EAP-FAST com o raio de servidor interno no exemplo autônomo da configuração do ponto de acesso

Índice

Introdução

Este documento descreve como configurar o Access point autônomo para atuar como um servidor Radius que execute a autenticação Protocolo flexível da autenticação extensível de Cisco através do protocolo seguro (EAP-FAST) para o authenticatication do cliente com a liberação a mais atrasada do ® do Cisco IOS (15.2JB), que foi atualizada para ter o olhar e a sensação de uma interface GUI.

Um servidor de raio externo é usado geralmente a fim autenticar usuários. Em alguns casos, esta não é uma solução possível. Nestas situações, um Access Point (AP) pode atuar como um servidor Radius. Nesta situação, os usuários são autenticados contra o base de dados local configurado no Access point. Isto é chamado uma característica local do servidor Radius. Você pode igualmente fazer outros Access point no uso da rede que o servidor Radius local caracteriza em um AP.

Pré-requisitos

Requisitos

Cisco recomenda que você tem o conhecimento destes assuntos antes que você tente esta

configuração:

- Cisco IOS GUI ou CLI
- Conceitos atrás do Extensible Authentication Protocol (EAP)
- Configuração do Service Set Identifier (SSID)
- RADIUS

Componentes Utilizados

A informação neste documento é baseada em uns 3600 AP que executem o Cisco IOS Release15.2JB e atuem como um raio de servidor interno.

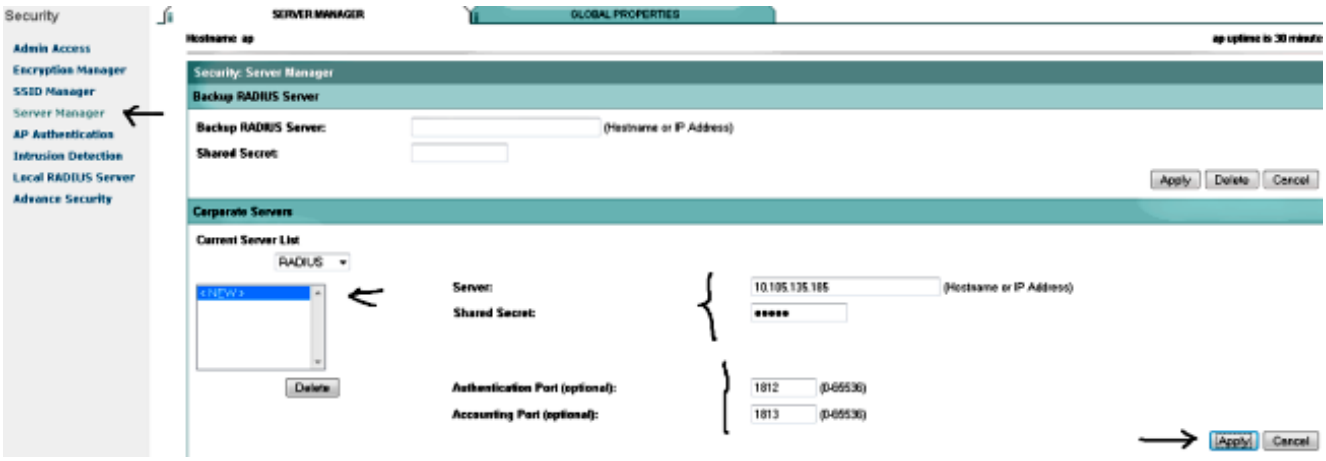
As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Configurar

Configuração com GUI

1. A fim configurar o AP como o servidor Radius local, navegue ao **> segurança > ao gerenciador do servidor AP GUI**, e incorpore estes detalhes:
   Hostname ou endereço IP de Um ou Mais Servidores Cisco ICM NTshared secretPorta de autenticaçãoPorta de relatório
   Note: Para a autenticação e as portas de relatório, este exemplo usa 1812 e 1813, respectivamente. Contudo, 1645 e 1646 podem igualmente ser usados.

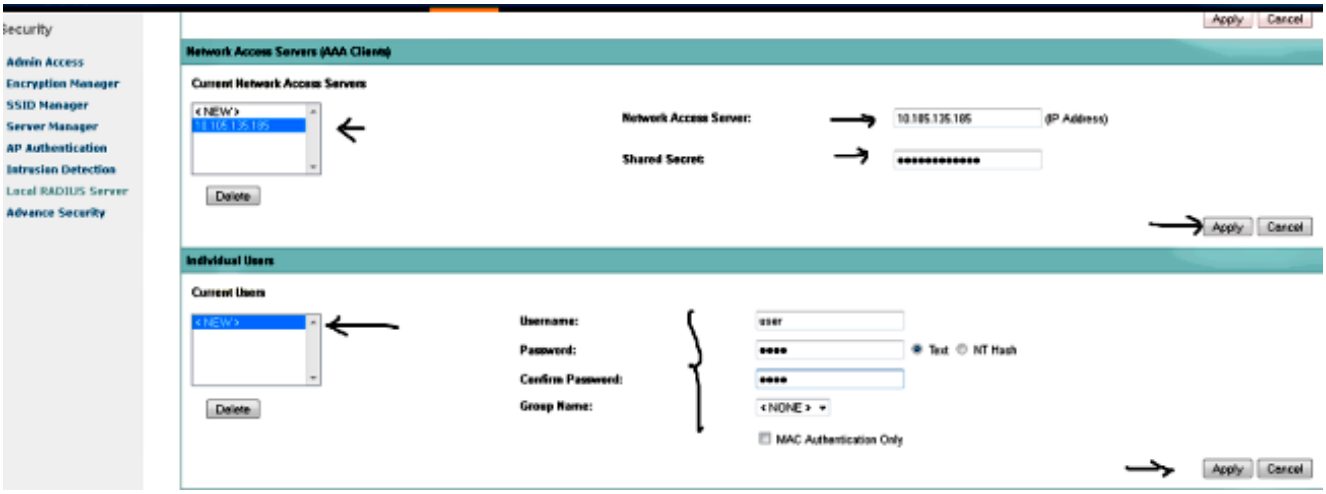
   Clique em Apply.



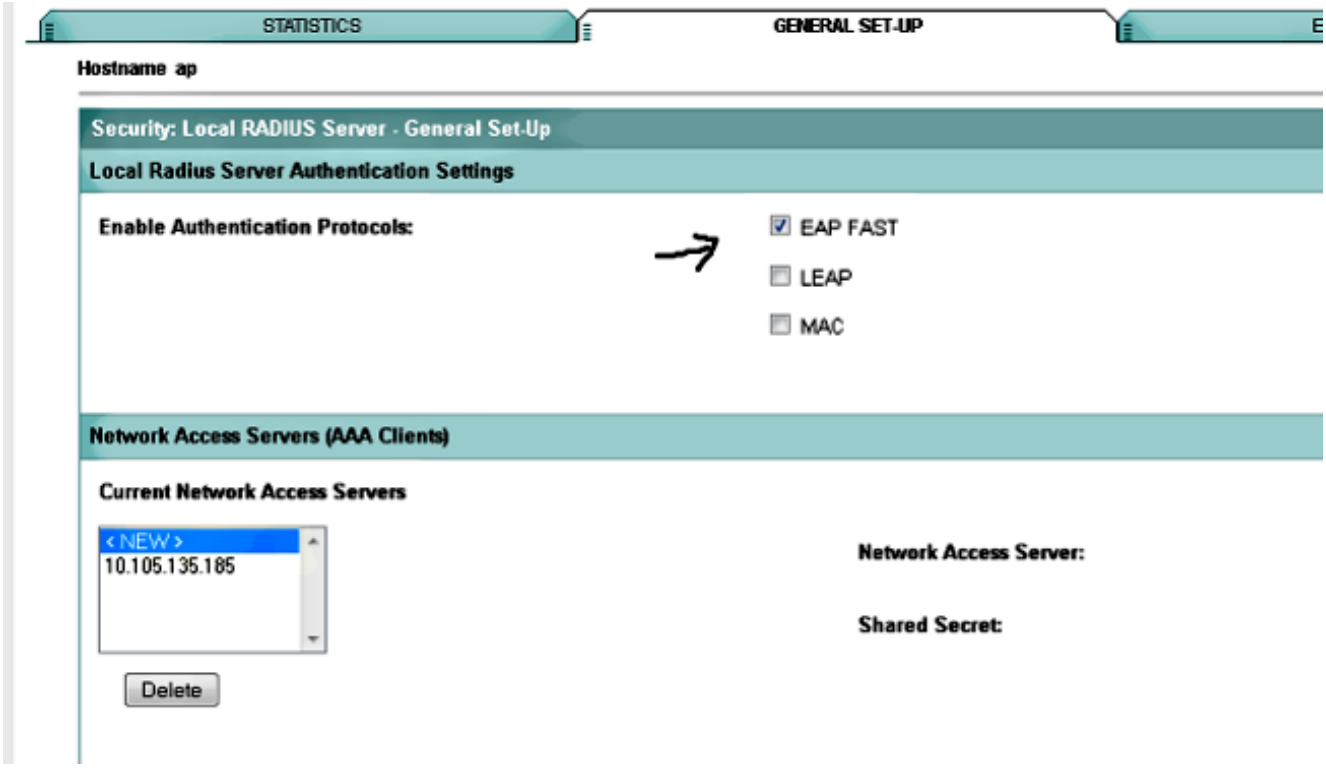
2. Navegue à **configuração de servidor RADIUS local no** AP, clique a aba **geral da instalação**, e incorpore estes detalhes:
   Servidor do acesso de rede (NAS) com o endereço IP de Um ou Mais Servidores Cisco ICM NT do AP (IP int do Bridge Group Virtual Interface (BVI))**shared secret**

Clique em Apply.

Crie um **usuário individual** com um **nome de usuário e senha**. Se um **nome do grupo** é exigido, a seguir configurar-lo (este exemplo não usa um **nome do grupo**).

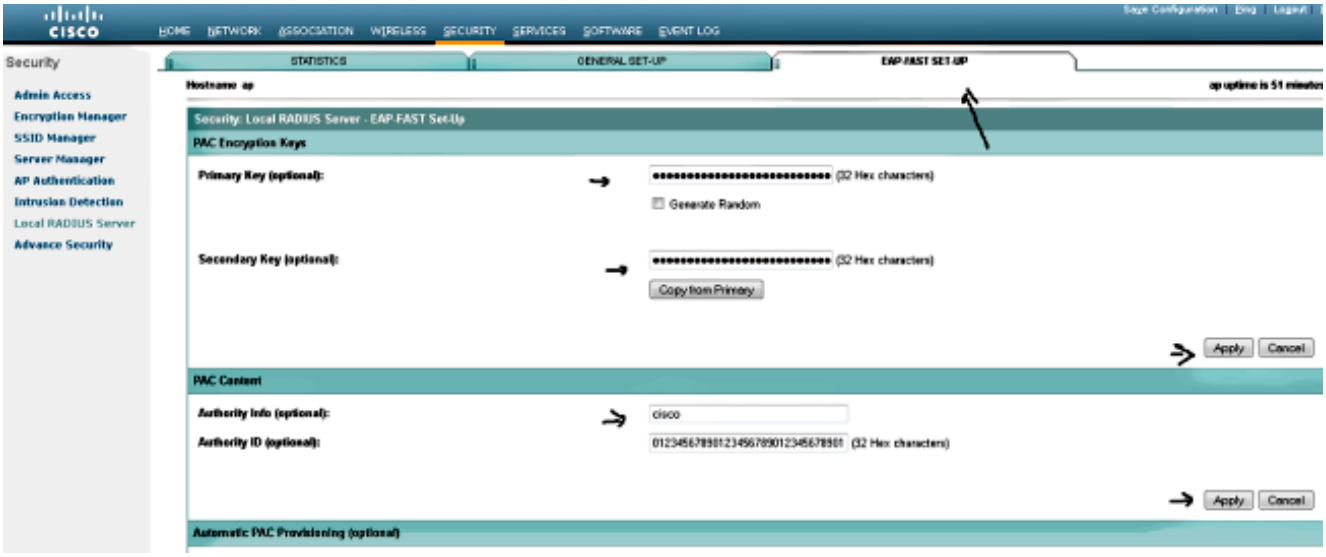


3. Desmarcar as caixas de seleção do **PULO** e **MAC**.

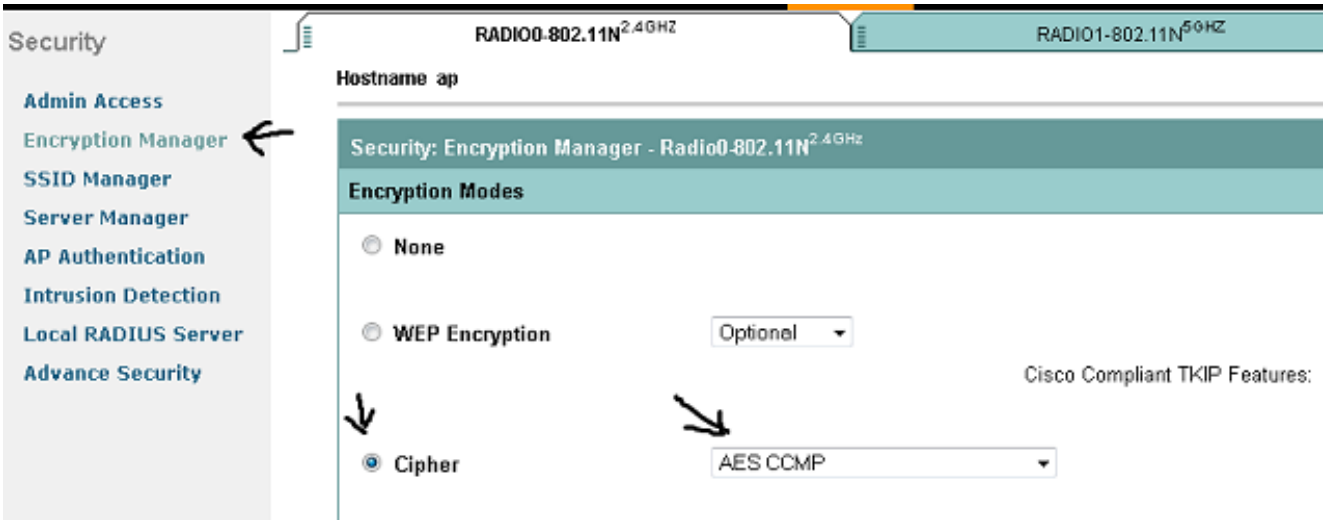


4. Clique a aba **EAP-FAST da instalação**, e incorpore os detalhes para as **chaves de criptografia PAC** e o **índice PAC**.

Note: Este exemplo usa zero a nove quatro vezes desde que manda 32 encantar caráteres.

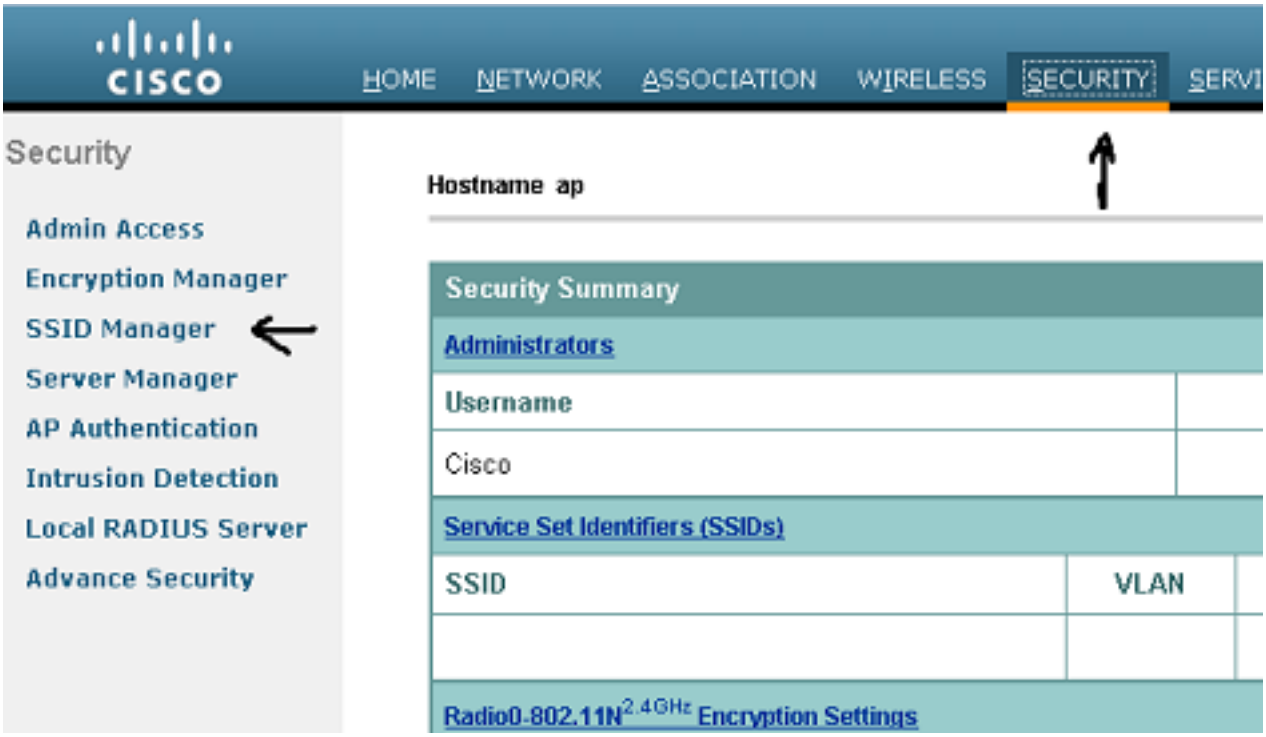


5. Navegue ao **gerenciador de criptografia**, configurar a **cifra** com **AES CCMP** como a criptografia, e o clique **aplica todos os rádios** ou **rádios exigidos**.

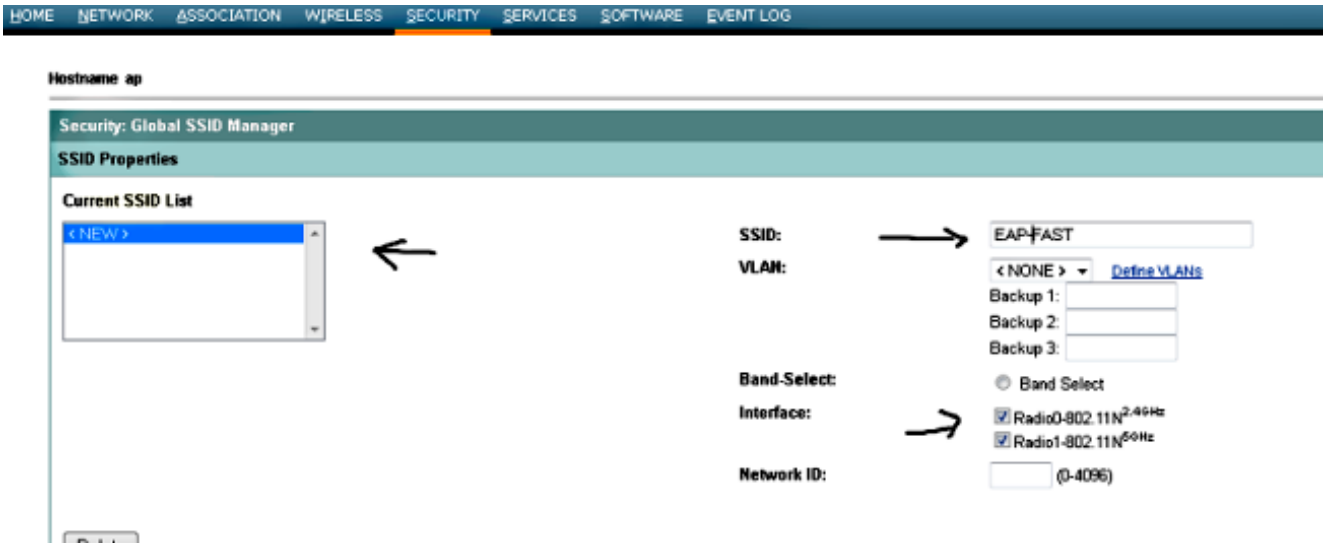


Configurar o SSID

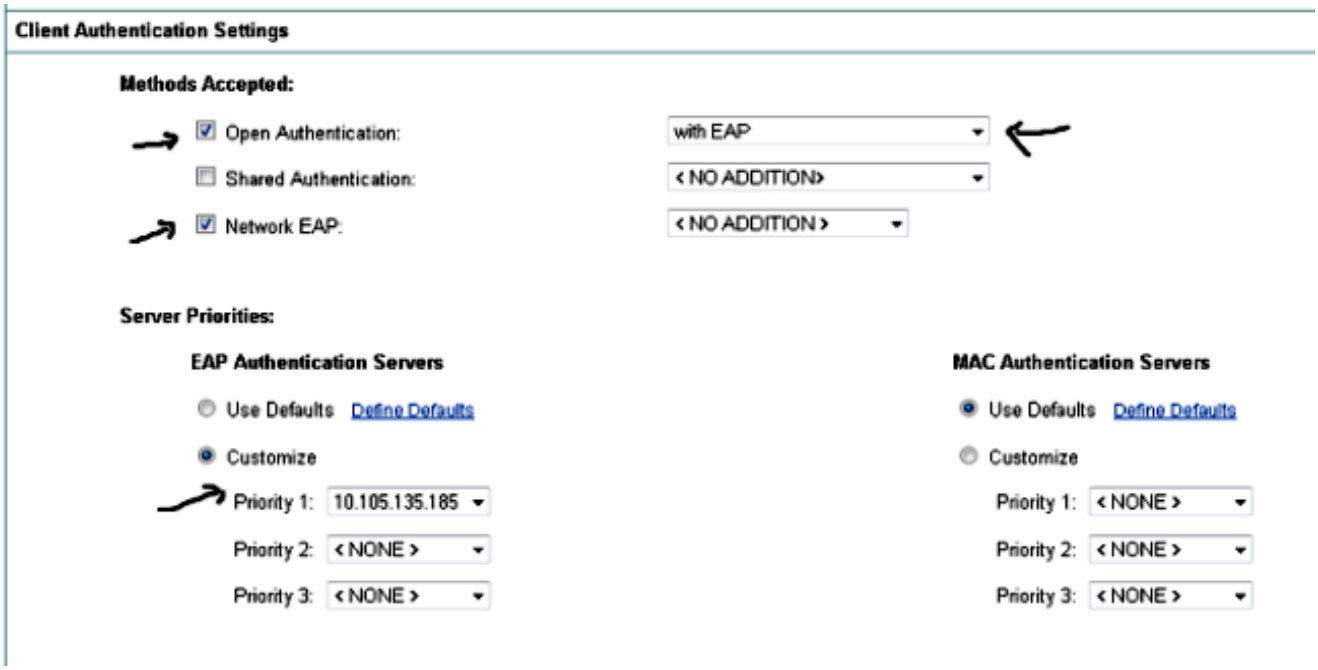
1. Navegue à **Segurança > ao gerenciador de SSID**, e o clique **cria novo**.



2. Incorpore os detalhes, e o clique **aplica-se**.

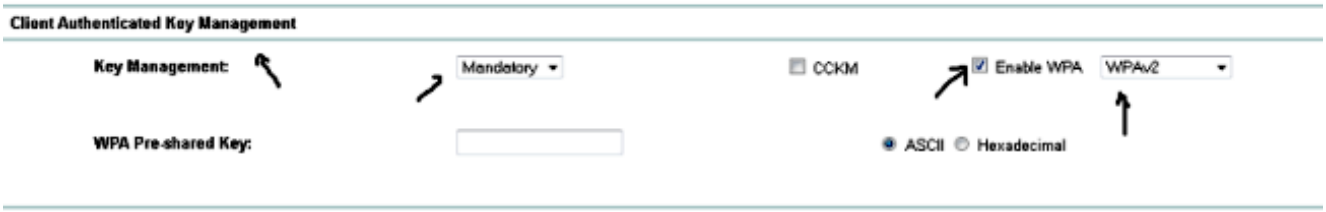


3. **Na authenticação do cliente os** ajustes selecionam, verificam a **caixa de verificação de autenticação aberta**, e selecionam-na **com o EAP do** menu suspenso. Verifique a **caixa de verificação de EAP de rede**, e selecione o **servidor Radius do** menu suspenso. Este deve ser o endereço IP de Um ou Mais Servidores Cisco ICM NT AP que você configurou como o AAA no gerenciador do servidor e na página de servidor radius local.

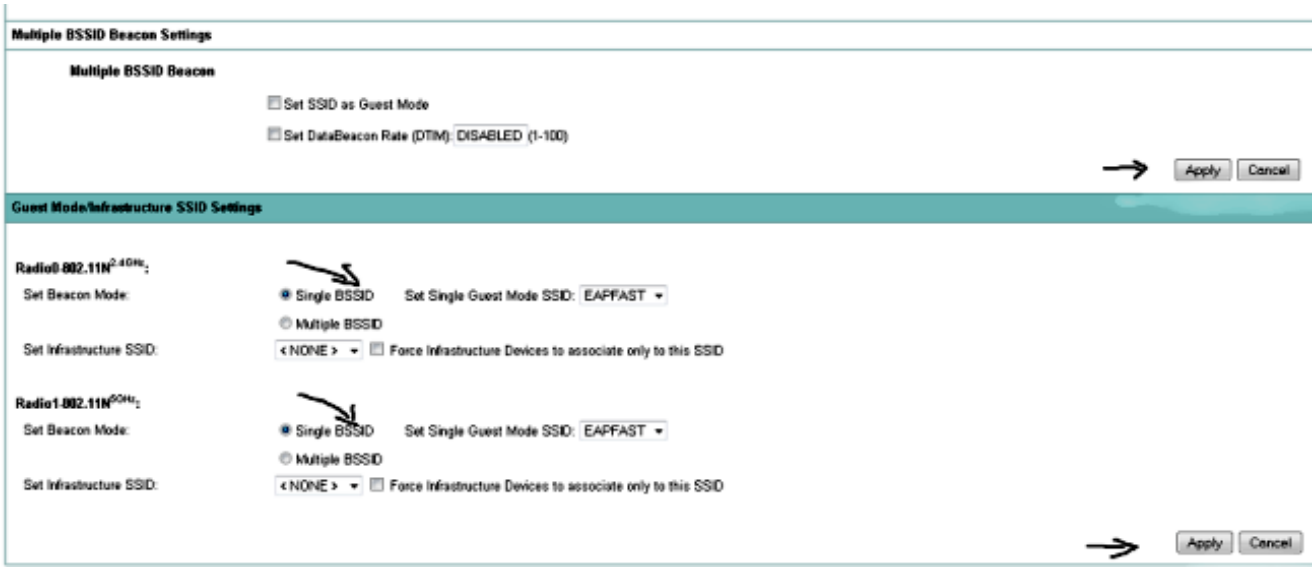


Configurar a versão 2 protegida Sem fio do acesso (WPAv2) como imperativo

1. **No cliente a** tela **autenticada do gerenciamento chave**, seleciona **imperativo do** menu suspenso do **gerenciamento chave**. Verifique a **caixa de verificação WPA da possibilidade**, e selecione **WPAv2 do** menu suspenso.



2. O clique **aplica-se na** parte inferior da página. A fim transmitir o SSID, para clicar os **únicos** botões de rádio **SSID**, para selecionar o **SSID do** menu suspenso, e o clique **aplica-se**.



3. Navegue às **redes**, e permita os rádios para **2.4 gigahertz gigahertz** e **5**. Assegure-se de que os rádios estejam em serviço.

Comando CLI para as configurações

```
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$0614$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 075A76681B514A2436465D28517D7A7178611403375342156777C79030
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#
```

Verificar

Se você conecta ao cliente, a seguir este é o log que indica no AP após uma autenticação bem sucedida:

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$0614$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 075A76681B514A2436465D28517D7A7178611403375342156777C79030
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

Termine estas etapas a fim pesquisar defeitos esta configuração.

1. A fim eliminar a possibilidade que as edições do Radio Frequency (RF) impedem a autenticação bem sucedida, ajuste o método no SSID **para abrir** a fim desabilitar temporariamente a autenticação.

2. Do GUI na página do **gerenciador de SSID**, desmarcar a **caixa de verificação de EAP de rede**, e verifique **aberto**.

3. Do CLI, não use os comandos authentication open e **nenhum eap_methods da autenticação rede-EAP**. Se o cliente associa com sucesso, o RF não contribui ao problema de associação.

4. Verifique se todas as senhas secretas compartilhadas estão sincronizadas. Estas linhas devem conter a mesma senha secundária compartilhada:
<shared_secret> chave da acct-porta x da autêntico-porta x do host de servidor RADIUS

x.x.x.x<shared_secret> da chave nas x.x.x.x

5. Remova todos os grupos de usuário e suas configurações associadas. Às vezes os conflitos ocorrem entre os grupos de usuário definidos pelo AP e os grupos de usuário no domínio.

Comandos debug

> **Note**: Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos **debug**.

Está aqui uma lista de comandos debug úteis.

- **debugar o autenticador todo aaa do dot11** - Isto debuga mostras as várias negociações que um cliente vai completamente enquanto o cliente associa e autentica com o 802.1x ou o processo EAP da perspectiva do autenticador (AP). Isto debuga foi introduzido no Cisco IOS Software Release 12.2(15)JA. Os obsoletes deste comando **debugam o dot1x todo aaa do dot11 n**este e em umas liberações mais atrasadas.

```
 *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]
```

- debugar a autenticação RADIUS - Isto debuga mostras as negociações de RADIUS entre o server e cliente, ambo, neste caso, é o AP.
- debugar o cliente do Servidor local do raio - Isto debuga mostras a autenticação do cliente da perspectiva do servidor 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]
```

- debugar pacotes do Servidor local do raio - Isto debuga mostras todos os processos por que são executados e da perspectiva do servidor Radius.