EAP-verificatie met RADIUS-server

Inhoud

Inleiding

Dit document biedt een voorbeeldconfiguratie van een Cisco IOS® gebaseerd access point voor uitgebreide verificatie Protocol (EAP)-verificatie van draadloze gebruikers tegen een database waartoe een RADIUS-server toegang heeft.

Vanwege de passieve rol die het toegangspunt speelt in EAP (bruggen draadloze pakketten van de cliënt in bedrade pakketten bestemd voor de authenticatieserver, en omgekeerd), wordt deze configuratie gebruikt met vrijwel alle MAP-methoden. Deze methoden omvatten (maar zijn niet beperkt tot) LEAP, Protected EAP (PEAP)-MS-Challenge Handshake Authentication Protocol (CHAP), versie 2, PEAP-Generic Token Card (GTC), EAP-Flexibele Verificatie via Secure Tunneling (FAST), EAP-Transport Layer Security (TLS) en EAP-Tunneled TLS (TTLS). U moet de verificatieserver voor elk van deze MAP-methoden correct configureren.

Dit document behandelt hoe u het access point (AP) en de RADIUS-server kunt configureren, een Cisco Secure ACS in het configuratievoorbeeld in dit document.

Voorwaarden

Vereisten

Zorg ervoor dat u aan deze vereisten voldoet voordat u deze configuratie probeert:

- U bent bekend met de Cisco IOS GUI of CLI.

- U kent de concepten achter MAP-authenticatie.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco Aironet AP producten die Cisco IOS uitvoeren.
- Aanname van slechts één Virtual LAN (VLAN) in het netwerk.
- Een RADIUS-serverproduct dat met succes in een gebruikersdatabase wordt geïntegreerd.Dit zijn de ondersteunde authenticatieservers voor Cisco LEAP en EAP-FAST:Cisco Secure Access Control Server (ACS)Cisco Access Registrar (CAR)Funk Steel Belted RADIUSInterlink MeritDit zijn de ondersteunde authenticatieservers voor Microsoft PEAP-MS-CHAP versie 2 en PEAP-GTC:Microsoft Internet Accounting Service (IAS)Cisco beveiligde ACSFunk Steel Belted RADIUSInterlink MeritAanvullende verificatieserver Microsoft kan toestemming geven.**Opmerking:** GTC of One-Time Pesach vereisen extra diensten die extra software aan zowel de client- als serverzijde vereisen, evenals hardware- of softwaretoken-generatoren.Raadpleeg de fabrikant van de klant voor nadere informatie over welke verificatieservers met hun producten worden ondersteund voor EAP-TLS, EAP-TTLS en andere MAP-methoden.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg de Cisco Technical Tips Convention voor meer informatie over documentconventies.

Configureren

In deze configuratie wordt beschreven hoe u EMAIT-verificatie kunt configureren op een IOS-gebaseerde AP. In het voorbeeld in dit document wordt LEAP gebruikt als een MAP-authenticatiemethode met een RADIUS-server.

Opmerking: Gebruik het Opname Gereedschap (alleen geregistreerde klanten) om meer informatie te verkrijgen over de opdrachten die in deze sectie worden gebruikt.

Net als bij de meeste op een wachtwoord gebaseerde authenticatiealgoritmen, is Cisco LEAP kwetsbaar voor woordenboekaanvallen. Dit is geen nieuwe aanval of nieuwe kwetsbaarheid van Cisco LEAP. De creatie van een sterk wachtwoordbeleid is de meest effectieve manier om woordenboekaanvallen te verzachten. Dit omvat het gebruik van sterke wachtwoorden en het periodiek aflopen van wachtwoorden. Raadpleeg Dictionary Attack op Cisco LEAP voor meer informatie over woordenboekaanvallen en hoe ze te voorkomen.

Dit document gebruikt deze configuratie voor zowel GUI als CLI:

- IP-adres van het AP is 10.0.106.
- IP-adres van de RADIUS-server (ACS) is 10.0.0.3.

PPP-verificatie of open verificatie met EAP

Bij elke op EAP/802.1x gebaseerde authenticatiemethode kun je je afvragen wat de verschillen zijn tussen netwerk-MAP en open authenticatie met MAP. Deze items verwijzen naar de waarden in het veld Verificatie-algoritme in de kopregels van beheer- en associatiepakketten. De meeste fabrikanten van draadloze klanten stelden dit veld op waarde 0 (Open authenticatie) in en gaven vervolgens aan dat zij later in het associatieproces de MAP-authenticatie willen doen. Cisco stelt de waarde anders in vanaf het begin van de associatie met de MAP-vlag.

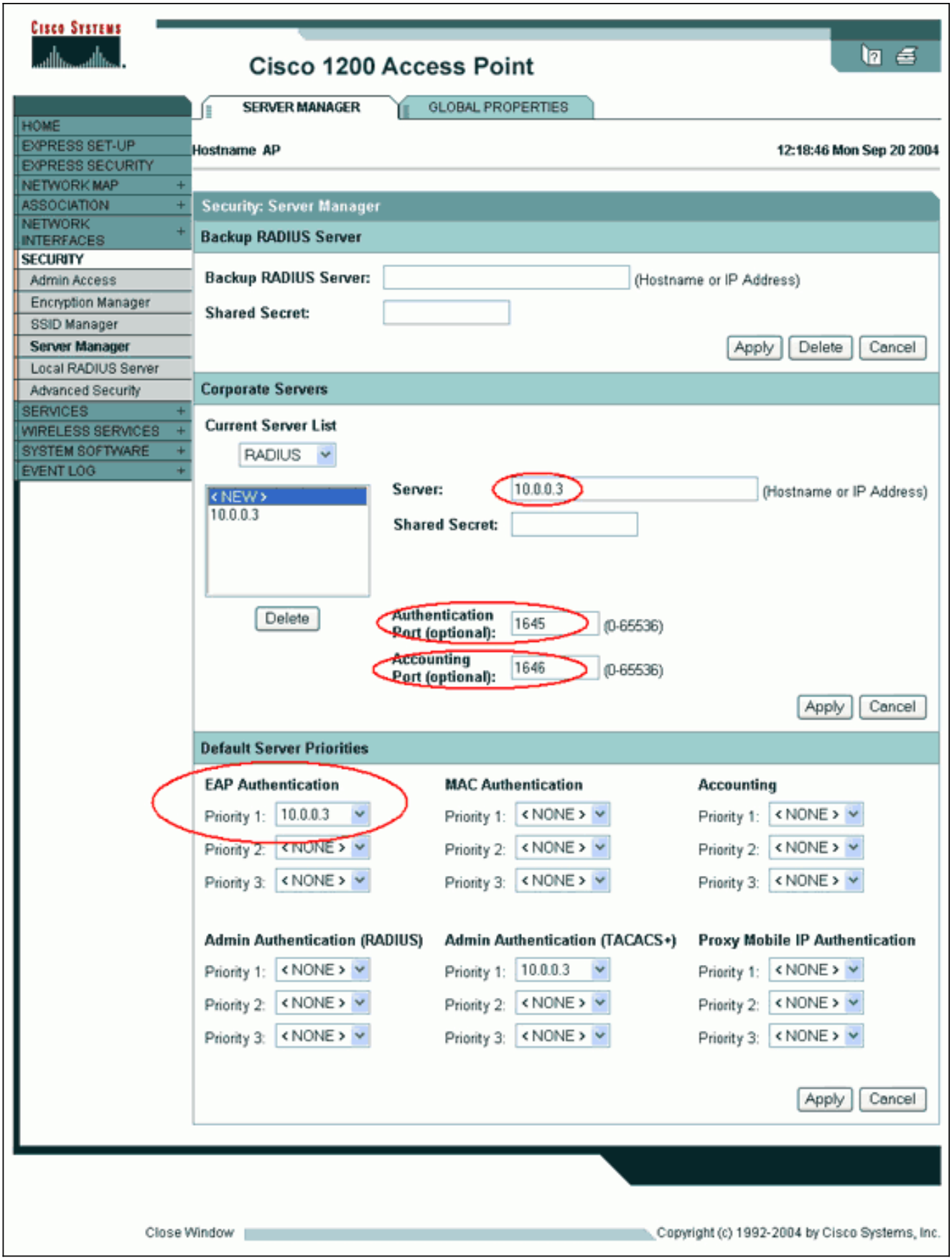
Als uw netwerk klanten heeft die zijn:

- Cisco client-Gebruik netwerk-EAP.
- Clients van derden (waaronder CCX-conforme producten)—Gebruik MAP openen.
- Een combinatie van zowel Cisco als klanten van derden — Kies zowel netwerk-EAP als Open met EAP.

Verificatieserver definiëren

De eerste stap in de MAP-configuratie is het definiëren van de authenticatieserver en het leggen van een relatie daarmee.

1. Voer in het tabblad Access Point Server Manager (onder de menuoptie **Security > Server Manager**) de volgende stappen in:Voer het IP-adres van de verificatieserver in het veld Server in.Specificeer het Gedeeld Gebied en de poorten.Klik op **Toepassen** om de definitie te maken en de vervolgkeuzelijsten te bevolken.Stel het veld EAP-verificatie-type Prioriteit 1 in op het IP-serveradres onder de standaardinstellingen van de server.Klik op **Apply** (Toepassen).

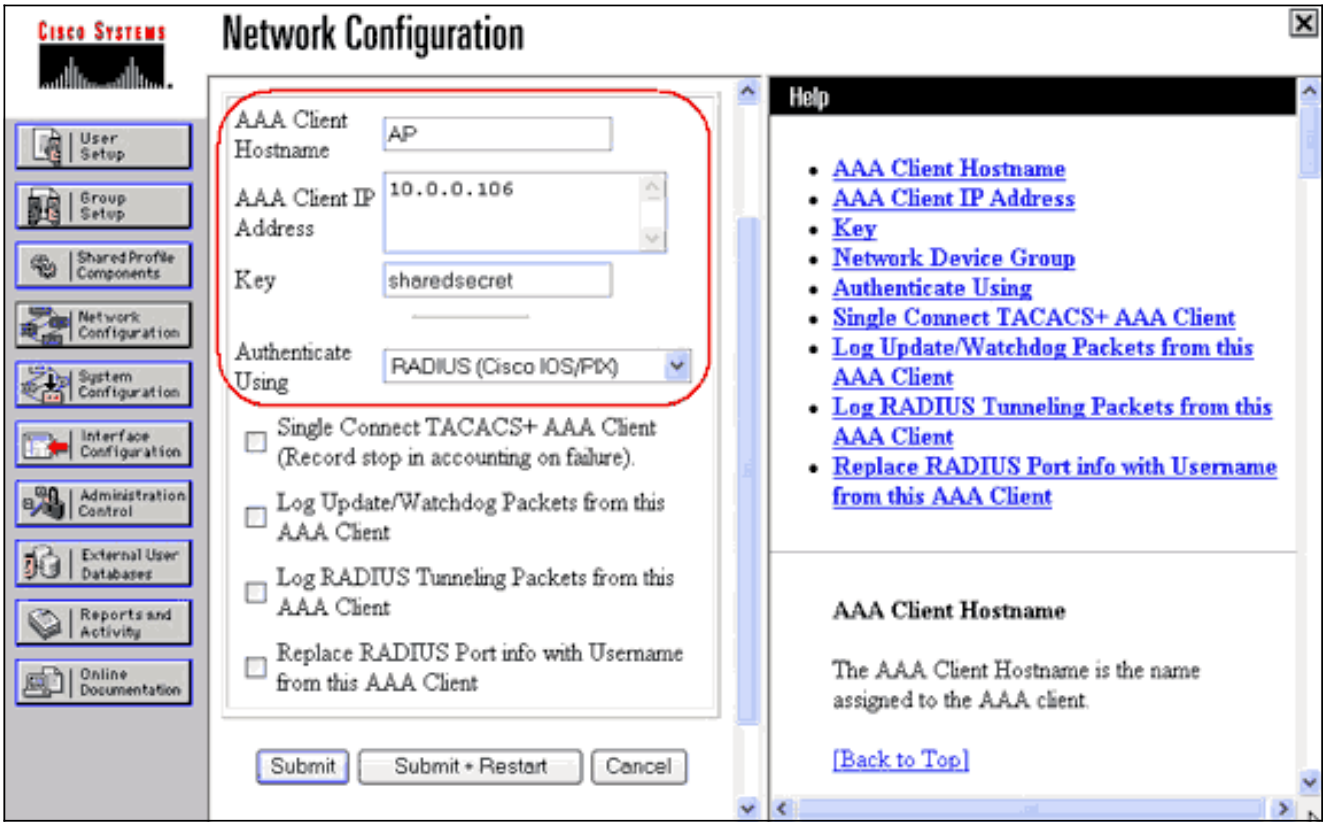


U kunt deze opdrachten ook via de CLI uitgeven:

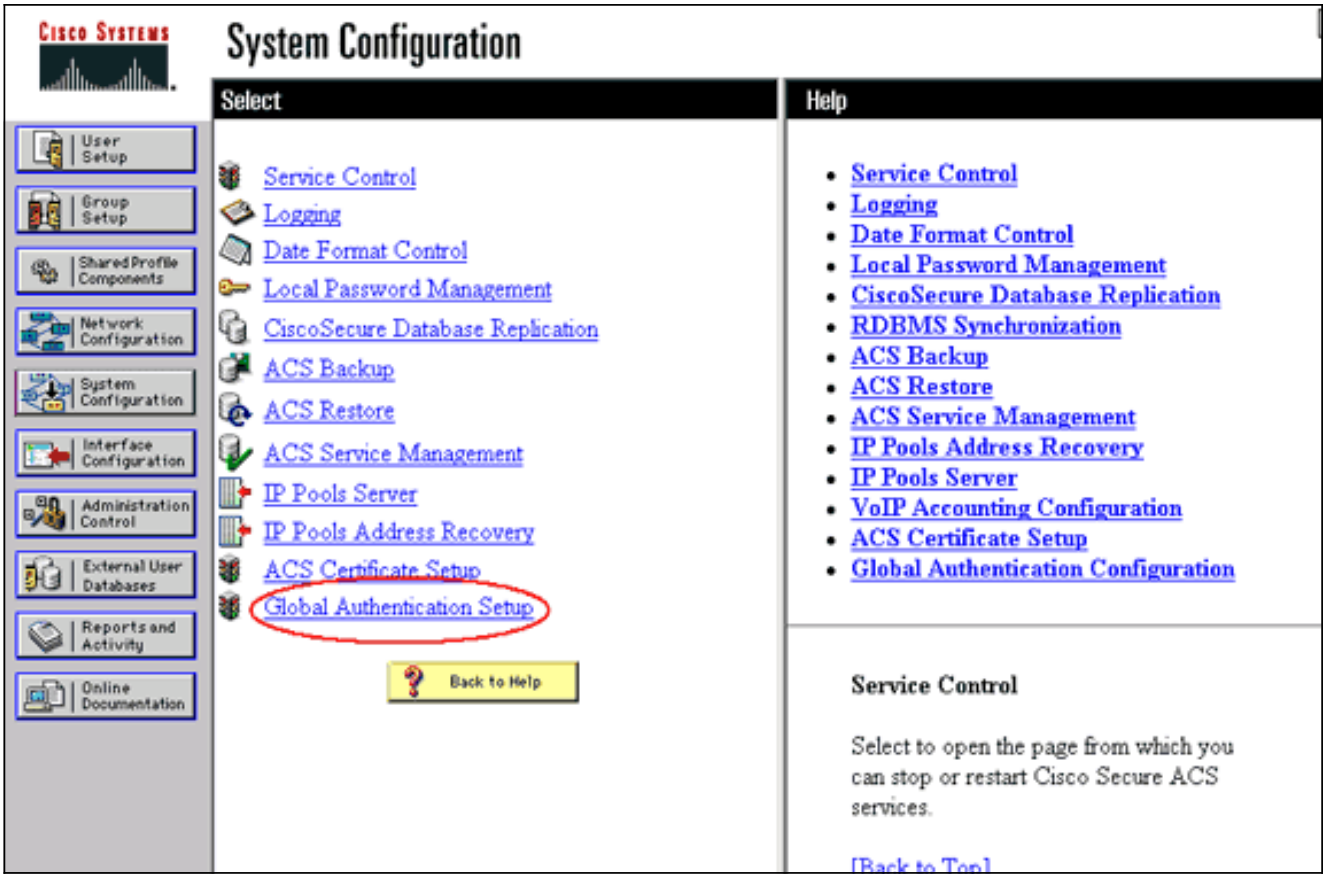
```
AP#configure terminal

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
```

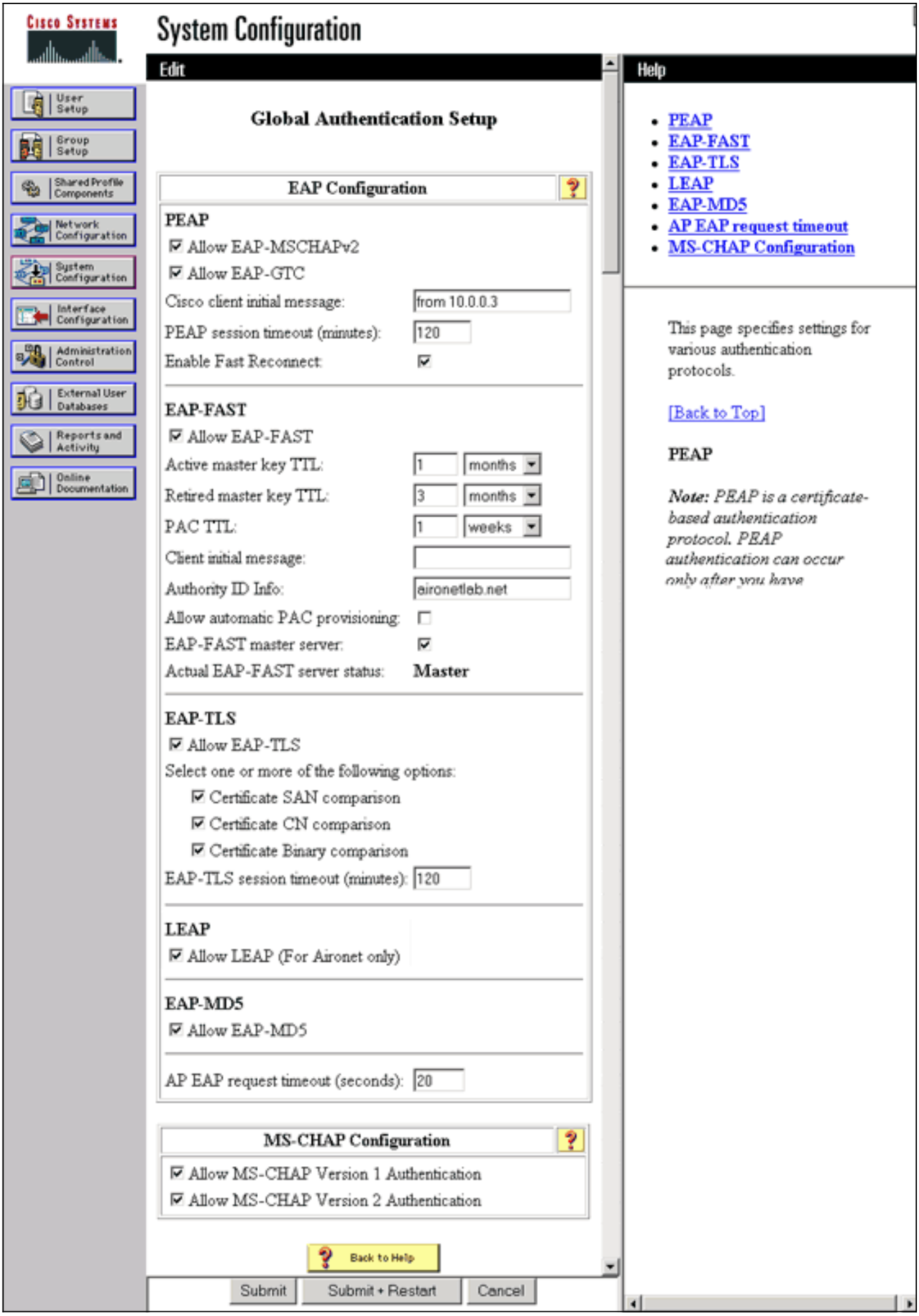
2. Het toegangspunt moet in de authenticatieserver als een AAA-client worden geconfigureerd.Bijvoorbeeld, in Cisco Secure ACS, gebeurt dit op de pagina Network Configuration waar de naam van het access point, IP-adres, gedeeld geheim en verificatiemethode (RADIUS Cisco Aironet of RADIUS Cisco IOS/PIX) wordt gedefinieerd. Raadpleeg de documentatie van de fabrikant voor andere niet-ACS-verificatieservers.



Zorg ervoor dat de verificatieserver is ingesteld om de gewenste MAP-verificatiemethode uit te voeren. Voor een Cisco Secure ACS dat LEAP uitvoert, moet u bijvoorbeeld de LEAP-verificatie op de System Configuration - de Global Verification Setup-pagina configureren. Klik op **System Configuration** en klik vervolgens op **Global Authentication Setup**. Raadpleeg de documentatie van de fabrikant voor andere niet-ACS-verificatieservers of andere MAP-methoden.



In deze afbeelding is te zien hoe Cisco Secure ACS is geconfigureerd voor PEAP, EAP-FAST, EAP-TLS, LEAP en EAP-
MD5.

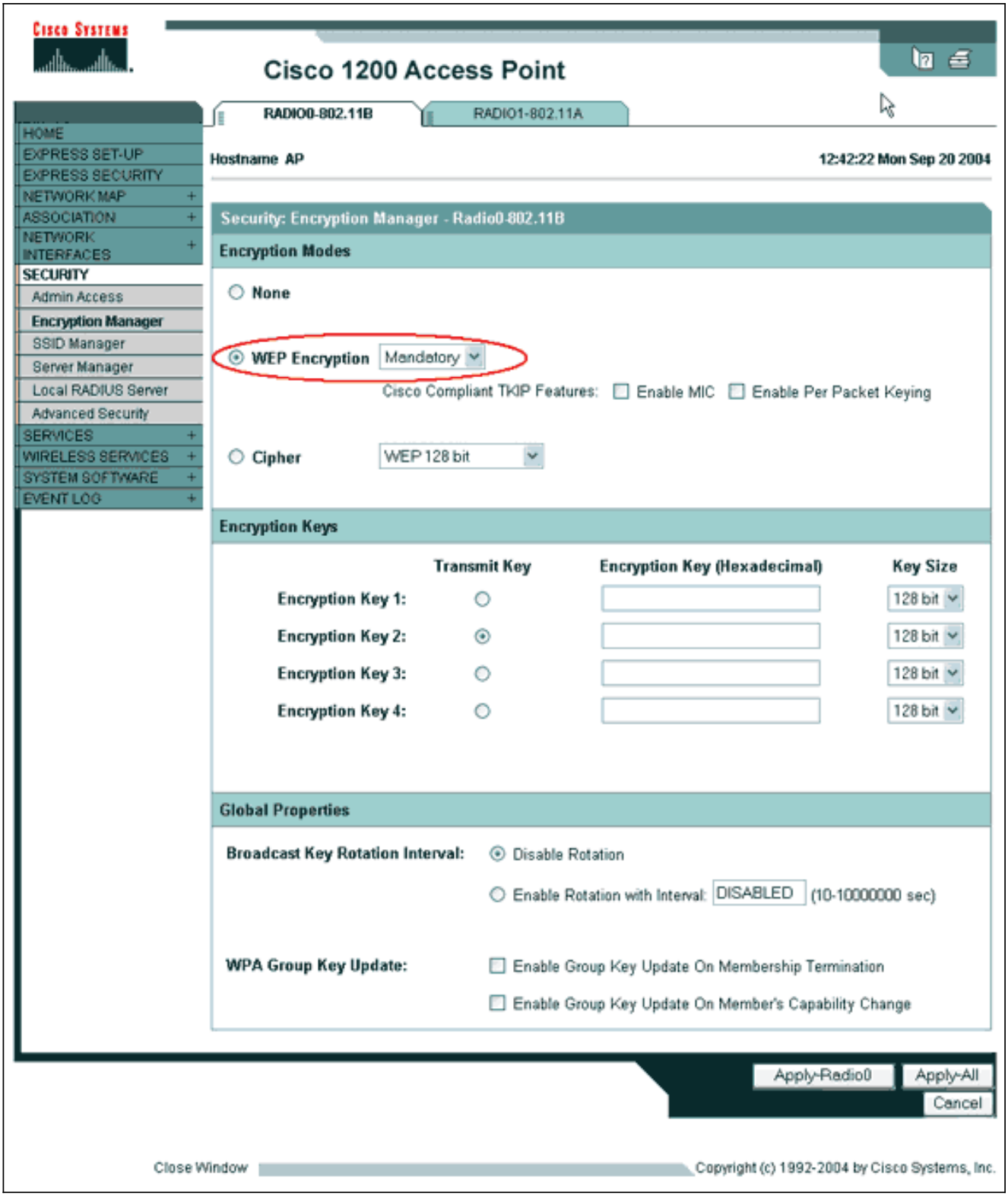


[Clientverificatiemethoden definiëren]

Zodra het access point weet waar je clientverificatieverzoeken moet versturen, moet je ze configureren om deze methoden te aanvaarden.

Opmerking: deze instructies zijn bedoeld voor een installatie die is gebaseerd op het gebruik van een koppelteken. Voor WAP (dat ciphers in plaats van NUL gebruikt), raadpleeg het Overzicht van de Configuratie van WAP.

1. Voer in het tabblad Encryption Manager (onder de menuoptie **Security > Encryption Manager**) de volgende stappen in:Specificeer dat u **de encryptie** van **EFN** wilt gebruiken.Specificeer dat de **verplicht** is.Controleer dat de grootte van de toets op **128 bits** is ingesteld.Klik op **Apply**
   (Toepassen).

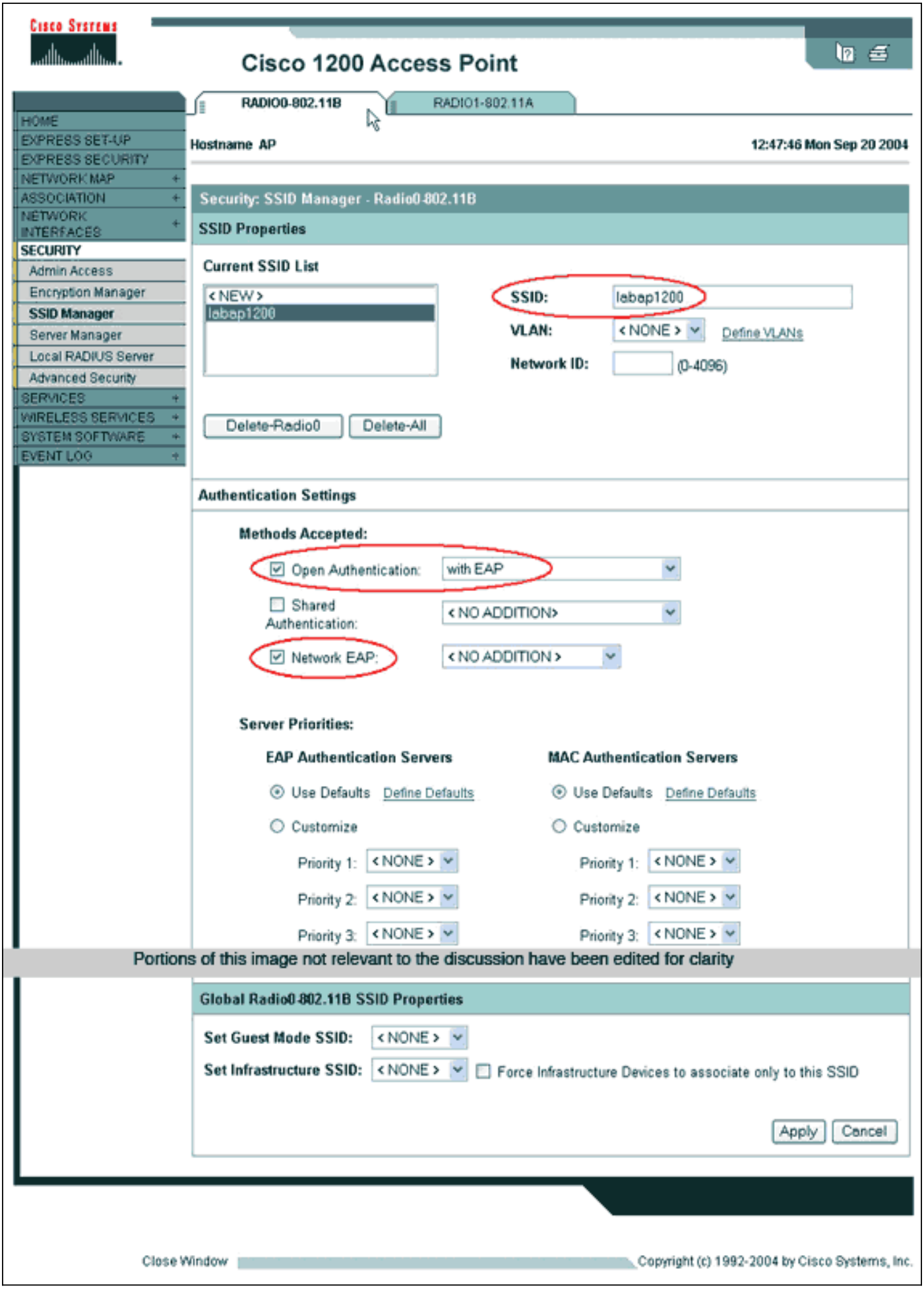


U kunt deze opdrachten ook via de CLI uitgeven:

```
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. Voltooi deze stappen op het tabblad SSID Manager (onder de menuoptie **Security > SSID**

Manager):Selecteer de gewenste SSID.Selecteer onder "Verificatiemethoden geaccepteerd" het vakje **Open** en gebruik de vervolgkeuzelijst om **met EAP** te kiezen.Schakel het vakje **Network-EAP** uit als u Cisco-clientkaarten hebt. Zie de discussie in het gedeelte netwerk EAP of Open Verificatie met EAP.Klik op **Apply** (Toepassen).



U kunt deze opdrachten ook via de CLI uitgeven:

```
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
```

Zodra u de basisfunctionaliteit met een basis-EAP configuratie hebt bevestigd, kunt u in een later tijdstip aanvullende functies en sleutelbeheer toevoegen. Layer 2 compacte functies bovenop functionele stichtingen om het oplossen van problemen te vergemakkelijken.

Verifiëren

Deze sectie verschaft informatie die u kunt gebruiken om te bevestigen dat uw configuratie correct werkt.

Bepaalde opdrachten met **show worden ondersteund door de tool** Output Interpreter (alleen voor geregistreerde klanten). Hiermee kunt u een analyse van de output van opdrachten met **show genereren.**

- **Straal server-groep all**-Hiermee geeft u een lijst weer van alle geconfigureerde RADIUS-servergroepen in het AP.

Problemen oplossen

Procedure voor probleemoplossing

Voltooi deze stappen om problemen met de configuratie op te lossen.

1. In de client-side voorziening of software, een nieuw profiel of verbinding maken met dezelfde of soortgelijke parameters om te verzekeren dat niets in de configuratie van de client gecorrumpeerd is.
2. Om de mogelijkheid van RF-emissies die succesvolle authenticatie voorkomen uit te sluiten, moet de authenticatie tijdelijk worden uitgeschakeld zoals in deze stappen wordt getoond:Van CLI, gebruik de opdrachten **geen authenticatie open eap_methods**, **geen authenticatie netwerk-eap_methods** en **verificatie open**.Vanuit de GUI, op de pagina van SSID Manager, **netwerk-EAP** uit-controle, **Open**, en stel de vervolgkeuzelijst terug naar **Geen Toevoeging** in.Als de client succesvol geassocieerd is, draagt RF niet bij aan het associatieprobleem.
3. Controleer dat gedeelde geheime wachtwoorden tussen het access point en de authenticatieserver gesynchroniseerd zijn. Anders kunt u deze foutmelding ontvangen:
   ```
   Invalid message authenticator in EAP request
   ```

Controleer vanuit de CLI de regel `straal-server host x.x.x.x.x auth-port x acct-port x key <gedeeld_geheim>`.Vanuit de GUI, op de pagina Server Manager, voer het gedeelde geheim voor de juiste server opnieuw in in het vak met het label "gedeeld geheim".De gedeelde geheime ingang voor het toegangspunt op de RADIUS-server moet hetzelfde gedeelde geheime wachtwoord bevatten als de eerder genoemde.

4. Verwijder gebruikersgroepen van de RADIUS-server. Soms kunnen er conflicten ontstaan tussen gebruikersgroepen die gedefinieerd zijn door de RADIUS-server en gebruikersgroepen in het onderliggende domein. Controleer de logs van de RADIUS-server op mislukte pogingen en geef de redenen op die pogingen.

Opdrachten voor probleemoplossing

Bepaalde opdrachten met **show worden ondersteund door de tool** Output Interpreter (alleen voor geregistreerde klanten). Hiermee kunt u een analyse van de output van opdrachten met **show genereren.**

Debugging Authentications biedt een aanzienlijke hoeveelheid details over hoe de output van debugs gerelateerd aan EAP moet worden verzameld en geïnterpreteerd.

Opmerking: Voordat u **debug-**opdrachten afgeeft, raadpleegt u de belangrijke informatie over debug-opdrachten.

- **debug dot11 a.state-machine**-Show grote divisies (of staten) van de onderhandeling tussen de client en de authenticatieserver. Hier is een resultaat van een **succesvolle** authenticatie:

```
*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)
```

Opmerking: In Cisco IOS-softwarereleases vóór 12.2(15)JA is de syntaxis van deze **debug** opdracht **debug dot11 a dot1x staatsmachine**.

- **debug dot11 a authenticator proces**-displays de individuele dialoogingangen van de onderhandeling tussen de client en de authenticatieserver.**Opmerking:** In Cisco IOS-softwarereleases vóór 12.2(15)JA is de syntaxis van deze debug-opdracht **debug dot11 a dot1x-proces**.
- **bug van detectie straal**-displays de RADIUS-onderhandelingen tussen de server en client, die beide worden overbrugd door AP. Dit is een output voor **mislukte** authenticatie:

```
*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 a authenticatie**-Hiermee geeft u de AAA-onderhandelingen voor verificatie tussen het clientapparaat en de verificatieserver weer.

Gerelateerde informatie

- Debug-verificatie
- Verificatietypen configureren
- LEAP-verificatie op een lokale RADIUS-server
- RADIUS- en TACACS+ servers configureren
- Cisco Secure ACS voor Windows v3.2 configureren met PEAP-MS-CHAPv2-machineverificatie
- Cisco Secure ACS voor Windows v3.2 met EAP-TLS-machineverificatie
- PEAP/EAP op Microsoft IAS configureren
- Problemen oplossen door Microsoft IAS als RADIUS-server
- Microsoft 802.1X verificatie-client
- Technische ondersteuning en documentatie – Cisco Systems