部署授权代码授予流程并排除故障 — OAuth增强功能：思科协作解决方案12.0

目录

[简介](#)
[先决条件](#)
[要求](#)
[使用的组件](#)
[背景信息](#)
[功能亮点](#)
[重要注意事项](#)
[授权码授权流的要素](#)
[配置](#)
[网络图](#)
[刷新令牌](#)
[撤销刷新令牌](#)
[验证](#)
[故障排除](#)
[相关信息](#)

简介

本文档介绍授权代码授权流如何基于刷新令牌来改善各种设备（尤其是移动版Jabber）的Jabber用户体验。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科统一通信管理器(CUCM)12.0版
- 单点登录(SSO)/SAML
- Cisco Jabber
- Microsoft ADFS
- 身份提供程序(IdP)

要获取有关这些主题的详细信息，请参阅以下链接：

- 思科统一通信的SAML SSO部署指南
- Unified Communications Manager SAML SSO配置示例：
- AD FS版本2.0的SAML SSO设置配置示例：

使用的组件

本文档中的信息基于以下软件：

- Microsoft ADFS(IdP)
- LDAP Active Directory
- Cisco Jabber客户端
- CUCM 12.0

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

截至目前，Jabber SSO流与基础设施基于隐式授予流，其中CUCM授权服务分配短期访问令牌。

访问令牌到期后，CUCM将Jabber重定向到IdP以进行重新身份验证。

这会导致不良的用户体验，尤其是在移动Jabber中，用户需要频繁输入凭证。

安全重新架构解决方案还建议授权代码授权流(使用刷新令牌方法（可扩展到终端/其他协作应用））,以统一SSO和非SSO场景的Jabber和终端登录流。

功能亮点

- 授权代码授权流程基于刷新令牌（可扩展至终端/其他协作应用），以改进各种设备（尤其是移动版Jabber）的Jabber用户体验。
- 支持自包含签名和加密的OAuth令牌，以允许各种协作应用验证和响应客户端资源请求。
- 保留隐式授权流模型，以便向后兼容。这还允许未移至授权代码授予流的其他客户端（如RTMT）的无缝路径。

重要注意事项

- 这样，旧Jabber客户端可以与新CUCM配合使用（因为它同时支持隐式授权和授权代码授权流）。 此外，新Jabber可与旧CUCM配合使用。Jabber可以确定CUCM是否支持授权码授权流，并且仅当它支持此模型时，它才会切换并使用隐式授权流。
- 授权服务在CUCM服务器上运行。
- AuthZ仅支持隐式授权流。这意味着没有刷新令牌/脱机访问令牌。每次客户端需要新的访问令牌时，用户都需要使用IdP重新进行身份验证。
- 只有在部署启用SSO时，才颁发访问令牌。在这种情况下，非SSO部署不起作用，并且访问令牌未在所有接口上一致使用。
- 访问令牌不是自包含的，而是保留在发出它们的服务器的内存中。如果CUCM1发出访问令牌，则只能由CUCM1验证。如果客户端尝试访问CUCM2上的服务，CUCM2需要验证CUCM1上的令牌。网络延迟（代理模式）。
- 移动客户端上的用户体验非常糟糕，因为当用户使用IdP重新进行身份验证时，用户必须在字母数字键盘上重新输入凭证（通常运行1到8小时，具体取决于多个因素）。
- 通过多个接口与多个应用程序通话的客户端需要维护多个凭证/块。不支持从2个类似客户端登录同一用户。例如，用户A从运行于2个不同iPhone的jabber实例登录。
- AuthZ，支持SSO和非SSO部署。
- AuthZ支持隐式授权流+授权代码授权流。由于它向后**兼容，它**允许RTMT等客**户**端继续工作，直到他们适应。

- 使用授权代码授予流，授权发出访问令牌和刷新令牌。刷新令牌可用于获取另一个访问令牌，而无需身份验证。
- 访问令牌是自包含、签名和加密的，并使用JWT（JSON Web令牌）标准（符合RFC）。
- 签名密钥和加密密钥对群集是通用的。群集中的任何服务器都可以验证访问令牌。无需在内存中维护。
- 在CUCM 12.0上运行的服务是集群中的集中身份验证服务器。
- 刷新令牌存储在数据库(DB)中。 管理员需要能够撤销它（如果需要）。撤销基于用户ID或用户ID和客户端ID。
- 签名访问令牌允许不同产品验证访问令牌，而无需存储它们。可配置访问令牌和刷新令牌生存期（分别默认为1小时和60天）。
- JWT格式与Spark相一致，它支持未来与Spark Hybrid服务的协同效应。
- 支持同一用户从2台类似设备登录。例如：用户A可以从运行于2个不同iPhone的jabber实例登录。

授权码授权流的要素

- 授权服务器
- 加密密钥
- 签名密钥
- 刷新令牌

配置

默认情况下，此功能未启用。

步骤1.要启用此功能，请导航至System > Enterprise Parameters。

步骤2.如图所示，将**具有刷新登录流**的参数OAuth设置为已启用。

- 访问令牌已签名并加密。签名和加密密钥对群集是通用的。这意味着群集中的任何节点都可以验证访问令牌。
- 访问令牌采用JWT格式(RFC 7519)。
- 访问令牌重复使用企业参数（OAuth访问令牌过期计时器），适用于旧令牌和新令牌格式。
- 默认值 — 60分钟。
- 最小值 — 1分钟
- 最大值 — 1440分钟


```
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6IjhkMGQ1MzI0LWY0ZjAtNGIwYi04MTFlLTRhNTlmZGI2YjcyMjpj
Mjc3MGM5N2JkYTlkMzRmZDA1YTdlYTFhZWQzZTU0Y2E4MGJkZDdlZTM1ZDk3MDNiNjBiNTQ5MTBiZDQ0ODRiIn0.eyJwcml2
YXRlIjoiZXlKaGJHY2lPaUprYVhJaUxDSmpkSGtpT2lKS1YxUWlMQ0psYm1NaU9pSkJNVEk0UTBKRExVaFRNalUySWl3aWEy
bGtJam9pT0dRd1pEVXpNalF0WmpSbU1DMDBZakJpTFRneE1XVXROR0UxT1daa1lqWmlOekl5T21Vd1ptUm1ZMk16WlRRMU5E
RTFOV0ZpTkRJek5tRTJOMlV4T0RCbU1qWmxZMkl3WXpJeE56SXlOREJtWlRFellXWXlOak14TkRkalpHVXpNR1l3TjJJaWZR
Li5xQWd6aGdRaTVMMkdlaDl5V2RvN25nLmdMTHNpaTRjQk50c1NEUXRJTE51RWRnWTl4WkJVczJ4YzBaeTFGQjZQNmNzWWJf
```

ZkRnaDRZby04V1NaNjUzdXowbnFOalpXT1E1dGdnYW9qMlp6ZFk2ZzN2SWFHbF9JWUtNdkNIWWNscmt4YUFGTk5MWExLQlJm
aTA2LVk2V3l1dUdxNmpNWk5DbnlKX1pTbUpkVFQwc1Z4RTdGTXVxaUJsMElrRGdyVDdvOFNXMEY5cXFadndEZDJSaDdqNkRJ
WGdkS3VtOWltU2xNU1pjejhueVdic01Udk5yMWY0M25VenJzMHk5WWN6NnBDX0czZmlWYjJsX2VWLVFkcFh4TUo2bnZodXcy
djRiUGVkM3VMQlpaVW1oQ3B6TUVDdW5NMlh1TVBrTGdlS1NqWG44aGhPRFNVcW1WQ0Uta3RZdnRBc2Q0RnJxcGNxWlZiS0Zi
VTFRbU0wV2pMYVJtUk9IVllQVkc0a3FBdTRWalVMUzVCRWszNnZ4Nmp3U3BMUy1IdTcwbVRNcmR3dmV5Q2ZOYkhyT0FlVmVv
ekFIR3JqdGlmaFpmSFVUTWZiNkMtX2tOQVJGQWdDclZTZy0wUzlxb1JvTWVkUENETEE4MDJiaWwtNDJjOC15MWo4X1FVaC02
UUtCV2dodVd4VWtBODRpekFFaWl0QTlsSHFKM3Nxd2JFNURkZmhIay05bTJfTTN5MWlWVkdoRVQ3ZW9XVDBqWllnRGRBQjFz
UGwxLTlaSFNYYmsydTE3SkJVRV9FOXI0V0tWMnBqWGtiN0lQSWgtQ3JWQTZkcVdQRHVIbmx1V19wblNLYnYtTkZVbGQ0WEY3
cmZLYmQySlg4eUhhX05pOVVVUnUwZVdsNWxGRUVabklubmFKZEdHLUZrb3VuN2xHSFlwSE4ydXVudmRnOHZVZzZsa0JPbmoz
eUFjc1ZTMGxKc1NWdUxFYldwd2c4YjdBdDM3d3AtMWt2Y1ZQaWpCQ1lCV181d2JzbTFYd2k4MVc2WHVpNzMzQVg3cEJVQnBf
T2VRNzQ2ZXJJekNUUFZCYUpZUGJuZWEtdFhsU3RmZzBGeVRmbnhnX1Vzazl3QXJkemE4c204T0FQaWMxZmFQOG0uUTdFN0FV
X2xUVnNmZFI2bnkydUdhQSJ9.u2fJrVA55NQC3esPb4kcodt5rnjc1o-5uEDdUf-
KnCYEPBZ7t2CTsMMVVE3nfRhM39MfTlNS-qVOVpuoW_51NYaENXQMxfxlU9aXp944QiU1OeFQKj_g-
n2dEINRStbtUc3KMKqtz38BFf1g2Z51sdlnBn4XyVWPgGCf4XSfsFIa9fF051awQ0LcCv6YQTGer_6nk7t6F1MzPzBZzja1a
bpm--6LNSzjPftEiexpD2oXvW8Vl0Z9ggNk5Pn3Ne4RzqK09J9WChaJSXkTTE5G39EZcePmVNtcbayq-
L2pAK5weDa2k4uYMfAQAwcTOhUrwK3yilwqjHAamcG-CoiPZQ

```
OAuth Refresh Token Expiry Timer" parameter in enterprise parameters page in CUCM.
Path: System -> Enterprise parameters
Values are integers ranging from 1 - 90
Minimum lifetime = 1 Day
Default lifetime = 60 days
Maximum lifetime = 90 days
```

每次客户端请求一个访问令牌时都会发出新的访问令牌。只要：

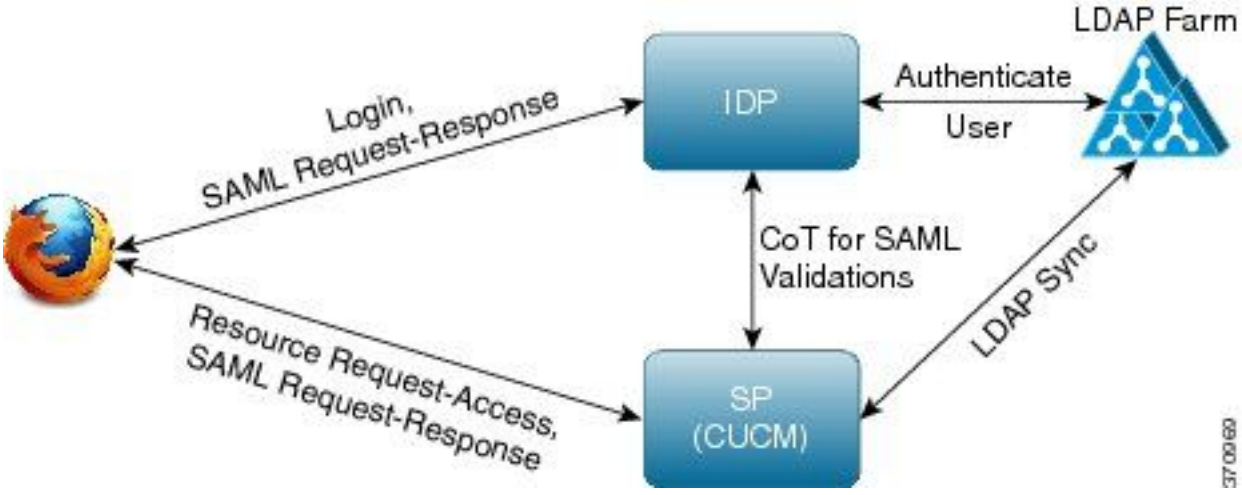
- 签名/加密密钥未更改
- 有效性（存储在令牌内）中断。
- JSON Web令牌：由三个部分组成，用点分隔，分为：报头、负载和签名。

访问令牌示例：

- 在标记的开头，以粗体突出显示的是标题。
- 中间部分是负载。
- 最后，如果标记以粗体突出显示，则表示该标记为签名。

网络图

以下是涉及的呼叫流的简要概述：



刷新令牌

- 刷新令牌已签名。
- 刷新令牌存储在数**据库的**refreshtokendetails表中，作为自身的哈希值。这是为了防止数据库复制，因为某人可以选择它。要查看表，可以运行：
  `run sql select * from refreshtokendetails`
  或者具有可读的有效日期：

  `run sql select pkid,refreshtokenindex,userid,clientid,dbinfo('utc_to_datetime',validity) as validity,state from refreshtokendetails`

```
admin:run sql select * from refreshtokendetails
pkid          refreshtokenindex userid   clientid validity            state
============= ================= ======== ======== =================== ==========
173e2283-1... 65483476618891... bvanturn C1b4b... 2019-01-05 14:11:46 1080686546
cd2c634c-7... 0bf6b2989db114... bvanturn C1b4b... 2019-01-05 14:28:41 569144456
a3706858-b... b4800f20dbfe0e... bvanturn C1b4b... 2019-01-05 14:38:12 1146722445
```

警告：有效期过期时，刷新令牌会从数据库中刷新。计时器线程每天凌晨2点运行（不能通过UI进行配置，但可以通过远程支持帐户进行修改）。如果表具有大量访问令牌，这些令牌无效，需要清空。这可能导致CPU峰值。

Sample refresh token:

```
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6IjhkMGQ1MzI0LWY0ZjAtNGIwYi04MTFlLTRhNTlmZGI2YjcyMjpj
Mjc3MGM5N2JkYTlkMzRmZDA1YTdlYTFhZWQzZTU0Y2E4MGJkZDdlZTM1ZDk3MDNiNjBiNTQ5MTBiZDQ0ODRiIn0.eyJleHAi
OjE1MDI2MjAwNTIsImlzcyI6IjhkMGQ1MzI0LWY0ZjAtNGIwYi04MTFlLTRhNTlmZGI2YjcyMiIsInR5cCI6InVzZXIiLCJ0
aWQiOiJiOTkxMjIxZi1mNDJlLTRlNTItODg3MS1jODc2ZTYzNWRkNWIiLCJjdHlwIjoicmVmcmVzaCIsImNjaWQiOiJDM2Iw
YWZmZWZlMTQzOTA0MTY4M2U5YzJjMzdkMzZmNDM4ZWYwZWYyN2MwOTM4YWRjNjIyNmUwYzAzZDE2OWYyYSJ9.creRusfwSYA
MAtttS2FIPAgIVvCiREvnzlouxeyGVndalJlMa-ZpRqv8FOBrsYwqEyulrl-
TeM8XGGQCUvFaqO9IkhJqSYz3zvFvvySWzDhl_pPyWIQteAhL1GaQkue6a5ZegeHRp1sjEczKMLC6H68CHCfletn5-
j2FNrAUOX99Vg5h4mHvlhfjJEel3dU_rciAIni12e3LOKajkzFxF6W0cXzzujyi2yPbY9gZsp9HoBbkkfThaZQbSlCEpvB3t
7yRfEMIEaHhEUU4M3-uSybuvitUWJnUIdTONiWGRh_fOFR9LV3Iv9J54dbsecpsncc369pYhu5IHwvsglNKEQ
```

撤销刷新令牌

管理员能够通过用户ID或用户ID和客户端ID撤销用户或仅设备刷新令牌**的所**有刷**新令牌**。

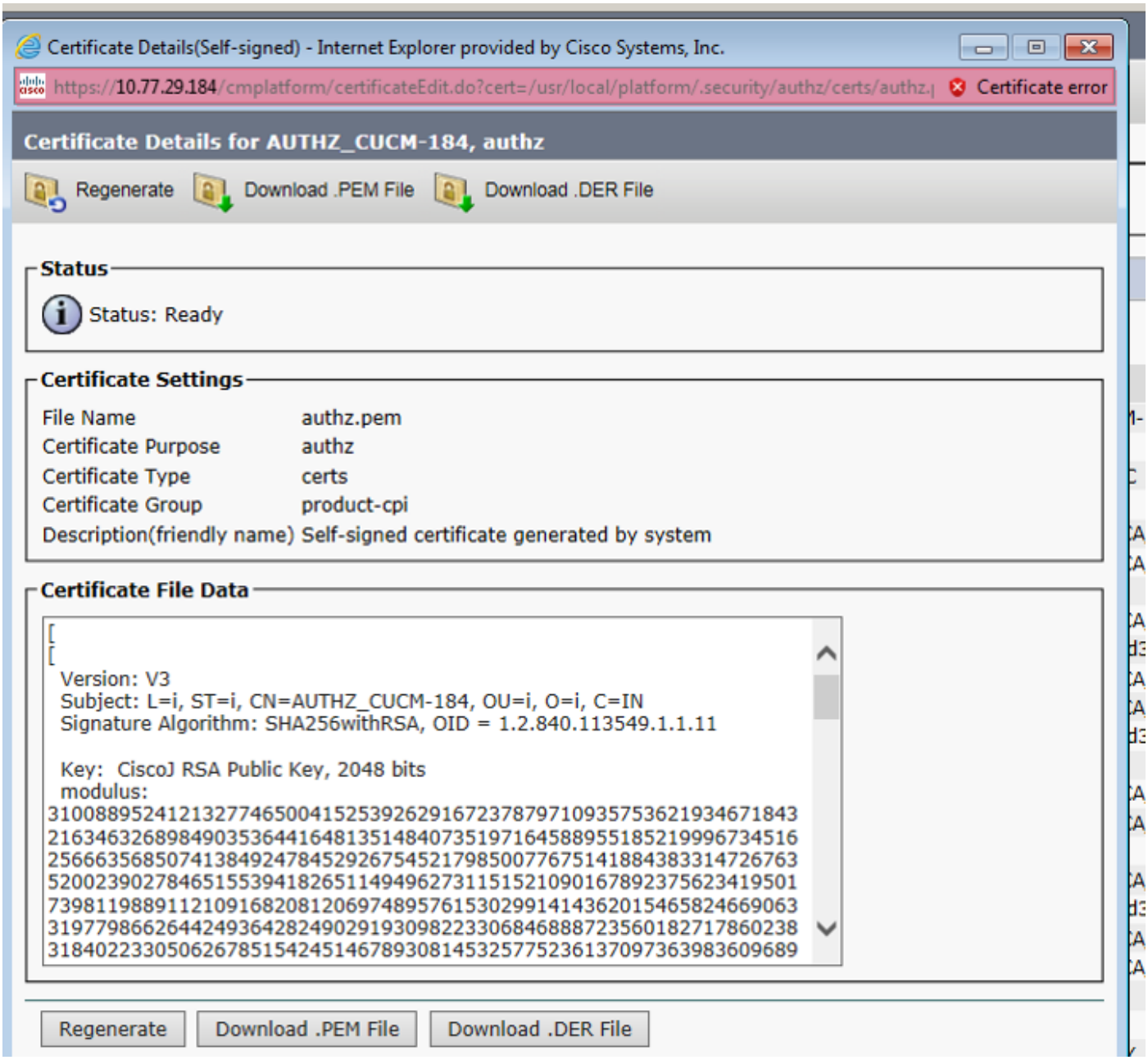
要撤销用户的基于设备的RT:

- 撤消用户xyz和由client_id abc标识的设备的RT。
- https://cucm-193:8443/ssosp/token/revoke?user_id=xyz&client_id=abc

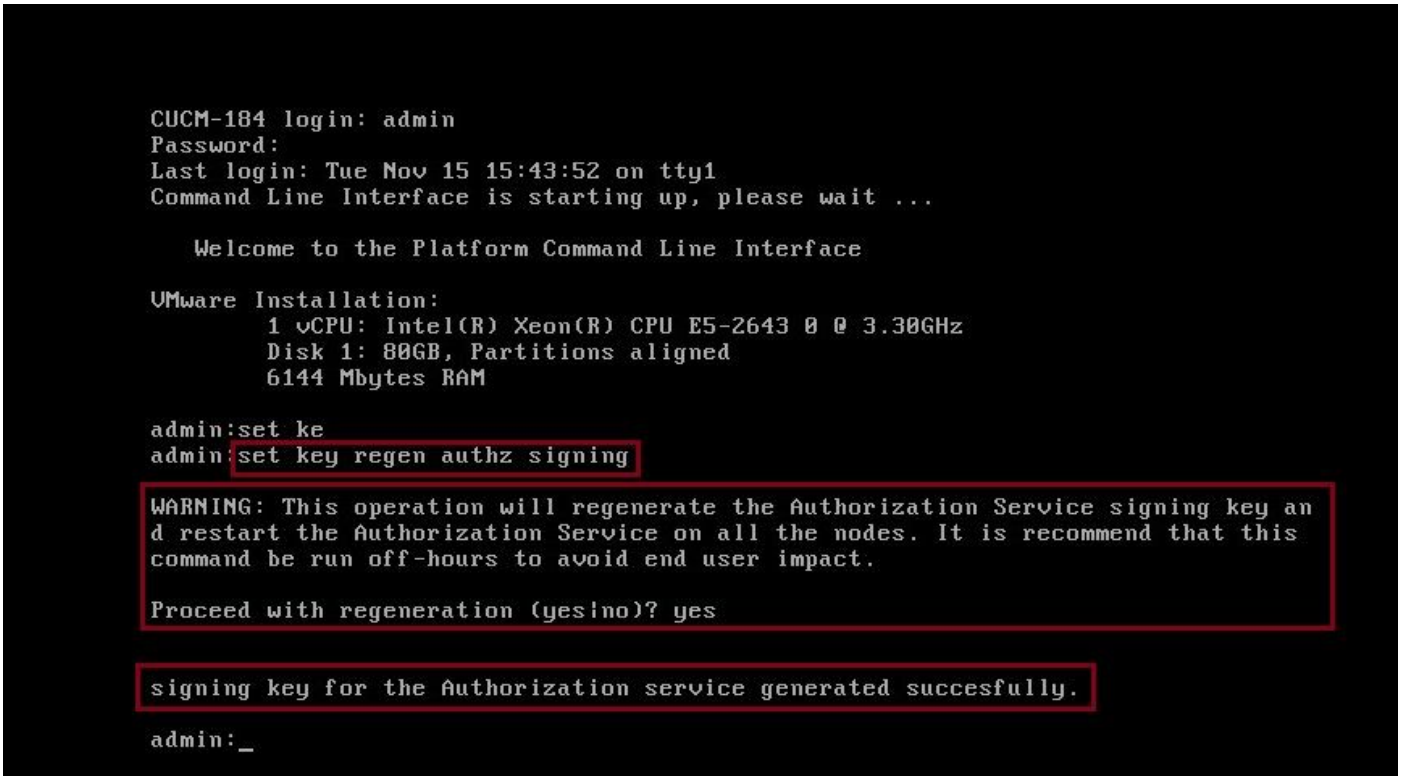
签名和加密密钥

- 签名密钥基于RSA，具有公钥/私钥对。
- 加密密钥是对称密钥。
- 这些密钥仅在发布者上创建，并分布在集群中的所有节点上。
- 使用列出的选项，可以重新生成签名密钥和加密密钥。但是，只有管理员认为密钥已受到危害时，才能执行此操作。重新生成这些密钥中的任一密钥的影响是，由授权服务发出的所有访问令牌都变为无效。
- 可使用UI和CLI重新生成签名密钥。
- 加密密钥只能通过CLI重新生成。

从CUCM上的Cisco Unified OS Administration页面重**新生成Authz证书**(签名密钥)如图所示。



如图所示，使用CLI命令重新生成授权签名密钥。



管理员可以使用CLI显示身份验证签名和加密密钥。将显示密钥的哈希值，而不是原始密钥。

用于显示键的命令是：

签名密钥：**show key authz signing**，如图所示。

```
admin:show key authz signing

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

加密密钥:**show key authz encryption**和，如图所示。

```
admin:show key authz encryption

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

注意：签名身份验证和加密身份验证始终不同。

验证

使用本部分可确认配置能否正常运行。

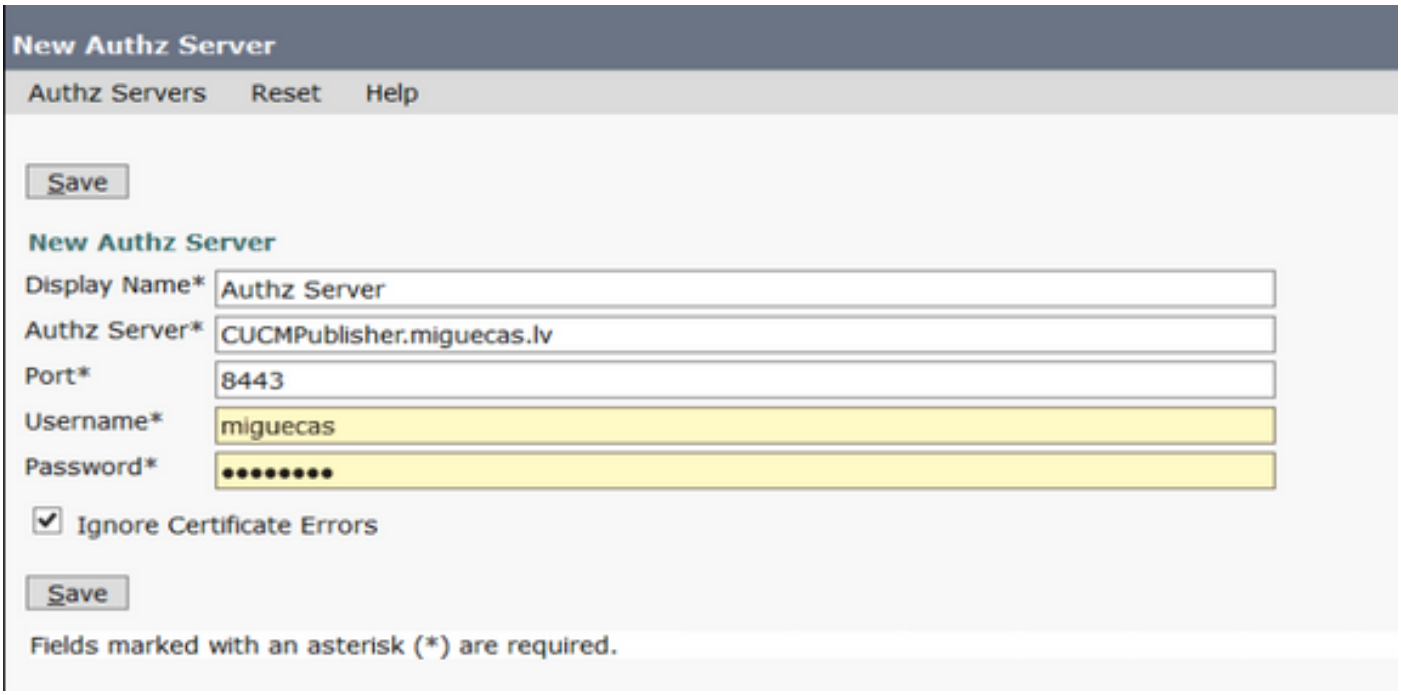
当要在Cisco Unity Connection(CUC)服务器上使用OAuth时，网络管理员必须执行两个步骤。

步骤1.配置Unity Connection服务器以从CUCM获取OAuth令牌签名和加密密钥。

步骤2.在CUC服务器上启用OAuth服务。

注意：要获取签名和加密密钥，必须为Unity配置CUCM主机详细信息和启用CUCM AXL访问的用户帐户。如果未配置，则Unity Server无法从CUCM检索OAuth令牌，用户的语音邮件登录不可用。

导航至Cisco Unity Connection Administration > System Settings > Authz Servers



故障排除

本节提供可用于排除配置故障的信息。

> **注意**：如果使用OAuth且Cisco Jabber用户无法登录，请始终查看CUCM和即时消息和在线状态(IM&P)服务器的签名和加密密钥。

网络管理员需**要**在所有CUCM和IM&P节点上运行以下两个命令：

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

如果签名授权和加密授权输出在所有节点之间不匹配，则需要重新生成。要执行此操作，需要在所有CUCM和IM&P节点上运行以下两个命令：

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

之后，需**要在**所有节点上重新启动Cisco Tomcat服务。

除密钥不匹配外，Cisco Jabber日志中还可以找到以下错误行：

```
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.
```

sso应用日志在以下位置生成：

- **文件视图活动日志**platform/log/ssoApp.log这不需要任何跟踪配置来收集日志。每次完成SSO应用操作后，ssoApp.log文件中都会生成新的日志条目。
- SSOSP日志： **文件列表激活tomcat/logs/ssosp/log4j**

每次启用sso时，都会在此位置创建一个名为ssosp00XXX.log的新日志文件。任何其他SSO操作和所有Oauth操作也会登录到此文件。

- 证书日志： **文件列表activevelog平台/log/certMgmt*.log**
  每次重新生成AuthZ证书（UI或CLI）时，都会为此事件生成新的日志文件。
  为了重新生成授权加密密钥，将为此事件生成新的日志文件。

相关信息

使用思科协作解决方案版本12.0部署OAuth