Configuratievoorbeeld van geconvergeerde access points 5760, 3850 en 3650 Series WLC EAP-FAST met interne RADIUS-server

Inhoud

Inleiding

Dit document beschrijft hoe u de Cisco geconvergeerde access controllers 5760, 3850 en 3650 Series draadloze LAN-controllers (WLCs) kunt configureren om op te treden als RADIUS-servers die Cisco Extensible Verification Protocol-Flexibele Verificatie via Secure Protocol (EAP-FAST, in dit voorbeeld) uitvoeren voor clientverificatie.

Meestal wordt een externe RADIUS-server gebruikt om gebruikers voor authentiek te verklaren, wat in sommige gevallen geen haalbare oplossing is. In deze situaties kan een geconvergeerde access WLC optreden als een RADIUS-server, waar de gebruikers geauthentiseerd zijn tegen de lokale database die is geconfigureerd in het WLC. Dit wordt een lokale RADIUS-serverfunctie genoemd.

Voorwaarden

Vereisten

Cisco raadt u aan om kennis te hebben van deze onderwerpen voordat u deze configuratie probeert:

- Cisco IOS: GUI of CLI met geconvergeerde access point 5760, 3850 en 3650 Series WLC
- Extensible Authentication Protocol (EAP)-concepten
- Configuratie van servicesinstelling (SSID)
- RADIUS

Gebruikte componenten

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

- Cisco 750 Series WLC release 3.3.2 (kabelkasten van de volgende generatie [NGWC])
- Cisco 3602 Series lichtgewicht access point (AP)
- Microsoft Windows XP met Intel PROset Suppliciet
- Cisco Catalyst 3560 Series-switches

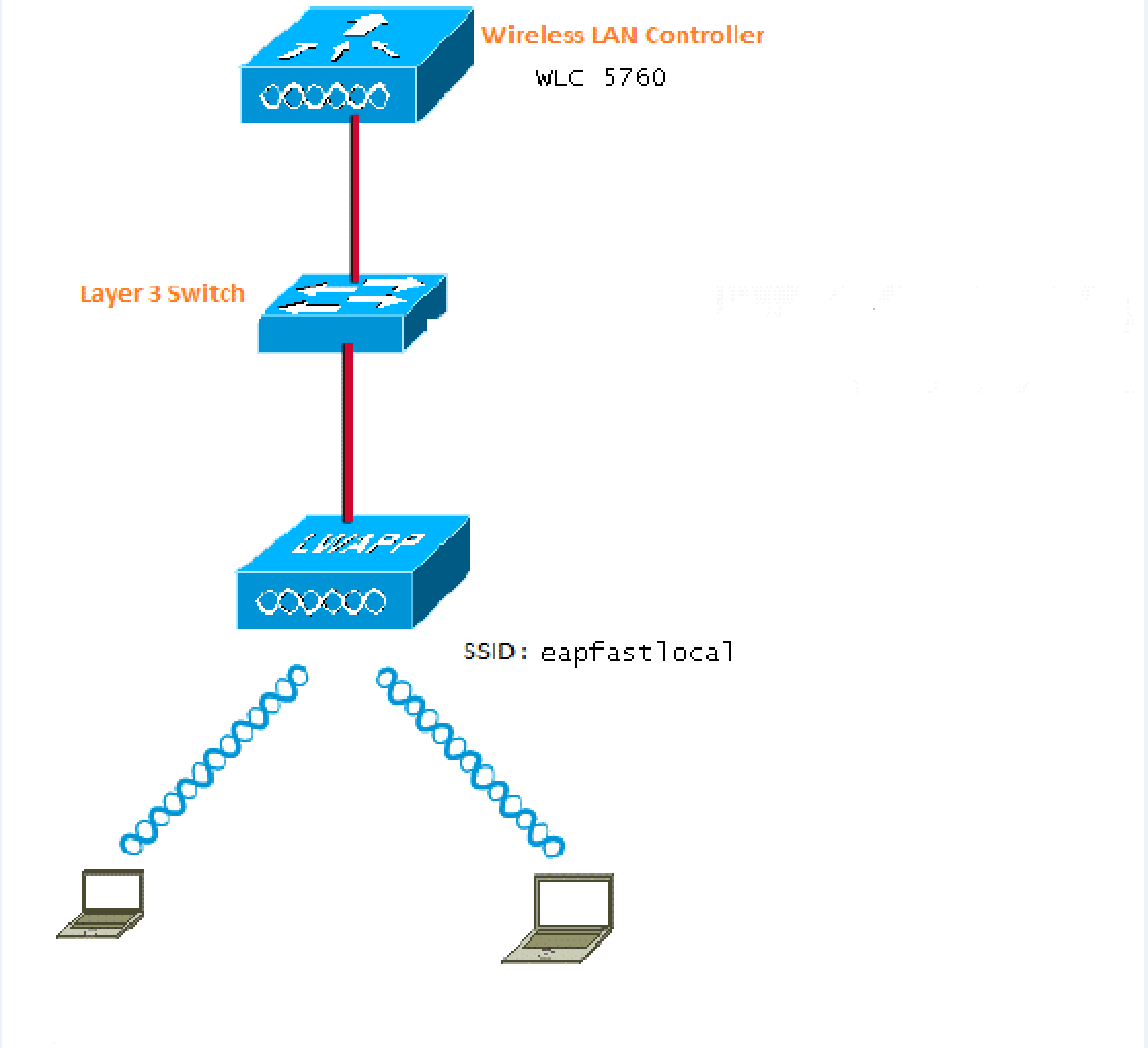
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Configureren

> Opmerking: Gebruik de Command Lookup Tool (alleen voor geregistreerde gebruikers) voor meer informatie over de opdrachten die in deze sectie worden gebruikt.

Netwerkdiagram

Dit beeld geeft een voorbeeld van een netwerkdiagram:



Overzicht van configuratie

Deze configuratie wordt in twee stappen voltooid:

1. Het configureren van de WLC voor de lokale MAP-methode en de bijbehorende authenticatie- en autorisatieprofielen met de CLI of GUI.

2. Configureer de WLAN’s en kaart de methodelijst met de verificatie- en autorisatieprofielen.

De WLC met de CLI configureren

Voltooi deze stappen om de WLC met de CLI te configureren:

1. Schakel het AAA-model in op de WLC:

```
aaa new-model
```

2. Vaststellen van de echtheidscontrole en de vergunning:

```
aaa local authentication eapfast authorization eapfast

aaa authentication dot1x eapfast local
aaa authorization credential-download eapfast local
aaa authentication dot1x default local
```

3. Configureer het lokale MAP-profiel en de methode (EAP-FAST wordt in dit voorbeeld gebruikt):

```
eap profile eapfast
 method fast
!
```

4. Configureer de geavanceerde parameters van EAP-FAST:

```
eap method fast profile eapfast
 description test
 authority-id identity 1
 authority-id information 1
 local-key 0 cisco123
```

5. Configureer het WLAN en kaart het lokale vergunningsprofiel aan de WLAN:

```
wlan eapfastlocal 13 eapfastlocal
 client vlan VLAN0020
 local-auth eapfast
 session-timeout 1800
 no shutdown
```

6. Configureer de infrastructuur ter ondersteuning van de clientconnectiviteit:

```
ip dhcp snooping vlan 12,20,30,40,50
ip dhcp snooping
!
ip dhcp pool vlan20
 network 20.20.20.0 255.255.255.0
 default-router 20.20.20.251
 dns-server 20.20.20.251



interface TenGigabitEthernet1/0/1
 switchport trunk native vlan 12
 switchport mode trunk
 ip dhcp relay information trusted
 ip dhcp snooping trust
```

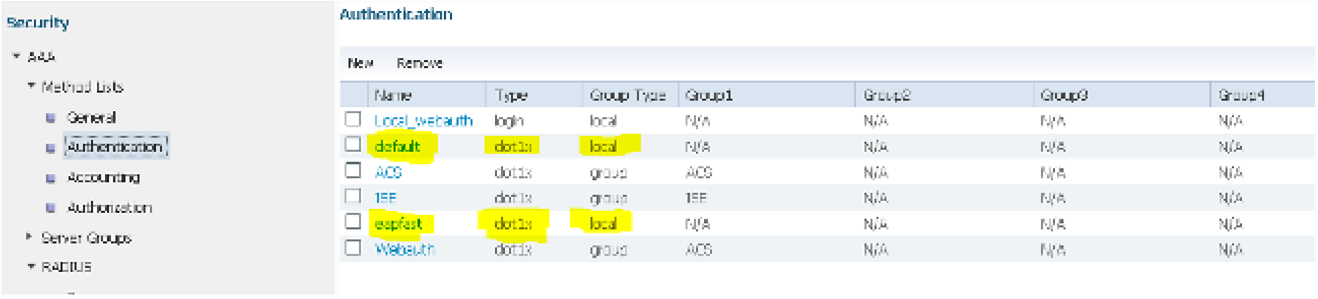
De WLC configureren met de GUI

Volg deze stappen om de WLC met de GUI te configureren:

1. Configuratie van de methodelijst voor Verificatie:

Configureer het **snelle** type als **Dot1x**.

Configuratie van het **snelle** groepstype als **Lokaal**.



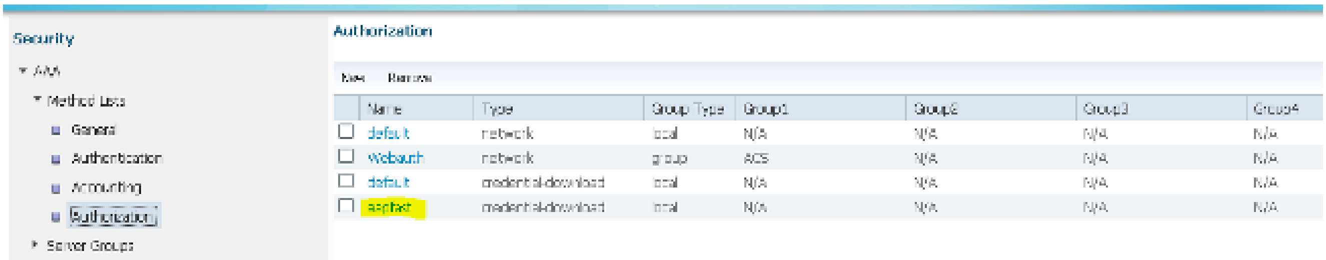
Authentication

	Name	Type	Group Type	Group1	Group2	Group3	Group4
□	Local_webauth	login	local	N/A	N/A	N/A	N/A
□	default	dot1x	local	N/A	N/A	N/A	N/A
□	ACS	dot1x	group	ACS	N/A	N/A	N/A
□	ISE	dot1x	group	ISE	N/A	N/A	N/A
□	eapfast	dot1x	local	N/A	N/A	N/A	N/A
□	Webauth	dot1x	group	ACS	N/A	N/A	N/A

2. Configureer de methodelijst voor autorisatie:

   Configureer het **snelle** type als **Credentiaal-download**.

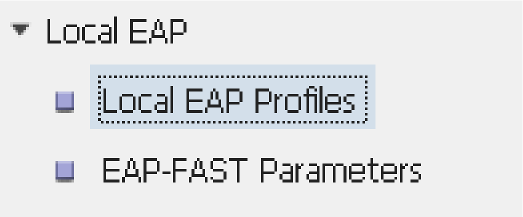
   Configuratie van het **snelle** groepstype als **Lokaal**.



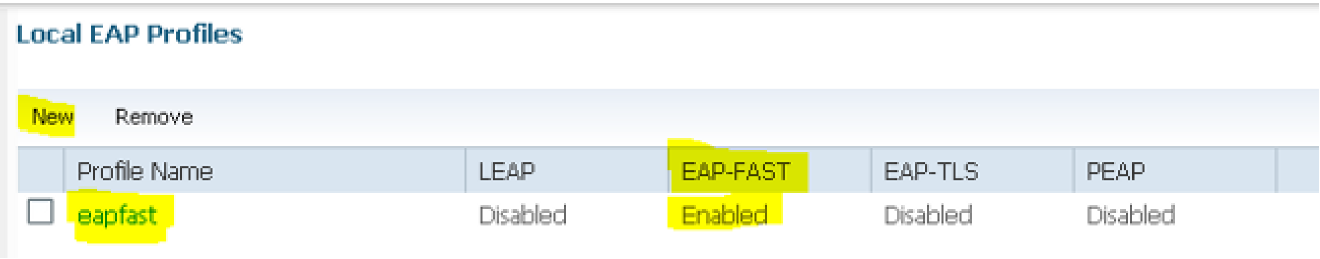
Authorization

	Name	Type	Group Type	Group1	Group2	Group3	Group4
□	default	network	local	N/A	N/A	N/A	N/A
□	Webauth	network	group	ACS	N/A	N/A	N/A
□	default	credential-download	local	N/A	N/A	N/A	N/A
□	eapfast	credential-download	local	N/A	N/A	N/A	N/A

3. Het lokale MAP-profiel configureren:



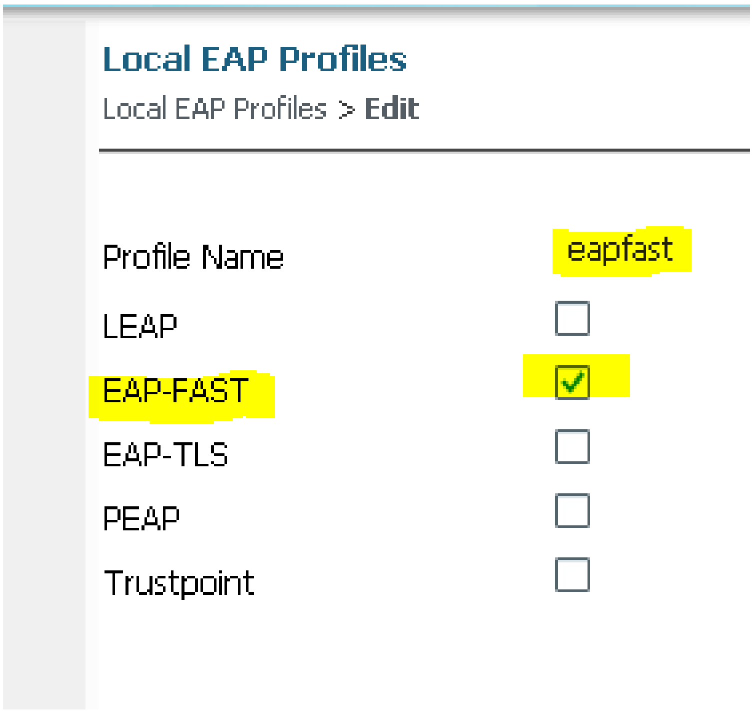
4. Maak een nieuw profiel en selecteer het MAP-type:



Local EAP Profiles

	Profile Name	LEAP	EAP-FAST	EAP-TLS	PEAP
□	eapfast	Disabled	Enabled	Disabled	Disabled

De profielnaam is **gemakkelijk** en het geselecteerde MAP-type is **MAP-FAST**:



Local EAP Profiles

Local EAP Profiles > **Edit**

Profile Name eapfast

LEAP □

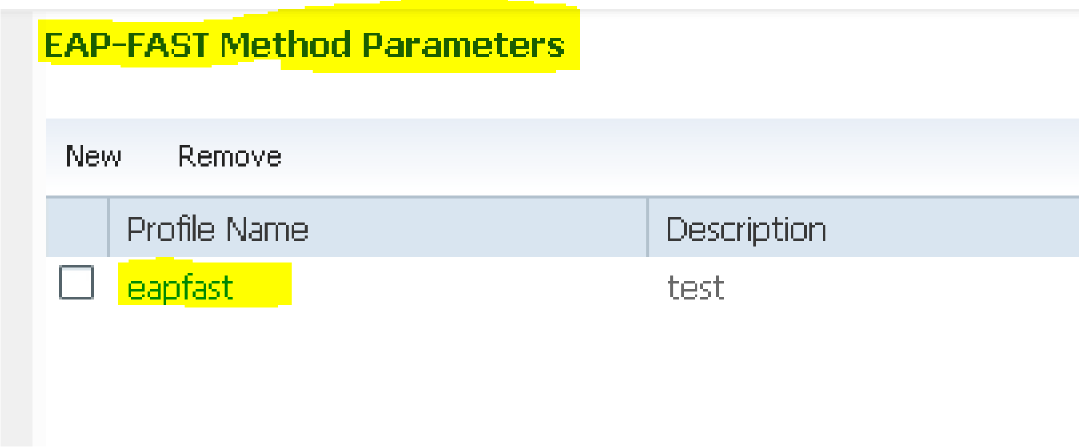
EAP-FAST ☑

EAP-TLS □

PEAP □

Trustpoint □

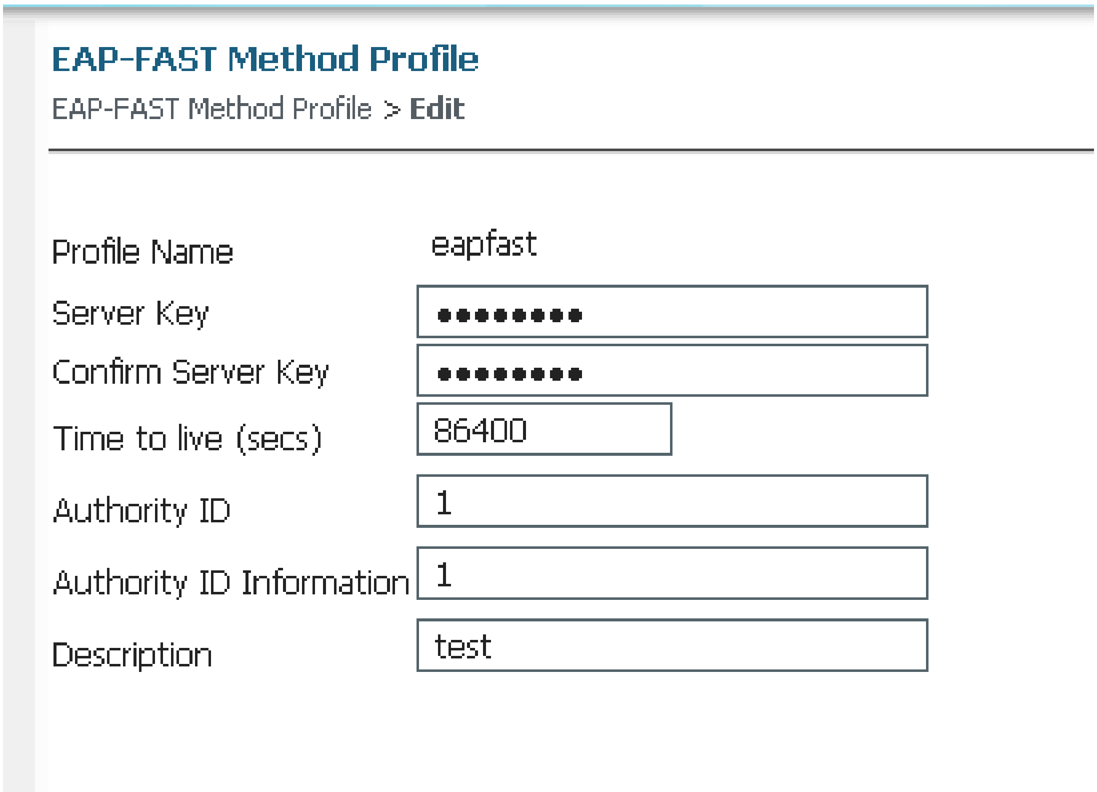
5. Configureer de parameters van de MAP-FAST-methode:



EAP-FAST Method Parameters

	Profile Name	Description
□	eapfast	test

De serversleutel is ingesteld als **Cisco123**.

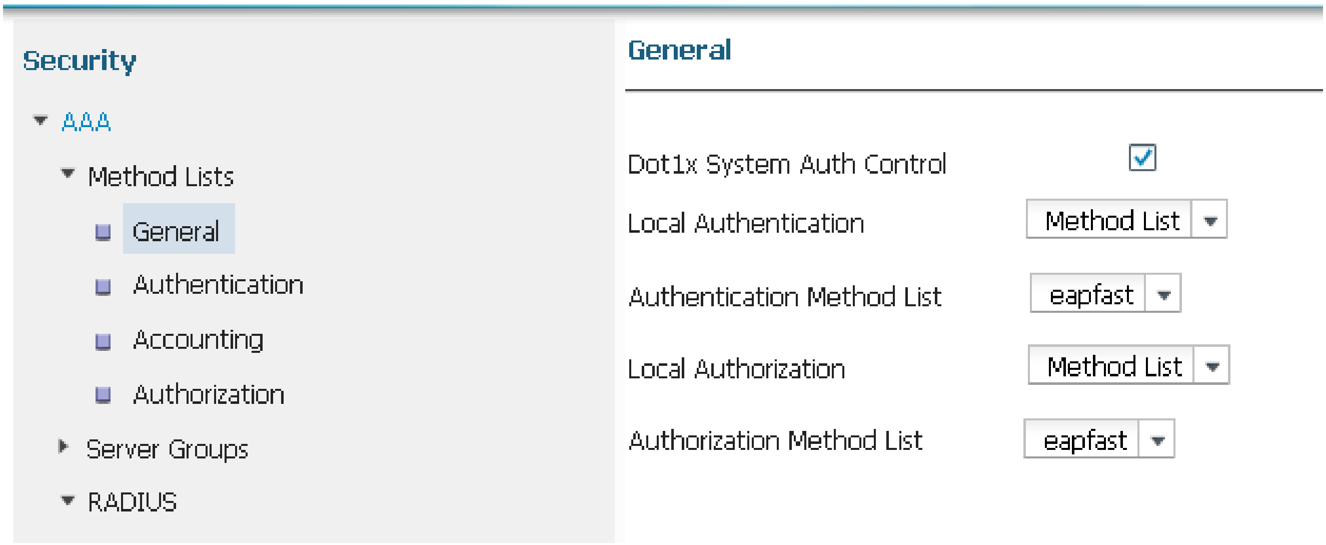


EAP-FAST Method Profile

EAP-FAST Method Profile > **Edit**

Profile Name	eapfast
Server Key	•••••••••
Confirm Server Key	•••••••••
Time to live (secs)	86400
Authority ID	1
Authority ID Information	1
Description	test

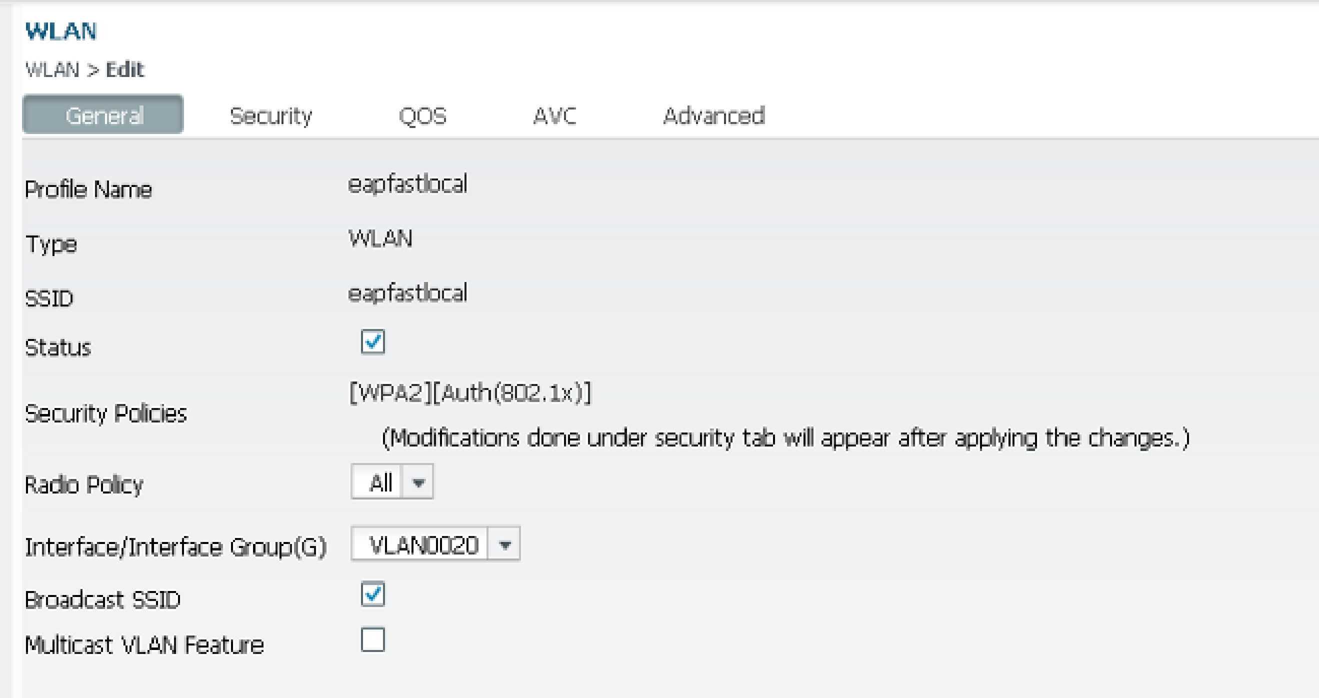
6. Controleer het vakje **Dot1x System Auth Control** en selecteer **snel** voor de methodelijsten. Dit helpt u de lokale MAP-authenticatie uit te voeren.



General

Dot1x System Auth Control	☑
Local Authentication	Method List
Authentication Method List	eapfast
Local Authorization	Method List
Authorization Method List	eapfast

7. Configuratie van WLAN voor WAP2 AES-encryptie:



WLAN

WLAN > Edit

Profile Name eapfastlocal

Type WLAN

SSID eapfastlocal

Status ☑

Security Policies [WPA2][Auth(802.1x)]

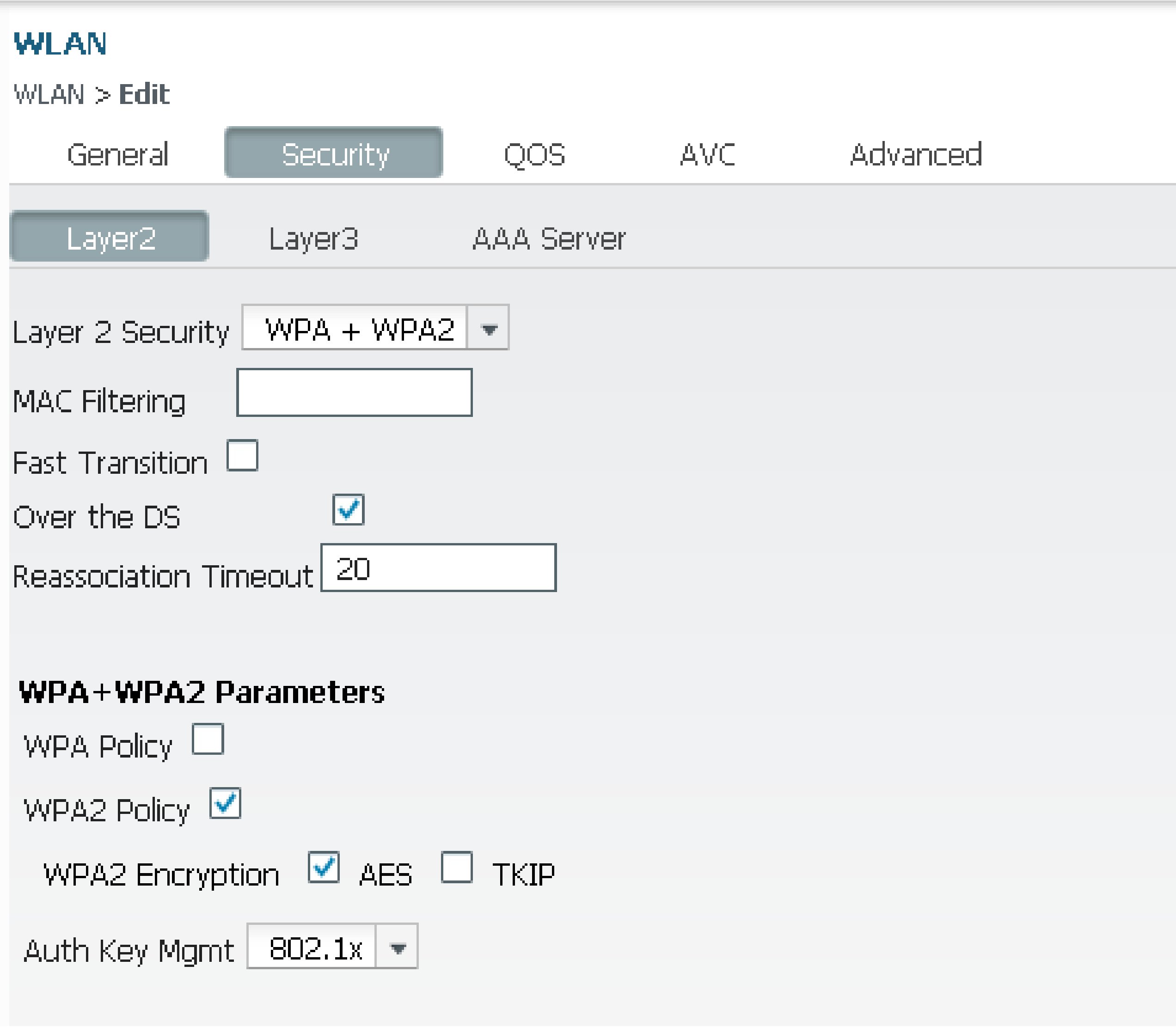
(Modifications done under security tab will appear after applying the changes.)

Radio Policy All

Interface/Interface Group(G) VLAN0020

Broadcast SSID ☑

Multicast VLAN Feature □



WLAN

WLAN > Edit

Layer 2 Security WPA + WPA2

MAC Filtering

Fast Transition □

Over the DS ☑

Reassociation Timeout 20

WPA+WPA2 Parameters

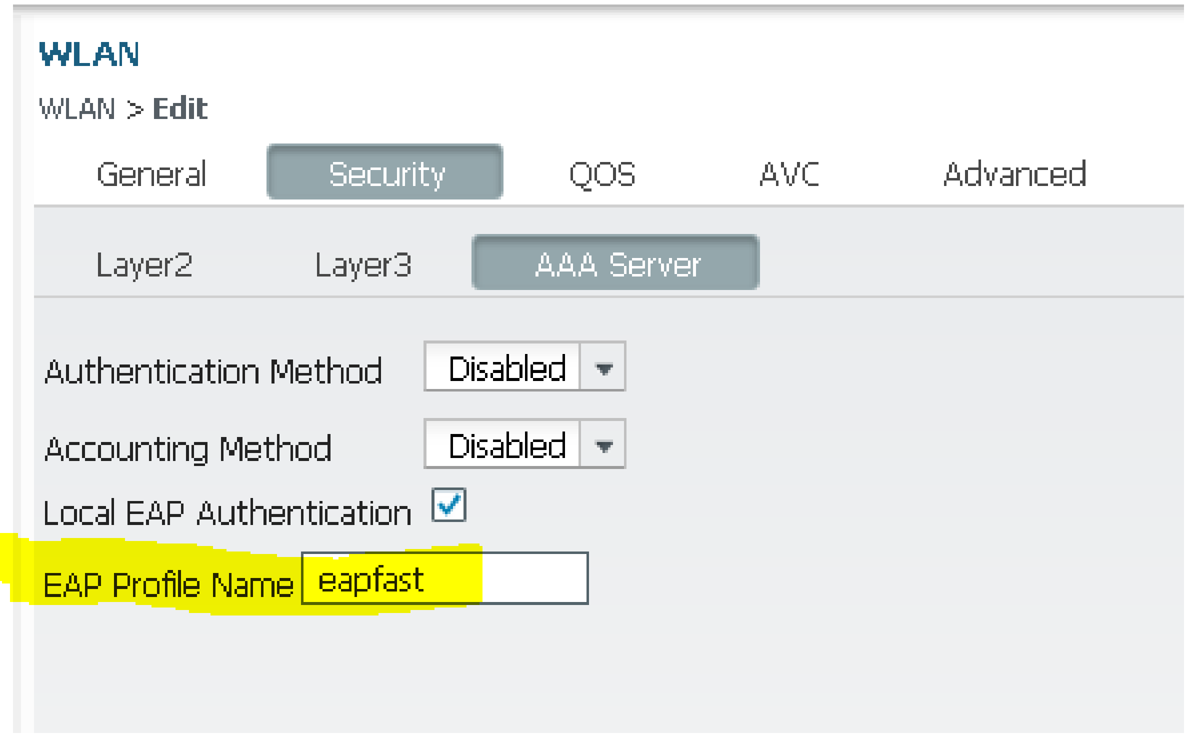
WPA Policy □

WPA2 Policy ☑

WPA2 Encryption ☑ AES □ TKIP

Auth Key Mgmt 802.1x

8. Stel in het tabblad **AAA-server** de MAP Profile Name **snel** in bij WLAN:



Authentication Method: Disabled

Accounting Method: Disabled

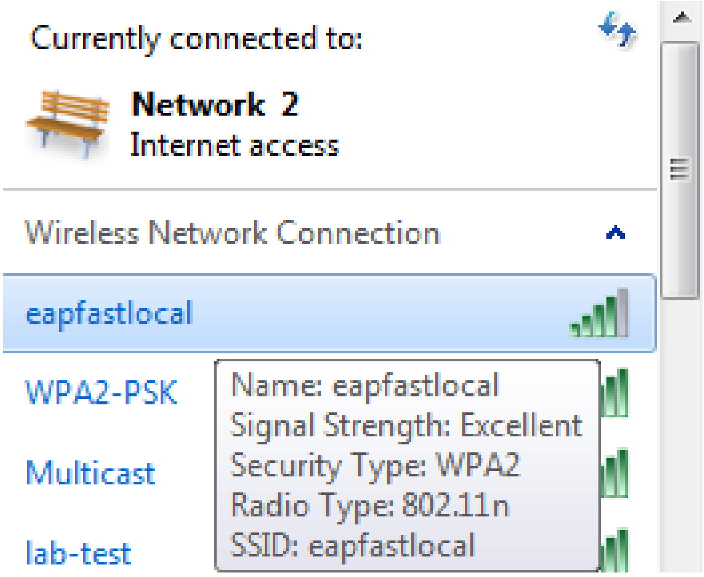
Local EAP Authentication ☑

EAP Profile Name: eapfast

Verifiëren

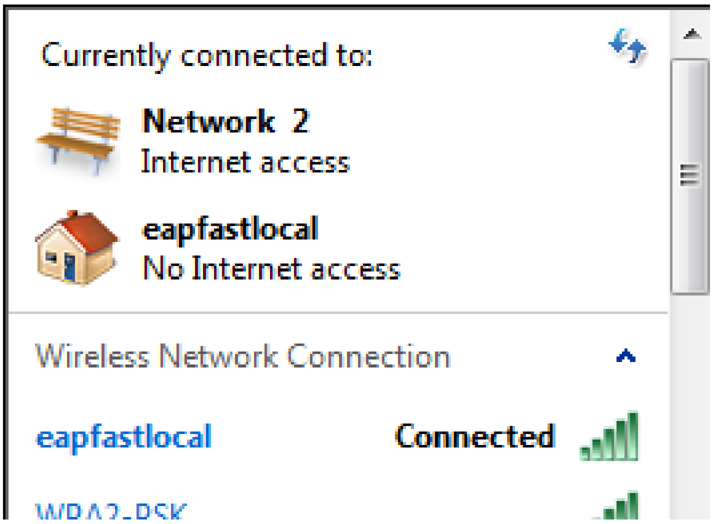
Volg deze stappen om te controleren of de configuratie goed werkt:

1. Sluit de client aan op WLAN:



Name: eapfastlocal
Signal Strength: Excellent
Security Type: WPA2
Radio Type: 802.11n
SSID: eapfastlocal

2. Controleer dat het pop-upvenster Protected Access Credentials (PAC) verschijnt en dat u dit moet accepteren om te authentiseren:



Problemen oplossen

Cisco raadt u aan sporen te gebruiken om draadloze problemen op te lossen. Traces worden opgeslagen in de circulaire buffer en zijn niet processorintensief.

Schakel deze sporen in om de L2 (Layer 2) auth-loggen te verkrijgen:

- **stel een veilig debug van de spoorgroep in**
- **set sporengroep-draadloos beveiligde filterkaart021.6a89.51ca**

Schakel deze sporen in om de DHCP-gebeurtenissen te verkrijgen:

- **dhcp-evenementen op maat instellen**
- **set sporen dhcp gebeurtenissen filter mac 0021.6a89.51ca**

Hier zijn een paar voorbeelden van succesvolle sporen:

```
[04/10/14 18:49:50.719 IST 3 8116] 0021.6a89.51ca Association received from
 mobile on AP  c8f9.f983.4260

[04/10/14 18:49:50.719 IST 4 8116] 0021.6a89.51ca qos upstream policy is
 unknown and downstream policy is unknown
[04/10/14 18:49:50.719 IST 5 8116] 0021.6a89.51ca apChanged 1 wlanChanged 0
 mscb ipAddr 20.20.20.6, apf RadiusOverride 0x0, numIPv6Addr=0
[04/10/14 18:49:50.719 IST 6 8116] 0021.6a89.51ca Applying WLAN policy on MSCB.
[04/10/14 18:49:50.719 IST 7 8116] 0021.6a89.51ca Applying WLAN ACL policies
 to client

[04/10/14 18:49:50.719 IST 9 8116] 0021.6a89.51ca Applying site-specific IPv6
 override for station  0021.6a89.51ca  - vapId 13, site 'default-group',
 interface 'VLAN0020'
[04/10/14 18:49:50.719 IST a 8116] 0021.6a89.51ca Applying local bridging
 Interface Policy for station  0021.6a89.51ca  - vlan 20, interface 'VLAN0020'
[04/10/14 18:49:50.719 IST b 8116] 0021.6a89.51ca STA - rates (8):
 140 18 152 36 176 72 96 108 48 72 96 108 0 0 0 0

[04/10/14 18:49:50.727 IST 2f 8116] 0021.6a89.51ca Session Manager Call Client
```

```
 57ca4000000048, uid 42, capwap id 50b94000000012,Flag 4, Audit-Session ID
 0a6987b253468efb0000002a, method list

[04/10/14 18:49:50.727 IST 30 22] ACCESS-CORE-SM-CLIENT-SPI-NOTF:
 [0021.6a89.51ca, Ca3] Session update from Client[1] for 0021.6a89.51ca,
 ID list 0x00000000
[04/10/14 18:49:50.727 IST 31 22] ACCESS-CORE-SM-CLIENT-SPI-NOTF:
 [0021.6a89.51ca, Ca3]  (UPD): method: Dot1X, method list: none, aaa id:
 0x0000002A
[04/10/14 18:49:50.727 IST 32 22] ACCESS-CORE-SM-CLIENT-SPI-NOTF:
 [0021.6a89.51ca, Ca3]  (UPD): eap profile: eapfast

[04/10/14 18:49:50.728 IST 4b 278] ACCESS-METHOD-DOT1X-DEB:[0021.6a89.51ca,Ca3]
 Posting AUTH_START for 0xF700000A
[04/10/14 18:49:50.728 IST 4c 278] ACCESS-METHOD-DOT1X-DEB:[0021.6a89.51ca,Ca3]
 0xF700000A:entering request state
[04/10/14 18:49:50.728 IST 4d 278] ACCESS-METHOD-DOT1X-NOTF:[0021.6a89.51ca,Ca3]
 Sending EAPOL packet
[04/10/14 18:49:50.728 IST 4e 278] ACCESS-METHOD-DOT1X-INFO:[0021.6a89.51ca,Ca3]
 Platform changed src mac  of EAPOL packet
[04/10/14 18:49:50.728 IST 4f 278] ACCESS-METHOD-DOT1X-INFO:[0021.6a89.51ca,Ca3]
 EAPOL packet sent to client 0xF700000A
[04/10/14 18:49:50.728 IST 50 278] ACCESS-METHOD-DOT1X-DEB:[0021.6a89.51ca,Ca3]
 0xF700000A:idle request action
[04/10/14 18:49:50.761 IST 51 8116] 0021.6a89.51ca 1XA: Received 802.11 EAPOL
 message (len 5) from mobile
[04/10/14 18:49:50.761 IST 52 8116] 0021.6a89.51ca 1XA: Received EAPOL-Start
 from mobile
[04/10/14 18:49:50.761 IST 53 8116] 0021.6a89.51ca 1XA:  EAPOL-Start -
 EAPOL start message from mobile as mobile is in Authenticating state, restart
 authenticating

[04/10/14 18:49:50.816 IST 95 278] ACCESS-METHOD-DOT1X-DEB:[0021.6a89.51ca,Ca3]
 0xF700000A:entering response state
[04/10/14 18:49:50.816 IST 96 278] ACCESS-METHOD-DOT1X-NOTF:[0021.6a89.51ca,Ca3]
 Response sent to the server from 0xF700000A
[04/10/14 18:49:50.816 IST 97 278] ACCESS-METHOD-DOT1X-DEB:[0021.6a89.51ca,Ca3]
 0xF700000A:ignore response action
[04/10/14 18:49:50.816 IST 98 203] Parsed CLID MAC Address = 0:33:106:137:81:202
[04/10/14 18:49:50.816 IST 99 203] AAA SRV(00000000): process authen req
[04/10/14 18:49:50.816 IST 9a 203] AAA SRV(00000000): Authen method=LOCAL

[04/10/14 18:49:50.846 IST 11d 181] ACCESS-CORE-SM-CLIENT-SPI-NOTF:
 [0021.6a89.51ca, Ca3] Session authz status notification sent to Client[1] for
 0021.6a89.51ca with handle FE000052, list 630007B2
[04/10/14 18:49:50.846 IST 11e 181]ACCESS-METHOD-DOT1X-NOTF:[0021.6a89.51ca,Ca3]
 Received Authz Success for the client 0xF700000A (0021.6a89.51ca)
[04/10/14 18:49:50.846 IST 11f 271] ACCESS-METHOD-DOT1X-DEB:[0021.6a89.51ca,Ca3]
 Posting AUTHZ_SUCCESS on Client 0xF700000A
[04/10/14 18:49:50.846 IST 120 271] ACCESS-METHOD-DOT1X-DEB:[0021.6a89.51ca,Ca3]
 0xF700000A:entering authenticated state
[04/10/14 18:49:50.846 IST 121 271]ACCESS-METHOD-DOT1X-NOTF:[0021.6a89.51ca,Ca3]
 EAPOL success packet was sent earlier.

[04/10/14 18:49:50.846 IST 149 8116] 0021.6a89.51ca 1XA:authentication succeeded
[04/10/14 18:49:50.846 IST 14a 8116] 0021.6a89.51ca 1XK: Looking for BSSID
 c8f9.f983.4263  in PMKID cache
[04/10/14 18:49:50.846 IST 14b 8116] 0021.6a89.51ca 1XK: Looking for BSSID
 c8f9.f983.4263  in PMKID cache
[04/10/14 18:49:50.846 IST 14c 8116] 0021.6a89.51ca Starting key exchange with
 mobile - data forwarding is disabled
[04/10/14 18:49:50.846 IST 14d 8116] 0021.6a89.51ca 1XA: Sending EAPOL message
 to mobile, WLAN=13 AP WLAN=13
[04/10/14 18:49:50.858 IST 14e 8116] 0021.6a89.51ca 1XA: Received 802.11 EAPOL
```

```
 message (len 123) from mobile
[04/10/14 18:49:50.858 IST 14f 8116] 0021.6a89.51ca 1XA: Received EAPOL-Key from
 mobile
[04/10/14 18:49:50.858 IST 150 8116] 0021.6a89.51ca 1XK: Received EAPOL-key in
 PTK_START state (msg 2) from mobile
[04/10/14 18:49:50.858 IST 151 8116] 0021.6a89.51ca 1XK: Stopping retransmission
 timer
[04/10/14 18:49:50.859 IST 152 8116] 0021.6a89.51ca 1XA: Sending EAPOL message
 to mobile, WLAN=13 AP WLAN=13
[04/10/14 18:49:50.862 IST 153 8116] 0021.6a89.51ca 1XA: Received 802.11 EAPOL
 message (len 99) from mobile
[04/10/14 18:49:50.862 IST 154 8116] 0021.6a89.51ca 1XA: Received EAPOL-Key from
 mobile
[04/10/14 18:49:50.862 IST 155 8116] 0021.6a89.51ca 1XK: Received EAPOL-key in
 PTKINITNEGOTIATING state (msg 4) from mobile

[04/10/14 18:49:50.863 IST 172 338] [WCDB] wcdb_ffcp_cb: client (0021.6a89.51ca)
 client (0x57ca4000000048): FFCP operation (UPDATE) return code (0)
[04/10/14 18:49:50.914 IST 173 273] dhcp pkt processing routine is called for pak
 with SMAC = 0021.6a89.51ca and SRC_ADDR = 0.0.0.0
[04/10/14 18:49:50.914 IST 174 219] sending dhcp packet outafter processing with
 SMAC = 0021.6a89.51ca and SRC_ADDR = 0.0.0.0
[04/10/14 18:49:50.914 IST 175 256] DHCPD: address 20.20.20.6 mask 255.255.255.0
[04/10/14 18:49:54.279 IST 176 273] dhcp pkt processing routine is called for pak
 with SMAC = 0021.6a89.51ca and SRC_ADDR = 20.20.20.6
[04/10/14 18:49:54.279 IST 177 219] sending dhcp packet outafter processing with
 SMAC = 0021.6a89.51ca and SRC_ADDR = 20.20.20.6
```