Configuración de la comunicación segura entre Finesse y el servidor CTI

Contenido

[Introducción](#)
[Prerequisites](#)
[Requirements](#)
[Componentes Utilizados](#)
[Antecedentes](#)
[Configurar](#)
[Servidor CCE CTI seguro](#)
[Configuración segura de Finesse](#)
[Generar certificado PG de agente (servidor CTI)](#)
[Obtenga el certificado CSR firmado por una CA](#)
[Importar certificados firmados por CA de CCE PGs](#)
[Generar certificado Finesse](#)
[Firmar certificado Finesse por una CA](#)
[Importar la aplicación Finesse y los certificados firmados raíz](#)
[Verificación](#)
[Troubleshoot](#)

Introducción

Este documento describe cómo implementar certificados firmados por la Autoridad de Certificación (CA) entre Cisco Finesse y Computer Telephony Integration (CTI) Server en la solución Cisco Contact Center Enterprise (CCE).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- CCE versión 12.0(1)
- Versión 12.0(1) de Finesse
- CTI Server

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software:

- Packaged CCE (PCCE) 12.0(1)

- Finesse 12.0(1)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

En la versión 11.5 de CCE, Cisco inició la compatibilidad con la versión 1.2 de seguridad de la capa de transporte (TLS), que permite que los mensajes de protocolo de inicio de sesión (SIP) y protocolo de transporte en tiempo real (RTP) se transporten de forma segura a través de TLS 1.2. Desde CCE 12.0 y como parte de la protección de los datos en movimiento, Cisco comenzó a admitir TLS 1.2 en la mayoría de los flujos de llamadas del centro de contacto: Voz entrante y saliente, multicanal y base de datos externa. El objetivo de este documento es la voz entrante, especialmente la comunicación entre Finesse y el servidor CTI.

El servidor CTI admite estos modos de conexión:

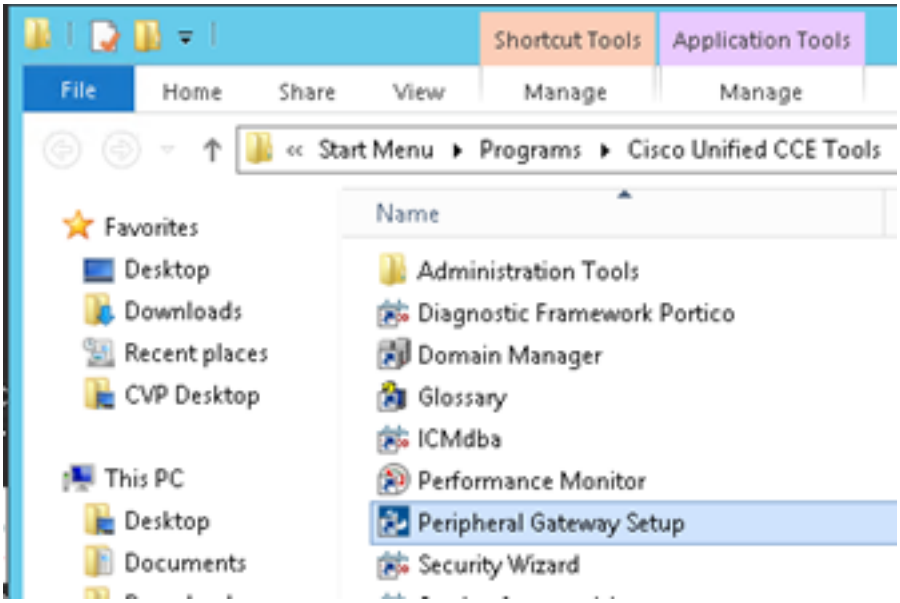
- **Conexión Sólo Segura**: Permite la conexión segura entre el servidor CTI y los clientes CTI (Finesse, dialer, CTIOS y ctitest).
- **Conexión segura y no segura (modo mixto):** Permite la seguridad, así como la conexión no segura entre el servidor CTI y los clientes CTI. Éste es el modo de conexión predeterminado. Este modo se configurará cuando actualice versiones anteriores a CCE 12.0(1).

Nota: No se admite el modo de sólo seguridad.

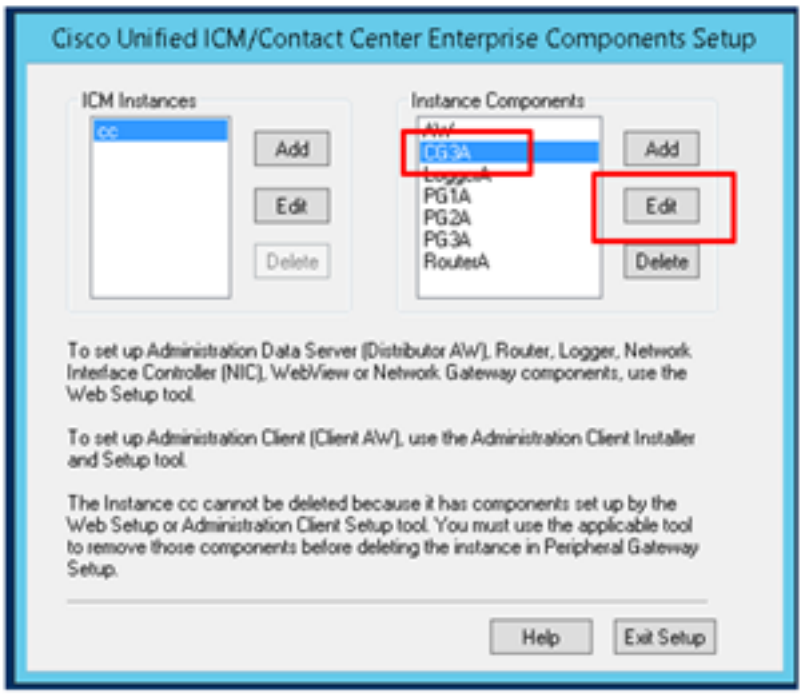
Configurar

Servidor CCE CTI seguro

Paso 1. En la estación de trabajo administrativa PCCE (AW), abra la carpeta **Herramientas de Unified CCE** y haga doble clic en **Configuración de gateway periférico**.

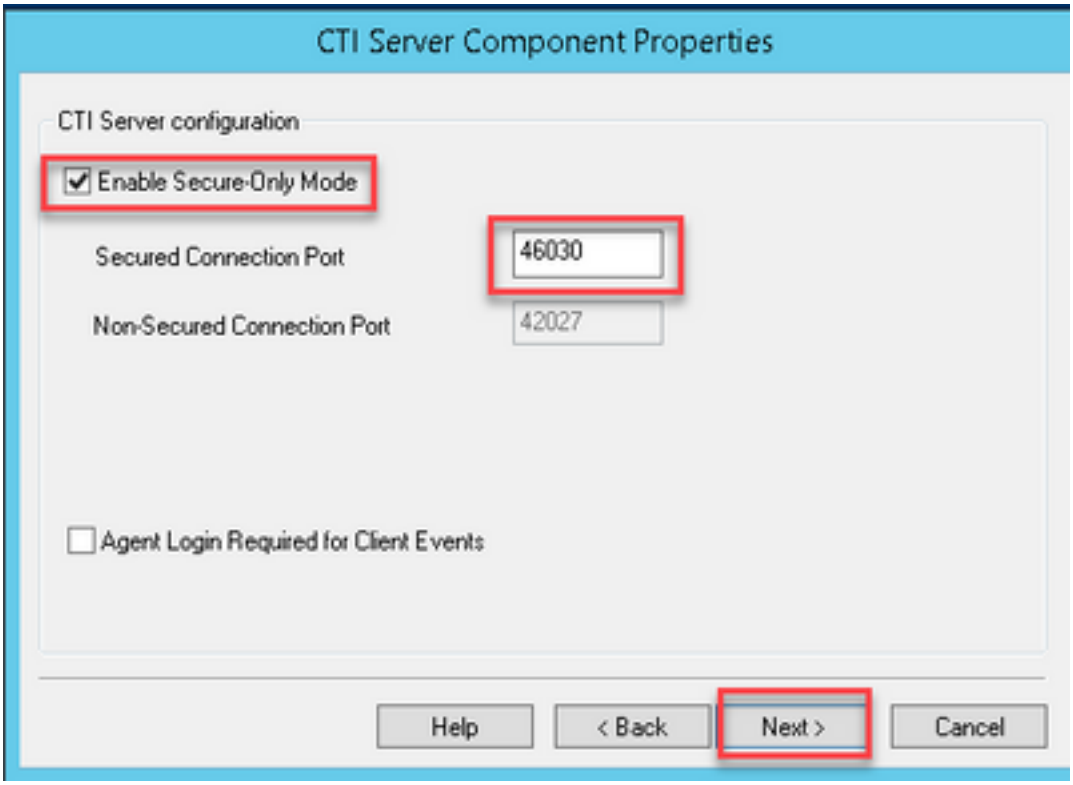


Paso 2. Seleccione **CG3A** y haga clic en **Editar**.



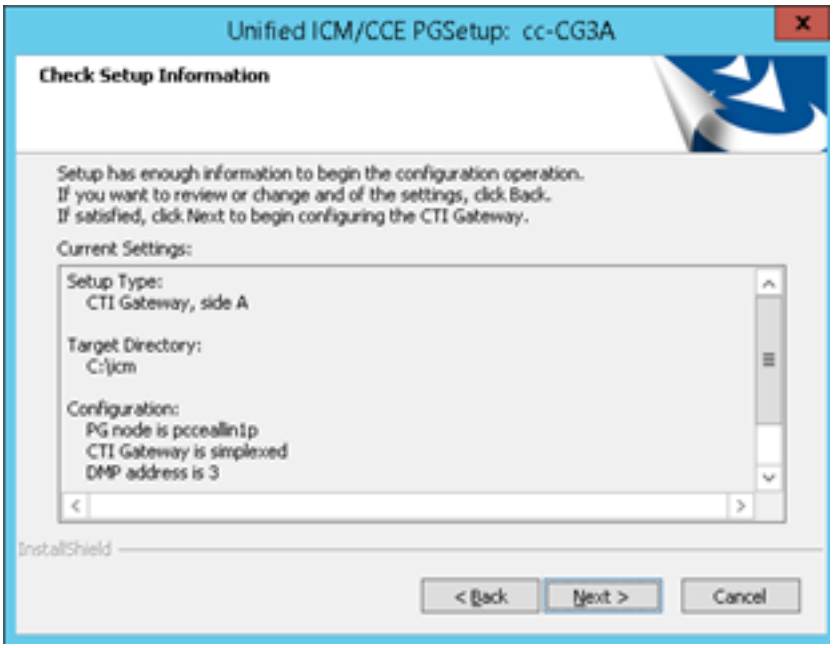
Paso 3. En las propiedades del servidor CTI, haga clic en **Next**. En la pregunta sobre la configuración que detiene el servicio **CG3A**, seleccione **Yes**.

Paso 4. En **CTI Server Components Properties**, seleccione **Enable Secured-only mode .** Observe el **Puerto de conexión seguro (46030)**, ya que debe configurar el mismo puerto en Finesse en el ejercicio siguiente. Haga clic en Next (Siguiente).

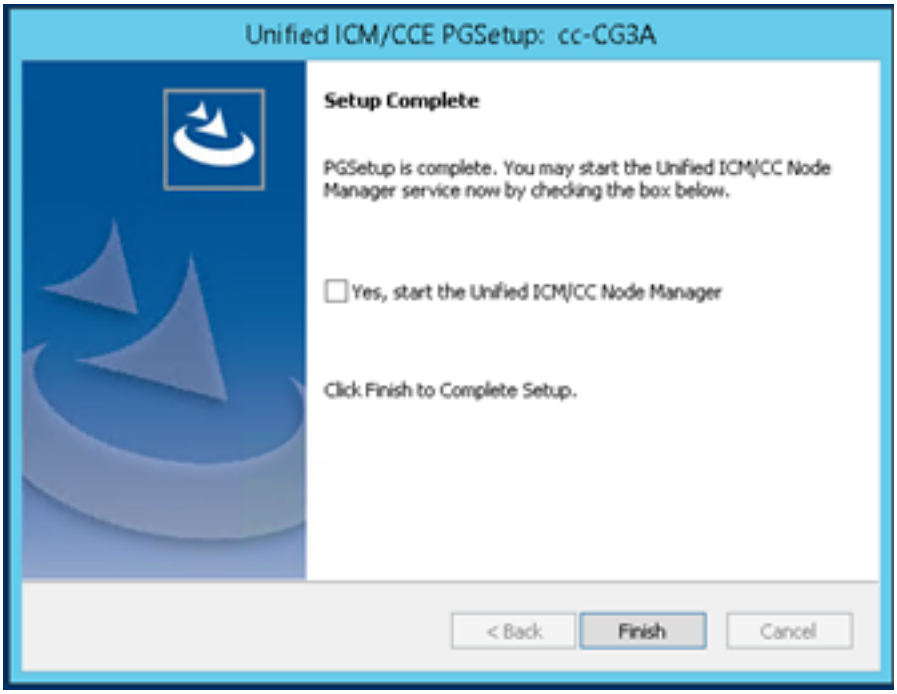


Nota: La comunicación segura predeterminada es 42030; sin embargo, el laboratorio utilizado para este documento es 40630. El número de puerto es parte de una fórmula que incluye el ID del sistema ICM. Cuando el ID del sistema es 1 (CG1a), el número de puerto predeterminado, en general, es 42030. Dado que la ID del sistema en el laboratorio es 3 (CG3a), el número de puerto predeterminado es 46030.

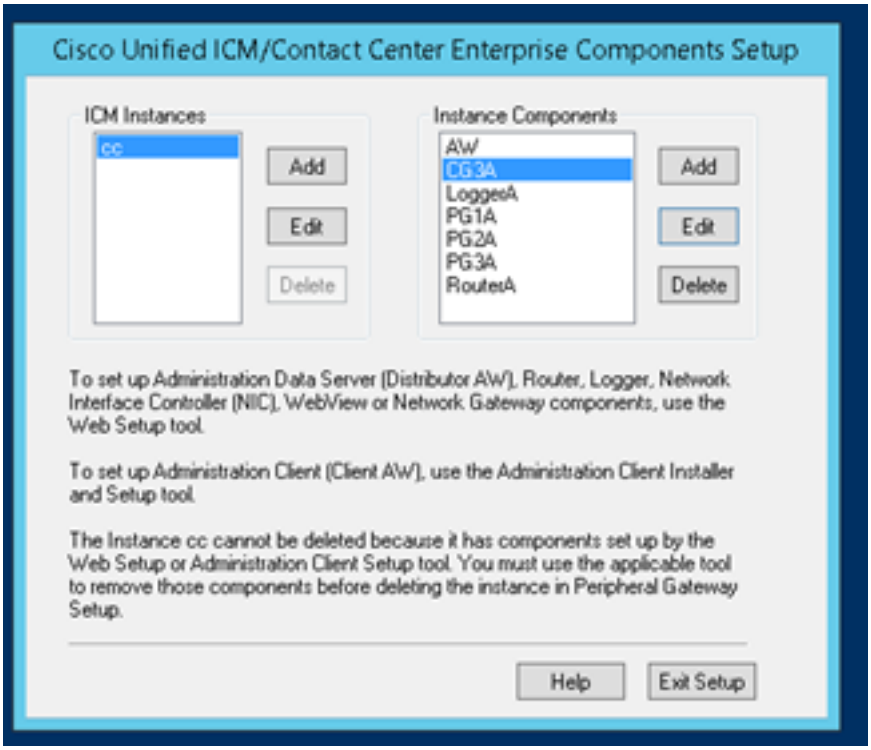
Paso 5. En **CTI Network Interface Properties**, haga clic en **Next**. Compruebe la **información de configuración** y haga clic en **Siguiente**.



Paso 6. Haga clic en **Finalizar** como se muestra en la imagen.



Paso 7. Haga clic en **Salir de la configuración** y espere hasta que la ventana de configuración se cierre como se muestra en la imagen.



Paso 8. En el escritorio PCCEAllin1, haga doble clic en **Unified CCE service Control**.

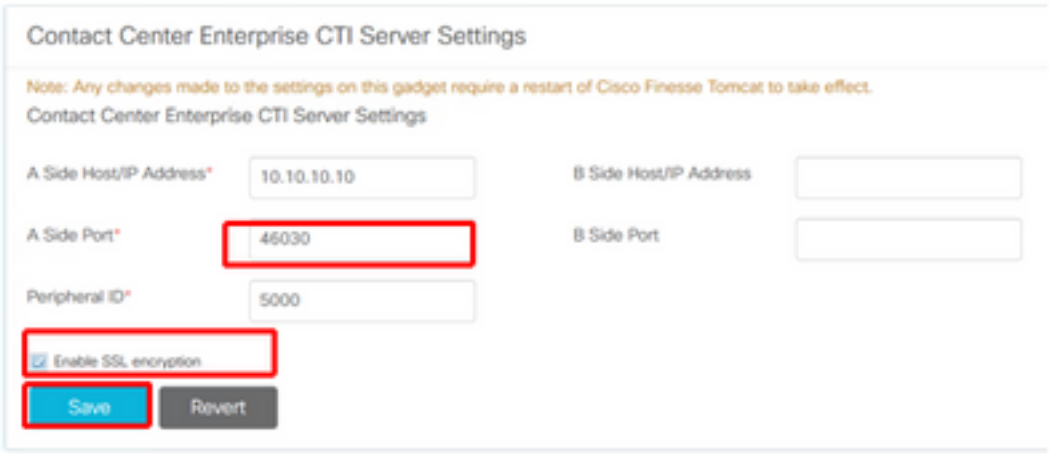
Paso 9. Seleccione Cisco ICM cc CG3A y haga clic en **Inicio**.

Configuración segura de Finesse

Paso 1. Abra un navegador web y navegue hasta **Administración de Finesse**.

Paso 2. Desplácese hacia abajo hasta la sección **Configuración del servidor CTI de Contact Center Enterprise** como se muestra en la imagen.

Paso 3. Cambie el puerto lateral A para el puerto de comunicación segura configurado en CG3A en el ejercicio anterior: **46030.** Marque **Enable SSL encryption** y haga clic en **Save**.



Nota: Para probar la conexión, primero debe reiniciar el servicio Finesse Tomcat o reiniciar el servidor Finesse.

Paso 4. Cierre sesión en la página Administración de Finesse.

Paso 5. Abra una sesión SSH con Finesse.

Paso 6. En la sesión FINESSEA SSH, ejecute el comando:

utils system restart

Ingrese **yes** cuando se le pregunte si desea reiniciar el sistema.

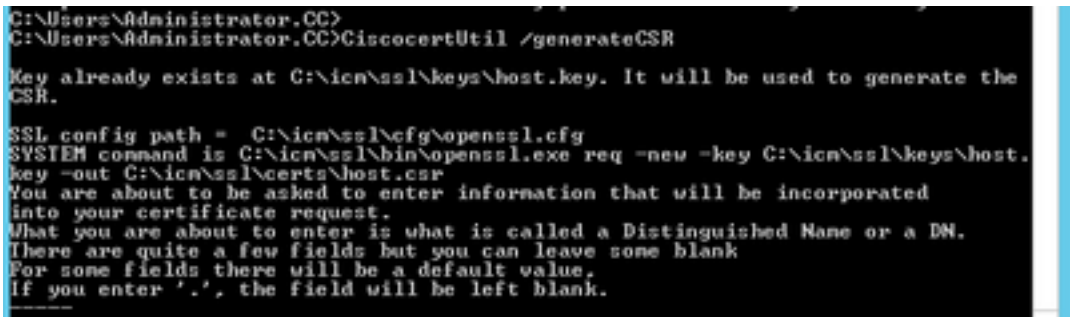
```
Using username "administrator".
Command Line Interface is starting up, please wait ...

   Welcome to the Platform Command Line Interface

VMware Installation:
        2 vCPU: Intel(R) Xeon(R) CPU E5-2680 0 @ 2.70GHz
        Disk 1: 146GB, Partitions aligned
        8192 Mbytes RAM

admin:utils system restart

Do you really want to restart ?

Enter (yes/no)? yes


 Appliance is being Restarted ...
Warning: Restart could take up to 5 minutes.
Stopping Service Manager...
```

Generar certificado PG de agente (servidor CTI)

CiscoCertUtils es una nueva herramienta lanzada en la versión 12 de CCE. Utilice esta herramienta para administrar todos los certificados CCE de voz entrante. En este documento,

usted utiliza estas CiscoCertUtils para generar las solicitudes de firma de certificados (CSR) de puertas de enlace periféricas (Gateways periféricos).

Paso 1. Ejecute este comando para generar un certificado CSR: **CiscoUtil /generateCSR**



Proporcione la información solicitada, por ejemplo:

Nombre del país: US

Nombre de estado o provincia: MA

Nombre de localidad: BXB

Nombre de la organización: Cisco

Unidad organizativa: CX

Nombre común: PCCEAllin1.cc.lab

Correo electrónico: jdoe@cc.lab

Una contraseña de desafío: Train1ng!

Nombre de la empresa opcional: Cisco

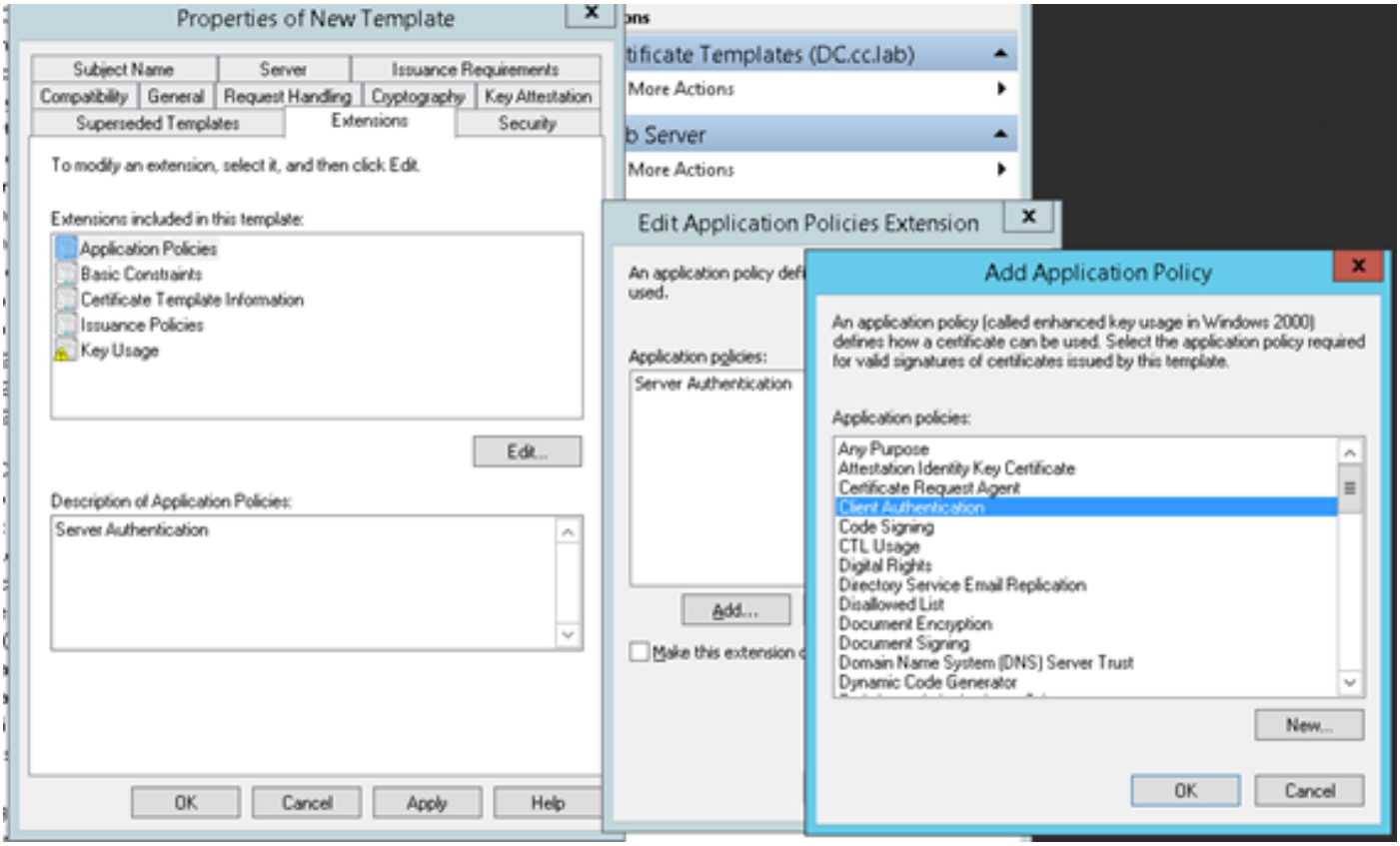
El certificado y la clave del host se almacenan en **C:\icm\ssl\certs** y **C:\icm\ssl\keys**.

Paso 2. Navegue hasta la carpeta **C:\icm\ssl\certs** y asegúrese de que el archivo **host.csr** se ha generado.

Obtener el certificado CSR Firmado por una CA

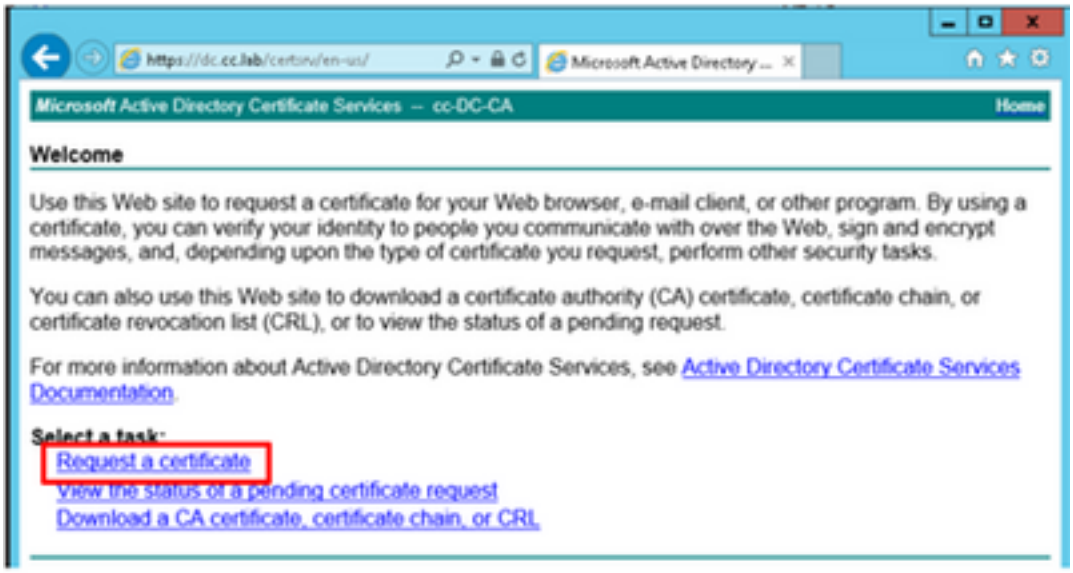
Una vez generados los certificados CSR, deben estar firmados por una CA de terceros. En este ejercicio, la CA de Microsoft instalada en el controlador de dominio se utiliza como la CA de terceros.

Asegúrese de que la plantilla de certificado utilizada por la CA incluya la autenticación de cliente y servidor como se muestra en la imagen cuando se utiliza Microsoft CA.

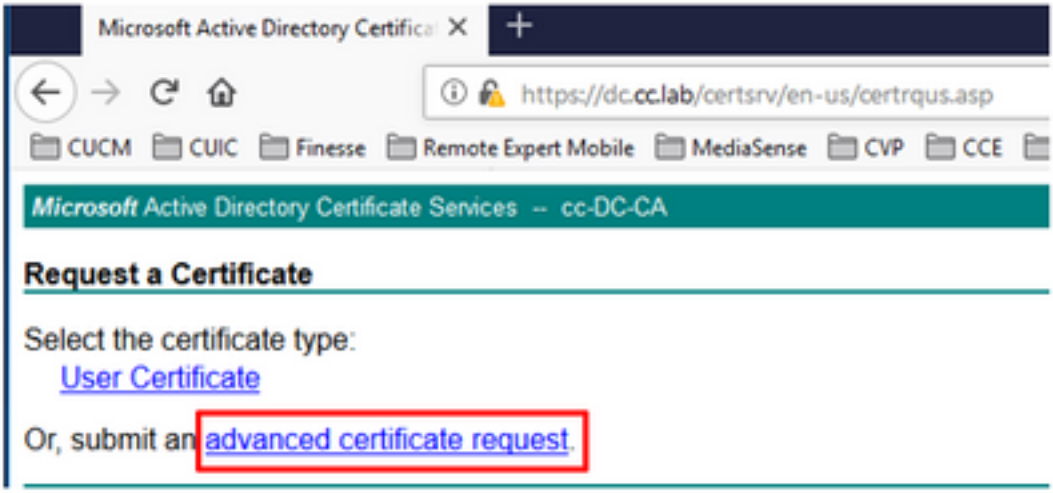


Paso 1. Abra un explorador web y navegue hasta la CA.

Paso 2. En **Microsoft Active Directory Certificate Services**, seleccione **Solicitar un certificado**.

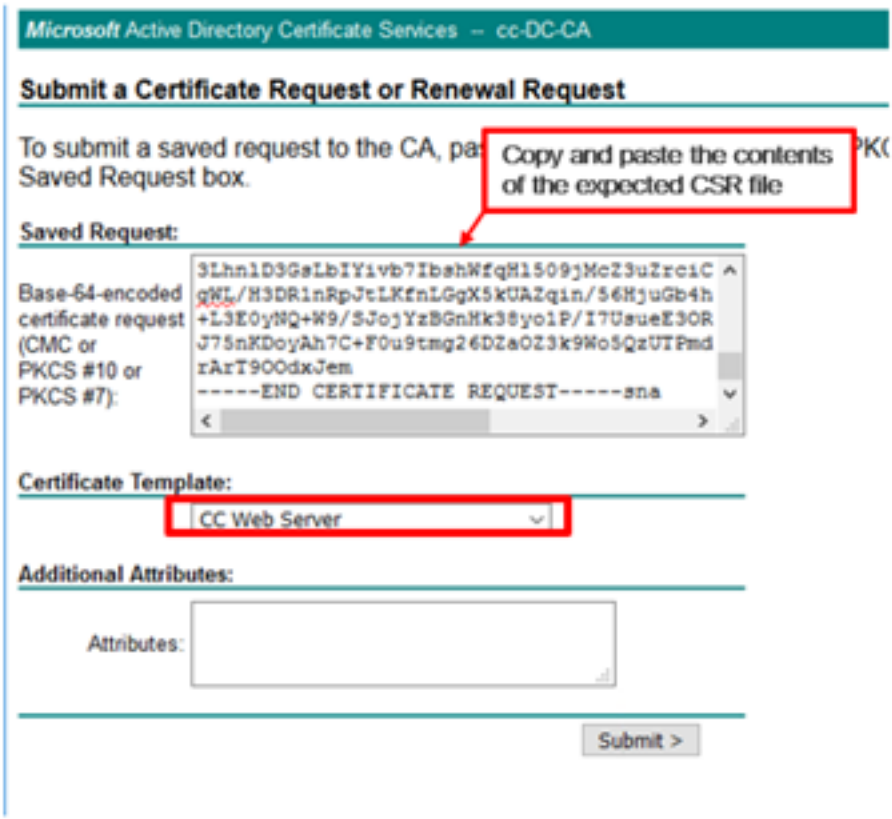


Paso 3. Seleccione la opción **advanced certificate request**.



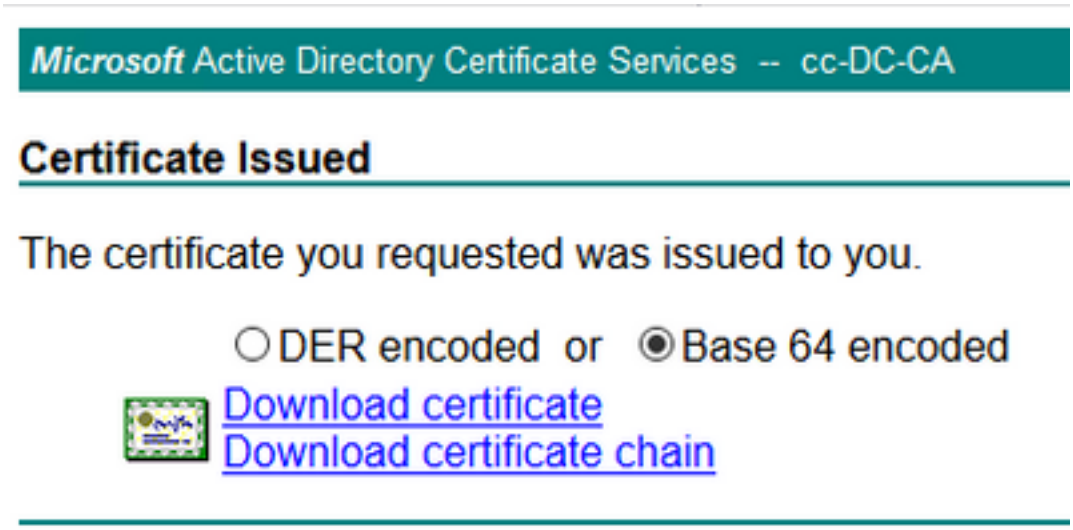
Paso 4. En la **solicitud de certificado avanzada,** copie y pegue el contenido del certificado CSR del agente PG en el **cuadro Solicitud guardada**.

Paso 5. Seleccione la plantilla **Web Server** con autenticación de cliente y servidor. En el laboratorio, la plantilla de servidor Web CC se creó con autenticación de cliente y servidor.



Paso 6. Haga clic en **Enviar**.

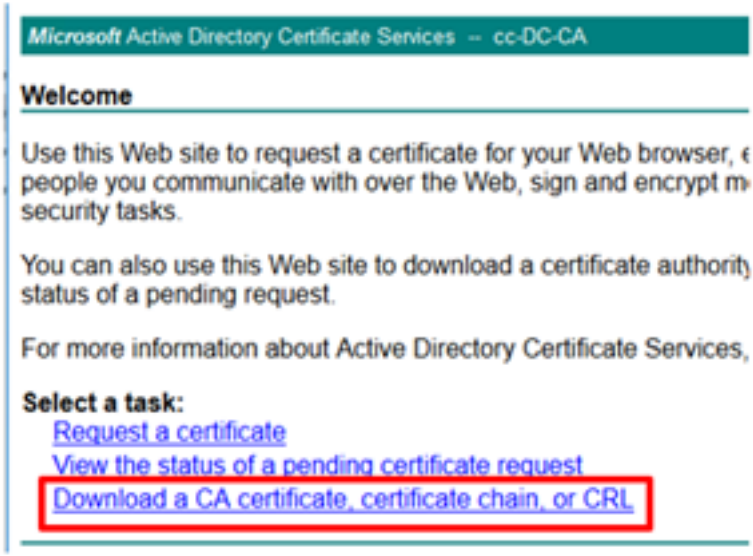
Paso 7. Seleccione **Base 64 codificada** y haga clic en **Descargar certificado** como se muestra en la imagen.



Paso 8. Guarde el archivo y haga clic en **Aceptar**. El archivo se guarda en la carpeta **Descargas**.

Paso 9. Cambie el nombre del archivo a **host.cer** (opcional).

Paso 10. También debe generar un certificado raíz. Vuelva a la página de certificados de CA y, a continuación, seleccione **Descargar un certificado de CA, cadena de certificados o CRL**. Solo tiene que realizar este paso una vez, ya que el certificado raíz será el mismo para todos los servidores (PG Agent y Finesse).



Paso 11. Haga clic en **Base 64** y seleccione **Descargar certificado CA**.

Paso 12. Haga clic en Guardar archivo y seleccione **Aceptar**. El archivo se guardará en la ubicación predeterminada, **Descargas**.

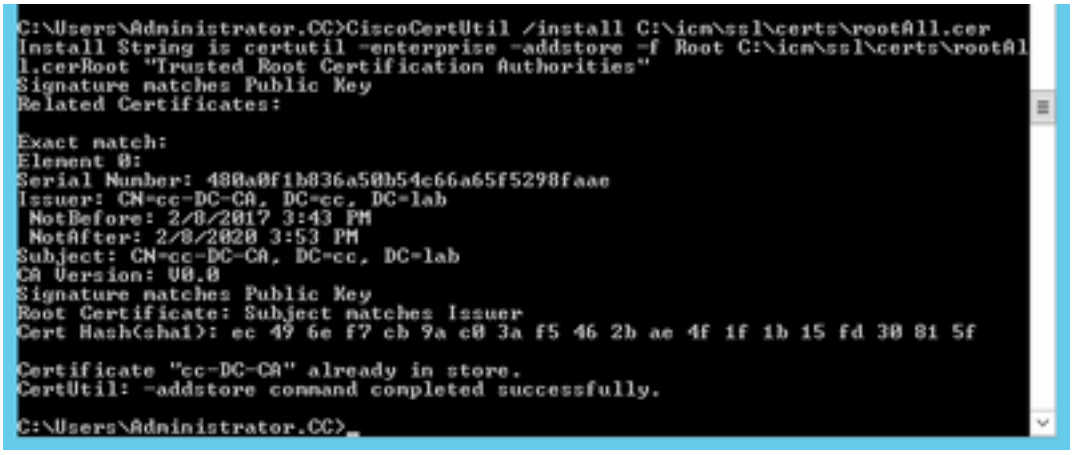
Importar certificados firmados por CA de CCE PGs

Paso 1. En el PG Agent navegue hasta **C:\icm\ssl\certs** y pegue aquí la raíz y los archivos firmados por el PG Agent.

Paso 2. Cambie el nombre del certificado host.pem en **c:\icm\ssl\certs** como **selfhost.pem**.

Paso 3. Cambie el nombre host.cer a host.pem en la carpeta **c:\icm\ssl\certs** .

Paso 4. Instale el certificado raíz. En el símbolo del sistema, ejecute este comando: **CiscoCertUtil /install C:\icm\ssl\certs\rootAll.cer**



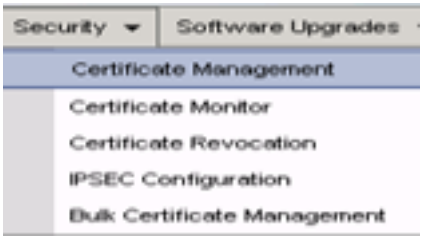
Paso 5. Instale el certificado firmado de la aplicación ejecutando el mismo comando: **CiscoCertUtil /install C:\icm\ssl\certs\host.pem**

Paso 6. Cicle el PG. Abra el control de servicio de Unified CCE y active el PG de Cisco ICM Agent.

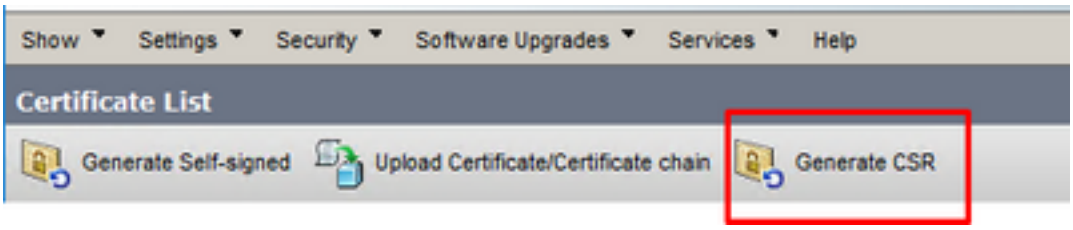
Generar certificado Finesse

Paso 1. Abra el navegador web y navegue hasta **Finesse OS Admin**.

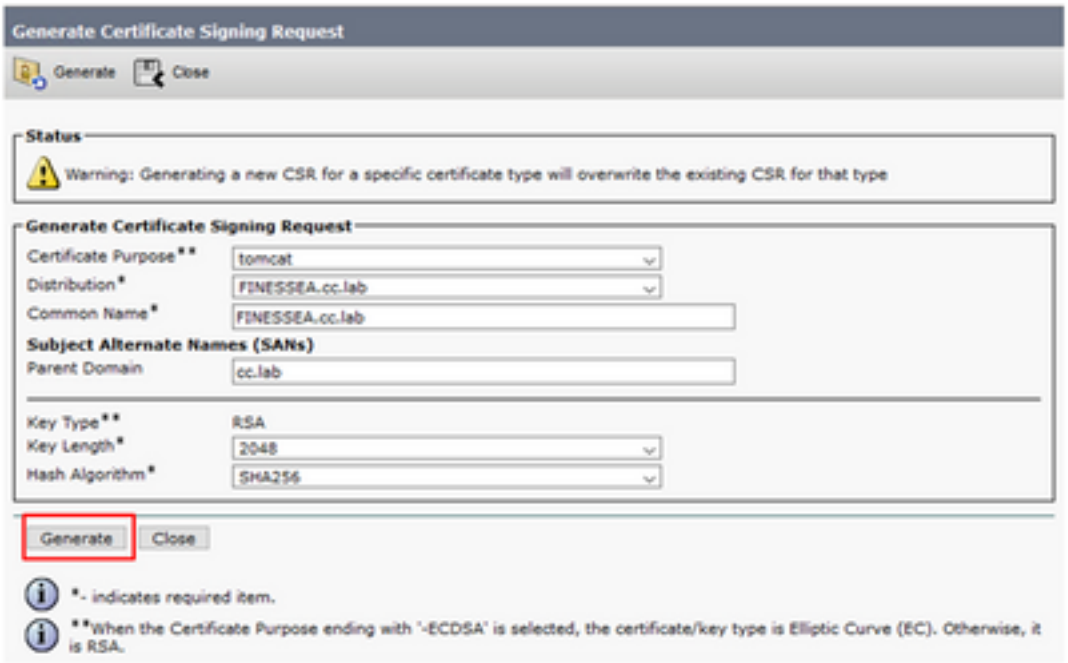
Paso 2. Inicie sesión con las credenciales de administración del sistema operativo y navegue hasta **Seguridad > Administración de certificados** como se muestra en la imagen.



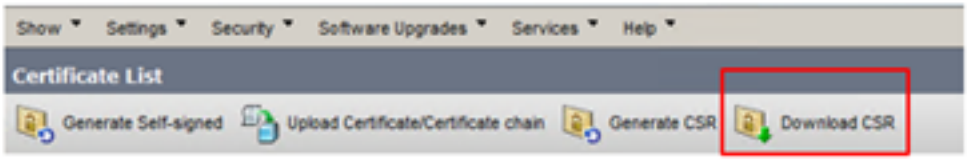
Paso 3. Haga clic en **Generar CSR** como se muestra en la imagen.



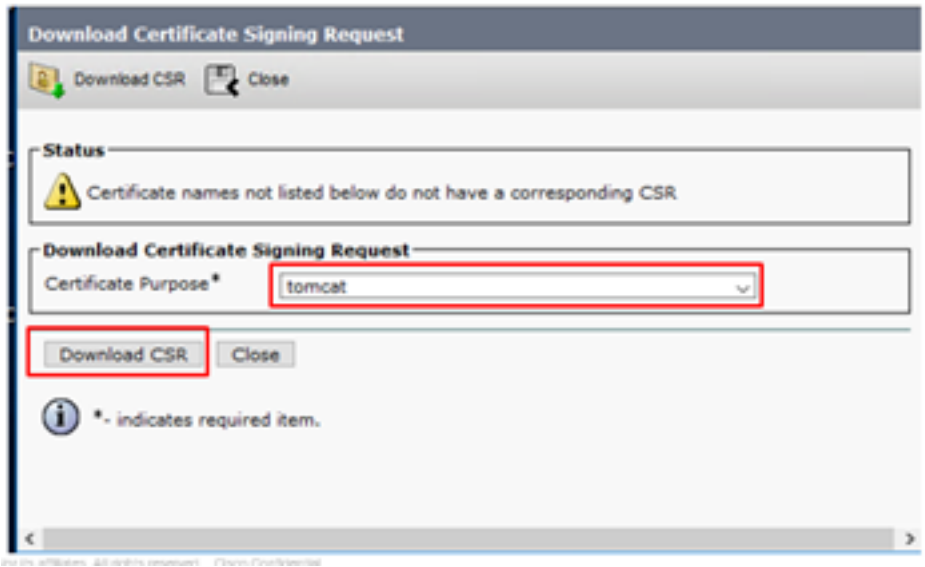
Paso 4. En la **Solicitud de firma de certificado**, utilice los valores predeterminados y haga clic en **Generar.**



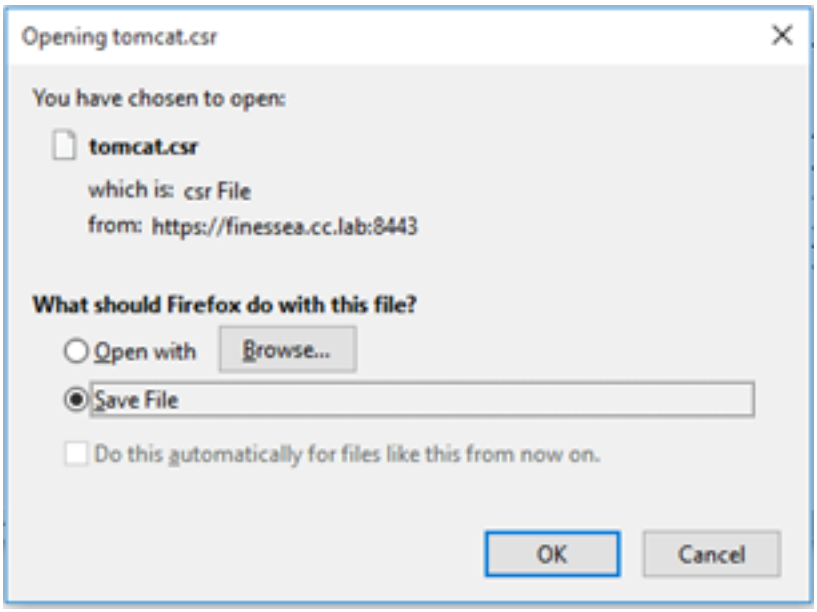
Paso 5. Cierre la ventana **Generar solicitud de firma de certificado** y seleccione **Descargar CSR**.



Paso 6. En Certificate Purpose, seleccione **tomcat** y haga clic en **Download CSR**.



Paso 7. Seleccione **Guardar archivo** y haga clic en **Aceptar** como se muestra en la imagen.



Paso 8. Cierre la ventana **Descargar solicitud de firma de certificado**. El certificado se guarda en la ubicación predeterminada **(This PC > Downloads)**.

Paso 9. Abra el Explorador de Windows y desplácese a esa carpeta. Haga clic con el botón derecho del ratón en este certificado y cámbiele el nombre: **finessetomcat.csr**

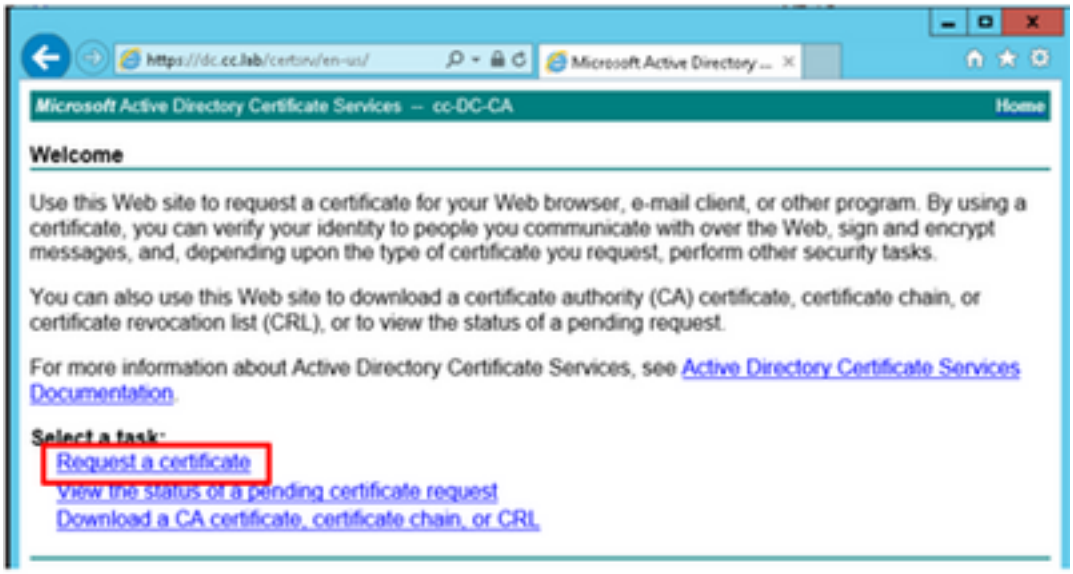
Firmar certificado Finesse por una CA

En esta sección, se utiliza la misma CA de Microsoft utilizada en el paso anterior que la CA de terceros.

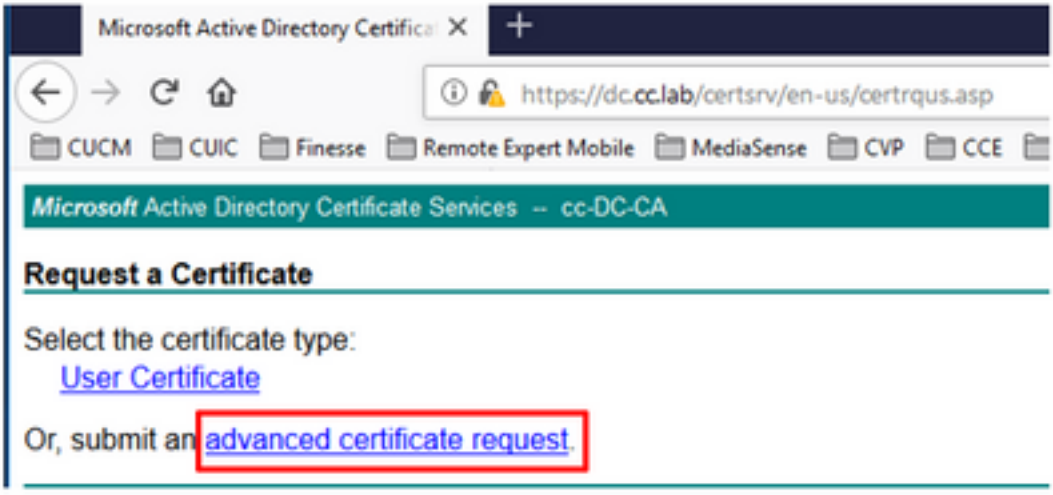
Nota: Asegúrese de que la plantilla de certificado utilizada por la CA incluya la autenticación de cliente y servidor.

Paso 1. Abra un explorador web y navegue hasta la CA.

Paso 2. En **Microsoft Active Directory Certificate Services**, seleccione **Solicitar un certificado**.

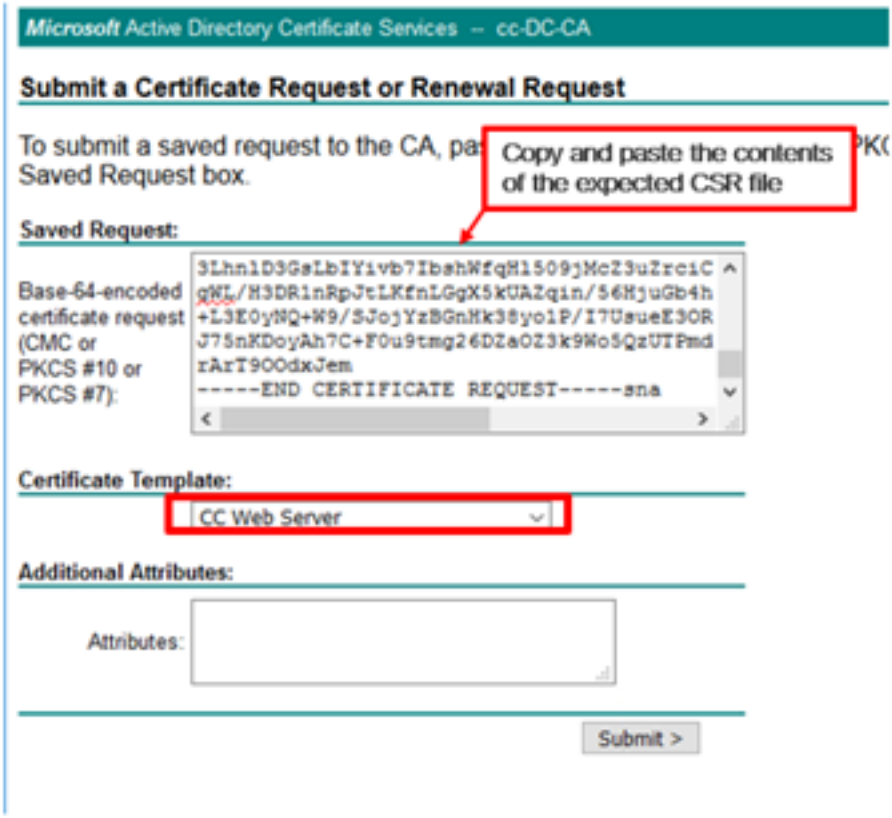


Paso 3. Seleccione la opción **advanced certificate request** como se muestra en la imagen.



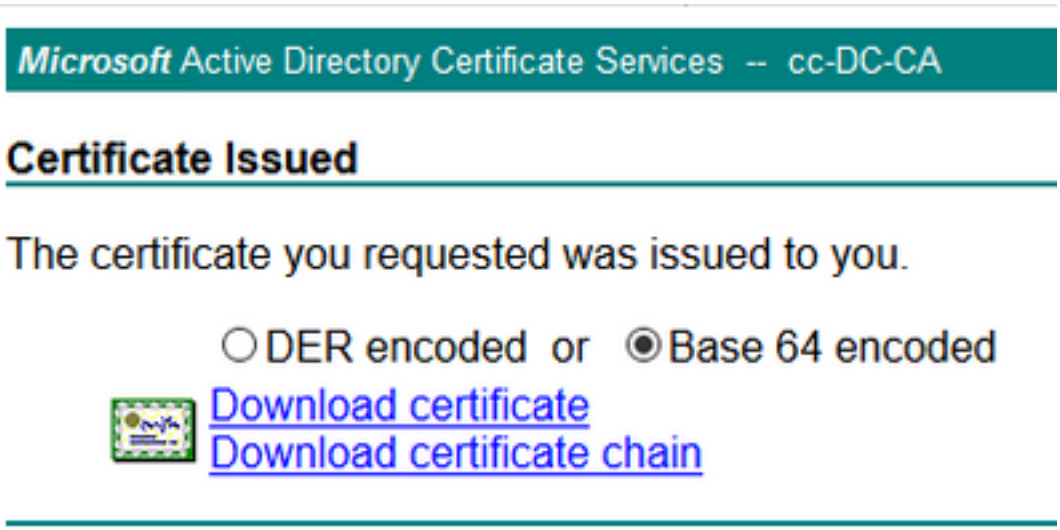
Paso 4. En la **solicitud de certificado avanzada,** copie y pegue el contenido del certificado CSR Finesse en el **cuadro Solicitud guardada**.

Paso 5. Seleccione la plantilla de servidor Web con autenticación de cliente y servidor. En este laboratorio, la plantilla de servidor Web CC se creó con autenticación de cliente y servidor.



Paso 6. Haga clic en **Enviar**.

Paso 7. Seleccione **Base 64 codificada** y haga clic en **Descargar certificado** como se muestra en la imagen.



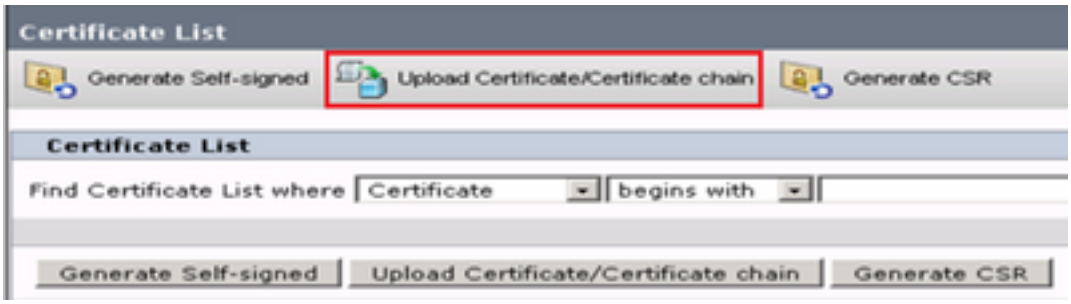
Paso 8. Guarde el archivo y haga clic en **Aceptar**. El archivo se guarda en la carpeta **Descargas**.

Paso 9. Cambie el nombre del archivo a **finesse.cer**.

Importar la aplicación Finesse y los certificados firmados raíz

Paso 1. En un proser web, abra la página **Finesse OS Admin** y navegue hasta **Security > Certificate Management**.

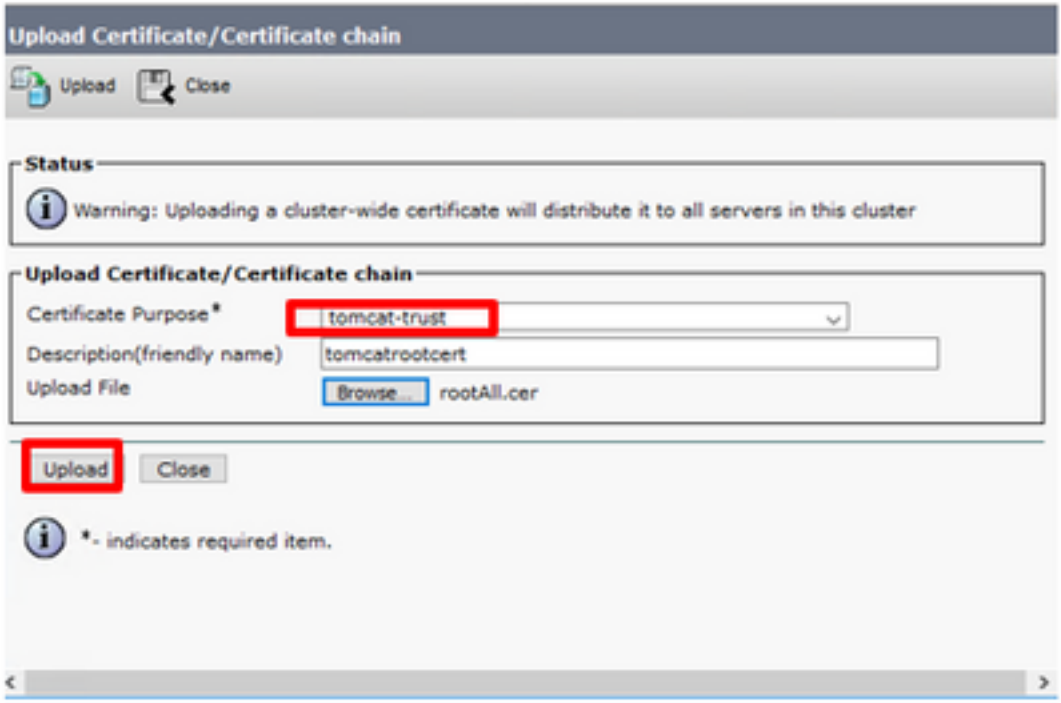
Paso 2. Haga clic en el botón **Cargar certificado/cadena de certificado** como se muestra en la imagen.



Paso 3. En la ventana emergente, seleccione **tomcat-trust** para **Certificate Purpose**.

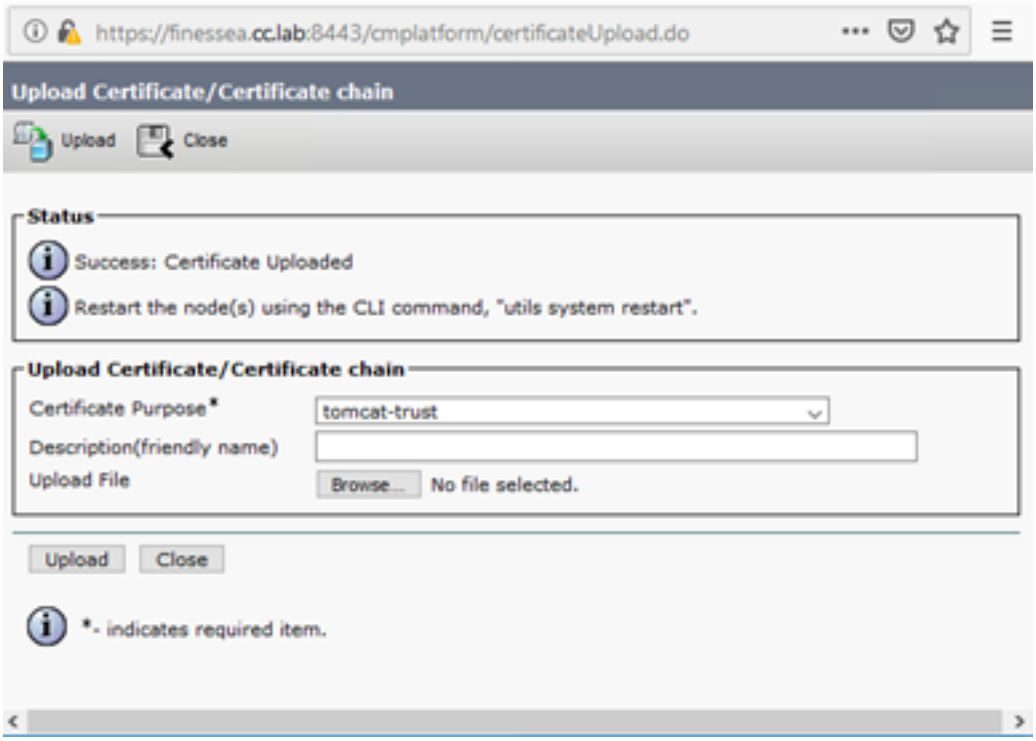
Paso 4. Haga clic en el botón **Examinar...** y seleccione el archivo de certificado raíz para importar. A continuación, haga clic en el botón **Abrir**.

Paso 5. En la descripción, escriba algo como **tomcatrootcert** y haga clic en el **botón Upload** como se muestra en la imagen.

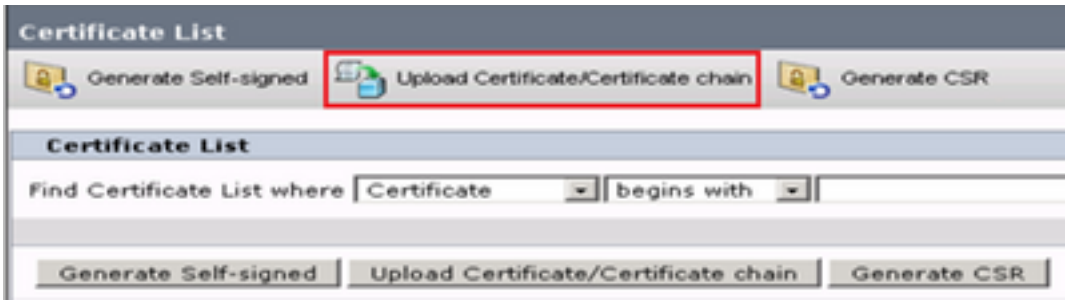


Paso 6. Espere hasta que vea el **éxito: Certificado cargado** para cerrar la ventana.

Se le solicitará que reinicie el sistema, pero primero continúe cargando el certificado firmado de la aplicación Finesse y, a continuación, podrá reiniciar el sistema.



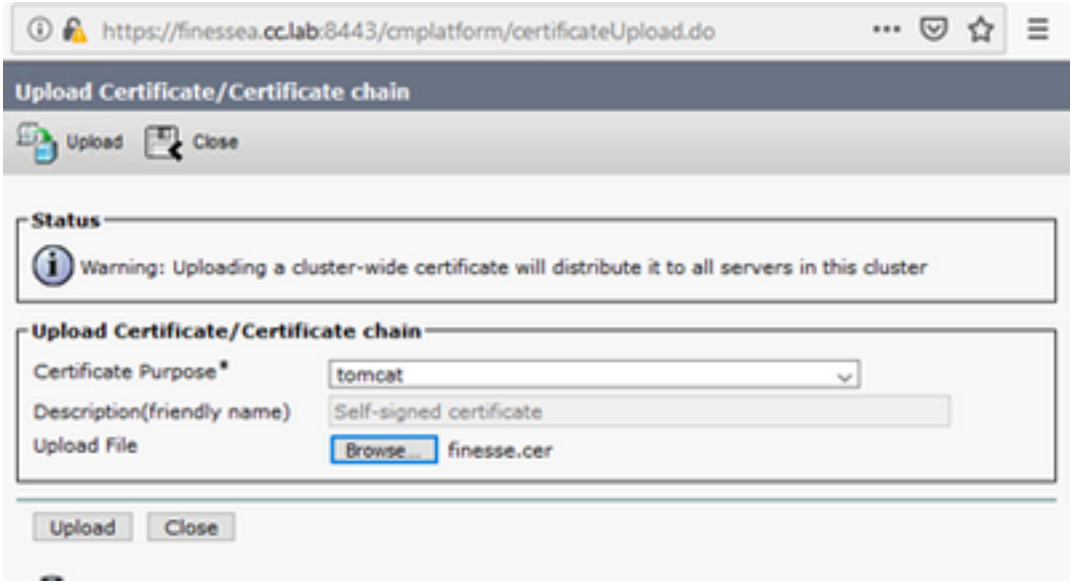
Paso 7. Haga clic en más tiempo en el botón **Cargar certificado/cadena de certificado** para importar el certificado de aplicación Finesse.



Paso 8. En la ventana emergente, seleccione **tomcat** para **Finalidad de certificado**.

Paso 9. Haga clic en el botón **Examinar...** y seleccione el archivo firmado por Finesse CA, **finesse.cer**. A continuación, haga clic en el botón **Abrir**.

Paso 10. Haga clic en el botón **Cargar**.



Paso 11. Espere hasta que vea el **éxito:** Mensaje **de certificado cargado**.

Una vez más, se le solicita que reinicie el sistema. Cierre la ventana y continúe reiniciando el sistema.

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.