

Esempio di configurazione delle modalità operative H-REAP

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Convenzioni](#)

[Premesse](#)

[H-REAP over REAP](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurazione](#)

[Preparazione dell'access point con un controller e configurazione di H-REAP](#)

[Teoria delle operazioni H-REAP](#)

[Stati di switching H-REAP](#)

[Autenticazione centrale, switching centrale](#)

[Verifica dell'autenticazione centrale, switching centrale](#)

[Autenticazione inattiva, Switching inattivo](#)

[Autenticazione centrale, switching locale](#)

[Verifica dell'autenticazione centrale, switching locale](#)

[Autenticazione non attiva, switching locale](#)

[Autenticazione locale, switching locale](#)

[Verifica autenticazione locale, switching locale](#)

[Risoluzione dei problemi](#)

[Informazioni correlate](#)

[Introduzione](#)

In questo documento viene introdotto il concetto di punto di accesso remoto ibrido (H-REAP) e ne vengono illustrate le diverse modalità operative con un esempio di configurazione.

[Prerequisiti](#)

[Requisiti](#)

Prima di provare questa configurazione, accertarsi di soddisfare i seguenti requisiti:

- Conoscenza dei Wireless LAN Controller (WLC) e come configurare i parametri base WLC

- Conoscenza di REAP

Componenti usati

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

- Cisco serie 4400 WLC con firmware versione 7.0.116.0
- Cisco 1131AG Lightweight Access Point (LAP)
- Cisco serie 2800 Router con versione 12.4(11)T.
- Cisco Aironet 802.11a/b/g Client Adapter con firmware versione 4.0
- Cisco Aironet Desktop Utility versione 4.0
- Cisco Secure ACS con versione 4.0

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.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento [Cisco sulle convenzioni nei suggerimenti tecnici](#).

Premesse

H-REAP è una soluzione wireless per le installazioni di filiali e uffici remoti. H-REAP consente ai clienti di configurare e controllare i punti di accesso (AP) in una filiale o in un ufficio remoto dall'ufficio aziendale tramite un collegamento WAN senza implementare un controller in ogni ufficio.

Gli H-REAP possono commutare il traffico di dati client localmente ed eseguire l'autenticazione client localmente quando la connessione al controller viene persa. Quando collegati al controller, gli H-REAP possono anche eseguire il tunnel del traffico verso il controller. In modalità connessa, l'access point ibrido REAP può anche eseguire l'autenticazione locale.

H-REAP è supportato solo su:

- AP 1130AG, 1140, 1240, 1250, 1260, AP801, AP 802, 1040 e AP3550
- Cisco serie 5500, 4400, 2100, 2500 e Flex 7500 Controller
- Catalyst 3750G Integrated Controller Switch
- Catalyst serie 6500 Wireless Services Module (WiSM)
- Wireless LAN Controller Module (WLCM) per ISR (Integrated Services Router)

Il traffico dei client sugli H-REAP può essere commutato localmente sull'access point o tunnelizzato nuovamente su un controller. Ciò dipende dalla configurazione per WLAN. Inoltre, il traffico client a commutazione locale sull'H-REAP può essere contrassegnato con 802.1Q per fornire la separazione tra cavi. Durante l'interruzione della WAN, il servizio su tutte le WLAN con commutazione locale autenticate persiste.

Nota: se gli access point sono in modalità H-REAP e sono commutati localmente sul sito remoto,

l'assegnazione dinamica degli utenti a una VLAN specifica basata sulla configurazione del server RADIUS non è supportata. Tuttavia, è possibile assegnare gli utenti a VLAN specifiche in base al mapping SSID (VLAN to Service Set Identifier) statico eseguito localmente nell'access point. Pertanto, un utente che appartiene a un SSID specifico può essere assegnato a una VLAN specifica a cui è mappato localmente l'SSID nell'access point.

Nota: Se la funzionalità Voice over WLAN è importante, gli access point devono essere eseguiti in modalità locale in modo da poter ricevere il supporto CCKM e CAC (Connection Admission Control), che non sono supportati in modalità H-REAP.

H-REAP over REAP

Per ulteriori informazioni sul protocollo REAP, fare riferimento agli [esempi di configurazione dei Remote-Edge AP \(REAP\) con Lightweight AP e Wireless LAN Controller \(WLC\)](#).

Il protocollo H-REAP è stato introdotto a causa delle seguenti carenze del protocollo REAP:

- Il protocollo REAP non dispone di separazione tra cavi. Ciò è dovuto alla mancanza del supporto 802.1Q. I dati delle WLAN vengono trasmessi sulla stessa subnet cablata.
- In caso di guasto della WAN, un REAP AP cessa il servizio offerto su tutte le WLAN, ad eccezione della prima specificata nel controller.

In questo modo H-REAP riesce a superare le due lacune seguenti:

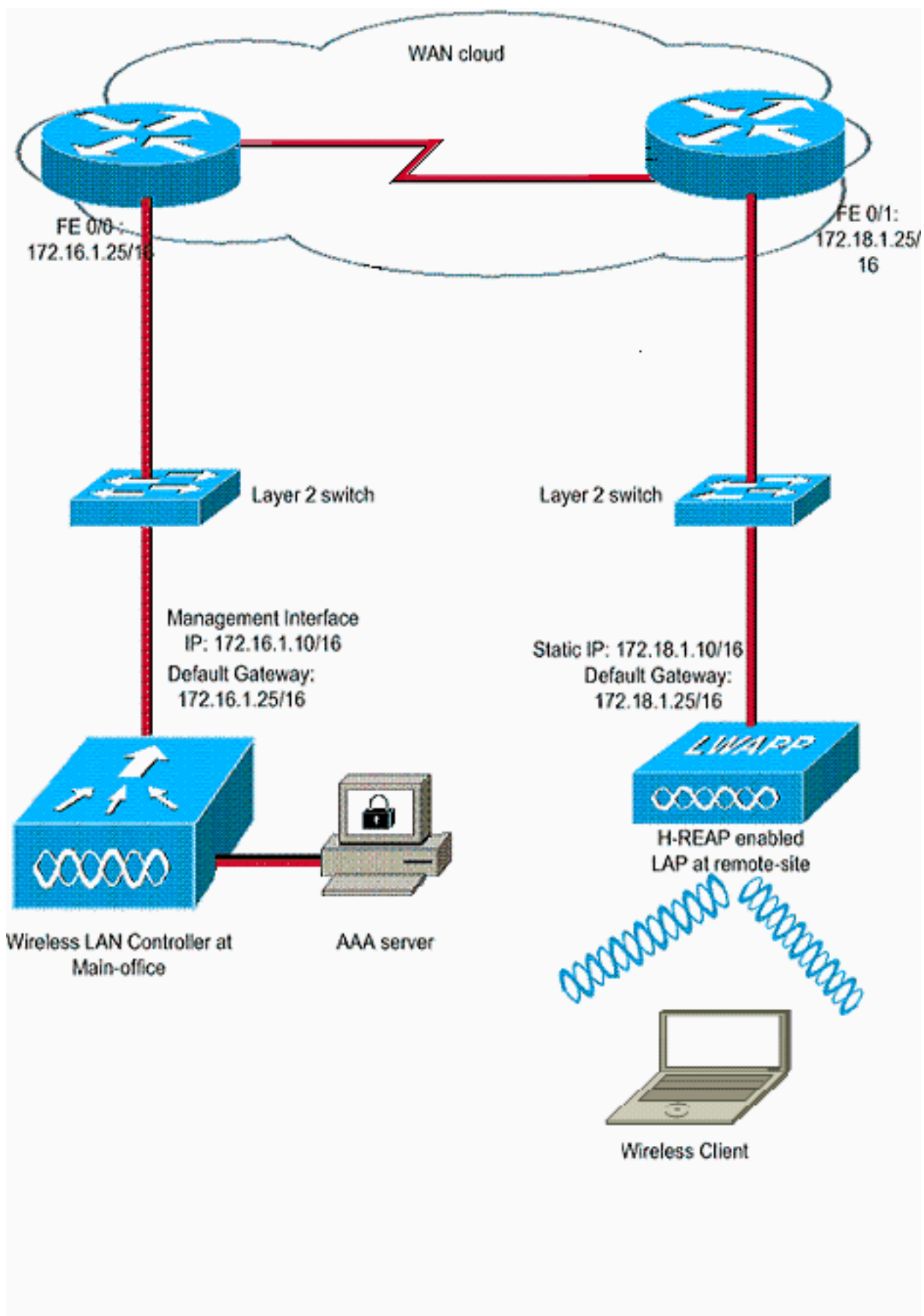
- Fornisce il supporto dot1Q e il mapping tra VLAN e SSID. Il mapping tra VLAN e SSID deve essere eseguito in H-REAP. Mentre si esegue questa operazione, verificare che le VLAN configurate siano consentite correttamente tramite le porte negli switch intermedi e nei router.
- Fornisce un servizio continuo a tutte le WLAN configurate per lo switching locale.

Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

Esempio di rete

Nel documento viene usata questa impostazione di rete:



Configurazione

L'esempio presuppone che il controller sia già configurato con configurazioni di base. Il controller utilizza le seguenti configurazioni:

- Indirizzo IP dell'interfaccia di gestione: 172.16.1.10/16
- Indirizzo IP interfaccia AP-Manager—172.16.1.11/16
- Indirizzo IP predefinito del router gateway: 172.16.1.25/16
- Indirizzo IP del gateway virtuale: 1.1.1.1

Nota: questo documento non mostra le configurazioni WAN e la configurazione dei router e degli switch disponibili tra l'H-REAP e il controller. In questo caso, si presume che l'utente sia a conoscenza dell'incapsulamento WAN e dei protocolli di routing utilizzati. Inoltre, in questo documento si presume che l'utente sia a conoscenza delle modalità di configurazione per mantenere la connettività tra l'H-REAP e il controller tramite il collegamento WAN. Nell'esempio, l'incapsulamento HDLC viene usato sul collegamento WAN.

[Preparazione dell'access point con un controller e configurazione di H-REAP](#)

Se si desidera che l'access point rilevi un controller da una rete remota in cui i meccanismi di rilevamento CAPWAP non sono disponibili, è possibile utilizzare il priming. Questo metodo consente di specificare il controller a cui l'access point deve connettersi.

Per configurare un access point compatibile con H-REAP, collegarlo alla rete cablata dell'ufficio principale. Durante l'avvio, l'access point compatibile con H-REAP cerca prima di tutto un indirizzo IP per se stesso. Una volta che acquisisce un indirizzo IP tramite un server DHCP, si avvia e cerca un controller per eseguire il processo di registrazione.

Un access point H-REAP può imparare l'indirizzo IP del controller in uno dei modi descritti in [Registrazione di un Lightweight AP \(LAP\) su un Wireless LAN Controller \(WLC\)](#).

Nota: è possibile anche configurare il LAP per rilevare il controller tramite i comandi CLI sull'access point. per ulteriori informazioni, fare riferimento a [H-REAP Controller Discovery using CLI commands](#).

Nell'esempio riportato in questo documento viene usata la procedura dell'opzione DHCP 43 per fare in modo che il punto di accesso H-REAP apprenda l'indirizzo IP del controller. Quindi si unisce al controller, scarica l'immagine software e la configurazione più recenti dal controller e inizializza il collegamento radio. La configurazione scaricata viene salvata nella memoria non volatile per l'utilizzo in modalità standalone.

Dopo aver registrato il LAP sul controller, procedere come segue:

1. Nell'interfaccia utente del controller, scegliere **Wireless>Access Point**. Visualizza il LAP registrato con questo controller.
2. Fare clic sull'access point che si desidera configurare.

AP Name	AP Model	AP MAC	AP Up Time	Admin Status	Operational Status
AP001a.219.a04d	AIR-LAP1131AG-A-K9	00:1e:a2:19:a0:4d	0 d, 00 h 06 m 12 s	Enabled	REG

3. Nella finestra AP>Dettagli, fare clic sulla scheda Alta disponibilità, definire i nomi dei controller che gli AP useranno per registrare, quindi fare clic su **Applica**.

The screenshot shows the Cisco Wireless configuration page for AP001a.a219.ad44. The 'High Availability' tab is selected. The configuration includes:

	Name	Management IP Address
Primary Controller	WLC-4400	172.16.1.10
Secondary Controller		
Tertiary Controller		

AP Failover Priority: Low

È possibile definire fino a tre nomi di controller (primario, secondario e terziario). Gli access point ricercano il controller nell'ordine specificato in questa finestra. Poiché in questo esempio viene utilizzato un solo controller, il controller viene definito come controller primario.

4. Configurare LAP per H-REAP. Per configurare il LAP in modo che funzioni in modalità H-REAP, nella finestra AP>Dettagli, nella scheda Generale, scegliere **AP mode** as H-REAP dal menu a discesa corrispondente. In questo modo il LAP viene configurato per funzionare in modalità H-REAP.

The screenshot shows the Cisco Wireless configuration page for AP001a.a219.ad44. The 'General' tab is selected. The configuration includes:

Field	Value
AP Name	AP001a.a219.ad44
Location	default location
AP MAC Address	00:1a:a2:19:ad:44
Base Radio MAC	00:1a:30:c0:a3:50
Admin Status	Enable
AP Mode	H-REAP
AP Sub Mode	local
Operational Status	
Port Number	

Static IP: 172.18.1.10

Nota: nell'esempio, è possibile notare che l'indirizzo IP dell'access point è stato impostato sulla modalità statica e che l'indirizzo IP statico 172.18.1.10 è stato assegnato. Questa assegnazione viene eseguita perché si tratta della subnet da utilizzare nell'ufficio remoto.

Pertanto, è possibile utilizzare l'indirizzo IP del server DHCP, ma solo durante la prima fase della registrazione. Dopo aver registrato l'access point sul controller, è possibile modificare l'indirizzo in un indirizzo IP statico.

Dopo aver avviato il LAP con il controller e averlo configurato per la modalità H-REAP, il passaggio successivo consiste nella configurazione di H-REAP sul lato del controller e nella descrizione degli stati di commutazione H-REAP.

Teoria delle operazioni H-REAP

Il LAP compatibile con H-REAP opera in queste due diverse modalità:

- **Modalità connessa:** Un punto di accesso H-REAP si trova in modalità di connessione quando il relativo control plane CAPWAP collegato al WLC è attivo e operativo. Ciò significa che il collegamento WAN tra il LAP e il WLC non è attivo.
- **Modalità standalone:** Un H-REAP si dice essere in modalità standalone quando il suo collegamento WAN al WLC è inattivo. Ad esempio, quando questo H-REAP non ha più connettività al WLC connesso tramite il collegamento WAN.

Il meccanismo di autenticazione utilizzato per autenticare un client può essere definito come **centrale** o **locale**.

- **Autenticazione centrale:** si riferisce al tipo di autenticazione che implica il processo del WLC dal sito remoto.
- **Autenticazione locale:** si riferisce ai tipi di autenticazione che non comportano alcuna elaborazione dal WLC per l'autenticazione.

Nota: tutta l'autenticazione 802.11 e l'elaborazione delle associazioni avvengono in H-REAP, indipendentemente dalla modalità in cui si trova il LAP. In modalità connessa, H-REAP inoltra quindi queste associazioni e autenticazioni al WLC. In modalità standalone, il LAP non può informare il WLC di tali eventi.

Quando un client si connette a un punto di accesso H-REAP, inoltra tutti i messaggi di autenticazione al controller. Una volta completata l'autenticazione, i pacchetti di dati vengono quindi commutati localmente o sottoposti a tunneling verso il controller. Ciò è conforme alla configurazione della WLAN a cui è connesso.

Con H-REAP, le WLAN configurate su un controller possono funzionare in due modalità diverse:

- **Switching centrale:** Una WLAN su H-REAP funziona in modalità di switching centrale se il traffico di dati della WLAN è configurato per essere tunneling sul WLC.
- **Switching locale:** Una WLAN su H-REAP funziona in modalità switching locale se il traffico di dati di tale WLAN termina localmente sull'interfaccia cablata del LAP stesso, senza essere tunneling sul WLC. **Nota:** solo le WLAN da 1 a 8 possono essere configurate per lo switching locale H-REAP perché solo queste WLAN possono essere applicate ai punti di accesso serie 1130, 1240 e 1250 che supportano la funzionalità H-REAP.

Stati di switching H-REAP

In combinazione con le modalità di autenticazione e commutazione di cui alla sezione precedente, un H-REAP può funzionare in uno dei seguenti stati:

- [Autenticazione centrale, switching centrale](#)
- [Autenticazione inattiva, Switching inattivo](#)
- [Autenticazione centrale, switching locale](#)
- [Autenticazione non attiva, switching locale](#)
- [Autenticazione locale, switching locale](#)

[Autenticazione centrale, switching centrale](#)

In questo stato, per la WLAN specificata, l'access point inoltra tutte le richieste di autenticazione del client al controller e tunnel tutti i dati del client al WLC. Questo stato è valido solo quando H-REAP è in modalità connessa. Qualsiasi rete WLAN configurata per funzionare in questa modalità viene persa durante l'interruzione della rete WAN, indipendentemente dal metodo di autenticazione utilizzato.

In questo esempio vengono utilizzate le impostazioni di configurazione seguenti:

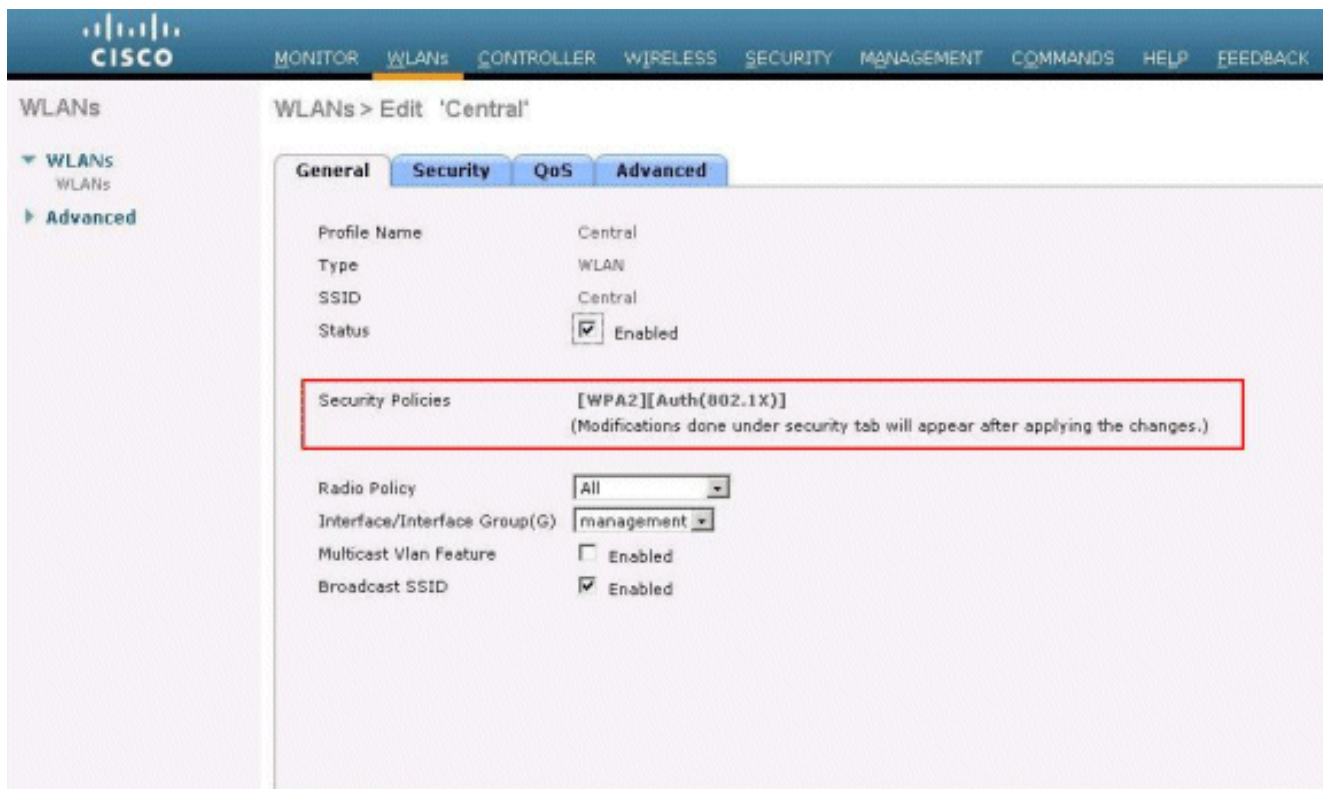
- Nome WLAN/SSID: **Centrale**
- Sicurezza di livello 2: **WPA2**
- Switching locale H-REAP: **disattivato**

Completare questi passaggi per configurare il WLC per l'autenticazione centrale e la commutazione centrale con l'interfaccia utente:

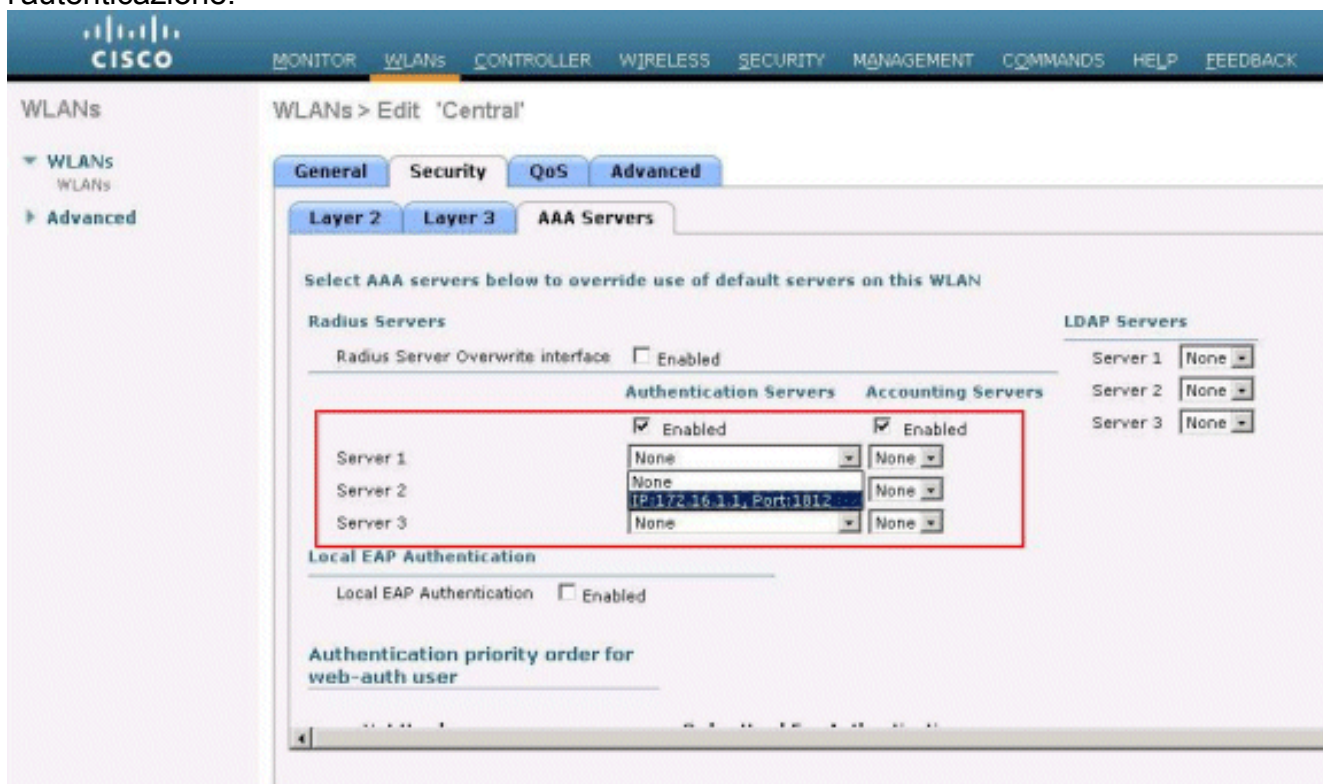
1. Fare clic su **WLAN** per creare una nuova WLAN denominata **Central**, quindi fare clic su **Apply** (Applica).



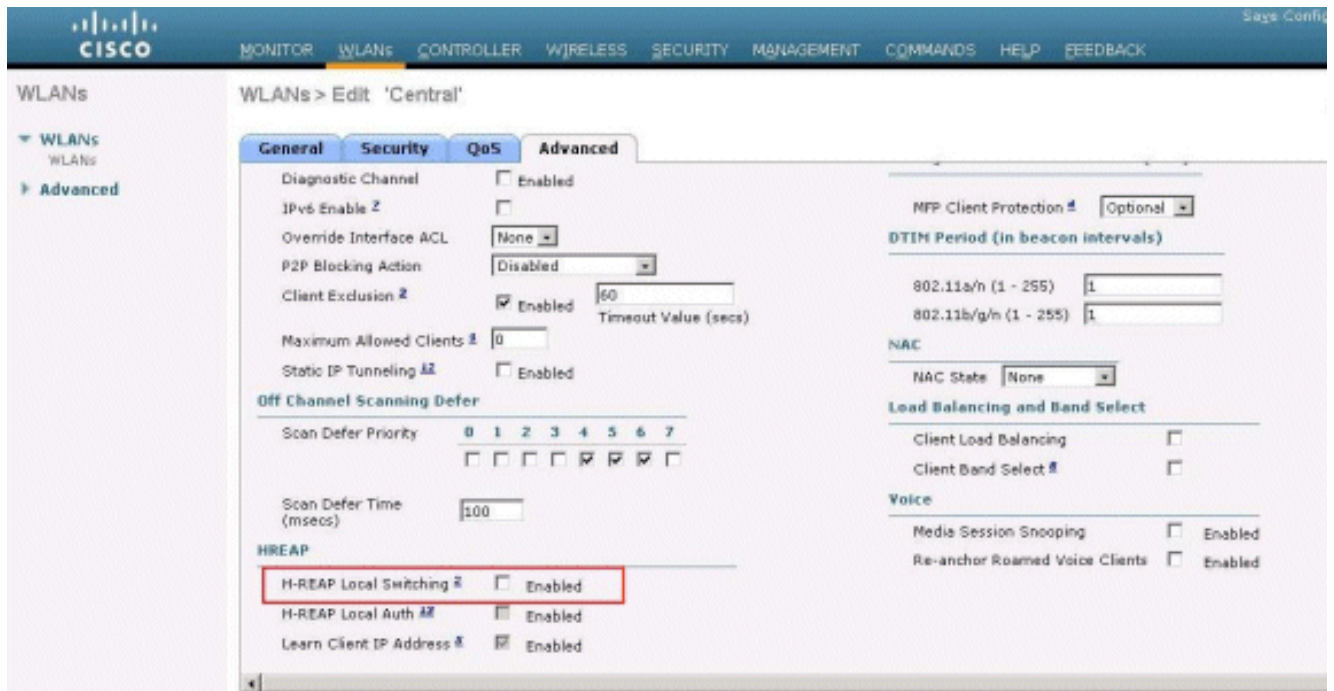
2. Poiché questa WLAN utilizza l'autenticazione centrale, nel campo Sicurezza di layer 2 viene utilizzata l'autenticazione WPA2. WPA2 è la sicurezza predefinita di layer 2 per una WLAN.



3. Selezionare la scheda Server AAA, quindi scegliere il server appropriato configurato per l'autenticazione.



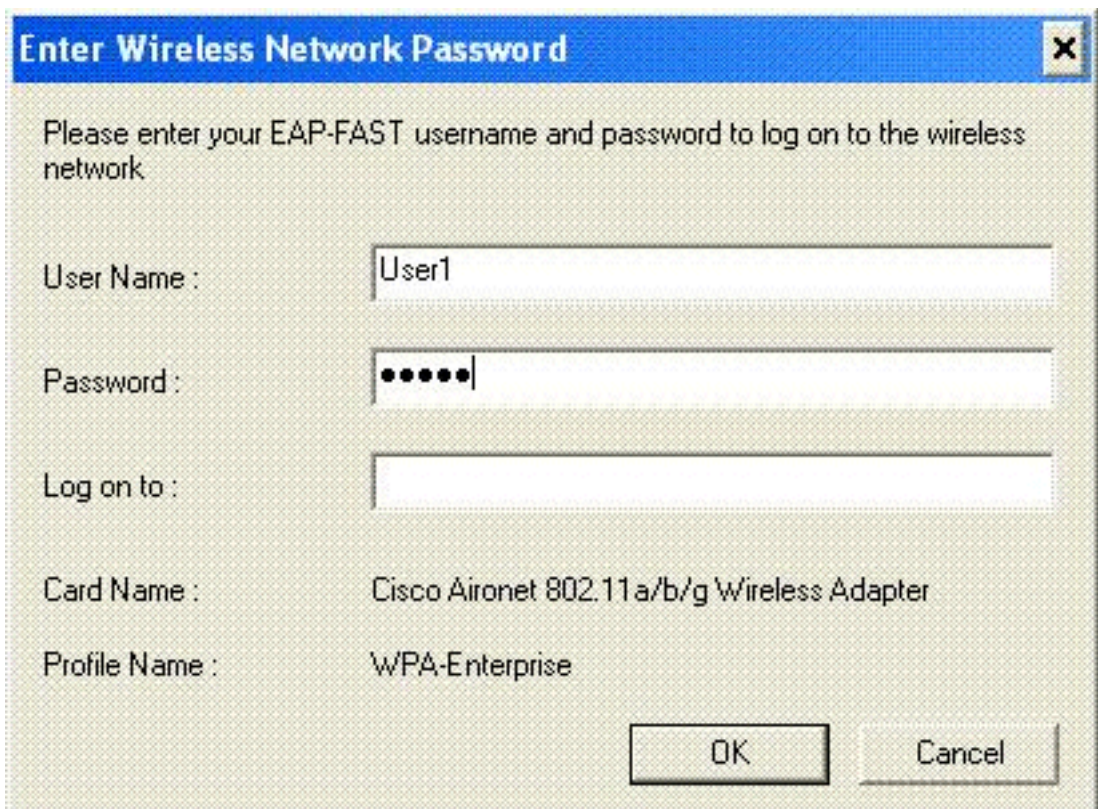
4. Poiché la WLAN utilizza la commutazione centrale, è necessario verificare che la casella di controllo H-REAP Local Switching sia disabilitata (ossia che la casella di controllo Local Switching non sia selezionata). Quindi fare clic su **Apply** (Applica).



Verifica dell'autenticazione centrale, switching centrale

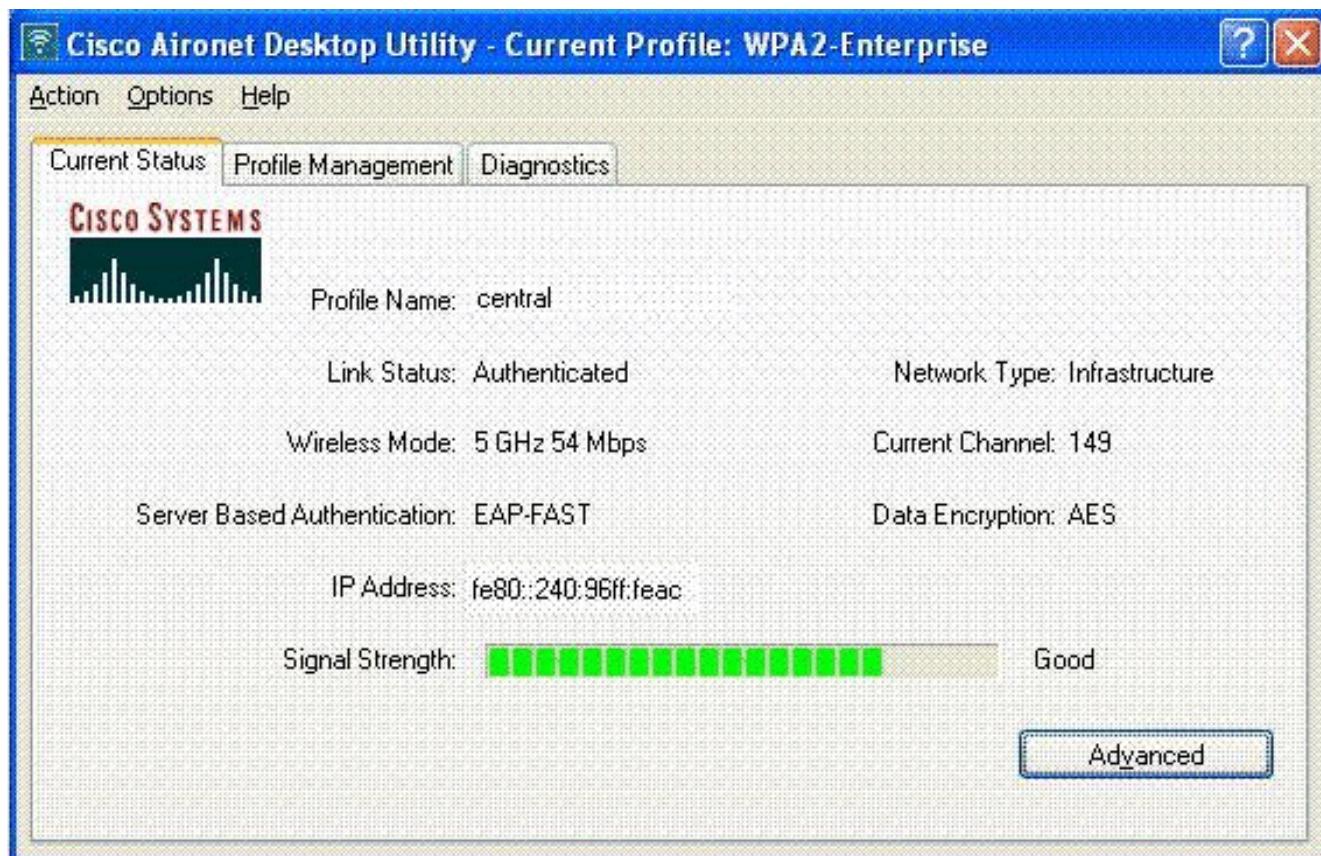
Attenersi alla seguente procedura:

1. Configurare il client wireless con gli stessi SSID e configurazioni di sicurezza. In questo esempio, il SSID è *Central* e il metodo di protezione è *WPA2*.
2. Immettere il nome utente e la password configurati nel server RADIUS>User Setup per attivare il SSID centrale nel client. In questo esempio vengono utilizzati *User1* come nome utente e



password.

Il client viene autenticato centralmente dal server RADIUS ed è associato all'access point H-REAP. Il protocollo H-REAP è ora in fase di **autenticazione centralizzata, commutazione centralizzata**.



[Autenticazione inattiva, Switching inattivo](#)

Con la stessa configurazione spiegata nella sezione [Autenticazione centrale, switching centrale](#), disabilitare il collegamento WAN che connette il controller. Ora il controller attende una risposta heartbeat dall'access point. Una risposta heartbeat è simile ai messaggi keepalive. Il controller prova cinque heartbeat consecutivi, ciascuno al secondo.

Poiché non viene ricevuta con una risposta heartbeat da parte dell'H-REAP, il WLC annulla la registrazione del LAP.

Per verificare il processo di annullamento della registrazione, usare il comando **debug capwap events enable** dalla CLI del WLC. Di seguito viene riportato l'output di esempio del comando **debug**:

```
Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 Did not receive heartbeat reply from AP 00:15:c7:ab:55:90
Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 apfSpamProcessStateChangeInSpamContext: Down capwap event for AP 00:15:c7:ab:55:90 slot 0
Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 apfSpamProcessStateChangeInSpamContext: Deregister capwap event for AP 00:15:c7:ab:55:90 slot 0
Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 apfSpamProcessStateChangeInSpamContext: Down capwap event for AP 00:15:c7:ab:55:90 slot 1
Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 apfSpamProcessStateChangeInSpamContext: Deregister capwap event for AP 00:15:c7:ab:55:90 slot 1
Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 Received capwap Down event for AP 00:15:c7:ab:55:90 slot 0!
Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 Deregister capwap event for AP 00:15:c7:ab:55:90 slot 0
Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 Received capwap Down event for AP 00:15:c7:ab:55:90 slot 1!
Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 Deregister capwap event for AP 00:15:
```

H-REAP entra in modalità standalone.

Poiché in precedenza questa WLAN era autenticata a livello centrale e commutata a livello centrale, il controllo e il traffico dati sono stati ricollegati al controller. Pertanto, senza il controller, il client non è in grado di mantenere l'associazione con l'H-REAP e viene disconnesso. Questo stato di H-REAP in cui sia l'associazione che l'autenticazione del client sono inattive viene indicato come Autenticazione inattiva, commutazione inattiva.

Autenticazione centrale, switching locale

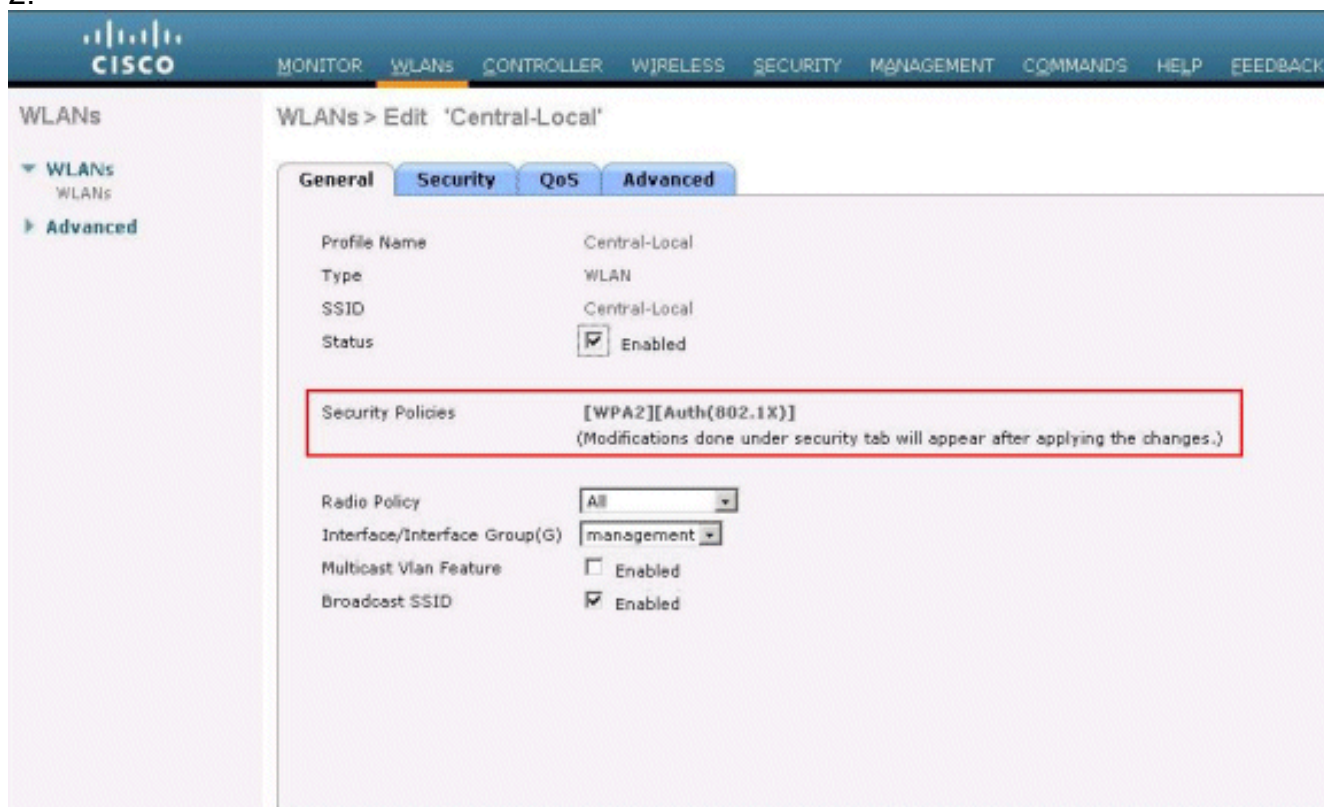
In questo stato, per la WLAN specificata, il WLC gestisce tutte le autenticazioni del client e il LAP H-REAP commuta i pacchetti di dati localmente. Dopo che l'autenticazione del client è riuscita, il controller invia comandi di controllo capwap all'H-REAP e indica al LAP di commutare localmente i pacchetti di dati del client. Questo messaggio viene inviato per client dopo l'autenticazione. Questo stato è applicabile solo in modalità connessa.

In questo esempio vengono utilizzate le impostazioni di configurazione seguenti:

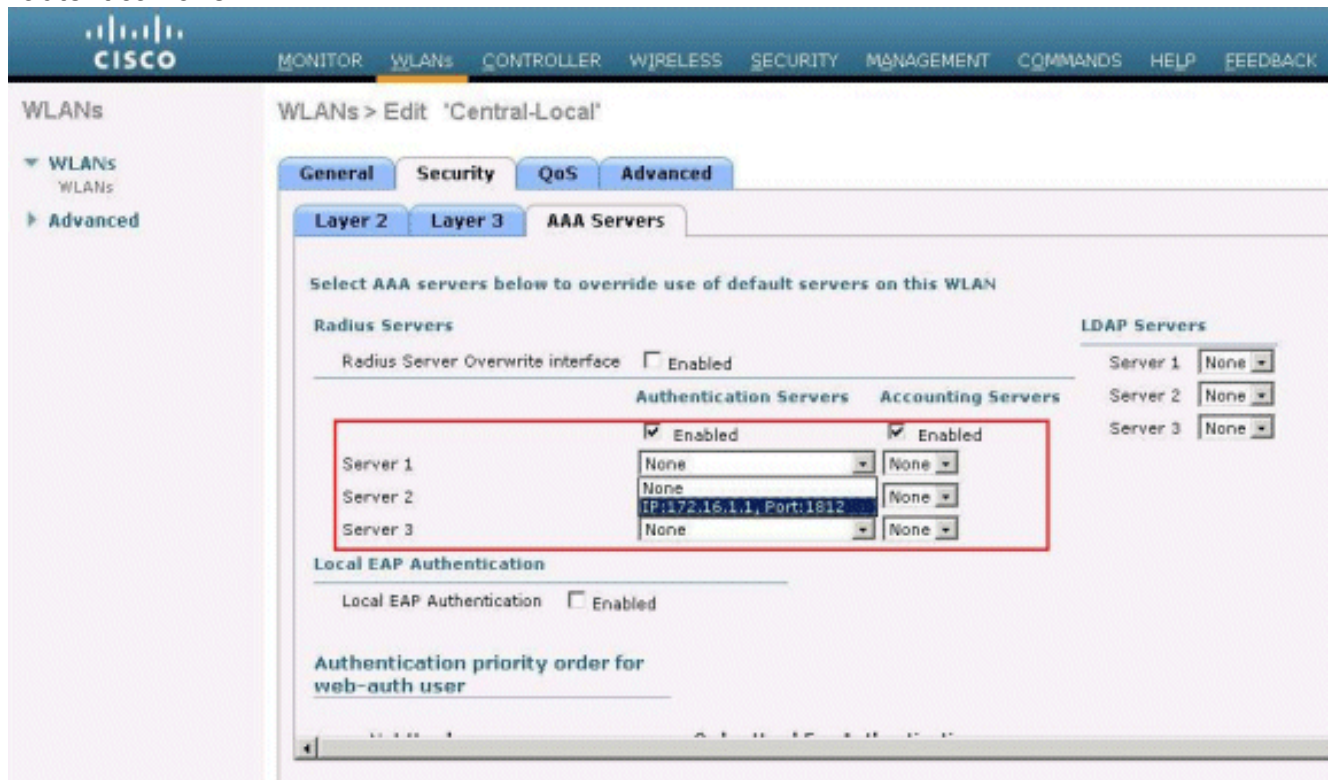
- Nome WLAN/SSID: **Centrale-Locale**
- Sicurezza di livello 2: **WPA2**.
- Switching locale H-REAP: **Attivato**

Dalla GUI del controller, attenersi alla seguente procedura:

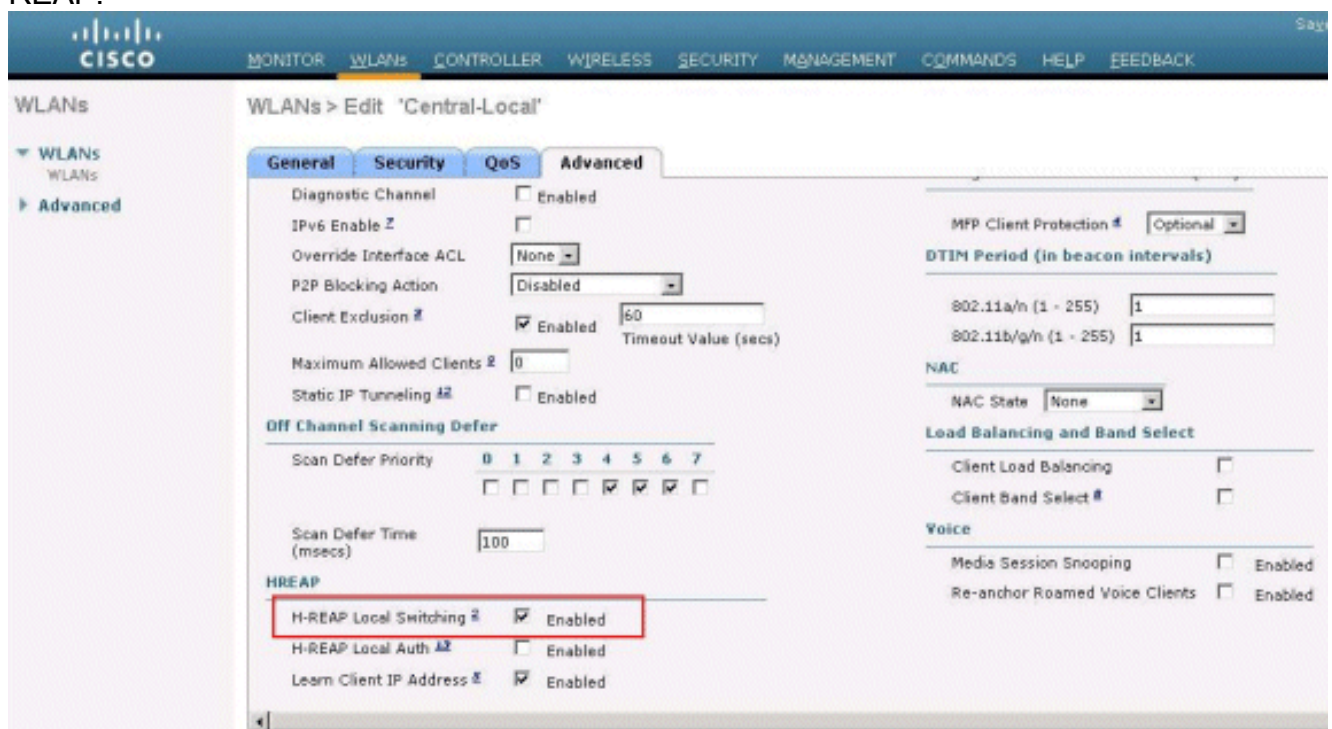
1. Fare clic su **WLAN** per creare una nuova WLAN denominata Central-Local, quindi fare clic su **Apply** (Applica).
2. Poiché la WLAN utilizza l'autenticazione centrale, scegliere l'autenticazione **WPA2** nel campo Sicurezza di layer 2.



3. Nella sezione Server Radius scegliere il server appropriato configurato per l'autenticazione.



4. Selezionare la casella di controllo H-REAP Local Switching per commutare il traffico client che appartiene a questa WLAN localmente sull'H-REAP.




[Verifica dell'autenticazione centrale, switching locale](#)

Attenersi alla seguente procedura:

1. Configurare il client wireless con gli stessi SSID e configurazioni di sicurezza. Nell'esempio, il SSID è *Central-Local* e il metodo di protezione è *WPA2*.

2. Immettere il nome utente e la password configurati nel server RADIUS>User Setup per attivare il SSID locale centrale nel client. In questo esempio vengono utilizzati *User1* come nome utente e



Enter Wireless Network Password

Please enter your EAP-FAST username and password to log on to the wireless network.

User Name : User1

Password : ●●●●●●

Log on to :

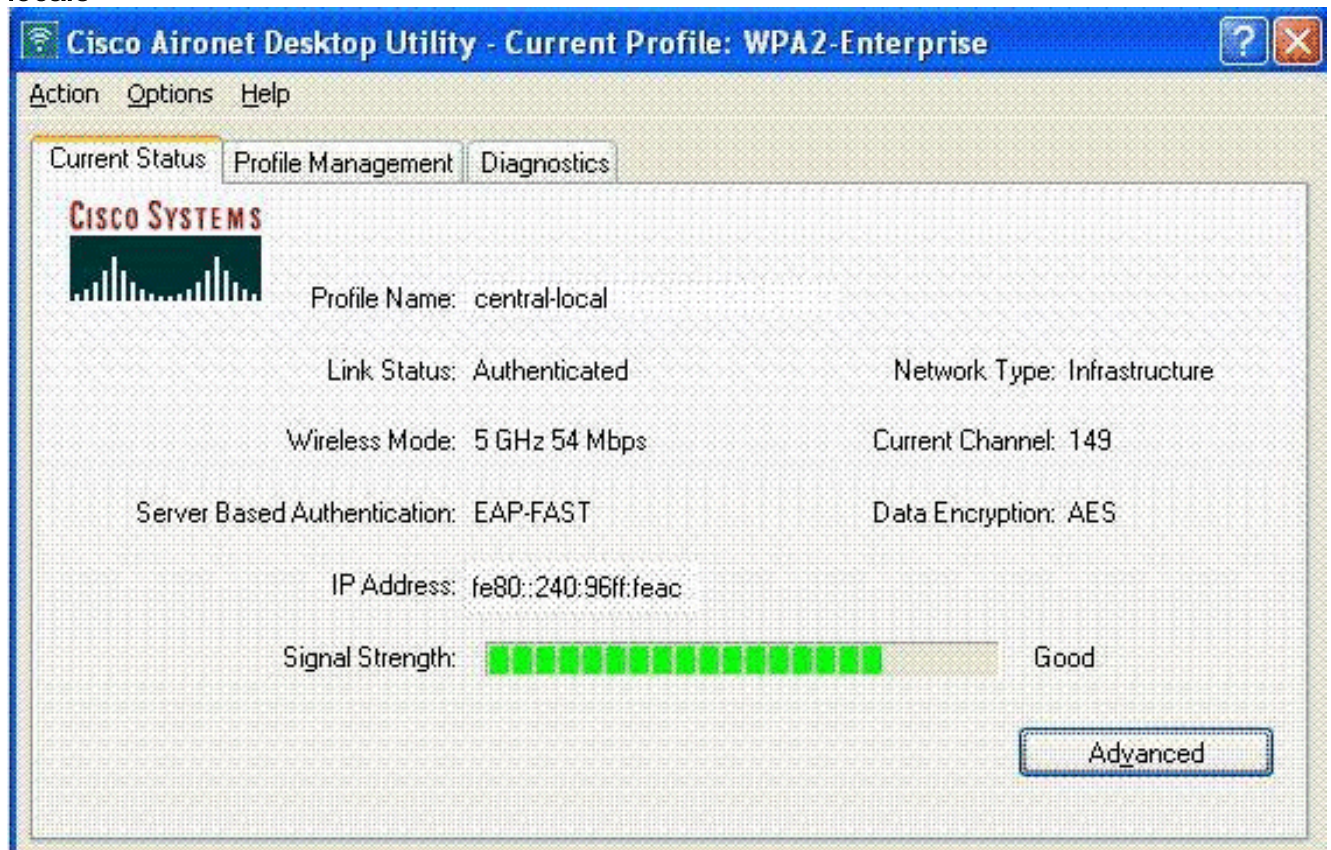
Card Name : Cisco Aironet 802.11 a/b/g Wireless Adapter

Profile Name : WPA-Enterprise

OK Cancel

password.

3. Fare clic su **OK**. Il client viene autenticato centralmente dal server RADIUS e viene associato all'access point H-REAP. Il protocollo H-REAP è ora in modalità di **autenticazione centrale, commutazione locale**.



Cisco Aironet Desktop Utility - Current Profile: WPA2-Enterprise

Action Options Help

Current Status Profile Management Diagnostics

CISCO SYSTEMS

Profile Name: central-local

Link Status: Authenticated Network Type: Infrastructure

Wireless Mode: 5 GHz 54 Mbps Current Channel: 149

Server Based Authentication: EAP-FAST Data Encryption: AES

IP Address: fe80::240:96ff:feac

Signal Strength: Good

Advanced

Autenticazione non attiva, switching locale

Se una WLAN a commutazione locale è configurata per un tipo di autenticazione che deve essere elaborato sul WLC (come l'autenticazione EAP [dynamic WEP/WPA/WPA2/802.11i], WebAuth o NAC), in caso di errore della WAN, entra nello stato di **autenticazione inattiva**. In questo stato, per la WLAN specificata, l'H-REAP rifiuta qualsiasi nuovo client che tenti di autenticarsi. Tuttavia, continua a inviare beacon e risposte probe per mantenere la corretta connessione dei client esistenti. Questo stato è valido solo in modalità autonoma.

Per verificare questo stato, utilizzare la stessa configurazione descritta nella sezione [Autenticazione centrale, switching locale](#).

Se il collegamento WAN che si connette al WLC è inattivo, il WLC procede all'annullamento della registrazione dell'H-REAP.

Una volta annullata la registrazione, H-REAP entra in modalità standalone.

Il client associato tramite questa WLAN mantiene ancora la connettività. Tuttavia, poiché il controller e l'autenticatore non sono disponibili, H-REAP non consente nuove connessioni da questa WLAN.

È possibile verificare questa condizione attivando un altro client wireless nella stessa WLAN. È possibile che l'autenticazione per il client non riesca e che il client non sia autorizzato ad associarsi.

Nota: quando il numero di client WLAN è uguale a zero, il protocollo H-REAP interrompe tutte le funzioni 802.11 associate e non emette più i beacon per il SSID specificato. In questo modo la WLAN passa allo stato H-REAP successivo, **l'autenticazione viene interrotta, la WLAN viene disattivata**.

Autenticazione locale, switching locale

In questo stato, H-REAP LAP gestisce le autenticazioni dei client e commuta i pacchetti di dati dei client localmente. Questo stato è valido solo in modalità standalone e solo per i tipi di autenticazione che possono essere gestiti localmente nell'access point e che non comportano l'elaborazione del controller

L'autenticazione H-REAP che in precedenza era nello stato di **autenticazione centrale, commutazione locale**, passa a questo stato, a condizione che il tipo di autenticazione configurato possa essere gestito localmente nell'access point. Se l'autenticazione configurata non può essere gestita localmente, ad esempio l'autenticazione 802.1x, in modalità standalone l'autenticazione H-REAP passa alla modalità di **commutazione locale disattivata**.

Di seguito sono riportati alcuni dei più comuni meccanismi di autenticazione che è possibile gestire localmente nel punto di accesso in modalità standalone:

- Open (Aperto)
- Condiviso
- WPA-PSK
- WPA2-PSK

Nota: tutti i processi di autenticazione sono gestiti dal WLC quando l'access point è in modalità

connessa. Mentre il protocollo H-REAP è in modalità standalone, le autenticazioni open, shared e WPA/WPA2-PSK vengono trasferite ai LAP dove avviene l'autenticazione client.

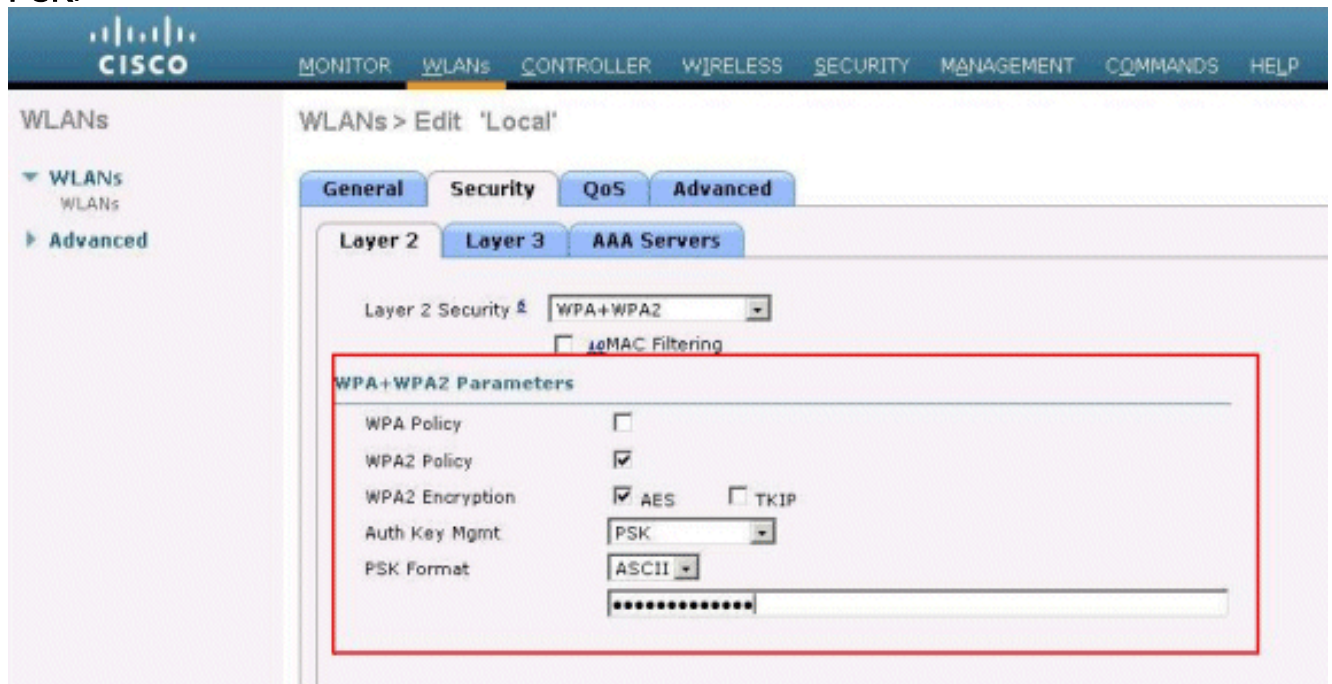
Nota: l'autenticazione Web esterna non è supportata quando si utilizza la tecnologia Hybrid-REAP con la commutazione locale abilitata sulla WLAN.

In questo esempio vengono utilizzate le impostazioni di configurazione seguenti:

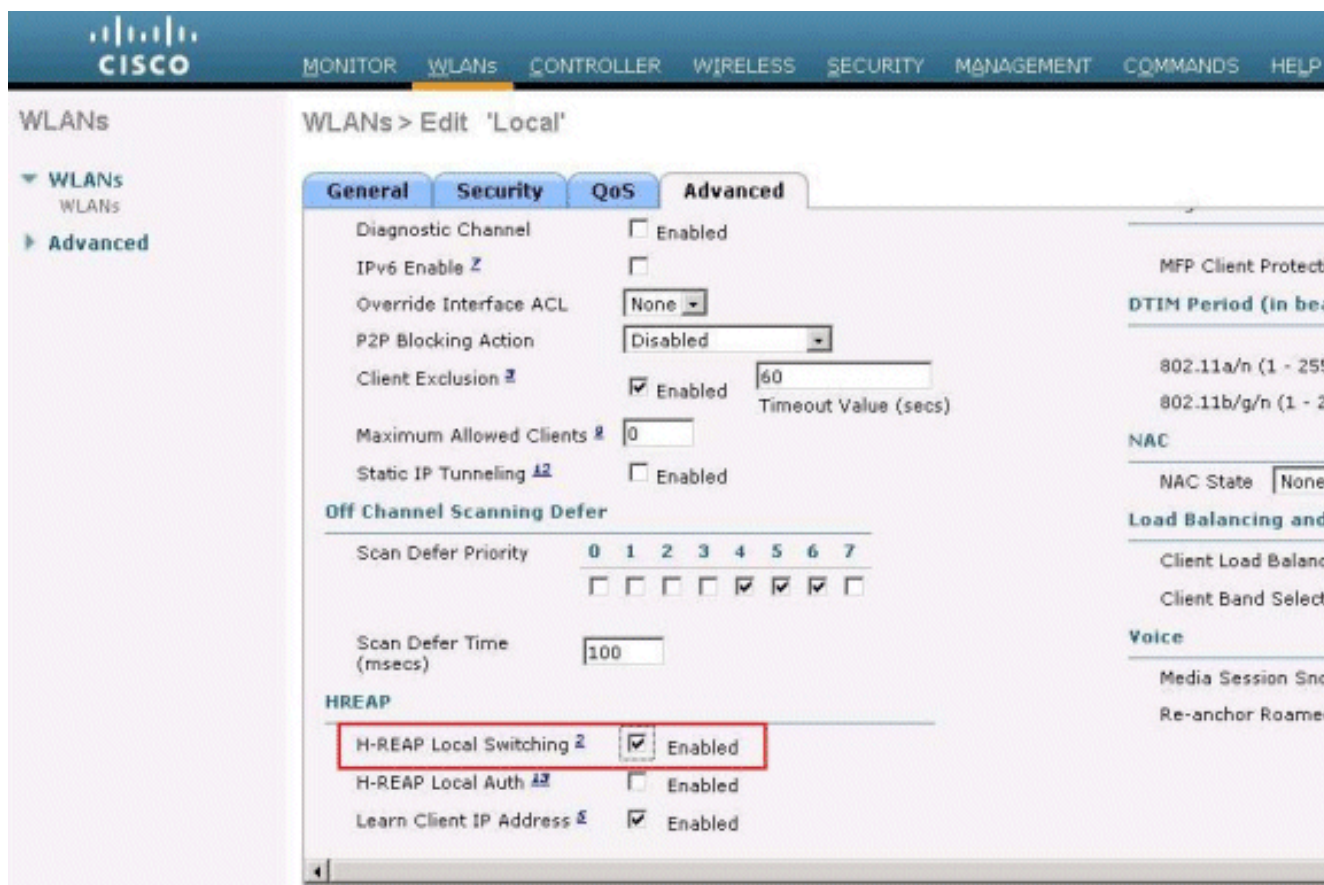
- Nome WLAN/SSID: **Locale**
- Sicurezza di livello 2: **WPA-PSK**
- Switching locale H-REAP: **attivato**

Dalla GUI del controller, attenersi alla seguente procedura:

1. Fare clic su **WLAN** per creare una nuova WLAN denominata Local, quindi fare clic su **Apply** (Applica).
2. Poiché la WLAN utilizza l'autenticazione locale, selezionare **WPA-PSK** o uno dei meccanismi di sicurezza menzionati che possono essere gestiti localmente nel campo Sicurezza di layer 2. In questo esempio viene utilizzato **WPA-PSK**.



3. Una volta scelto, è necessario configurare la chiave/frase di accesso già condivisa da utilizzare. Affinché l'autenticazione abbia esito positivo, è necessario che questa condizione sia uguale sul lato client.
4. Selezionare la casella di controllo **H-REAP Local Switching** per commutare il traffico client che appartiene a questa WLAN localmente sull'H-REAP.



Verifica autenticazione locale, switching locale

Attenersi alla seguente procedura:

1. Configurare il client con lo stesso SSID e le stesse configurazioni di sicurezza. Qui, il SSID è *Locale* e il metodo di sicurezza è *WPA-PSK*.
2. Attivare il SSID locale nel client. Il client viene autenticato a livello centrale nel controller e associato all'H-REAP. Il traffico del client è configurato per commutare localmente. Ora, il punto di accesso H-REAP è nello stato di autenticazione centrale e commutazione locale.
3. Disabilitare il collegamento WAN che si connette al controller. Il controller come al solito viene sottoposto al processo di annullamento della registrazione. H-REAP non è registrato sul controller. Una volta annullata la registrazione, H-REAP entra in modalità standalone. Tuttavia, il client che appartiene a questa WLAN mantiene l'associazione con H-REAP. Inoltre, poiché il tipo di autenticazione può essere gestito localmente nell'access point senza controller, H-REAP consente le associazioni da qualsiasi nuovo client wireless attraverso questa WLAN.
4. Per verificare questa condizione, attivare qualsiasi altro client wireless sulla stessa WLAN. È possibile verificare che il client sia stato autenticato e associato correttamente.

Risoluzione dei problemi

- Per risolvere ulteriormente i problemi di connettività dei client sulla porta della console dell'H-REAP, immettere questo comando:

```
AP_CLI#show capwap reap association
```
- Per risolvere ulteriormente i problemi di connettività del client nel controller e limitare l'output

di ulteriori operazioni di debug, utilizzare questo comando:

```
AP_CLI#debug mac addr
```

- Per eseguire il debug dei problemi di connettività 802.11 di un client, utilizzare questo comando:

```
AP_CLI#debug dot11 state enable
```

- Eseguire il debug del processo di autenticazione 802.1X di un client e gli errori con questo comando:

```
AP_CLI#debug dot1x events enable
```

- È possibile eseguire il debug dei messaggi del controller back-end o RADIUS utilizzando questo comando:

```
AP_CLI#debug aaa events enable
```

- In alternativa, per abilitare tutti i comandi di **debug** del client, usare questo comando:

```
AP_CLI#debug client
```

Informazioni correlate

- [Esempio di configurazione base di Wireless LAN Controller e Lightweight Access Point](#)
- [Esempio di configurazione delle VLAN nei Wireless LAN Controller](#)
- [Guida alla configurazione di Cisco Wireless LAN Controller, versione 7.0](#)
- [Guida alla progettazione e alla distribuzione di Hybrid REAP](#)
- [Risoluzione dei problemi di base di Hybrid Remote Edge Access Point \(H-REAP\)](#)
- [Esempio di configurazione del failover del controller WLAN per i Lightweight Access Point](#)
- [Supporto dei prodotti wireless](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)