Contenido

Introducción

Este documento describe cómo identificar si el certificado firmado del Certificate Authority (CA) hace juego la solicitud de firma del certificado existente (CSR) para Cisco unificó a los servidores de aplicaciones.

Prerrequisitos

Requisitos

Reccommends de Cisco que usted tiene el conocimiento de X.509/CSR.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

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

Una petición de la certificación consiste en un nombre distintivo, una clave pública, y un conjunto opcional de los atributos, firmado colectivamente por la entidad que pide la certificación. Las peticiones de la certificación se envían a las autoridades de certificación que transforman la petición en un certificado de la clave pública X.509. En qué forma las autoridades de certificación vuelven nuevamente el certificado firmado está fuera del ámbito de este documento. PKCS-7 un mensaje es un possibility.(RFC:2986)

Administración de certificados del administrador de comunicaciones de Cisco

La intención de incluir un conjunto de los atributos es doble:

- Para proporcionar la otra información sobre una entidad dada, o una contraseña de impugnación por la cual la entidad puede pedir más adelante la revocación de certificado.
- Para proporcionar los atributos para la inclusión en los Certificados X.509. Los servidores actuales UC no soportan una contraseña de impugnación.

Los servidores actuales de Cisco UC requieren estos atributos en un CSR tal y como se muestra en de esta tabla:

Información	Descripción
orgunit	unidad organizativa
orgname	nombre de organización
lugar	ubicación de la organización
estado	estado de la organización
país	el código del país no puede ser cambiado
alternatehostname	nombre del host alterno

Productos Relacionados

Este documento se puede también utilizar con estas versiones de software y hardware:

- Administrador de las Comunicaciones unificadas de Cisco (CUCM)
- Cisco unificó IM y la presencia
- Cisco unificó el Unity Connection
- CUIS
- Cisco Meidasence
- Cisco Unified Contact Center Express (UCCX)

Problema

En soportar el UC, usted encuentra muchos casos donde el certificado firmado de CA no puede ser cargado en los servidores UC. Usted no puede identificar siempre qué ha ocurrido durante la creación del certificado firmado, puesto que usted no es la persona que utilizó el CSR para crear el certificado firmado. En la mayoría de los escenarios, la re-firma de un nuevo certificado tarda más de 24 horas. Los servidores UC tales como CUCM no han detallado el registro/la traza para ayudar a identificar porqué la carga del certificado falla pero apenas dan un mensaje de error. Este artículo se piensa para ayudar a estrecharse abajo del problema, si es un servidor UC o un problema de CA.

Práctica general para los Certificados CA-firmados en CUCM

CUCM soporta la integración con los CA de tercera persona usando PKCS-10 un mecanismo CSR que sea accesible en el Certificate Manager GUI del sistema operativo de las Comunicaciones unificadas de Cisco. Los clientes, que utilizan actualmente los CA de tercera

persona deben utilizar el mecanismo CSR para publicar los Certificados para el Cisco CallManager, el CAPF, el IPSec, y Tomcat.

Paso 1. Cambie la identificación antes de generar el CSR

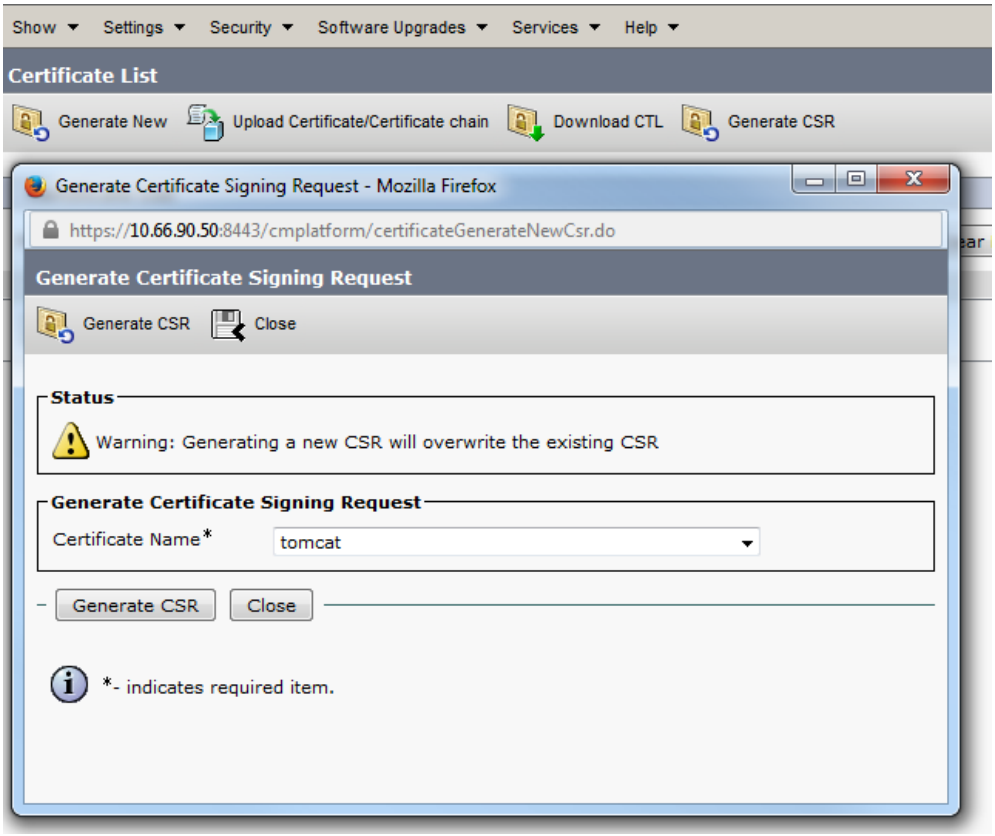
La identidad del servidor CUCM para generar un CSR se puede modificar usando la red-**Seguridad del** comando set tal y como se muestra en de esta imagen.

```
admin:set web-security  ?
Syntax:
set web-security orgunit orgname locality state [country] [alternatehostname]
orgunit  mandatory   organizational unit
orgname  mandatory   organizational name
locality mandatory   location of organization
state    mandatory   state of organization
country  optional    country code can not be changed
alternatehostname  optional   alternate host name

admin:set web-security
```

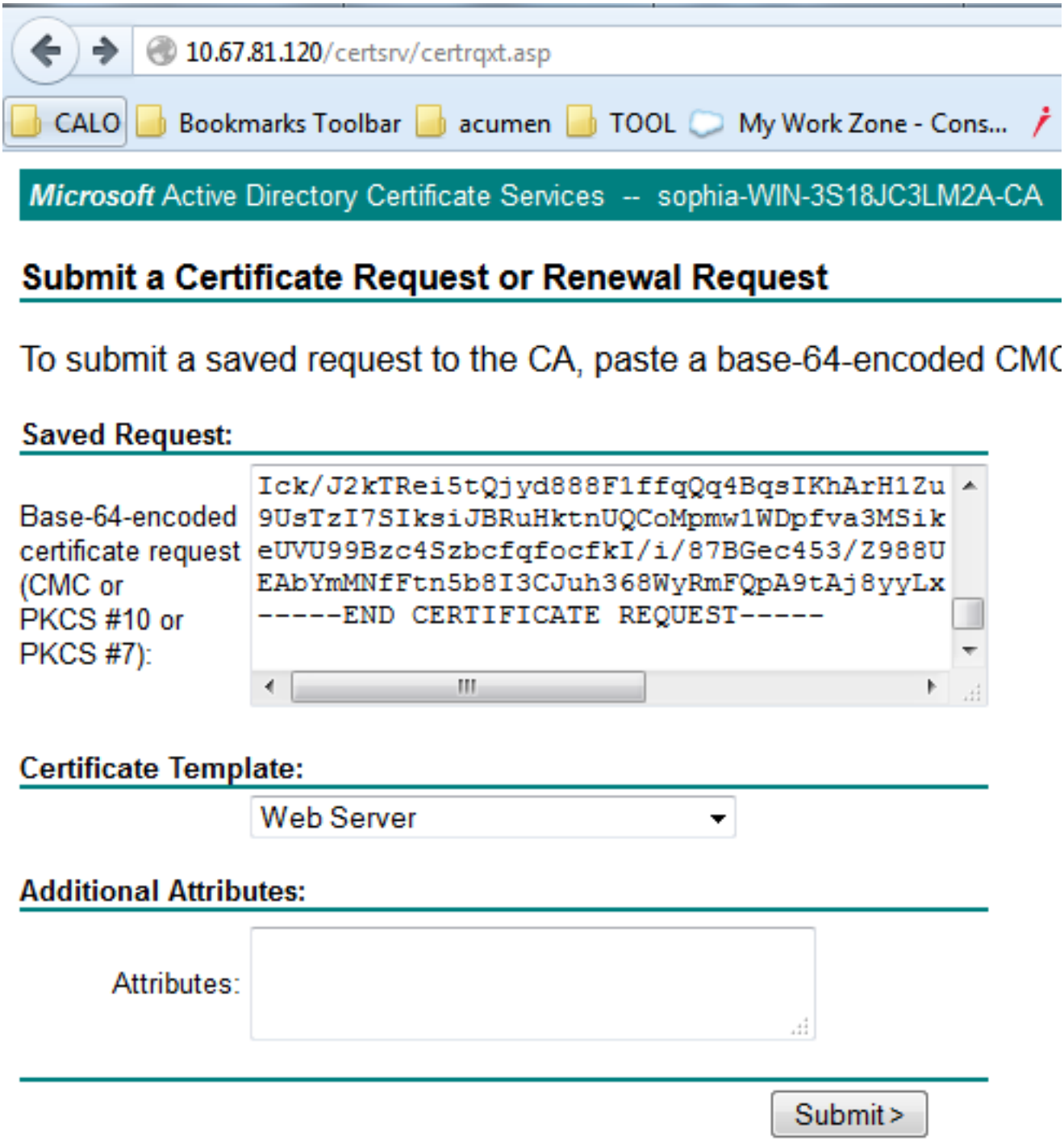
¿Si usted tiene espacio en los campos antedichos, utilice por favor?? para alcanzar el comando como:

```
admin:set web-security "Cisco Systems" "Cisco TAC" "St Leonard" NSW AU CUCM105.sophia.li

WARNING: Country code can not be changed.
Country code for existing web-security is : AU

WARNING: This operation creates self signed certificate for web access (tomcat) with the
r, certificates for other components (ipsec, callmanager, CAPF, etc.) still contain the o
erate these self-signed certificates to update them.

Regenerating web security certificates please wait ...

WARNING: This operation will overwrite any CA signed certificate previously imported for
Proceed with regeneration (yes|no)?
```

Paso 2. Genere el CSR.

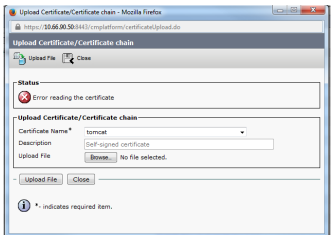


Paso 3. Descargue el CSR y consígalo firmado por CA.



Paso 4. Cargue certificado firmado por CA al servidor.

Una vez que se genera el CSR y se firma el certificado, si usted no puede cargarlo con un **error de lectura del** mensaje de error el **certificado** (tal y como se muestra en de esta imagen), después usted necesita marcar si el CSR esté regenerado o si el certificado firmado sí mismo es la causa del problema.



Hay tres maneras de marcar si el CSR está regenerado o el certificado firmado sí mismo es la causa del problema.

Solución 1. Utilice el comando del OpenSSL en la raíz (o el linux)

1. Inicie sesión a la raíz y navegue a la carpeta.

```
[root@CCM105PUB keys]# pwd
/usr/local/platform/.security/tomcat/keys
[root@CCM105PUB keys]# ls -thl
total 28K
-rwxr-xr-x. 1 certbase ccmbase 1.7K Sep  1 23:22 tomcat_priv_csr.pem
-rwxr-xr-x. 1 certbase ccmbase 1.2K Sep  1 23:22 tomcat_priv_csr.der
-rwxr-xr-x. 1 certbase ccmbase 1.4K Sep  1 23:22 tomcat.csr
-rwxr-xr-x. 1 certbase ccmbase 1.2K Aug 13 16:11 tomcat_priv.der
-rwxr-xr-x. 1 certbase ccmbase 1.7K Aug 13 16:11 tomcat_priv.pem
-rwxr-xr-x. 1 certbase ccmbase   16 Apr 26 15:10 tomcat-trust.passphrase
-rwxr-xr-x. 1 certbase ccmbase   16 Apr 26 15:10 tomcat.passphrase
[root@CCM105PUB keys]#
```

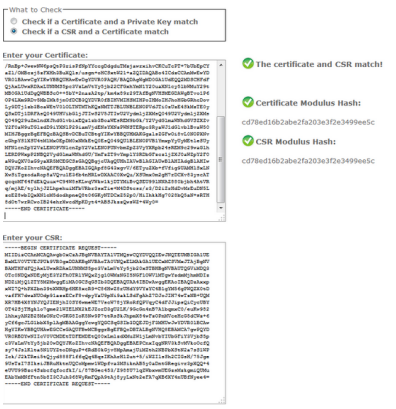
2. Copie el certificado firmado a la misma carpeta usando FTP seguro (SFTP). Si usted no puede configurar a un servidor SFTP, después cargarlo a la carpeta TFTP también consigue el certificado sobre el CUCM.

```
[root@CCM105PUB keys]# sftp cisco@10.66.90.19
bash: sftp: command not found
[root@CCM105PUB keys]# sftp cisco@10.66.90.19
Connecting to 10.66.90.19...
Authenticated with partial success.
cisco@10.66.90.19's password:
Hello, I'm freeFTPd 1.0sftp> get tomcat.cer
Fetching /tomcat.cer to tomcat.cer
/tomcat.cer                                   100% 2140     2.1KB/s   00:00
sftp>
```

3. Marque el MD5 para el CSR y el certificado firmado.

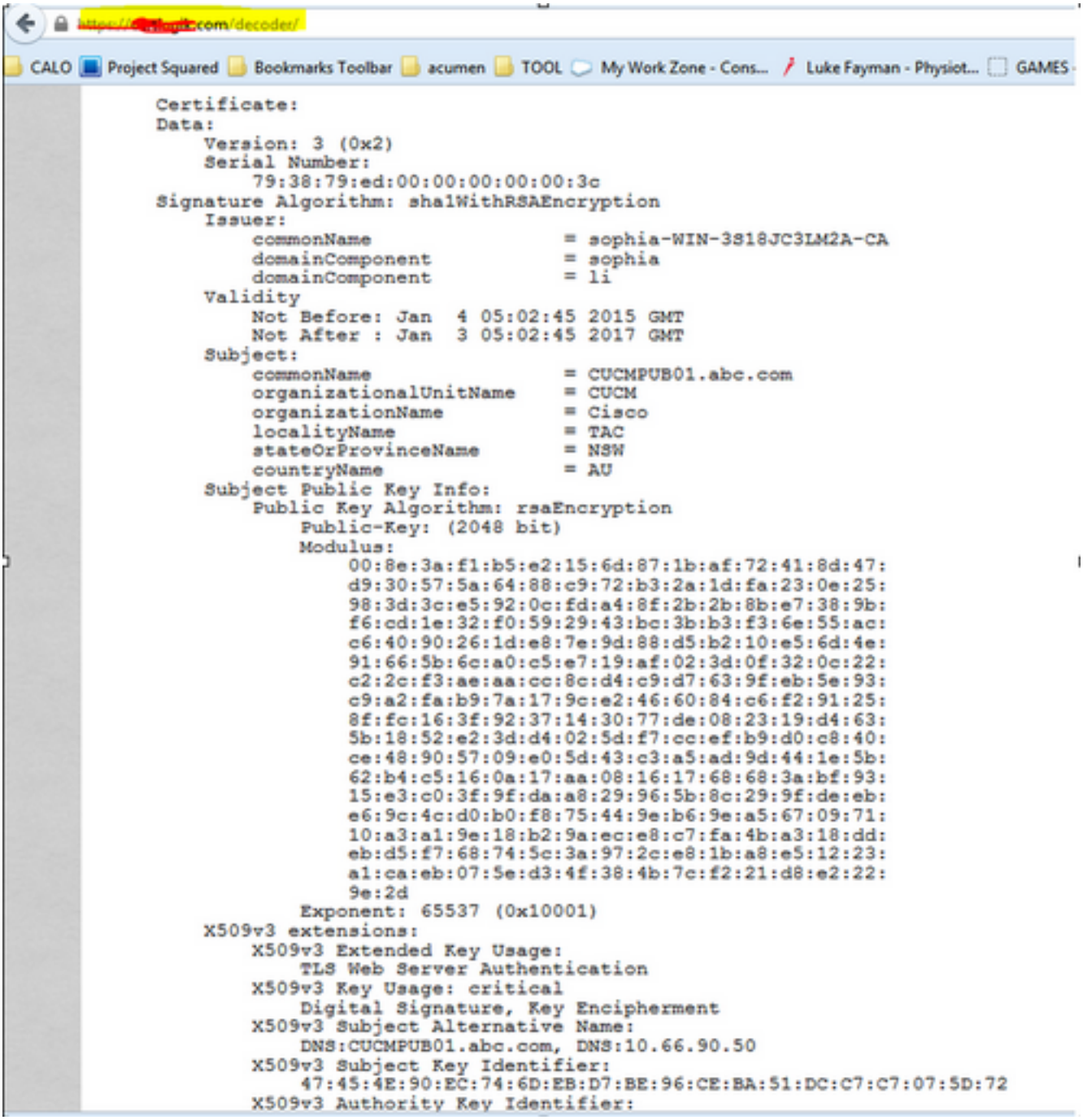
```
[root@CUCMPUB01 keys]# openssl req -noout -modulus -in tomcat.csr | openssl md5
cd78ed16b2abe2fa203e3f2e3499ee5c
[root@CUCMPUB01 keys]# openssl x509 -noout -modulus -in certnew.cer | openssl md5
cd78ed16b2abe2fa203e3f2e3499ee5c
[root@CUCMPUB01 keys]#
```

Solución 2. Utilice cualquier unidad emparejadora de la clave del certificado SSL de Internet



La solución 3. compara el contenido de cualquier decodificador CSR de Internet

1. Copie la **información detallada del certificado de la** sesión para cada uno tal y como se muestra en de esta imagen.



2. Compárelos en una herramienta tal como Notepad++ con el comparar plug-in tal y como se muestra en de esta imagen.