Cargar certificado personalizado en el punto de acceso inalámbrico Cisco Business

Objetivo

El objetivo de este documento es mostrar cómo cargar un certificado personalizado en su punto de acceso (AP) Cisco Business Wireless (CBW).

Dispositivos aplicables | Versión de software

- Punto de acceso Cisco Business Wireless 140AC | 10.6.1.0 (última descarga)
- Punto de acceso Cisco Business Wireless 145AC | 10.6.1.0 (última descarga)
- Punto de acceso Cisco Business Wireless 240AC | 10.6.1.0 (última descarga)

Introducción

En la versión de firmware 10.6.1.0 de los AP CBW y posteriores, ahora puede importar sus propios certificados WEBAUTH (que gestiona la página del portal cautivo) o WEBADMIN (la página CBW Primary AP Management) a la interfaz de usuario web (UI) en la que pueden confiar sus dispositivos y sistemas internos. De forma predeterminada, las páginas WEBAUTH y WEBADMIN utilizan certificados autofirmados que normalmente no son de confianza y pueden dar lugar a advertencias de certificado cuando intenta conectarse a su dispositivo.

Con esta nueva función, puede cargar fácilmente certificados personalizados en su punto de acceso CBW. Comencemos.

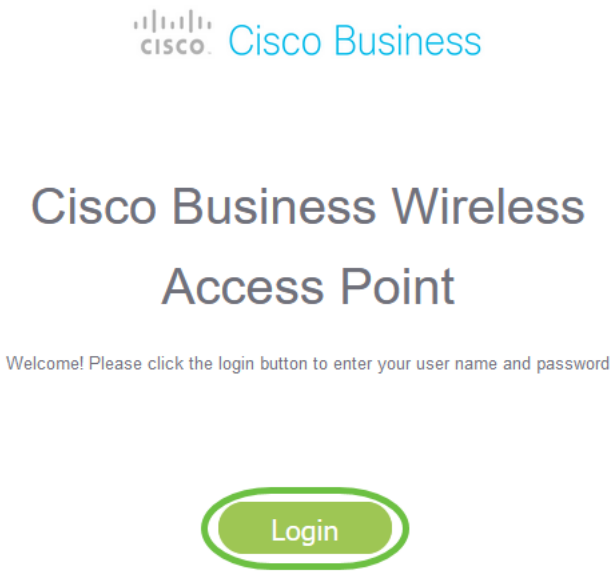
Prerequisites

- Asegúrese de haber actualizado el firmware de CBW AP a 10.6.1.0. Haga clic si desea obtener instrucciones paso a paso para realizar una actualización del firmware.
- Se necesita una autoridad de certificación privada o interna (CA) para emitir los certificados WEBAUTH o WEBADMIN necesarios para CBW. Los certificados se pueden instalar en cualquier equipo de administración que pueda conectarse a la interfaz de usuario web de CBW.
- El certificado de CA raíz correspondiente se debe instalar en el explorador del cliente para utilizar el certificado personalizado para el portal cautivo o el acceso de administración para evitar posibles advertencias de certificado.
- CBW utiliza una dirección IP redirigida internamente 192.0.2.1 para la redirección del portal cautivo. Por lo tanto, es mejor incluirlo como el nombre común (CN) o el nombre alternativo del asunto (SAN) del certificado WEBAUTH.
- Los requisitos de nombres para los certificados WEBADMIN incluyen: CN-cisobusiness.cisco; SAN debe ser dns-ciscobusiness.cisco; si se utiliza una dirección IP estática, la SAN también puede incluir dns=<ip address>.

Cargar certificados

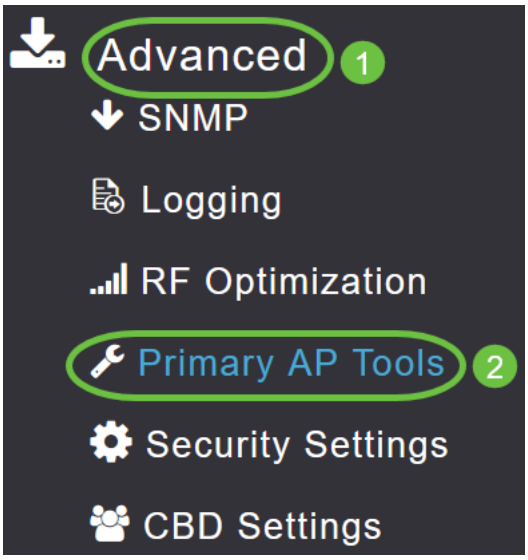
Paso 1

Inicie sesión en la interfaz de usuario web del punto de acceso CBW.



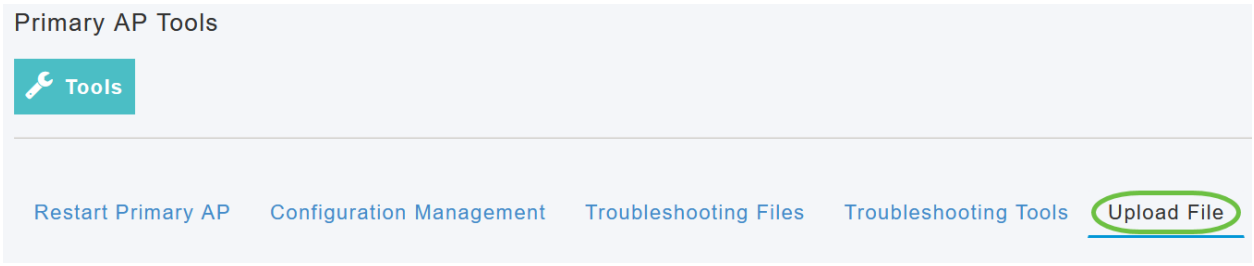
Paso 2

Para cargar certificados, vaya **a Advanced > Primary AP Tools**.



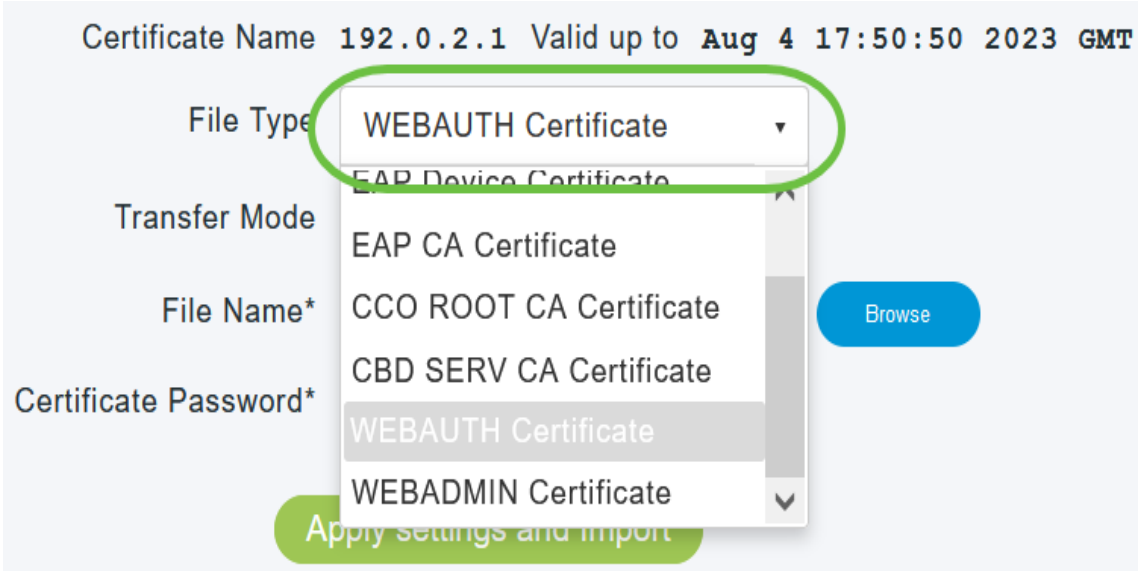
Paso 3

Elija la pestaña **Cargar archivo**.



Paso 4

En el menú desplegable *Tipo de archivo*, elija *WEBAUTH* o *Certificado WEBADMIN*.



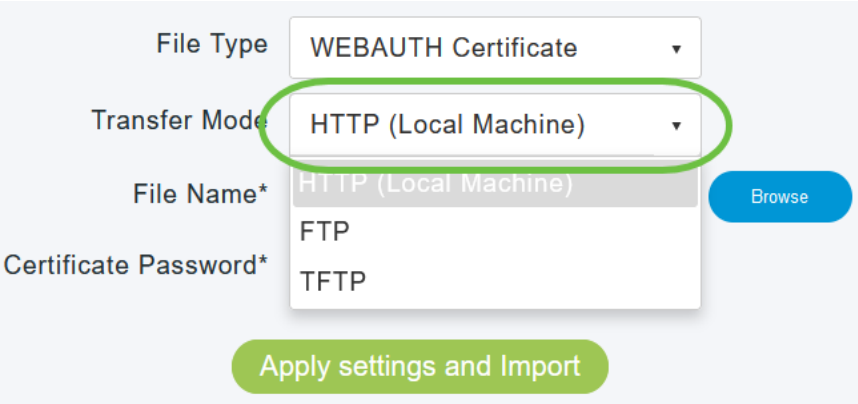
Los archivos DEBEN estar en formato PEM y deben contener las claves Public y Private. También debe estar protegido mediante contraseña. Los certificados WEBAUTH y WEBADMIN DEBEN tener un nombre común (CN) como ciscobusiness.cisco. Por lo tanto, deberá utilizar una CA interna para emitir certificados.

Paso 5

Elija el *Modo de transferencia* en el menú desplegable. Las opciones son:

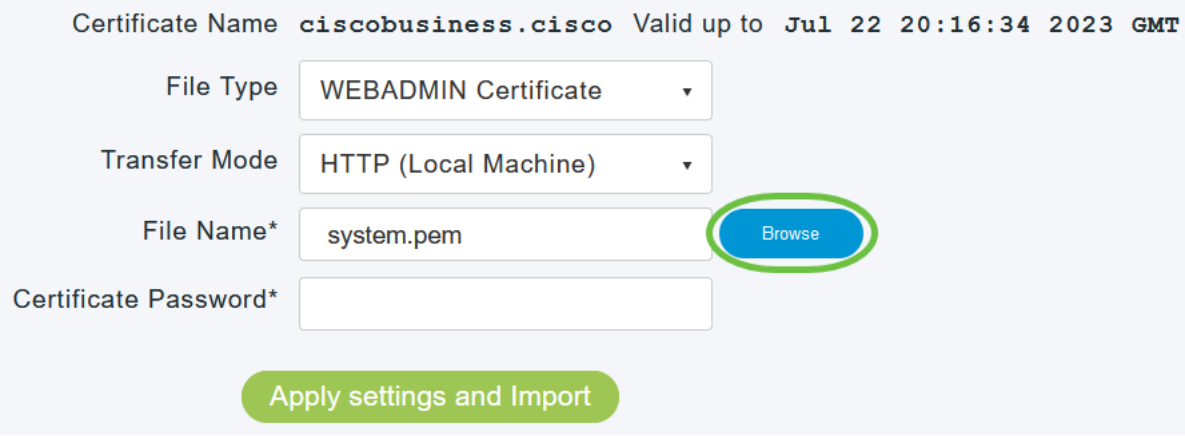
- *HTTP (máquina local)*
- *FTP*
- *TFTP*

En este ejemplo, se selecciona **HTTP**.



Paso 6

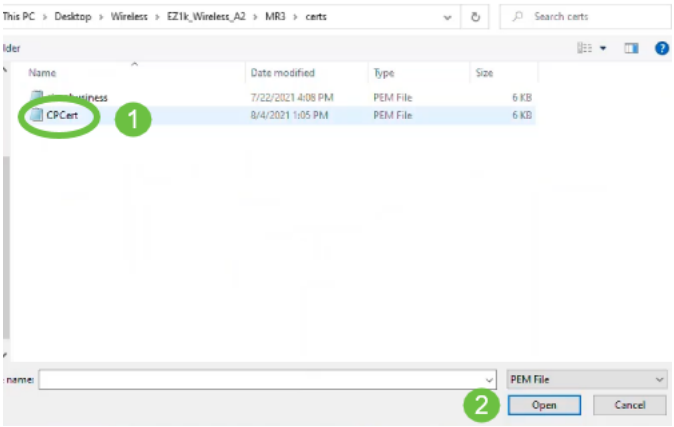
Haga clic en **Examinar**.



Si el *modo de transferencia* es *FTP o TFTP*, introduzca la *dirección IP del servidor, la ruta de acceso del archivo* y otros campos obligatorios.

Paso 7

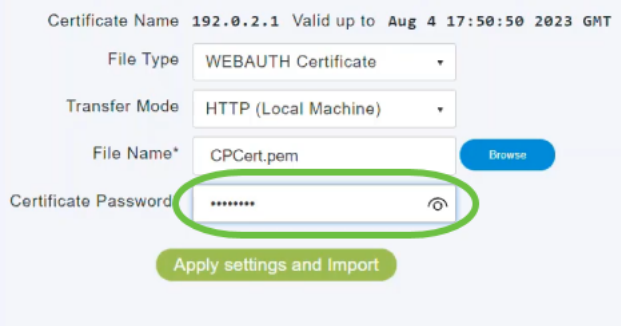
Para cargar el archivo desde el PC local, vaya a la carpeta que contiene el certificado personalizado. Seleccione el archivo de certificado y haga clic en **Abrir**.



El certificado debe ser un archivo PEM.

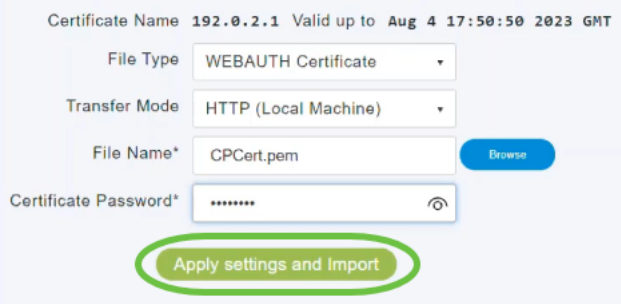
Paso 8

Introduzca la *contraseña del certificado*.



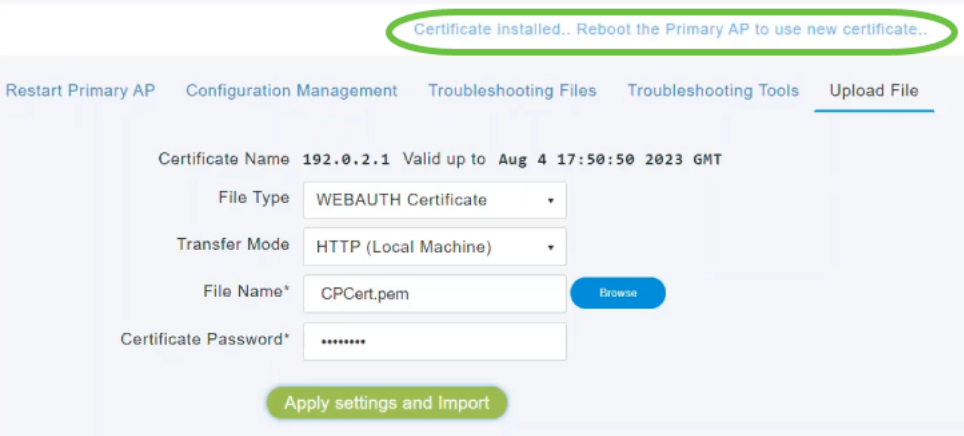
Paso 9

Haga clic en **Aplicar configuración e Importar**.



Paso 10

Verá una notificación una vez que el certificado se haya instalado correctamente. Reinicie el AP primario.



Para cambiar el certificado, simplemente cargue un nuevo certificado. Esto sobrescribirá el certificado que se instaló anteriormente. Si desea volver al certificado autofirmado predeterminado, deberá restablecer de fábrica el AP primario.

Conclusión

¡Todos están listos! Ahora ha cargado correctamente los certificados personalizados en su punto de acceso CBW.