Aggiunta manuale di certificati autofirmati al controller per i punti di accesso convertiti in LWAPP

Sommario

Introduzione

In questo documento vengono illustrati i metodi che è possibile utilizzare per aggiungere manualmente certificati autofirmati (SSC) a un controller Cisco Wireless LAN (WLAN).

Il SSC di un punto di accesso (AP) deve esistere su tutti i WLC della rete a cui l'AP è autorizzato a registrarsi. Come regola generale, applicare il SSC a tutti i WLC dello stesso gruppo di mobilità. Quando l'aggiunta del SSC al WLC non avviene tramite la utility di aggiornamento, è necessario aggiungere manualmente il SSC al WLC usando la procedura descritta in questo documento. Questa procedura è necessaria anche quando un AP viene spostato su una rete diversa o quando vengono aggiunti altri WLC alla rete esistente.

Èpossibile riconoscere questo problema quando un access point convertito in Lightweight AP Protocol (LWAPP) non è associato al WLC. Quando si risolvono i problemi relativi alle associazioni, vengono visualizzati questi output quando si eseguono i seguenti debug:

- Quando si esegue il comando **debug pm pki enable**, viene visualizzato:

```
(Cisco Controller) >debug pm pki enable
Thu Jan 26 20:22:50 2006: sshpmGetIssuerHandles: locking ca cert table
Thu Jan 26 20:22:50 2006: sshpmGetIssuerHandles: calling x509_alloc() for user cert
Thu Jan 26 20:22:50 2006: sshpmGetIssuerHandles: calling x509_decode()
Thu Jan 26 20:22:50 2006: sshpmGetIssuerHandles: <subject> L=San Jose, ST=
California, C=US, O=Cisco Systems, MAILTO=support@cisco.com, CN=C1130-00146a1b3744
```

```
Thu Jan 26 20:22:50 2006: sshpmGetIssuerHandles: <issuer>  L=San Jose, ST=
California, C=US, O=Cisco Systems, MAILTO=support@cisco.com, CN=C1130-00146a1b3744
Thu Jan 26 20:22:50 2006: sshpmGetIssuerHandles: Mac Address in subject is
00:XX:XX:XX:XX
Thu Jan 26 20:22:50 2006: sshpmGetIssuerHandles: Cert is issued by Cisco Systems.
Thu Jan 26 20:22:50 2006: sshpmGetIssuerHandles: SSC is not allowed by config;
bailing...
Thu Jan 26 20:22:50 2006: sshpmFreePublicKeyHandle: called with (nil)
Thu Jan 26 20:22:50 2006: sshpmFreePublicKeyHandle: NULL argument.
```

- Quando si esegue il comando **debug lwapp events enable**, viene visualizzato quanto segue:

```
(Cisco Controller) >debug lwapp errors enable
....
Thu Jan 26 20:23:27 2006: Received LWAPP DISCOVERY REQUEST from AP
00:13:5f:f8:c3:70 to ff:ff:ff:ff:ff:ff on port '1'
Thu Jan 26 20:23:27 2006: Successful transmission of LWAPP Discovery-Response to
AP 00:13:5f:f8:c3:70 on Port 1
Thu Jan 26 20:23:27 2006: Received LWAPP JOIN REQUEST from AP 00:13:5f:f9:dc:b0 to
06:0a:10:10:00:00 on port '1'
Thu Jan 26 20:23:27 2006: sshpmGetIssuerHandles: locking ca cert table
Thu Jan 26 20:23:27 2006: sshpmGetIssuerHandles: calling x509_alloc() for user cert
Thu Jan 26 20:23:27 2006: sshpmGetIssuerHandles: calling x509_decode()
Thu Jan 26 20:23:27 2006: sshpmGetIssuerHandles: <subject> L=San Jose, ST=
California, C=US, O=Cisco Systems, MAILTO=support@cisco.com, CN=C1130-00146a1b321a
Thu Jan 26 20:23:27 2006: sshpmGetIssuerHandles: <issuer>  L=San Jose, ST=
California, C=US, O=Cisco Systems, MAILTO=support@cisco.com, CN=C1130-00146a1b321a
Thu Jan 26 20:23:27 2006: sshpmGetIssuerHandles: Mac Address in subject is
00:14:6a:1b:32:1a

Thu Jan 26 20:23:27 2006: sshpmGetIssuerHandles: Cert is issued by Cisco Systems.
Thu Jan 26 20:23:27 2006: sshpmGetIssuerHandles: SSC is not allowed by config;
bailing...
Thu Jan 26 20:23:27 2006: LWAPP Join-Request does not include valid certificate
in CERTIFICATE_PAYLOAD from AP 00:13:5f:f9:dc:b0.
Thu Jan 26 20:23:27 2006: sshpmFreePublicKeyHandle: called with (nil)
Thu Jan 26 20:23:27 2006: sshpmFreePublicKeyHandle: NULL argument.
Thu Jan 26 20:23:27 2006: Unable to free public key for AP  00:13:5F:F9:DC:B0
Thu Jan 26 20:23:27 2006: spamDeleteLCB: stats timer not initialized for AP
00:13:5f:f9:dc:b0
Thu Jan 26 20:23:27 2006: spamProcessJoinRequest : spamDecodeJoinReq failed
```

Prerequisiti

Requisiti

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

- Il WLC non contiene il SSC generato dall'utility di aggiornamento.
- Gli access point contengono un SSC.
- Telnet è abilitato sul WLC e sull'access point.
- La versione minima del codice software Cisco IOS® precedente a LWAPP è sull'access point da aggiornare.

Componenti usati

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

- Cisco 2006 WLC con firmware 3.2.116.21 senza SSC installato
- Cisco Aironet serie 1230 AP con SSC

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

Fare riferimento a Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.

Premesse

Nell'architettura WLAN centralizzata Cisco, gli access point funzionano in modalità lightweight. Gli AP vengono associati a un WLC Cisco con l'uso del LWAPP. LWAPP è un protocollo IETF (Internet Engineering Task Force) draft che definisce i messaggi di controllo per l'installazione e l'autenticazione dei percorsi e le operazioni di runtime. LWAPP definisce anche il meccanismo di tunneling per il traffico di dati.

Un Lightweight AP (LAP) rileva un WLC usando i meccanismi di rilevamento LWAPP. Il LAP invia quindi al WLC una richiesta di join a LWAPP. Il WLC invia al LAP una risposta di join LWAPP che consente al LAP di unirsi al WLC. Quando il LAP è collegato al WLC, il LAP scarica il software WLC se le revisioni sul LAP e sul WLC non corrispondono. Successivamente, il LAP è completamente sotto il controllo del WLC.

LWAPP protegge la comunicazione di controllo tra l'access point e il WLC tramite una distribuzione sicura delle chiavi. Per la distribuzione della chiave protetta sono necessari certificati digitali X.509 con provisioning già eseguito sia sul LAP che sul WLC. Ai certificati preinstallati viene fatto riferimento con il termine "MIC", acronimo di Manufacturing Installed Certificate (Certificato di produzione installato). I punti di accesso Aironet forniti prima del 18 luglio 2005 non dispongono di MIC. In questo modo, questi access point creano un SSC quando vengono convertiti per funzionare in modalità lightweight. I controller sono programmati per accettare SSC per l'autenticazione di access point specifici.

Questo è il processo di aggiornamento:

1. L'utente esegue un'utility di aggiornamento che accetta un file di input con un elenco di access point e i relativi indirizzi IP, oltre alle credenziali di accesso.
2. L'utility stabilisce sessioni Telnet con gli access point e invia una serie di comandi del software Cisco IOS nel file di input per preparare l'access point per l'aggiornamento. Questi comandi includono i comandi per creare gli SSC. Inoltre, l'utility stabilisce una sessione Telnet con il WLC per programmare il dispositivo in modo da consentire l'autorizzazione di access point SSC specifici.
3. L'utility carica quindi il software Cisco IOS versione 12.3(7)JX sull'access point in modo che l'access point possa collegarsi al WLC.
4. Dopo che l'access point si è unito al WLC, scarica una versione completa del software Cisco IOS dal WLC. L'utility di aggiornamento genera un file di output che include l'elenco dei punti di accesso e dei corrispondenti valori hash della chiave SSC che possono essere importati nel software di gestione Wireless Control System (WCS).

5. Il sistema WCS può quindi inviare queste informazioni ad altri WLC sulla rete.

Dopo che un access point si è unito a un WLC, è possibile riassegnare l'access point a qualsiasi WLC sulla rete, se necessario.

Individuare l'hash della chiave SHA1

Se il computer che ha eseguito la conversione AP è disponibile, è possibile ottenere l'hash della chiave SHA1 (Secure Hash Algorithm 1) dal file con estensione csv presente nella directory dello strumento di aggiornamento di Cisco. Se il file con estensione csv non è disponibile, è possibile eseguire un comando di **debug** sul WLC per recuperare l'hash della chiave SHA1.

Attenersi alla seguente procedura:

1. Accendere il punto di accesso e collegarlo alla rete.
2. Abilitare il debug sull'interfaccia della riga di comando (CLI) del WLC.Il comando è **debug pm pki enable**.

```
(Cisco Controller) >debug pm pki enable
Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: getting (old) aes ID cert handle...
Mon May 22 06:34:10 2006: sshpmGetCID: called to evaluate <bsnOldDefaultIdCert>
Mon May 22 06:34:10 2006: sshpmGetCID: comparing to row 0, CA cert
>bsnOldDefaultCaCert<
Mon May 22 06:34:10 2006: sshpmGetCID: comparing to row 1, CA cert
>bsnDefaultRootCaCert<
Mon May 22 06:34:10 2006: sshpmGetCID: comparing to row 2, CA cert
>bsnDefaultCaCert<
Mon May 22 06:34:10 2006: sshpmGetCID: comparing to row 3, CA cert
>bsnDefaultBuildCert<
Mon May 22 06:34:10 2006: sshpmGetCID: comparing to row 4, CA cert
>cscoDefaultNewRootCaCert<
Mon May 22 06:34:10 2006: sshpmGetCID: comparing to row 5, CA cert
>cscoDefaultMfgCaCert<
Mon May 22 06:34:10 2006: sshpmGetCID: comparing to row 0, ID cert
>bsnOldDefaultIdCert<
Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Calculate SHA1 hash on Public Key
Data
Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data  30820122 300d0609
2a864886 f70d0101
Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data  01050003 82010f00
3082010a 02820101
Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data  00c805cd 7d406ea0
cad8df69 b366fd4c
Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data  82fc0df0 39f2bff7
ad425fa7 face8f15
Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data  f356a6b3 9b876251
43b95a34 49292e11
Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data  038181eb 058c782e
56f0ad91 2d61a389
Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data  f81fa6ce cd1f400b
b5cf7cef 06ba4375
Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data  dde0648e c4d63259
774ce74e 9e2fde19
Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data  0f463f9e c77b79ea
65d8639b d63aa0e3
Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data  7dd485db 251e2e07
9cd31041 b0734a55
Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data  463fbacc 1a61502d
c54e75f2 6d28fc6b
Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data  82315490 881e3e31
```

```
02d37140 7c9c865a
Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data  9ef3311b d514795f
7a9bac00 d13ff85f
Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data  97e1a693 f9f6c5cb
88053e8b 7fae6d67
Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data  ca364f6f 76cf78bc
bc1acc13 0d334aa6
Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data  031fb2a3 b5e572df
2c831e7e f765b7e5
Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data  fe64641f de2a6fe3
23311756 8302b8b8
Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data  1bfae1a8 eb076940
280cbed1 49b2d50f
Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data  f7020301 0001
Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: SSC Key Hash is
9e4ddd8dfcdd8458ba7b273fc37284b31a384eb9
Mon May 22 06:34:14 2006: LWAPP Join-Request MTU path from AP 00:0e:84:32:04:f0
is 1500, remote debug mode is 0
Mon May 22 06:34:14 2006: spamRadiusProcessResponse: AP Authorization failure for
00:0e:84:32:04:f0
```

Aggiunta del SSC al WLC

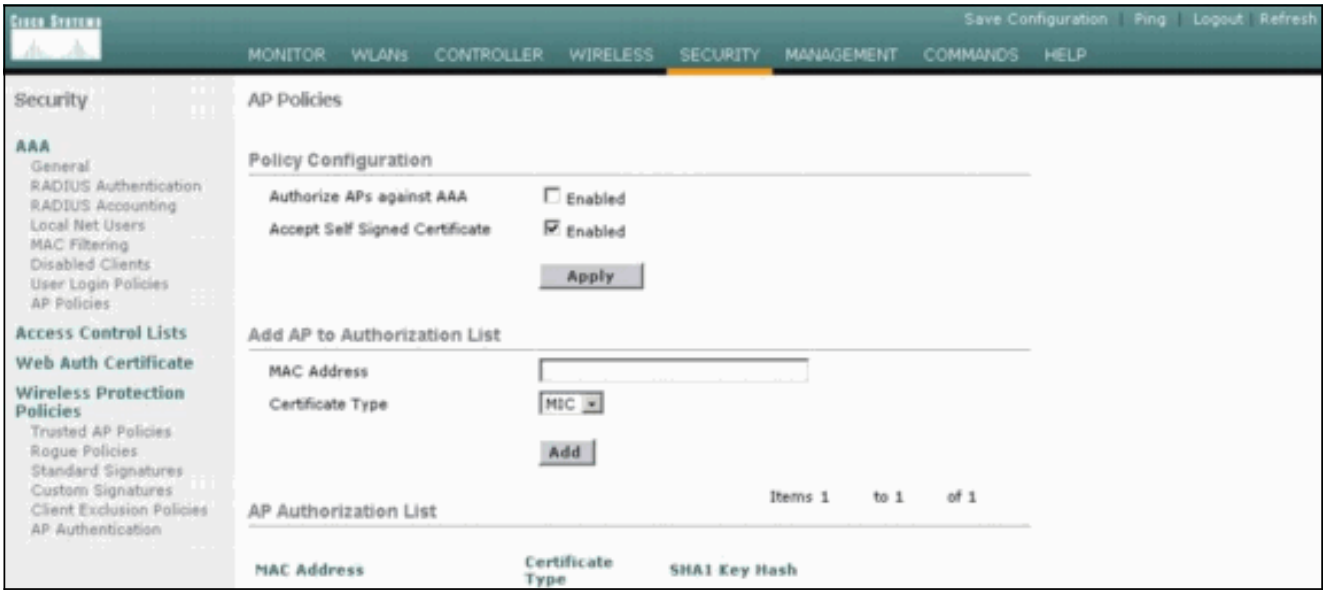
Attività

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

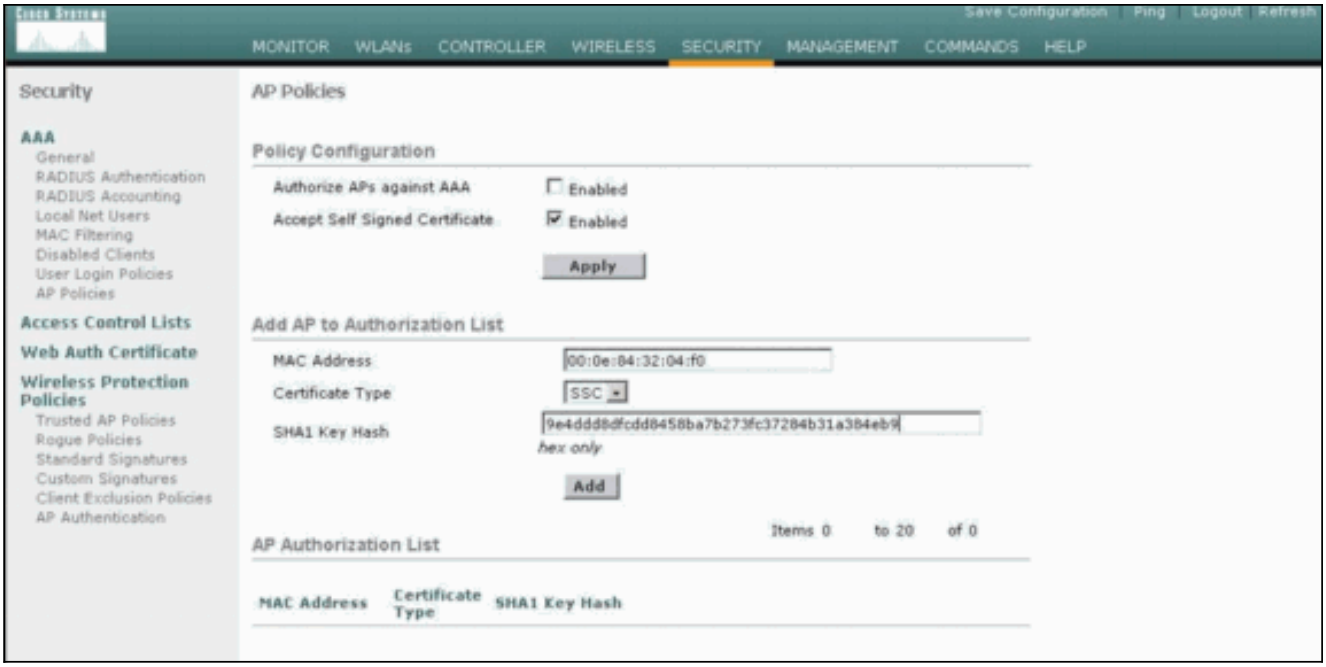
Configurazione GUI

Eseguire questi passaggi dalla GUI:

1. Scegliere **Sicurezza > Criteri PA** e fare clic su **Abilitato** accanto ad Accetta certificato autofirmato.



2. Selezionare **SSC** dal menu a discesa Tipo di certificato.



3. Immettere l'indirizzo MAC dell'access point e la chiave hash e fare clic su **Add** (Aggiungi).

Configurazione CLI

Completare questi passaggi dalla CLI:

1. Abilitare Accetta certificato autofirmato sul WLC.Il comando è **config auth-list ap-policy ssc enable**.
```
(Cisco Controller) >config auth-list ap-policy ssc enable
```

2. Aggiungere l'indirizzo MAC AP e la chiave hash all'elenco delle autorizzazioni.Il comando è **config auth-list add ssc *AP_MAC AP_key***.
```
(Cisco Controller) >config auth-list add ssc 00:0e:84:32:04:f0
9e4ddd8dfcdd8458ba7b273fc37284b31a384eb9
!--- This command should be on one line.
```

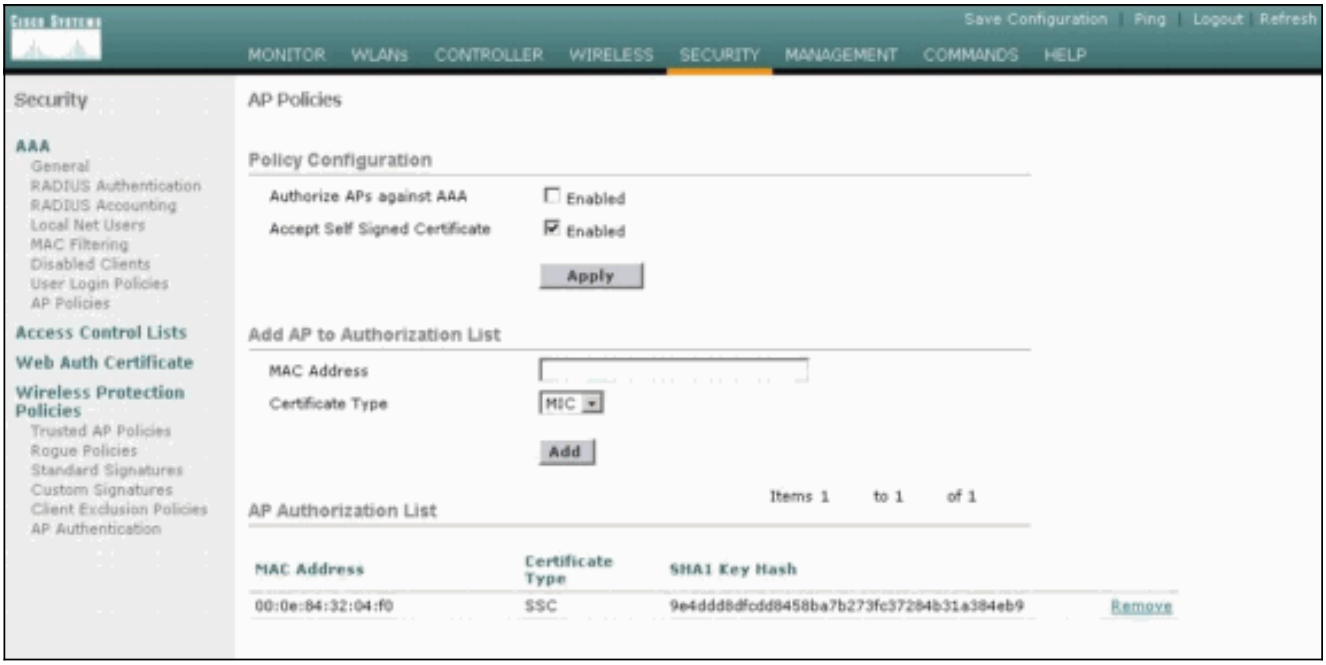
Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

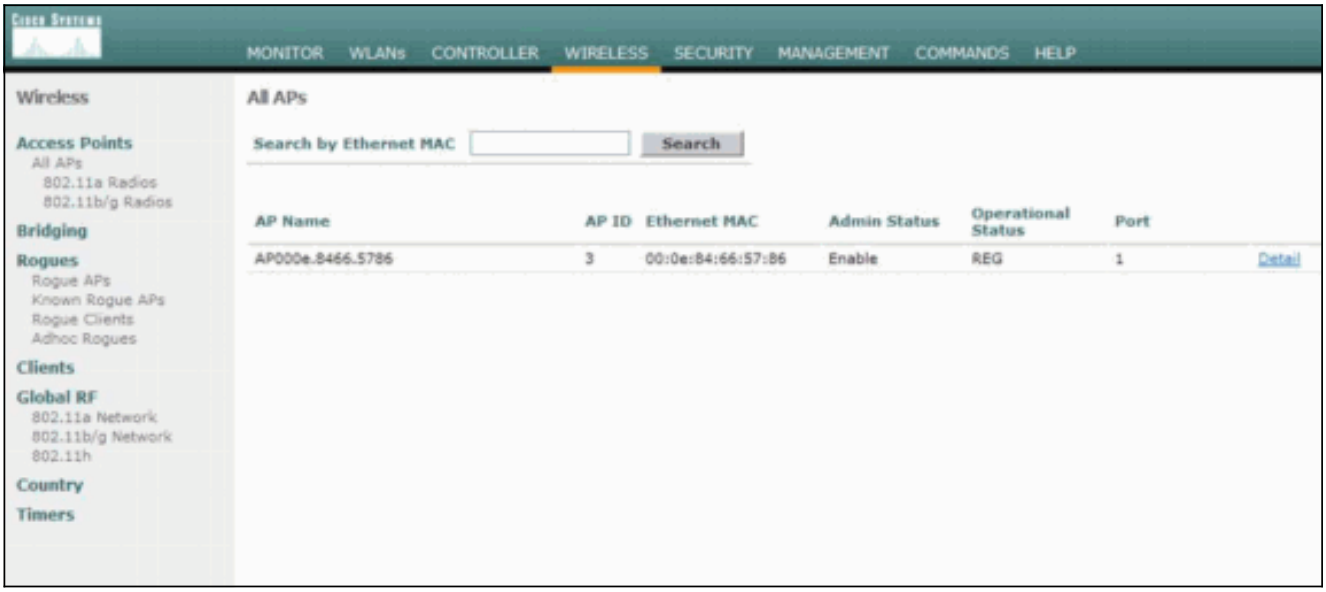
Verifica GUI

Attenersi alla seguente procedura:

1. Nella finestra Criteri PA, verificare che l'indirizzo MAC AP e l'hash della chiave SHA1 siano visualizzati nell'area Elenco autorizzazioni
AP.



2. Nella finestra All AP, verificare che tutti gli AP siano registrati sul WLC.



Verifica CLI

Lo strumento Output Interpreter (solo utenti registrati) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

- **show auth-list**: visualizza l'elenco di autorizzazioni AP.
- **show ap summary**: visualizza un riepilogo di tutti gli access point connessi.

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

Informazioni correlate

- Domande frequenti (FAQ) sul controller WLC
- Guida alla configurazione di Cisco Wireless LAN Controller, versione 3.2
- Esempio di configurazione base di Wireless LAN Controller e Lightweight Access Point
- Documentazione e supporto tecnico – Cisco Systems