# Crear certificado raíz personalizado de Umbrella con Servicios de certificados de AD

## Contenido



## Introducción

Este documento describe instrucciones para crear un certificado raíz personalizado mediante los Servicios de certificados de Active Directory (AD) de Microsoft Windows.

## Prerequisites

### Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Una versión de Microsoft Windows Server que actualmente es compatible con Microsoft
- Servicios de certificados de Active Directory instalados en Windows Server
- Una cuenta con las funciones Servicios de certificados de Active Directory y Servicio web/Servicio de inscripción en web
- Servicios de Certificate Server configurados para emitir certificados con codificación UTF-8 ("UTF8STRING")

### Componentes Utilizados

La información de este documento se basa en Cisco Umbrella.

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.

# Overview

Este artículo contiene instrucciones para crear un certificado raíz personalizado (que se utiliza en lugar del certificado estándar de la CA raíz de Cisco Umbrella) mediante los Servicios de certificados de Active Directory de Microsoft Windows y, a continuación, utilizar ese certificado raíz para firmar una Solicitud de firma de certificado (CSR) desde la función de certificado CA firmado por el cliente de Umbrella.

# Codificación de cadena de certificado

Si los Servicios de Certificate Server están configurados para utilizar la codificación predeterminada ("PRINTABLESTRING"), la cadena de certificados generada no puede ser de confianza para ciertos clientes web, especialmente Firefox.

El proxy de Cisco Umbrella Secure Web Gateway utiliza una cadena de certificados que codifica cadenas con codificación UTF8STRING. Si su certificado de emisión (por ejemplo, su certificado raíz) que firma el CSR para crear el certificado intermedio de la CA de Cisco Umbrella Customers está codificado con PRINTABLESTRING, la codificación del campo Asunto del certificado de la CA de Cisco Umbrella Customers es PRINTABLESTRING. Esta codificación no puede coincidir con la codificación UTF8STRING del campo Emisor del certificado intermedio de CA Cisco Umbrella R1, que es el siguiente en la cadena de certificados.

RFC 5280 La sección 4.1.2.6 requiere que una cadena de certificados mantenga la misma codificación de cadena entre el campo Emisor de un certificado emitido y el campo Asunto del certificado emisor:

"Cuando el sujeto del certificado es una CA, el campo de asunto DEBE codificarse de la misma manera que se codifica en el campo del emisor (sección 4.1.2.4) en todos los certificados emitidos por la CA del sujeto."

Muchos navegadores no hacen cumplir este requisito, pero algunos (más notablemente Firefox) lo hacen. Como resultado, los clientes web como Firefox pueden generar un error de sitio no fiable y no cargar sitios web cuando se usa Secure Web Gateway (SWG) con la función de certificado CA firmado por CA del cliente.

Para solucionar este problema, utilice un navegador como Chrome, que no aplica los requisitos de RFC 5280.

# Paso 1: Preparando plantilla de Servicios de Certificate Server de AD

1. Abra la Autoridad de certificación de Active Directory MMC navegando hasta Inicio > Ejecutar > MMC.

2. Seleccione Archivo > Agregar o quitar complemento y agregue los complementos Plantillas de certificado y Entidad de certificación. Seleccione Aceptar.

3. Expanda Plantillas de certificado y haga clic con el botón derecho en Autoridad de certificación

subordinada. Haga clic en Plantilla duplicada.

Ahora puede crear una plantilla de certificado personalizada para cumplir con los requisitos enumerados en la documentación de Umbrella.

Estos son los requisitos que se detallan en el momento de la creación de este artículo:

- Ficha General
  - Asigne a la plantilla un nombre que le represente un significado.
  - Establezca el Período de validez para 35 meses (3 años menos al mes).
  - Establezca el Período de renovación en 20 Días.
- Ficha Extensiones
  - Haga doble clic en Restricciones básicas.
    - Asegúrese de que la opción Make this extension critical esté seleccionada.
  - En Uso de claves:
    - Asegúrese de que la opción Firma de certificado & Firma de CRL esté seleccionada.
    - Anule la selección de Firma digital.
    - Asegúrese de que Make this extension critical esté marcado aquí también.
- Seleccione Apply y OK.

## Paso 2: Emita la plantilla

1. Vuelva a la MMC que configuró en el paso 2 del proceso anterior, expanda la sección Autoridad de certificación.

2. En la sección recién expandida, haga clic con el botón derecho en la carpeta Plantillas de certificado y seleccione Nuevo > Plantilla de certificado para emitir.

3. En la nueva ventana, seleccione el nombre de la plantilla de certificado que creó en la última sección y seleccione Aceptar.

La CA ya está lista para facilitar la solicitud.

## Paso 3: Descarga y firma del CSR

1. Inicie sesión en el Panel de Umbrella (https://dashboard.umbrella.com).

2. Vaya a Despliegues > Configuración > Certificado raíz.

3. Seleccione el icono Agregar (+) en la esquina y asigne un nombre a la CA en la nueva ventana.

4. Descargue la Solicitud de firma de certificado (CSR).

5. En una nueva pestaña del explorador, navegue hasta los servicios web para Servicios de certificados de Active Directory. (Si utiliza un equipo local, sería 127.0.0.1/certsrv/ o similar.)

6. En la nueva página, seleccione Solicitar un Certificado.

7. Seleccione Solicitud de Certificado Avanzada.

8. En Solicitud guardada, copie y pegue el contenido del CSR que descargó en el paso 4 (debe abrirlo con un editor de texto).

9. En Plantilla de certificado, seleccione el nombre de la plantilla de certificado que creó en la sección "Preparación de la plantilla de Servicios de Certificate Server de AD" y seleccione Enviar.

10. Asegúrese de seleccionar Base64 Codificado y seleccione Descargar certificado y tome nota de la ubicación del archivo .cer.

## Paso 4: Cargar la CSR firmada (y el certificado raíz público)

1. En el Panel de Control de Umbrella, navegue hasta Implementación > Configuración > Certificado Raíz.

2. Seleccione el certificado raíz que creó en el paso 3 de la sección anterior.

3. Seleccione Cargar CA en la esquina inferior derecha de la línea*.

4. Seleccione el botón Examinar superior (Autoridad de Certificación (CSR firmado)).

5. Busque la ubicación del archivo .cer que creó en la sección anterior y seleccione Guardar.

6. Seleccione Siguiente y los grupos de ordenadores/usuarios con los que desea utilizar el certificado (en lugar del certificado raíz de Cisco) y seleccione Guardar.

*También puede cargar el certificado de la CA de forma opcional. Se puede recuperar desde la interfaz web del servidor de la entidad emisora de certificados (http://127.0.0.1/certsrv/) y, a continuación, seleccionando Descargar certificado de CA, cadena de certificados o CRL. Complete las indicaciones en pantalla para "Descargar el certificado de CA" en Base 64.

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).