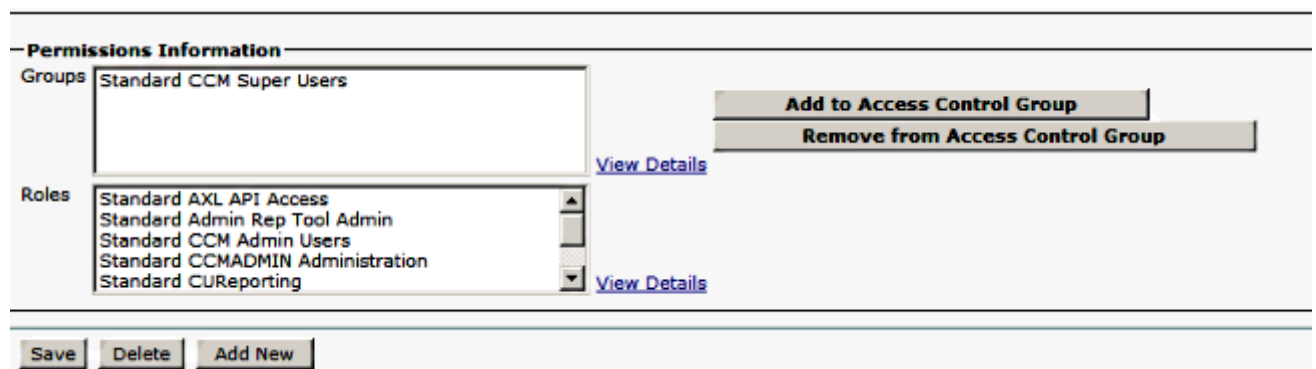
The screenshot shows the 'LDAP Server Information' configuration page. It includes a text input field for 'Host Name or IP Address for Server' containing 'adfs1.ciscolive.com', a 'LDAP Port' field with '3268', and a 'Use SSL' checkbox which is unchecked. Below these fields is a button labeled 'Add Another Redundant LDAP Server'. At the bottom of the page, there are five buttons: 'Save', 'Delete', 'Copy', 'Perform Full Sync Now', and 'Add New'.

9. 導航到User Management > End User，然後選擇要向其授予CUCM管理角色的使用者(此示例選擇使用者SSO)。



The screenshot displays the 'Find and List Users' interface. At the top, there are navigation tabs for System, Call Routing, Media Resources, Advanced Features, Device, Application, User Management, Bulk Administration, and Help. Below the tabs are action buttons: '+ Add New', 'Select All', 'Clear All', and 'Delete Selected'. A 'Status' section indicates '3 records found'. The main area is a table titled 'User (1 - 3 of 3)' with columns: User ID, First Name, Last Name, Department, Directory URI, and User Status. The table contains two rows: one for user 'ss0' (SamI SSO) and one for 'user2' (User 2). Both are 'Active LDAP Synchronized User'.

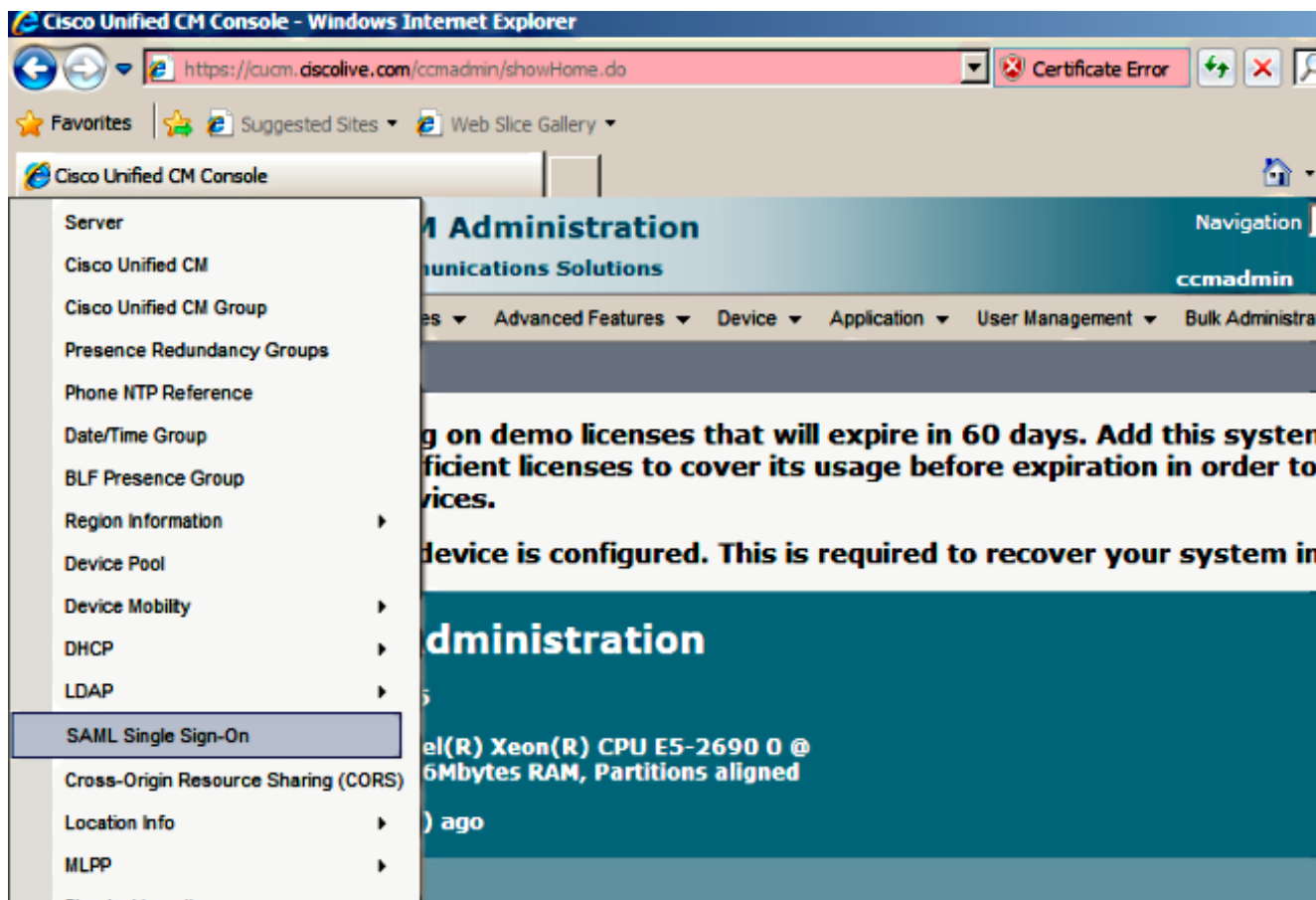
10. 向下滾動到「Permissions Information (許可權資訊)」，然後按一下「Add to Access Control Group (新增到訪問控制組)」。選擇標準CCM超級使用者，按一下Add Selected，然後按一下Save。



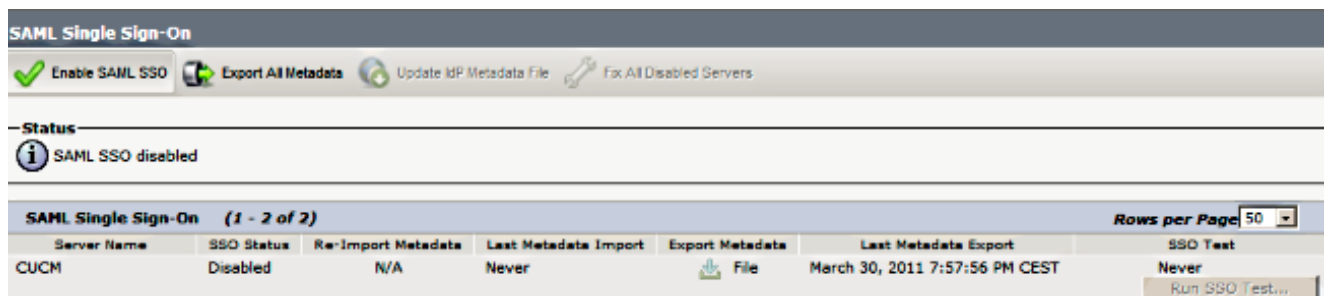
The screenshot shows the 'Permissions Information' configuration page. It features two list boxes: 'Groups' containing 'Standard CCM Super Users' and 'Roles' containing 'Standard AXL API Access', 'Standard Admin Rep Tool Admin', 'Standard CCM Admin Users', 'Standard CCMADMIN Administration', and 'Standard CUReporting'. To the right of the 'Groups' list are two buttons: 'Add to Access Control Group' and 'Remove from Access Control Group'. Below the 'Roles' list is a 'View Details' link. At the bottom, there are three buttons: 'Save', 'Delete', and 'Add New'.

啟用SAML SSO

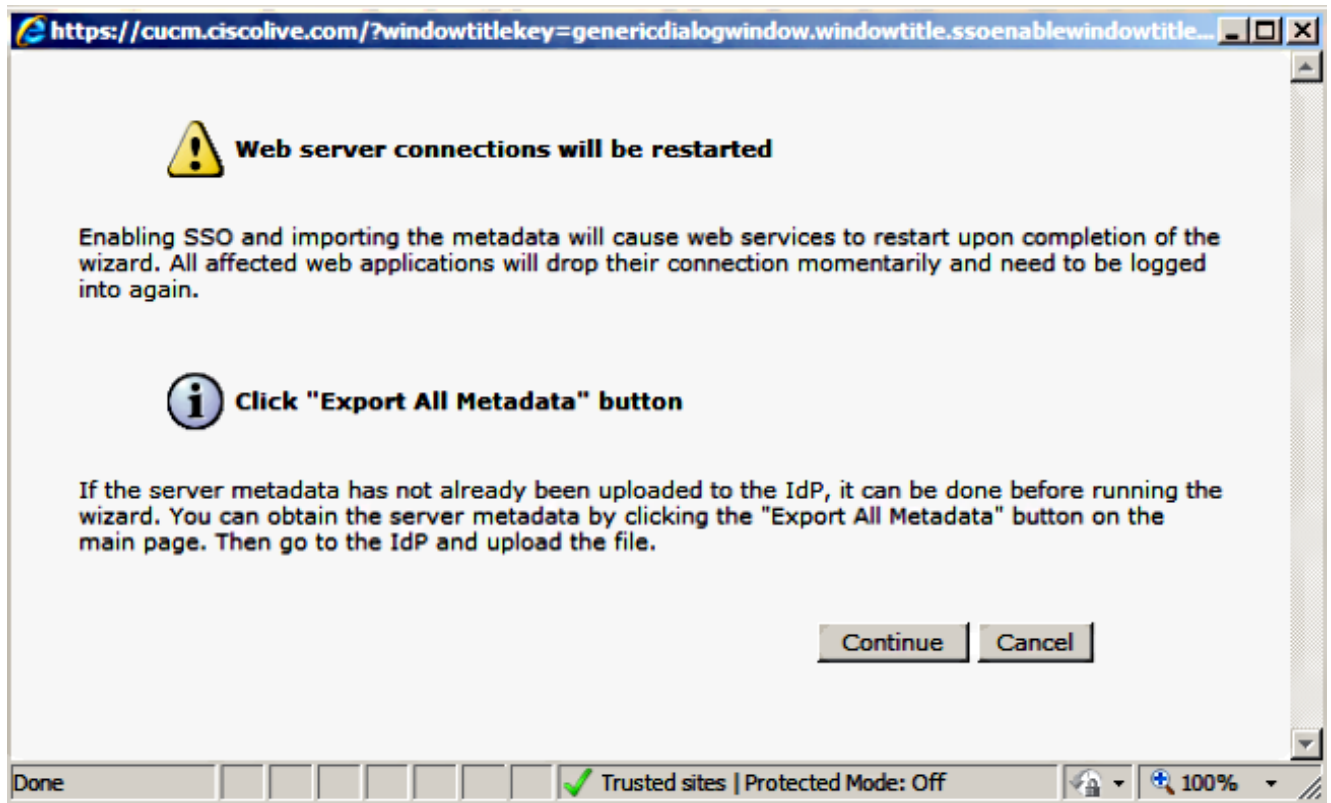
1. 登入到CUCM管理使用者介面。
2. 選擇System > SAML Single Sign-On，此時將開啟SAML Single Sign-On Configuration視窗。



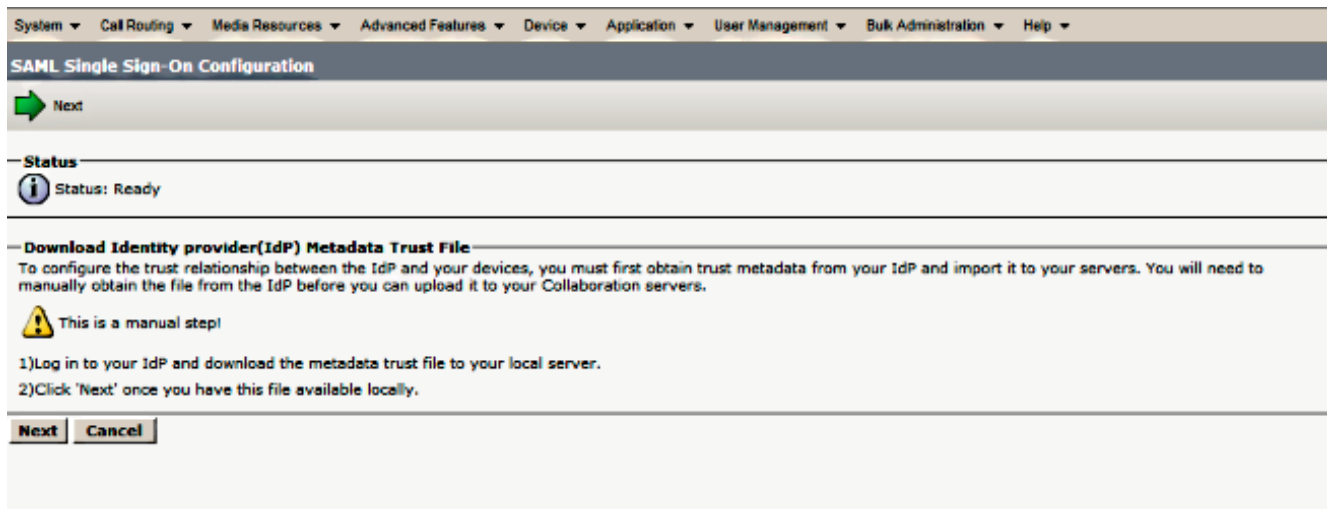
3. 要在群集中啟用SAML SSO，請按一下Enable SAML SSO。



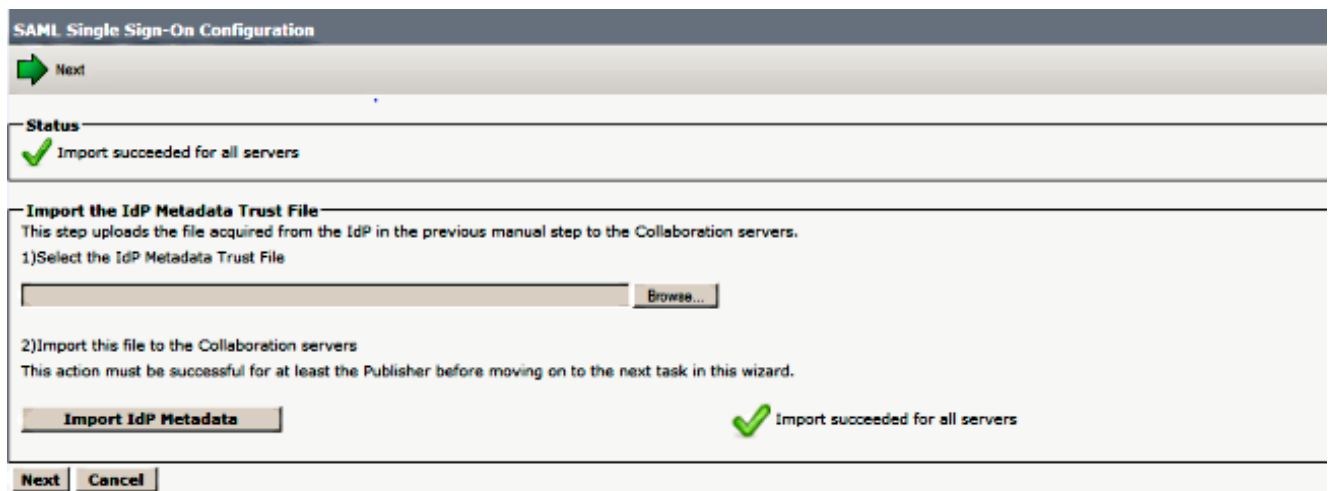
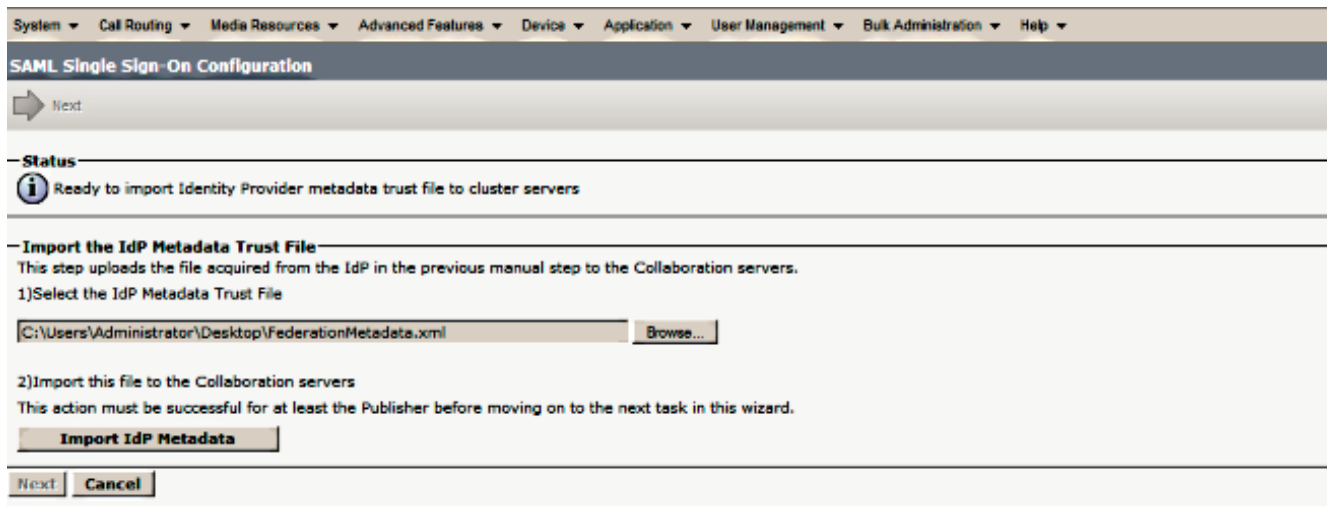
4. 在「重置警告」視窗中，按一下繼續。



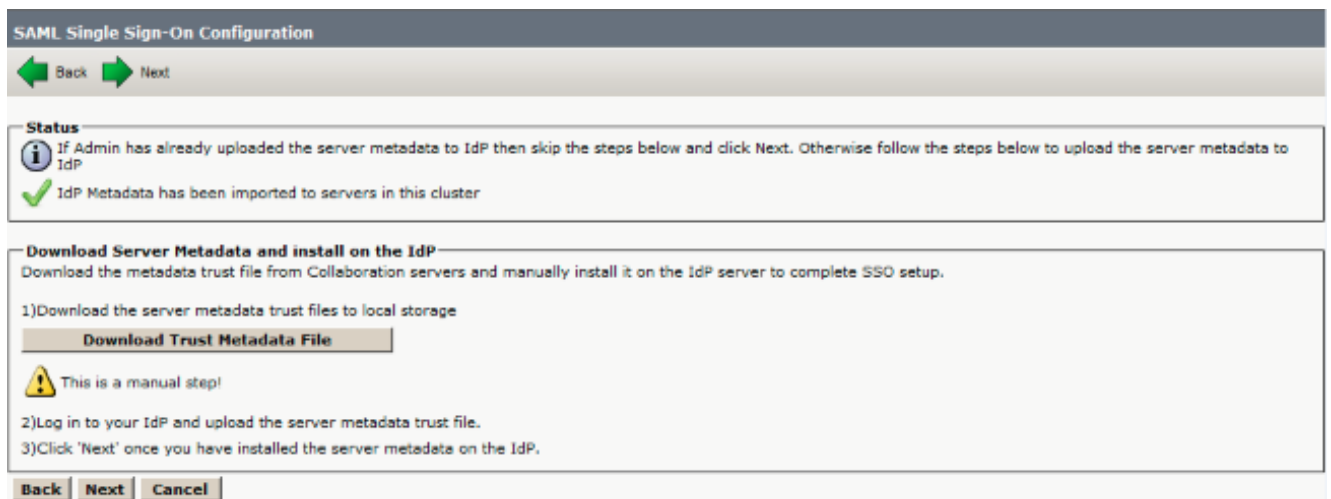
5. 在SSO螢幕上，按一下**Browse**，以使用**下載IdP後設資料**步驟匯入IdP(**FederationMetadata.xml**)後設資料XML檔案。



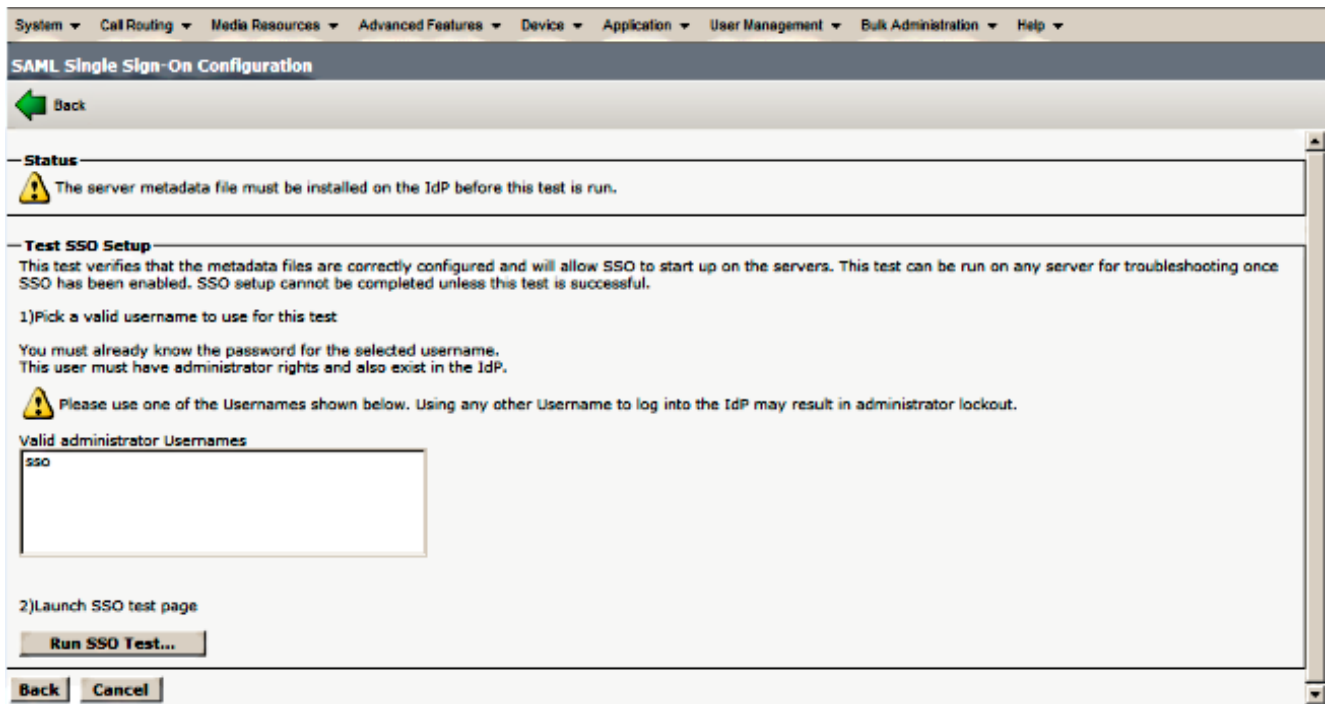
6. 上傳後設資料檔案後，按一下**Import IdP Metadata**以將IdP資訊匯入CUCM。確認匯入成功，然後按一下**下一步**以繼續。



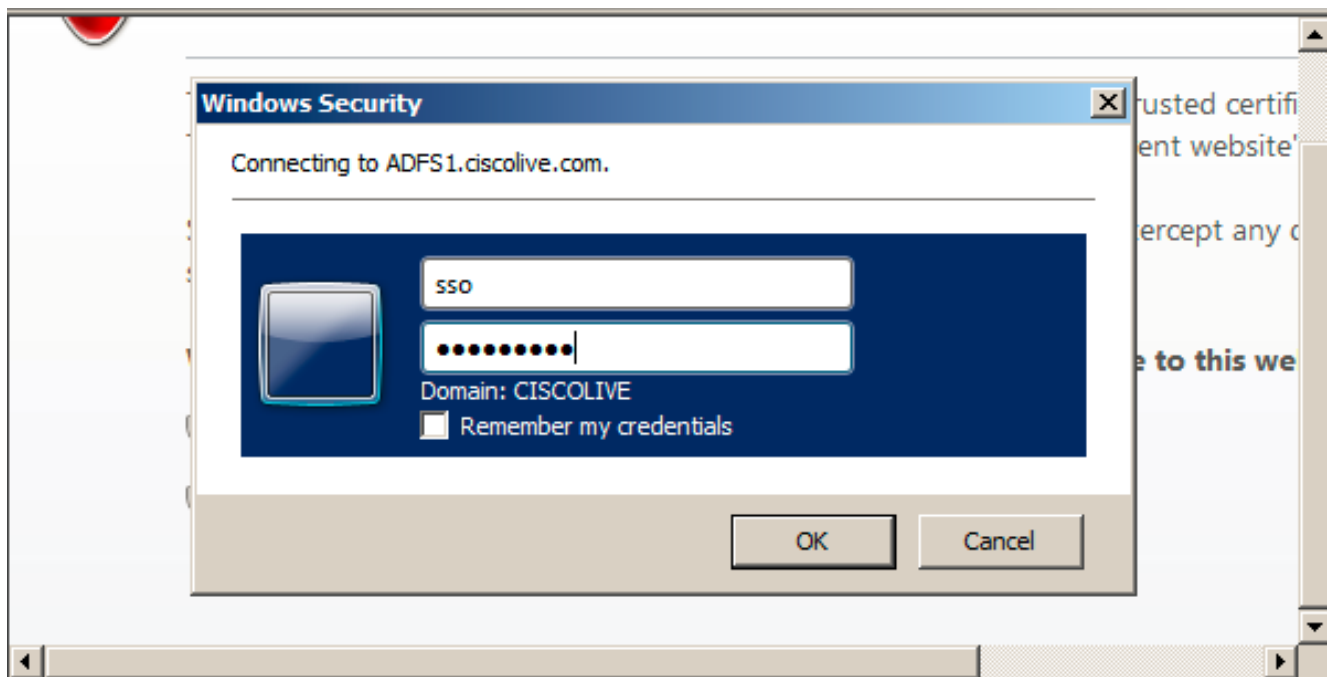
- 按一下 **Download Trust Metadata File** (可選)，將CUCM和CUCM IM and Presence後設資料儲存到本地資料夾，並轉至[Add CUCM as Relying Party Trust](#)。完成AD FS配置後，請繼續執行步驟8。



- 選擇SSO作為管理使用者，然後按一下**運行SSO測試**。

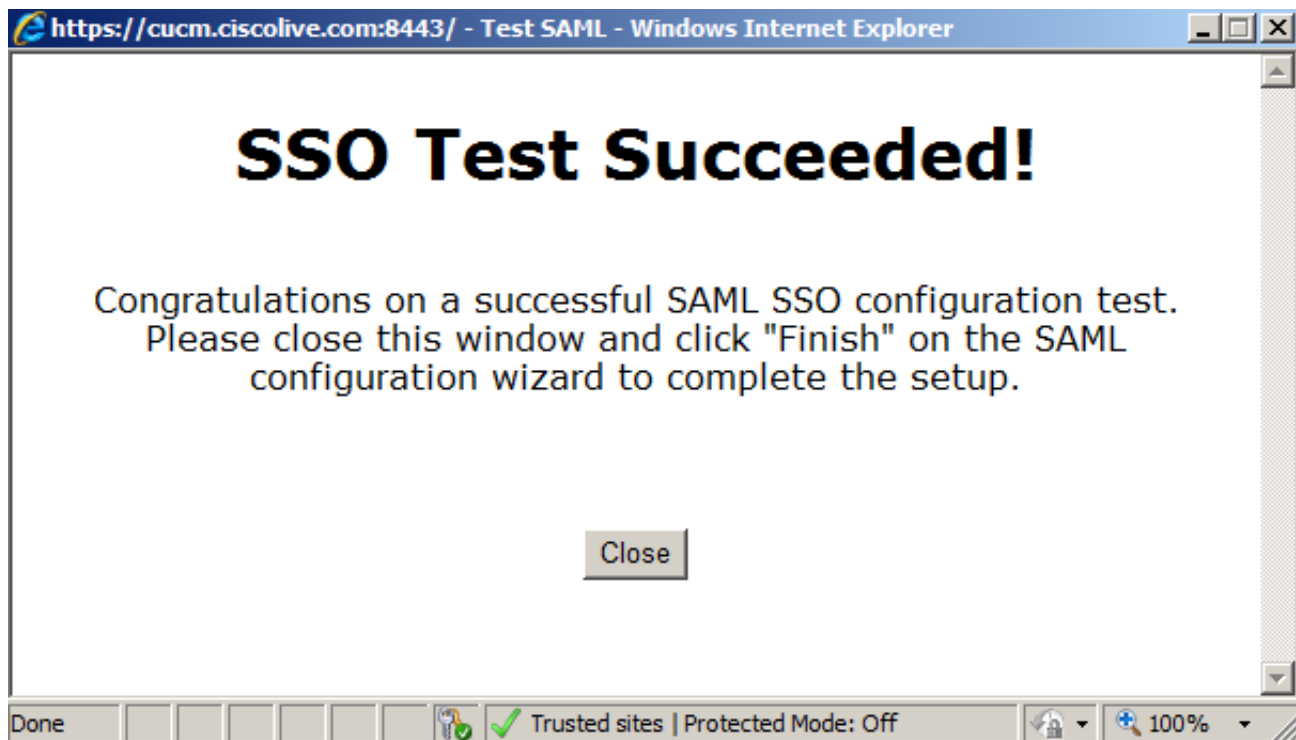


9. 忽略證書警告並繼續。當系統提示您輸入憑據時，請輸入使用者SSO的使用者名稱和密碼，然後按一下**確定**。



附註：此配置示例基於CUCM和AD FS自簽名證書。如果使用證書頒發機構(CA)證書，必須在AD FS和CUCM上安裝適當的證書。如需詳細資訊，請參閱[憑證管理和驗證](#)。

10. 完成所有步驟後，「SSO測試成功！」顯示消息。按一下**Close**和**Finish**以繼續。您現在已成功完成配置任務，以便在CUCM上啟用SSO with AD FS。



11. 由於CUCM IM and Presence與CUCM使用者類似，您必須將[Add CUCM IM and Presence as Relisting Party Trust](#)配置，然後運行Run SSO Test，以便從CUCM SAML SSO頁面本身啟用SAML SSO。

附註：如果在IdP上配置所有節點的后設資料XML檔案，並且在一個節點上啟用SSO操作，則集群中的所有節點上都會啟用SAML SSO。

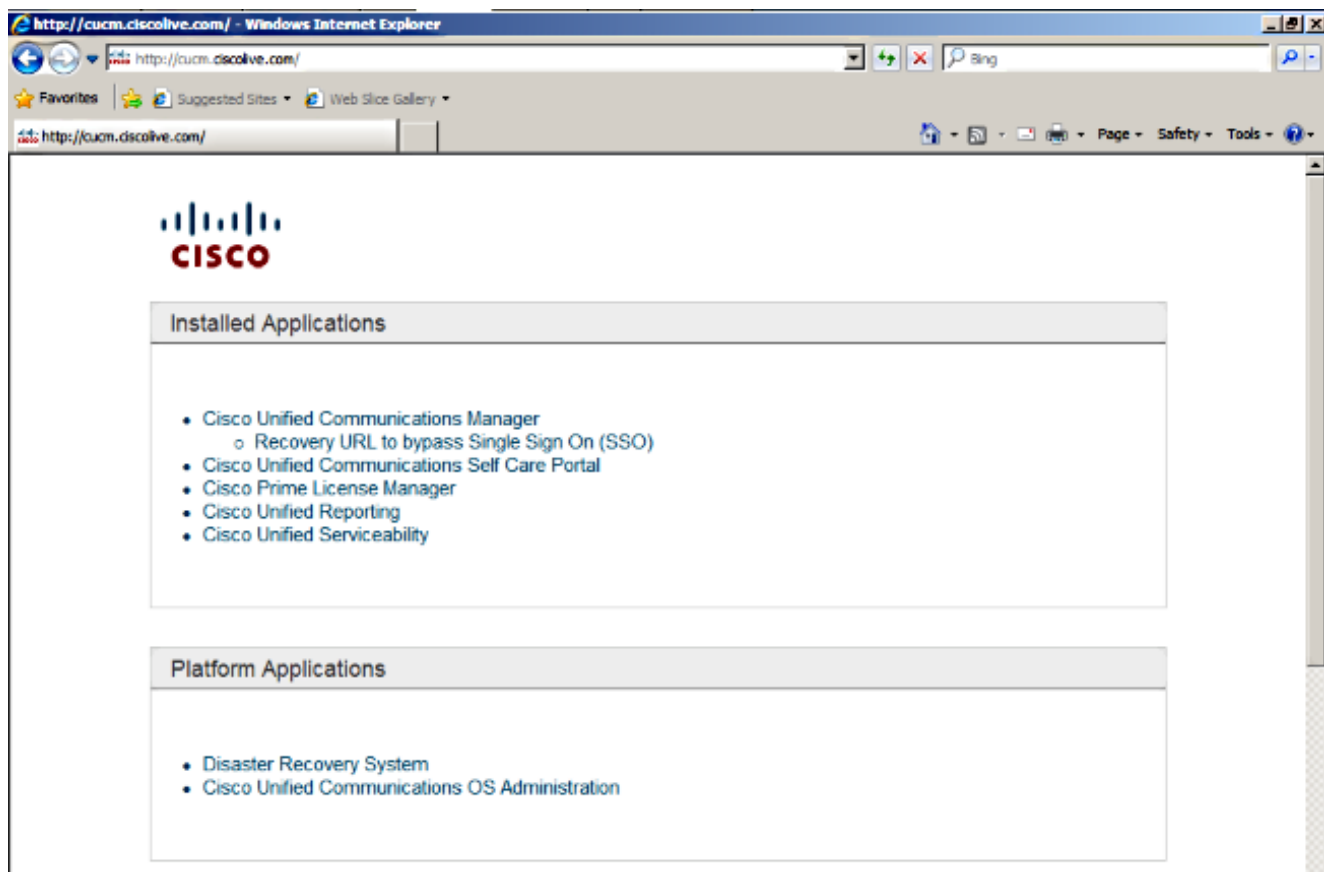
必須將群集中CUCM和CUCM IM and Presence的所有節點配置為中繼方。

提示：如果您希望對Cisco Jabber客戶端使用SAML SSO體驗，則還應配置Cisco Unity Connection以及CUCM IM and Presence for SAML SSO。

驗證

使用本節內容，確認您的組態是否正常運作。

1. 開啟Web瀏覽器並輸入CUCM的FQDN。
2. 按一下「Cisco Unified Communications Manager」。
3. 選擇Web應用(CM管理/統一可維護性/Cisco Unified Reporting)並按Go,AD FS將提示您輸入憑據。輸入使用者SSO的憑證後，您即成功登入到選定的Web應用(CM管理頁面、Unified Serviceability頁面、Cisco Unified Reporting)。



附註：SAML SSO不允許訪問以下頁面：

- Prime Licensing Manager
- 作業系統管理
- 災難恢復系統

疑難排解

如果您無法啟用SAML且無法登入，請使用名為**Recovery URL**的已安裝應用程式下的新選項繞過單點登入(SSO)，該選項可用於使用在安裝期間建立的憑據或本地建立的CUCM管理使用者登入。

Cisco Unified CM Console - Windows Internet Explorer

https://cuom.discohive.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.

如需進一步的疑難排解，請參閱[適用於合作產品10.x的SAML SSO疑難排解](#)。