Acceso protegido de Wi-Fi (WPA) en un ejemplo de la configuración de red del Cisco Unified Wireless

Contenido

Introducción

Este documento describe cómo configurar el Acceso protegido de Wi-Fi (WPA) en una red del Cisco Unified Wireless.

prerrequisitos

Requisitos

Asegúrese de que usted tenga conocimiento básico de estos temas antes de que usted intente esta configuración:

- WPA
- Soluciones acerca de la seguridad del Wireless LAN (red inalámbrica (WLAN))**Nota:** Refiera a la descripción de la Seguridad de LAN de la tecnología inalámbrica de Cisco para la información sobre las soluciones de la Seguridad de WLAN de Cisco.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco 1000 Series Lightweight Access Point (REVESTIMIENTO)
- Regulador del Wireless LAN de Cisco 4404 (WLC) ese firmware 4.2.61.0 de los funcionamientos
- Adaptador del cliente de Cisco 802.11a/b/g que funciona con el firmware 4.1
- Utilidad Aironet Desktop (ADU) ese firmware 4.1 de los funcionamientos
- Versión del servidor 4.1 del Cisco Secure ACS

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 la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Soporte WPA y WPA2

La red del Cisco Unified Wireless incluye el soporte para las certificaciones WPA y WPA2 del Wi-Fi Alliance. El WPA fue introducido por el Wi-Fi Alliance en 2003. El WPA2 fue introducido por el Wi-Fi Alliance en 2004. Todo el con certificación Wi-Fi de los Productos para el WPA2 se requiere ser interoperable con los Productos que son con certificación Wi-Fi para el WPA.

El WPA y el WPA2 ofrecen un nivel elevado de garantía para los usuarios finales y los administradores de la red que sus datos seguirán siendo soldado y que el acceso a sus redes será restringido a los usuarios autorizados. Ambos tienen modos de operación personales y de la empresa que cubran las necesidades distintas de los dos segmentos de mercado. El modo de empresa de cada uno utiliza el IEEE 802.1X y el EAP para la autenticación. El modo personal de cada uno utiliza la clave previamente compartida (PSK) para la autenticación. Cisco no recomienda al modo personal para las implementaciones del negocio o del gobierno porque utiliza un PSK para la autenticación de usuario. El PSK no es seguro para los entornos para empresas.

El WPA dirige todas las vulnerabilidades sabidas WEP en la instrumentación de seguridad original del IEEE 802.11 que trae una solución acerca de la seguridad inmediata a los WLAN en la empresa y los entornos del small office/home office (SOHO). El WPA utiliza el TKIP para el cifrado.

El WPA2 es la última generación de Seguridad del Wi-Fi. Es la implementación interoperable de Alliance del Wi-Fi del estándar ratificado de IEEE 802.11i. Implementa el algoritmo de encripción AES recomendado del National Institute of Standards and Technology (NIST) usando el modo contrario con el protocolo del Message Authentication Code del Cipher Block Chaining (CCMP). El WPA2 facilita la conformidad del gobierno FIP 140-2.

Comparación de los tipos de modo WPA y WPA2

	WPA	WPA2

Modo de empresa (negocio, gobierno, educación)	• Autenticación: IEEE 802.1X/EAP • Cifrado: TKIP/MIC	• Autenticación: IEEE 802.1X/EAP • Cifrado: AES-CCMP
Modo personal (SOHO, hogar/personal)	• Autenticación: PSK • Cifrado: TKIP/MIC	• Autenticación: PSK • Cifrado: AES-CCMP

En el modo de operación WPA y WPA2 uso 802.1X/EAP de la empresa para la autenticación. el 802.1x proporciona los WLAN con fuerte, la autenticación recíproca entre un cliente y un servidor de autenticación. Además, el 802.1x proporciona dinámico por usuario, las claves de encripción del por session, quitando la carga administrativa y los problemas de seguridad que rodean las claves de encripción estáticas.

Con el 802.1x, las credenciales usadas para la autenticación, tal como contraseñas del inicio, nunca se transmiten en el claro, o sin el cifrado, sobre el media inalámbrico. Mientras que los tipos de autenticación del 802.1x proporcionan la autenticación robusta para la Tecnología inalámbrica LAN, el TKIP o el AES es necesario para el cifrado además del 802.1x desde la encripción WEP estándar del 802.11, es vulnerable a los ataques a la red.

Varios tipos de autenticación del 802.1x existen, cada uno que proporciona a un diverso acercamiento a la autenticación mientras que confían en el mismo marco y EAP para la comunicación entre un cliente y un Punto de acceso. Los Productos del Cisco Aironet apoyan más tipos de la autenticación EAP del 802.1x que cualquier otro producto de WLAN. Los tipos admitidos incluyen:

- Cisco LEAP
- Autenticación adaptable de EAP vía el Tunelización seguro (EAP-FAST)
- Seguridad de la capa del EAP-transporte (EAP-TLS)
- Protocolo extensible authentication protegido (PEAP)
- TLS EAP-tunneled (EAP-TTLS)
- Módulo de identidad del suscriptor EAP (EAP-SIM)

Otra ventaja de la autenticación del 802.1x es administración centralizada para los grupos de usuario WLAN, incluyendo la rotación de la clave del policy basado, la asignación de clave dinámica, la asignación del VLAN dinámico, y la restricción SSID. Estas características giran las claves de encripción.

En el modo de operación personal, una clave previamente compartida (contraseña) se utiliza para la autenticación. El modo personal requiere solamente un Punto de acceso y un dispositivo del cliente, mientras que el modo de empresa requiere típicamente el RADIUS o al otro servidor de autenticación en la red.

Este documento proporciona los ejemplos para configurar WPA2 (modo de empresa) y WPA2-PSK (modo personal) en una red del Cisco Unified Wireless.

Configuración de la red

En esta configuración, un WLC de Cisco 4404 y un REVESTIMIENTO de las Cisco 1000 Series están conectados con un Layer 2 Switch. Un servidor RADIUS externo (Cisco Secure ACS) también está conectado con el mismo Switch. Todos los dispositivos están en la misma subred. El Punto de acceso (REVESTIMIENTO) se registra inicialmente al regulador. Dos LAN inalámbricos, uno para el modo de empresa WPA2 y el otro para el modo personal WPA2, necesitan ser creados.

red inalámbrica (WLAN) del modo WPA2-Enterprise (SSID: WPA2-Enterprise) utilizará el EAP-FAST para autenticar los clientes de red inalámbrica y el AES para el cifrado. El servidor del Cisco Secure ACS será utilizado como el servidor RADIUS externo para autenticar a los clientes de red inalámbrica.

red inalámbrica (WLAN) del modo WPA2-Personal (SSID: WPA2-PSK) utilizará WPA2-PSK para la autenticación con la clave previamente compartida “abcdefghijk”.

Usted necesita configurar los dispositivos para esta configuración:

Configure los dispositivos para el modo de empresa WPA2

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Realice estos pasos para configurar los dispositivos para el modo de operación de la empresa WPA2:

1. Configure el WLC para la autenticación de RADIUS a través de un servidor RADIUS externo
2. Configure la red inalámbrica (WLAN) para la autenticación del modo de empresa WPA2 (el EAP-FAST)
3. Configure al cliente de red inalámbrica para el modo de empresa WPA2

Configure el WLC para la autenticación de RADIUS a través de un servidor RADIUS externo

El WLC necesita ser configurado para remitir los credenciales de usuario a un servidor RADIUS externo. El servidor RADIUS externo después valida los credenciales de usuario usando el EAP-FAST y proporciona el acceso a los clientes de red inalámbrica.

Complete estos pasos para configurar el WLC para un servidor RADIUS externo:

1. Elija la **Seguridad** y la **autenticación de RADIUS del** regulador GUI para visualizar la página de los servidores de autenticación de RADIUS. Entonces, haga clic **nuevo** para definir a un servidor de RADIUS.
2. Defina los parámetros del servidor de RADIUS en los **servidores de autenticación de RADIUS > nueva** página. Estos parámetros incluyen:Dirección IP del servidor de RADIUSsecreto compartidonúmero de puertoEstado del servidorEste documento utiliza al servidor ACS con una dirección IP de 10.77.244.196.
3. Haga clic en Apply (Aplicar).

Configure la red inalámbrica (WLAN) para el modo de operación de la empresa WPA2

Después, configure la red inalámbrica (WLAN) que los clientes utilizarán para conectar con la red inalámbrica. La red inalámbrica (WLAN) SSID para el modo de empresa WPA2 será WPA2-Enterprise. Este ejemplo asigna esta red inalámbrica (WLAN) a la interfaz de administración.

Complete estos pasos para configurar la red inalámbrica (WLAN) y sus parámetros relacionados:

1. Haga clic los **WLAN del** GUI del regulador para visualizar la página WLAN.Esta página enumera los WLAN que existen en el regulador.
2. Tecleo **nuevo** para crear una nueva red inalámbrica (WLAN).
3. Ingrese el nombre WLAN SSID, y el nombre del perfil en los **WLAN > nueva** página. Entonces, el tecleo **se aplica**.Este ejemplo utiliza **WPA2-Enterprise** como el SSID.
4. Una vez que usted crea una nueva red inalámbrica (WLAN), la **red inalámbrica (WLAN) > edita la** página para la nueva red inalámbrica (WLAN) aparece. En esta página, usted puede definir los diversos parámetros específicos a esta red inalámbrica (WLAN). Esto incluye las políticas generales, las políticas de seguridad, las directivas QOS y los parámetros avanzados.
5. Bajo políticas generales, marque el cuadro de **revisión de estado** para habilitar la red inalámbrica (WLAN).
6. Si usted quisiera que el AP transmitiera el SSID en sus tramas de recuperación de problemas, marque la **casilla de verificación SSID del broadcast**.
7. Haga clic en la ficha Security (Seguridad). Bajo Seguridad de la capa 2, elija **WPA+WPA2**.Esto habilita la autenticación WPA para la red inalámbrica (WLAN).
8. Navegue hacia abajo la página para modificar los **parámetros WPA+WPA2**.En este ejemplo, se seleccionan la directiva WPA2 y la encripción AES.
9. Bajo el mgmt de la clave del auth, elija el **802.1x**.Esto habilita el WPA2 usando la autenticación 802.1x/EAP y la encripción AES para la red inalámbrica (WLAN).
10. Haga clic la lengueta de los **servidores de AAA**. Bajo los servidores de autenticación, elija el dirección IP del servidor apropiado.En este ejemplo, 10.77.244.196 se utiliza como el servidor de RADIUS.
11. Haga clic en Apply (Aplicar).**Nota:** Ésta es la única configuración EAP que necesita ser configurada en el regulador para la autenticación EAP. El resto de las configuraciones específicas al EAP-FAST necesitan ser hechas en el servidor de RADIUS y los clientes que necesitan ser autenticadas.

Configure al servidor de RADIUS para la autenticación del modo de empresa WPA2 (el EAP-FAST)

En este ejemplo, el Cisco Secure ACS se utiliza como el servidor RADIUS externo. Realice estos pasos para configurar al servidor de RADIUS para la autenticación del EAP-FAST:

1. Cree una base de datos de usuarios para autenticar a los clientes
2. Agregue el WLC como cliente AAA al servidor de RADIUS
3. Configure la autenticación del EAP-FAST en el servidor de RADIUS con el aprovisionamiento anónimo de la En-banda PAC**Nota:** El EAP-FAST se puede configurar con el aprovisionamiento anónimo de la En-banda PAC o el aprovisionamiento autenticado

de la En-banda PAC. Este ejemplo utiliza el aprovisionamiento anónimo de la En-banda PAC. Para la información detallada y los ejemplos en configurar el EAP RÁPIDAMENTE con el aprovisionamiento anónimo de la En-banda PAC y el aprovisionamiento autenticado de la En-banda, refiera a la autenticación del EAP-FAST con el ejemplo de configuración de los reguladores y del servidor RADIUS externo del Wireless LAN.

Cree una base de datos de usuarios para autenticar a los clientes del EAP-FAST

Complete estos pasos para crear una base de datos de usuarios para los clientes del EAP-FAST en el ACS. Este ejemplo configura el nombre de usuario y contraseña del cliente del EAP-FAST como el user1 y user1, respectivamente.

1. Del ACS GUI en la barra de navegación, seleccione la **configuración de usuario**. Cree una Tecnología inalámbrica del usuario nuevo, y después haga clic **agregan/editan** para ir a la página del editar de este usuario.
2. De la configuración de usuario edite la página, Nombre real de la configuración y descripción así como las configuraciones de la contraseña tal y como se muestra en de este ejemplo.Este documento utiliza la **base de datos interna ACS** para la autenticación de contraseña.
3. Elija la **base de datos interna ACS de la** casilla desplegable de la autenticación de contraseña.
4. Configure el resto de parámetros obligatorios y el tecleo **somete**.

Agregue el WLC como cliente AAA al servidor de RADIUS

Complete estos pasos para definir el regulador como cliente AAA en el servidor ACS:

1. Haga clic la **configuración de red del** ACS GUI. Bajo sección del cliente AAA del agregar de la página de la configuración de red, el tecleo **agrega la entrada** para agregar el WLC como el cliente AAA al servidor de RADIUS.
2. De la página del cliente AAA, defina el nombre del WLC, de la dirección IP, del secreto compartido y del método de autentificación (Airespace RADIUS/Cisco). Refiera a la documentación del fabricante para otros servidores de autenticación NON-ACS.**Nota:** La clave secreta compartida que usted configura en el WLC y el servidor ACS debe hacer juego. El secreto compartido es con diferenciación entre mayúsculas y minúsculas.
3. Tecleo **Submit+Apply**.

Configure la autenticación del EAP-FAST en el servidor de RADIUS con el aprovisionamiento anónimo de la En-banda PAC

Aprovisionamiento anónimo de la En-banda

Éste es uno de los dos métodos del aprovisionamiento de la en-banda en los cuales el ACS establece una conexión asegurada con el cliente del usuario final con el fin de proveer del cliente un nuevo PAC. Esta opción permite una entrada en contacto TLS anónima entre el cliente del usuario final y el ACS.

Este método actúa el interior un túnel autenticado del protocolo del acuerdo de Diffie-HellmanKey (ADHP) antes de que el par autentique al servidor ACS.

Entonces, el ACS requiere la autenticación EAP-MS-CHAPv2 del usuario. En la autenticación de usuario acertada, el ACS establece un túnel de Diffie Hellman con el cliente del usuario final. El ACS genera un PAC para el usuario y lo envía al cliente del usuario final en este túnel, junto con la información sobre este ACS. Este método de aprovisionamiento utiliza el EAP MSCHAPv2 como el método de autentificación en la fase cero y EAP-GTC en la fase dos.

Porque un servidor del unauthenticated es aprovisionado, no es posible utilizar una contraseña del sólo texto. Por lo tanto, solamente las credenciales MS-CHAP se pueden utilizar dentro del túnel. MS-CHAPv2 se utiliza para probar la identidad del par y para recibir un PAC para sesiones más futuras de la autenticación (EAP-MS-CHAP será utilizado como método interno solamente).

Complete estos pasos para configurar la autenticación del EAP-FAST en el servidor de RADIUS para el aprovisionamiento anónimo de la en-banda:

1. Haga clic la **configuración del sistema del** servidor de RADIUS GUI. De la página de la configuración del sistema, elija la **configuración de la autenticación global**.
2. De la página de configuración de la autenticación global, haga clic la **configuración del EAP-FAST** para ir a la página de las configuraciones del EAP-FAST.
3. De la página Configuración del EAP-FAST, marque la casilla de verificación del **EAP-FAST de la permit** para habilitar el EAP-FAST en el servidor de RADIUS.
4. Configure el Active/los valores jubilados de TTL de la clave principal (Tiempo para vivir) según lo deseado, o fíjelos al valor predeterminado tal y como se muestra en de este ejemplo.Refiera a las claves principales para la información sobre el Active y las claves principales jubiladas. También, refiera a las claves principales y a PAC TTL para más información.El campo de información ID de la autoridad representa la identidad textual de este servidor ACS, que un usuario final puede utilizar para determinar contra quien servidor ACS que se autenticará. El completar este campo es obligatorio.El campo del mensaje de la visualización de la inicial del cliente especifica un mensaje que se enviará a los usuarios que autentican con un cliente del EAP-FAST. El Largo máximo es 40 caracteres. Un usuario verá el mensaje inicial solamente si los soportes de cliente del usuario final la visualización.
5. Si usted quisiera que el ACS realizara el aprovisionamiento anónimo de la en-banda PAC, marque la casilla de verificación **anónima del aprovisionamiento de la en-banda PAC de la permit**.
6. **Métodos internos permitidos** — Esta opción determina que los métodos EAP internos pueden ejecutar dentro del túnel del EAP-FAST TLS. Para el aprovisionamiento anónimo de la en-banda, usted debe habilitar el EAP-GTC y EAP-MS-CHAP para la compatibilidad descendente. Si usted selecciona permita el aprovisionamiento anónimo de la en-banda PAC, usted debe seleccionar EAP-MS-CHAP (fase cero) y EAP-GTC (fase dos).

Configure al cliente de red inalámbrica para el modo de operación de la empresa WPA2

El siguiente paso es configurar al cliente de red inalámbrica para el modo de operación de la empresa WPA2.

Complete estos pasos para configurar al cliente de red inalámbrica para el modo de empresa WPA2.

1. Utilidad Aironet Desktop de la ventana, haga clic la **Administración del perfil > nuevo** para

crear un perfil para el usuario WLAN WPA2-Enterprise.Según lo mencionado anterior, este documento utiliza el nombre del WLAN/SSID como **WPA2-Enterprise** para el cliente de red inalámbrica.
2. De la ventana de administración del perfil, haga clic la **ficha general** y configure el nombre del perfil, el Nombre del cliente y el nombre SSID tal y como se muestra en de este ejemplo. Entonces, **AUTORIZACIÓN del** tecleo
3. Haga clic la **ficha de seguridad** y elija **WPA/WPA2/CCKM** habilitar el modo de operación WPA2. Conforme WPA/WPA2/CCKM al tipo EAP, elija el **EAP-FAST**. Haga clic la **configuración** para configurar la configuración del EAP-FAST.
4. De la ventana del EAP-FAST de la configuración, marque la casilla de verificación **automática del aprovisionamiento de la permit PAC**. Si usted quiere configurar el aprovisionamiento anónimo PAC, EAP-MS-CHAP será utilizado como el único método interno en la fase cero.
5. Elija el Nombre de usuario y la contraseña del MSCHAPv2 como el método de autentificación de la casilla desplegable del método de autentificación del EAP-FAST. Haga clic en Configure (Configurar).
6. Del Nombre de usuario y de la ventana de contraseña del MSCHAPv2 de la configuración, elija las configuraciones apropiadas del nombre de usuario y contraseña.Este ejemplo elige **automáticamente el prompt para el Nombre de usuario y la contraseña**.El mismo nombre de usuario y la contraseña se deben registrar en el ACS. Según lo mencionado anterior, este ejemplo utiliza el user1 y el user1 respectivamente como el nombre de usuario y contraseña. También, observe que esto es un aprovisionamiento anónimo de la en-banda. Por lo tanto, el cliente no puede validar el certificado de servidor. Usted necesita aseegurarse que la casilla de verificación de la identidad del servidor del validar esté desmarcada.
7. Haga clic en OK.

Verifique el modo de operación de la empresa WPA2

Complete estos pasos para verificar si su configuración del modo de empresa WPA2 trabaja correctamente:

1. Utilidad Aironet Desktop de la ventana, seleccione el perfil **WPA2-Enterprise** y el tecleo **activan** para activar el perfil del cliente de red inalámbrica.
2. Si usted ha habilitado MS-CHAP ver2 como su autenticación, después el cliente indicará para el nombre de usuario y contraseña.
3. Durante el proceso del EAP-FAST del usuario, al cliente a le indicará que pida el PAC del servidor de RADIUS. Cuando usted hace clic **sí**, el aprovisionamiento PAC comienza.
4. Después del aprovisionamiento acertado PAC en la fase cero, el fase uno y dos siguen y un procedimiento de la autenticación satisfactoria ocurre.Sobre la autenticación satisfactoria el cliente de red inalámbrica consigue asociado a la red inalámbrica (WLAN) WPA2-Enterprise. Aquí está el tiro de pantalla:Usted puede también verificar si el servidor de RADIUS reciba y valide el pedido de autenticación del cliente de red inalámbrica. Marque los informes pasajeros de las autenticaciones y de los intentos fallidos sobre el servidor ACS para lograr esto. Estos informes están disponibles bajo los informes y actividades en el servidor ACS.

Configure los dispositivos para el modo personal WPA2

Realice estos pasos para configurar los dispositivos para el modo de operación WPA2-Personal:

1. Configure la red inalámbrica (WLAN) para la autenticación del modo personal WPA2
2. Configure al cliente de red inalámbrica para el modo personal WPA2

Configure la red inalámbrica (WLAN) para el modo de operación personal WPA2

Usted necesita configurar la red inalámbrica (WLAN) que los clientes utilizarán para conectar con la red inalámbrica. La red inalámbrica (WLAN) SSID para el modo personal WPA2 será WPA2-Personal. Este ejemplo asigna esta red inalámbrica (WLAN) a la interfaz de administración.

Complete estos pasos para configurar la red inalámbrica (WLAN) y sus parámetros relacionados:

1. Haga clic los **WLAN del** GUI del regulador para visualizar la página WLAN.Esta página enumera los WLAN que existen en el regulador.
2. Tecleo **nuevo** para crear una nueva red inalámbrica (WLAN).
3. Ingrese el nombre, el nombre del perfil y el ID DE WLAN WLAN SSID en los WLAN > nueva página. Entonces, el tecleo **se aplica**.Este ejemplo utiliza **WPA2-Personal** como el SSID.
4. Una vez que usted crea una nueva red inalámbrica (WLAN), la **red inalámbrica (WLAN) > edita la** página para la nueva red inalámbrica (WLAN) aparece. En esta página, usted puede definir los diversos parámetros específicos a esta red inalámbrica (WLAN). Esto incluye las políticas generales, las políticas de seguridad, las directivas QOS y los parámetros avanzados.
5. Bajo políticas generales, marque el cuadro de **revisión de estado** para habilitar la red inalámbrica (WLAN).
6. Si usted quisiera que el AP transmitiera el SSID en sus tramas de recuperación de problemas, marque la **casilla de verificación SSID del broadcast**.
7. Haga clic en la ficha Security (Seguridad). Bajo Seguridad de la capa, elija **WPA+WPA2**.Esto habilita la autenticación WPA para la red inalámbrica (WLAN).
8. Navegue hacia abajo la página para modificar los **parámetros WPA+WPA2**.En este ejemplo, se seleccionan la directiva WPA2 y la encripción AES.
9. Bajo el mgmt de la clave del auth, elija el **PSK** para habilitar WPA2-PSK.
10. Ingrese la clave previamente compartida en el campo adecuado como se muestra.**Nota:** La clave previamente compartida usada en el WLC debe hacer juego con el que está configurado en los clientes de red inalámbrica.
11. Haga clic en Apply (Aplicar).

Configure al cliente de red inalámbrica para el modo personal WPA2

El siguiente paso es configurar al cliente de red inalámbrica para el modo de operación WPA2-Personal.

Complete estos pasos para configurar al cliente de red inalámbrica para el modo WPA2-Personal:

1. Utilidad Aironet Desktop de la ventana, haga clic la **Administración del perfil > nuevo** para crear un perfil para el usuario WLAN del WPA2-PSK.
2. De la ventana de administración del perfil, haga clic la **ficha general** y configure el nombre del perfil, el Nombre del cliente y el nombre SSID tal y como se muestra en de este ejemplo.

Entonces, **AUTORIZACIÓN del** tecleo.

3. Haga clic la **ficha de seguridad** y elija **WPA/WPA2 el passphrase** para habilitar WPA2-PSK el modo de operación. Haga clic la **configuración** para configurar la clave previamente compartida WPA-PSK.
4. Ingrese la clave del preshared y haga clic la **AUTORIZACIÓN**.

Verifique el modo de operación WPA2-Personal

Complete estos pasos para verificar si su configuración de modo WPA2-Enterprise trabaja correctamente:

1. Utilidad Aironet Desktop de la ventana, seleccione el perfil **WPA2-Personal** y el tecleo **activan** para activar el perfil del cliente de red inalámbrica.
2. Una vez que se activa el perfil, el cliente de red inalámbrica se asocia a la red inalámbrica (WLAN) sobre la autenticación satisfactoria.Aquí está el tiro de pantalla:

Troubleshooting

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

Estos **comandos debug** serán útiles para resolver problemas la configuración:

Nota: Consulte Información Importante sobre Comandos de Debug antes de usar un **comando debug**.

- **haga el debug del permiso de los eventos del dot1x** — Habilita el debug de todos los eventos del dot1x. Aquí está una salida de los debugs del ejemplo basada en la autenticación satisfactoria:**Nota:** Algunas de las líneas de esta salida han sido segundas líneas movidas debido a las limitaciones de espacio.(Cisco Controller)>**debug dot1x events enable** Wed Feb 20 14:19:57 2007: 00:40:96:af:3e:93 Sending EAP -Request/Identity to mobile 00:40:96:af:3e:93 (EAP Id 1) Wed Feb 20 14:19:57 2007: 00:40:96:af:3e:93 **Received EAPOL START from mobile 00:40:96:af:3e:93** Wed Feb 20 14:19:57 2007: 00:40:96:af:3e:93 **Sending EAP-Request/Identity to mobile 00:40:96:af:3e:93 (EAP Id 2)** Wed Feb 20 14:19:57 2007: 00:40:96:af:3e:93 Received EAP Response packet with mismatching id (currentid=2, eapid=1) from mobile 00:40:96:af:3e:93 Wed Feb 20 14:19:57 2007: 00:40:96:af:3e:93 **Received Identity Response (count=2) from mobile 00:40:96:af:3e:93** Wed Feb 20 14:19:57 2007: 00:40:96:af:3e:93 **Processing Access-Challenge for mobile 00:40:96:af:3e:93**
  ..... Wed Feb 20 14:20:00 2007: 00:40:96:af:3e:93 **Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 19, EAP Type 43)** Wed Feb 20 14:20:00 2007: 00:40:96:af:3e:93 **Processing Access-Challenge for mobile 00:40:96:af:3e:93** Wed Feb 20 14:20:00 2007: 00:40:96:af:3e:93 **Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 20)** Wed Feb 20 14:20:01 2007: 00:40:96:af:3e:93 **Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 20, EAP Type 43)** Wed Feb 20 14:20:29 2007: Creating dot1x interface with key 00:0b:85:91:c3:c0 -0 Wed Feb 20 14:20:29 2007: Resetting the group key timer for 3689 seconds on AP 00:0b:85:91:c3:c0 Wed Feb 20 14:20:29 2007: Creating dot1x interface with key 00:0b:85:91:c3:c0 -1 Wed Feb 20 14:20:29 2007: Resetting the group key timer for 3696 seconds on AP 00:0b:85:91:c3:c0 Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Received EAPOL START from mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Sending EAP-Request/Identity to mobile 00:40:96:af:3e:93 (EAP Id 22) Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Received Identity Response (count=3)

from mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 WARNING: updated EAP-Identifer 22 ===> 19 for STA 00:40:96:af:3e:93 Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 19) Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 19, EAP Type 3) Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 20) Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 20, EAP Type 43) Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 21) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 21, EAP Type 43) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 22) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 22, EAP Type 43) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 23) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 23, EAP Type 43) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 24) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 24, EAP Type 43) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 25) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 25, EAP Type 43) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 26) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 26, EAP Type 43) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 27) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 27, EAP Type 43) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Reject for mobile00:40:96:af:3e:93 Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP-Failure to mobile 00:4096:af:3e:93 (EAP Id 27) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Setting quiet timer for 5 seconds for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP-Request/Identity to mobile 00:40:96:af:3e:93 (EAP Id 1) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP-Request/Identity to mobile 00:40:96:af:3e:93 (EAP Id 1) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAPOL START from mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP-Request/Identity to mobile 00:40:96:af:3e:93 (EAP Id 2) Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received Identity Response (count=2) from mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 WARNING: updated EAP-Identifer 2 ===> 20 for STA 00:40:96:af:3e:93 Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 20) Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 20, EAP Type 3) Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 21) Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 21, EAP Type 43) Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 22) Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 22, EAP Type 43) Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 WARNING: updated EAP-Identifer 22 ===> 24 for STA 00:40:96:af:3e:93 Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 24) Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 24, EAP Type 43) Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 **Processing Access-Challenge for mobile 00:40:96:af:3e:93** Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 **Sending**

```
EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 25) Wed Feb 20 14:20:32 2007:
00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 25, EAP Type
43) Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Processing Access-Accept for mobile
00:40:96:af:3e:93 Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Creating a new PMK Cache Entry
for tation 00:40:96:af:3e:93 (RSN 0) Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending
EAP-Success to mobile 00:40:96:af:3e:93 (EAP Id 25) Wed Feb 20 14:20:32 2007:
00:40:96:af:3e:93 Sending default RC4 key to mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:32
2007: 00:40:96:af:3e:93 Sending Key-Mapping RC4 key to mobile 00:40:96:af:3e:93 Wed Feb 20
14:20:32 2007: 00:40:96:af:3e:93 Received Auth Success while in Authenticating state for
mobile 00:40:96:af:3e:93
```

- **permiso del paquete del dot1x del debug** — Habilita el debug de los mensajes de paquete del 802.1x.
- **permiso de los eventos aaa del debug** — Habilita la salida de los debugs de todos los eventos aaa.

Información Relacionada

- WPA2 - Acceso protegido Wi-Fi 2
- Autenticación del EAP-FAST con el ejemplo de configuración de los reguladores y del servidor RADIUS externo del Wireless LAN
- Ejemplo de Configuración de Autenticación de EAP con Controladores de WLAN (WLC)
- Introducción a la configuración WPA
- Soporte de Productos de Red Inalámbrica
- Soporte Técnico y Documentación - Cisco Systems