Adição Manual do Certificado Autoassinado ao Controlador para APs com LWAPP convertidos

Contents

Introduction

Este documento explica os métodos que você pode usar para adicionar manualmente certificados autoassinados (SSCs) a um Cisco Wireless LAN (WLAN) Controller (WLC).

O SSC de um ponto de acesso (AP) deve existir em todas as WLCs na rede para a qual o AP tem permissão para se registrar. Como regra geral, aplique o SSC a todas as WLCs no mesmo grupo de mobilidade. Quando a adição do SSC à WLC não ocorre através do utilitário de atualização, você deve adicionar manualmente o SSC à WLC com o uso do procedimento neste documento. Você também precisa deste procedimento quando um AP é movido para uma rede diferente ou quando WLCs adicionais são adicionadas à rede existente.

Você pode reconhecer esse problema quando um AP convertido em LWAPP (Lightweight AP Protocol) não se associa à WLC. Quando você soluciona o problema de associação, você vê essas saídas quando emite estas depurações:

- Ao emitir o comando **debug pm pki enable**, você verá:

```
(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 você emite o comando **debug lwapp events enable**, você vê:

```
(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
```

Prerequisites

Requirements

Certifique-se de atender a estes requisitos antes de tentar esta configuração:

- A WLC não contém o SSC que o utilitário de atualização gerou.
- Os APs contêm um SSC.
- O Telnet é ativado no WLC e no AP.
- A versão mínima do código do software Cisco IOS® pré-LWAPP está no AP a ser atualizado.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco 2006 WLC que executa o firmware 3.2.116.21 sem SSC instalado
- AP Cisco Aironet 1230 Series com SSC

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Informações de Apoio

Na arquitetura da WLAN centralizada da Cisco, os APs operam no modo lightweight. Os APs se associam a um Cisco WLC com o uso do LWAPP. O LWAPP é um projeto de protocolo da força-tarefa de engenharia da Internet (IETF) que define as mensagens de controle para configuração e autenticação de caminho e operações de tempo de execução. O LWAPP também define o mecanismo de tunelamento para o tráfego de dados.

Um AP leve (LAP) descobre uma WLC com o uso de mecanismos de descoberta LWAPP. Em seguida, o LAP envia à WLC uma solicitação de união LWAPP. A WLC envia ao LAP uma resposta de união LWAPP que permite ao LAP ingressar na WLC. Quando o LAP é associado à WLC, o LAP faz o download do software da WLC se as revisões no LAP e na WLC não coincidirem. Subsequentemente, o LAP está completamente sob o controle da WLC.

O LWAPP protege a comunicação de controle entre o AP e a WLC por meio de uma distribuição de chave segura. A distribuição de chave segura exige certificados digitais X.509 já provisionados no LAP e no WLC. Os certificados na fábrica são conhecidos pelo termo “MIC”, que é um acrônimo em inglês para Certificado Instalado na Fábrica. Os APs Aironet enviados antes de 18 de julho de 2005 não possuem MICs. Assim, esses APs criam um SSC quando são convertidos para operar no modo lightweight. As controladoras são programadas para aceitar SSCs para a autenticação de APs específicos.

Este é o processo de atualização:

1. O usuário executa um utilitário de atualização que aceita um arquivo de entrada com uma lista de APs e seus endereços IP, além de suas credenciais de login.
2. O utilitário estabelece sessões Telnet com os APs e envia uma série de comandos do Cisco IOS Software no arquivo de entrada para preparar o AP para a atualização. Esses comandos incluem os comandos para criar os SSCs. Além disso, o utilitário estabelece uma sessão Telnet com a WLC para programar o dispositivo para permitir a autorização de APs SSC específicos.
3. Em seguida, o utilitário carrega o Cisco IOS Software Release 12.3(7)JX no AP para que o AP possa ingressar na WLC.
4. Depois que o AP se une à WLC, o AP baixa uma versão completa do Cisco IOS Software da WLC. O utilitário de atualização gera um arquivo de saída que inclui a lista de APs e os valores de hash de chave SSC correspondentes que podem ser importados para o software de gerenciamento do Wireless Control System (WCS).
5. O WCS pode então enviar essas informações para outras WLCs na rede.

Depois que um AP se une a uma WLC, você pode reatribuir o AP a qualquer WLC na sua rede, se necessário.

Localize o hash da chave SHA1

Se o computador que executou a conversão de AP estiver disponível, você poderá obter o Hash da chave do Algoritmo de Hash Seguro 1 (SHA1) do arquivo .csv que está no diretório da Cisco Upgrade Tool. Se o arquivo .csv não estiver disponível, você pode emitir um comando **debug** na WLC para recuperar o hash da chave SHA1.

Conclua estes passos:

1. Ligue o AP e conecte-o à rede.
2. Ative a depuração na interface de linha de comando (CLI) da WLC.O comando é **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
```

Adicione o SSC à WLC

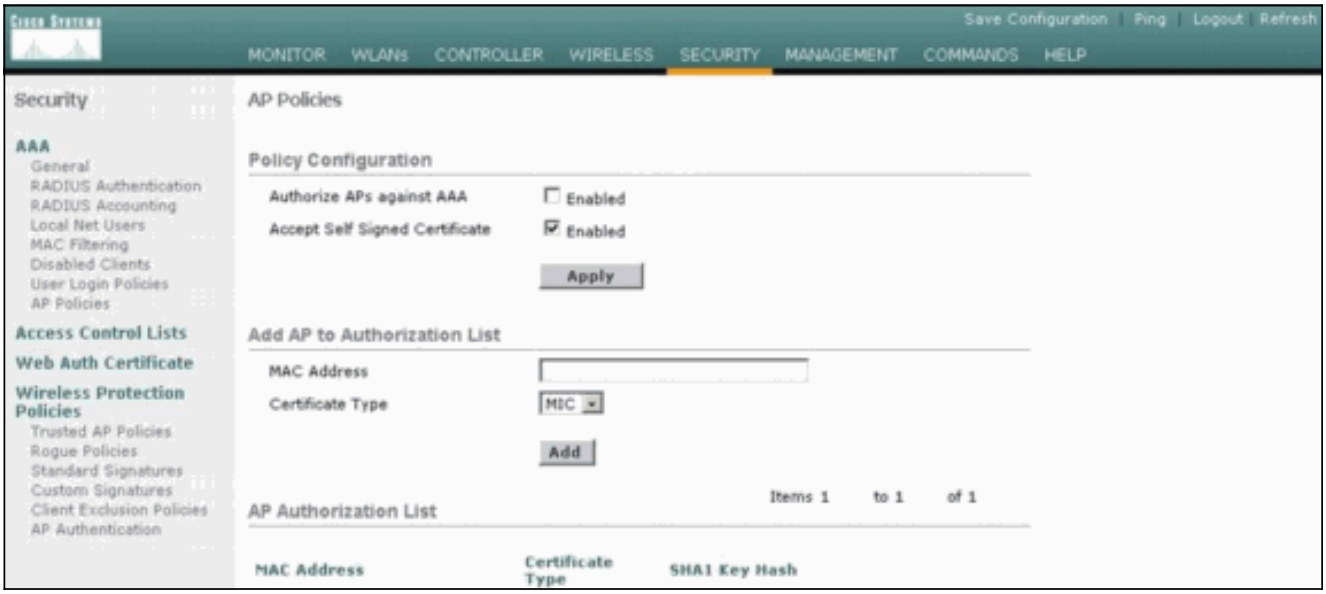
Tarefa

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

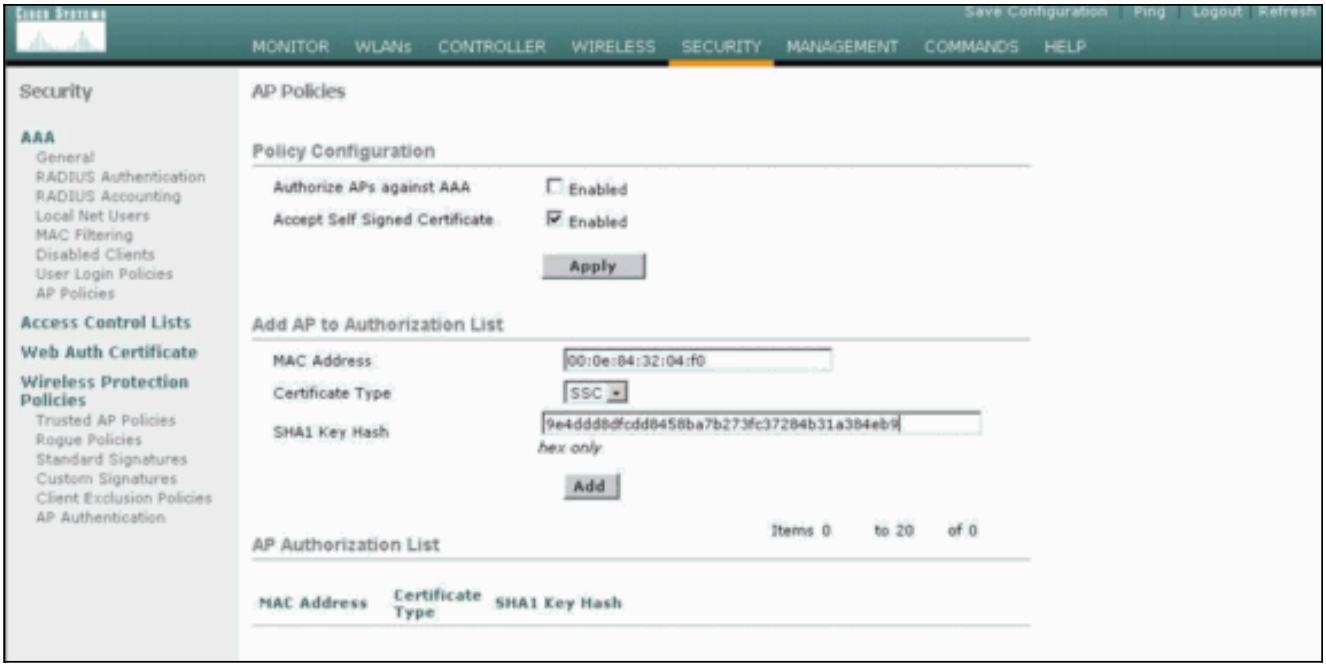
Configuração de GUI

Conclua estes passos da GUI:

1. Escolha **Security > AP Policies** e clique em **Enabled** ao lado de Accept Self Signed Certificate.



2. Selecione **SSC** no menu suspenso Tipo de certificado.



3. Insira o endereço MAC do AP e a chave hash e clique em **Adicionar**.

Configuração de CLI

Conclua estes passos da CLI:

1. Ative a opção Aceitar certificado autoassinado na WLC.O comando é **config auth-list ap-policy ssc enable**.
```
(Cisco Controller) >config auth-list ap-policy ssc enable
```

2. Adicione o endereço MAC do AP e a chave de hash à lista de autorização.O comando é **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.
```

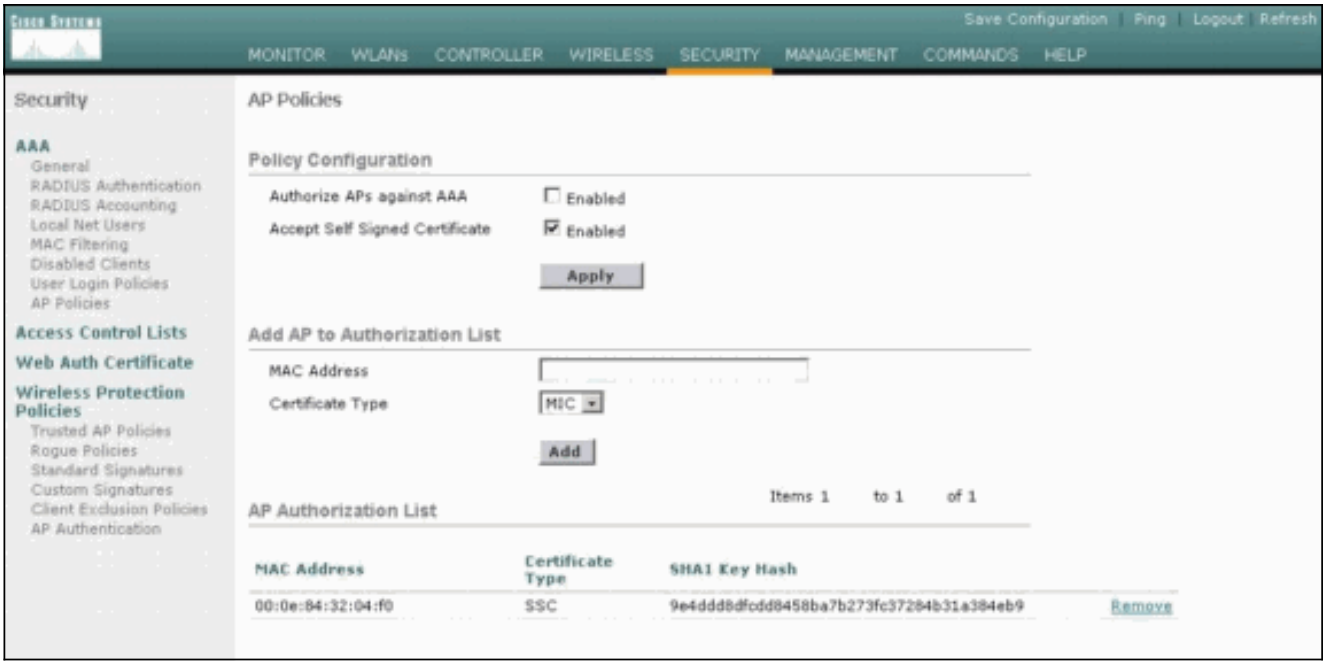
Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

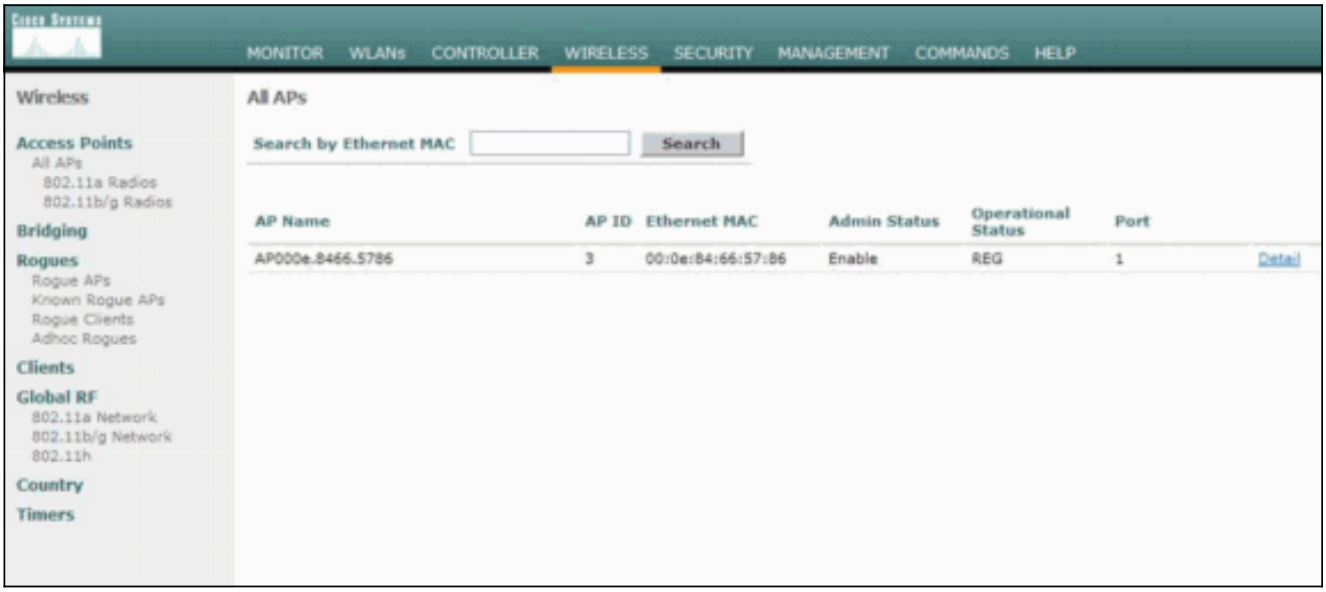
Verificação da GUI

Conclua estes passos:

1. Na janela Políticas de AP, verifique se o endereço MAC do AP e o hash da chave SHA1 aparecem na área Lista de autorização do
AP.



2. Na janela Todos os APs, verifique se todos os APs estão registrados na WLC.



Verificação da CLI

A Output Interpreter Tool (somente clientes registrados) (OIT) oferece suporte a determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

- **show auth-list** — Exibe a lista de autorização do AP.
- **show ap summary** — Exibe um resumo de todos os APs conectados.

Troubleshoot

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Informações Relacionadas

- Perguntas Frequentes de Troubleshooting de Controladoras Wireless LAN (WLC)
- Guia de Configuração da Cisco Wireless LAN Controller Release 3.2
- Exemplo de configuração básica dos controladores LAN sem fio e do access point lightweight
- Suporte Técnico e Documentação - Cisco Systems