

# Certificado firmado de CA de la configuración vía el CLI en el sistema operativo de la Voz de Cisco (VOS)

## Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Genere el certificado firmado de CA](#)

[Comandos summary](#)

[Información correcta del certificado del control](#)

[Genere la petición de la muestra del certificado \(el CSR\)](#)

[Genere el certificado de servidor de Tomcat](#)

[Importe el certificado de Tomcat al servidor de Cisco VOS](#)

[Importe el certificado de CA](#)

[Importe el certificado de Tomcat](#)

[Reiniciar el servicio](#)

[Verificación](#)

[Troubleshooting](#)

[Se retira el plan](#)

[Artículos relacionados](#)

## Introducción

Este documento describe los pasos para la configuración en cómo cargar el certificado firmado del Certificate Authority (CA) de las de otras compañías en cualquier Collaboration Server basado del sistema operativo de la Voz de Cisco (VOS) usando el comando line interface(cli).

## Prerrequisitos

### Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Comprensión básica del Public Key Infrastructure (PKI) y de su implementación en los servidores de Cisco VOS y Microsoft CA
- Se preconfigura la infraestructura DNS

## Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Servidor VOS: Versión 9.1.2 del administrador de las Comunicaciones unificadas de Cisco (CUCM)
- CA: Servidor de Windows 2012
- Buscador del cliente: Versión 47.0.1 de Firefox del Mozilla

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

## Antecedentes

En todo el Cisco los Productos unificados de Communications VOS allí son por lo menos dos tipos de las credenciales: la aplicación tiene gusto (ccmadmin, ccmervice, cuadmin, cfadmin, cuic) y plataforma VOS (cmplatform, drf, cli).

En algunos escenarios específicos es muy conveniente manejar las aplicaciones vía la página web y realizar las actividades relacionadas plataforma vía la línea de comando. Debajo de usted puede encontrar un procedimiento en cómo importar el certificado firmado de las de otras compañías solamente vía el CLI. En este Tomcat del ejemplo el certificado está cargado. Para el CallManager o cualquier otra aplicación mira lo mismo.

## Genere el certificado firmado de CA

### Comandos summary

Una lista de los comandos usados en el artículo.

```
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
```

### Información correcta del certificado del control

Enumere todos los certificados confiables cargados.

```
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

Marque quién publicó el certificado para el servicio de Tomcat.

```
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>
```

Esto es un certificado autofirmado puesto que el emisor hace juego el tema.

## Genere la petición de la muestra del certificado (el CSR)

Genere el CSR.

```
admin:set csr gen tomcat
Successfully Generated CSR for tomcat
```

Verifique que el request de la muestra del certificado fuera generado con éxito.

```
admin:show csr list own
tomcat/tomcat.csr
```

Ábralo y copie el contenido al archivo de texto. Sávelo como archivo `tac_tomcat.csr`.

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

```
-----BEGIN CERTIFICATE REQUEST-----
MIIDSjCCAjICAQAwgb0xCzAJBgNVBAYTAlBMMRQwEgYDVQQIEwtNYWxvcG9sc2tp
ZTEPMA0GA1UEBxMGS3Jha293MQ4wDAYDVQQKEwVDaXNjbzEMMAoGA1UECxDVFEFD
MR4wHAYDVQQDExV1Y20xLTEuYWxsZXZpY2gubG9jYXNjbzEMMAoGA1UECxDVFEFD
NDA5M2VjOGYxNj1jODhmNGUyZTYwZTYzM2RjNj1hZmFkNDY1YTgzMDhkNjRhNGU1
MzExOGQ0YjZkZjcwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCvO5jh
lMqTUnYbHQUnYPt00PTflWbj7hi6PSYI7pVCbGUZBpIZ5PKwTD56OZ8SgppjYX5Pf
l9D09H2gtQJTMVv1GmleGdlJsbuABRKn6lWkO6b706MiGSgqel+41vnItjn3Y3kU
7h51nrUjYe3HpPQzvXXpOKJ/JeJc8InEvQcC/UQmFMKn0ul00veFBHnG7TLDwDaQ
WlA1lrwrezN9Lwn2a/XZQR1P65sjmnkFFF2/FON4BmooeiINJD0G+F4bKiglymLR
84faF27plWhjcw8Wan2HwJT607TaE6EOJd0sgLU+HFAI3txKycS0NvLuMZYQH81s
/C74CIRWibEWT2qLAgMBAAGgRzBFBGkqhkiG9w0BCQ4xODAMCmGAlUdJQQgMB4G
CCsGAQUFBwMBBggrBgEFBQcDAGYIKwYBBQUHAWUwCwYDVDR0PBAQDAgO4MA0GCSqG
SIb3DQEBBQUAA4IBAQBULFhKuyQ1X58A6+7KPkySwtioS0PoycltuQsVo0aav82
PiJkCvzWTeEo6v9qG0nnaI53e15+RPPWxpEgAIPPhht6asDuW30SqSx4eClfgmKH
ak/tTuWmZbfyk2iqNFy0YgYTeBkG3AqPwWUCNoduPZ0/fo41QoJPwje184U64WXB
gCzhIHfsV5DzYp3IR5C13hEa5fDgpD2ubQWja2LId85NGHEiqyiWqwm07pTkBc+
7ZKa6fKnpACehrtVqEn02jOi+sanfKQGQqH8VYMFsW2uYFj9pf/Wn4aDGUJoqdOH
StV2Eh0afxPEq/1rQP3/rzq4NMYlJ7glyNFGPUVP
-----END CERTIFICATE REQUEST-----
```

## Genere el certificado de servidor de Tomcat

Genere un certificado para el servicio de Tomcat en CA.

Abra la página web para el Certificate Authority en un navegador. Ponga las credenciales correctas en el prompt de la autenticación.

## 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](#)

---

Descargue el certificado raíz de CA. Seleccione la **descarga un certificado de CA, una Cadena de certificados, o un menú CRL**. En el menú siguiente elija CA apropiado de la lista. El método de codificación debe ser **base 64**. Descargue el certificado de CA y sávelo al sistema operativo con el nombre **ca.cer**.

Presione la **petición un certificado** y un **pedido de certificado** entonces **avanzado**. Fije el **Certificate Template plantilla de certificado** al servidor Web y pegue el contenido CSR del archivo de texto **tac\_tomcat.csr** como se muestra.

## 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):	<pre>PiJkCvzWTeEo6v9qG0nnaI53e15+RPpWxpEgAIPP ak/tTuWmZbfyk2iqNFy0YgYTeBkG3AqPwWUCNodu gCzhIHfsV5DzYp3IR5C13hEa5fDgpD2ubQWja2LI 7ZKa6fKnpACehrtVqEn02jOi+sanfQKGQqH8VYMF StV2Eh0afxPEq/1rQP3/rzq4NMYlJ7glyNFGPUVP -----END CERTIFICATE REQUEST-----</pre>
---	---

### Certificate Template:

Web Server

### Additional Attributes:

Attributes:

Submit >

Consejo: Si la operación se hace en el laboratorio (o el servidor de Cisco VOS y CA está bajo mismo dominio administrativo) para salvar la copia del tiempo y para pegar el CSR de memoria intermedia.

La prensa **somete**. Seleccione la opción **codificada base 64** y descargue el certificado para el servicio de Tomcat.

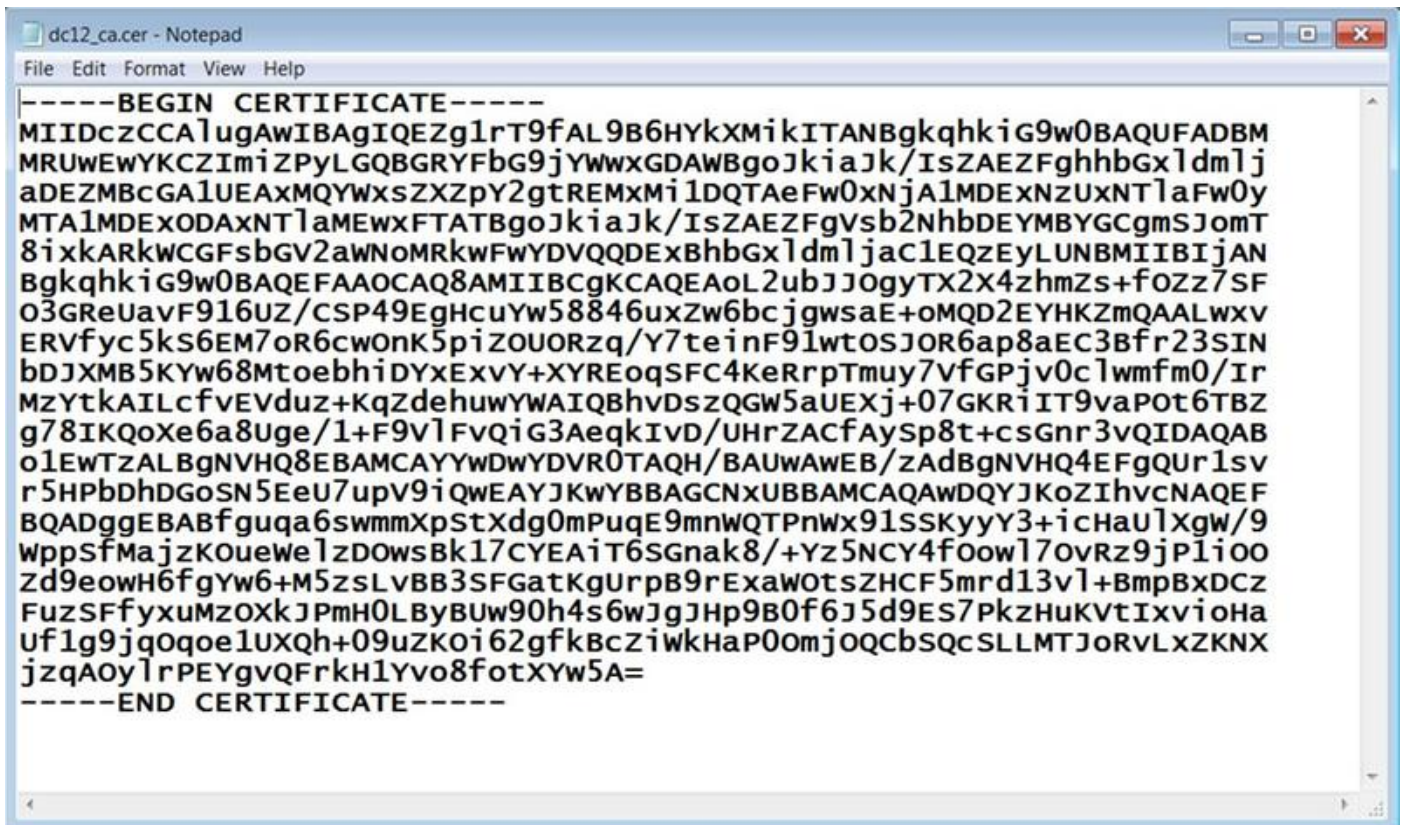
Nota: Si la generación del certificado se realiza en el bulto asegure para cambiar un nombre del certificado meaningful.

## Importe el certificado de Tomcat al servidor de Cisco VOS

### Importe el certificado de CA

Abra el certificado de CA que fue salvado con un nombre **ca.cer**. Debe ser importado primero.





Copie su contenido al buffer y teclee el siguiente comando en el CUCM CLI:

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

Paste the Certificate and Hit Enter

El prompt para pegar el certificado de CA será visualizado. Pegúelo como se muestra abajo.

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

Paste the Certificate and Hit Enter

En caso de que una carga del certificado de confianza sea acertada esta salida será visualizada.

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

Paste the Certificate and Hit Enter

Verifique que el certificado de CA esté importado con éxito como Tomcat-confianza una.

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

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

## Importe el certificado de Tomcat

El siguiente paso es importar el certificado firmado de Tomcat CA. La operación mira lo mismo que con el CERT de la Tomcat-confianza, apenas el comando es diferente.

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

## Reiniciar el servicio

Y recomience pasado el servicio de Tomcat.

```
utils service restart Cisco Tomcat
```

Precaución: Tenga en cuenta que interrumpe la operación de los servicios dependientes del servidor Web, como la movilidad de la extensión, las llamadas faltadas, Corporate Directory (Directorio corporativo) y el otros.

## Verificación

Verifique el certificado que fue generado.

```
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=ucml-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
```

Asegúrese de que el nombre del emisor pertenezca a CA que construyó ese certificado.

Inicie sesión a la página web tecleando el FQDN del servidor en un navegador y no se visualizará ninguna advertencia del certificado.

## Troubleshooting

La meta de este artículo es dar un procedimiento con la sintaxis de los comandos en cómo cargar el certificado vía el CLI, para no resaltar la lógica de la clave pública Infrastructure (PKI). No cubre el certificado SAN, CA subordinado, la longitud de clave de 4096 certificados y muchos otros escenarios.

En algunos casos pocos probables al cargar un certificado del servidor Web vía el CLI la operación falla con un mensaje de error “incapaz de leer el certificado de CA”. Una solución alternativa para ésta es instalar el certificado usando la página web.

Una configuración no estándar del Certificate Authority puede llevar al problema con la instalación del certificado. Intente generar y instalar el certificado de otro CA con una configuración predeterminada básica.

## Se retira el plan

En caso de que haya una necesidad de generar un certificado autofirmado puede también ser hecho en el CLI.

Teclee el comando abajo y el certificado de Tomcat será regenerado uno mismo-firmado.

```
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.  
**Para aplicar un nuevo servicio de Tomcat del certificado debe ser recomenzada.**

```
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]
```

## Artículos relacionados

[Certificado de la carga vía la página web](#)

[Procedimiento para obtener y para cargar el - del uno mismo del Servidor Windows firmado o el Certificate Authority \(CA\)...](#)