Autenticación EAP con el servidor de RADIUS

Contenido

Introducción

Este documento proporciona una configuración de muestra de un Punto de acceso basado IOS® de Cisco para la autenticación del Protocolo de Autenticación Extensible (EAP) de los usuarios de red inalámbrica contra una base de datos accedida por un servidor de RADIUS.

Debido al rol pasivo que el Punto de acceso juega en EAP (paquetes inalámbricos de los Bridges del cliente en los paquetes atados con alambre destinados al servidor de autenticación, y vice versa), esta configuración se utiliza con virtualmente todos los métodos EAP. Estos métodos incluyen (pero no se limitan a) el SALTO, EAP protegido (PEAP) - versión 2 del protocolo de autenticación por desafío mutuo del MS-desafío (GRIETA), la placa Token PEAP-genérica (GTC), la autenticación adaptable de EAP vía el Tunelización seguro (RÁPIDO), la Seguridad de la capa del EAP-transporte (TLS), y TLS EAP-tunneled (TTL). Usted debe configurar apropiadamente al servidor de autenticación para cada uno de estos métodos EAP.

Este documentos abarca cómo configurar el punto de acceso y al servidor de RADIUS, que es Cisco Secure ACS en el ejemplo de configuración en este documento.

prerrequisitos

Requisitos

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Usted es familiar con el Cisco IOS GUI o CLI.
- Usted es familiar con los conceptos detrás de la autenticación EAP.

Componentes Utilizados

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

- Productos del Cisco Aironet AP que funcionan con el Cisco IOS.
- Suposición de solamente un Virtual LAN (VLAN) en la red.
- Un producto del servidor de autenticación de RADIUS que integra con éxito en una base de datos de usuarios.Éstos son los servidores de autenticación soportados para el Cisco LEAP y el EAP-FAST:Cisco Secure Access Control Server (ACS)Access Registrar de Cisco (CAR)Funk Steel Belted RADIUSInterlink MeritÉstos son los servidores de autenticación soportados para la versión 2 de Microsoft PEAP-MS-CHAP y el PEAP-GTC:Internet Authentication Service de Microsoft (IAS)Cisco Secure ACSFunk Steel Belted RADIUSInterlink MeritCualquier servidor de autenticación adicional Microsoft puede autorizar.**Nota:** El GTC o las contraseñas de USO único requiere los servicios adicionales que requieren el software adicional en ambos el lado del cliente y servidor, así como hardware o los generadores de ficha de software.Consulte el fabricante del supplicant del cliente para los detalles sobre los cuales soportan a los servidores de autenticación con sus Productos para el EAP-TLS, el EAP-TTLS y otros métodos EAP.

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.

Configurar

Esta configuración describe cómo configurar la autenticación EAP en un AP basado IOS. En el ejemplo en este documento, el SALTO se utiliza como método de autenticación EAP con el servidor de RADIUS.

Nota: Utilice la herramienta Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos utilizados en esta sección.

Como ocurre con la mayoría de los algoritmos de autenticación basados en contraseñas, Cisco LEAP es vulnerable a los ataques del diccionario. Este no es un ataque o vulnerabilidad nueva del LEAP de Cisco. La creación de una política de contraseña fuerte es la mayoría de la manera eficaz de atenuar los establecimientos de diccionario. Esto incluye el uso de las contraseñas fuertes y del vencimiento periódico de contraseñas. Refiera al establecimiento de diccionario en el Cisco LEAP para conseguir más información sobre los establecimientos de diccionario y cómo prevenirlos.

Este documento utiliza esta configuración para el GUI y el CLI:

- La dirección IP del AP es 10.0.0.106.
- La dirección IP del servidor de RADIUS (ACS) es 10.0.0.3.

Red EAP (Protocolo de autenticación extensible) o autenticación abierta con EAP.

En cualquier EAP/802.1x basado método de autentificación, usted puede preguntar cuáles están las diferencias entre la red EAP y la autenticación abierta con el EAP. Estos elementos refieren a los valores en el campo del algoritmo de autenticación en los encabezamientos de administración y los paquetes de asociación. La mayoría de los fabricantes de conjunto de los clientes de red inalámbrica este campo en el valor 0 (autenticación abierta), entonces señalan un deseo de hacer la autenticación EAP más adelante en el proceso de asociación. Cisco establece un valor distinto, desde el comienzo de la asociación con el indicador de red EAP.

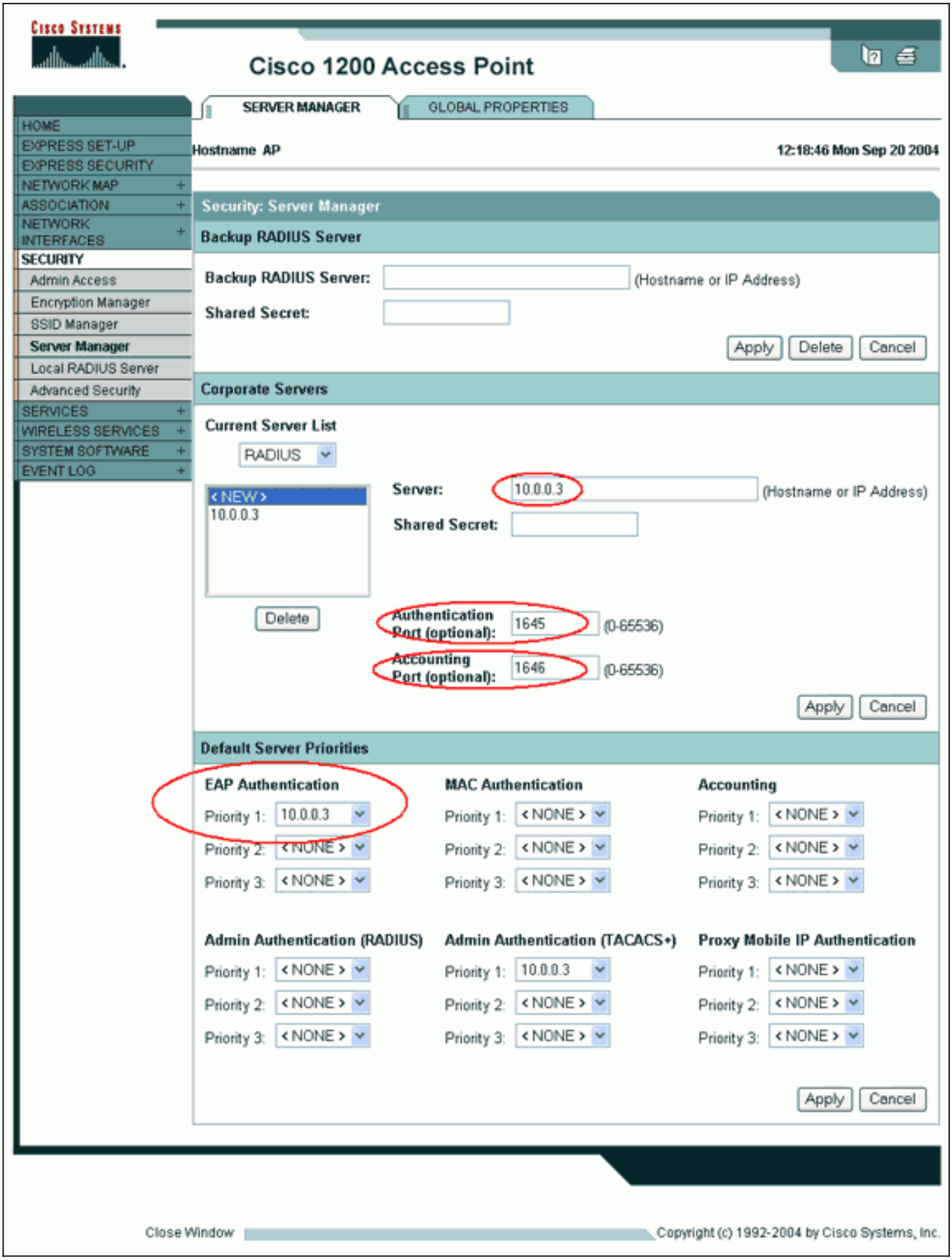
Si su red posee clientes que son:

- Clientes de Cisco — Utilice el Network EAP.
- Clientes del otro vendedor (incluya los productos compatibles con CCX) — Utilice abierto con el EAP.
- Una combinación de ambo Cisco y los clientes del otro vendedor — elija el Network EAP y ábrase con el EAP.

Defina al servidor de autenticación

El primer paso en la configuración EAP es definir al servidor de autenticación y establecer una relación con él.

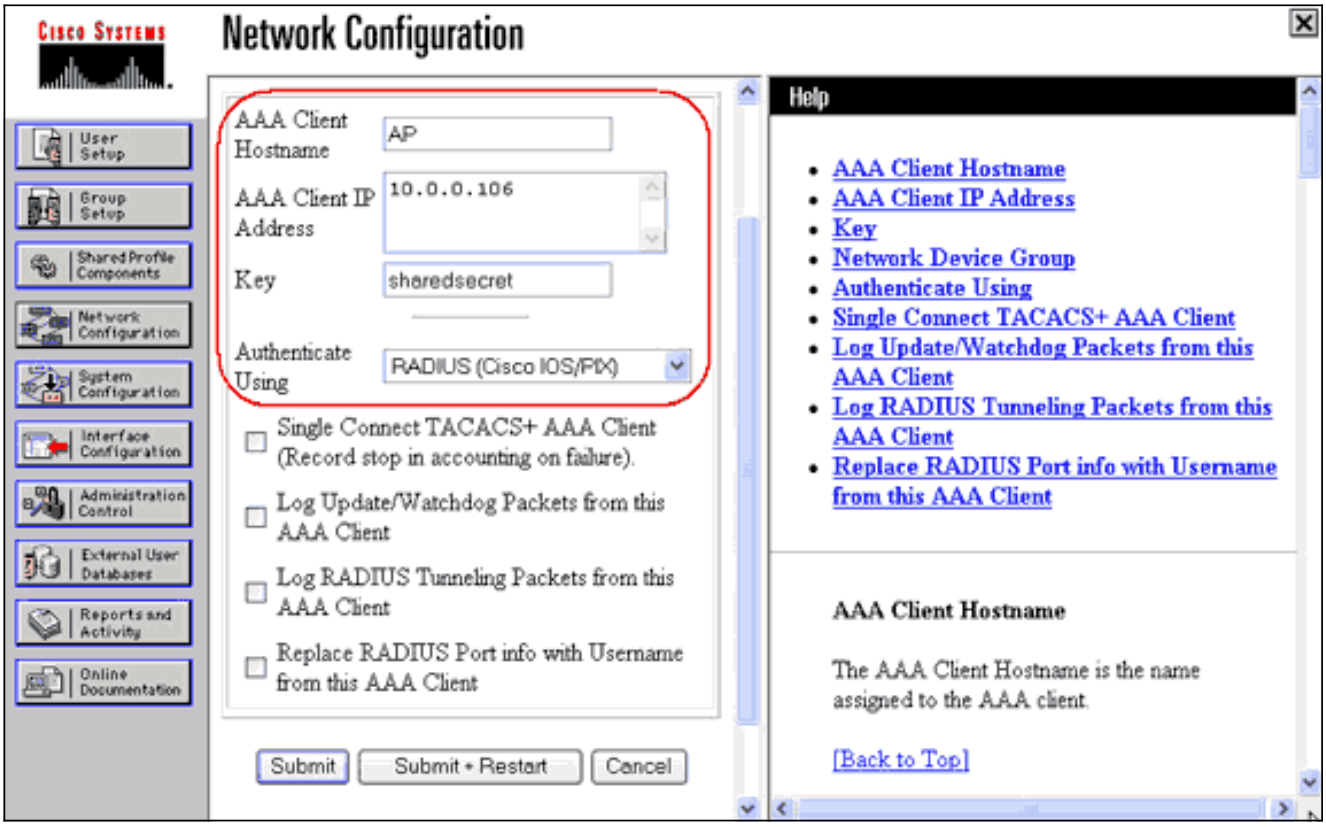
1. En la lengueta del administrador de servidor del Punto de acceso (conforme al elemento de menú de la **Seguridad > del administrador de servidor**), complete estos pasos:Ingrese el IP Address del servidor de autenticación en el campo del servidor.Especifique el secreto compartido y los puertos.El tecleo **se aplica** para crear la definición y poblar las listas desplegables.Fije el campo de la prioridad 1 del tipo de la autenticación EAP al dirección IP del servidor bajo prioridades predeterminadas del servidor.Haga clic en Apply (Aplicar).



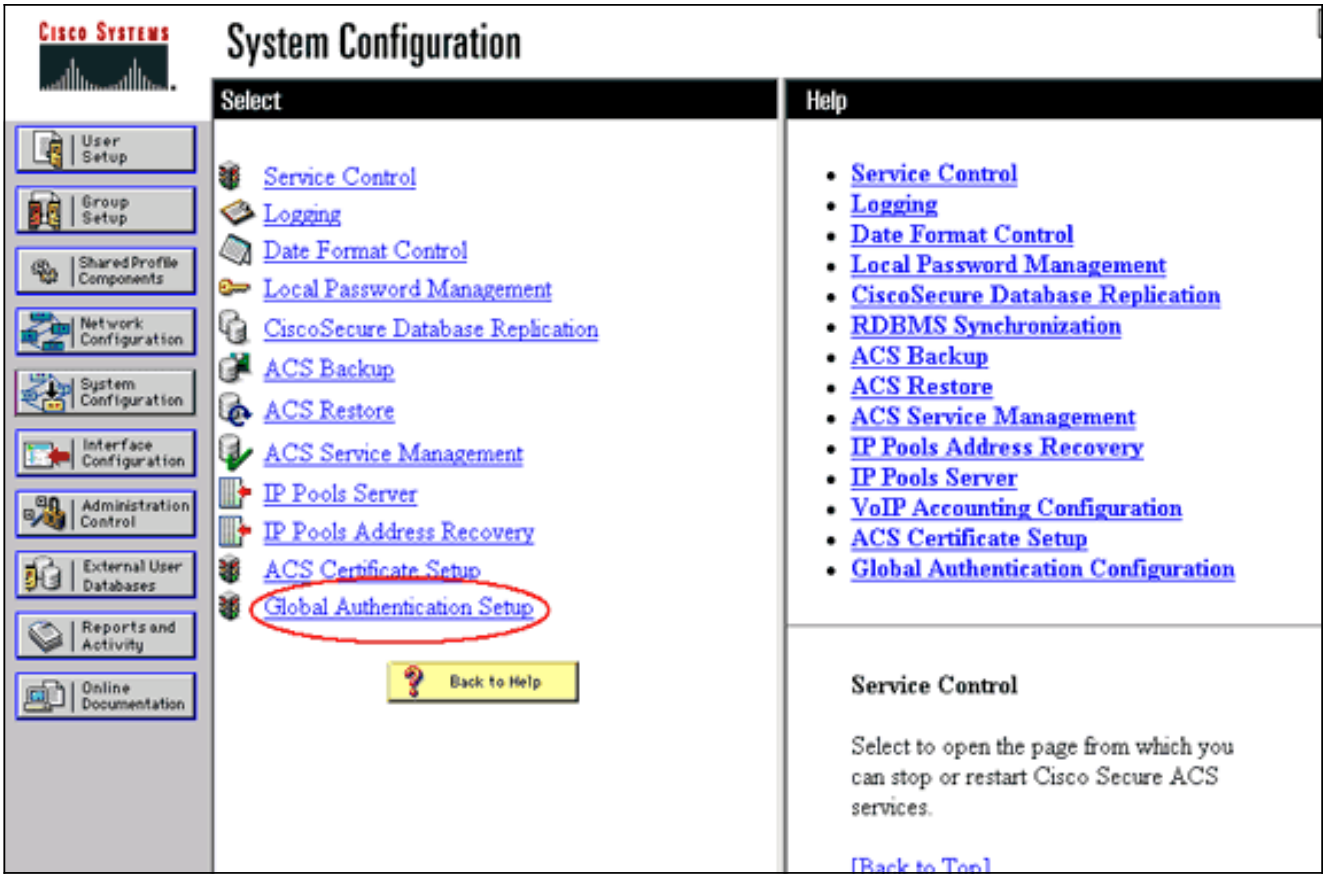
Usted puede también publicar estos comandos del CLI:`AP#configure terminal Enter configuration commands, one per line. End with CNTL/Z. AP(config)#aaa group server radius rad_eap AP(config-sg-radius)#server 10.0.0.3 auth-port 1645 acct-port 1646 AP(config-sg-radius)#exit AP(config)#aaa new-model AP(config)#aaa authentication login eap_methods group rad_eap AP(config)#radius-server host 10.0.0.3 auth-port 1645 acct-port 1646 key labap1200ip102 AP(config)#end AP#write memory`

2. El Punto de acceso se debe configurar en el servidor de autenticación como cliente AAA.Por ejemplo, en el Cisco Secure ACS, esto sucede en la página de la [configuración de red]

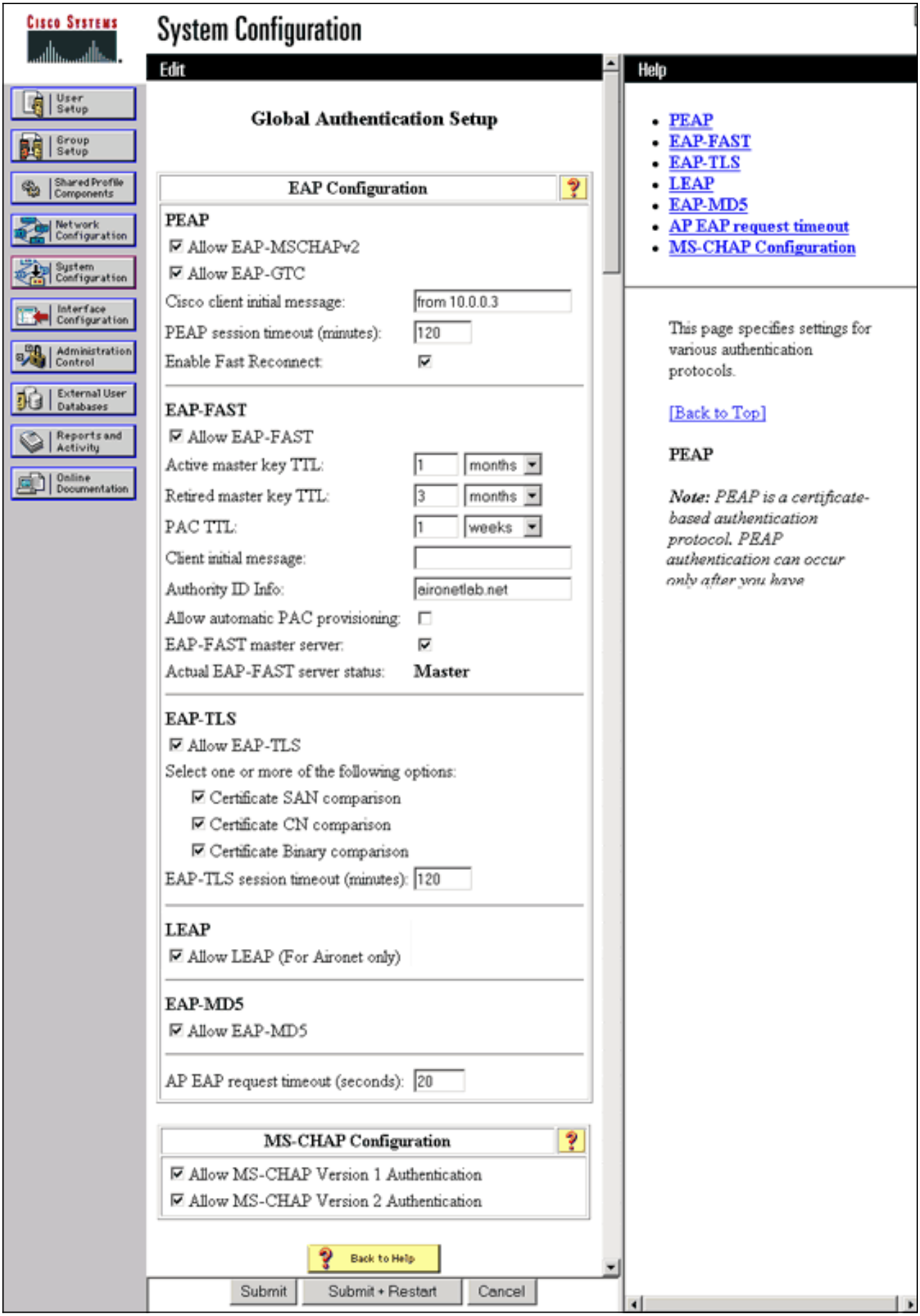
donde el nombre del Punto de acceso, la dirección IP, el secreto compartido y el método de autentificación (Cisco Aironet o RADIUS Cisco IOS/PIX RADIUS) se definen. Refiera a la documentación del fabricante para otros servidores de autenticación NON-ACS.



Asegúrese de que configuren al servidor de autenticación para realizar el método de autenticación EAP deseado. Por ejemplo, para un Cisco Secure ACS que SALTA, configurar la autenticación LEAP en la configuración del sistema - página de configuración de la autenticación global. **La configuración del sistema del** tecleo, entonces hace clic la **configuración de la autenticación global**. Refiera a la documentación del fabricante para otros servidores de autenticación NON-ACS u otros métodos EAP.



Esta imagen muestra el Cisco Secure ACS configurado para el PEAP, el EAP-FAST, el EAP-TLS, el SALTO y el EAP-
MD5.

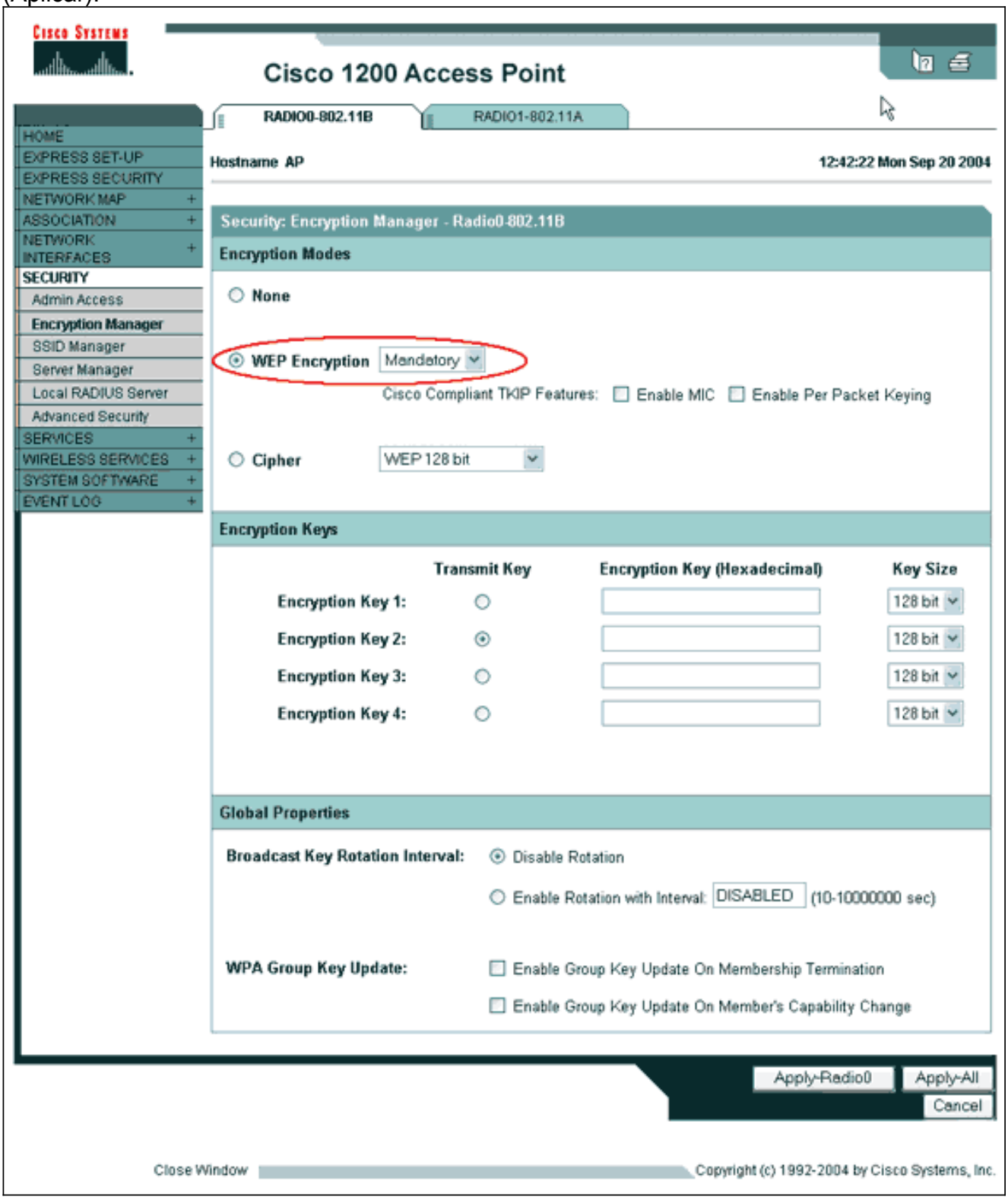


[Defina los métodos de autenticación de cliente]

Una vez que el Punto de acceso sabe dónde enviar las peticiones de la autenticación de cliente, la configura para validar esos métodos.

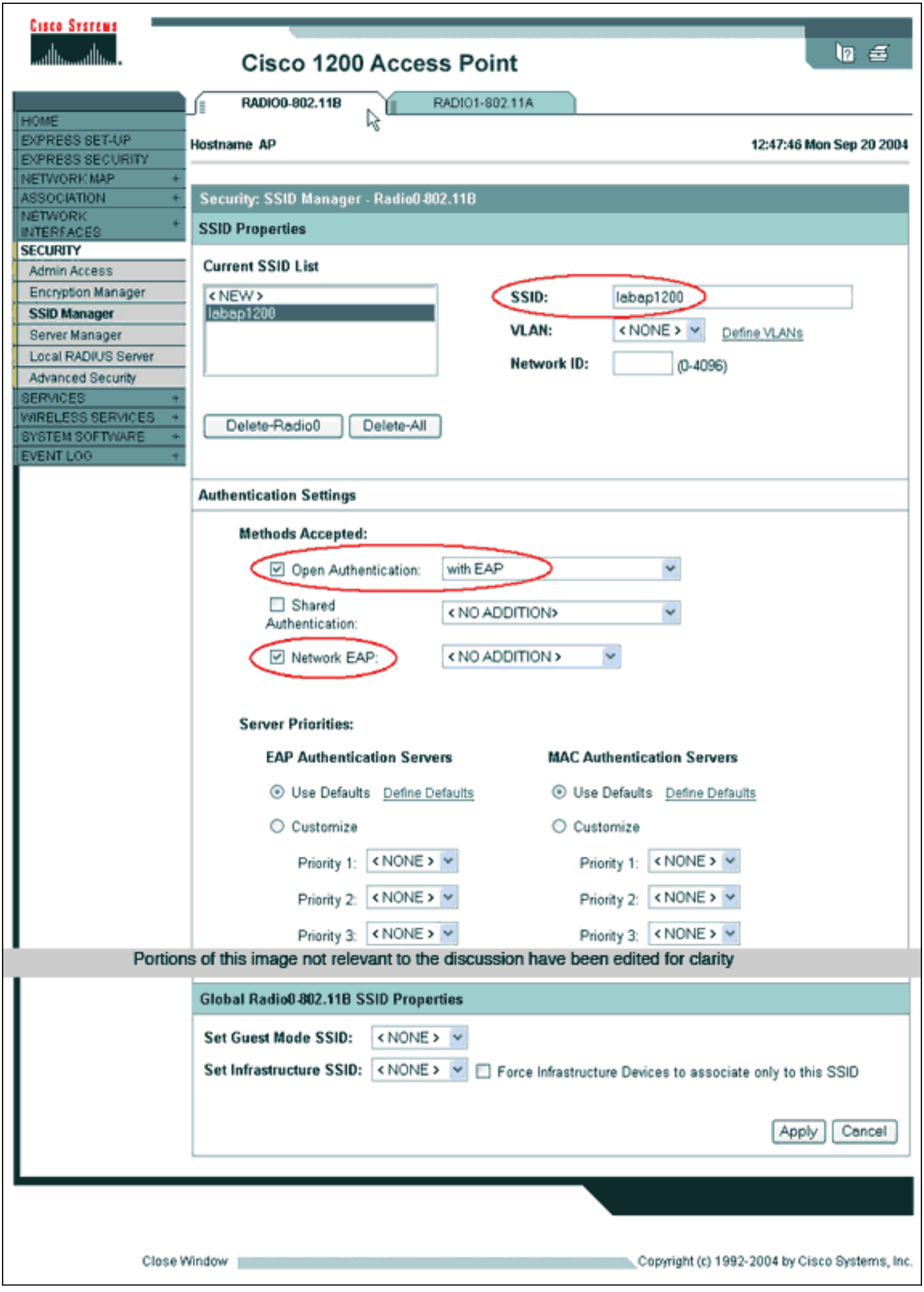
Nota: Estas instrucciones están para una instalación basada en el WEP. Para el WPA (que utiliza las cifras en vez del WEP), refiera a la introducción a la configuración de WPA.

1. En la ficha Manager del cifrado del Punto de acceso (conforme a la **Seguridad > al** elemento de menú del **administrador del cifrado**), complete estos pasos:Especifique que usted quiere utilizar la **encripción WEP**.Especifique que el WEP es **obligatorio**.Verifique que el tamaño de clave esté fijado al **128-bits**.Haga clic en Apply (Aplicar).



Usted puede también publicar estos comandos del CLI:`AP#configure terminal Enter configuration commands, one per line. End with CNTL/Z. AP(config)#interface dot11radio 0 AP(config-if)#encryption mode wep mandatory AP(config-if)#end AP#write memory`

2. Complete estos pasos en la lengueta del administrador SSID del Punto de acceso (conforme al elemento de menú de la **Seguridad > del administrador SSID**):Seleccione el SSID deseado.Bajo “métodos de autentificación validados,” marque el cuadro etiquetado **abierto** y utilice la lista desplegable para elegir **con el EAP**.Marque el cuadro etiquetado **Network EAP** si usted tiene indicadores luminosos LED amarillo de la placa muestra gravedad menor del cliente de Cisco. Vea la discusión en la red EAP o la autenticación abierta con la sección EAP.Haga clic en Apply (Aplicar).



Usted puede también publicar estos comandos del CLI:

```
AP#configure terminal Enter configuration commands, one per line. End with CNTL/Z.
AP(config)#interface dot11radio 0 AP(config-if)#ssid labap1200 AP(config-if-ssid)#authentication
open eap eap_methods AP(config-if-ssid)#authentication network-eap eap_methods AP(config-if-
ssid)#end AP#write memory
```

Una vez que usted confirma la funcionalidad básica con una configuración de EAP básica, usted puede agregar las características adicionales y la administración de claves en otro momento. Acode funciones más complejas encima de las bases funcionales para hacer resolver problemas más fácil.

Verificación

En esta sección encontrará información que puede utilizar para comprobar que su configuración funcione correctamente.

La herramienta Output Interpreter (sólo para clientes registrados) permite utilizar algunos comandos “show” y ver un análisis del resultado de estos comandos.

- **muestre el grupo de servidores todo del radio** — Visualiza una lista de todos los grupos de servidores configurados RADIUS en el AP.

Troubleshooting

Procedimiento de resolución de problemas

Complete estos pasos para resolver problemas su configuración.

1. En la utilidad o el software del client cara, cree un nuevo perfil o conexión con el mismo o los parámetros similares para asegurarse de que nada se ha corrompido en la configuración del cliente.
2. Para eliminar la posibilidad de los problemas RF que previenen la autenticación satisfactoria, temporalmente autenticación de la neutralización tal y como se muestra en de estos pasos:Del CLI, utilice los comandos no authentication open eap eap_methods, no authentication network-eap eap_methods y authentication open.Del GUI, en la página del administrador SSID, el **Network EAP del O.N.U-**control, marca **abierto**, y fijó la lista desplegable de nuevo a **ninguna adición**.Si el cliente se asocia con éxito, después el RF no contribuye al problema de asociación.
3. Verifique que las contraseñas del secreto compartido estén sincronizadas entre el Punto de acceso y el servidor de autenticación. Si no, usted puede recibir este mensaje de error:`Invalid message authenticator in EAP request`Del CLI, marque la línea `clave del acct-puerto x del auténtico-puerto x del host de servidor RADIUS x.x.x.x <shared_secret>`.Del GUI, en la página del administrador de servidor, entre el secreto compartido de nuevo para el servidor apropiado en el cuadro etiquetado “secreto compartido.”La entrada del secreto compartido para el Punto de acceso en el servidor de RADIUS debe contener la misma contraseña del secreto compartido que ésas mencionaron previamente.
4. Elimine cualquier grupo de usuarios del servidor RADIUS. Los conflictos pueden ocurrir a veces entre los grupos de usuarios definidos por el servidor de RADIUS, y los grupos de usuarios en el dominio subyacente. Marque los registros del servidor de RADIUS para los intentos fallidos, y las razones que esas tentativas fallaron.

Comandos para Troubleshooting

La herramienta Output Interpreter (sólo para clientes registrados) permite utilizar algunos comandos “show” y ver un análisis del resultado de estos comandos.

Hacer el debug de las autenticaciones proporciona a una cantidad significativa de detalle sobre cómo recolectar e interpretar la salida de los debugs relacionados con el EAP.

Nota: Antes de que usted publique los **comandos debug**, refiera a la información importante en los comandos Debug.

- **haga el debug de la estado-máquina del authenticator aaa del dot11** — Las visualizaciones major las divisiones (o los estados) de la negociación entre el cliente y el servidor de autenticación. Aquí está una salida de una **autenticación satisfactoria**:`*Mar 1 02:37:46.846: dot11_auth_dot1x_send_id_req_to_client: Sending identity request to 0040.96ac.dd05 *Mar 1 02:37:46.846: dot11_auth_dot1x_send_id_req_to_client: 0040.96ac.dd05 timer started for 30 seconds *Mar 1 02:37:46.930: dot11_auth_dot1x_run_rfsm: Executing Action(CLIENT_WAIT,EAP_START) for 0040.96ac.dd05 *Mar 1 02:37:46.931: dot11_auth_dot1x_send_id_req_to_client:` **`Sending identity request to 0040.96ac.dd05 (client)`** `*Mar 1 02:37:46.931: dot11_auth_dot1x_send_id_req_to_client: Client 0040.96ac.dd05 timer started for 30 seconds *Mar 1 02:37:46.938: dot11_auth_dot1x_run_rfsm: Executing Action(CLIENT_WAIT,CLIENT_REPLY) for 0040.96ac.dd05 *Mar 1 02:37:46.938: dot11_auth_dot1x_send_response_to_server:` **`Sending client 0040.96ac.dd05 data (User Name) to server`** `*Mar 1 02:37:46.938: dot11_auth_dot1x_send_response_to_server: Started timer server_timeout 60 seconds *Mar 1 02:37:47.017: dot11_auth_dot1x_run_rfsm: Executing Action(SERVER_WAIT,SERVER_REPLY) for 0040.96ac.dd05 *Mar 1 02:37:47.017: dot11_auth_dot1x_send_response_to_client:` **`Forwarding server message(Challenge) to client 0040.96ac.dd05`** `*Mar 1 02:37:47.018: dot11_auth_dot1x_send_response_to_client: Started timer client_timeout 20 seconds *Mar 1 02:37:47.025: dot11_auth_dot1x_run_rfsm: Executing Action(CLIENT_WAIT,CL IENT_REPLY) for 0040.96ac.dd05 *Mar 1 02:37:47.025: dot11_auth_dot1x_send_response_to_server:` **`Sending client 0040.96ac.dd05 data(User Credentials) to server`** `----------Lines Omitted for simplicity---------- *Mar 1 02:37:47.030: dot11_auth_dot1x_send_response_to_client: Started timer client_timeout 20 seconds *Mar 1 02:37:47.041: dot11_auth_dot1x_run_rfsm: Executing Action (SERVER_WAIT,`**`SE RVER_PASS)`** `for 0040.96ac.dd05 *Mar 1 02:37:47.041: dot11_auth_dot1x_send_response_to_client:` **`Forwarding server message(Pass Message) to client 0040.96ac.dd05`** `*Mar 1 02:37:47.042: dot11_auth_dot1x_send_response_to_client: Started timer client_timeout 30 seconds *Mar 1 02:37:47.043: %DOT11-6-ASSOC:` **`Interface Dot11Radio0, Station TACWEB 0040 .96ac.dd05 Associated KEY_MGMT[NONE] (Client stays associated to the access point)`** **Nota:** En las versiones de Cisco IOS Software antes de 12.2(15)JA, el sintaxis de este **comando debug** es estado-**máquina del dot1x aaa del dot11 del debug**.
- **proceso del authenticator aaa del dot11 del debug** — Visualiza las entradas de diálogo individual de la negociación entre el cliente y el servidor de autenticación.**Nota:** En las versiones de Cisco IOS Software antes de 12.2(15)JA, el sintaxis de este comando debug es **proceso del dot1x aaa del dot11 del debug**.
- **autenticación de RADIUS del debug** — Visualiza las negociaciones RADIUS entre el servidor y el cliente, que, es interligado por el AP. Esto es una salida para la **autenticación fallida**:`*Mar 1 02:34:55.086: RADIUS/ENCODE(00000031):Orig. component type = DOT11 *Mar 1 02:34:55.086: RADIUS: AAA Unsupported Attr: ssid [264] 5 *Mar 1 02:34:55.086: RADIUS: 73 73 69 [ssi] *Mar 1 02:34:55.086: RADIUS: AAA Unsupported Attr: interface [157] 3 *Mar 1 02:34:55.087: RADIUS: 32 [2] *Mar 1 02:34:55.087: RADIUS(00000031): Config` **`NAS IP: 10.0.0.106`** `*Mar 1 02:34:55.087: RADIUS/ENCODE(00000031): acct_session_id: 47 *Mar 1 02:34:55.087: RADIUS(00000031): Config NAS IP: 10.0.0.106 *Mar 1 02:34:55.087: RADIUS(00000031): sending *Mar 1 02:34:55.087:`

```
RADIUS(00000031): Send Access-Request to 10.0.0.3 :164 5 id 1645/61, len 130 *Mar 1
02:34:55.088: RADIUS: authenticator 0F 6D B9 57 4B A3 F2 0E - 56 77 A4 7E D3 C2 26 EB *Mar 1
02:34:55.088: RADIUS: User-Name [1] 8 "wirels" *Mar 1 02:34:55.088: RADIUS: Framed-MTU [12]
6 1400 *Mar 1 02:34:55.088: RADIUS: Called-Station-Id [30] 16 "0019.a956.55c0" *Mar 1
02:34:55.088: RADIUS: Calling-Station-Id [31] 16 "0040.96ac.dd05" *Mar 1 02:34:55.088:
RADIUS: Service-Type [6] 6 Login [1] *Mar 1 02:34:55.088: RADIUS: Message-Authenticato[80]
18 *Mar 1 02:34:55.089: RADIUS: 73 8C 59 C4 98 51 53 9F 58 4D 1D EB A5 4A AB 88
[s?Y??QS?XM???J??] *Mar 1 02:34:55.089: RADIUS: EAP-Message [79] 13 *Mar 1 02:34:55.089:
RADIUS: NAS-Port-Id [87] 5 "299" *Mar 1 02:34:55.090: RADIUS: NAS-IP-Address [4] 6
10.0.0.106 *Mar 1 02:34:55.090: RADIUS: Nas-Identifier [32] 4 "ap" *Mar 1 02:34:55.093:
RADIUS: Received from id 1645/61 10.0.0.3 :1645, Access-Challenge, len 79 *Mar 1
02:34:55.093: RADIUS: authenticator 72 FD C6 9F A1 53 8F D2 - 84 87 49 9B B4 77 B8 973 -----
----------------------Lines Omitted---------------------------------- *Mar 1 02:34:55.117:
RADIUS(00000031): Config NAS IP: 10.0.0.106 *Mar 1 02:34:55.118: RADIUS/ENCODE(00000031):
acct_session_id: 47 *Mar 1 02:34:55.118: RADIUS(00000031): Config NAS IP: 10.0.0.106 *Mar 1
02:34:55.118: RADIUS(00000031): sending *Mar 1 02:34:55.118: RADIUS(00000031): Send Access-
Request to 10.0.0.3 :164 5 id 1645/62, len 168 *Mar 1 02:34:55.118: RADIUS: authenticator 49
AE 42 83 C0 E9 9A A7 - 07 0F 4E 7C F4 C7 1F 24 *Mar 1 02:34:55.118: RADIUS: User-Name [1] 8
"wirels" *Mar 1 02:34:55.119: RADIUS: Framed-MTU [12] 6 1400 ----------------------------
---Lines Omitted---------------------- *Mar 1 02:34:55.124: RADIUS: Received from id
1645/62 10.0.0.3 :1645, Access-Reject, len 56 *Mar 1 02:34:55.124: RADIUS: authenticator A6
13 99 32 2A 9D A6 25 - AD 01 26 11 9A F6 01 37 *Mar 1 02:34:55.125: RADIUS: EAP-Message [79]
6 *Mar 1 02:34:55.125: RADIUS: 04 15 00 04 [????] *Mar 1 02:34:55.125: RADIUS: Reply-Message
[18] 12 *Mar 1 02:34:55.125: RADIUS: 52 65 6A 65 63 74 65 64 0A 0D [Rejected??] *Mar 1
02:34:55.125: RADIUS: Message-Authenticato[80] 18 *Mar 1 02:34:55.126: RADIUS(00000031):
Received from id 1645/62 *Mar 1 02:34:55.126: RADIUS/DECODE: EAP-Message fragments, 4, total
4 bytes *Mar 1 02:34:55.126: RADIUS/DECODE: Reply-Message fragments, 10, total 10 bytes *Mar
1 02:34:55.127: %DOT11-7-AUTH_FAILED: Station 0040.96ac.dd05 Authentication failed
```

- **autenticación aaa del debug** — Visualiza las Negociaciones AAA para autenticación entre el dispositivo del cliente y el servidor de autenticación.

Información Relacionada

- Autenticaciones del debug
- Configuración de los tipos de autenticación
- Autenticación LEAP en un servidor de RADIUS local
- Configuración de los servidores RADIUS y TACACS+
- Configurar el v3.2 del Cisco Secure ACS for Windows con la autenticación de la máquina PEAP-MS-CHAPv2
- V3.2 del Cisco Secure ACS for Windows con la autenticación de la máquina del EAP-TLS
- Configurar el PEAP/EAP en el Microsoft IAS
- Resolver problemas el Microsoft IAS como servidor de RADIUS
- Autenticación de clientes del 802.1x de Microsoft
- Soporte Técnico y Documentación - Cisco Systems