

通过在思科语音操作系统(VOS)的CLI配置CA签名证书

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[生成CA签名证书](#)

[Summary命令](#)

[检查正确证书信息](#)

[生成证书符号请求\(CSR\)](#)

[生成Tomcat服务器证书](#)

[导入Tomcat证书到思科VOS服务器](#)

[导入 CA 证书](#)

[导入Tomcat证书](#)

[重新启动服务](#)

[验证](#)

[故障排除](#)

[取消规划](#)

[相关条款](#)

简介

本文描述关于怎样的配置步骤上传第三方在所有Cisco语音操作系统(VOS)通过使用命令行界面(CLI)，基于Collaboration Server的Certificate Authority (CA)签名证书。

先决条件

要求

Cisco 建议您了解以下主题：

- 公共密钥基础设施(PKI)基本的了解和其在思科VOS服务器和Microsoft CA的实施
- 预先配置DNS基础设施

使用的组件

本文档中的信息基于以下软件和硬件版本：

- VOS服务器：Cisco Unified Communications Manager (CUCM)版本9.1.2
- CA:Windows 2012服务器
- 客户端浏览器：Mozilla Firefox版本47.0.1

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。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

背景信息

在所有Cisco Unified Communications VOS产品中有至少两个凭证类型：应用程序喜欢(ccmadmin、ccmservice、cuadmin，cfadmin，cuic)和VOS平台(cmplatform、drf，cli)。

在一些特定方案中通过网页管理应用程序和通过line命令执行平台涉及的活动是非常方便的。在您之下可以查找关于怎样的一个步骤通过CLI独自地导入第三方签名证书。在此示例Tomcat证书上传。对于CallManager或其他应用程序它查找同样。

生成CA签名证书

Summary命令

用于条款的命令的列表。

```
show cert list own
show cert own tomcat
```

```
set csr gen CallManager
show csr list own
show csr own CallManager
```

```
show cert list trust
set cert import trust CallManager
set cert import own CallManager CallManager-trust/allevich-DC12-CA.pem
```

检查正确证书信息

列出所有上传的信任证书。

```
admin:show cert list own
```

```
tomcat/tomcat.pem: Self-signed certificate generated by system
ipsec/ipsec.pem: Self-signed certificate generated by system
CallManager/CallManager.pem: Certificate Signed by allevich-DC12-CA
CAPF/CAPF.pem: Self-signed certificate generated by system
TVS/TVS.pem: Self-signed certificate generated by system
```

检查谁发出Tomcat服务的证书。

```
admin:show cert own tomcat
```

```
[
  Version: V3
  Serial Number: 85997832470554521102366324519859436690
  SignatureAlgorithm: SHA1withRSA (1.2.840.113549.1.1.5)
  Issuer Name: L=Krakow, ST=Malopolskie, CN=ucm1-1.allevich.local, OU=TAC, O=Cisco, C=PL
  Validity From: Sun Jul 31 11:37:17 CEST 2016
               To:   Fri Jul 30 11:37:16 CEST 2021
  Subject Name: L=Krakow, ST=Malopolskie, CN=ucm1-1.allevich.local, OU=TAC, O=Cisco, C=PL
```

Key: RSA (1.2.840.113549.1.1.1)

Key value: 3082010a0282010100a2

<output omitted>

因为发布者匹配主题，这是自签名证书。

生成证书符号请求(CSR)

生成CSR。

```
admin:set csr gen tomcat
```

```
Successfully Generated CSR for tomcat
```

验证证书符号request顺利地生成。

```
admin:show csr list own
```

```
tomcat/tomcat.csr
```

打开它并且复制内容到文本文件。保存它，`tac_tomcat.csr`文件。

```
admin:show csr own tomcat
```

```
-----BEGIN CERTIFICATE REQUEST-----
```

```
MIIDSjCCAjICAQAwb0xCzAJBgNVBAYTA1BMMRQwEgYDVQQLIEwtNYWxvcG9sc2tp
ZTEPMA0GA1UEBxMGS3Jha293MQ4wDAYDVQQKEwVDaXNjbzEMMAoGA1UECxDVFEFD
MR4wHAYDVQDExv1Y20xLTEuYWxsZXZpY2gubG9jYWxsSTBHBGVBVAUTQDlhMWJk
NDA5M2VjOGYxNj1jODhmNGUyZTYwZTYzM2RjNj1hZmFkNDY1YTgzMDhkNjRhNGU1
MzExOGQ0YjZkZjcwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCVo5jh
lMqTUnYbHQUnYPt00PTflWbj7hi6PSYI7pVCbGUZBpIZ5PKwTD56OZ8SgppjYX5Pf
l9D09H2gtQJTMVv1GmleGdlJsbuABRKn6lWkO6b706MiGSgqel+41vnItjn3Y3kU
7h51nruJye3HpPQzvXXpOKJ/JeJc8InEvQcC/UQmFMKn0ul00veFBHnG7TLDwDaQ
W1A11rwrezN9Lwn2a/XZQR1P65sjmnkFFF2/FON4BmooeiiNJD0G+F4bKig1ymLR
84faF27plwHjcw8WAn2HwJT607TaE6EOJd0sgLU+HFAl3txKycS0NvLuMZYQH81s
/C74CIRWibEWT2qLAgMBAAGgRzBFBgkqhkiG9w0BCQ4xODAMCccGA1UdJQQgMB4G
CCsGAQUFBwMBBggrBgEFBQcDAGYlKwYBBQUHAWUwCwYDVR0PBAQDAgO4MA0GCSqG
SIb3DQEBBQUAA4IBAQBUu1FhKuyQ1X58A6+7KPkYsWtioS0PoycltuQsVo0aav82
PiJkCvzWTeo6v9qG0nnaI53e15+RPpWxpEgAIPPhtt6asDuW30SqSx4eClfgmKH
ak/tTuWmZbfyk2iqNFy0YgYTeBkG3AqPwWUCNoduPZ0/fo41QoJPwje184U64WXB
gCzhIHfsV5DzYp3IR5C13hEa5fDgpD2ubQWja2LId85NGHEiqyiWqgmt07pTkBc+
7ZKa6fKnpACehrtVqEn02jOi+sanfQKGQqH8VYMFsW2uYFj9pf/Wn4aDGuJoqdOH
StV2Eh0afxPEq/1rQP3/rzq4NMY1J7glyNFGPUVP
```

```
-----END CERTIFICATE REQUEST-----
```

生成Tomcat服务器证书

生成Tomcat服务的一证书在CA。

打开的网页认证机关在浏览器。放置正确凭证在验证提示符。

<http://dc12.allewich.local/certsrv/>

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see [Active Directory Certificate Services Documentation](#).

Select a task:

[Request a certificate](#)

[View the status of a pending certificate request](#)

[Download a CA certificate, certificate chain, or CRL](#)

下载CA根证明。选择**下载CA证书、证书链或者CRL**菜单。在Next菜单请从列表选择适当的CA。编码方法应该是Base64。下载CA证书并且保存它到有命名ca.cer的操作系统。

按**请求证书**然后**提前的证书请求**。设置**认证模板**为Web服务器并且粘贴CSR内容从文本文件tac_tomcat.csr如显示。

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
PiJkCvzWTeEo6v9qG0nnaI53e15+RPpWxpEgAIPP
ak/tTuWmZbfyk2iqNFy0YgYTeBkG3AqPwWUCNodu
gCzhIHfsV5DzYp3IR5C13hEa5fDgpD2ubQWja2LI
7ZKa6fKnpACehrtVqEn02jOi+sanfQKGQqH8VYMF
StV2Eh0afxPEq/1rQP3/rzq4NMYlJ7glyNFGPUVP
-----END CERTIFICATE REQUEST-----
```

Certificate Template:

Web Server

Additional Attributes:

Attributes:

Submit >

提示：如果操作在实验室里完成(或思科VOS服务器和CA在)节省时间的同一管理域下复制和插入从存储器缓冲区的CSR。

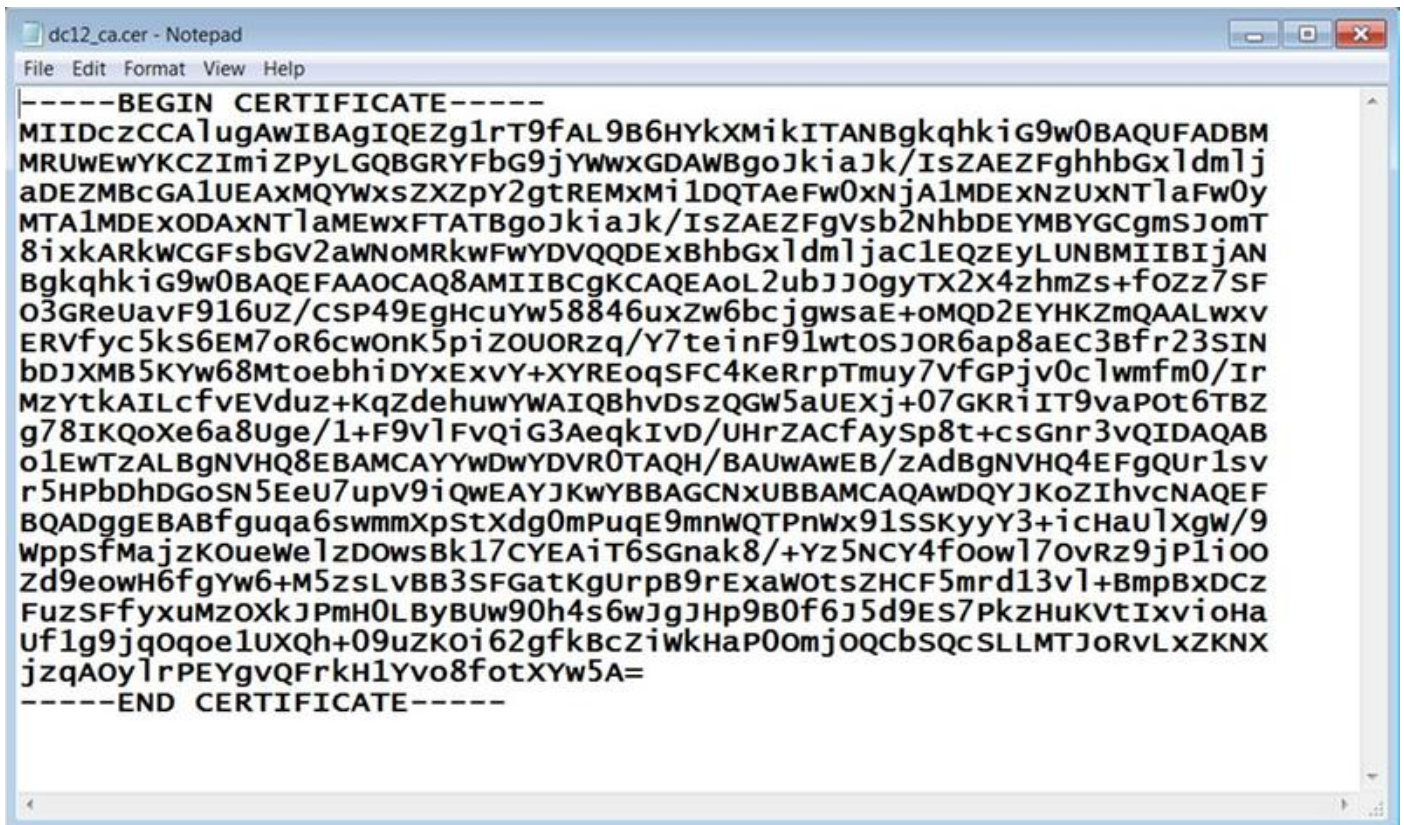
按提交。选择**Base64编码**的选项并且下载Tomcat服务的证书。

注意：如果证书生成进行散装请保证更改证书的名称到一个有意义的。

导入Tomcat证书到思科VOS服务器

导入 CA 证书

打开存储与命名**ca.cer**的CA证书。必须首先导入它。



复制其内容到缓冲区并且键入以下in命令CUCM CLI：

```
admin:set cert import trust tomcat
```

Paste the Certificate and Hit Enter

粘贴CA证书的提示符将显示。粘贴它如下所示。

```
admin:set cert import trust tomcat
```

Paste the Certificate and Hit Enter

万一信任认证加载是成功的此输出将显示。

```
admin:set cert import trust tomcat
```

Paste the Certificate and Hit Enter

验证CA证书顺利地导入作为Tomcat托拉斯一。

```
admin:show cert list trust
```

```
tomcat-trust/ucml-1.pem: Trust Certificate
tomcat-trust/allevich-win-CA.pem: w2008r2 139
<output omitted for brevity>
```

导入Tomcat证书

下一步是导入Tomcat CA签名证书。操作查找同一样与Tomcat托拉斯cert，命令不同的。

```
set cert import own tomcat tomcat-trust/allevich-DC12-CA.pem
```

重新启动服务

并且请最后重新启动Tomcat服务。

```
utils service restart Cisco Tomcat
```

警告：记住它打乱Web服务器从属的服务的操作，类似Extension Mobility、未接呼叫，公司目录和其他。

验证

验证生成的证书。

```
admin:show cert own tomcat
```

```
[
  Version: V3
  Serial Number: 2765292404730765620225406600715421425487314965
  SignatureAlgorithm: SHA1withRSA (1.2.840.113549.1.1.5)
  Issuer Name: CN=allevich-DC12-CA, DC=allevich, DC=local
  Validity From: Sun Jul 31 12:17:46 CEST 2016
                To: Tue Jul 31 12:17:46 CEST 2018
  Subject Name: CN=ucm1-1.allevich.local, OU=TAC, O=Cisco, L=Krakow, ST=Malopolskie, C=PL
  Key: RSA (1.2.840.113549.1.1.1)
  Key value: 3082010a028201010095a
```

保证发证者名字属于修建该证书的CA。

登陆对网页通过键入服务器的FQDN在浏览器的，并且证书警告不会显示。

故障排除

此条款目标是给与命令语法的一个步骤关于怎样通过CLI上传证书，不突出显示逻辑公共密钥Infrastructure (PKI)。它不包括SAN证书、辅助CA、4096证书密钥长度和许多其他方案。

少许罕见的情况，当上传Web服务器证书通过CLI操作失效与无法的错误消息“读CA证书”时。那的一应急方案是安装证书使用网页。

一非标准的认证机关配置可能导致与认证安装的问题。设法生成和安装从另一个CA的证书与一个基本默认配置。

取消规划

万一将有需要生成自签名证书在CLI可能也执行。

键入下面命令，并且Tomcat证书将被重新生成到自己签署的一个。

```
admin:set cert regen tomcat
```

```
WARNING: This operation will overwrite any CA signed certificate previously imported for tomcat
```

```
Proceed with regeneration (yes|no)? yes
Successfully Regenerated Certificate for tomcat.
```

You must restart services related to tomcat for the regenerated certificates to become active.
必须重新启动要运用新证书Tomcat服务。

```
admin:utils service restart Cisco Tomcat
```

```
Don't press Ctrl-c while the service is getting RESTARTED.If Service has not Restarted
```

Properly, execute the same Command Again

```
Service Manager is running
Cisco Tomcat[STOPPING]
Cisco Tomcat[STOPPING]
Commanded Out of Service
Cisco Tomcat[NOTRUNNING]
Service Manager is running
Cisco Tomcat[STARTING]
Cisco Tomcat[STARTING]
Cisco Tomcat[STARTED]
```

相关条款

[加载证书通过网页](#)

[步骤获得并上载Windows服务器赛弗-签字的或Certificate Authority \(CA\)...](#)