Configuración de la inscripción y renovación automáticas de certificados a través de CAPF Online CA

Contenido

Introducción

En este documento se describe la inscripción y renovación automáticas de certificados mediante la función en línea Certificate Authority Proxy Function (CAPF) para Cisco Unified Communications Manager (CUCM).

Colaboración de Michael Mendoza, ingeniero del TAC de Cisco.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco Unified Communications Manager
- Certificados X.509
- Servidor Windows
- Active Directory (AD) de Windows
- Servicios de Windows Internet Information Server (IIS)
- Autenticación NT (nueva tecnología) LAN Manager (NTLM)

Componentes Utilizados

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

- CUCM, versión 12.5.1.10000-22

- Windows Server 2012 R2
- IP Phone CP-8865 / Firmware: SIP 12-1-1SR1-4 y 12-5-1SR2.

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 tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Este documento trata la configuración de la función y los recursos relacionados para una investigación adicional.

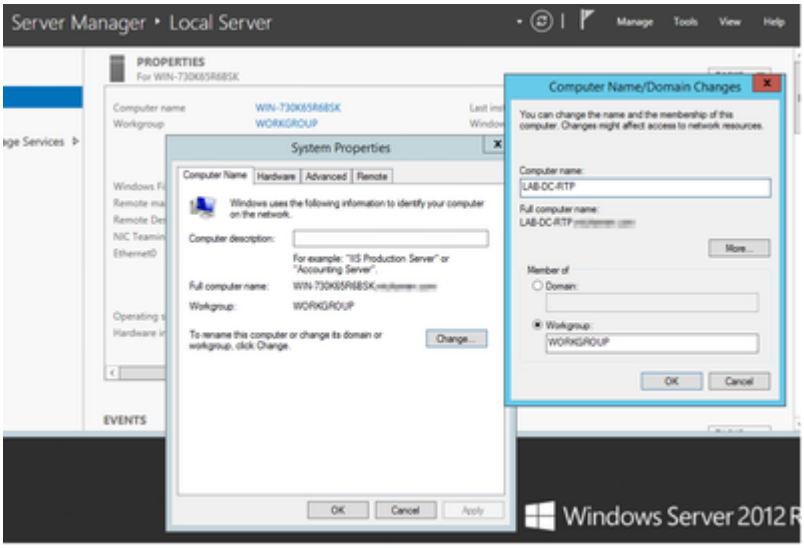
Validar la fecha y la hora del servidor

Asegúrese de que el servidor de Windows tiene la fecha, hora y zona horaria correctas configuradas, ya que afectan a los tiempos de validez del certificado de la CA (autoridad de certificación) raíz del servidor, así como a los certificados emitidos por él.

Actualizar nombre de equipo del servidor

De forma predeterminada, el nombre del equipo del servidor tiene un nombre aleatorio, como WIN-730K65R6BSK. Lo primero que se debe hacer antes de habilitar los Servicios de dominio de AD es asegurarse de actualizar el nombre de equipo del servidor a lo que desea que sean el nombre de host y el nombre de emisor de la CA raíz del servidor al final de la instalación; de lo contrario, se necesitan muchos pasos adicionales para cambiar esto después de instalar los servicios de AD.

- Vaya a **Servidor local**, seleccione el nombre del equipo para abrir las **Propiedades del sistema**
- Seleccione el botón **Change** y escriba el nuevo nombre de equipo:



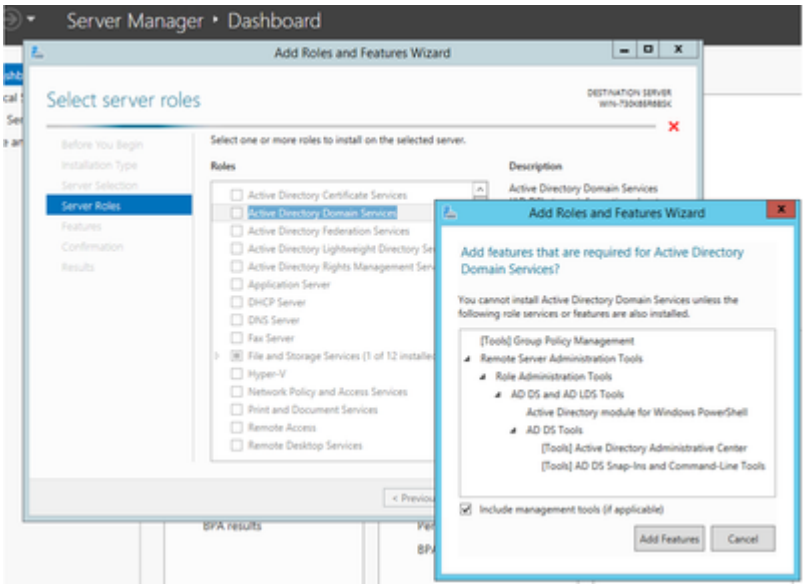
- Reinicie el servidor para aplicar los cambios

Configurar

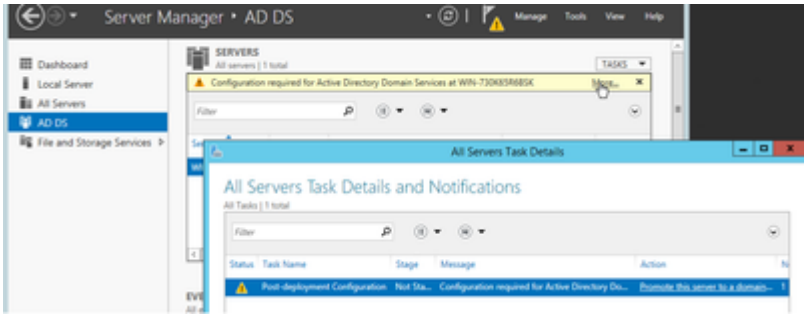
Plantilla de certificados, usuarios y servicios de AD

Habilitar y configurar servicios de Active Directory

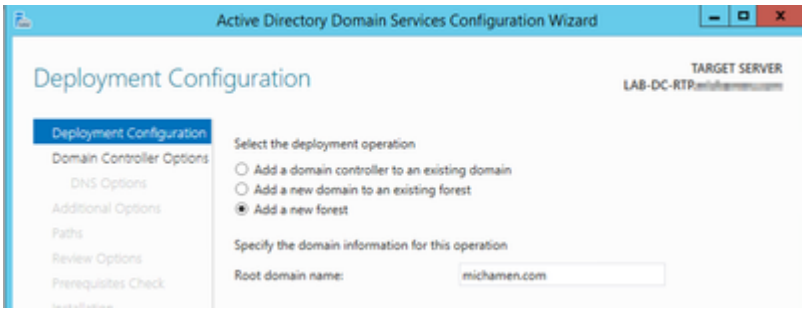
- En Administrador del servidor, seleccione la opción **Agregar funciones y características**, seleccione **Instalación basada en funciones o en características** y elija el servidor del grupo (sólo debe haber uno en el grupo) y, a continuación, Servicios de dominio de Active Directory:

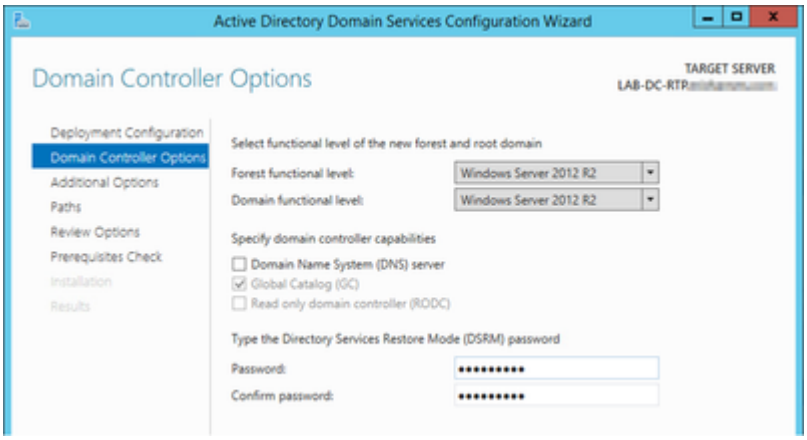


- Continúe seleccionando el botón **Next** y, a continuación, **Install**
- Seleccione el botón **Close** después de completar la instalación
- Aparecerá una ficha de advertencia en **Administrador del servidor > AD DS** con el título Configuración necesaria para los Servicios de dominio de Active Directory; Seleccione el vínculo **más** y, a continuación, la acción disponible para iniciar el asistente de configuración:

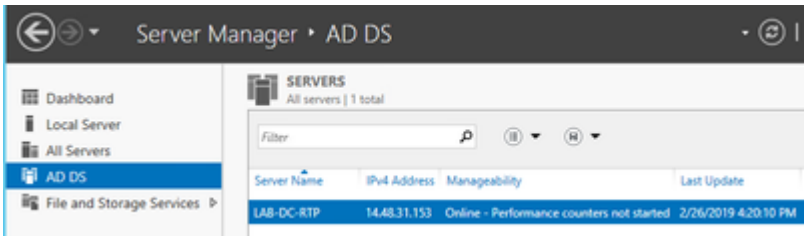


- Siga las indicaciones del asistente de configuración de dominio, agregue un nuevo bosque con el nombre de dominio raíz deseado (usado michamen.com para este laboratorio) y desmarque la casilla DNS cuando esté disponible, defina la contraseña de DSRM (usada *C1sc0123!* para este laboratorio):



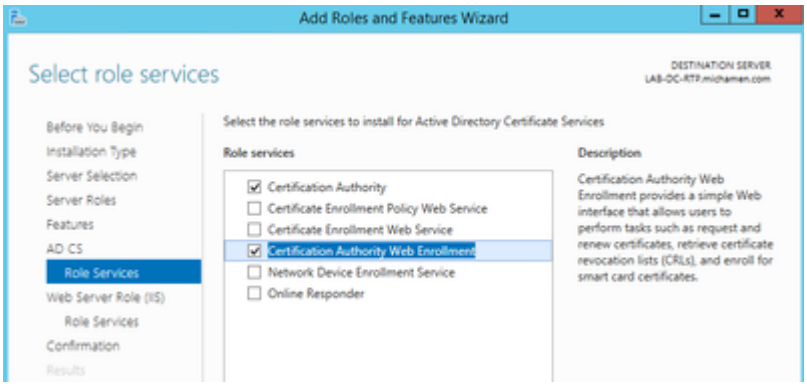


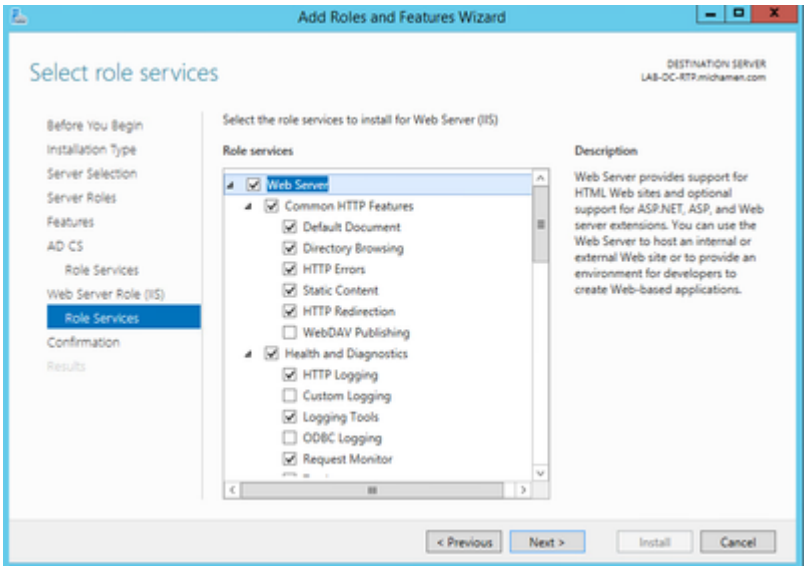
- Es necesario especificar un nombre de dominio NetBIOS (se utilizó MICHAMEN1 en este laboratorio).
- Siga el asistente hasta el final. A continuación, el servidor se reinicia para completar la instalación.
- A continuación, deberá especificar el nuevo nombre de dominio la próxima vez que inicie sesión. Por ejemplo, MICHAMEN1\Administrator.



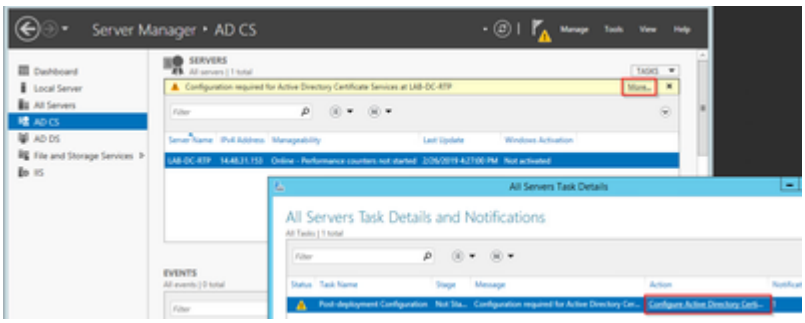
Habilitar y configurar Servicios de Certificate Server

- En Administrador del servidor, seleccione Agregar funciones y características
- Seleccione Servicios de certificados de Active Directory y siga las indicaciones para agregar las características necesarias (todas las características disponibles se seleccionaron de los servicios de rol habilitados para este laboratorio)
- Para servicios de rol, marque Entidad de certificación Inscripción en Web

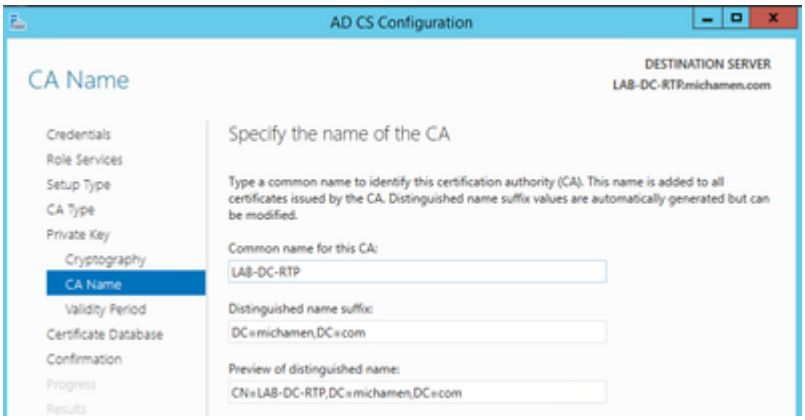




- Debe aparecer una ficha de advertencia en **Administrador del servidor >AD DS** con el título Configuración necesaria para los Servicios de certificados de Active Directory; seleccione el vínculo **más** y, a continuación, la acción disponible:



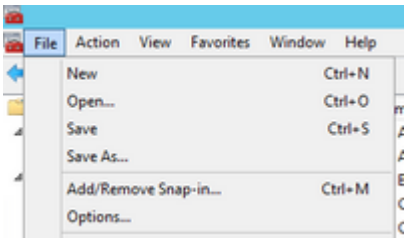
- En el Asistente para configuración posterior a la instalación de AD-CS, desplácese por estos pasos:
- Seleccione las **funciones** de **inscripción en Web Entidad de certificación** y **Entidad de certificación**
- Elija Enterprise CA con opciones:
- CA raíz
- Crear una nueva clave privada
- Usar clave privada: SHA1 con la configuración predeterminada
- Establezca un nombre común para la CA (debe coincidir con el nombre de host del servidor):

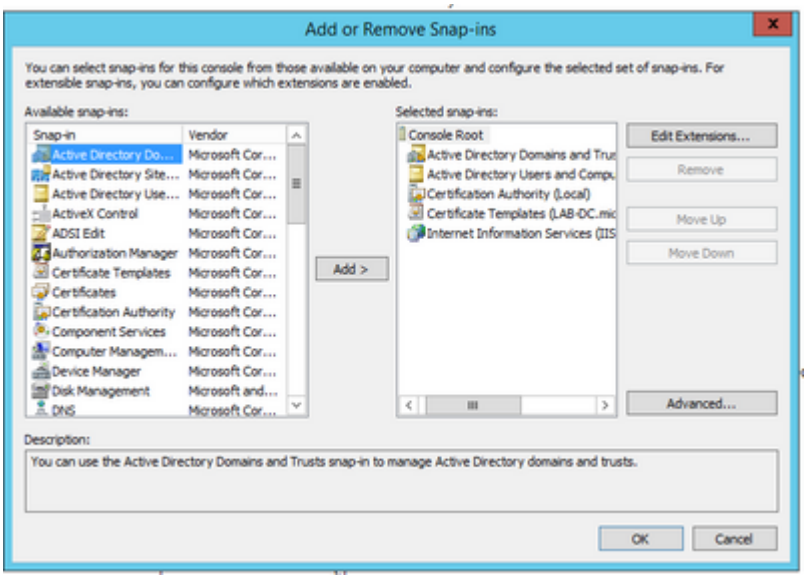


- Establecer validez para 5 años (o más si se desea)
- Seleccione el botón **Next** en el resto del asistente

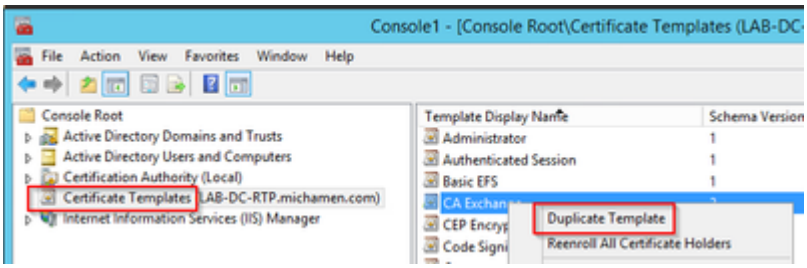
Creación de plantillas de certificados para CiscoRA

- Abra MMC. Seleccione el logotipo de inicio de Windows y escriba *mmc* en Ejecutar
- Abra una ventana MMC y agregue los siguientes complementos (utilizados en diferentes puntos de la configuración) y, a continuación, seleccione **Aceptar**:

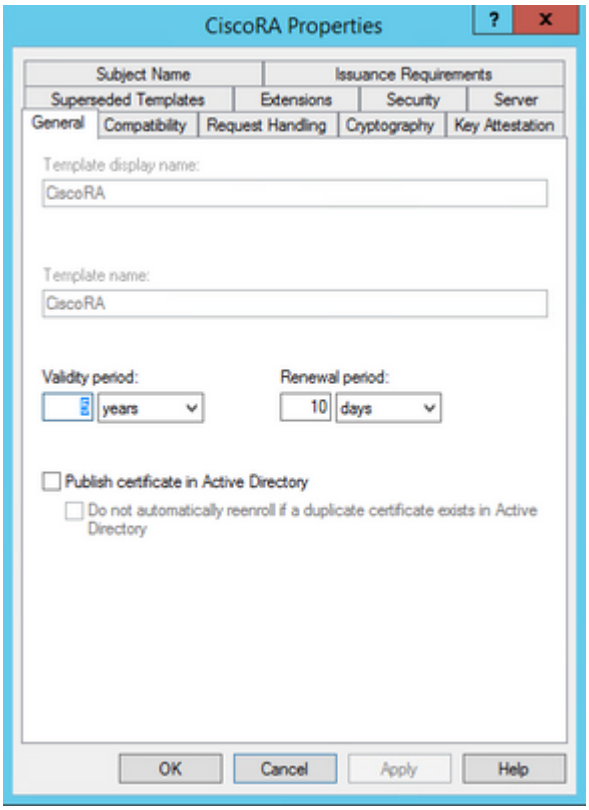




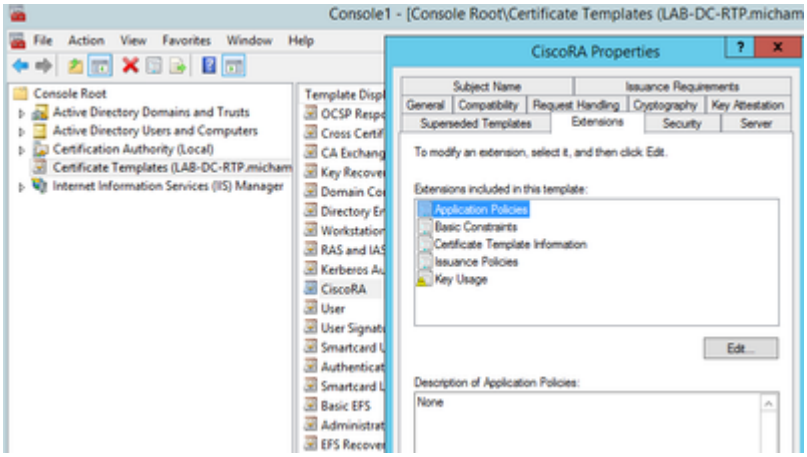
- Seleccione **File > Save** y guarde esta sesión de consola en el escritorio para acceder de nuevo rápidamente
- En los complementos, seleccione **Plantillas de certificado**
- Cree o clone una plantilla (preferiblemente la plantilla "*Entidad emisora de certificados raíz*", si está disponible) y asígnele el nombre CiscoRA



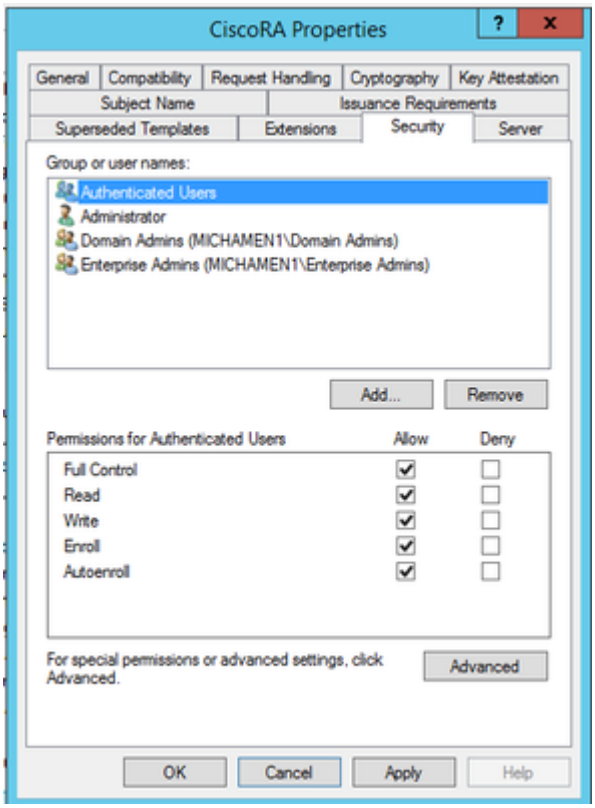
- Modifique la plantilla. Haga clic con el botón derecho del ratón y seleccione **Propiedades**
- Seleccione la pestaña **General** y establezca el período de validez en 20 años (u otro valor si lo desea). En esta ficha, asegúrese de que los valores "nombre para mostrar" y "nombre" de la plantilla coinciden



- Seleccione la ficha **Extensiones**, resalte **Directivas de aplicación** y, a continuación, seleccione **Editar**

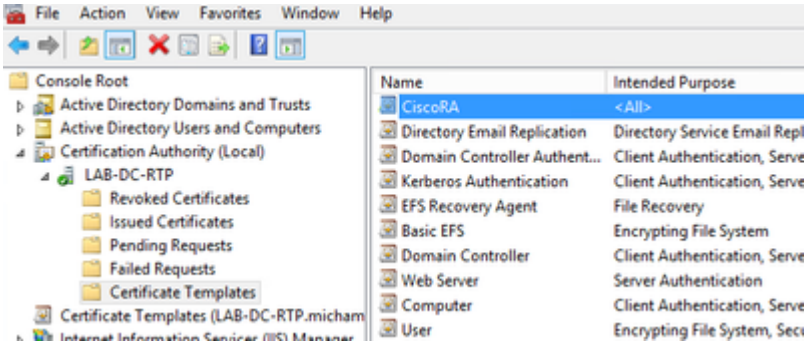


- Elimine las directivas que se muestran en la ventana que aparece
- Seleccione la pestaña **Nombre del asunto** y el botón de opción **Aprovisionar en solicitud**
- Seleccione la ficha **Seguridad** y conceda todos los permisos para todos los grupos o nombres de usuario que se muestran



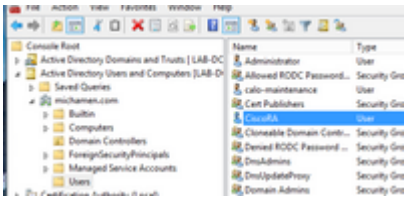
Hacer que la plantilla de certificado esté disponible para su emisión

- En los complementos MMC, seleccione **Entidad emisora de certificados** y expanda el árbol de carpetas para localizar la carpeta **Plantillas de certificados**
- Haga clic con el botón secundario en el espacio en blanco del marco que contiene Nombre y Propósito esperado
- Seleccione la plantilla **New** y **Certificate para emitir**
- Seleccione la plantilla de CiscoRA recién creada y editada



Creación de cuenta CiscoRA de Active Directory

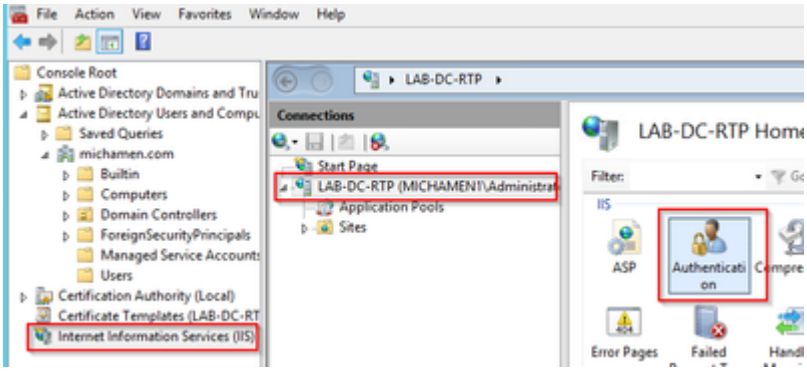
- Vaya a los complementos MMC y seleccione **Usuarios y equipos de Active Directory**
- Seleccione la carpeta **Users** en el árbol del panel del extremo izquierdo
- Haga clic con el botón secundario en el espacio en blanco del marco que contiene Nombre, Tipo y Descripción
- Seleccione **Nuevo** y **Usuario**
- Cree la cuenta CiscoRA con nombre de usuario/contraseña (*ciscora/Cisco123* se utilizó para este laboratorio) y seleccione la casilla de verificación Password never expires cuando se muestre



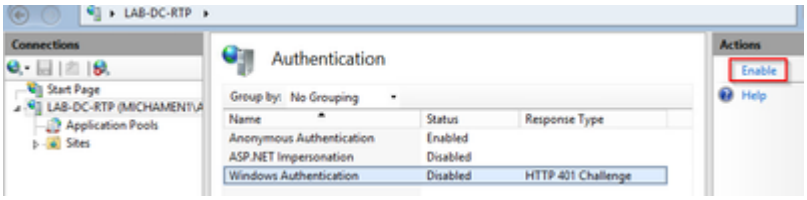
IIS Configuración de Autenticación y Enlace SSL

Habilitar NTLM Autenticación

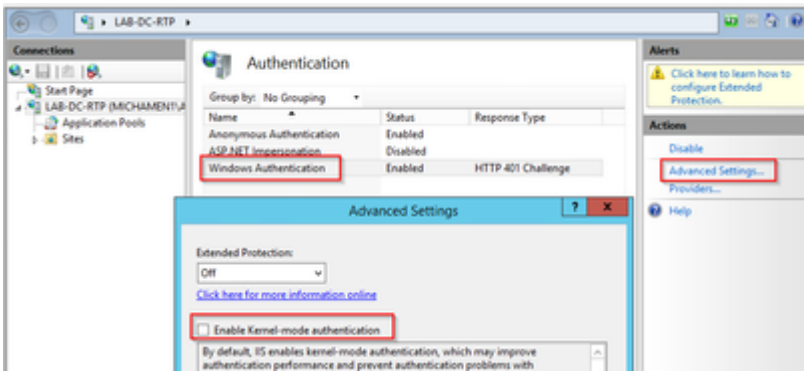
- Vaya a los complementos MMC y, en el complemento Administrador de Internet Information Services (IIS), seleccione el nombre del servidor
- La lista de funciones se muestra en el siguiente fotograma. Haga doble clic en el icono de la función **Authentication**



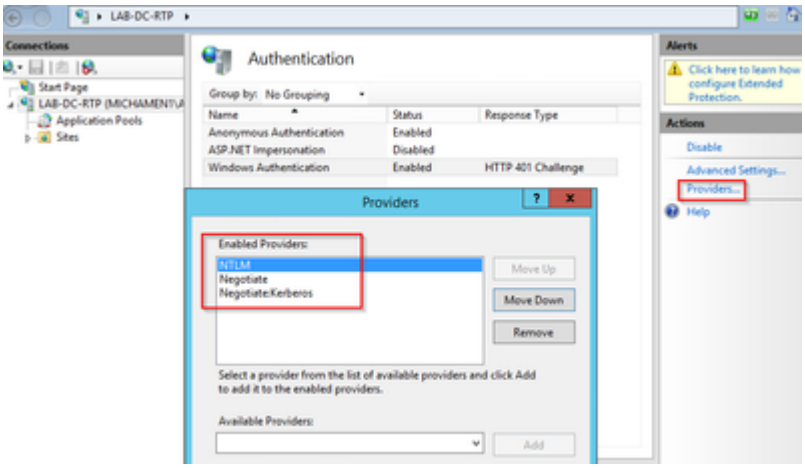
- Resalte **Autenticación de Windows** y en el marco Acciones (panel derecho) seleccione la opción **Habilitar**



- El panel Acciones muestra la opción **Configuración avanzada**; selecciónela y desactive **Habilitar autenticación en modo kernel**



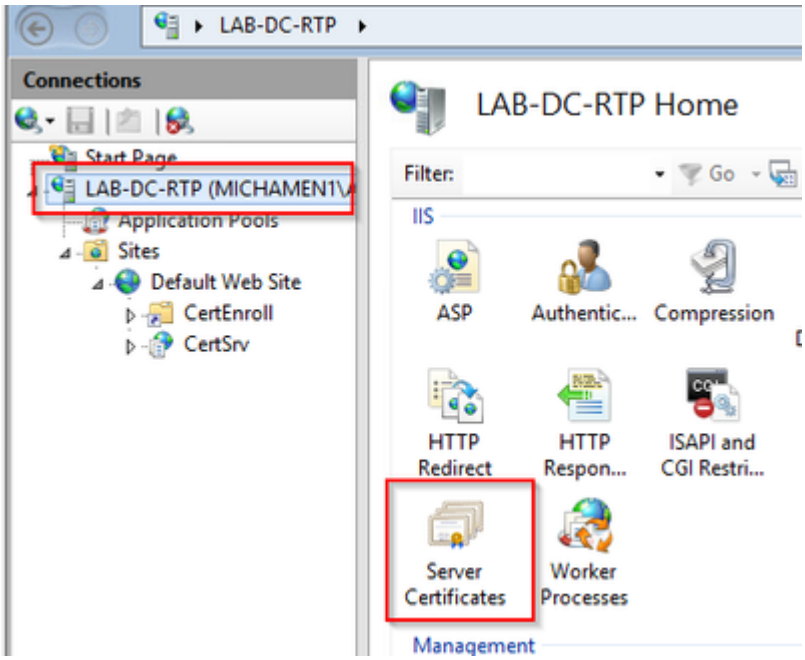
- Seleccione **Providers** y ponga en orden **NTML** y, a continuación, **Negotiate.**



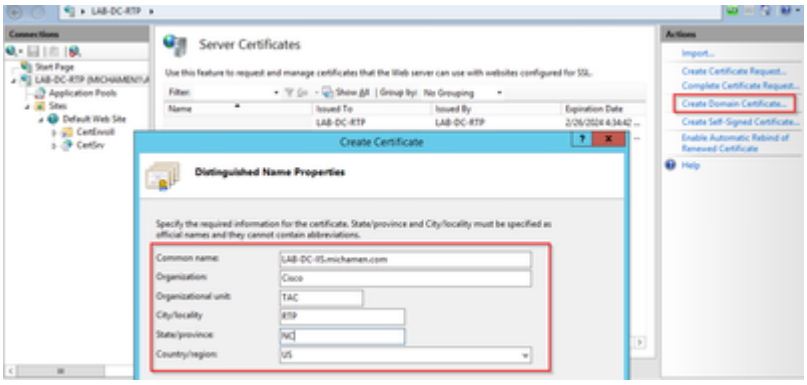
Generar el certificado de identidad para el servidor Web

Si todavía no es el caso, debe generar un certificado y un certificado de identidad para el servicio Web firmado por la CA porque CiscoRA no puede conectarse a él si el certificado del servidor Web es de firma automática:

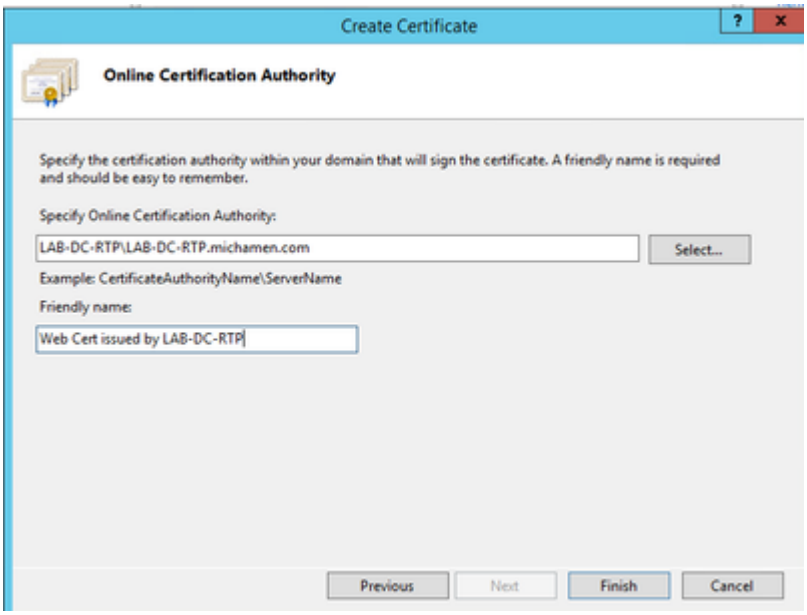
- Seleccione el servidor Web en el **complemento IIS** y haga doble clic en el icono de la función **Certificados de servidor**:



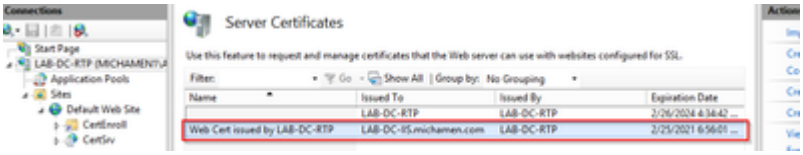
- De forma predeterminada, puede ver un certificado enumerado allí: el certificado de CA raíz autofirmado. En el menú **Acciones**, seleccione la opción **Crear certificado de dominio**. Ingrese los valores en el asistente de configuración para crear su nuevo certificado. Asegúrese de que el nombre común es un FQDN (nombre de dominio completamente calificado) que se pueda resolver y, a continuación, seleccione **Siguiente**:



- Seleccione el certificado de la CA raíz para que sea el emisor y seleccione **Finalizar**:

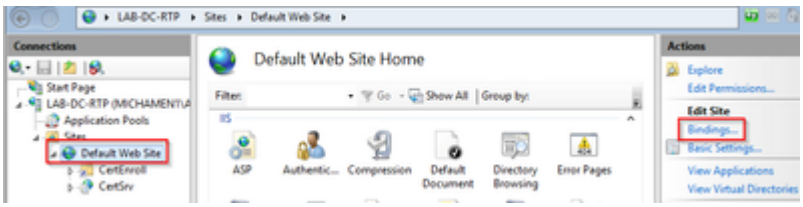


- Puede ver ambos, el certificado de CA y el certificado de identidad del servidor Web:

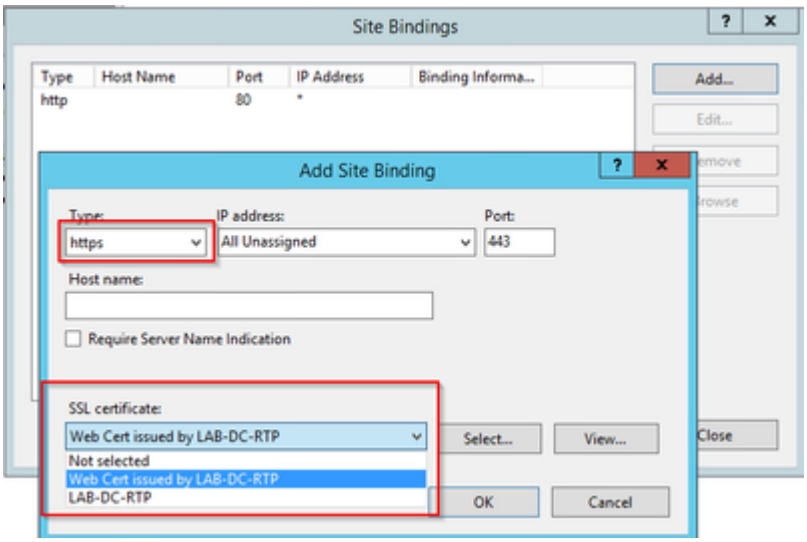


Enlace SSL de servidor web

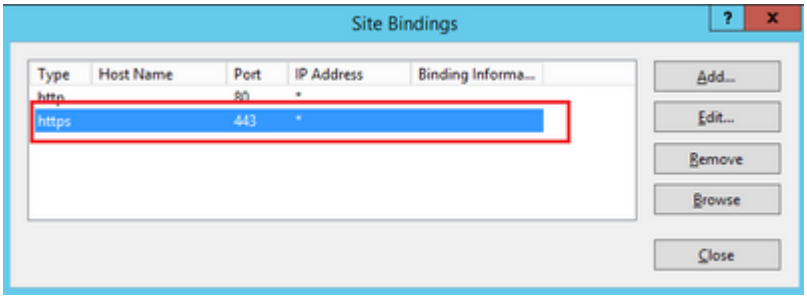
- Seleccione un sitio en la vista de árbol (puede utilizar el sitio Web predeterminado o hacerlo más granular para sitios específicos) y seleccione **Enlaces** en el panel Acciones. De este modo, aparece el editor de enlaces que permite crear, editar y eliminar enlaces para el sitio Web. Seleccione **Agregar** para agregar su nuevo enlace SSL al sitio.

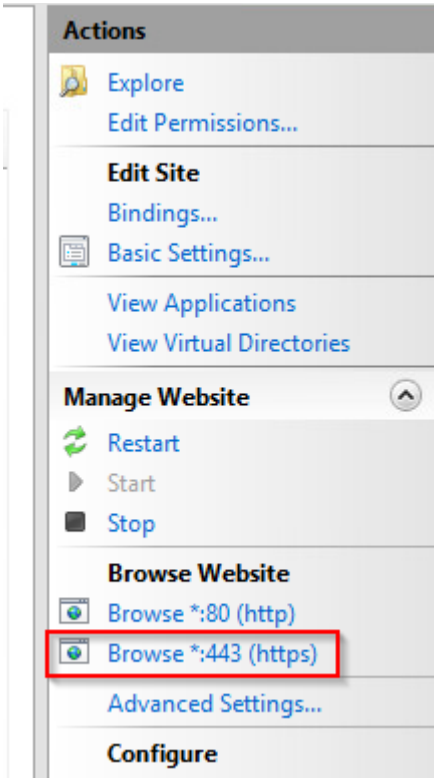


- La configuración predeterminada para un nuevo enlace se establece en HTTP en el puerto 80. Seleccione **https** en la lista desplegable **Type**. Seleccione el certificado autofirmado que creó en la sección anterior de la lista desplegable **Certificado SSL** y luego seleccione **Aceptar**.



- Ahora tiene un nuevo enlace SSL en su sitio y todo lo que queda es verificar que funciona seleccionando la opción **Browse *:443 (https)** del menú y asegúrese de que la página Web de IIS predeterminada utiliza HTTPS:

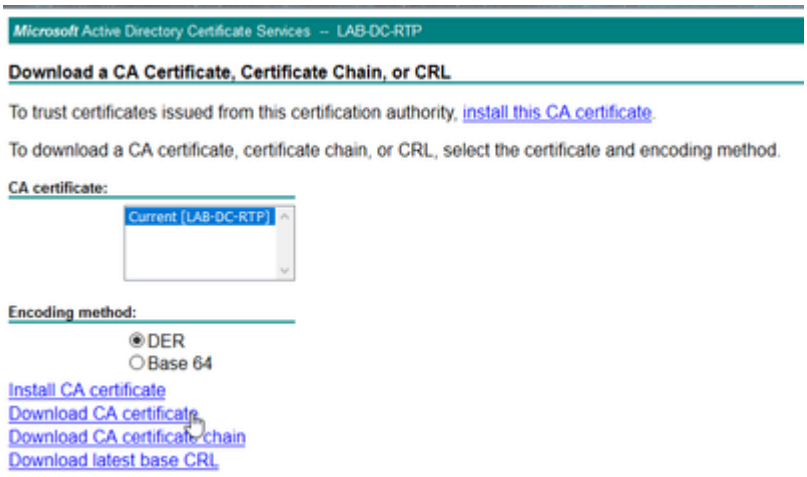




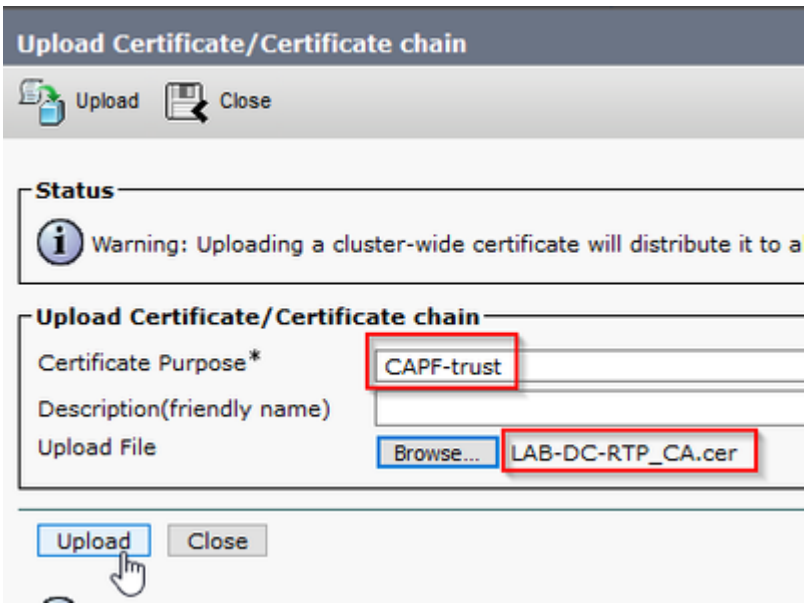
- Recuerde reiniciar el servicio IIS después de los cambios de configuración. Utilice la opción **Reiniciar** del panel Acciones.

Configuración de CUCM

- Vaya a la página web de AD CS (https://YOUR_SERVER_FQDN/certsrv/) y descargue el certificado de CA

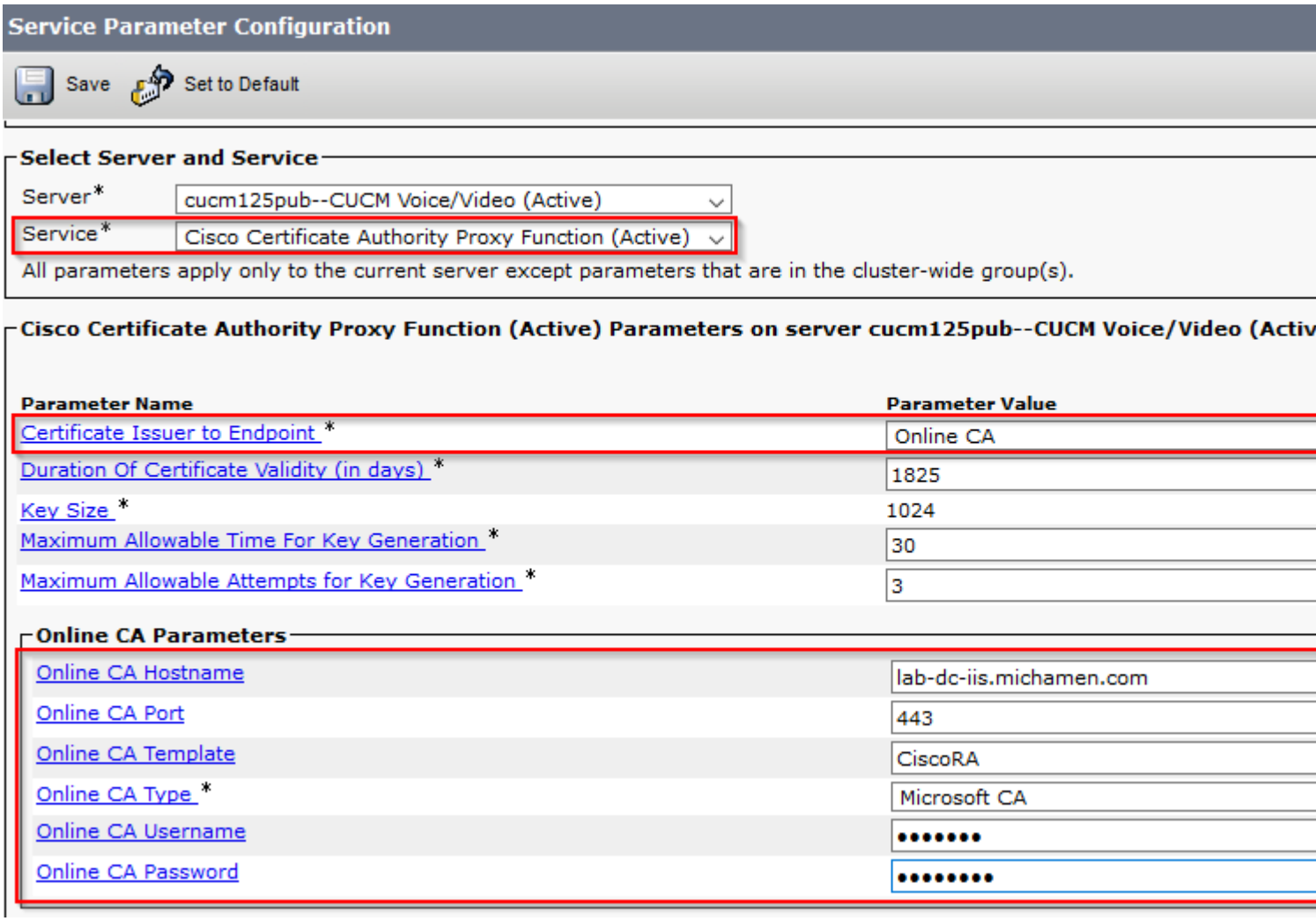


- Navegue hasta **Seguridad > Administración de certificados** desde la página Administración del SO y seleccione el botón **Cargar certificado/cadena de certificado** para cargar el certificado de CA con el *propósito* establecido en *CAPF-trust.*

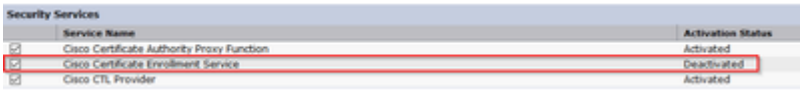


... En este punto, también es buena idea cargar ese mismo certificado de CA como *CallManager-trust* porque es necesario si el cifrado de señalización segura está habilitado (o se habilitará) para los terminales; lo que es probable si el clúster está en modo mixto.

- Vaya a **Sistema > Parámetros de servicio.** Seleccione el servidor del Publicador de Unified CM en el campo del servidor y **Cisco Certificate Authority Proxy Function** en el campo Servicio
- Establezca el valor de Emisor de certificado en Terminal en CA en línea e introduzca los valores para los campos Parámetros de CA en línea. Asegúrese de utilizar el FQDN del servidor Web, el nombre de la plantilla de certificado creada anteriormente (CiscoRA), el tipo de CA como CA de Microsoft y las credenciales de la cuenta de usuario de CiscoRA creada anteriormente



- Una ventana emergente le informa de que es necesario reiniciar el servicio CAPF. Pero primero, active Cisco Certificate Enrollment Service a través de **Cisco Unified Serviceability > Tools > Service Activation**, seleccione el publicador en el campo Server y marque la casilla de verificación Cisco Certificate Enrollment Service, y luego seleccione el botón **Save**:



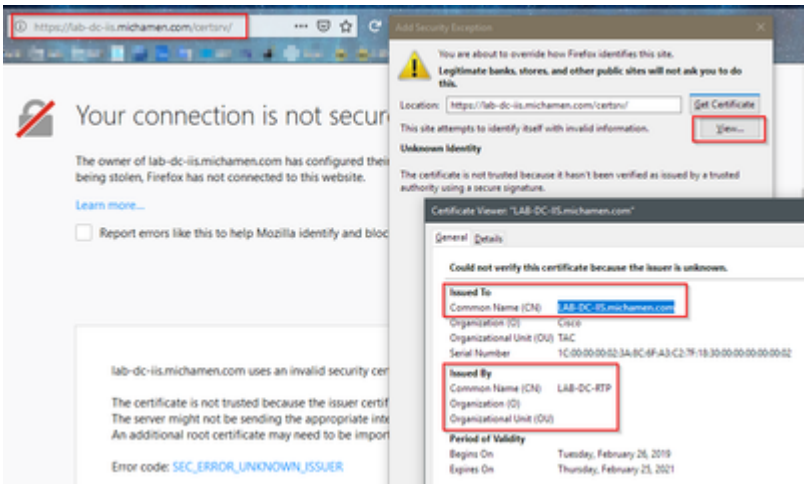
Verificación

Verificar certificados IIS

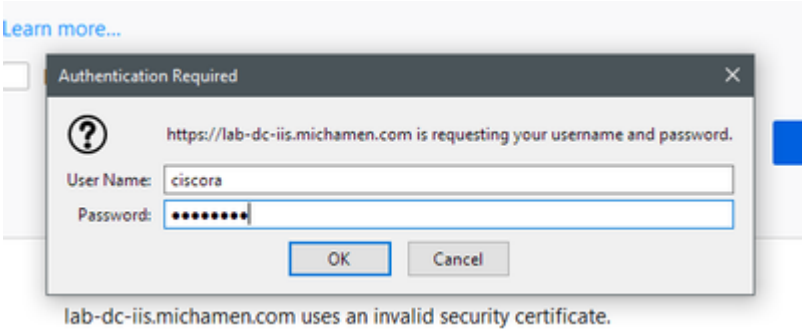
- Desde un explorador Web en un PC con conectividad al servidor (preferiblemente en la misma red que el publicador de CUCM), navegue hasta la dirección URL:

  https://YOUR_SERVER_FQDN/certsrv/

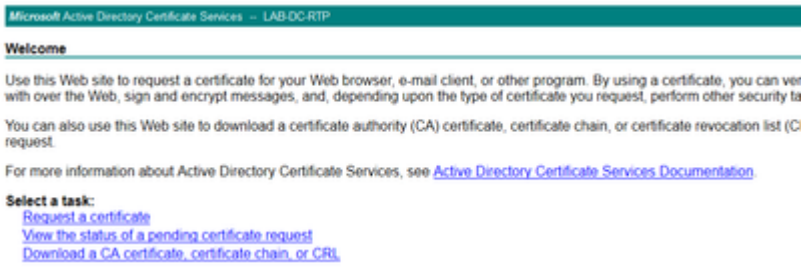
- Se muestra la alerta de certificado no fiable. Agregue la excepción y compruebe el certificado. Asegúrese de que coincide con el FQDN esperado:



- Después de aceptar la excepción, debe autenticarse; en este punto, debe utilizar las credenciales configuradas para la cuenta CiscoRA anteriormente:



- Después de la autenticación, debe poder ver la página de bienvenida de AD CS (Servicios de certificados de Active Directory):



Verificar configuración de CUCM

Realice los pasos que sigue normalmente para instalar un certificado LSC en uno de los teléfonos.

Paso 1. Abra la página CallManager Administration, Device y luego Phone

Paso 2. Seleccione el botón **Find** para mostrar los teléfonos

Paso 3. Seleccione el teléfono en el que desea instalar el LSC

Paso 4. Desplácese hasta Información de la función proxy de la entidad de certificación (CAPF)

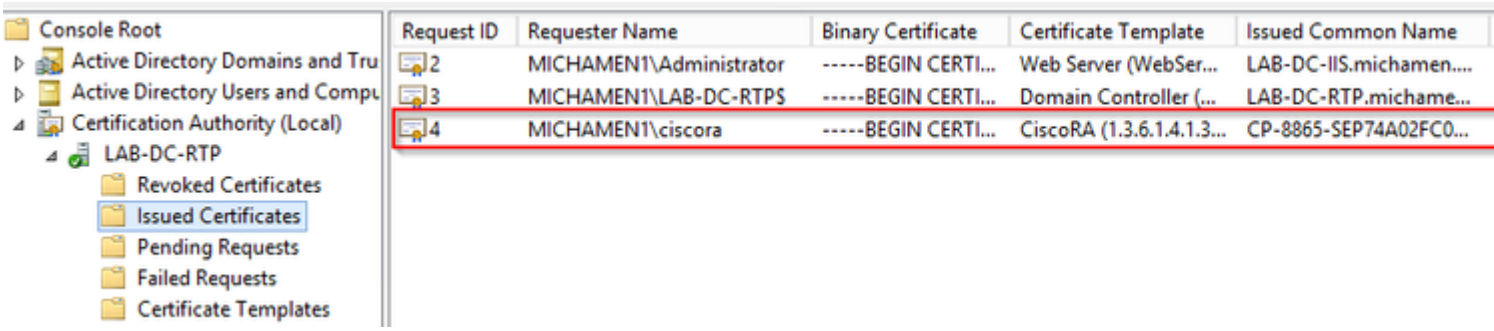
Paso 5. Seleccione la opción Instalar/Actualizar en la operación de certificado.

Paso 6. Seleccione el modo de autenticación. (By Null String is fine for test purposes)

Paso 7. Desplácese hasta la parte superior de la página y seleccione **save** y **Apply Config** para el teléfono.

Paso 8. Después de que el teléfono se reinicie y vuelva a registrarse, utilice el filtro Estado de LSC para confirmar que el LSC se ha instalado correctamente.

- En el servidor de AD, abra MMC y expanda el complemento Entidad de certificación para seleccionar la carpeta Certificados emitidos
- La entrada del teléfono se muestra en la vista de resumen. Estos son algunos de los detalles que se muestran:
  - ID de solicitud: número de secuencia único
  - Nombre del solicitante: se debe mostrar el nombre de usuario de la cuenta CiscoRA configurada
  - Plantilla de certificado: debe mostrarse el nombre de la plantilla de CiscoRA creada
  - Nombre común emitido: se debe mostrar el modelo del teléfono anexado al nombre del dispositivo
  - Fecha en Vigor del Certificado y Fecha de Vencimiento del Certificado



Enlaces relacionados

- **Troubleshooting de CAPF Online CA**
- **Soporte Técnico y Documentación - Cisco Systems**

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).