

# 為Jabber客戶端啟用SAML SSO配置示例

## 目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[設定](#)

[網路圖表](#)

[驗證](#)

[疑難排解](#)

## 簡介

本檔案介紹如何為安全斷言標籤語言(SAML)單一登入(SSO)配置Cisco Jabber客戶端和基礎設施伺服器。

## 必要條件

必須為Jabber使用者預配Cisco Unified Communications Manager(CUCM)IM and Presence、Cisco Unity Connection(UCXN)和CUCM等基礎設施伺服器，並且必須準備好基本Jabber客戶端配置。

## 需求

思科建議您瞭解以下主題：

- CUCM IM和狀態版本10.5(1)或更高版本
- UCXN 10.5(1)版或更高版本
- CUCM 10.5(1)或更高版本
- Cisco Jabber使用者端版本10.5

## 採用元件

本文件所述內容不限於特定軟體和硬體版本。

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。

# 設定

## 網路圖表

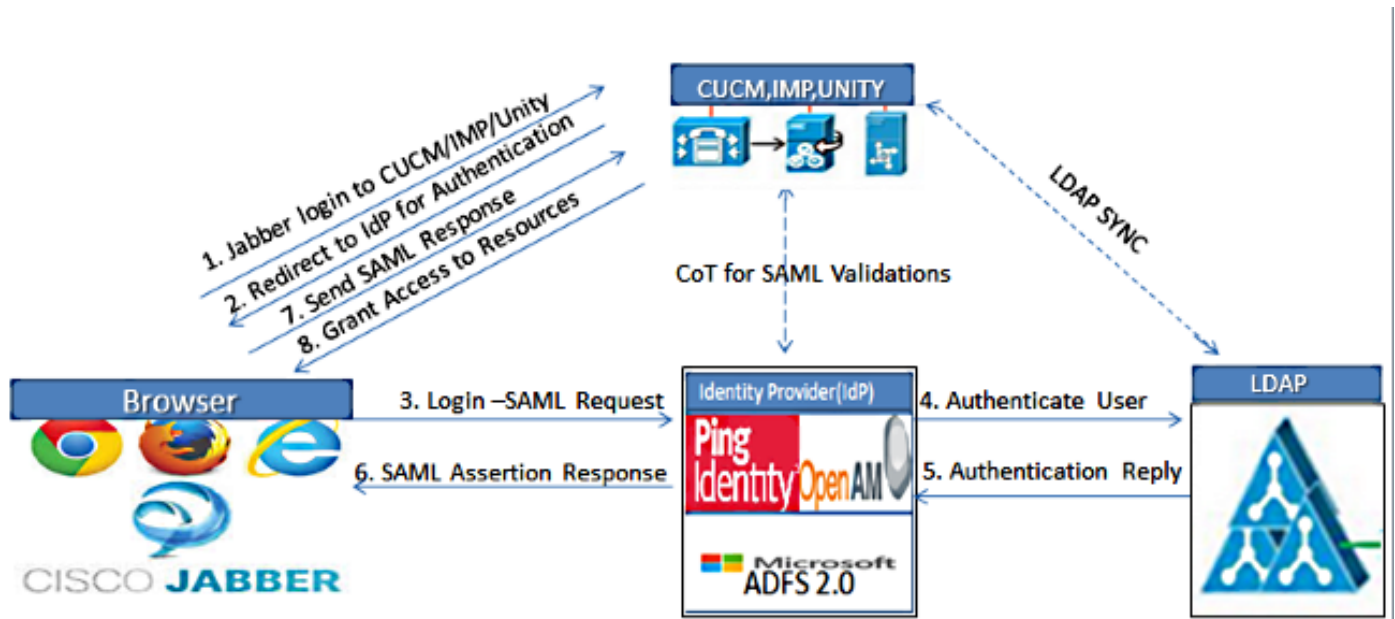


Figure :SAML Single sign SSO Call Flow for Collaboration Servers

1. 在所有伺服器上部署證書，以便證書可以由Web瀏覽器驗證；否則，使用者會收到有關無效證書的警告消息。有關憑證驗證的詳細資訊，請參閱[憑證驗證](#)。
2. 確保客戶端中的SAML SSO的服務發現。客戶端使用標準服務發現以在客戶端中啟用SAML SSO。 使用以下配置引數啟用服務發現：**ServicesDomain**、**VoiceServicesDomain**和**ServiceDiscoveryExcludedServices**。  
  
有關如何啟用服務發現的更多資訊，請參閱[客戶端如何查詢服務](#)。
3. 請參閱[統一通訊管理器10.5版SAML SSO配置示例](#)，以啟用Jabber對電話服務使用SSO。
4. 請參閱[統一通訊管理器10.5版SAML SSO配置示例](#)，以啟用IM功能的SSO的Jabber使用。
5. 請參閱[Unity Connection版本10.5 SAML SSO配置示例](#)，以啟用語音郵件的SSO的Jabber使用。
6. 請參閱[使用Kerberos驗證的SAML SSO設定配置示例](#)，以配置客戶端電腦以進行自動登入（僅限Windows版Jabber）
7. 在CUCM和IMP上啟用SSO後，預設情況下所有Jabber使用者均使用SSO登入。管理員可以針對每個使用者進行更改，以便某些使用者不使用SSO，而是使用其Jabber使用者名稱和密碼登入。若要為Jabber使用者禁用SSO，請將SSO\_Enabled引數的值設定為**FALSE**。

如果您將Jabber配置為不要求使用者輸入其電子郵件地址，則他們第一次登入Jabber可能是非SSO。在某些部署中，**ServicesDomainSsoEmailPrompt**引數必須設定為**ON**。這可確保

Jabber擁有執行首次SSO登入所需的資訊。如果使用者之前已登入Jabber，則不需要此提示，因為所需資訊可用。

## **驗證**

啟動Windows版Jabber時，它應自動登入，而不提示輸入任何憑據或輸入。對於其他Jabber客戶端，將只提示您輸入憑據一次。

## **疑難排解**

如果您遇到問題，請收集Jabber問題報告並聯絡思科技術協助中心(TAC)。