

Unity Connection版本10.5 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

本文說明如何為Cisco Unity Connection(UCXN)配置和驗證安全斷言標籤語言(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。有關同步時鐘的資訊，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。

必須安裝和配置Active Directory聯合身份驗證服務(AD FS)版本2.0才能處理SAML請求。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- AD FS版本2.0作為IdP

- 作為服務提供商的UCXN
- Microsoft Internet Explorer版本10

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是一種基於XML的開放式標準資料格式，用於資料交換。這是服務提供商用於驗證使用者身份的身份驗證協定。安全身份驗證資訊在IdP和服務提供商之間傳遞。

SAML是一種開放標準，它使客戶端能夠根據任何支援SAML的合作（或統一通訊）服務進行身份驗證，而不管客戶端平台如何。

所有Cisco Unified Communication Web介面(如Cisco Unified Communications Manager(CUCM)或UCXN)都使用SAML SSO功能中的SAML 2.0版協定。為了對輕量級目錄訪問協定(LDAP)使用者進行身份驗證，UCXN將身份驗證請求委託給IdP。由UCXN生成的身份驗證請求為SAML請求。IdP驗證並返回SAML斷言。SAML Assertion顯示Yes(authenticated)或No(authentication failed)。

SAML SSO允許LDAP使用者使用在IdP上進行身份驗證的使用者名稱和密碼登入客戶端應用程式。啟用SAML SSO功能後，使用者登入統一通訊產品上任何受支援的Web應用，還可以訪問UCXN上的這些Web應用（除CUCM和CUCM IM和線上狀態外）：

Unity Connection使用者	Web應用程式
具有管理員許可權的LDAP使用者	<ul style="list-style-type: none"> • UCXN管理 • Cisco UCXN可維護性 • Cisco Unified Serviceability • 思科個人通訊助理 • Web收件箱 • 迷你Web收件箱（案頭版本） • 思科個人通訊助理
無管理員許可權的LDAP使用者	<ul style="list-style-type: none"> • Web收件箱 • 迷你Web收件箱（案頭版本） • Cisco Jabber使用者端

設定

網路圖表

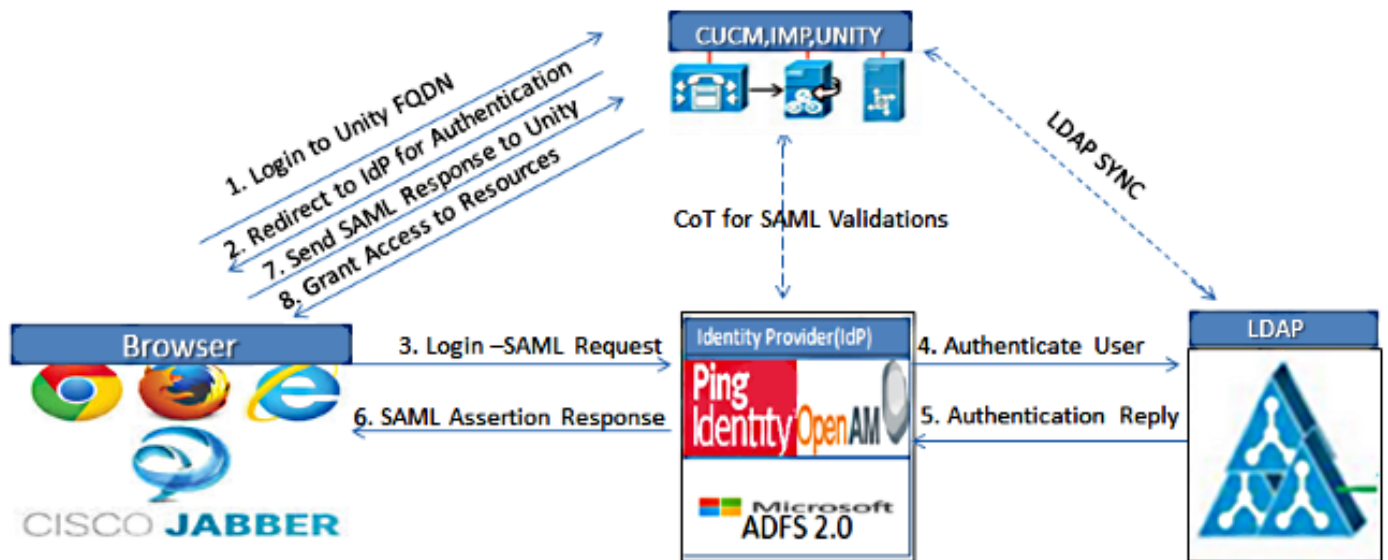


Figure :SAML Single sign SSO Call Flow for Collaboration Servers

目錄設定

1. 登入到UCXN管理頁面，然後選擇LDAP，然後按一下LDAP設定。
2. 選中Enable Synchronizing from LDAP Server，然後按一下Save。

LDAP System Configuration

Save

Status

Status: Ready

LDAP System Information

Enable Synchronizing from LDAP Server

LDAP Server Type: Microsoft Active Directory

LDAP Attribute for User ID: sAMAccountName

Save

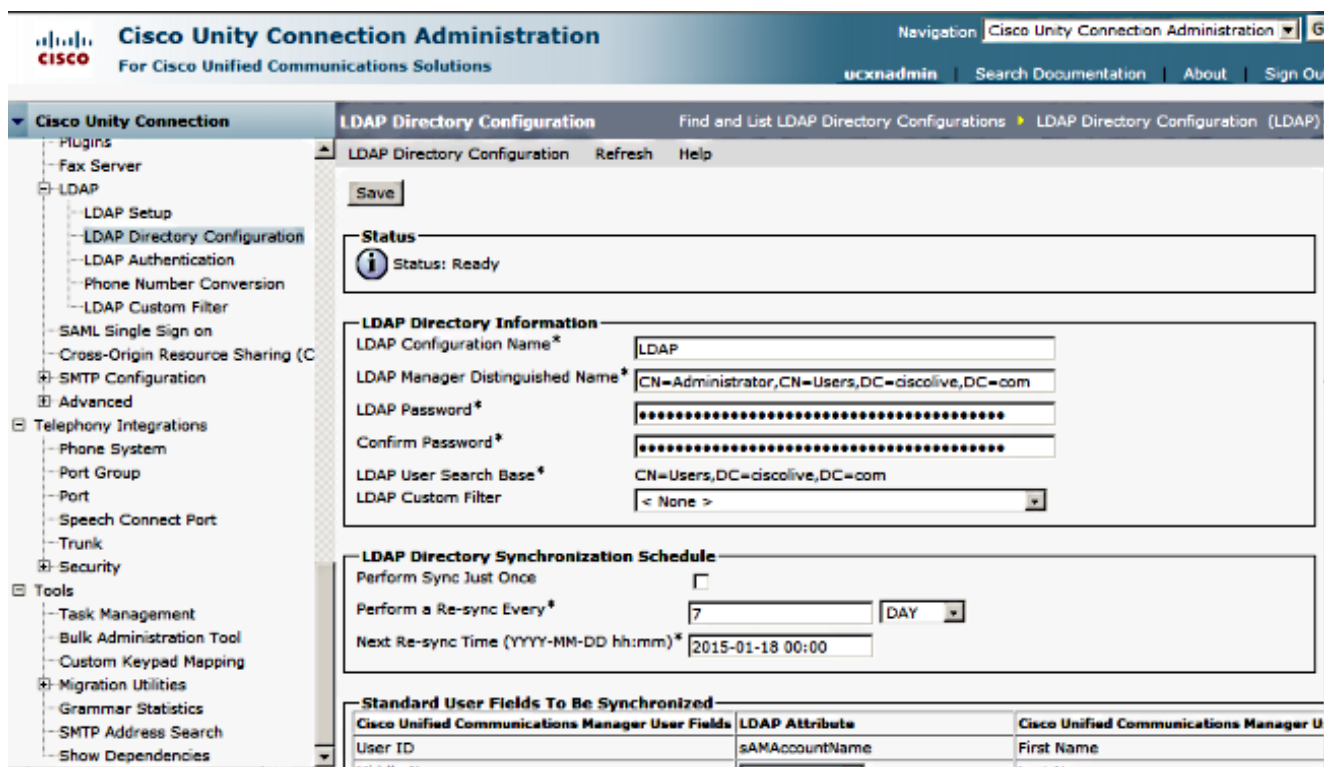
3. 按一下LDAP。
4. 按一下LDAP Directory Configuration。
5. 按一下「Add New」。

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

7. 如果要使用安全套接字層(SSL)與LDAP目錄通訊，請選中Use SSL。

提示：如果通過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。

9. 展開Users並選擇Import Users。

10. 在Find Unified Communications Manager End Users清單中，選擇LDAP Directory。

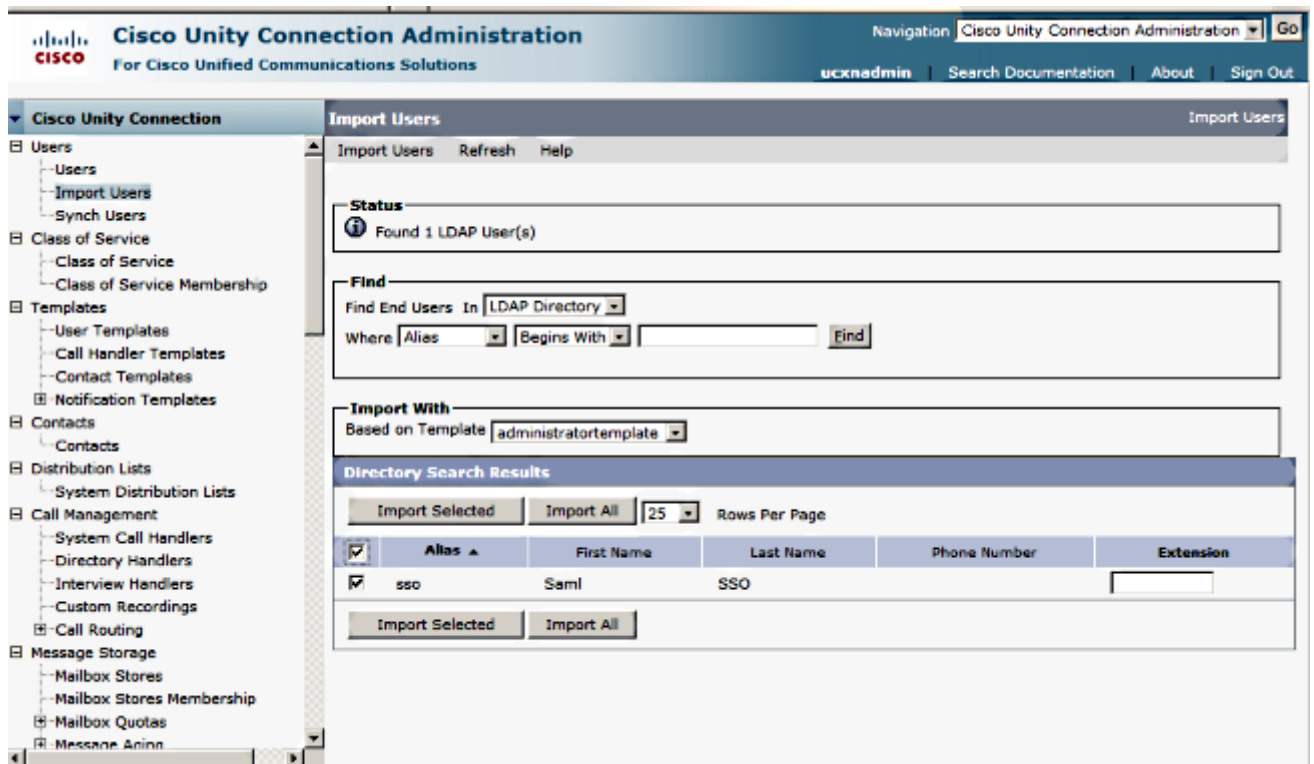
11. 如果您希望僅匯入已整合UCXN的LDAP目錄中的使用者子集，請在搜尋欄位中輸入適用的規範。

12. 選擇查詢。

13. 在「基於模板」清單中，選擇**希望UCXN**在建立所選使用者時使用的管理員模板。

注意：如果指定管理員模板，使用者將沒有郵箱。

14. 選中要為其建立UCXN使用者的LDAP使用者的覈取方塊，然後按一下**Import Selected**。

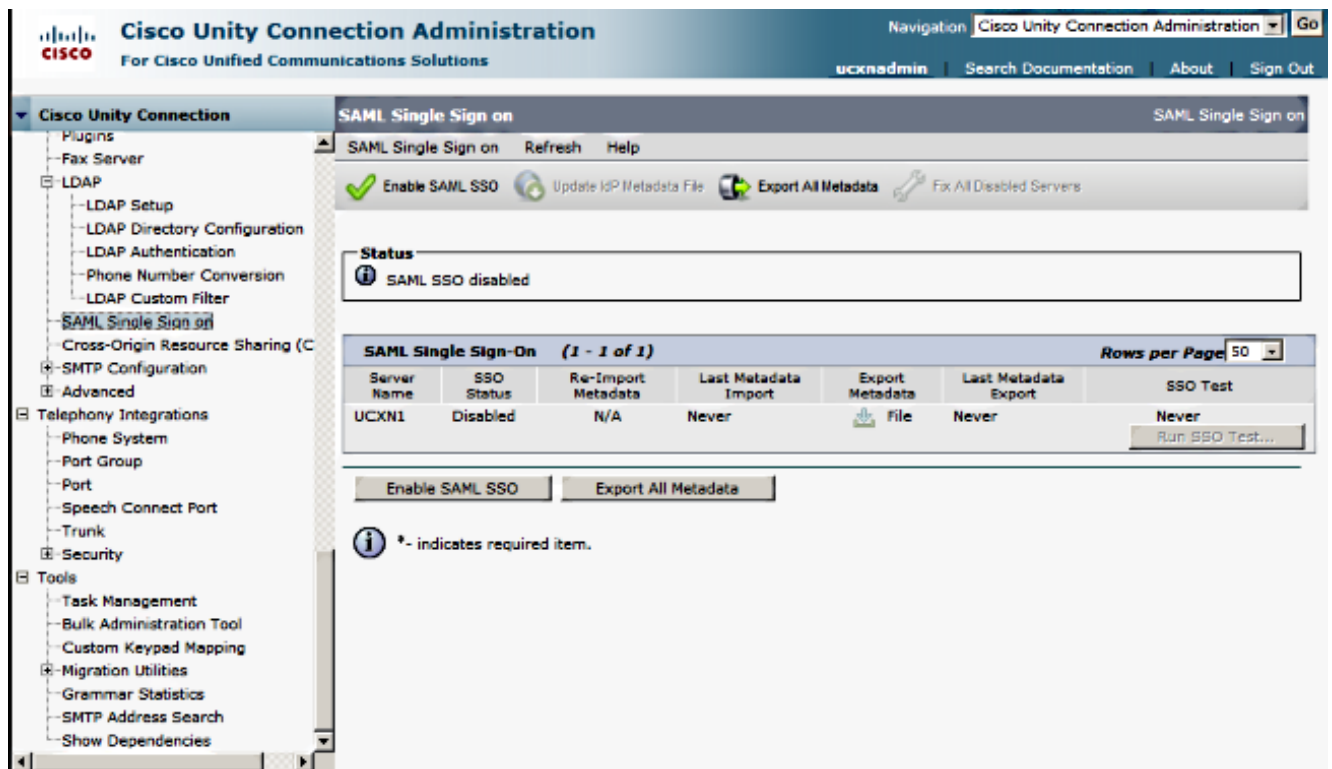


The screenshot shows the Cisco Unity Connection Administration interface. The left sidebar contains a navigation tree with categories like Users, Class of Service, Templates, Contacts, Distribution Lists, Call Management, and Message Storage. The main content area is titled 'Import Users' and includes a 'Status' section indicating 'Found 1 LDAP User(s)'. Below this is a 'Find' section with search criteria: 'Find End Users In' set to 'LDAP Directory', 'Where' set to 'Alias', and 'Begins With' set to an empty field. The 'Import With' section shows 'Based on Template' set to 'administratortemplate'. The 'Directory Search Results' section features a table with columns: Alias, First Name, Last Name, Phone Number, and Extension. The table contains one row with the following data: Alias: sso, First Name: Saml, Last Name: SSO, Phone Number: (empty), Extension: (empty). The 'Alias' column has a checked checkbox. Below the table are 'Import Selected' and 'Import All' buttons.

啟用SAML SSO

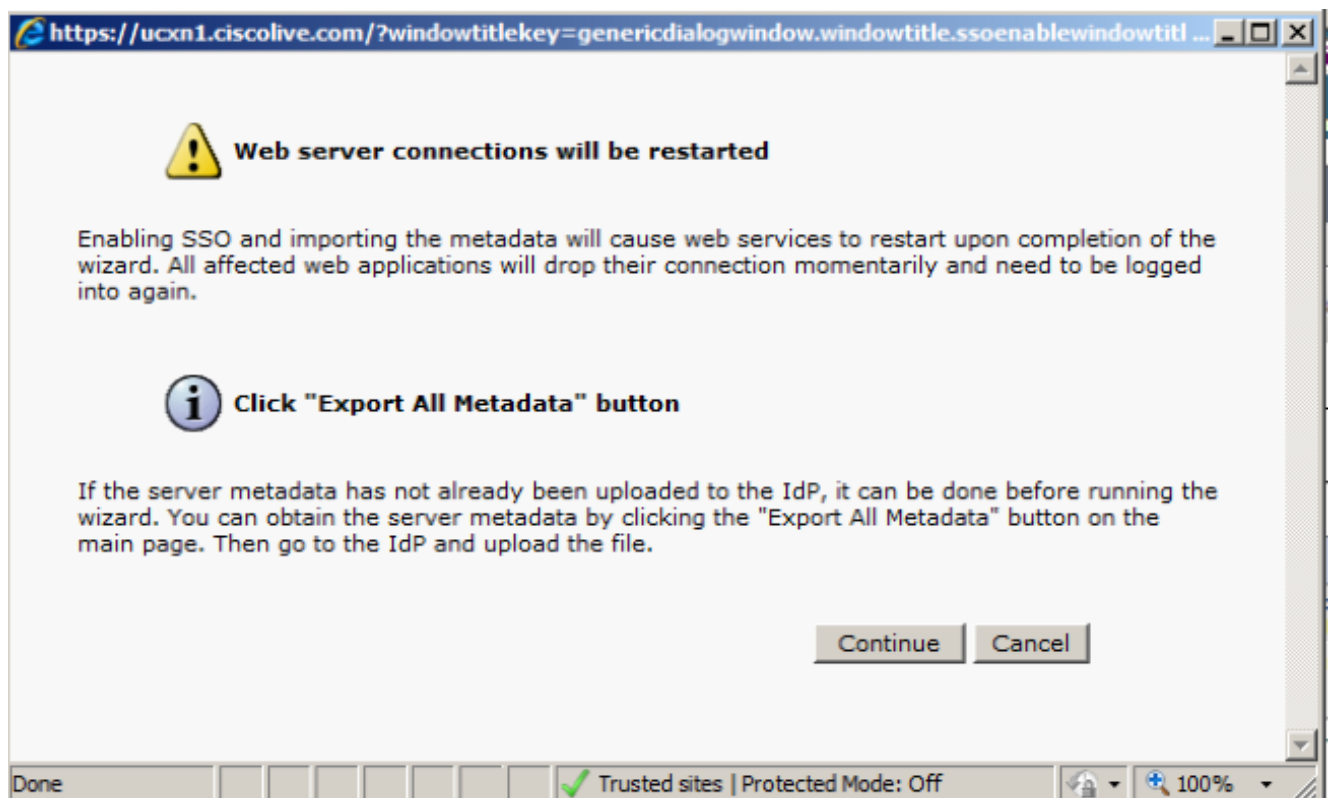
1. 登入到UCXN管理使用者介面。

2. 選擇**System > SAML Single Sign-on**，此時將開啟SAML SSO Configuration視窗。

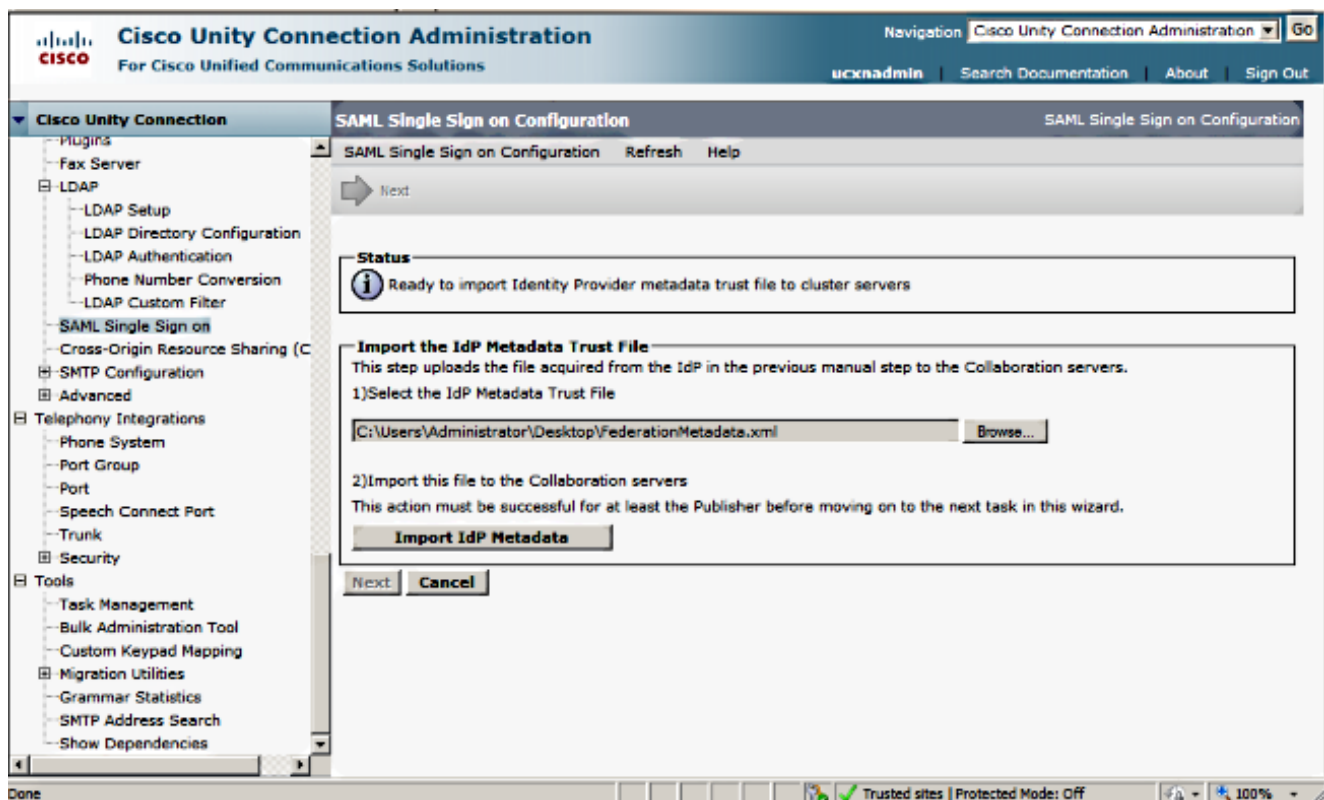


3. 要在群集中啟用SAML SSO，請按一下**Enable SAML SSO**。

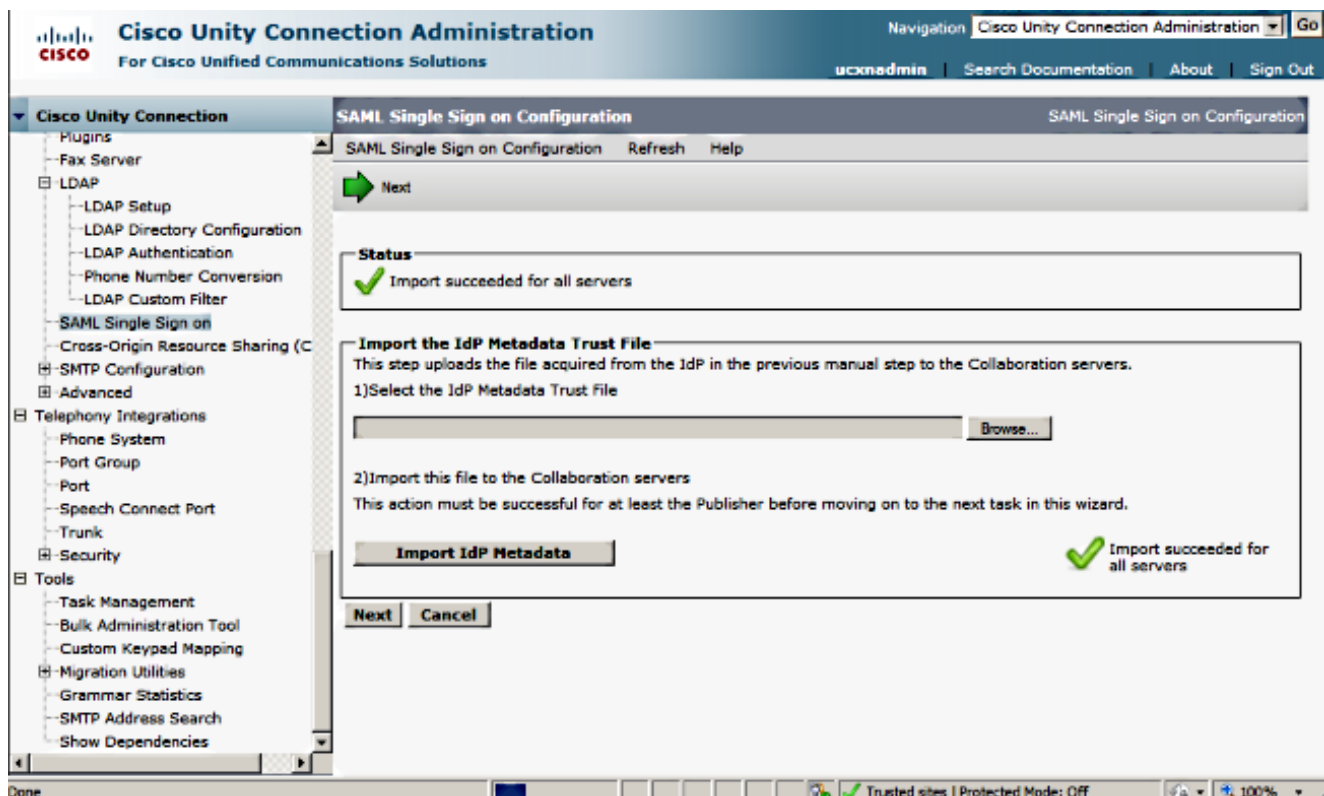
4. 在「重置警告」視窗中，按一下**繼續**。



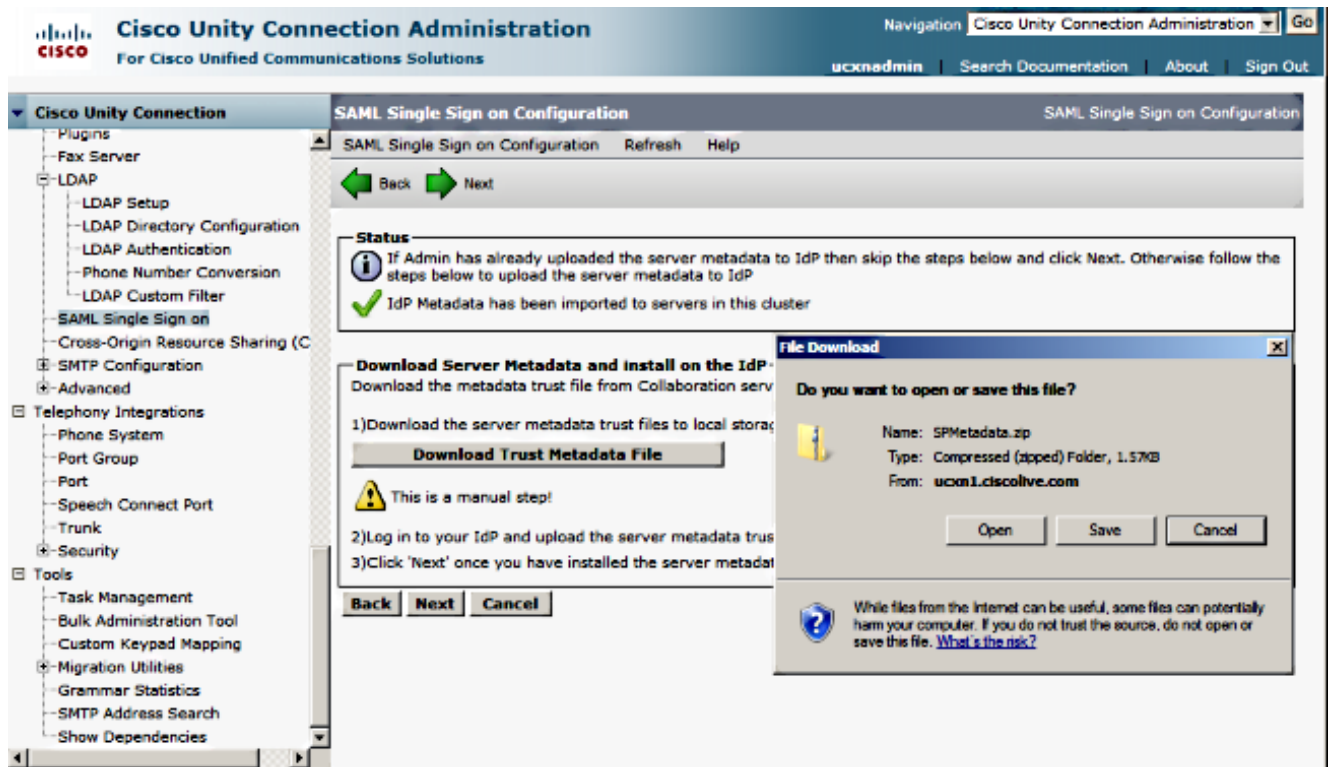
5. 在SSO螢幕上，按一下**Browse**，以使用**Download Idp Metadata**步驟匯入**FederationMetadata.xml**後設資料XML檔案。



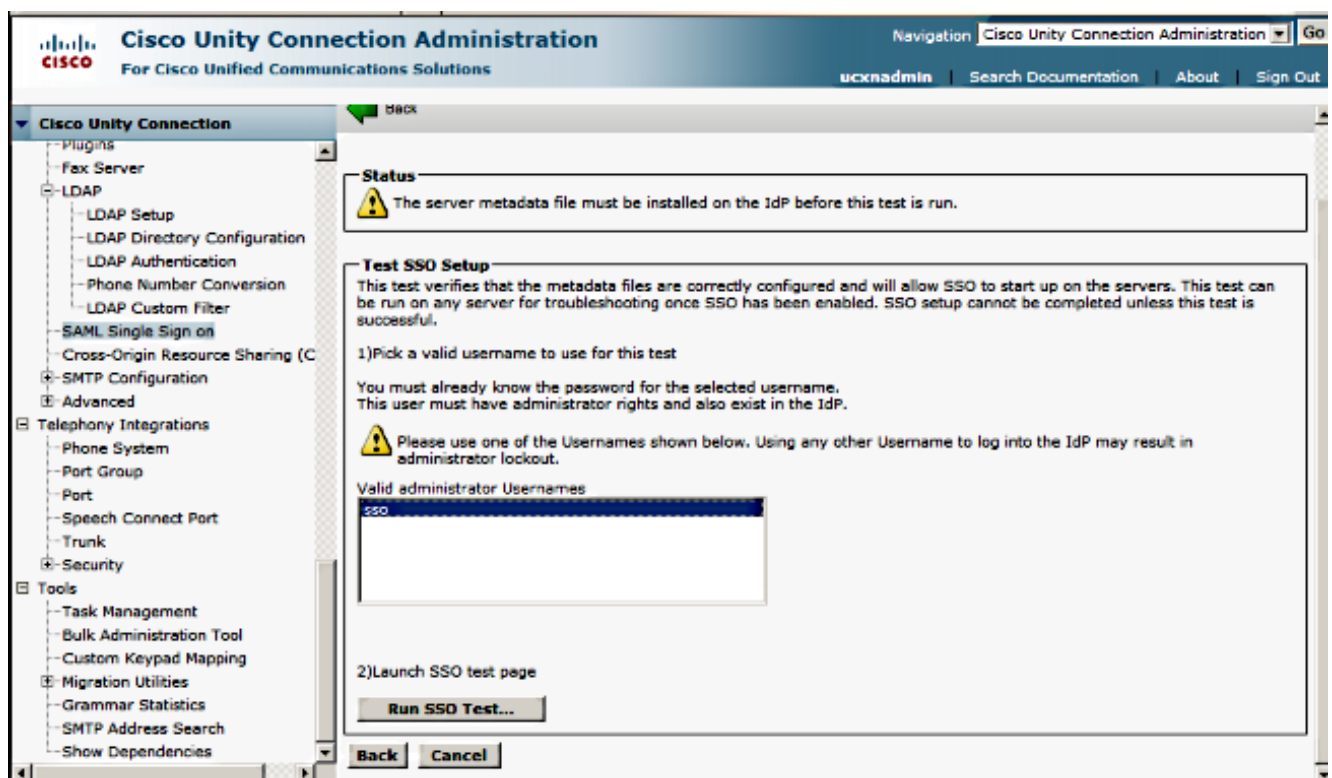
6. 上載後設資料檔案後，按一下 **Import IdP Metadata** 以將 IdP 資訊匯入 UCXN。確認匯入成功，然後按一下下一步繼續。



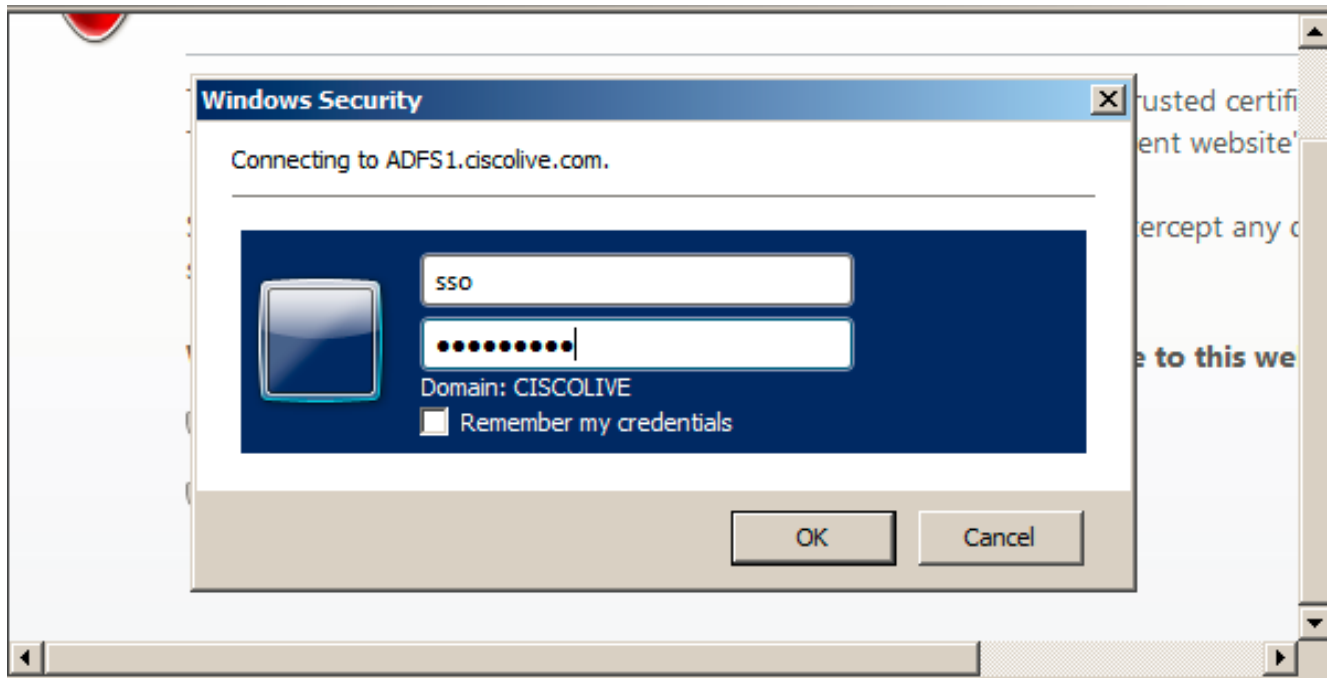
7. 按一下 **Download Trust Metadata Fileset** (僅當尚未使用 UCXN Metadata 配置 ADFS 時才執行此操作) 以將 UCXN 後設資料儲存到本地資料夾，並轉至 [Add UCXN as Relaying Party Trust](#)。完成 AD FS 配置後，請繼續執行步驟 8。



8. 選擇SSO作為管理使用者，然後按一下運行SSO測試。

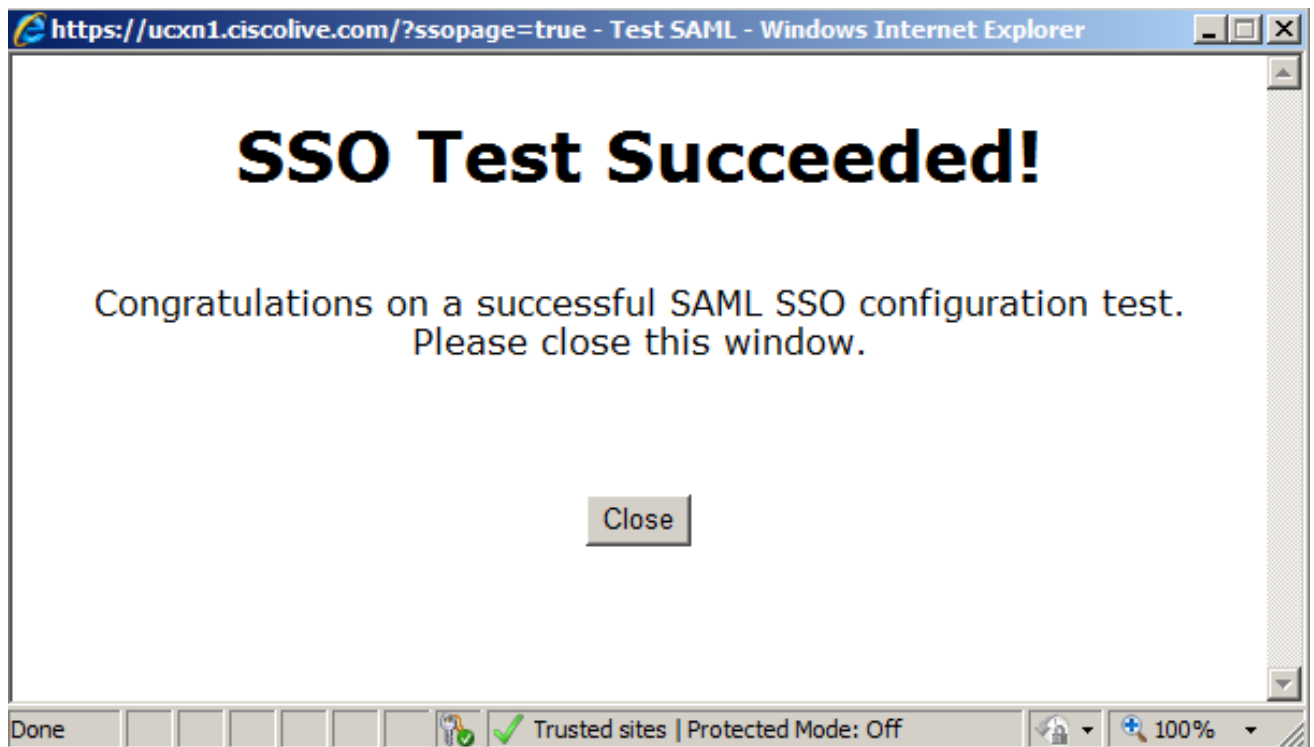


9. 忽略證書警告並繼續操作。當系統提示您輸入憑據時，輸入使用者SSO的使用者名稱和密碼，然後按一下OK。



附註：此配置示例基於UCXN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UCXN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，您將收到「SSO測試成功！」消息。按一下「Close」和「Finish」以繼續。



現在，您已成功完成配置任務，以便在UCXN上啟用SSO（使用AD FS）。

必需附註：如果UCXN訂戶是集群，請運行SSO測試以啟用SAML SSO。必須為群集中UCXN的所有節點配置AD FS。

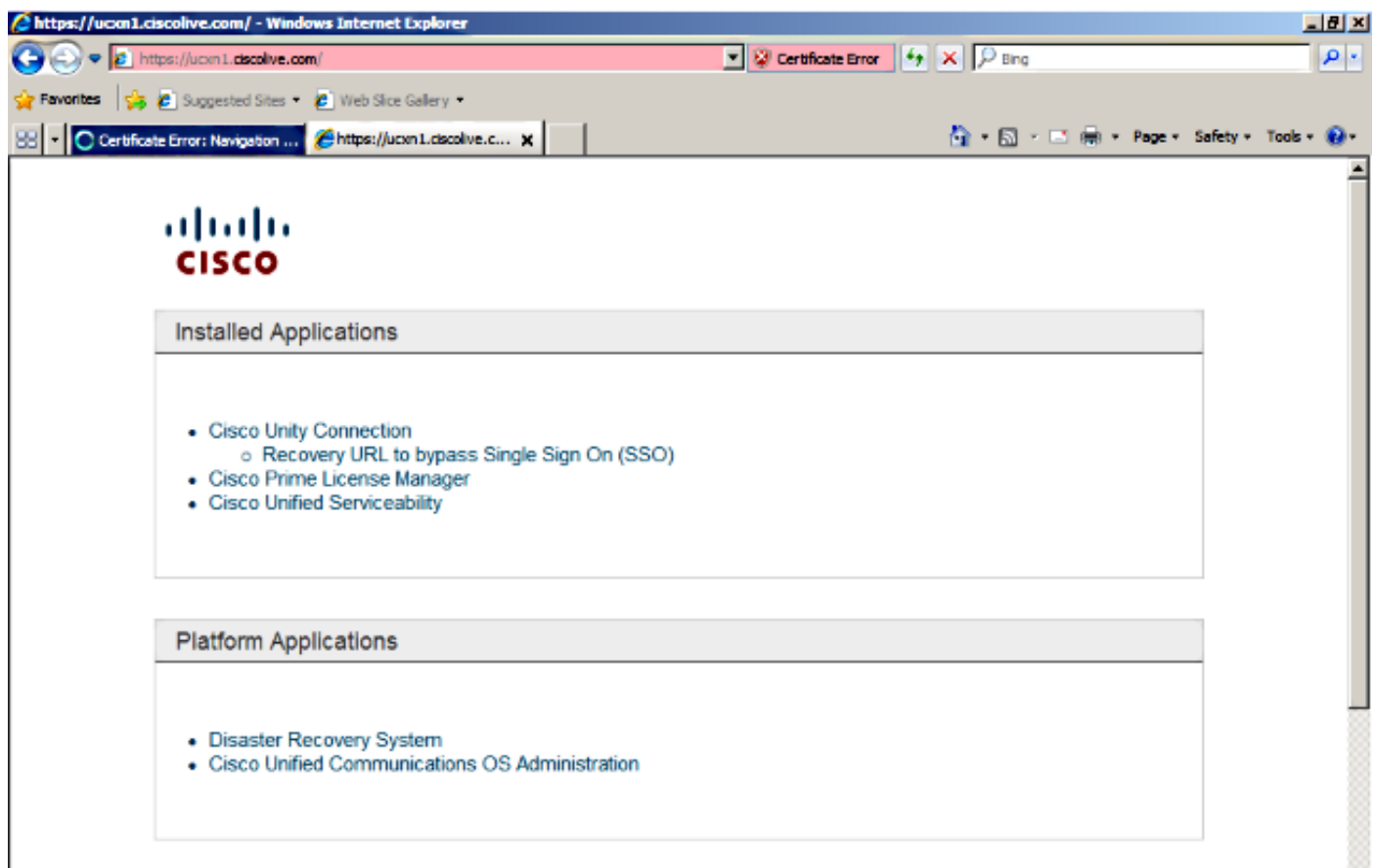
提示：如果在IdP上配置所有節點的後設資料XML檔案，並且開始在一個節點上啟用SSO操作

，則將自動在群集中的所有節點上啟用SAML SSO。

如果您希望對Cisco Jabber客戶端使用SAML SSO，並為終端使用者提供真正的SSO體驗，您還可以為SAML SSO配置CUCM和CUCM IM和線上狀態。

驗證

開啟Web瀏覽器並輸入UCXN的FQDN，您會看到「已安裝的應用程式」(稱為「Recovery URL」)下有一個新選項，用於繞過單點登入(SSO)。按一下Cisco Unity Connection連結後，AD FS會提示您輸入憑證。輸入使用者SSO的憑據後，您將成功登入到Unity Administration頁面Unified Serviceability頁面。



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

目前尚無適用於此組態的具體疑難排解資訊。

如需詳細資訊，請參閱[適用於協同合作產品10.x的SAML SSO疑難排解](#)。