EAP-FAST con el servidor RADIUS interno en el ejemplo autónomo de la Configuración de punto de acceso

Contenido

Introducción

Este documento describe cómo configurar el Punto de acceso autónomo para actuar como servidor de RADIUS que realice la autenticación de Protocol Flexible de autenticación ampliable de Cisco vía el protocolo seguro (EAP-FAST) para el authenticatication del cliente con la última versión del ® del Cisco IOS (15.2JB), que se ha puesto al día para tener la mirada y la sensación de una interfaz GUI.

Utilizan generalmente a un servidor RADIUS externo para autenticar a los usuarios. En algunos casos, esto no es una solución factible. En estas situaciones, un punto de acceso puede actuar como servidor de RADIUS. En esta situación, autentican a los usuarios contra la base de datos local configurada en el Punto de acceso. Esto se llama una característica local del servidor de RADIUS. Usted puede también hacer otros Puntos de acceso en el uso de la red que el servidor de RADIUS local ofrece en un AP.

Prerrequisitos

Requisitos

Cisco recomienda que usted tiene conocimiento de estos temas antes de que usted intente esta

configuración:

- Cisco IOS GUI o CLI
- Conceptos detrás del Protocolo de Autenticación Extensible (EAP)
- Configuración del Service Set Identifier (SSID)
- RADIUS

Componentes Utilizados

La información en este documento se basa en 3600 AP que funciona con el Cisco IOS Release15.2JB y actúa como servidor RADIUS interno.

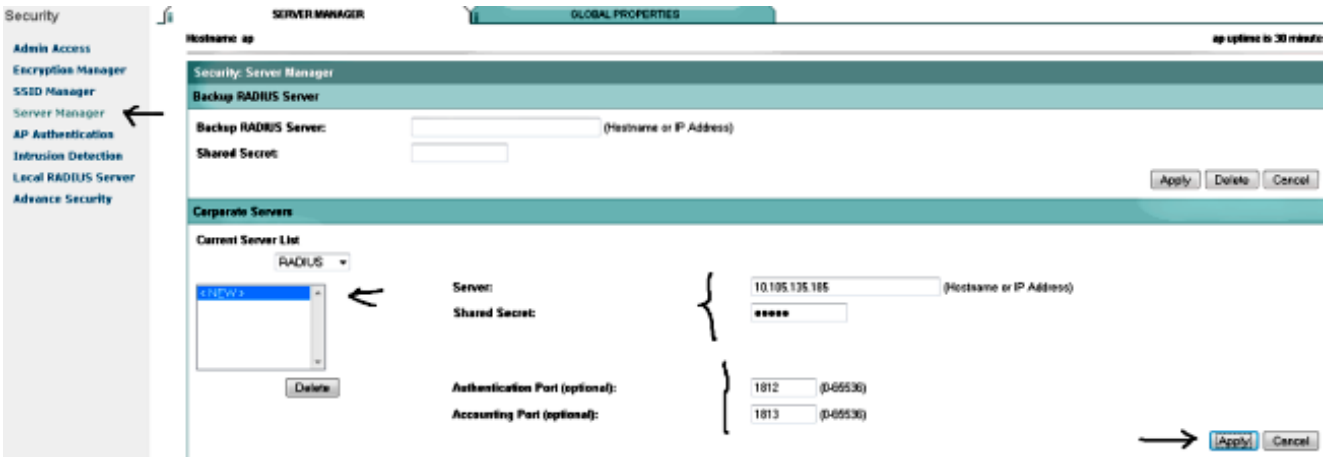
La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Configurar

Configuración con el GUI

1. Para configurar el AP como el servidor de RADIUS local, navegue al **> Security (Seguridad) > al administrador de servidor AP GUI**, y ingrese estos detalles:
   Nombre de host o dirección IPsecreto compartidoPuerto de autenticaciónPuerto de contabilidad
   Nota: Para la autenticación y los puertos de contabilidad, este ejemplo utiliza 1812 y 1813, respectivamente. Sin embargo, 1645 y 1646 pueden también ser utilizados.

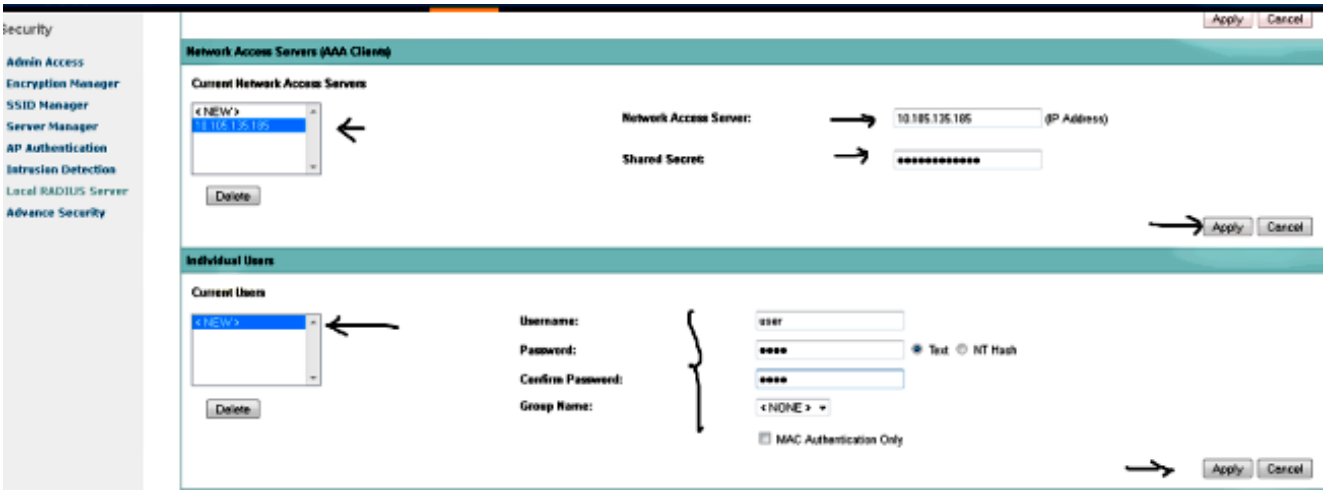
   Haga clic en Apply (Aplicar).



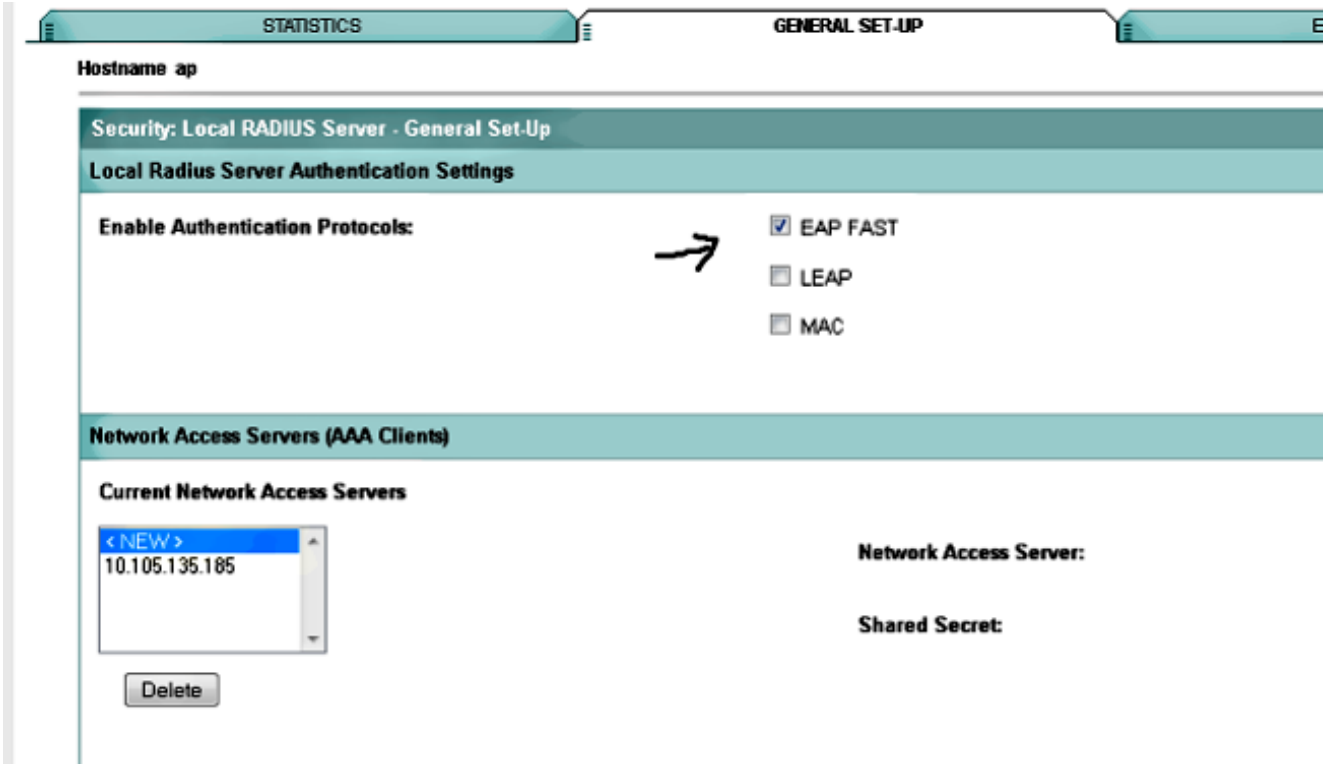
2. Navegue a la **configuración de servidor de RADIUS local** en el AP, haga clic la lengueta **general de la configuración**, y ingrese estos detalles:
   Servidor de acceso a la red (NAS) con la dirección IP del AP (IP del (BVI) internacional del Interfaz Virtual de Bridge-Group)**secreto compartido**

Haga clic en Apply (Aplicar).

Cree a un **usuario individual** con un **nombre de usuario y contraseña**. Si se requiere un **nombre del grupo**, después configurelo (este ejemplo no utiliza un **nombre del grupo**).

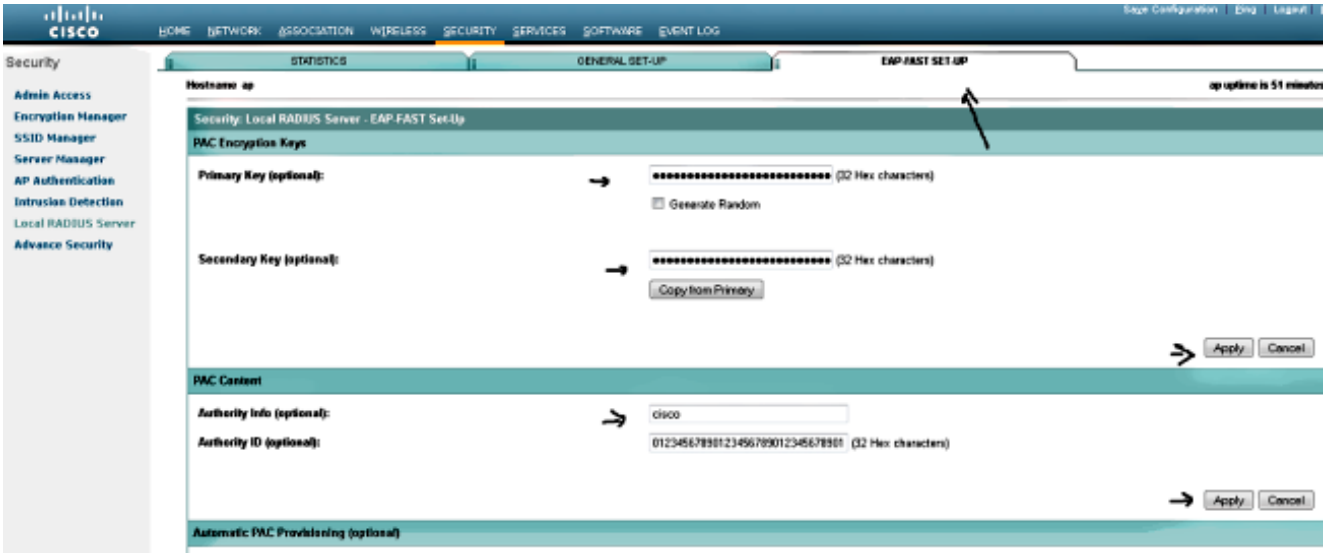


3. Desmarque las casillas de verificación del **SALTO** y **MAC**.

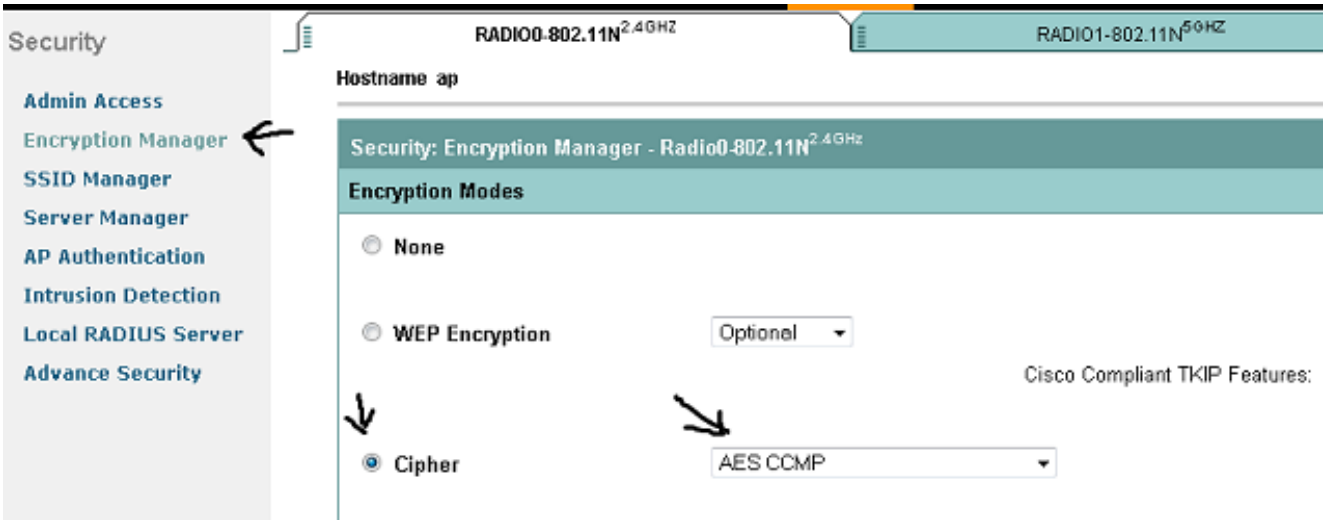


4. Haga clic la lengueta de la **configuración del EAP-FAST**, y ingrese los detalles por las **claves de encripción PAC** y el **contenido PAC**.

   Nota: Este ejemplo utiliza cero a nueve cuatro veces puesto que tiene 32 caracteres hexadecimales.

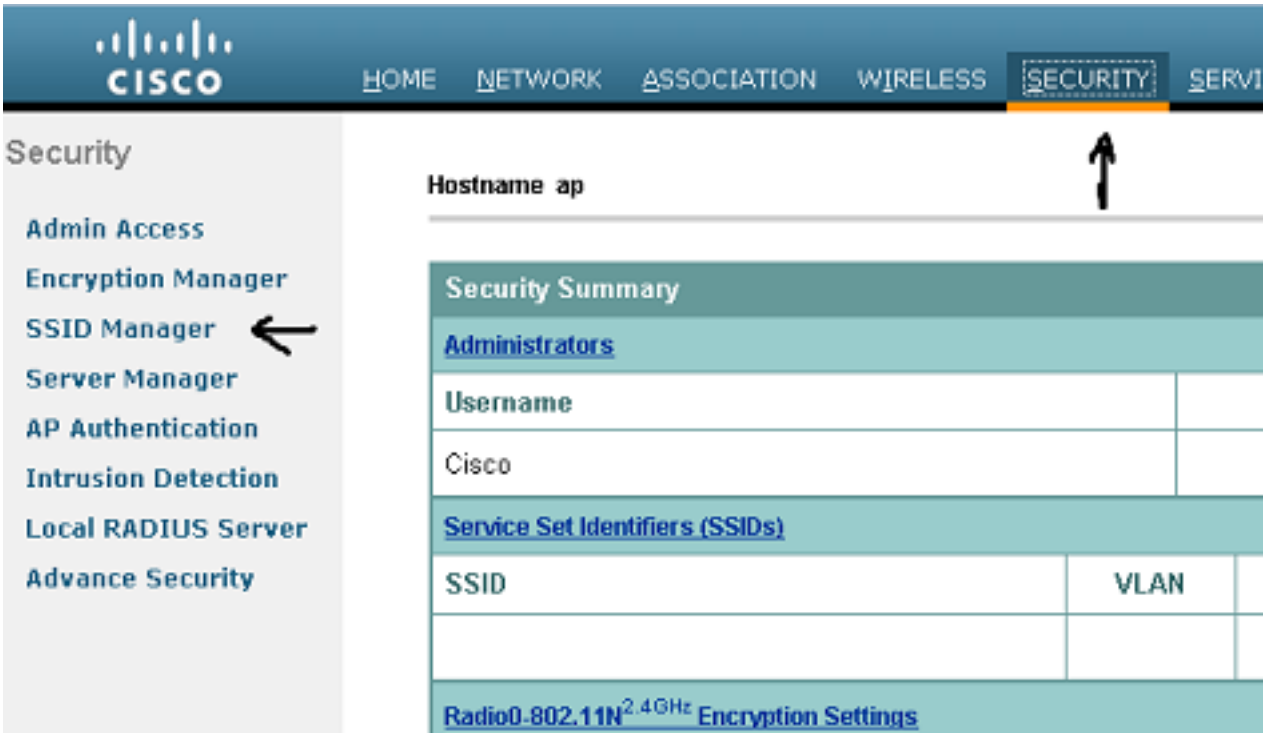


5. Navegue al **administrador del cifrado**, **cifra de la** configuración con el **CCMP AES** como el cifrado, y el tecleo **aplica todas las radios** o las **radios requeridas**.

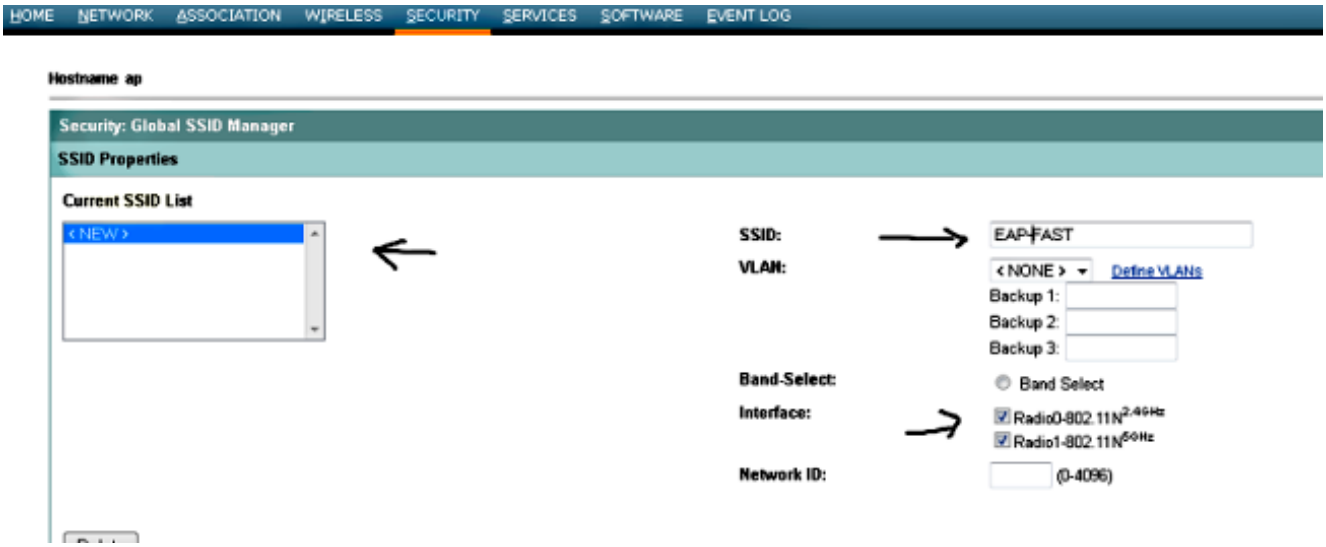


Configure el SSID

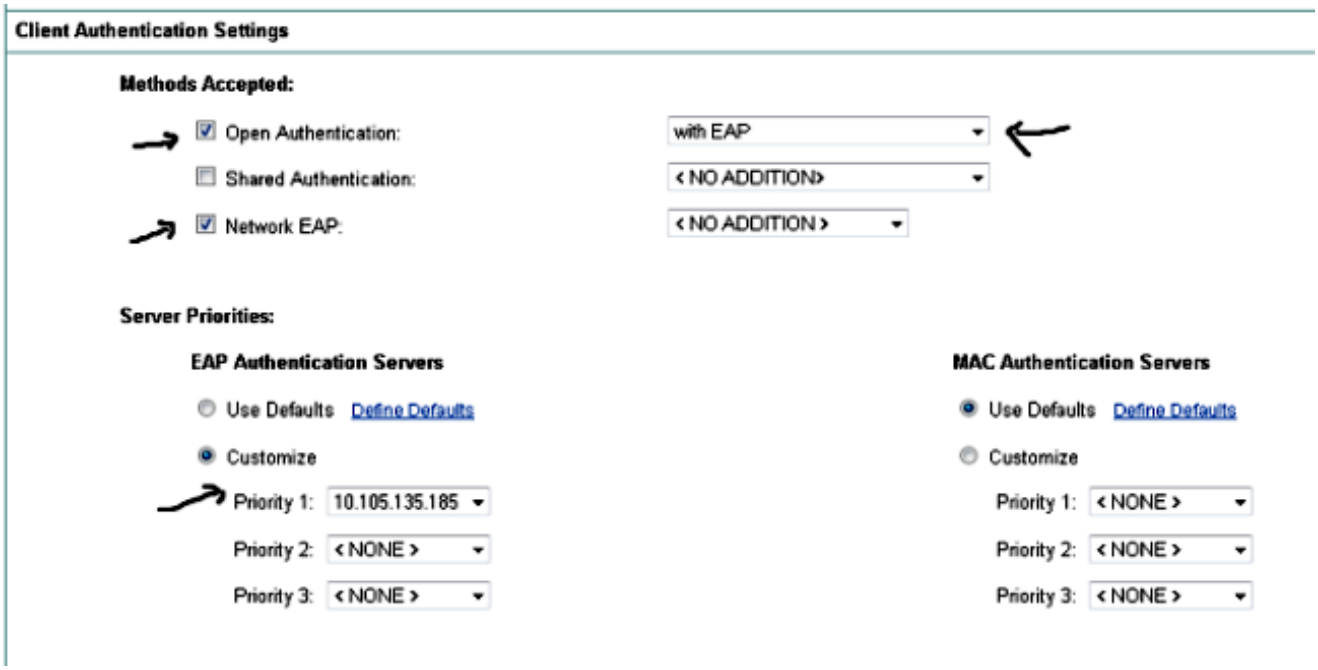
1. Navegue a la **Seguridad > al administrador SSID**, y el tecleo **crea nuevo**.



2. Ingrese los detalles, y el tecleo **se aplica**.

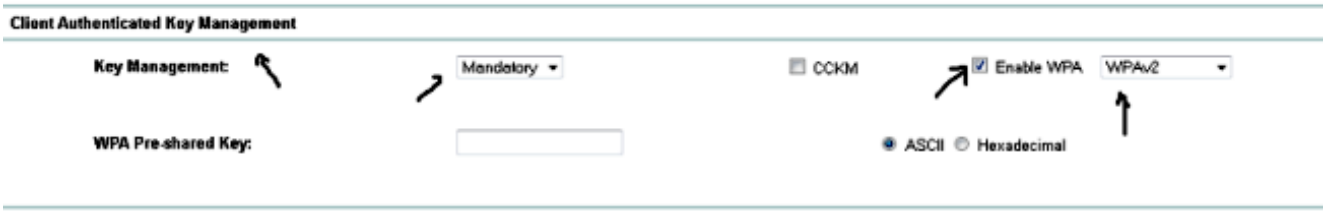


3. En la **autenticación de cliente las** configuraciones defienden, marcan el **casilla "Abrir autenticación"**, y lo seleccionan **con el EAP del** menú desplegable. Marque **Casilla de verificación EAP de la red.**, y seleccione al **servidor de RADIUS del** menú desplegable. Ésta debe ser la dirección IP AP que usted configuró como AAA en el administrador de servidor y la página del servidor RADIUS local.

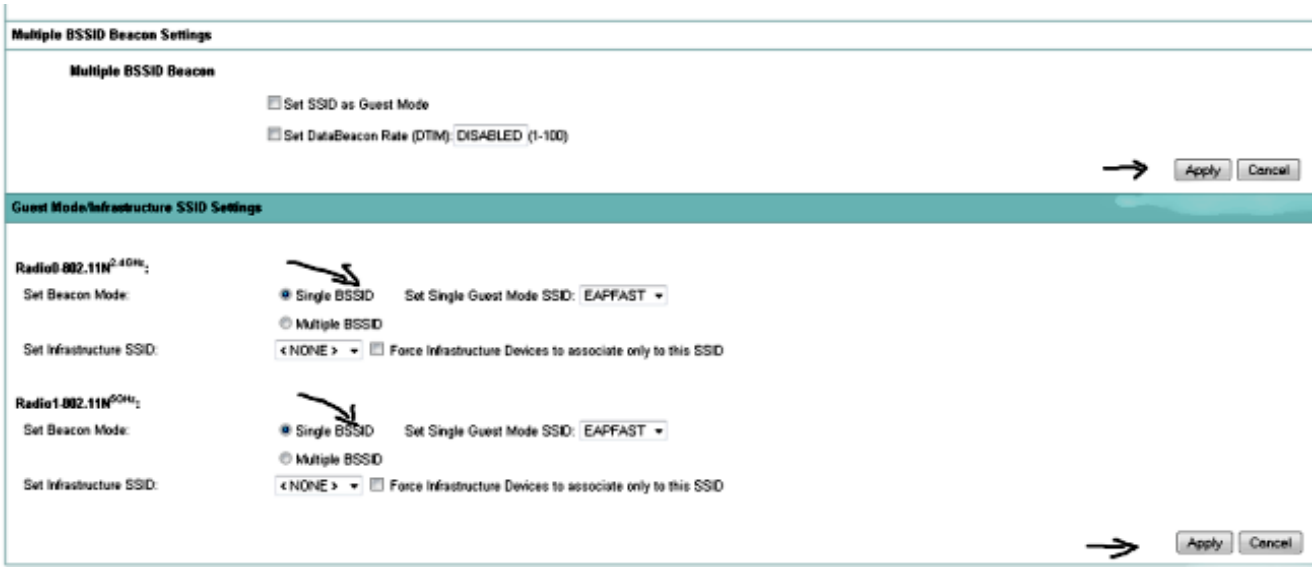


La Tecnología inalámbrica de la configuración protegió el acceso versión 2 (WPAv2) como obligatorio

1. En el **cliente la** pantalla **autenticada de la administración de claves**, selecciona **obligatorio del** menú desplegable de la **administración de claves**. Marque la **casilla de verificación WPA del permiso**, y seleccione **WPAv2 del** menú desplegable.



2. Haga clic en **Aplicar** en la parte inferior de la página. Para transmitir el SSID, hacer clic los **solos** botones de radio **SSID**, seleccionar el **SSID del** menú desplegable, y el tecleo **se aplica**.



3. Navegue a las **redes**, y habilite las radios para **2.4 gigahertz** y **5 gigahertz**. Asegúrese de que las radios sean en servicio.

Comando CLI para las configuraciones

```
show run
Building configuration...

Current configuration : 3204 bytes
!
! Last configuration change at 01:11:36 UTC Mon Mar 1 1993
version 15.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname ap
!
!
logging rate-limit console 9
enable secret 5 $1$06l4$E2pi.VeGTKUxxiwPScUEp.
!
aaa new-model
!
!
aaa group server radius rad_eap
 server 10.105.135.185 auth-port 1812 acct-port 1813
!
aaa group server radius rad_mac
!
aaa group server radius rad_acct
!
aaa group server radius rad_admin
!
aaa group server tacacs+ tac_admin
!
aaa group server radius rad_pmip
!
aaa group server radius dummy
!
aaa group server radius rad_eap1
 server 10.105.135.185 auth-port 1812 acct-port 1813
```

```
!
aaa authentication login eap_methods group rad_eap
aaa authentication login mac_methods local
aaa authentication login eap_methods1 group rad_eap1
aaa authorization exec default local
aaa accounting network acct_methods start-stop group rad_acct
!
!
!
!
!
aaa session-id common
no ip routing
no ip cef
!
!
!
dot11 syslog
!
dot11 ssid EAPFAST
  authentication open eap eap_methods1
  authentication network-eap eap_methods1
  authentication key-management wpa version 2
  guest-mode
!
!
crypto pki token default removal timeout 0
!
!
username Cisco password 7 01300F175804
!
!
!
class-map match-all _class_voice0
 match ip dscp ef
 class-map match-all _class_voice1
 match ip dscp default
!
!
policy-map voice
 class _class_voice0
 set cos 6
 class _class_voice1
 set cos 6
!
bridge irb
!
!
!
interface Dot11Radio0
 no ip address
 no ip route-cache
 !
 encryption mode ciphers aes-ccm
 !
 ssid EAPFAST
 !
 antenna gain 0
 stbc
 power local 14
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 spanning-disabled
```

```
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
!
interface Dot11Radio1
 no ip address
 no ip route-cache
 !
 encryption mode ciphers aes-ccm
 !
 ssid EAPFAST
 !
 antenna gain 0
 dfs band 3 block
 stbc
 channel dfs
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 spanning-disabled
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
!
interface GigabitEthernet0
 no ip address
 no ip route-cache
 duplex auto
 speed auto
 bridge-group 1
 bridge-group 1 spanning-disabled
 no bridge-group 1 source-learning
!
interface BVI1
 ip address 10.105.135.185 255.255.255.128
 no ip route-cache
!
ip forward-protocol nd
ip http server
no ip http secure-server
ip http help-path http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag
ip radius source-interface BVI1
!
radius-server local
 eapfast authority id 01234567890123456789012345678901
 eapfast authority info cisco
 eapfast server-key primary 7 E1F54D861DC7150A7B949E5B4E630D8E5B
 eapfast server-key secondary 7 E7281DB670D36C052F60D36337436ABA13
 nas 10.105.135.185 key 7 01100F175804
 user user nthash 7 075A76681B514A2436465D28517D7A71786114033753342156777C79030
D2D5448
!
radius-server attribute 32 include-in-access-req format %h
radius-server host 10.105.135.185 auth-port 1812 acct-port 1813 key 7 045802150C2E
radius-server vsa send accounting
!
bridge 1 route ip
!
!
!
line con 0
line vty 0 4
transport input all
!
```

```
end

ap#
```

Verificación

Si usted conecta con el cliente, después éste es el registro que visualiza en el AP después de una autenticación satisfactoria:

```
show run
Building configuration...

Current configuration : 3204 bytes
!
! Last configuration change at 01:11:36 UTC Mon Mar 1 1993
version 15.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname ap
!
!
logging rate-limit console 9
enable secret 5 $1$06l4$E2pi.VeGTKUxxiwPScUEp.
!
aaa new-model
!
!
aaa group server radius rad_eap
 server 10.105.135.185 auth-port 1812 acct-port 1813
!
aaa group server radius rad_mac
!
aaa group server radius rad_acct
!
aaa group server radius rad_admin
!
aaa group server tacacs+ tac_admin
!
aaa group server radius rad_pmip
!
aaa group server radius dummy
!
aaa group server radius rad_eap1
 server 10.105.135.185 auth-port 1812 acct-port 1813
!
aaa authentication login eap_methods group rad_eap
aaa authentication login mac_methods local
aaa authentication login eap_methods1 group rad_eap1
aaa authorization exec default local
aaa accounting network acct_methods start-stop group rad_acct
!
!
!
!
!
aaa session-id common
no ip routing
no ip cef
```

```
!
!
!
dot11 syslog
!
dot11 ssid EAPFAST
  authentication open eap eap_methods1
  authentication network-eap eap_methods1
  authentication key-management wpa version 2
  guest-mode
!
!
crypto pki token default removal timeout 0
!
!
username Cisco password 7 01300F175804
!
!
!
class-map match-all _class_voice0
 match ip dscp ef
 class-map match-all _class_voice1
 match ip dscp default
!
!
policy-map voice
 class _class_voice0
 set cos 6
 class _class_voice1
 set cos 6
!
bridge irb
!
!
!
interface Dot11Radio0
 no ip address
 no ip route-cache
 !
 encryption mode ciphers aes-ccm
 !
 ssid EAPFAST
 !
 antenna gain 0
 stbc
 power local 14
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 spanning-disabled
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
!
interface Dot11Radio1
 no ip address
 no ip route-cache
 !
 encryption mode ciphers aes-ccm
 !
 ssid EAPFAST
 !
 antenna gain 0
 dfs band 3 block
```

```
 stbc
 channel dfs
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 spanning-disabled
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
!
interface GigabitEthernet0
 no ip address
 no ip route-cache
 duplex auto
 speed auto
 bridge-group 1
 bridge-group 1 spanning-disabled
 no bridge-group 1 source-learning
!
interface BVI1
 ip address 10.105.135.185 255.255.255.128
 no ip route-cache
!
ip forward-protocol nd
ip http server
no ip http secure-server
ip http help-path http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag
ip radius source-interface BVI1
!
radius-server local
 eapfast authority id 01234567890123456789012345678901
 eapfast authority info cisco
 eapfast server-key primary 7 E1F54D861DC7150A7B949E5B4E630D8E5B
 eapfast server-key secondary 7 E7281DB670D36C052F60D36337436ABA13
 nas 10.105.135.185 key 7 01100F175804
 user user nthash 7 075A76681B514A2436465D28517D7A71786114033753342156777C79030
D2D5448
!
radius-server attribute 32 include-in-access-req format %h
radius-server host 10.105.135.185 auth-port 1812 acct-port 1813 key 7 045802150C2E
radius-server vsa send accounting
!
bridge 1 route ip
!
!
!
line con 0
line vty 0 4
transport input all
!
end

ap#
```

Troubleshooting

Complete estos pasos para resolver problemas esta configuración.

1. Para eliminar la posibilidad que los problemas del Radiofrecuencia (RF) previenen la autenticación satisfactoria, fije el método en el SSID **para abrirse** para inhabilitar temporalmente la autenticación.

2. Del GUI en la página del **administrador SSID**, desmarque **Casilla de verificación EAP de la red.**, y marque **abierto**.

3. Del CLI, utilice los comandos authentication open y **ningunos eap_methods de la autenticación red-EAP**. Si el cliente se asocia con éxito, el RF no contribuye al problema de asociación.

4. Verifique que todas las contraseñas secretas compartidas estén sincronizadas. Estas líneas deben contener la misma contraseña del secreto compartido:
clave del acct-puerto x del auténtico-puerto x del host de servidor RADIUS x.x.x.x <shared_secret>clave NAS x.x.x.x <shared_secret>
5. Quite cualquier grupo de usuarios y sus configuraciones asociadas. Los conflictos ocurren a veces entre los grupos de usuarios definidos por el AP y los grupos de usuarios en el dominio.

Comandos de Debug

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

Aquí está una lista de comandos debug útiles.

- **authenticator todo aaa del dot11 del debug** - Este debug muestra a diversas negociaciones que va un cliente a través mientras que el cliente se asocia y autentica con el 802.1x o el proceso EAP desde la perspectiva del authenticator (AP). Este debug fue introducido en el Cisco IOS Software Release 12.2(15)JA. Este **dot1x todo aaa del dot11 del debug de los** obsoletes del comando en esto y posterior versiones.

```
 *Mar  1 00:26:03.097: dot11_auth_add_client_entry:
Create new client 0040.96af.3e93 for application 0x1
*Mar 1 00:26:03.097: dot11_auth_initialize_client:
0040.96af.3e93 is added to the client list for application 0x1
-----------------------------------------------
Lines Omitted for simplicity -----------------
*Mar 1 00:26:03.098: dot11_auth_dot1x_start:
in the dot11_auth_dot1x_start


*Mar 1 00:26:03.132: dot11_auth_dot1x_run_rfsm:
Executing Action(CLIENT_WAIT,EAP_START) for 0040.96af.3e93
*Mar 1 00:26:03.132: dot11_auth_dot1x_send_id_req_to_client:
Sending identity request to 0040.96af.3e93(client)

*Mar 1 00:26:03.133: *Mar 1 00:26:03.099:
dot11_auth_dot1x_send_id_req_to_client:
Client 0040.96af.3e93 timer started for 30 seconds
*Mar 1 00:26:03.132: dot11_auth_parse_client_pak:
Received EAPOL packet from 0040.96af.3e93
-----------------------------------------------
Lines Omitted----------------------------------
*Mar 1 00:26:03.138: EAP code: 0x2 id: 0x1 length:
0x000A type: 0x1
```

01805BF0: 0100000A 0201000A 01757365 7231
.........**user1*(User Name of the client)***

*Mar1 00:26:03.146: dot11_auth_dot1x_run_rfsm:
Executing Action(CLIENT_WAIT,CLIENT_REPLY) for 0040.96af.3e93
*Mar1 00:26:03.147: dot11_auth_dot1x_send_response_to_server:
Sending client 0040.96af.3e93 data toserver
*Mar1 00:26:03.147: dot11_auth_dot1x_send_response_to_server:
Started timer server_timeout 60 seconds

Lines Omitted---
*Mar1 00:26:03.150: dot11_auth_dot1x_parse_aaa_resp:
Received server response:GET_CHALLENGE_RESPONSE
*Mar1 00:26:03.150: dot11_auth_dot1x_parse_aaa_resp:
found session timeout 10 sec

*Mar 1 00:26:03.150: dot11_auth_dot1x_run_rfsm:
Executing Action(SERVER_WAIT,SERVER_REPLY) for 0040.96af.3e93
*Mar 1 00:26:03.150: dot11_auth_dot1x_send_response_to_client:
Forwarding server message to client 0040.96af.3e93

Lines Omitted---
*Mar 1 00:26:03.151: dot11_auth_send_msg:
Sending EAPOL to requestor
*Mar 1 00:26:03.151: dot11_auth_dot1x_send_response_to_client:
Started timer client_timeout 10 seconds
*Mar 1 00:26:03.166: dot11_auth_parse_client_pak:
Received EAPOL packet*(User Credentials)* from 0040.96af.3e93
*Mar 1 00:26:03.166: EAP code: 0x2 id: 0x11 length: 0x0025
type: 0x1101805F90: 01000025 02110025...%...%01805FA0:
11010018 7B75E719 C5F3575E EFF64B27 **....{ug.EsW^ovK'**

Executing Action(CLIENT_WAIT,CLIENT_REPLY) for 0040.96af.3e93
*Mar 1 00:26:03.186: dot11_auth_dot1x_send_response_to_server:
**Sending client 0040.96af.3e93 data
(User Credentials) to server**
*Mar 1 00:26:03.186: dot11_auth_dot1x_send_response_to_server:
Started timer server_timeout 60 seconds

Lines Omitted---
*Mar 1 00:26:03.196: dot11_auth_dot1x_parse_aaa_resp:
Received server response: PASS

*Mar 1 00:26:03.197: dot11_auth_dot1x_run_rfsm:
Executing Action(SERVER_WAIT,SERVER_PASS) for 0040.96af.3e93
*Mar 1 00:26:03.197: dot11_auth_dot1x_send_response_to_client:
Forwarding server message*(Pass Message)* to client

Lines Omitted---
*Mar 1 00:26:03.198: dot11_auth_send_msg:
Sending EAPOL to requestor
*Mar 1 00:26:03.199: dot11_auth_dot1x_send_response_to_client:
Started timer client_timeout 30 second
*Mar 1 00:26:03.199: dot11_auth_send_msg:
client authenticated 0040.96af.3e93,
node_type 64 for application 0x1
*Mar 1 00:26:03.199: dot11_auth_delete_client_entry:
0040.96af.3e93 is deleted for application 0x1
*Mar 1 00:26:03.200: %DOT11-6-ASSOC:
Interface Dot11Radio0, Station *Station Name*

```
0040.96af.3e93 Associated KEY_MGMT[NONE]
```

- **autenticación de RADIUS del debug** - Este debug muestra las negociaciones RADIUS entre el servidor y el cliente, que, en este caso, son el AP.

- **cliente del servidor local del radio del debug** - Este debug muestra la autenticación del cliente desde la perspectiva del servidor de RADIUS.

```
 *Mar 1 00:30:00.742: RADIUS(0000001A):
SendAccess-Request(Client's User Name)
to 10.77.244.194:1812(Local Radius Server)


id 1645/65, len 128
*Mar 1 00:30:00.742: RADIUS:
User-Name [1] 7 "user1"
*Mar 1 00:30:00.742: RADIUS:
Called-Station-Id [30] 16 "0019.a956.55c0"
*Mar 1 00:30:00.743: RADIUS:
Calling-Station-Id [31] 16 "0040.96af.3e93" (Client)


*Mar 1 00:30:00.743: RADIUS:
Service-Type [6] 6 Login [1]
*Mar 1 00:30:00.743: RADIUS:
Message-Authenticato[80]
*Mar 1 00:30:00.743: RADIUS:
23 2E F4 42 A4 A3 72 4B 28 44 6E 7A 58 CA 8F 7B [#.?B??rK(DnzX??{]
*Mar 1 00:30:00.743: RADIUS:
EAP-Message [79] 12
*Mar 1 00:30:00.743:
RADIUS:   02 02 00 0A 01 75 73 65 72 31
[?????user1]
*Mar 1 00:30:00.744: RADIUS:
NAS-Port-Type [61] 6 802.11 wireless
-------------------------------
Lines Omitted For Simplicity--------------------
*Mar 1 00:30:00.744: RADIUS:
NAS-IP-Address [4] 6 10.77.244.194(Access Point IP)

*Mar 1 00:30:00.744: RADIUS: Nas-Identifier [32] 4 "ap"

---------------------------------
Lines Omitted---------------------------------
*Mar 1 00:30:00.745: RADIUS:
Received from id 1645/65 10.77.244.194:1812, Access-Challenge, len 117
*Mar 1 00:30:00.746: RADIUS:
75 73 65 72 31 [user1]
*Mar 1 00:30:00.746: RADIUS:
Session-Timeout [27] 6 10
*Mar 1 00:30:00.747: RADIUS: State [24] 50
*Mar 1 00:30:00.747: RADIUS:
BF 2A A0 7C 82 65 76 AA 00 00 00 00 00 00 00 00
[?*?|?ev?????????]
-------------------------------------
Lines Omitted for simplicity -------------
*Mar 1 00:30:00.756:
RADIUS/ENCODE(0000001A):Orig. component type = DOT11
*Mar 1 00:30:00.756: RADIUS: AAA Unsupported Attr: ssid [264] 5
*Mar 1 00:30:00.756: RADIUS: 63 69 73 [cis]
*Mar 1 00:30:00.756: RADIUS: AAA Unsupported Attr: interface [157] 3
```

```
*Mar 1 00:30:00.756: RADIUS: 32 [2]
*Mar 1 00:30:00.757: RADIUS(0000001A): Config NAS IP: 10.77.244.194
*Mar 1 00:30:00.757: RADIUS/ENCODE(0000001A): acct_session_id: 26
*Mar 1 00:30:00.757: RADIUS(0000001A): Config NAS IP: 10.77.244.194


*Mar 1 00:30:00.779: RADIUS(0000001A):
Send Access-Request to 10.77.244.194:1812 id 1645/67, len 189
*Mar 1 00:30:00.779: RADIUS:
authenticator B0 15 3C C1 BC F6 31 85 - 66 5D 41 F9 2E B4 48 7F
*Mar 1 00:30:00.779: RADIUS: User-Name [1] 7 "user1"
*Mar 1 00:30:00.780: RADIUS: Framed-MTU [12] 6 1400
*Mar 1 00:30:00.780: RADIUS: Called-Station-Id [30] 16"0019.a956.55c0"
*Mar 1 00:30:00.780: RADIUS: Calling-Station-Id [31] 16"0040.96af.3e93"
*Mar 1 00:30:00.758: RADIUS:
92 D4 24 49 04 C2 D2 0A C3 CE E9 00 6B F1 B2 AF [??$I????????k???]
*Mar 1 00:30:00.759: RADIUS: EAP-Message [79] 39
*Mar 1 00:30:00.759: RADIUS:
02 17 00 25 11 01 00 18 05 98 8B BE 09 E9 45 E2  [??????????????E?]
*Mar 1 00:30:00.759: RADIUS:
73 5D 33 1D F0 2F DB 09 50 AF 38 9F F9 3B BD D4 [s]3??/??P?8??;??]
*Mar 1 00:30:00.759: RADIUS:
75 73 65 72 31 [user1]
----------------------------------------
Lines Omitted----------------------------
*Mar 1 00:30:00.781: RADIUS: State [24] 50 RADIUS:
NAS-IP-Address [4] 6 10.77.244.194
*Mar 1 00:30:00.783: RADIUS: Nas-Identifier [32] 4 "ap"

*Mar 1 00:30:00.822: RADIUS:
Received from id 1645/67 10.77.244.194:1812, Access-Accept, len 214
*Mar 1 00:30:00.822:
RADIUS: authenticator 10 0C B6 EE 7A 96 3A 46 - 36 49 FC D3 7A F4 42 2A
----------------------------------------
Lines Omitted----------------------------
*Mar 1 00:30:00.823: RADIUS: 75 73 65 72 31 [user1]
*Mar 1 00:30:00.823: RADIUS: Vendor, Cisco [26] 59
*Mar 1 00:30:00.823: RADIUS:
Cisco AVpair [1] 53 "EAP-FAST:session-key=?+*ve=];q,oi[d6|-z."
*Mar 1 00:30:00.823:
RADIUS: User-Name [1] 28 "user1 *Mar 1 00:30:00.824: RADIUS:
Message-Authenticato[80] 18
*Mar 1 00:30:00.824: RADIUS:
06 2D BA 93 10 C0 91 F8 B4 B8 A4 00 82 0E 11 36
[?-?????????????6]
*Mar 1 00:30:00.826: RADIUS/DECODE: EAP-Message fragments,
37, total 37 bytes
*Mar 1 00:30:00.826: found leap session key
*Mar 1 00:30:00.830: %DOT11-6-ASSOC:
Interface Dot11Radio0, Station Station Name
Associated KEY_MGMT[NONE]
```

- paquetes del servidor local del radio del debug - Este debug muestra todos los procesos por los cuales sean ejecutados y desde la perspectiva del servidor de RADIUS.