# Configurar el redireccionamiento HTTPS mediante autenticación web

## Contenido



## Introducción

En este documento se describe la configuración para el redireccionamiento de autenticación web a través de HTTPS. Esta es una función incorporada en la versión 8.0 de la red inalámbrica unificada de Cisco (CUWN, Cisco Unified Wireless Network).

## Prerequisites

### Requirements

Cisco recomienda tener conocimientos de estos temas:

- Conocimiento básico de la autenticación web del controlador de LAN inalámbrica (WLC)
- Cómo configurar el WLC para la autenticación Web.

### Componentes Utilizados

La información en este documento se basa en el WLC de la serie 5500 de Cisco que ejecuta la versión 8.0 del firmware CUWN.

> **Nota:** La explicación de configuración y autenticación web proporcionada en este documento es aplicable a todos los modelos WLC y cualquier imagen CUWN igual o posterior a 8.0.100.0.

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. If your network is live, make sure that you understand the potential impact of any command.

# Antecedentes

La autenticación Web es una función de seguridad de capa 3. Bloquea todo el tráfico de datos/IP, excepto los paquetes relacionados con DHCP/los paquetes relacionados con DNS, de un cliente particular hasta que un cliente inalámbrico haya proporcionado un nombre de usuario y una contraseña válidos.La autenticación Web es utilizada normalmente por los clientes que desean implementar una red de acceso de invitado.La autenticación Web comienza cuando el controlador intercepta el primer paquete TCP HTTP (puerto 80) GET del cliente.

Para que el navegador web del cliente llegue hasta aquí, primero el cliente debe obtener una dirección IP y hacer una traducción de la dirección URL a la dirección IP (resolución DNS) para el navegador web. Esto permite que el navegador web sepa qué dirección IP enviar el HTTP GET. Cuando el cliente envía el primer HTTP GET al puerto TCP 80, el controlador redirige el cliente a https:<virtual IP>/login.html para su procesamiento. Este proceso finalmente abre la página web de inicio de sesión.

Antes de las versiones anteriores a CUWN 8.0 (es decir, hasta 7.6), si el cliente inalámbrico presenta una página HTTPS (TCP 443), la página no se redirige al portal de autenticación web. A medida que cada vez más sitios web comienzan a utilizar HTTPS, esta función se incluye en las versiones CUWN 8.0 y posteriores. Con esta función implementada, si un cliente inalámbrico intenta https://<website>, se redirige a la página de inicio de sesión de web-auth. Además, esta función es muy útil para los dispositivos que envían solicitudes https con una aplicación (pero no con un navegador).

## Error de certificado

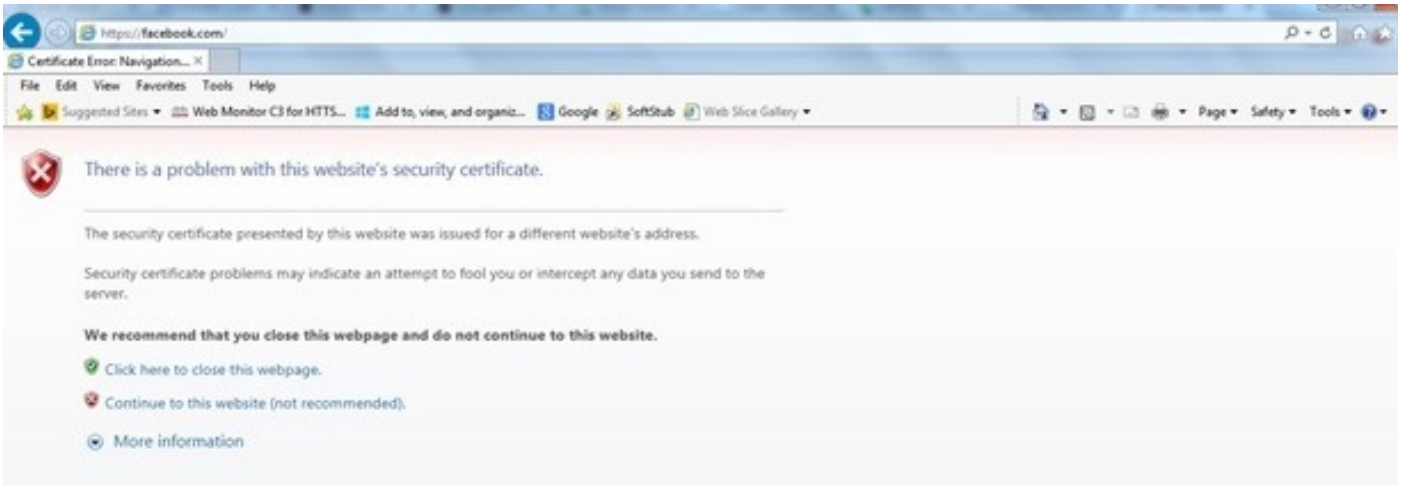
El mensaje de advertencia "el certificado no es emitido por una autoridad de certificación de confianza". aparece en el navegador después de configurar la función https-redirect. Esto se ve incluso si tiene un certificado raíz o encadenado válido en el controlador, como se muestra en la Figura 1 y la Figura 2. La razón es que el certificado que instaló en el controlador se emite a su dirección IP virtual.

> **Nota:** Si intenta una redirección HTTP y tiene este certificado en el WLC, no obtiene este error de advertencia de certificado.  Sin embargo, en el caso de redirección HTTPS, aparece este error.

Cuando el cliente intenta HTTPS://<web-site> , el navegador espera que el certificado emitido a la dirección IP del sitio resuelto por el DNS. Sin embargo, lo que reciben es el certificado que se emitió al servidor web interno del WLC (dirección IP virtual) que hace que el navegador emita la advertencia. Esto se debe exclusivamente a la forma en que funciona HTTPS y siempre sucede si intenta interceptar la sesión HTTPS para que la redirección de autenticación web funcione.

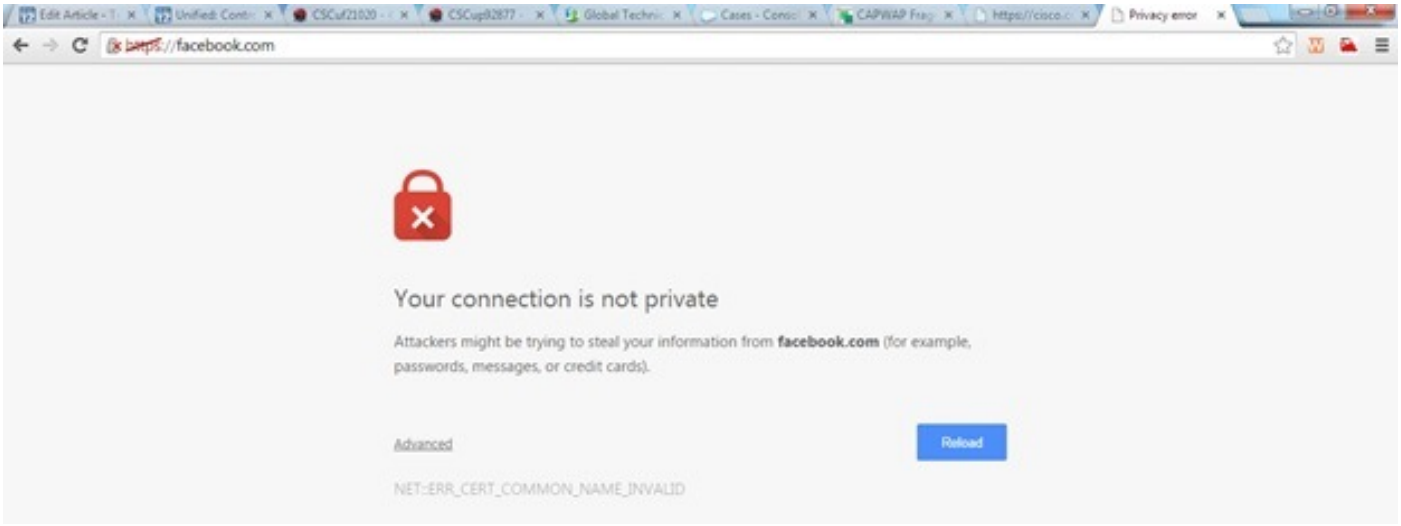
Es posible que vea mensajes de error de certificados diferentes en exploradores diferentes, pero todos están relacionados con el mismo problema que se ha descrito anteriormente.

Figure 1




Este es un ejemplo de cómo puede aparecer el error en Chrome:

Figure 2




# Configurar

## Configuración del WLC para redirección HTTPS

Esta configuración supone que la LAN inalámbrica (WLAN) ya está configurada para la seguridad de autenticación Web de capa 3. Para habilitar o inhabilitar la redirección HTTPS en esta WLAN de autenticación Web:

```
(WLC)>config wlan security web-auth enable 10
(WLC)>config network web-auth https-redirect enable
WARNING! - You have chosen to enable https-redirect.
This might impact performance significantly
```

Como muestra la configuración de ejemplo, esto podría afectar al rendimiento de un redireccionamiento HTTPS pero no a la redirección HTTP

Para obtener más información y una configuración de las WLANs de autenticación Web, vea

Autenticación Web en el Controlador WLAN.

# Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

La herramienta de interpretación de información de salida (disponible para clientes registrados únicamente) admite ciertos comandos show. Utilice la herramienta para ver una análisis de información de salida del comando show.

```
(WLC)>show network summary

Web Auth Secure Web ..................... Enable
Web Auth Secure Redirection ............. Enable
```

1. Habilitar estos debugs:
   ```
   (WLC) debug client
   ```

   ```
   (WLC)> debug web-auth redirect enable
   ```
2. Verifique las depuraciones:
   ```
   (WLC) >show debug

   MAC Addr 1.............................. 24:77:03:52:56:80

   Debug Flags Enabled:
   webauth redirect enabled.
   ```
3. Asocie el cliente al SSID habilitado para web-auth.
4. Busque estos debugs:
   ```
   *webauthRedirect: Jan 16 03:35:35.678: 24:77:3:52:56:80- received connection.
   client socket = 9
   *webauthRedirect: Jan 16 03:35:35.679: 24:77:3:52:56:80- trying to read on socket 95
   *webauthRedirect: Jan 16 03:35:35.679: 24:77:3:52:56:80- calling parser with bytes = 204
   *webauthRedirect: Jan 16 03:35:35.679: 24:77:3:52:56:80- bytes parsed = 204
   *webauthRedirect: Jan 16 03:35:35.679: captive-bypass detection enabled,
   checking for wispr in HTTP GET, client mac=24:77:3:52:56:80
   *webauthRedirect: Jan 16 03:35:35.679: 24:77:3:52:56:80- Preparing redirect
   URL according to configured Web-Auth type
   *webauthRedirect: Jan 16 03:35:35.679: 24:77:3:52:56:80- got the hostName
   for virtual IP(wirelessguest.test.com)
   *webauthRedirect: Jan 16 03:35:35.679: 24:77:3:52:56:80- Checking custom-web
   config for WLAN ID:10
   *webauthRedirect: Jan 16 03:35:35.679: 24:77:3:52:56:80- Global status is
   enabled, checking on web-auth type
   *webauthRedirect: Jan 16 03:35:35.679: 24:77:3:52:56:80- Web-auth type Customized,
   using URL:https://wirelessguest.test.com/fs/customwebauth/login.html
   ```

   **Nota:** Asegúrese de que Secure web (config network secure web enable/disable) o web-auth secure (config network web-auth secureweb enable/disable) estén habilitados para hacer que funcione la redirección HTTPS. Tenga en cuenta también que puede haber una ligera reducción en el rendimiento cuando se utiliza la redirección sobre HTTPS.

# Troubleshoot

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