Resolución de problemas de autenticación Web en un controlador de LAN inalámbrica (WLC)

Contenido

Introducción

Este documento describe sugerencias para resolver problemas de autenticación Web en un entorno de controlador de LAN inalámbrica (WLC).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Control y aprovisionamiento de puntos de acceso inalámbricos (CAPWAP).
- Cómo configurar el Lightweight Access Point (LAP) y el WLC para el funcionamiento básico.
- Conocimiento básico de la autenticación Web y cómo configurar la autenticación Web en WLCs.

Para obtener información sobre cómo configurar la autenticación Web en los WLC, consulte Ejemplo de Configuración de Autenticación Web del Controlador de LAN Inalámbrica.

Componentes Utilizados

La información de este documento se basa en un WLC 5500 que ejecuta la versión de firmware 8.3.121.

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.

Productos Relacionados

Este documento también se puede utilizar con este hardware:

- Controladores inalámbricos de Cisco serie 5500
- Controladores inalámbricos de Cisco serie 8500
- Controladores inalámbricos de Cisco serie 2500
- Cisco Airespace 3500 Series WLAN Controller
- Cisco Airespace 4000 Series Wireless LAN Controller
- Controladores inalámbricos Cisco Flex serie 7500
- Módulo 2 de servicios inalámbricos de Cisco (WiSM2)

Autenticación Web en WLCs

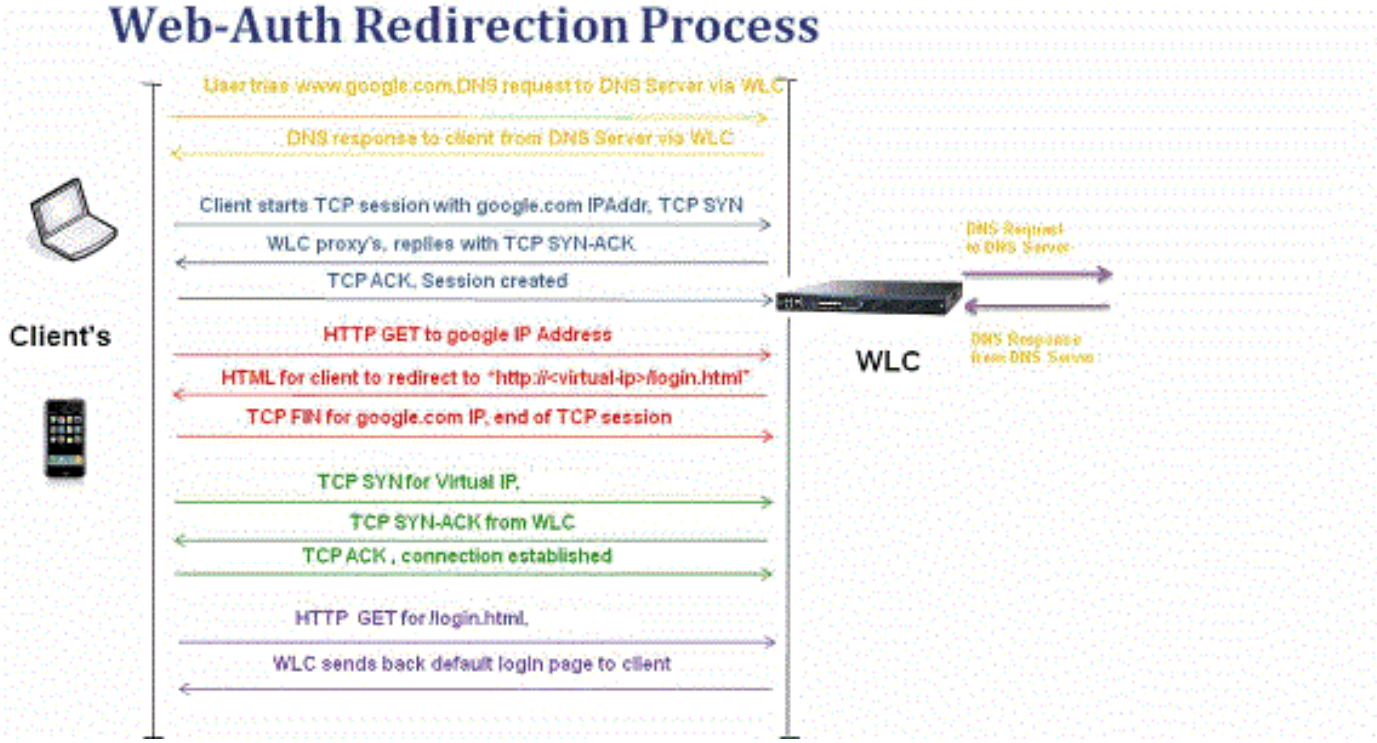
La autenticación web es una función de seguridad de Capa 3 que hace que el controlador no permita el tráfico IP, excepto los paquetes relacionados con DHCP/paquetes relacionados con el Sistema de nombres de dominio (DNS), de un cliente particular hasta que ese cliente haya proporcionado correctamente un nombre de usuario y una contraseña válidos con una excepción del tráfico permitido a través de una lista de control de acceso (ACL) previa a la autenticación. La autenticación Web es la única política de seguridad que permite al cliente obtener una dirección IP antes de la autenticación. Es un método de autenticación simple sin la necesidad de un solicitante o de una utilidad de cliente. La autenticación Web se puede hacer localmente en un WLC o sobre un servidor RADIUS. La autenticación Web es utilizada típicamente por los clientes que quieren implementar una red de acceso de invitados.

La autenticación Web se inicia cuando el controlador intercepta el primer paquete GET TCP HTTP (puerto 80) del cliente. Para que el explorador web del cliente llegue hasta aquí, el cliente debe obtener primero una dirección IP y realizar una traducción de la dirección URL a la dirección IP (resolución DNS) para el explorador web. Esto permite que el navegador web sepa qué dirección IP debe enviar el HTTP GET.

Cuando se configura la autenticación web en la WLAN, el controlador bloquea todo el tráfico (hasta que se completa el proceso de autenticación) del cliente, excepto el tráfico DHCP y DNS. Cuando el cliente envía el primer HTTP GET al puerto TCP 80, el controlador redirige al cliente a https://192.0.2.1/login.html (si ésta es la IP virtual configurada) para su procesamiento. Este proceso finalmente abre la página web de inicio de sesión.

> **Nota**: Cuando usted utiliza un servidor Web externo para la autenticación Web, las plataformas del WLC necesitan una ACL de la pre-autenticación para el servidor Web externo.

Esta sección explica el proceso de redirección de la autenticación Web en detalle.



- Abra el explorador web y escriba una dirección URL, por ejemplo, http://www.site.com. El cliente envía una solicitud DNS para que dicha URL obtenga la IP para el destino. El WLC pasa la solicitud DNS al servidor DNS y el servidor DNS responde con una respuesta DNS, que contiene la dirección IP del destino www.site.com que a su vez se reenvía a los clientes inalámbricos.
- El cliente entonces intenta abrir una conexión con el la dirección IP de destino. Envía un paquete TCP SYN destinado a la dirección IP de www.site.com.
- El WLC tiene reglas configuradas para el cliente y por lo tanto puede actuar como proxy para www.site.com. Devuelve un paquete TCP SYN-ACK al cliente con la fuente como la dirección IP de www.site.com. El cliente devuelve un paquete TCP ACK para completar el intercambio de señales TCP de tres vías y la conexión TCP está completamente establecida.
- El cliente envía un paquete HTTP GET destinado a www.site.com. El WLC intercepta este paquete y lo envía para el manejo de redireccionamiento. El aplicación HTTP gateway prepara a un cuerpo HTML y lo envía de vuelta como respuesta al HTTP GET solicitado por el cliente. Este HTML hace que el cliente vaya a la URL de la página Web predeterminada, por ejemplo, http:// /login.html.
- El cliente cierra la conexión TCP con la dirección IP; por ejemplo, www.site.com.
- Ahora el cliente quiere ir a http://<virtualip>/login.html y así intenta abrir una conexión TCP con la dirección IP virtual del WLC. Envía un paquete SYN TCP para 192.0.2.1 (que es nuestra IP virtual aquí) al WLC.
- El responde con un TCP SYN-ACK y el cliente devuelve un TCP ACK al WLC para completar la aceptación de contacto.
- El cliente envía un HTTP GET para /login.html destinado a 192.0.2.1 para solicitar la página de inicio de sesión.
- Esta solicitud se permite hasta el servidor web del WLC y el servidor responde con la página de inicio de sesión predeterminada. El cliente recibe la página de login en la ventana del navegador donde el usuario puede continuar el inicio de sesión.

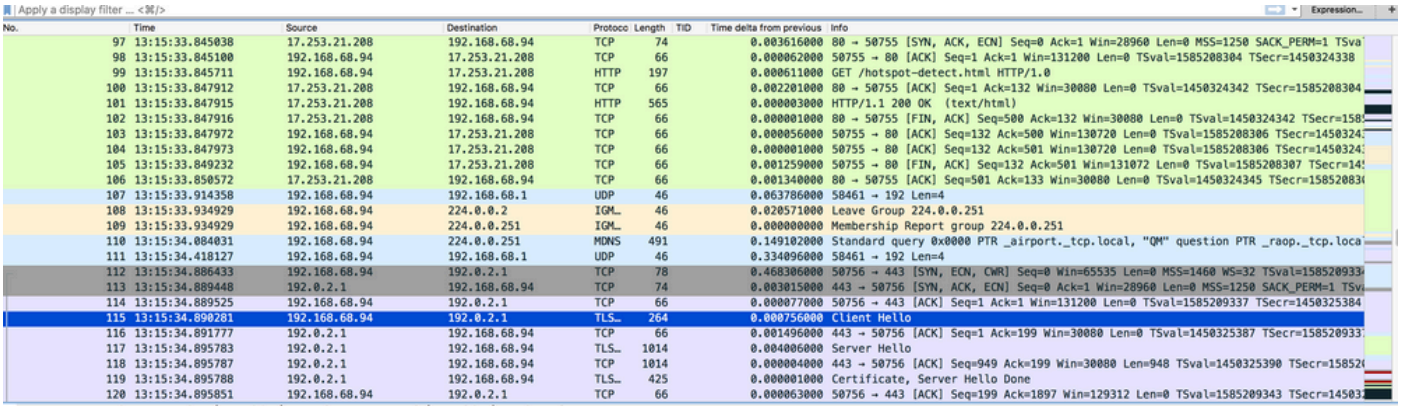
En este ejemplo, la dirección IP del cliente es 192.168.68.94. El cliente resolvió la URL al servidor web al que accedió, 10.1.0.13. Como puede ver, el cliente realizó el protocolo de enlace de tres

vías para iniciar la conexión TCP y luego envió un paquete HTTP GET que comenzó con el paquete 96 (00 es el paquete HTTP). El usuario no activó esta función, sino que fue el sistema operativo el que activó la detección automática del portal (como podemos adivinar en la URL solicitada). El controlador intercepta los paquetes y responde con el código 200. El paquete de código 200 tiene una URL de redirección:

```
<HTML><HEAD>
<TITLE> Web Authentication Redirect</TITLE>
<META http-equiv="Cache-control" content="no-cache">
<META http-equiv="Pragma" content="no-cache">
<META http-equiv="Expires" content="-1">
<META http-equiv="refresh" content="1;
URL=https://192.0.2.1/login.html?redirect=http://captive.apple.com/hotspot-detect.html">
</HEAD></HTML>
```

A continuación, cierra la conexión TCP mediante el protocolo de enlace de tres vías.

A continuación, el cliente inicia la conexión HTTPS con la URL de redirección que la envía a 192.0.2.1, que es la dirección IP virtual del controlador. El cliente tiene que validar el certificado del servidor o ignorarlo para activar el túnel SSL. En este caso, es un certificado autofirmado, por lo que el cliente lo ignoró. La página web de inicio de sesión se envía a través de este túnel SSL. El paquete 112 inicia las transacciones.



Tiene la opción de configurar el nombre de dominio para la dirección IP virtual del WLC. Si configura el nombre de dominio para la dirección IP virtual, este nombre de dominio se devuelve en el paquete HTTP OK del controlador en respuesta al paquete HTTP GET del cliente. A continuación, debe realizar una resolución DNS para este nombre de dominio. Una vez que obtiene una dirección IP de la resolución DNS, intenta abrir una sesión TCP con esa dirección IP, que es una dirección IP configurada en una interfaz virtual del controlador.

Finalmente, la página web pasa a través del túnel al cliente y el usuario devuelve el nombre de usuario/contraseña a través del túnel de capa de conexión segura (SSL).

La autenticación Web se realiza mediante uno de estos tres métodos:

- Utilice una página Web interna (valor predeterminado).
- Utilice una página de inicio de sesión personalizada.
- Utilice una página de inicio de sesión de un servidor Web externo.

Notas:
- El paquete de autenticación web personalizado tiene un límite de hasta 30 caracteres para los nombres de archivo. Asegúrese de que ningún nombre de archivo del paquete tiene más de 30 caracteres.

- A partir de la versión 7.0 del WLC en adelante, si la autenticación Web está habilitada en el WLAN y usted también tiene reglas de la ACL de la CPU, las reglas de la autenticación Web basadas en el cliente siempre tienen prioridad más alta mientras que el cliente esté no autenticado en el estado WebAuth_Reqd. Una vez que el cliente pasa al estado RUN, se aplican las reglas de CPU ACL.

- Por lo tanto, si las ACL de la CPU están habilitadas en el WLC, se requiere una regla de permiso para la IP de la interfaz virtual (en CUALQUIER dirección) en estas condiciones:
 - Cuando la ACL de la CPU no tiene una regla de permitir TODO para ambas direcciones.
 - Cuando existe una regla de permitir TODO, pero también existe una regla de DENEGACIÓN para el puerto 443 u 80 de mayor precedencia.

- La regla de permiso para la IP virtual debe ser para el protocolo TCP y el puerto 80 si secureweb está inhabilitado, o el puerto 443 si secureweb está habilitado. Esto es necesario para permitir el acceso del cliente a la dirección IP de la interfaz virtual después de la autenticación exitosa cuando las ACL de la CPU están en su lugar.

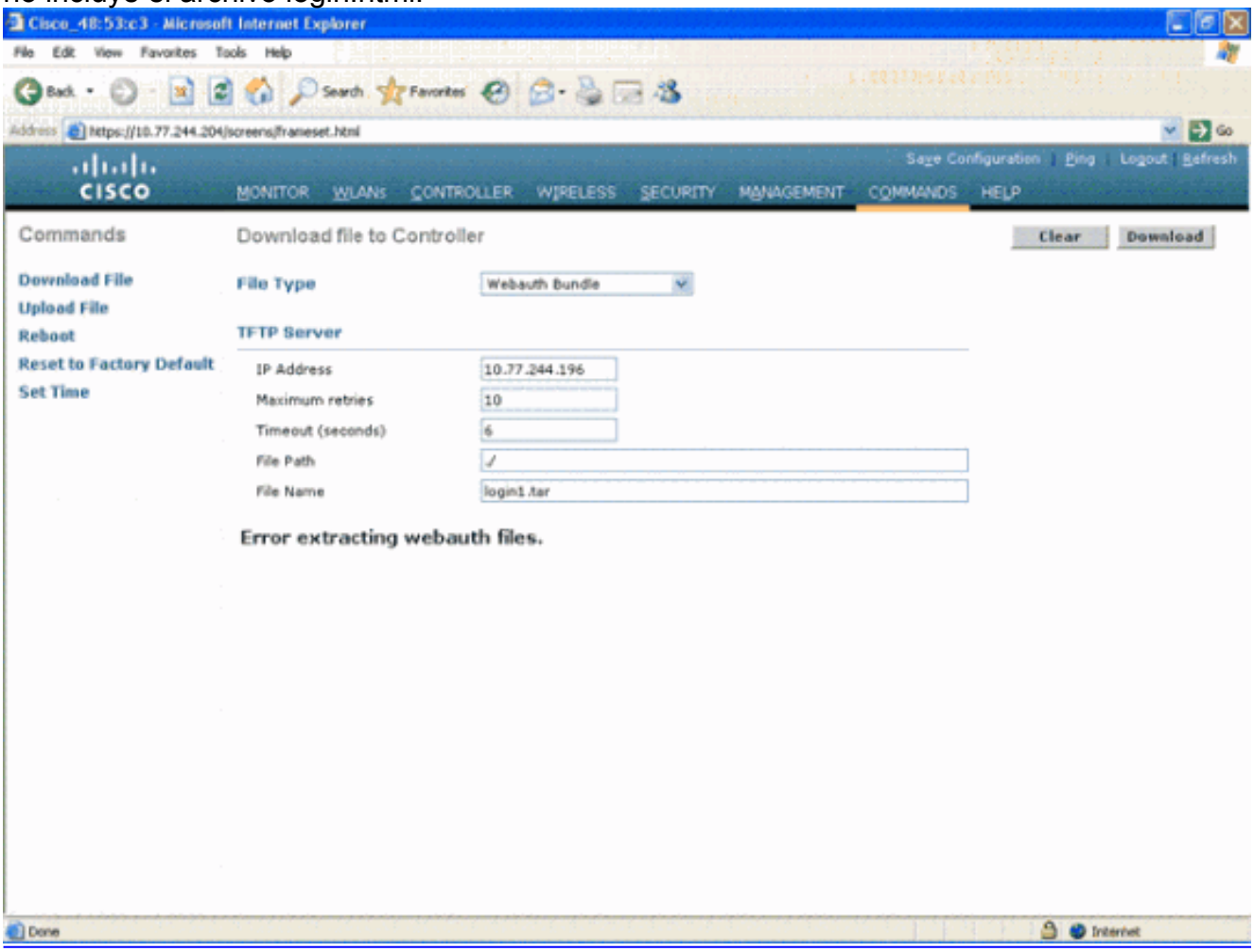
Troubleshooting de Autenticación Web

Después de configurar la autenticación web y si la función no funciona como se espera, complete estos pasos:

1. Verifique si el cliente obtiene una dirección IP. Si no es así, los usuarios pueden desmarcar la casilla de verificación **DHCP Required** en la WLAN y darle al cliente inalámbrico una dirección IP estática. Esto supone una asociación con el punto de acceso.
2. El siguiente paso del proceso es la resolución de DNS de la URL en el navegador web. Cuando un cliente WLAN se conecta a una WLAN configurada para la autenticación Web, el cliente obtiene una dirección IP del servidor DHCP. El usuario abre un navegador web e introduce una dirección de sitio web. A continuación, el cliente realiza la resolución DNS para obtener la dirección IP del sitio web. Ahora, cuando el cliente intenta alcanzar el Web site, el WLC intercepta la sesión HTTP GET del cliente y redirige al usuario a la página de login de la autenticación Web.
3. Por lo tanto, asegúrese de que el cliente pueda realizar la resolución DNS para que la redirección funcione. En Microsoft Windows, elija **Start > Run**, ingrese **CMD** para abrir una ventana de comando, y haga un "nslookup www.cisco.com" y vea si la dirección IP regresa. En Macs/Linux, abra una ventana de terminal y haga un "nslookup www.cisco.com" y vea si la dirección IP regresa.Si cree que el cliente no obtiene la resolución DNS, puede:Introduzca la dirección IP de la URL (por ejemplo, http://www.cisco.com es http://192.168.219.25).Intente escribir cualquier dirección IP (incluso no existente) que deba resolverse a través del adaptador inalámbrico.Al introducir esta URL, ¿aparece la página web? En caso afirmativo, lo más probable es que sea un problema de DNS. También puede ser un problema de certificado. El controlador, de forma predeterminada, utiliza un certificado autofirmado y la mayoría de los navegadores web advierten contra su uso.
4. Para la autenticación Web con una página Web personalizada, asegúrese de que el código HTML de la página Web personalizada es el apropiado. Puede descargar un script de autenticación web de ejemplo de Descargas de software de Cisco. Por ejemplo, para los controladores 5508, elija **Products > Wireless > Wireless LAN Controller > Standalone Controllers > Cisco 5500 Series Wireless LAN Controllers > Cisco 5508 Wireless LAN**

Controller > Software on Chassis > Wireless LAN Controller Web Authentication Bundle y descargue el archivo **webauth_bundle.zip**.Estos parámetros se agregan a la URL cuando el navegador de Internet del usuario se redirige a la página de inicio de sesión personalizada:ap_mac: Dirección MAC del punto de acceso al que está asociado el usuario inalámbrico.switch_url: URL del controlador al que se deben enviar las credenciales del usuario.redireccionar: URL a la que se redirige al usuario una vez que la autenticación se ha realizado correctamente.statusCode: código de estado devuelto desde el servidor de autenticación web del controlador.wlan: SSID de WLAN al que está asociado el usuario inalámbrico.Estos son los códigos de estado disponibles:Código de estado 1: "Ya ha iniciado sesión. No se requiere ninguna otra acción por su parte".Código de estado 2: "No está configurado para autenticarse en el portal web. No se requiere ninguna otra acción por su parte".Código de estado 3: "El nombre de usuario especificado no se puede utilizar en este momento. ¿Es posible que el nombre de usuario ya esté conectado al sistema?"Código de estado 4: "Se le ha excluido."Código de estado 5: "La combinación de nombre de usuario y contraseña que ha introducido no es válida. Inténtelo de nuevo."

5. Todos los archivos e imágenes que deben aparecer en la página web personalizada deben ser agrupados en un archivo .tar antes de que se cargue en el WLC. Asegúrese de que uno de los archivos incluidos en el paquete .tar sea login.html. Recibirá este mensaje de error si no incluye el archivo login.html:



Refiérase a la sección Pautas para la Autenticación Web Personalizada del Ejemplo de Configuración de Autenticación Web del Controlador de LAN Inalámbrica para obtener más información sobre cómo crear una ventana de autenticación Web personalizada.**Nota**: Los archivos que son grandes y los archivos que tienen nombres largos pueden dar lugar a un error de extracción. Se recomienda que las imágenes estén en formato .jpg.

6. Asegúrese de que la opción **Scripting** no esté bloqueada en el navegador del cliente, ya que la página web personalizada en el WLC es básicamente una secuencia de comandos HTML.
7. Si tiene un **nombre de host** configurado para la **interfaz virtual** del WLC, asegúrese de que la resolución DNS esté disponible para el nombre de host de la interfaz virtual. **Nota**: Navegue al menú **Controlador > Interfaces** desde la GUI del WLC para asignar un **nombre de host DNS** a la interfaz virtual.
8. Algunas veces el firewall instalado en el equipo cliente bloquea las páginas de Login de Autenticación Web. Inhabilite el firewall antes de acceder a la página Login. El firewall puede ser habilitado otra vez una vez que se termina la autenticación web.
9. El firewall de la solución/topología se puede colocar entre el cliente y el servidor de autenticación web, que depende de la red. En cuanto a cada diseño o solución de red implementada, el usuario final debe asegurarse de que estos puertos están permitidos en el firewall de red.

10. Para que ocurra la autenticación Web, el cliente primero debe asociarse a la WLAN apropiada en el WLC. Navegue al menú **Monitor > Clients** en la GUI del WLC para ver si el cliente está asociado al WLC. Compruebe si el cliente tiene una dirección IP válida.
11. Deshabilite la configuración de proxy en el navegador del cliente hasta que se complete la autenticación web.
12. El método de autenticación web predeterminado es el protocolo de autenticación de contraseña (PAP). Asegúrese de que la autenticación PAP esté permitida en el servidor RADIUS para que esto funcione. Para verificar el estado de la autenticación del cliente, verifique las depuraciones y los mensajes de registro del servidor RADIUS. Puede utilizar el comando **debug aaa all** en el WLC para ver las depuraciones del servidor RADIUS.
13. Actualice el controlador de hardware del equipo con el código más reciente del sitio web del fabricante.
14. Verifique la configuración en el solicitante (programa en portátil).
15. Cuando utiliza el suplicante de configuración rápida de Windows integrado en Windows: Compruebe que el usuario tiene instalados los parches más recientes.Ejecute los debugs en el suplicante.
16. En el cliente, active los registros EAPOL (WPA+WPA2) y RASTLS desde una ventana de comandos. Elija **Start > Run > CMD**:
    ```
    netsh ras set tracing eapol enable
          netsh ras set tracing rastls enable
    ```
    Para inhabilitar los registros, ejecute el mismo comando pero reemplace enable por disable. Para XP, todos los registros se pueden encontrar en C:\Windows\tracing.
17. Si aún no tiene ninguna página web de inicio de sesión, recopile y analice esta salida desde un único cliente:
    ```
    debug client <mac_address in format xx:xx:xx:xx:xx:xx>
    debug dhcp message enable
    debug aaa all enable
    debug dot1x aaa enable
    debug mobility handoff enable
    ```
18. Si el problema no se resuelve después de completar estos pasos, recopile estas depuraciones y utilice el Administrador de casos de soporte para abrir una solicitud de servicio.
    ```
    debug pm ssh-appgw enable
    debug pm ssh-tcp enable
    debug pm rules enable
    debug emweb server enable
    debug pm ssh-engine enable packet <client ip>
    ```

Información Relacionada

- Ejemplo de Configuración de la Autenticación Web del Controlador LAN Inalámbrico
- Ejemplo de configuración de autenticación web externa con controladores de LAN inalámbrica
- 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).