

部署授權代碼授權流程並對其進行故障排除 — OAuth增強功能：思科合作解決方案12.0

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[功能要點](#)

[重要注意事項](#)

[授權碼授權流程要素](#)

[設定](#)

[網路圖表](#)

[刷新令牌](#)

[撤銷刷新令牌](#)

[驗證](#)

[疑難排解](#)

[相關資訊](#)

簡介

本文檔介紹授權碼授權流如何基於刷新令牌，以便改善各種裝置（尤其是流動裝置上的Jabber）的Jabber使用者體驗。

必要條件

需求

思科建議您瞭解以下主題：

- 思科整合通訊管理員(CUCM)12.0版本
- 單一登入(SSO)/SAML
- Cisco Jabber
- Microsoft ADFS
- 身份提供程式(IdP)

若要取得有關這些主題的詳細資訊，請參閱以下連結：

- [思科統一通訊SAML SSO部署指南](#)
- [Unified Communications Manager SAML SSO配置示例：](#)
- [用於SAML SSO的AD FS 2.0版設定配置示例：](#)

採用元件

本檔案中的資訊是根據以下軟體：

- Microsoft ADFS(IdP)
- LDAP Active Directory
- Cisco Jabber使用者端
- CUCM 12.0

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。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

目前，基礎設施中的Jabber SSO流基於隱式授權流，其中CUCM Authz服務分配短期訪問令牌。

訪問令牌到期後，CUCM將Jabber重定向到IdP以進行重新身份驗證。

這會導致使用者體驗不佳，尤其是使用Jabber在流動裝置上時，使用者需要經常輸入憑證。

安全重新架構解決方案還提出了授權碼授權流程(使用刷新令牌方法（可擴展到終端/其他合作應用）)，以便在SSO和非SSO場景中統一Jabber和終端登入流程。

功能要點

- 授權碼授權流程基於刷新令牌（可擴展到終端/其他合作應用），以便改善各種裝置之間的Jabber使用者體驗，尤其是移動版Jabber。
- 支援自包含簽名和加密的OAuth令牌，以允許各種合作應用程式驗證和響應客戶端資源請求。
- 保留隱式授權流模型，允許向後相容。這還允許未遷移到授權代碼授予流程的其他客戶端（如RTMT）使用無縫路徑。

重要注意事項

- 實現，以便舊jabber客戶端可以與新CUCM配合使用（因為它支援隱式授予和授權碼授予流程）。此外，新的jabber可以與舊CUCM配合使用。Jabber可以確定CUCM是否支援授權碼授權流，並且僅當它支援此模型時，它才切換並使用隱式授權流。
- 身份驗證服務在CUCM伺服器上運行。
- AuthZ僅支援隱式授權流。這表示沒有刷新令牌/離線訪問令牌。每次使用者端需要新的存取權杖時，使用者需要使用IdP重新進行驗證。
- 僅當部署啟用了SSO時，才會頒發訪問令牌。非SSO部署在此情況下不起作用，訪問令牌未在所有介面上一致使用。
- 訪問令牌不是獨立的，而是保留在發出它們的伺服器的記憶體中。如果CUCM1發出了訪問令牌，則只能由CUCM1進行驗證。如果客戶端嘗試訪問CUCM2上的服務，CUCM2需要在CUCM1上驗證該令牌。網路延遲（代理模式）。
- 移動客戶端上的使用者體驗非常糟糕，因為使用者使用IdP重新進行身份驗證時，必須在字母數字鍵盤上重新輸入憑據（通常從1小時到8小時運行，這取決於多個因素）。
- 通過多個介面與多個應用程式進行通訊的客戶端需要維護多個憑據/塊。對於從2個類似客戶端登入的同一使用者，沒有無縫支援。例如，使用者A從在2個不同iPhone上運行的jabber例項登入。
- AuthZ，支援SSO和非SSO部署。
- 支援隱式授權流+授權代碼授權流的授權流。因為它具有向後相容，允許RTMT這樣的客戶端繼

續工作，直到它們適應為止。

- 透過授權碼授權流程，AuthZ會發出存取權杖和刷新權杖。刷新令牌可用於獲取另一個訪問令牌，而無需身份驗證。
- 訪問令牌是自包含、簽名和加密的，並使用JWT (JSON Web令牌) 標準 (與RFC相容)。
- 簽名和加密金鑰對群集是通用的。群集中的任何伺服器都可以驗證訪問令牌。沒有必要在記憶體中保留。
- 在CUCM 12.0上運行的服務是群集中的集中身份驗證伺服器。
- 刷新令牌儲存在資料庫(DB)中。 如果需要，管理員需要能夠撤銷它。吊銷基於使用者ID或使用者ID和客戶端ID。
- 簽名訪問令牌允許不同的產品驗證訪問令牌而無需儲存它們。可配置的訪問令牌和刷新令牌生存期 (預設分別為1小時和60天)。
- JWT格式與Spark保持一致，從而可在未來與Spark Hybrid服務實現協同效應。
- 支援同一使用者從2個類似裝置登入。例如：使用者A可以從運行在2個不同iPhone上的jabber例項登入。

授權碼授權流程要素

- Auth Z Server
- 加密金鑰
- 簽名金鑰
- 刷新令牌

設定

預設情況下未啟用此功能。

步驟1. 若要啟用此功能，請導覽至System > Enterprise Parameters。

步驟2. 將「Refresh Login Flow」引數設定為「Enabled」，如下圖所示。

SSO and OAuth Configuration		
OAuth Access Token Expiry Timer (minutes) *	60	60
OAuth Refresh Token Expiry Timer (days) *	60	60
Redirect URIs for Third Party SSO Client		
SSO Login Behavior for iOS *	Use embedded browser (WebView)	Use embedded browser (WebView)
OAuth with Refresh Login Flow *	Enabled	Disabled
Use SSO for RTMT *	True	True




- 訪問令牌已簽名並加密。簽名和加密金鑰對群集是通用的。這意味著群集中的任何節點都可以驗證訪問令牌。
- 訪問令牌採用JWT格式(RFC 7519)。
- 訪問令牌重複使用企業引數 (OAuth訪問令牌到期計時器)，它適用於舊令牌和新令牌格式。
- 預設值 — 60分鐘。
- 最小值-1分鐘
- 最大值 — 1440分鐘

eyJhbGciOiJIUzU1NiIsInR5cCI6IkpXVCIsImt0IjoiIj04MTF1LTRhNTlmZGI2YjcyMjMjMjc3MGM5N2JkYTlkMzRmZDA1YTdlYTZhZWQzZTU0Y2E4MGJkZDdlZTM1ZDk3MDNiNjBiNTQ5MTBiZDQ0ODRiIn0.eyJwcm12YXR1Ijo1ZX1KaGJHY2lPaUprYVhJaUxDSmpkSGtpT2lks1YxUWlMQ0psYm1NaU9pSkJNVEk0UTBKRExVaFRNaUySWl3aWEybGtJam9pT0dRdlpEVXpNa1F0WmpSbU1DMDBZakJpTFRneE1XVXROR0UxTldaallqWmlOek15T21Vd1ptUm1ZMk16WlRRMU5ERTFOV0ZpTkrJek5tRTJOM1V4T0RCbU1qWmxZMk13WXpJeE56SXlOREJtWlRFellXWXlOak14TkRkalpHVXpNR113TjJJaWZR


Certificate Details(Self-signed) - Internet Explorer provided by Cisco Systems, Inc.

https://10.77.29.184/cmplatform/certificateEdit.do?cert=/usr/local/platform/.security/authz/certs/authz.j Certificate error

Certificate Details for AUTHZ_CUCM-184, authz

 Regenerate
  Download .PEM File
  Download .DER File

Status

 Status: Ready

Certificate Settings

File Name	authz.pem
Certificate Purpose	authz
Certificate Type	certs
Certificate Group	product-cpi
Description(friendly name)	Self-signed certificate generated by system

Certificate File Data

```

[
[
Version: V3
Subject: L=i, ST=i, CN=AUTHZ_CUCM-184, OU=i, O=i, C=IN
Signature Algorithm: SHA256withRSA, OID = 1.2.840.113549.1.1.11

Key: CiscoJ RSA Public Key, 2048 bits
modulus:
310088952412132774650041525392629167237879710935753621934671843
216346326898490353644164813514840735197164588955185219996734516
256663568507413849247845292675452179850077675141884383314726763
520023902784651553941826511494962731151521090167892375623419501
739811988911210916820812069748957615302991414362015465824669063
319779866264424936428249029193098223306846888723560182717860238
318402233050626785154245146789308145325775236137097363983609689
  
```

使用CLI命令重新生成Authz簽名金鑰的過程如下圖所示。

```
CUCM-184 login: admin
Password:
Last login: Tue Nov 15 15:43:52 on tty1
Command Line Interface is starting up, please wait ...
```

```
Welcome to the Platform Command Line Interface
```

```
UMware Installation:
 1 vCPU: Intel(R) Xeon(R) CPU E5-2643 0 @ 3.30GHz
Disk 1: 80GB, Partitions aligned
6144 Mbytes RAM
```

```
admin:set ke
admin:set key regen authz signing
```

```
WARNING: This operation will regenerate the Authorization Service signing key and restart the Authorization Service on all the nodes. It is recommend that this command be run off-hours to avoid end user impact.
```

```
Proceed with regeneration (yes/no)? yes
```

```
signing key for the Authorization service generated succesfully.
```

```
admin:_
```

管理員可以使用CLI顯示授權簽名和加密金鑰。顯示金鑰的雜湊值，而不是原始金鑰。

用於顯示金鑰的命令有：

簽名金鑰：`show key authz signing`和，如下圖所示。

```
admin:show key authz signing
authz signing key with checksum: a155d81be734850226f990a62816f1ae last synced on: 06/09/2017 13:04:47
```

加密金鑰：`show key authz encryption`和，如下圖所示。

```
admin:show key authz encryption
authz encryption key with checksum: 88edce92173e33f9cedbbfb09cd0e8c4 last synced on: 06/14/2017 16:22:06
```

附註：簽名授權和加密授權始終不同。

驗證

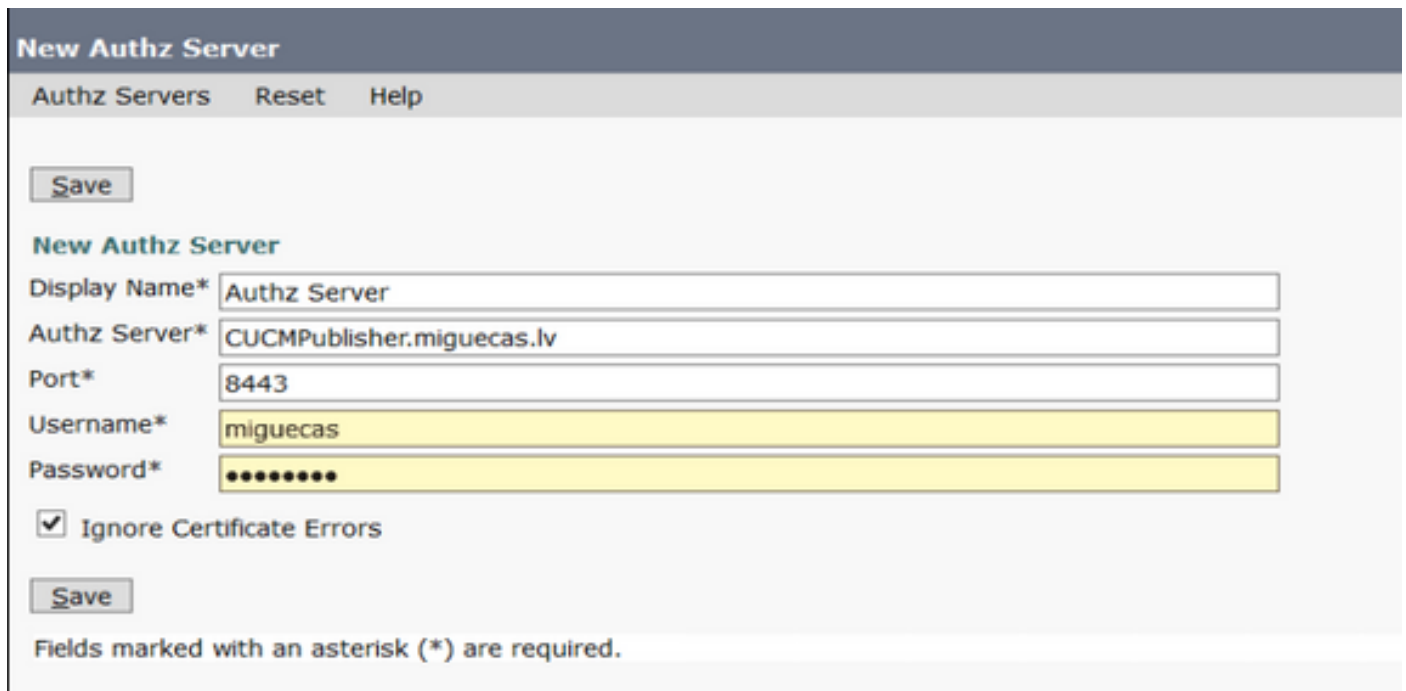
使用本節內容，確認您的組態是否正常運作。

當在Cisco Unity Connection(CUC)伺服器上使用OAuth時，網路管理員必須執行兩個步驟。

步驟1.配置Unity Connection伺服器以從CUCM獲取OAuth令牌簽名和加密金鑰。

步驟2.在CUC伺服器上啟用OAuth服務。

注意：要獲取簽名和加密金鑰，必須使用CUCM主機詳細資訊和CUCM AXL訪問啟用的使用者帳戶配置Unity。如果未進行配置，則Unity Server無法從CUCM檢索OAuth令牌，並且使用者的語音郵件登入不可用。



New Authz Server

Authz Servers Reset Help

Save

New Authz Server

Display Name* Authz Server

Authz Server* CUCMPublisher.miguecas.lv

Port* 8443

Username* miguecas

Password*

Ignore Certificate Errors

Save

Fields marked with an asterisk (*) are required.

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

附註： 如果使用OAuth且Cisco Jabber使用者無法登入，請始終檢視CUCM和即時消息和線上狀態(IM&P)伺服器的簽名和加密金鑰。

網路管理員需要在所有CUCM和IM&P節點上運行以下兩個命令：

- **show key authz signing**
- **show key authz encryption**

如果所有節點的簽名authz和加密authz輸出不匹配，則需要重新生成它們。為此，需要在所有CUCM和IM&P節點上運行以下兩個命令：

- **set key regen authz encryption**
- **set key regen authz signing**

然後，需要在所有節點上重新啟動Cisco Tomcat服務。

除了金鑰不匹配之外，在Cisco Jabber日誌中還可以找到此錯誤行：

```
2021-03-30 14:21:49,631 WARN [0x0000264c] [vices\impl\system\SingleSignOn.cpp(1186)] [Single-Sign-On-Logger] [CSFUnified::SingleSignOn::Impl::handleRefreshTokenFailure] - Failed to get valid access token from refresh token, maybe server issue.
```

在以下位置生成sso應用日誌：

- **file view activelog platform/log/ssoApp.log** 這不需要對日誌收集進行任何跟蹤配置。每次完成SSO App操作時，都會在ssoApp.log檔案中生成新的日誌條目。
- SSOSP日誌：**file list activelog tomcat/logs/ssosp/log4j**

每次啟用sso時，都會在此位置建立一個名為ssosp00XXX.log的新日誌檔案。任何其他SSO操作和所有Oauth操作也登入到該檔案中。

- 證書日誌：**file list activelog platform/log/certMgmt*.log**
每次重新生成AuthZ證書（UI或CLI）時，都會為此事件生成新的日誌檔案。
為了重新生成授權加密金鑰，將為此事件生成一個新的日誌檔案。

相關資訊

[使用思科合作解決方案版本12.0部署OAuth](#)