Esempio di configurazione di Converged Access serie 5760, 3850 e 3650 WLC EAP-FAST con server RADIUS interno

Sommario

[Introduzione](#)
[Prerequisiti](#)
[Requisiti](#)
[Componenti usati](#)
[Configurazione](#)
[Esempio di rete](#)
[Panoramica della configurazione](#)
[Configurazione del WLC con la CLI](#)
[Configurare il WLC con la GUI](#)
[Verifica](#)
[Risoluzione dei problemi](#)

Introduzione

In questo documento viene descritto come configurare i Cisco Converged Access Controller (WLC) serie 5760, 3850 e 3650 in modo che agiscano come server RADIUS che eseguono Cisco Extensible Authentication Protocol-Flexible Authentication via Secure Protocol (EAP-FAST, in questo esempio) per l'autenticazione dei client.

Per l'autenticazione degli utenti viene in genere utilizzato un server RADIUS esterno, che in alcuni casi non è una soluzione fattibile. In queste situazioni, un WLC ad accesso convergente può fungere da server RADIUS, in cui gli utenti vengono autenticati sul database locale configurato nel WLC. Questa funzionalità è denominata Server RADIUS locale.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti prima di provare la configurazione:

- GUI o CLI di Cisco IOS® con WLC Converged Access serie 5760, 3850 e 3650
- Concetti relativi al protocollo EAP (Extensible Authentication Protocol)
- Configurazione SSID (Service Set Identifier)
- RAGGIO

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e

hardware:

- Cisco serie 5760 WLC release 3.3.2 (Next-Generation Wiring Closet [NGWC])
- Cisco serie 3602 Lightweight Access Point (AP)
- Microsoft Windows XP con Intel PROset Supplicant
- Switch Cisco Catalyst serie 3560

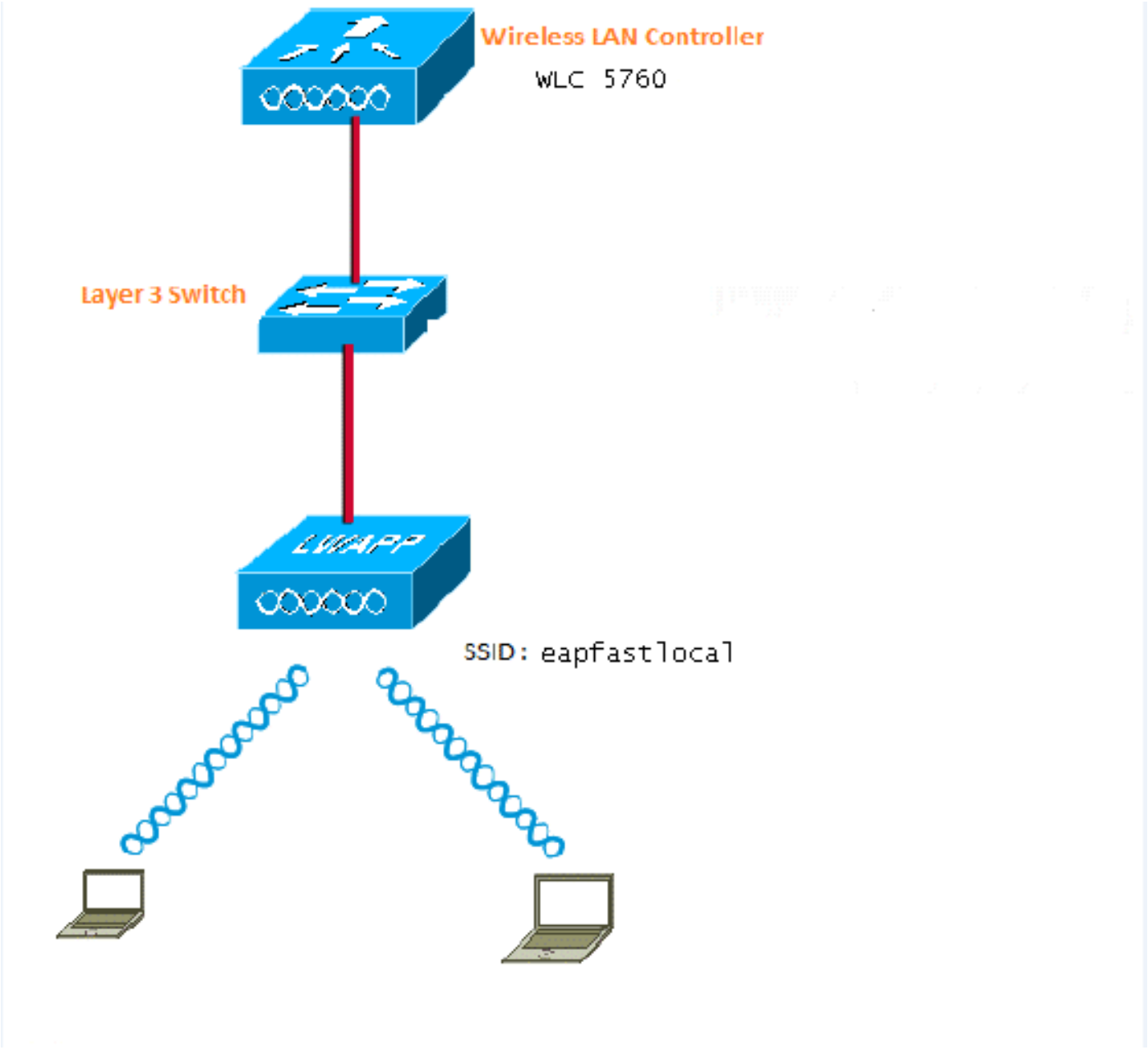
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

> **Nota:** per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento di ricerca dei comandi (solo utenti registrati).

Esempio di rete

L'immagine mostra un esempio di diagramma di rete:



Panoramica della configurazione

Questa configurazione viene completata in due passaggi:

1. Configurare il WLC per il metodo EAP locale e i relativi profili di autenticazione e autorizzazione con la CLI o la GUI.

2. Configurare la WLAN ed eseguire il mapping dell'elenco di metodi che dispone dei profili di autenticazione e autorizzazione.

Configurazione del WLC con la CLI

Completare questi passaggi per configurare il WLC con la CLI:

1. Abilitare il modello AAA sul WLC:

```
aaa new-model
```

2. Definire l'autenticazione e l'autorizzazione:

```
aaa local authentication eapfast authorization eapfast

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

3. Configurare il profilo EAP locale e il metodo (nell'esempio riportato viene utilizzato EAP-FAST):

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

4. Configurare i parametri EAP-FAST avanzati:

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

5. Configurare la WLAN e mappare il profilo di autorizzazione locale alla WLAN:

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

6. Configurare l'infrastruttura per supportare la connettività client:

```
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
```

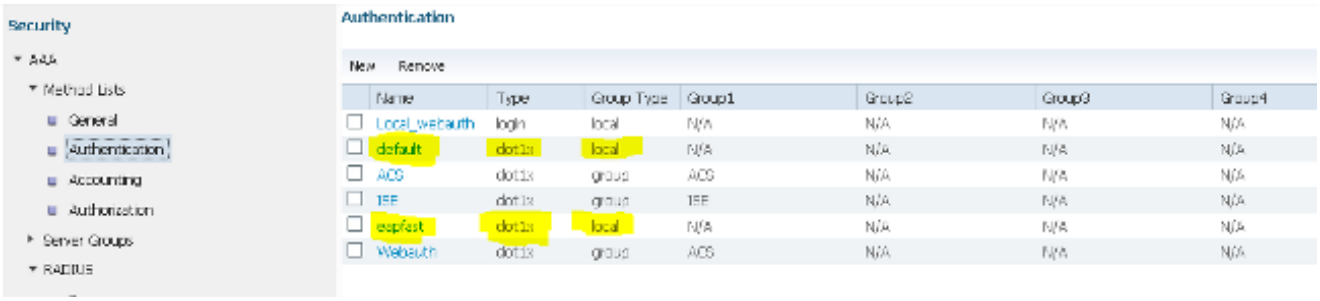
Configurare il WLC con la GUI

Completare questi passaggi per configurare il WLC con la GUI:

1. Configurare l'elenco dei metodi per l'autenticazione:

Configurare **eapfast** Type come **Dot1x**.

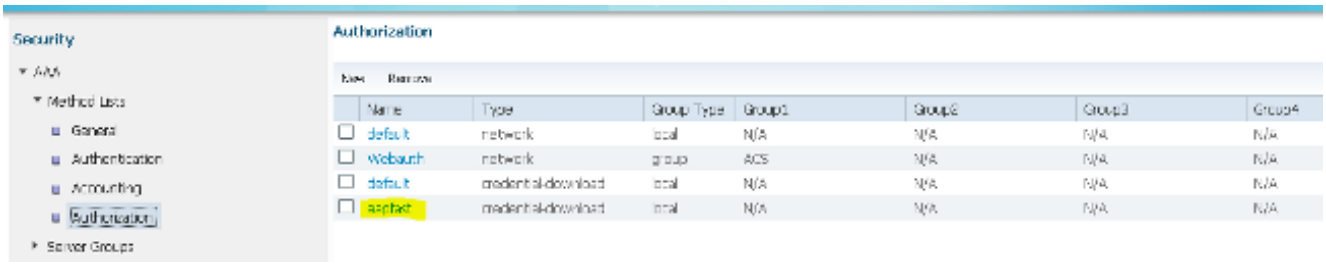
Configurare **eapfast** Group Type come **Local**.



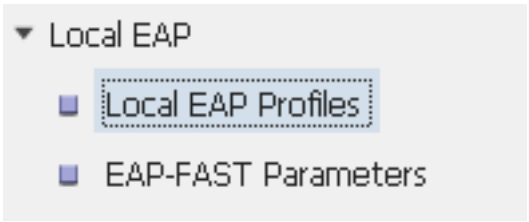
2. Configurare l'elenco dei metodi per Authorization:

Configurare **eapfast** Type come **Credential-Download**.

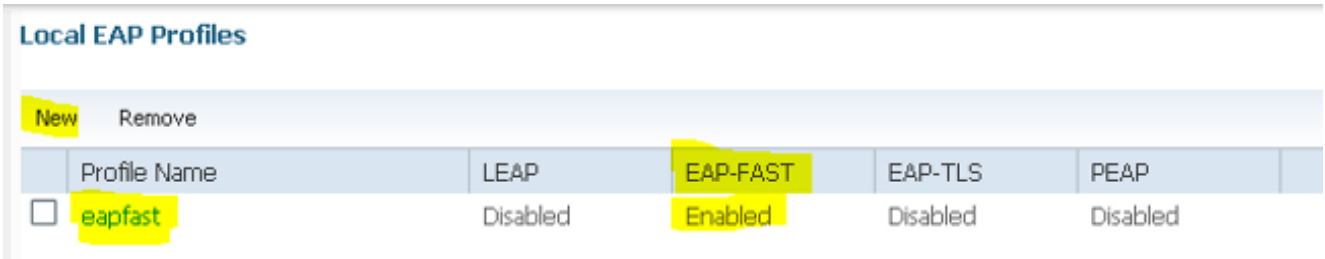
Configurare **eapfast** Group Type come **Local**.



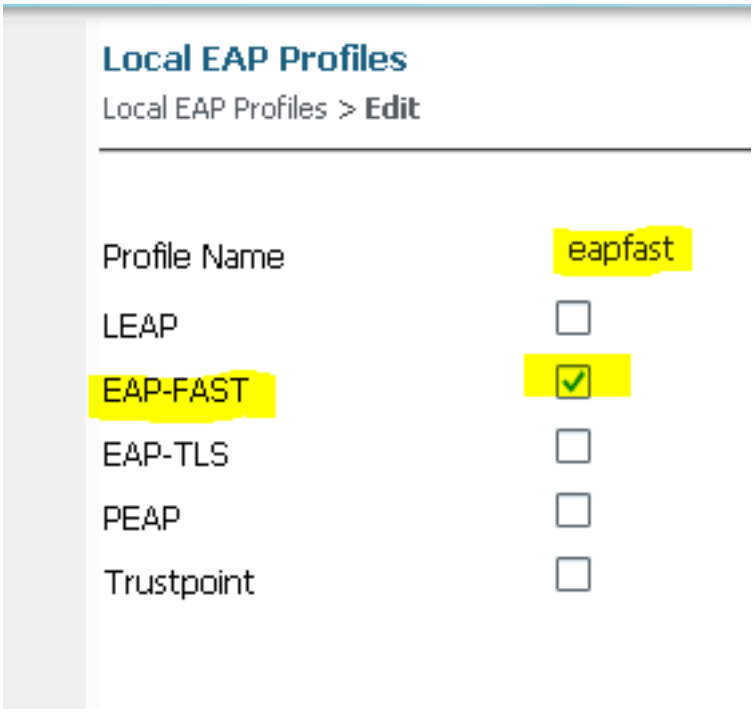
3. Configurare il profilo EAP locale:



4. Creare un nuovo profilo e selezionare il tipo EAP:

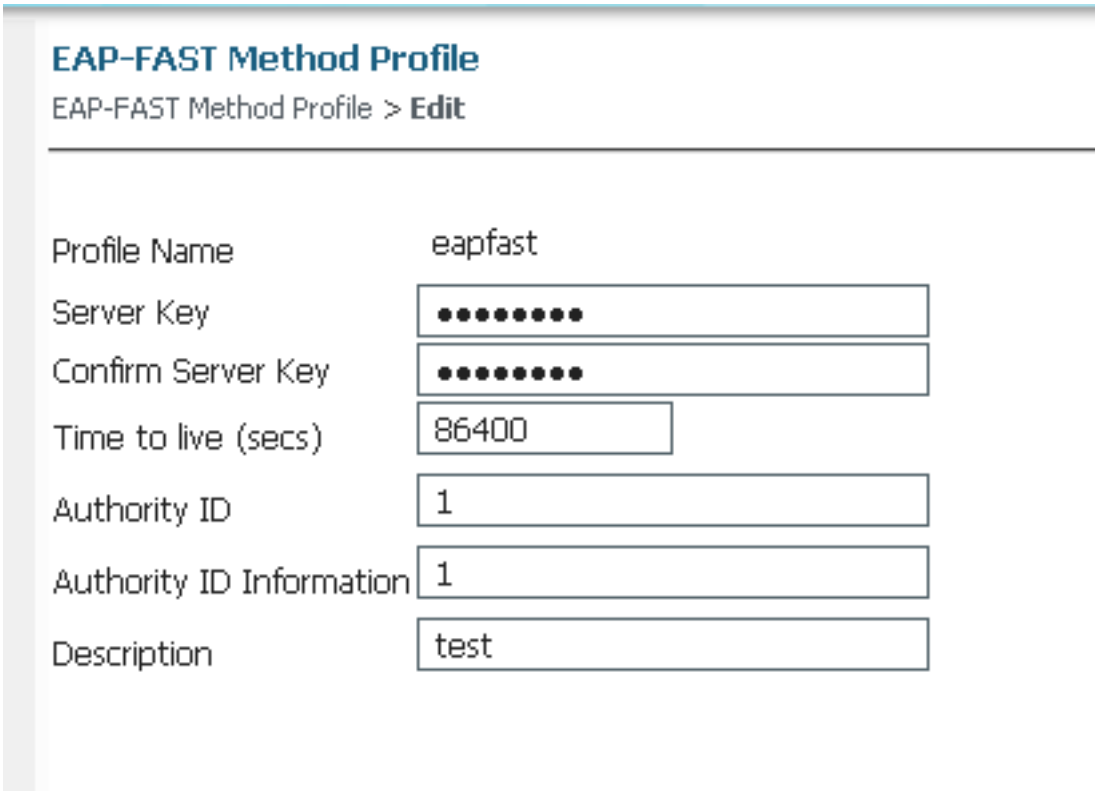


Il nome del profilo è **eapfast** e il tipo EAP selezionato è **EAP-FAST**:

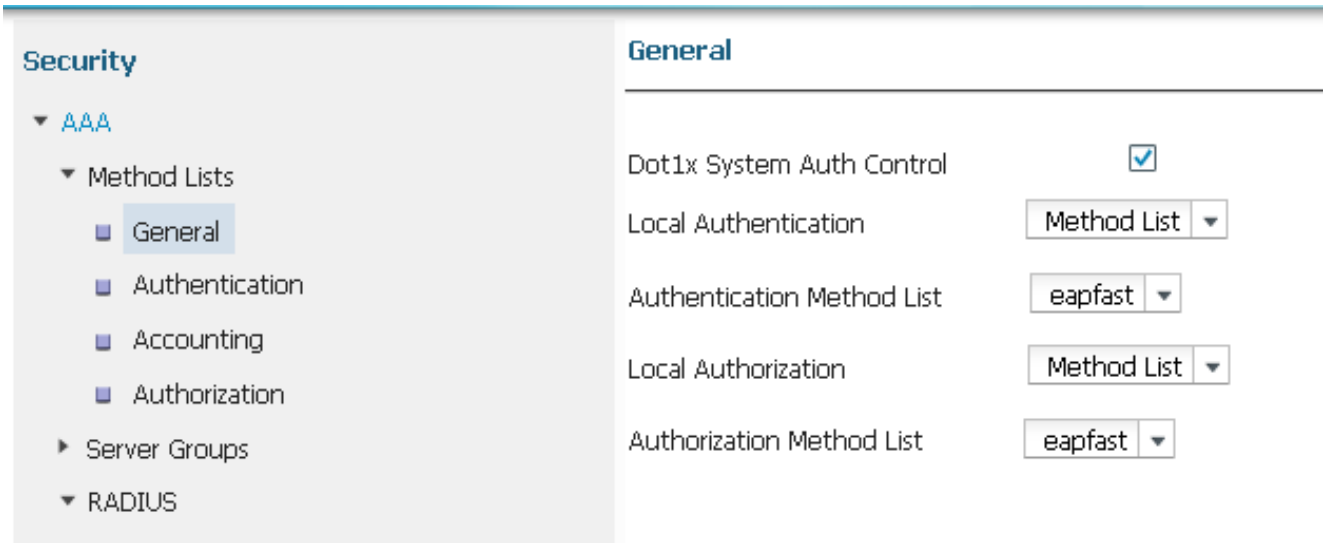


5. Configurare i parametri del metodo EAP-FAST:

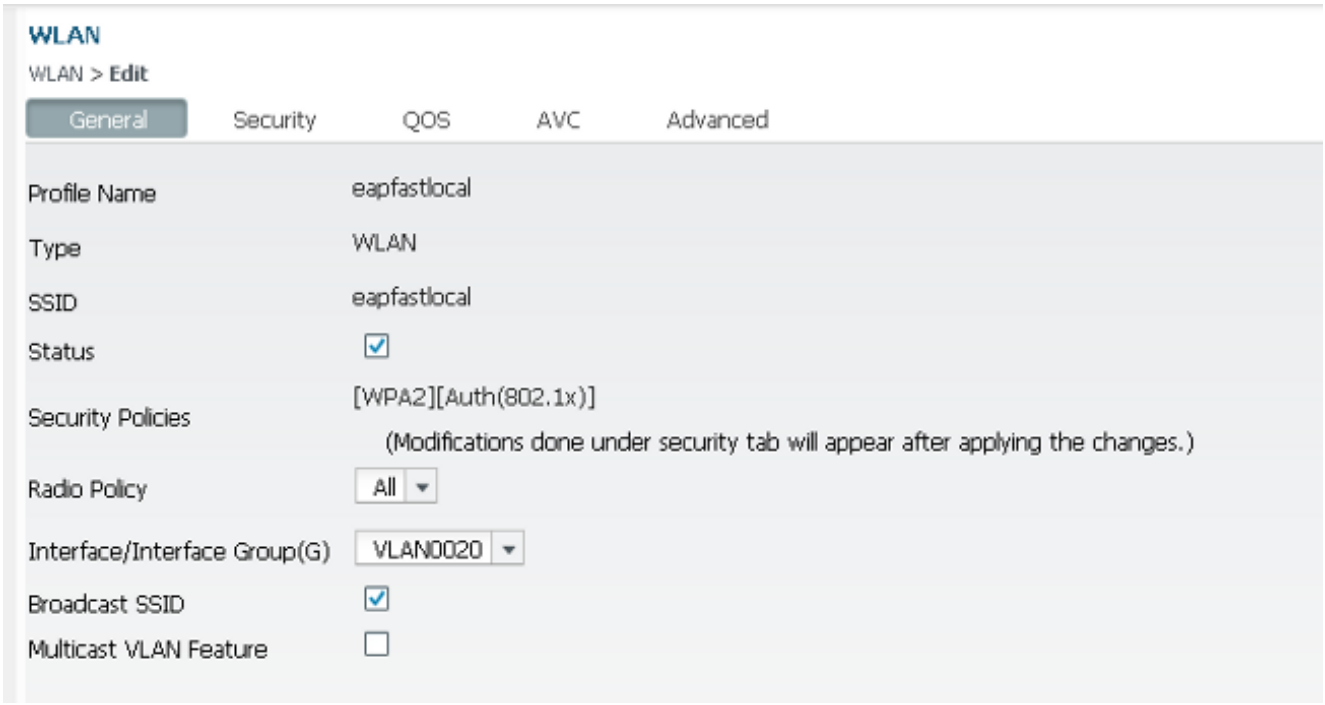
La chiave del server è configurata come **Cisco123**.

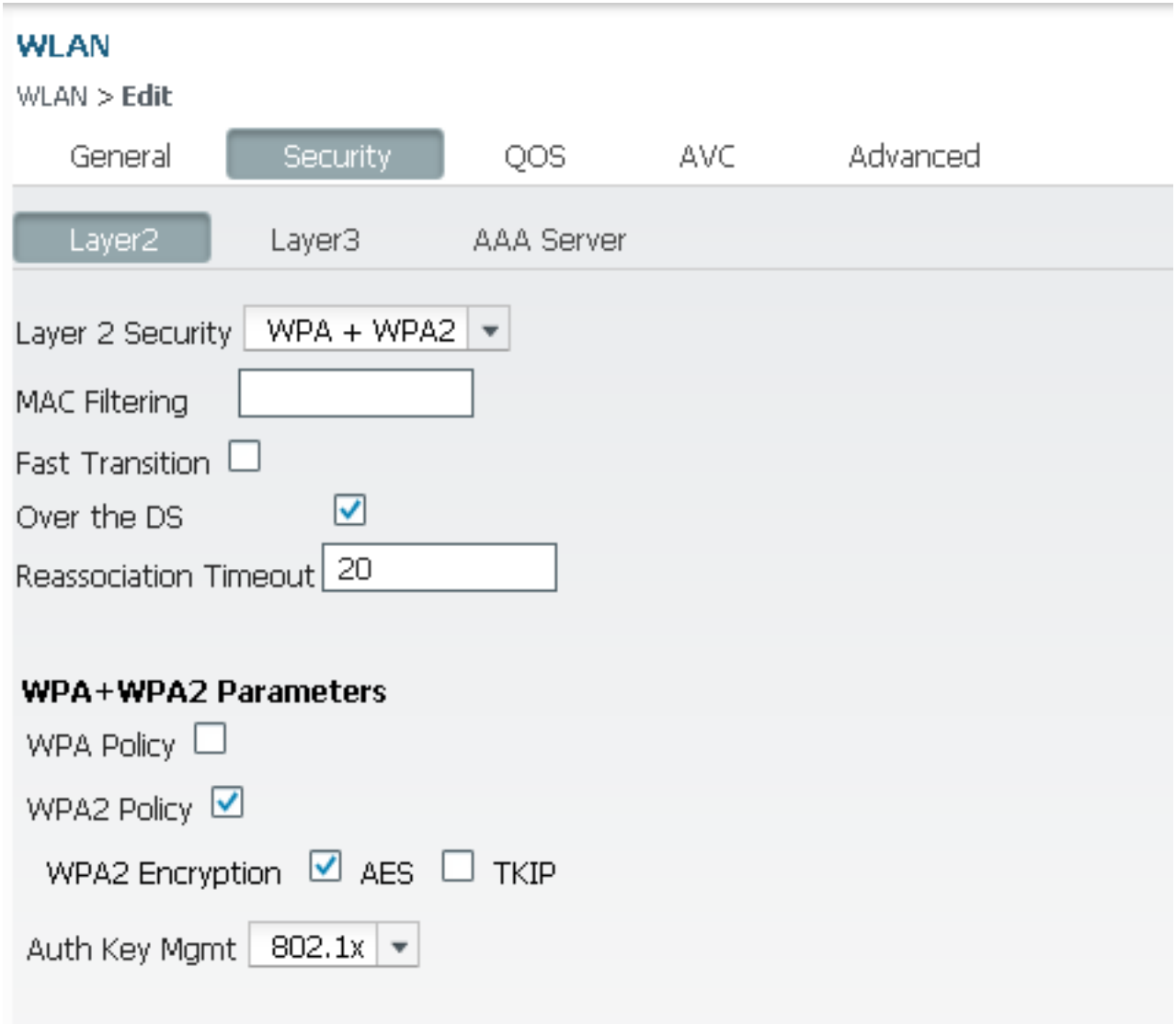


6. Selezionare la casella di controllo **Dot1x System Auth Control** e selezionare **eapfast** per gli elenchi di metodi. Ciò consente di eseguire l'autenticazione EAP locale.

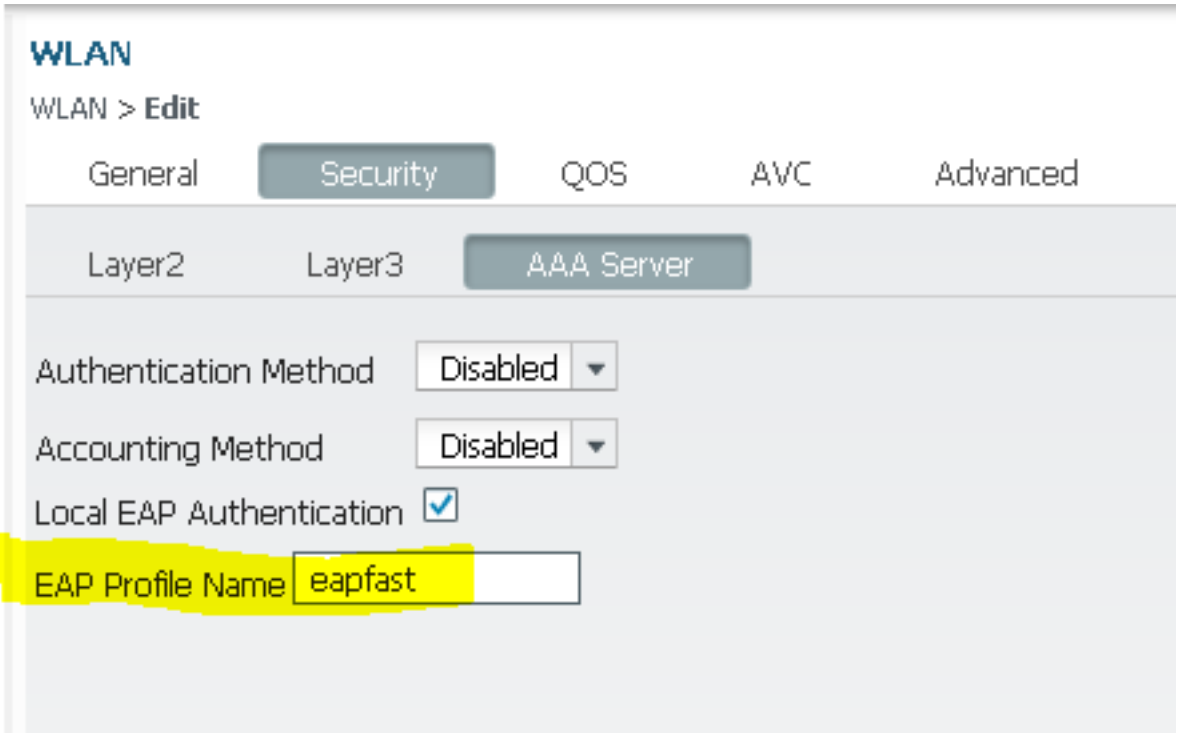


7. Configurare la WLAN per la crittografia AES WPA2:





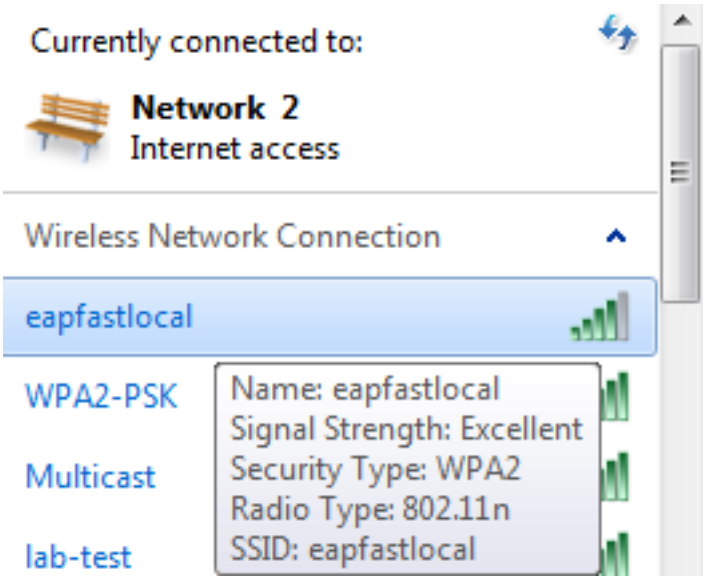
8. Nella scheda **AAA Server**, mappare il nome del profilo EAP **eapfast** alla WLAN:



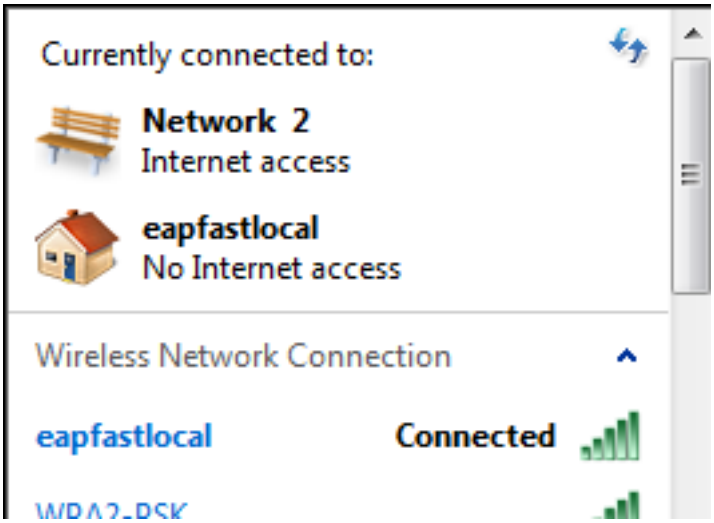
Verifica

Per verificare che la configurazione funzioni correttamente, attenersi alla seguente procedura:

1. Collegare il client alla WLAN:



2. Verificare che venga visualizzato il popup Credenziali di accesso protetto (PAC) e che sia necessario accettare per autenticare correttamente:



Risoluzione dei problemi

Cisco consiglia di utilizzare le tracce per risolvere i problemi relativi alle reti wireless. Le tracce vengono salvate nel buffer circolare e non richiedono un utilizzo intensivo del processore.

Per ottenere i log di autenticazione di layer 2 (L2), abilitare le seguenti tracce:

- **set trace group-wireless-secure level debug**
- **set trace group-wireless-secure filter mac0021.6a89.51ca**

Abilitare queste tracce per ottenere i registri eventi DHCP:

- **set trace dhcp events level debug**
- **set trace dhcp events filter mac 0021.6a89.51ca**

Di seguito sono riportati alcuni esempi di tracce riuscite:

```
[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