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 el punto de acceso (AP) Cisco Business Wireless (CBW).

Dispositivos aplicables | Versión de software

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

Introducción

En la versión de firmware 10.6.1.0 y posterior de los puntos de acceso de CBW, ahora puede importar sus propios certificados WEBAUTH (que administra la página del portal cautivo) o WEBADMIN (la página de administración del punto de acceso principal de CBW) en la interfaz de usuario (IU) web 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 al dispositivo.

Con esta nueva función, puede cargar fácilmente certificados personalizados en su AP CBW. Comencemos ahora mismo.

Prerequisites

- Asegúrese de que ha actualizado el firmware de CBW AP a 10.6.1.0. Haga clic en si

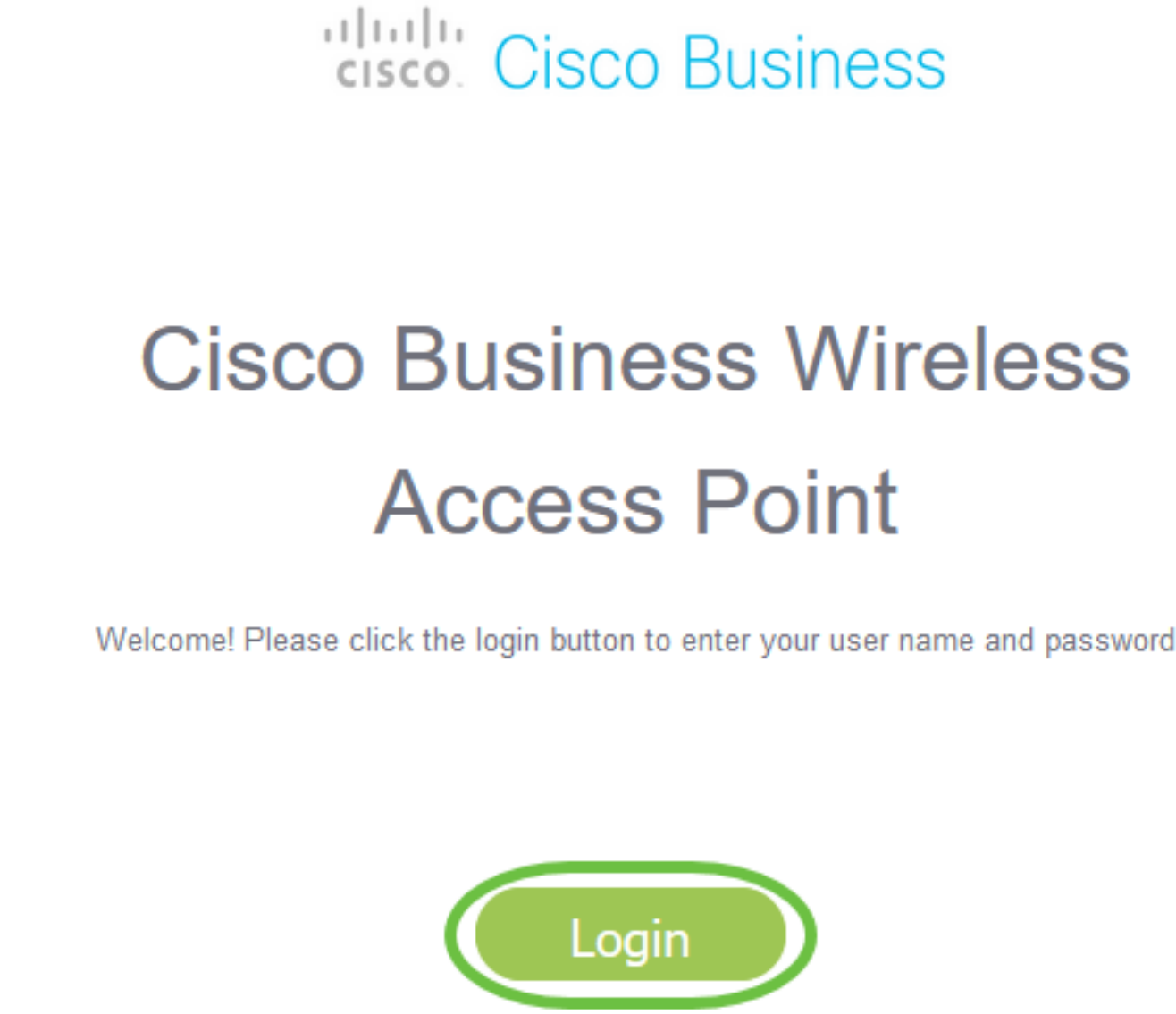
desea obtener instrucciones paso a paso sobre cómo realizar una actualización del firmware.

- Se necesita una autoridad de certificación (CA) privada o interna para emitir los certificados WEBAUTH o WEBADMIN necesarios para CBW. Los certificados se pueden instalar en cualquier PC de administración que se pueda conectar a la interfaz de usuario web de CBW.
- El certificado de CA raíz correspondiente debe estar instalado en el explorador del cliente para utilizar el certificado personalizado para el portal cautivo o el acceso a la 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 incluir esto como el nombre común (CN) o el nombre alternativo del sujeto (SAN) del certificado WEBAUTH.
- Los requisitos de denominación para los certificados WEBADMIN incluyen: CN-cisobusiness.cisco; La SAN debe ser dns-ciscobusiness.cisco; si se utiliza una dirección IP estática, la SAN también puede incluir dns=<dirección ip>.

Cargar certificados

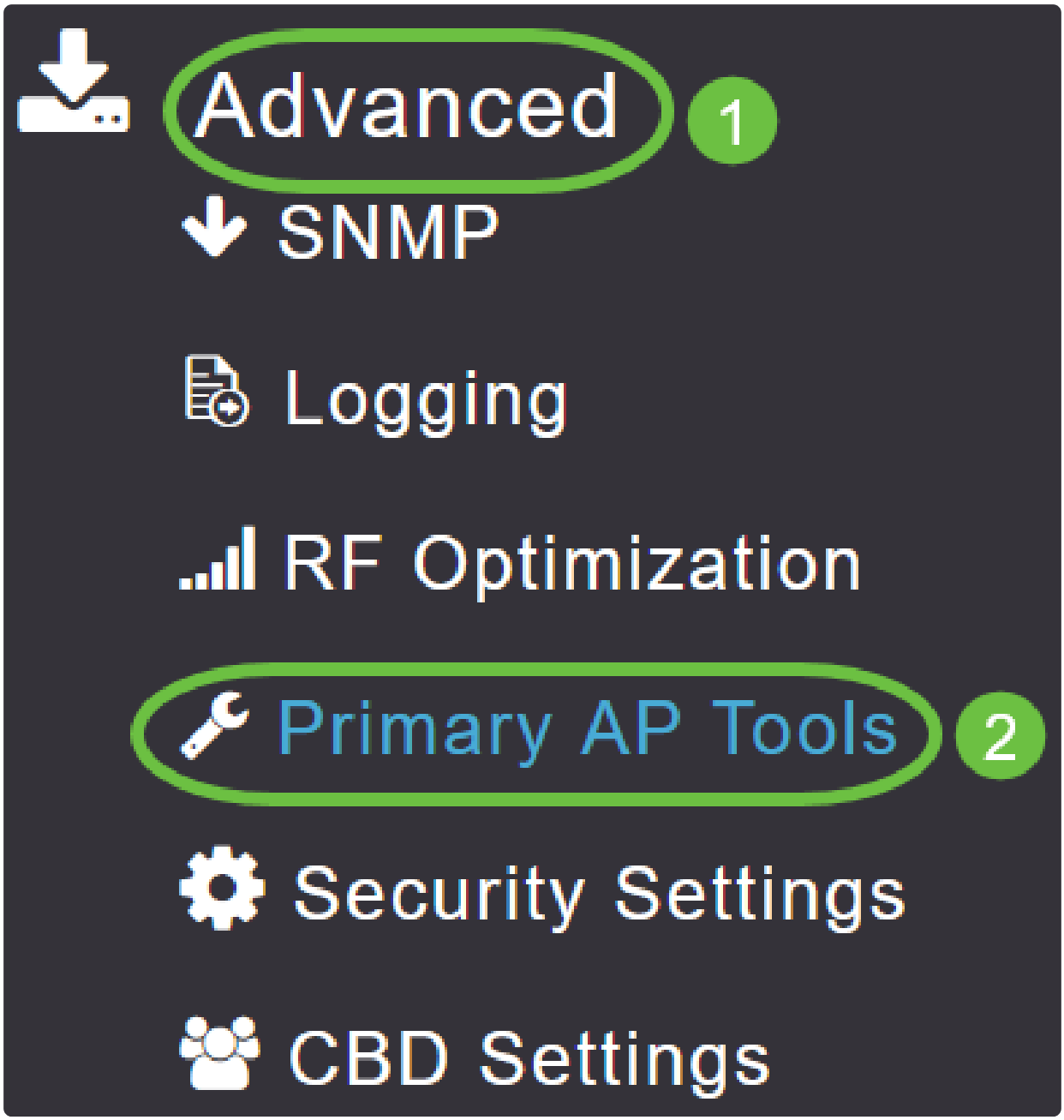
Paso 1

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



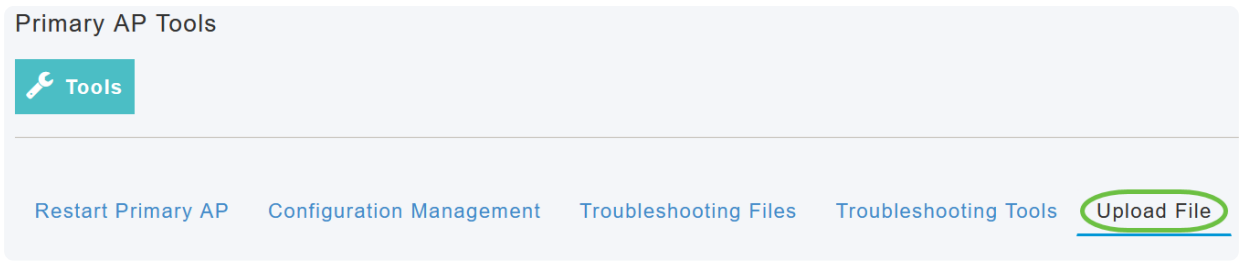
Paso 2

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



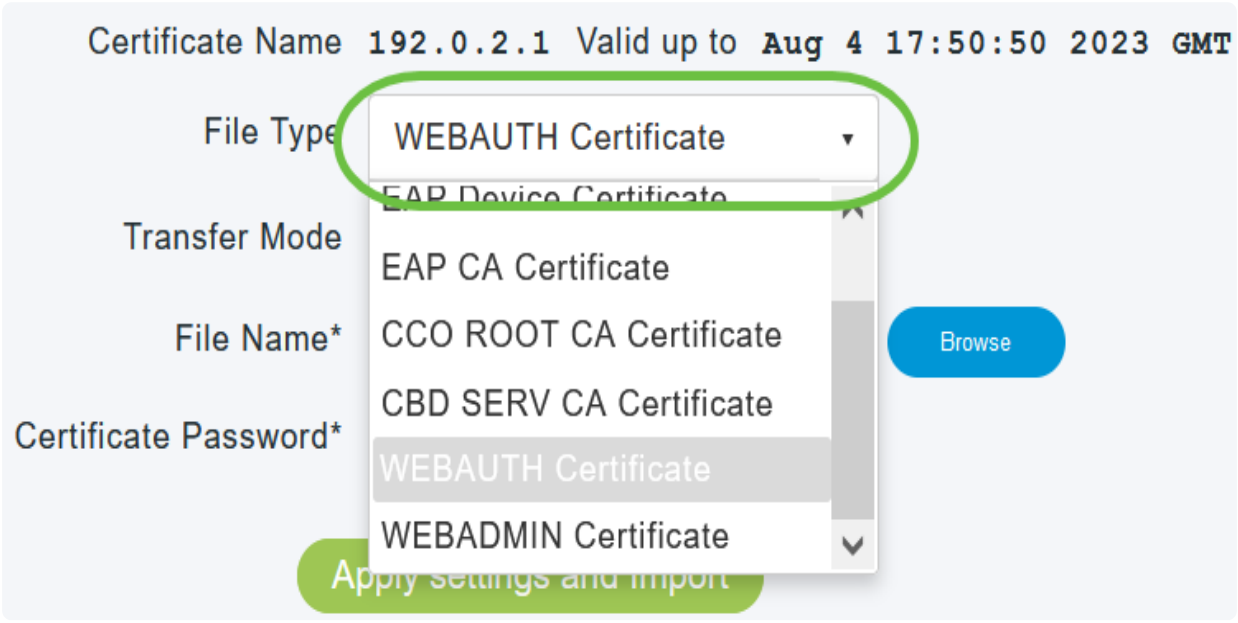
Paso 3

Elija la pestaña Cargar archivo.



Paso 4

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



ⓘ Note:

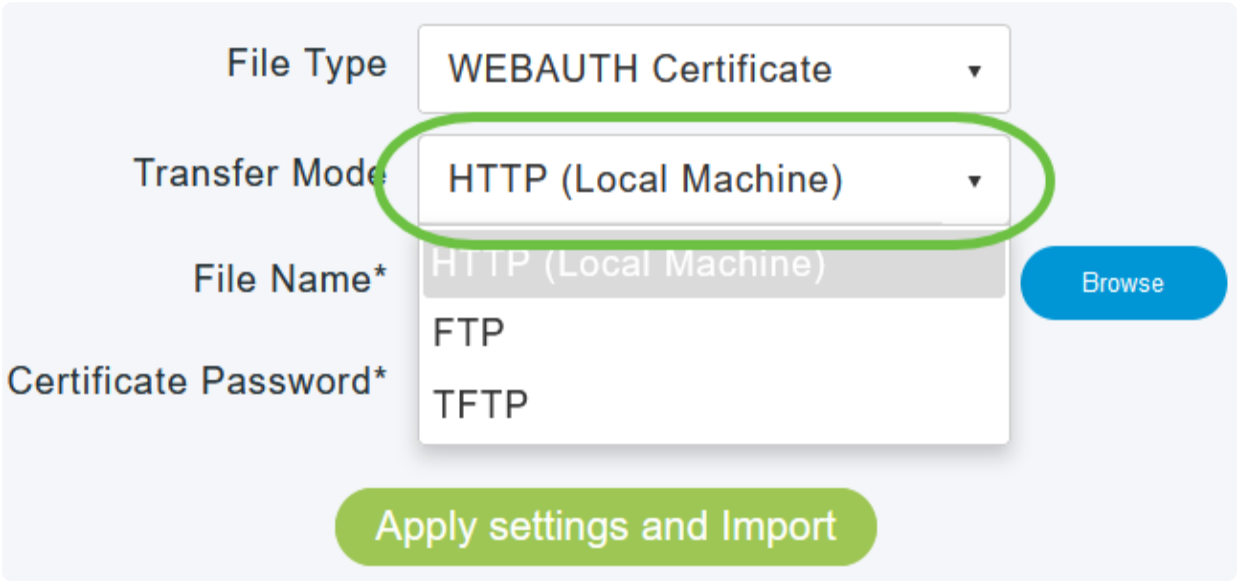
Los archivos DEBEN estar en formato PEM y contener las claves Public y Private. También debe estar protegida por contraseña. Tanto los certificados WEBAUTH como WEBADMIN DEBEN tener un nombre común (CN) como ciscobusiness.cisco. Por lo tanto, deberá utilizar una CA interna para emitir certificados.

Paso 5

Elija Transfer Mode en el menú desplegable. Las opciones son:

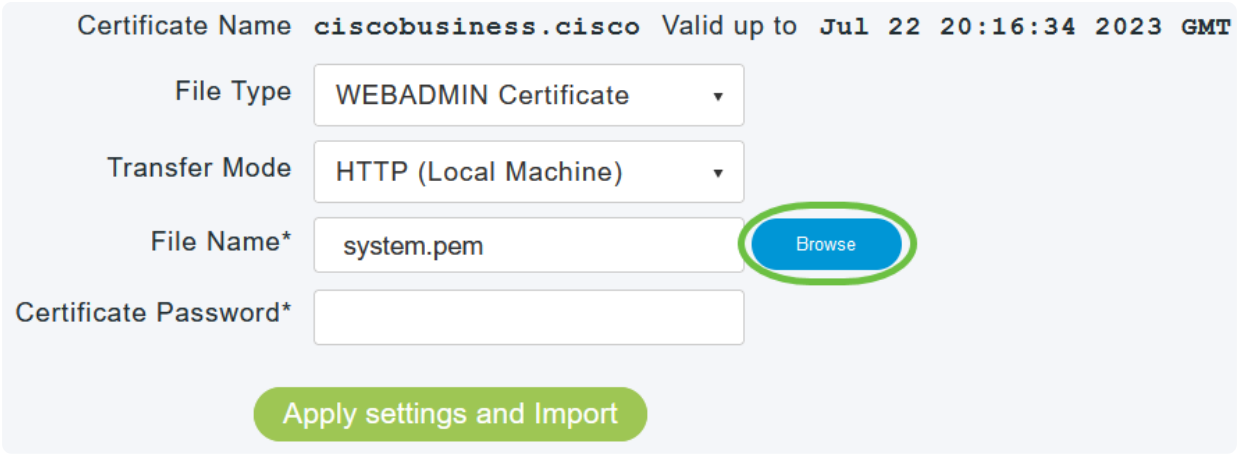
- HTTP (equipo local)
- FTP
- TFTP

En este ejemplo, se selecciona HTTP.



Paso 6

Haga clic en Browse.

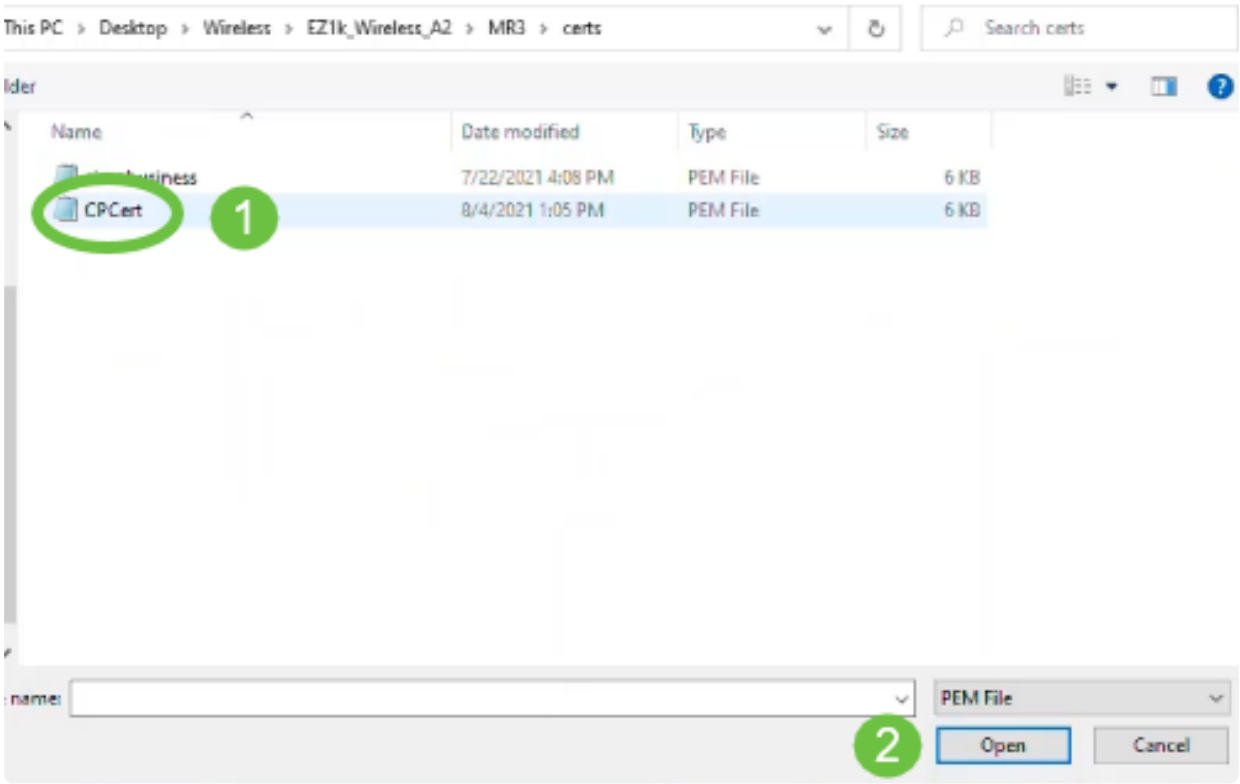


ⓘ Note:

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

Paso 7

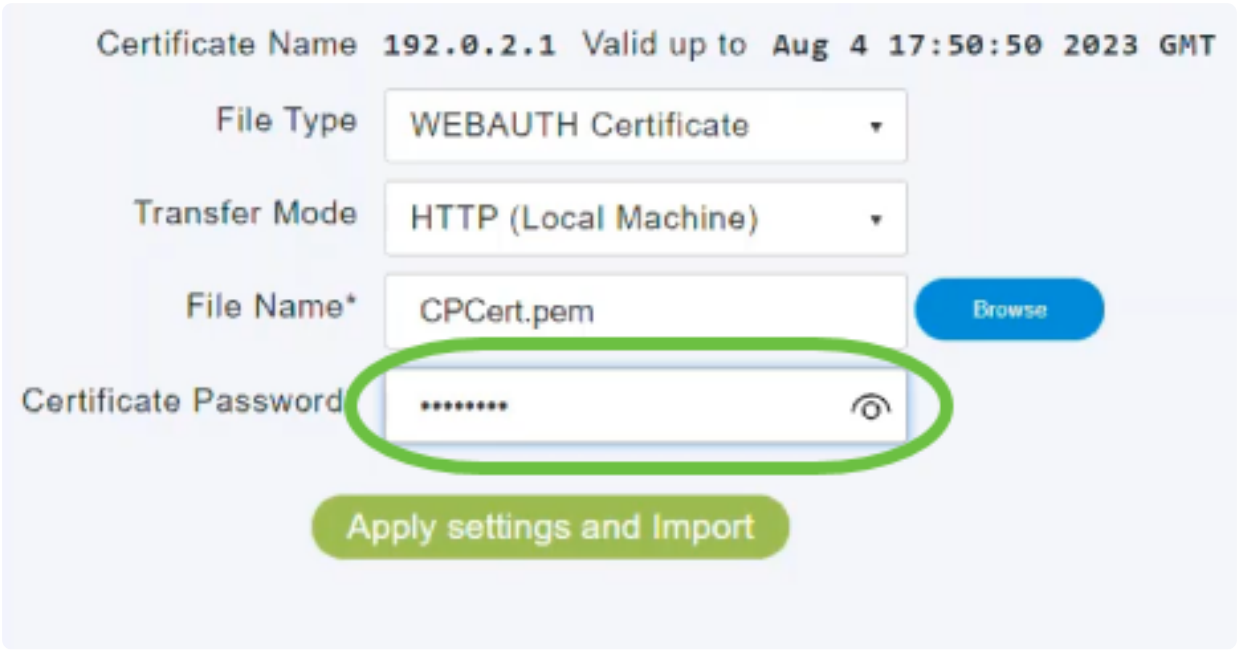
Cargue el archivo desde el equipo local; para ello, vaya a la carpeta que contiene el certificado personalizado. Seleccione el archivo de certificado y haga clic en Abrir.



> ⓘ Note:
>
> El certificado debe ser un archivo PEM. Para cargar correctamente certificados WEBADMIN, asegúrese de incluir la cadena de certificados completa, que es el certificado del dispositivo, el certificado de la CA emisora y el certificado de la CA raíz.

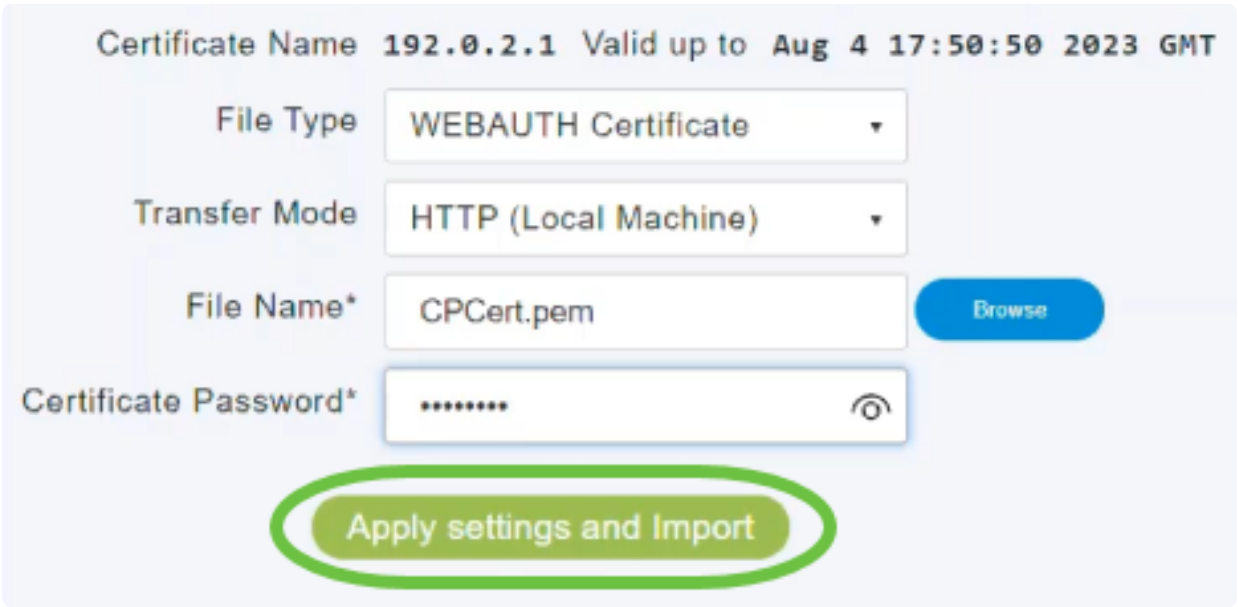
Paso 8

Ingrese la Contraseña del Certificado.



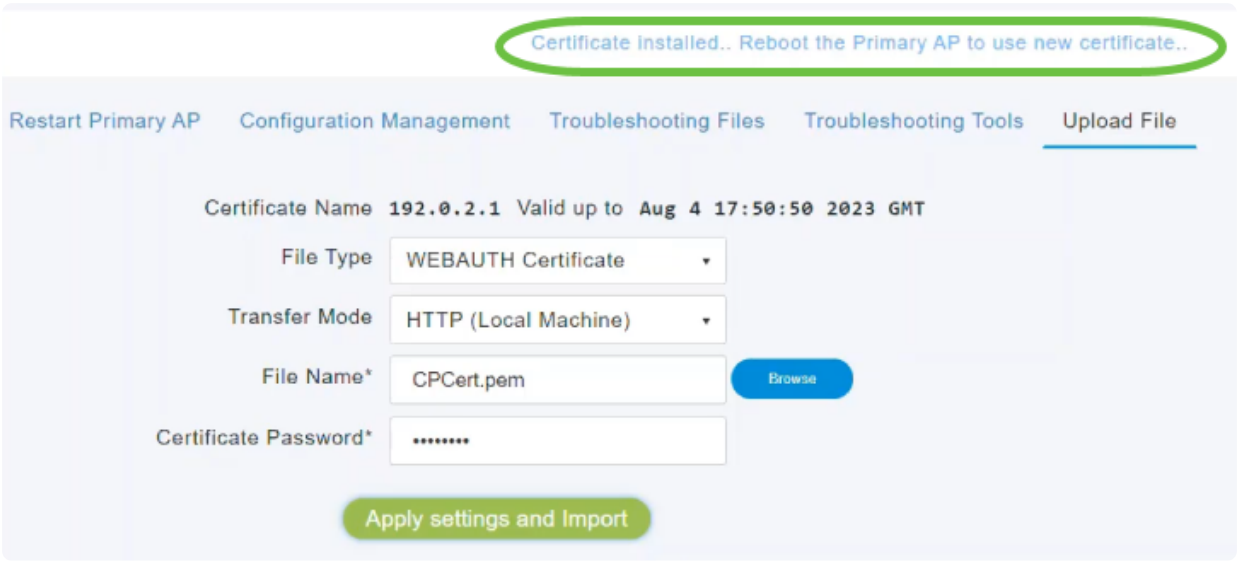
Paso 9

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.



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

Conclusión

¡Estás listo! Ahora ha cargado correctamente certificados personalizados en el AP CBW.

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).