

自簽名證書手動新增到控制器，用於LWAPP轉換的AP

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[慣例](#)

[背景資訊](#)

[找到SHA1金鑰雜湊](#)

[將SSC新增到WLC](#)

[工作](#)

[GUI配置](#)

[CLI組態](#)

[驗證](#)

[疑難排解](#)

[相關資訊](#)

簡介

本檔案將說明您可以用來將自簽署憑證(SSC)手動新增至思科無線LAN(WLAN)控制器(WLC)的方法。

接入點(AP)的SSC應存在於AP有權向其註冊的網路中的所有WLC上。通常，將SSC應用於同一移動組中的所有WLC。如果不能通過升級實用程式將SSC新增到WLC，則必須使用本文檔中的過程手動將SSC新增到WLC。當AP移動到其他網路或向現有網路新增其他WLC時，也需要此過程。

當由輕量AP協定(LWAPP)轉換的AP未與WLC關聯時，您可以識別此問題。解決關聯問題時，在發出以下調試命令時會顯示以下輸出：

- 當您發出`debug pm pki enable`命令時，您會看到：

```
(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=C1130-00146alb3744
Thu Jan 26 20:22:50 2006: sshpmGetIssuerHandles: <issuer> L=San Jose, ST=
California, C=US, O=Cisco Systems, MAILTO=support@cisco.com, CN=C1130-00146alb3744
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.
```

- 當您發出**debug lwapp events enable**命令時，您會看到：

```
(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=C1130-00146alb321a
Thu Jan 26 20:23:27 2006: sshpmGetIssuerHandles: <issuer> L=San Jose, ST=
California, C=US, O=Cisco Systems, MAILTO=support@cisco.com, CN=C1130-00146alb321a
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
```

必要條件

需求

嘗試此組態之前，請確保符合以下要求：

- WLC不包含升級實用程式生成的SSC。
- AP包含SSC。
- WLC和AP上啟用Telnet。
- 要升級的AP上有LWAPP之前Cisco IOS®軟體代碼的最低版本。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco 2006 WLC (運行韌體3.2.116.21，未安裝SSC)
- 採用SSC的Cisco Aironet 1230系列AP

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除 (預設) 的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

請參閱[思科技術提示慣例以瞭解更多有關文件慣例的資訊。](#)

背景資訊

在Cisco集中式WLAN架構中，AP以輕量模式運行。AP使用LWAPP與Cisco WLC關聯。LWAPP是Internet工程任務組(IETF)的草案協定，它定義了設定和路徑身份驗證以及運行時操作的控制消息。LWAPP還定義了資料流量的隧道機制。

輕量AP(LAP)使用LWAPP發現機制發現WLC。然後LAP向WLC傳送LWAPP加入請求。WLC向LAP傳送LWAPP加入回應，該回應允許LAP加入WLC。當LAP連線到WLC時，如果LAP和WLC上的版本不匹配，LAP將下載WLC軟體。隨後，LAP完全在WLC的控制之下。

LWAPP通過安全金鑰分發來保護AP和WLC之間的控制通訊。安全金鑰分發要求在LAP和WLC上已預配X.509數位證書。工廠安裝的證書引用了術語「MIC」，這是製造安裝證書的縮寫。2005年7月18日之前出廠的Aironet AP沒有MIC。因此，這些AP在轉換為輕量模式運行時會建立SSC。控制器被程式設計為接受SSC以進行特定AP的身份驗證。

升級程式如下：

1. 使用者運行一個升級實用程式，該實用程式接受一個包含接入點及其IP地址及其登入憑證清單的輸入檔案。
2. 該實用程式與AP建立Telnet會話，並在輸入檔案中傳送一系列Cisco IOS軟體命令，以準備AP進行升級。這些命令包括用於建立SSC的命令。此外，該實用程式還會與WLC建立Telnet會話，以便對該裝置進程式設計，以允許對特定SSC AP進行授權。
3. 然後，該實用程式將Cisco IOS軟體版本12.3(7)JX載入到AP，以便AP可以加入WLC。
4. AP加入WLC後，AP會從WLC下載完整的Cisco IOS軟體版本。升級實用程式生成一個輸出檔案，該檔案包含可以匯入到無線控制系統(WCS)管理軟體中的AP清單和相應的SSC金鑰雜湊值。
5. 然後WCS可以將此資訊傳送到網路上的其他WLC。

AP加入WLC後，如有必要，您可以將AP重新分配給網路上的任何WLC。

找到SHA1金鑰雜湊

如果執行AP轉換的電腦可用，則可以從思科升級工具目錄中的.csv檔案獲取安全雜湊演算法1(SHA1)金鑰雜湊。如果.csv檔案不可用，則可以在WLC上發出**debug**命令以檢索SHA1金鑰雜湊。

請完成以下步驟：

1. 開啟AP並將其連線到網路。
2. 在WLC命令列介面(CLI)上啟用調試。命令是**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
>cscDefaultNewRootCaCert<
Mon May 22 06:34:10 2006: sshpmGetCID: comparing to row 5, CA cert
>cscDefaultMfgCaCert<
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
bclacc13 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
280cbcd1 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
```

[將SSC新增到WLC](#)

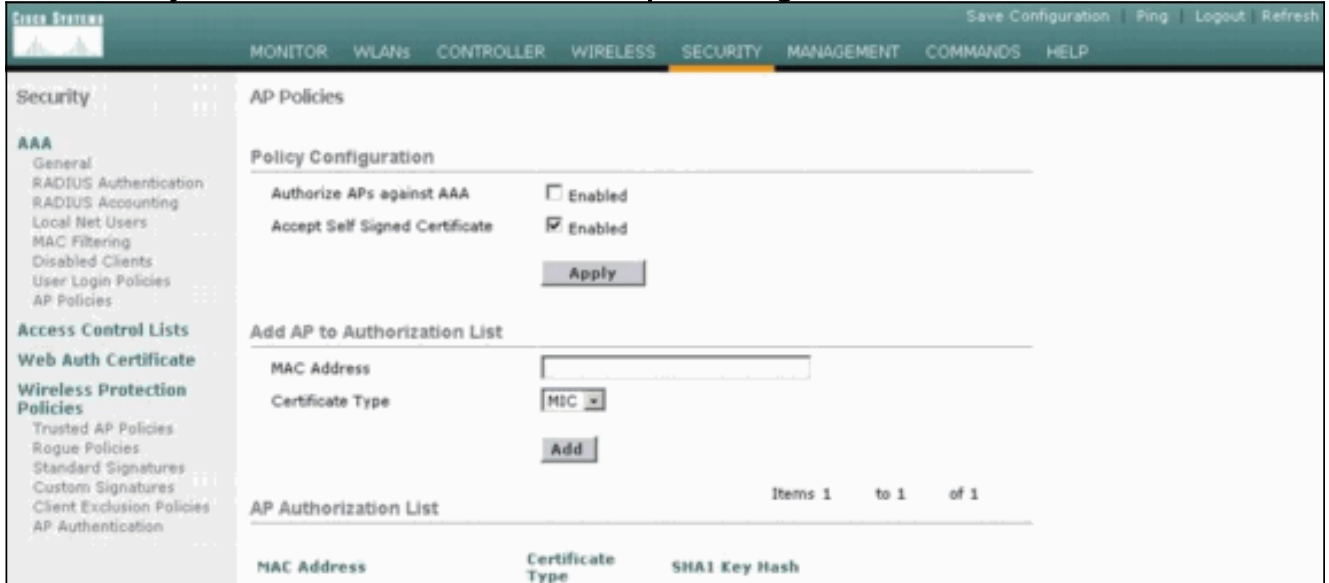
[工作](#)

本節提供用於設定本文件中所述功能的資訊。

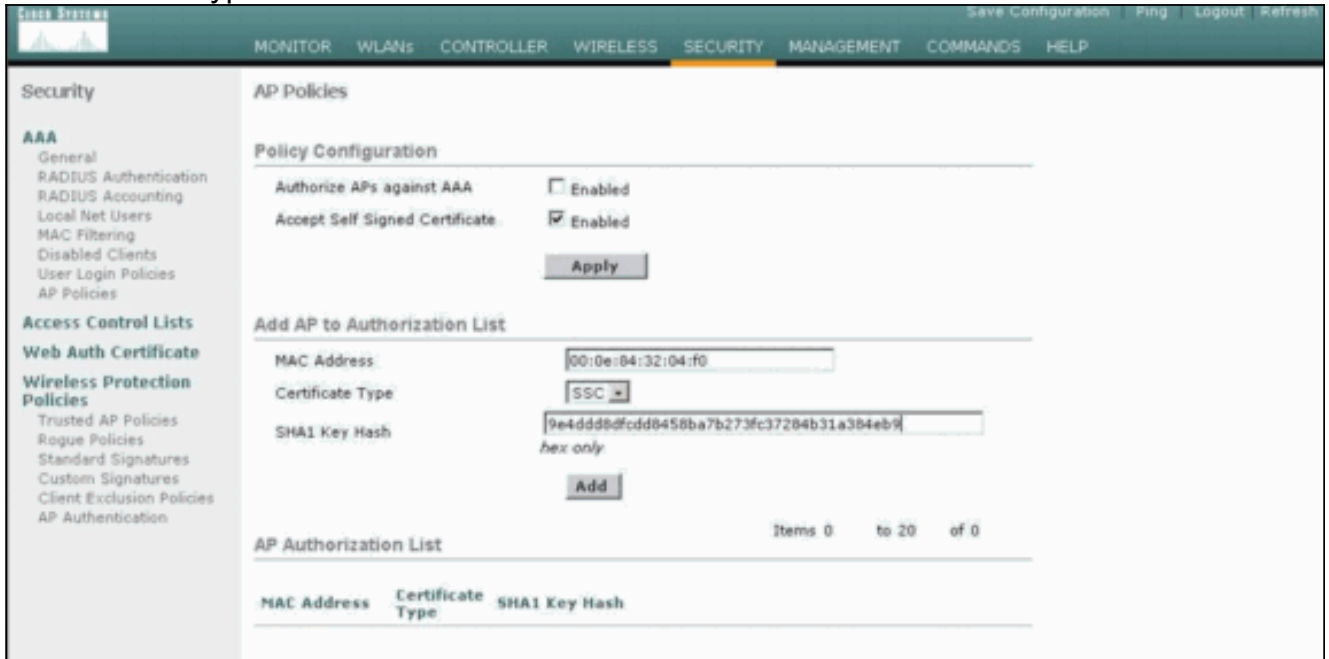
[GUI配置](#)

在GUI上完成以下步驟：

1. 選擇Security > AP Policies，然後按一下Accept Self-Signed Certificate旁邊的Enabled。



2. 從Certificate Type下拉選單中選擇SSC。



3. 輸入AP的MAC地址和雜湊鍵，然後按一下Add。

CLI組態

從CLI完成以下步驟：

1. 在WLC上啟用接受自簽名證書。命令是config auth-list ap-policy ssc enable。
(Cisco Controller) >config auth-list ap-policy ssc enable
2. 將AP MAC地址和雜湊金鑰新增到授權清單。命令是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.

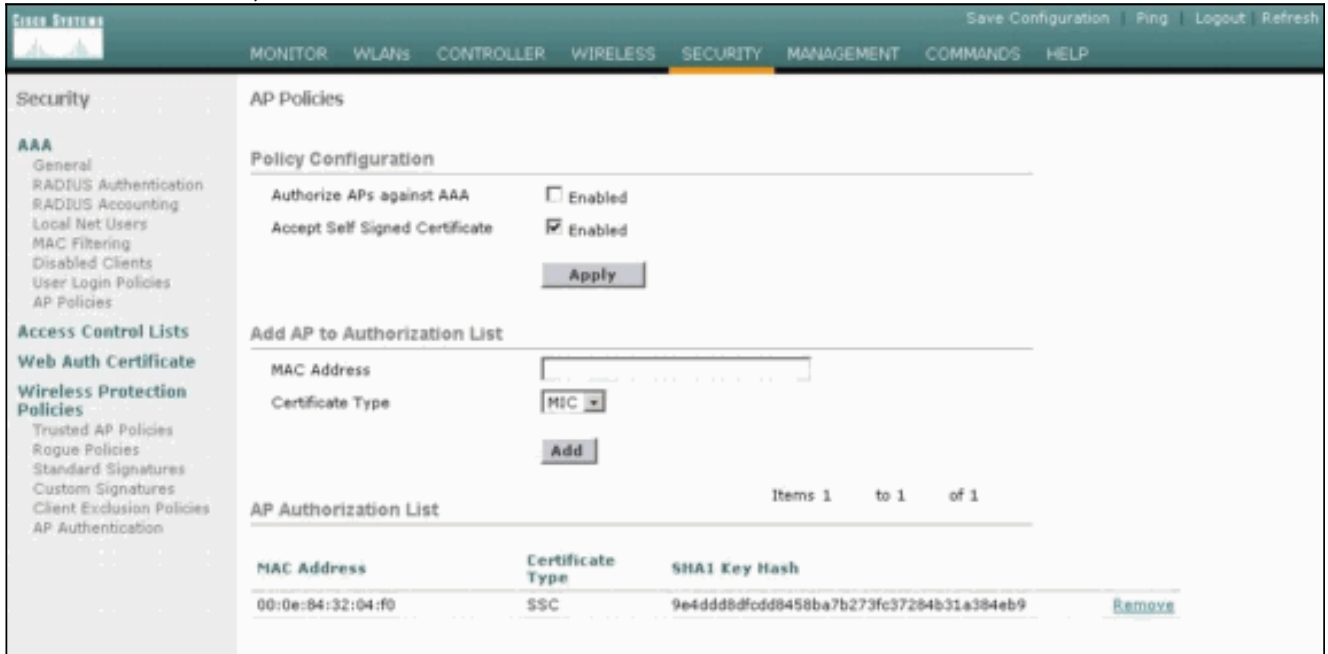
驗證

使用本節內容，確認您的組態是否正常運作。

GUI驗證

請完成以下步驟：

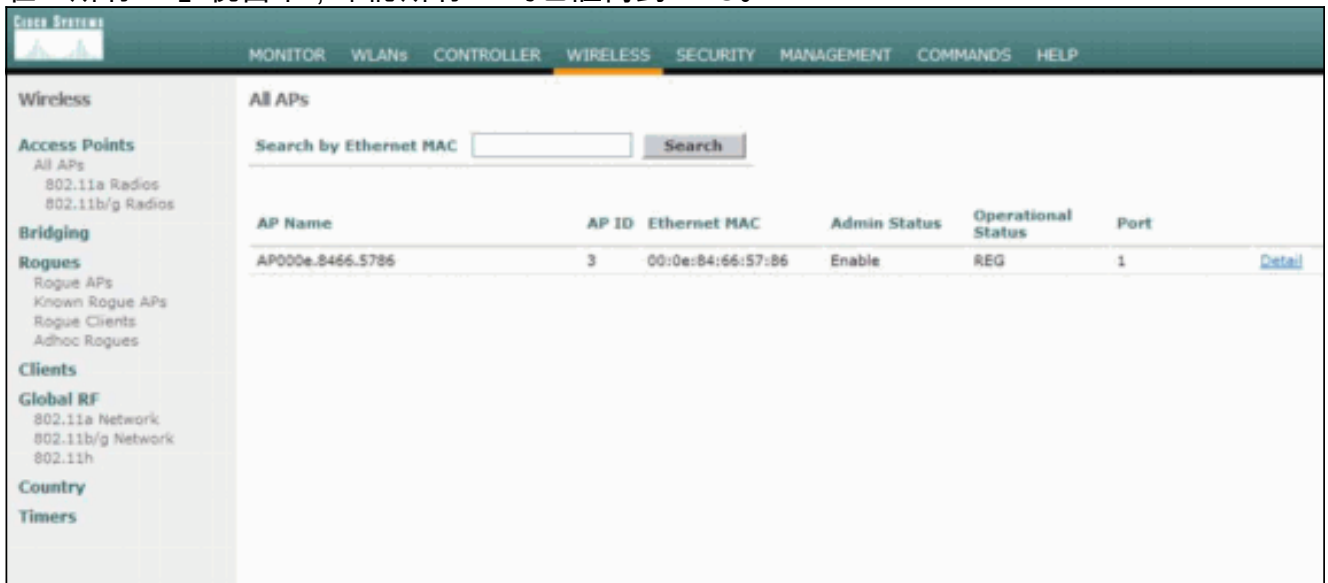
1. 在AP策略視窗中，驗證AP MAC地址和SHA1金鑰雜湊是否出現在AP授權清單區域中。



The screenshot shows the 'AP Policies' configuration page in the Cisco Systems GUI. The 'AP Authorization List' table is as follows:

| MAC Address | Certificate Type | SHA1 Key Hash | |
|-------------------|------------------|---|------------------------|
| 00:0e:84:32:04:f0 | SSC | 9e4ddd8fd0d8458ba7b273fc37284b31a384eb9 | Remove |

2. 在「所有AP」視窗中，確認所有AP均已註冊到WLC。



The screenshot shows the 'All APs' view in the Cisco Systems GUI. The table lists the following AP:

| AP Name | AP ID | Ethernet MAC | Admin Status | Operational Status | Port | |
|------------------|-------|-------------------|--------------|--------------------|------|------------------------|
| AP000e.8466.5786 | 3 | 00:0e:84:66:57:86 | Enable | REG | 1 | Detail |

CLI 驗證

輸出直譯器工具(僅供已註冊客戶使用)(OIT)支援某些show命令。使用OIT檢視show命令輸出的分析

。

- show auth-list — 顯示AP授權清單。
- show ap summary — 顯示所有連線的AP的摘要。

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

相關資訊

- [無線區域網路控制器\(WLC\)疑難排解常見問題](#)
- [思科無線LAN控制器組態設定指南3.2版](#)
- [無線LAN控制器和輕量型存取點基本組態範例](#)
- [技術支援與文件 - Cisco Systems](#)