为LWAPP-Converted AP添加自签名证书手工到控制器

目录

[简介](#)
[先决条件](#)
[要求](#)
[使用的组件](#)
[规则](#)
[背景信息](#)
[找到SHA1密钥哈希](#)
[将SSC添加到WLC](#)
[任务](#)
[GUI 配置](#)
[CLI 配置](#)
[验证](#)
[故障排除](#)
[相关信息](#)

简介

本文档介绍可用于手动将自签名证书(SSC)添加到思科无线局域网(WLAN)控制器(WLC)的方法。

接入点(AP)的SSC应存在于AP有权注册到的网络中的所有WLC上。一般来说，将SSC应用于同一移动组中的所有WLC。如果不通过升级实用程序将SSC添加到WLC中，则必须手动将SSC添加到WLC使用本文档中的过程。当AP移动到其他网络或将其他WLC添加到现有网络时，您还需要执行此过程。

当轻量AP协议(LWAPP)转换的AP未与WLC关联时，您可以识别此问题。排除关联问题故障时，发出以下调试时会看到以下输出：

- 当您发出debug pm pki enable**命令时**，您会看到：

```
(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=C1130-00146a1b3744
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.
```

- 当您发出debug lwapp events **enable命令时**，您会看到：

```
(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=C1130-00146a1b321a
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
```

先决条件

要求

尝试进行此配置之前，请确保满足以下要求：

- WLC不包含升级实用程序生成的SSC。
- AP包含SSC。
- 在WLC和AP上启用Telnet。
- LWAPP之前的Cisco IOS®软件代码的最低版本位于要升级的AP上。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行固件3.2.116.21且未安装SSC的Cisco 2006 WLC
- 带SSC的Cisco Aironet 1230系列AP

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档约定的更多信息，请参考 Cisco 技术提示约定。

背景信息

在思科集中式WLAN架构中，AP在轻量模式下运行。AP使用LWAPP关联到Cisco WLC。LWAPP 是一种 Internet 工程任务组 (IETF) 草案协议，它定义了设置和路径验证操作以及运行时操作的控制消息传递。此外，LWAPP 也定义了数据流量的隧道机制。

轻量AP(LAP)使用LWAPP发现机制发现WLC。然后，LAP向WLC发送LWAPP加入请求。WLC向LAP发送允许LAP加入WLC的LWAPP加入响应。当LAP加入WLC时，如果LAP和WLC上的修订版不匹配，LAP将下载WLC软件。随后，LAP完全由WLC控制。

LWAPP通过安全密钥分发保护AP和WLC之间的控制通信。安全密钥分发要求在LAP和WLC上都已调配X.509数字证书。出厂安装的证书可以通过术语“MIC”来标识，它是厂商预装证书 (Manufacturing Installed Certificate) 的缩写。在2005年7月18日之前发货的Aironet AP没有MIC。因此，当这些AP转换为在轻量模式下运行时，会创建SSC。控制器被设定为接受 SSC，以便可以验证特定 AP 的身份。

升级过程如下：

1. 用户运行升级实用程序，该实用程序除了接收AP的登录凭证外，还接受包含AP及其IP地址列表的输入文件。
2. 该实用程序与AP建立Telnet会话，并在输入文件中发送一系列Cisco IOS软件命令，以便为AP升级做好准备。这些命令包括创建SSC的命令。此外，该实用程序与WLC建立Telnet会话，以便对设备进行编程以允许授权特定SSC AP。
3. 然后，该实用程序将Cisco IOS软件版本12.3(7)JX加载到AP上，以便AP可以加入WLC。
4. AP加入WLC后，AP从WLC下载完整的Cisco IOS软件版本。升级实用程序生成一个输出文件，该输出文件包括AP列表和可导入无线控制系统(WCS)管理软件的相应SSC密钥哈希值。
5. 然后，WCS可以将此信息发送到网络上的其他WLC。

在AP加入WLC后，如有必要，您可以将AP重新分配给网络上的任何WLC。

找到SHA1密钥哈希

如果执行AP转换的计算机可用，则可以从Cisco升级工具目录中的.csv文件获取安全散列算法1(SHA1)密钥散列。如果.csv文件不可用，则可以在WLC上发出**debug**命令以检索SHA1密钥散列。

请完成以下步骤：

1. 打开AP并将其连接到网络。
2. 在WLC命令行界面(CLI)上启用调试。命令为**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
```

将SSC添加到WLC

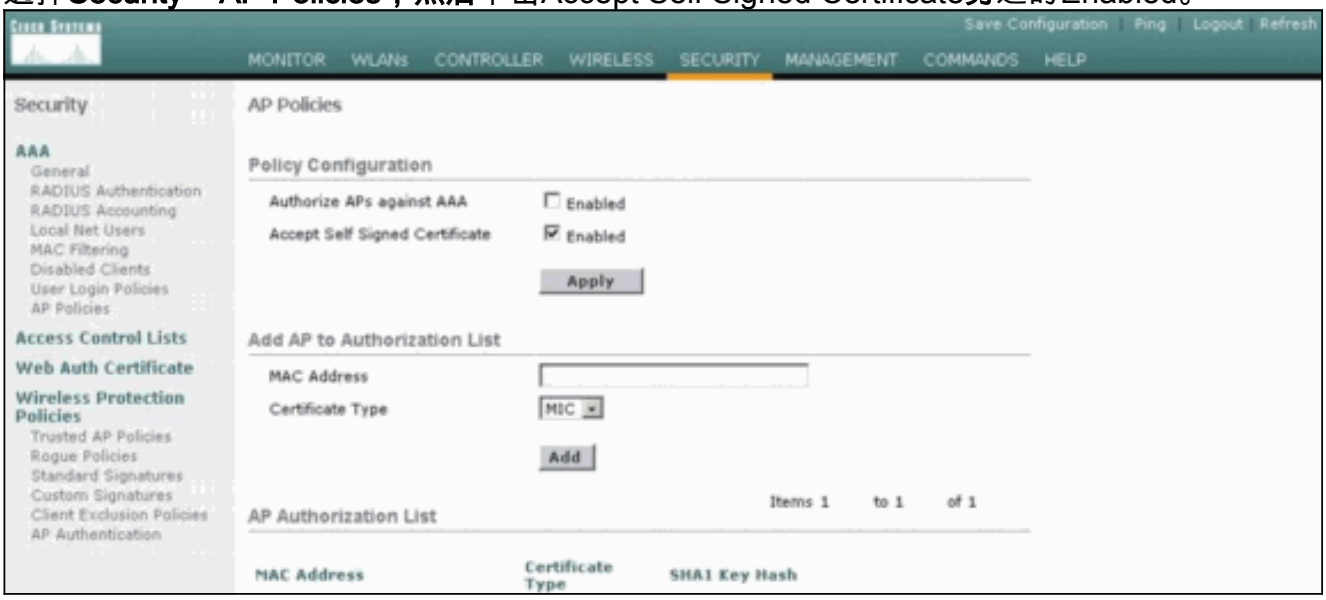
任务

本部分提供有关如何配置本文档所述功能的信息。

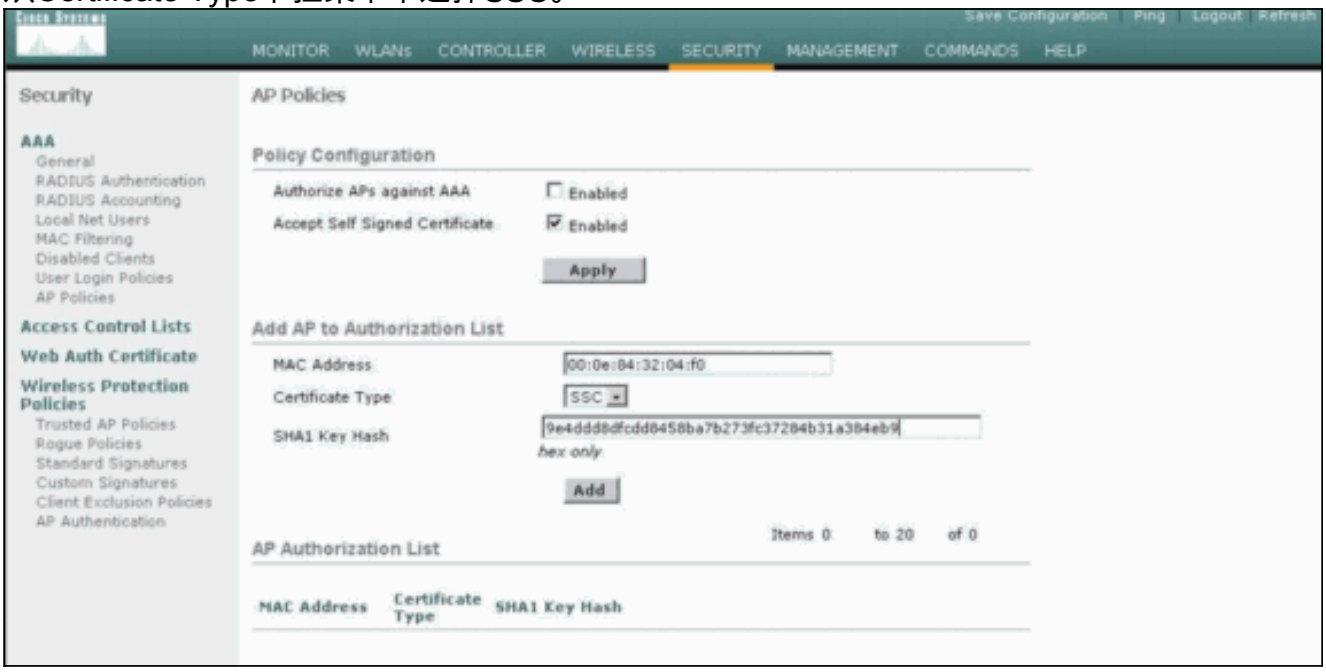
GUI 配置

从GUI中完成以下步骤：

1. 选择**Security > AP Policies，然后**单击Accept Self Signed Certificate**旁**边的Enabled。



2. 从Certificate Type下拉菜单中选择**SSC**。



3. 输入AP的MAC地址和哈希密钥，然后单击**Add**。

CLI 配置

从 CLI 中完成以下这些步骤：

1. 在WLC上启用接受自签名证书。命令为**config auth-list ap-policy ssc enable**。

```
(Cisco Controller) >config auth-list ap-policy ssc enable
```

2. 将AP MAC地址和哈希密钥添加到授权列表。命令为**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.
```

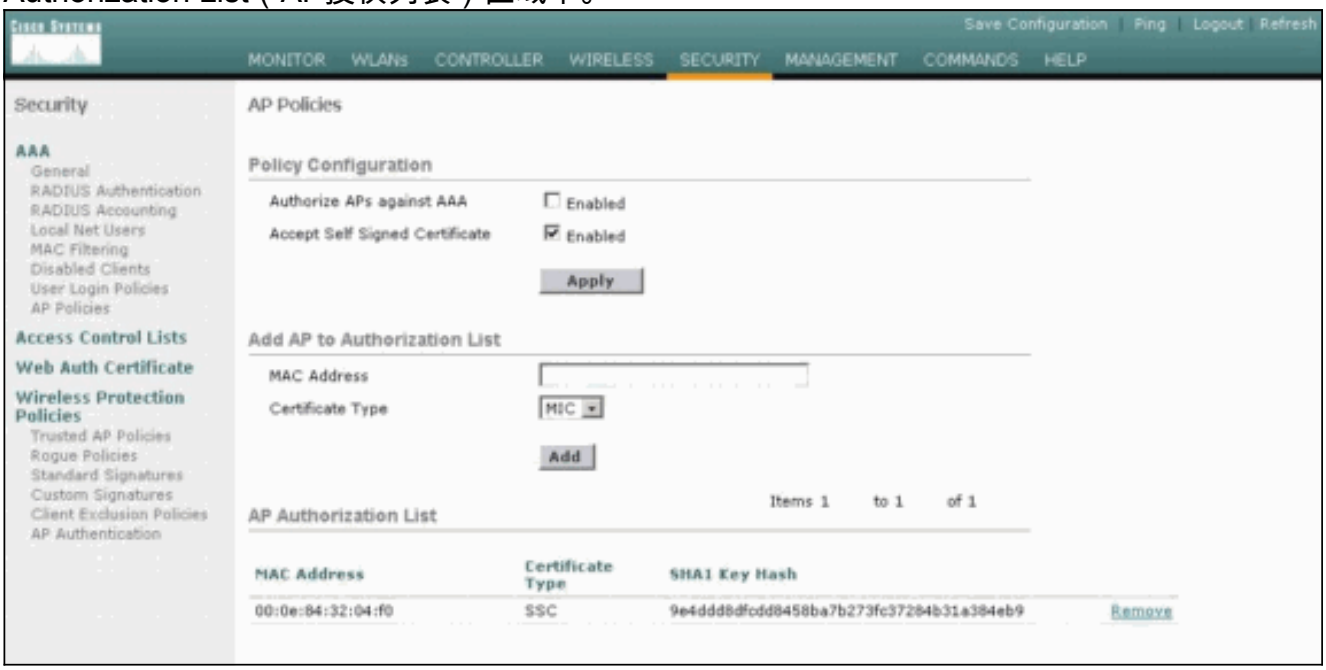
验证

使用本部分可确认配置能否正常运行。

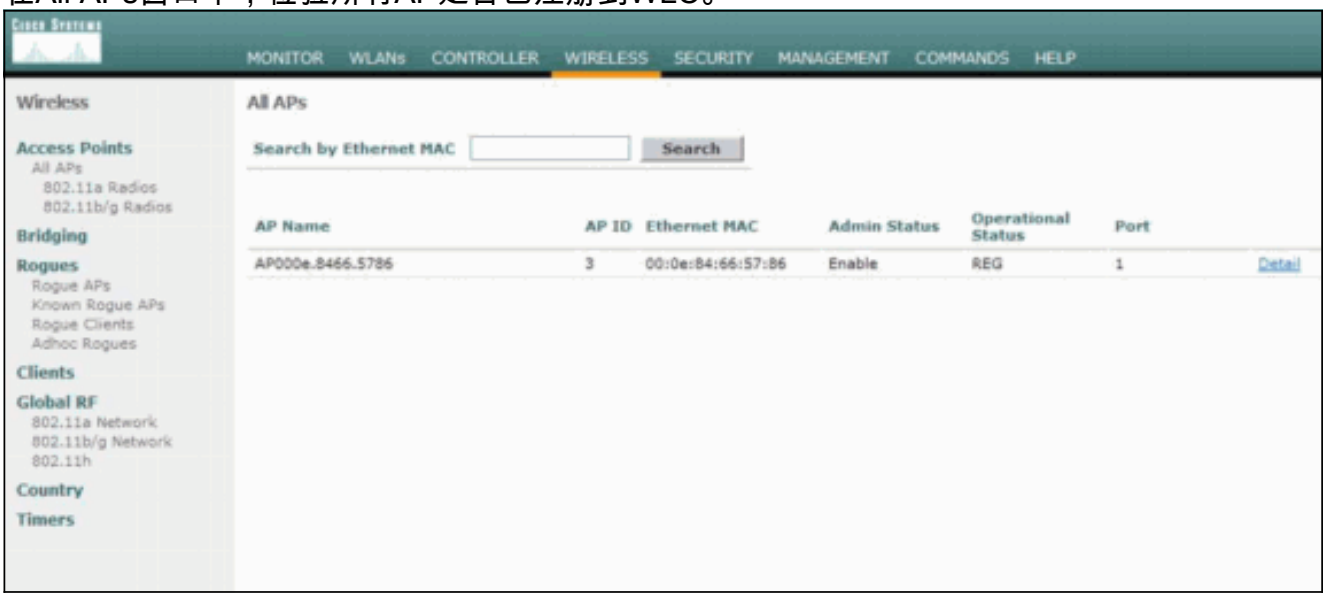
GUI验证

请完成以下步骤：

1. 在AP Policies（AP策略）窗口中，验证AP MAC地址和SHA1密钥哈希是否显示在AP Authorization List（AP授权列表）区域中。



2. 在All APs窗口中，检验所有AP是否已注册到WLC。



CLI验证

命令输出解释程序（仅限注册用户）(OIT) 支持某些 show 命令。使用 OIT 可查看对 show 命令输出的分析。

- **show auth-list** — 显示AP授权列表。

- show ap summary — 显示所有已连接AP的摘要。

故障排除

目前没有针对此配置的故障排除信息。

相关信息

- 无线 LAN 控制器 (WLC) 故障排除常见问题
- Cisco 无线 LAN 控制器配置指南 3.2 版
- 无线 LAN 控制器和轻量接入点基本配置示例
- 技术支持和文档 - Cisco Systems