# Autenticación del EAP con servidor RADIUS

## Contenido


Introducción
Prerequisites
Requirements
Componentes Utilizados
Convenciones
Configurar
Red EAP (Protocolo de autenticación extensible) o autenticación abierta con EAP.
Definir servidor de autenticación
Definir métodos de autenticación de cliente
Verificación
Troubleshoot
Procedimiento de resolución de problemas
Comandos para Troubleshooting
Información Relacionada


## Introducción

Este documento proporciona una configuración de ejemplo de un punto de acceso basado en Cisco IOS® para la autenticación EAP (Extensible Authentication Protocol, protocolo de autenticación extensible) de usuarios inalámbricos en una base de datos a la que se accede a través de un servidor RADIUS.

Debido a la función pasiva que el punto de acceso desempeña en EAP (une paquetes inalámbricos del cliente en paquetes cableados destinados al servidor de autenticación y viceversa), esta configuración se utiliza con prácticamente todos los métodos EAP. Estos métodos incluyen (pero no se limitan a) LEAP, EAP protegido (PEAP)-MS-Challenge Handshake Authentication Protocol (CHAP) versión 2, PEAP-Generic Token Card (GTC), EAP-autenticación flexible a través de tunelación segura (FAST), EAP-seguridad de capa de transporte (TLS) y EAP-TLS tunelado (TTLS). Debe configurar apropiadamente el servidor de autenticación para cada uno de estos métodos EAP.

Este documento describe cómo configurar el punto de acceso (AP) y el servidor RADIUS, que es Cisco Secure ACS en el ejemplo de configuración de este documento.

## Prerequisites

### Requirements

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Está familiarizado con la GUI o CLI de Cisco IOS.
- Está familiarizado 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 Cisco Aironet AP que ejecutan Cisco IOS.
- Suposición de una sola LAN virtual (VLAN) en la red.
- Un producto de servidor de autenticación RADIUS que se integra correctamente en una base de datos de usuarios.Estos son los servidores de autenticación soportados para Cisco LEAP y EAP-FAST:Cisco Secure Access Control Server (ACS)Access Registrar de Cisco (CAR)Funk Steel Belted RADIUSInterlink MeritEstos son los servidores de autenticación soportados para Microsoft PEAP-MS-CHAP versión 2 y PEAP-GTC:Servicio de autenticación de Internet (IAS) de MicrosoftCisco Secure ACSFunk Steel Belted RADIUSInterlink MeritCualquier servidor de autenticación adicional que Microsoft pueda autorizar.**Nota:** Las contraseñas GTC o One-Time requieren servicios adicionales que requieren software adicional tanto en el lado del cliente como del servidor, así como generadores de token de hardware o software.Consulte al fabricante del solicitante del cliente para obtener detalles sobre qué servidores de autenticación son compatibles con sus productos para EAP-TLS, EAP-TTLS y otros métodos EAP.

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.

## 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 en IOS. En el ejemplo de este documento, LEAP se utiliza como método de autenticación EAP con servidor RADIUS.

Nota: Utilice la herramienta Command Lookup (sólo para clientes registrados) 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 segura es la forma más eficaz de mitigar los ataques de diccionario. Esto incluye el uso de contraseñas seguras y la caducidad periódica de contraseñas. Refiérase a Dictionary Attack on Cisco LEAP para obtener más información sobre los ataques de diccionario y cómo prevenirlos.

Este documento utiliza esta configuración tanto para la GUI como para la CLI:

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

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

En cualquier método de autenticación basado en EAP/802.1x, puede preguntarse cuáles son las diferencias entre EAP de red y autenticación abierta con EAP. Estos elementos hacen referencia a los valores del campo Authentication Algorithm en los encabezados de los paquetes de administración y asociación. La mayoría de los fabricantes de clientes inalámbricos configuran este campo en el valor 0 (autenticación abierta) y, a continuación, señalan el deseo de realizar 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.

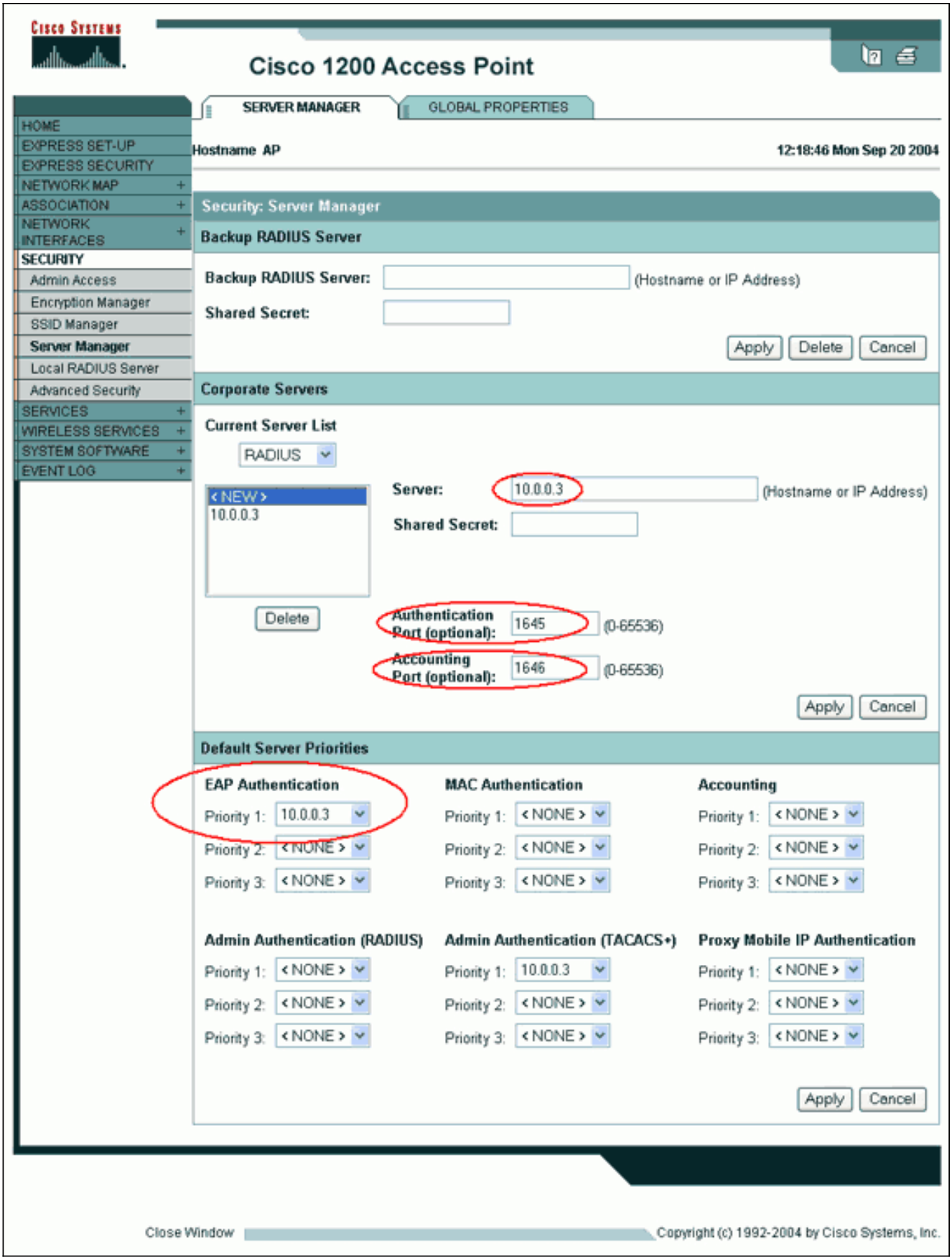
Si su red posee clientes que son:

- Los clientes de Cisco—usan EAP de red.
- Los clientes de terceros (incluidos los productos compatibles con CCX)—utilizan Abrir con EAP.
- Una combinación de clientes de Cisco y de terceros: elija Network-EAP y Open con EAP.

## Definir servidor de autenticación

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

1. En la ficha Administrador del servidor del punto de acceso (en el elemento de menú **Seguridad > Administrador del servidor**), siga estos pasos:Introduzca la dirección IP del servidor de autenticación en el campo Servidor.Especifique el secreto compartido y los puertos.Haga clic en **Aplicar** para crear la definición y rellenar las listas desplegables.Establezca el campo EAP Authentication type Priority 1 en la dirección IP del servidor bajo Default Server Priorities.Haga clic en Apply (Aplicar).

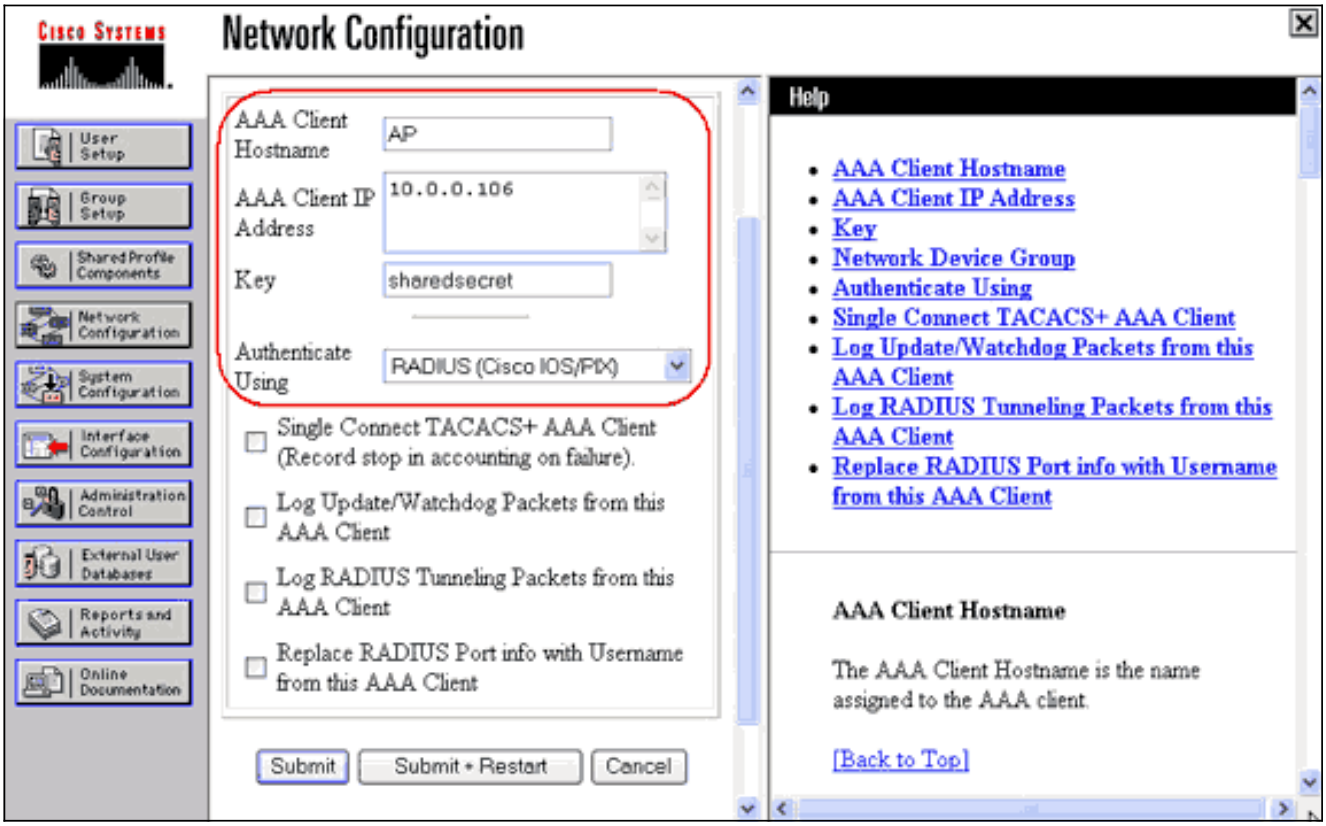



También puede ejecutar estos comandos desde la CLI:

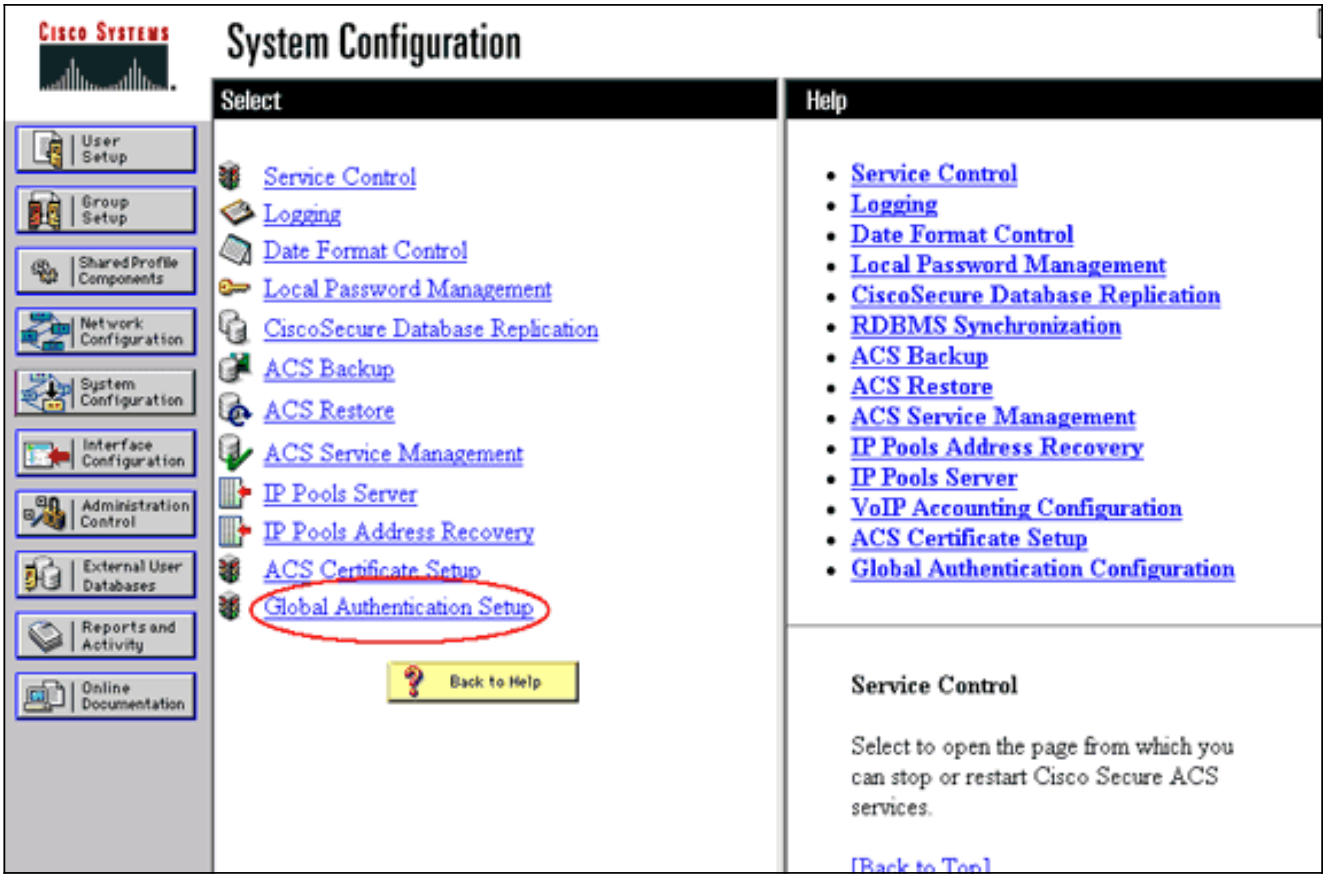
```
AP#configure terminal

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
```

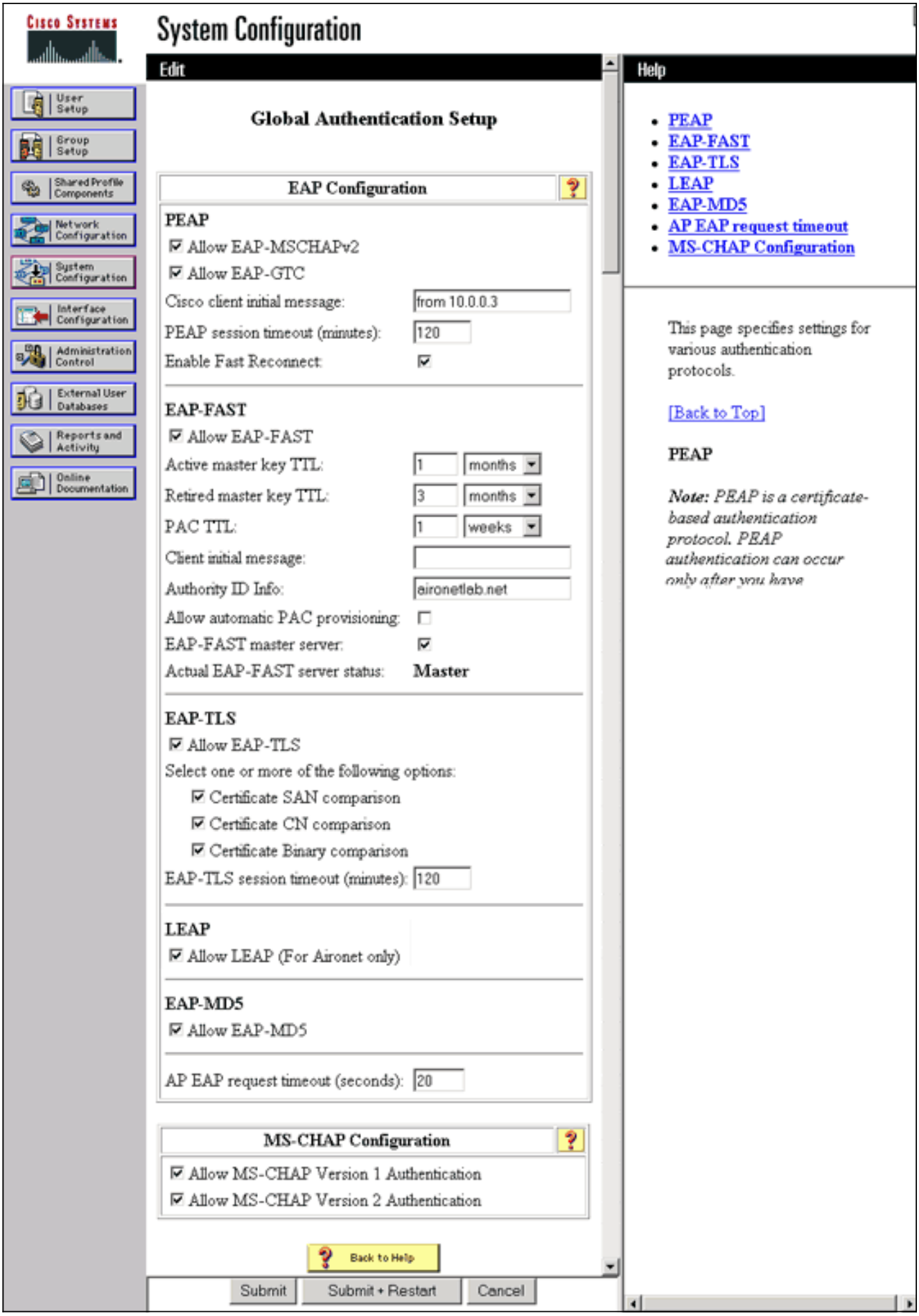
2. El punto de acceso se debe configurar en el servidor de autenticación como cliente AAA.Por ejemplo, en Cisco Secure ACS, esto sucede en la página Configuración de Red donde se define el nombre del punto de acceso, la dirección IP, el secreto compartido y el método de autenticación (RADIUS Cisco Aironet o RADIUS Cisco IOS/PIX). Consulte la documentación del fabricante para otros servidores de autenticación no ACS.




Asegúrese de que el servidor de autenticación esté configurado para realizar el método de autenticación EAP deseado. Por ejemplo, para un Cisco Secure ACS que ejecuta LEAP, configure la autenticación LEAP en la página Configuración del sistema - Configuración de autenticación global. Haga clic en **Configuración del sistema** y, a continuación, haga clic en **Configuración de autenticación global**. Consulte la documentación del fabricante para otros servidores de autenticación no ACS u otros métodos EAP.




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

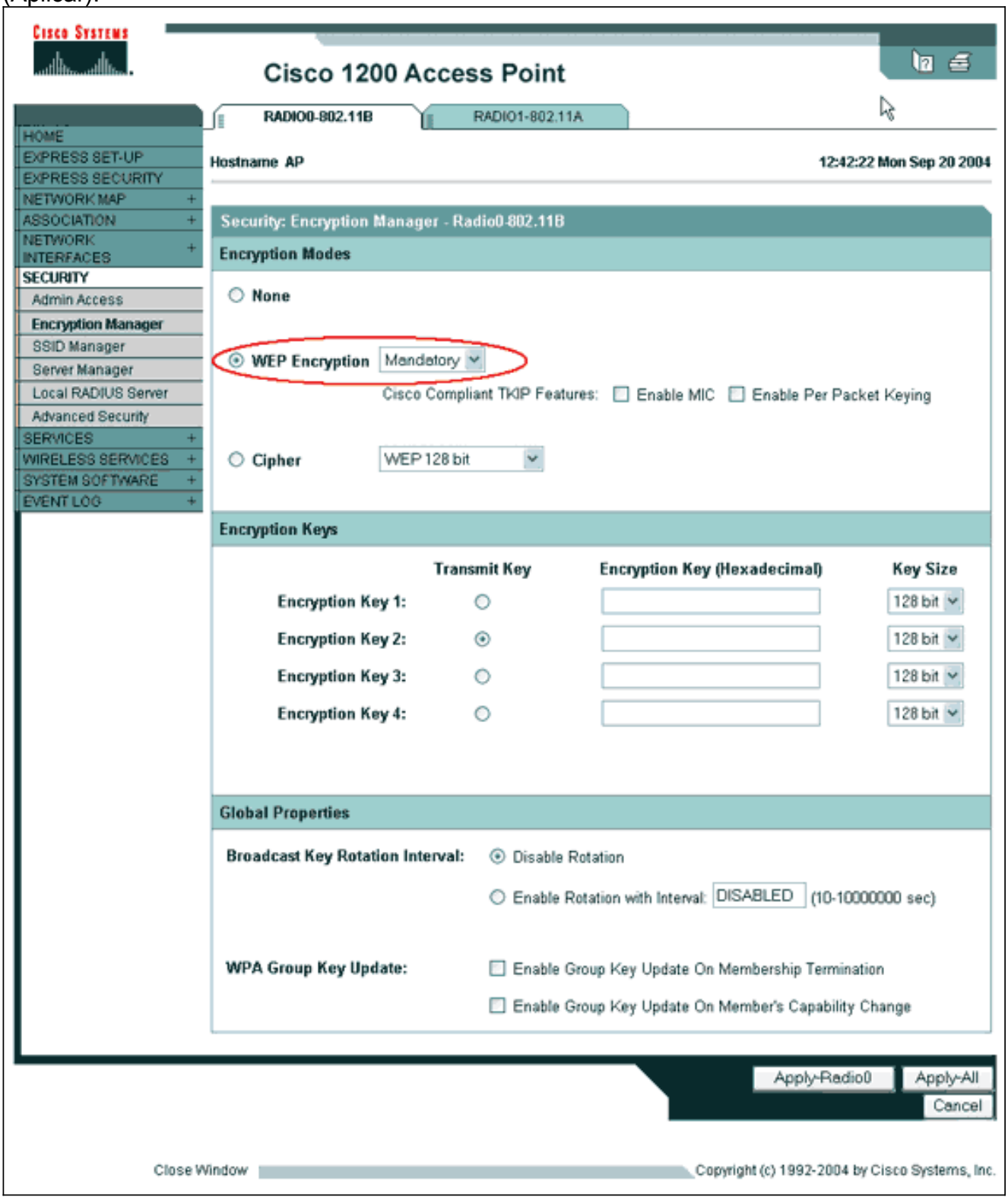



Definir métodos de autenticación de cliente

Una vez que el punto de acceso sabe dónde enviar las solicitudes de autenticación del cliente, configúrelo para que acepte esos métodos.

**Nota:** Estas instrucciones son para una instalación basada en WEP. Para WPA (que utiliza cifrados en lugar de WEP), consulte Descripción general de la configuración WPA.

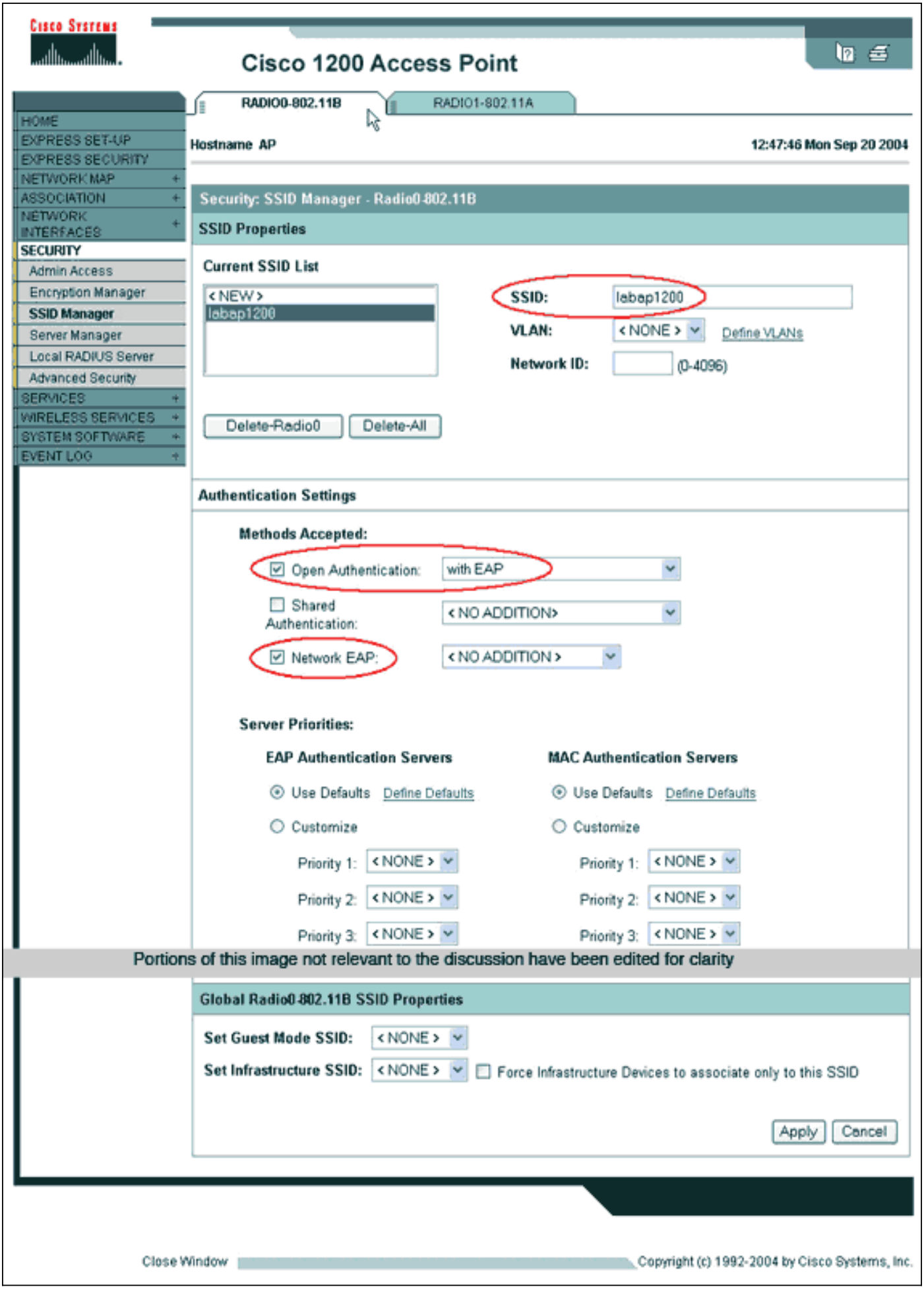
1. En la ficha Administrador de cifrado del punto de acceso (en el elemento de menú **Seguridad > Administrador de cifrado**), realice estos pasos:Especifique que desea utilizar la **encriptación WEP**.Especifique que WEP es **obligatorio**.Verifique que el tamaño de la clave esté establecido en **128 bits**.Haga clic en Apply (Aplicar).



También puede ejecutar estos comandos desde la 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 pestaña Administrador de SSID del punto de acceso (en el elemento de menú **Seguridad > Administrador de SSID**):Seleccione el SSID deseado.En "Métodos de autenticación aceptados", marque la casilla **Abrir** y use la lista desplegable para elegir **Con EAP**.Marque la casilla **Network-EAP** si tiene tarjetas de cliente de Cisco. Vea la discusión en la sección EAP de red o Autenticación abierta con EAP.Haga clic en Apply (Aplicar).




También puede ejecutar estos comandos desde la 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 confirma la funcionalidad básica con una configuración EAP básica, puede agregar funciones adicionales y administración de claves más adelante. Capte funciones más complejas sobre bases funcionales para facilitar la resolución de problemas.

# 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.

- **show radius server-group all**: muestra una lista de todos los grupos de servidores RADIUS configurados en el AP.

# Troubleshoot

## Procedimiento de resolución de problemas

Complete estos pasos para resolver los problemas de configuración.

1. En la utilidad o el software del lado del cliente, cree un nuevo perfil o conexión con los mismos parámetros o similares para asegurarse de que nada se ha corrompido en la configuración del cliente.
2. Para eliminar la posibilidad de problemas de RF que impiden una autenticación exitosa, inhabilite temporalmente la autenticación como se muestra en estos pasos:Desde la CLI, utilice los comandos **no authentication open eap_method**, **no authentication network-eap eap_method** y **authentication open**.Desde la GUI, en la página SSID Manager, desmarque **Network-EAP**, marque **Open** y vuelva a establecer la lista desplegable en **No Addition**.Si el cliente se asocia correctamente, RF no contribuye al problema de asociación.
3. Verifique que las contraseñas secretas compartidas estén sincronizadas entre el punto de acceso y el servidor de autenticación. De lo contrario, puede recibir este mensaje de error: `Invalid message authenticator in EAP request`
   Desde la CLI, verifique la línea `radius-server host x.x.x.x auth-port x acct-port x key`

<shared_secret>.En la GUI, en la página Administrador de servidores, vuelva a introducir el secreto compartido del servidor correspondiente en el cuadro con el nombre "Secreto compartido".La entrada secreta compartida para el punto de acceso en el servidor RADIUS debe contener la misma contraseña secreta compartida que las mencionadas anteriormente.

4. Elimine cualquier grupo de usuarios del servidor RADIUS. A veces pueden producirse conflictos entre grupos de usuarios definidos por el servidor RADIUS y grupos de usuarios en el dominio subyacente. Verifique los registros del servidor RADIUS para los intentos fallidos y las razones por las que esos intentos 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.

Debugging Authentications proporciona una cantidad significativa de detalles sobre cómo recopilar e interpretar el resultado de las depuraciones relacionadas con EAP.

**Nota:** Antes de ejecutar **comandos debug**, consulte la Información Importante sobre Comandos Debug.

- **debug dot11 aaa authenticator state-machine**: muestra las principales divisiones (o estados) de la negociación entre el cliente y el servidor de autenticación. A continuación se muestra un resultado de una autenticación **exitosa**:

```
*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 del software Cisco IOS anteriores a 12.2(15)JA, la sintaxis de este comando **debug** es **debug dot11 aaa dot1x state-machine**.

- **debug dot11 aaa authenticator process**: muestra las entradas de diálogo individuales de la negociación entre el cliente y el servidor de autenticación.**Nota:** En las versiones del software Cisco IOS anteriores a 12.2(15)JA, la sintaxis de este comando de depuración es **debug dot11 aaa dot1x process**.
- **debug radius authentication**—Muestra las negociaciones RADIUS entre el servidor y el cliente, ambos con puente por el AP. Este es un resultado 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
```

- **debug aaa authentication**: muestra las negociaciones AAA para la autenticación entre el dispositivo cliente y el servidor de autenticación.

# Información Relacionada

- Autenticaciones de depuración
- Configuración de los tipos de autenticación
- Autenticación LEAP en un Servidor RADIUS Local
- Configuración de los servidores RADIUS y TACACS+
- Configuración de Cisco Secure ACS para Windows v3.2 con autenticación de máquina PEAP-MS-CHAPv2
- Cisco Secure ACS para Windows v3.2 con autenticación de máquina EAP-TLS
- Configuración de PEAP/EAP en Microsoft IAS
- Resolución de problemas de Microsoft IAS como servidor RADIUS
- Cliente de autenticación 802.1X de Microsoft
- Soporte Técnico y Documentación - Cisco Systems