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

Índice

Introdução
Pré-requisitos
Requisitos
Componentes Utilizados
Convenções
Informações de Apoio
Encontre a mistura da chave SHA1
Adicionar SSC ao WLC
Tarefa
Configuração de GUI
Configuração de CLI
Verificar
Troubleshooting
Informações Relacionadas

Introdução

Este documento explica os métodos que você pode usar a fim adicionar manualmente certificados auto-assinados (SSCs) a um controlador do Cisco Wireless LAN (WLAN) (WLC).

SSC de um Access Point (AP) deve existir em todos os WLC na rede a que o AP tem a permissão se registrar. Em regra geral, aplique SSC a todos os WLC no mesmo grupo da mobilidade. Quando a adição de SSC ao WLC não ocorre com a utilidade da elevação, você deve manualmente adicionar SSC ao WLC com uso do procedimento neste documento. Você igualmente precisa este procedimento quando um AP está movido para uma rede diferente ou quando os WLC adicionais estão adicionados à rede existente.

Você pode reconhecer este problema quando um protocolo de pouco peso AP (LWAPP) - AP convertido não associa ao WLC. Quando você pesquisa defeitos o problema de associação, você vê que estas saídas quando você emite estes debuga:

- Quando você emite o **comando debug pm pki enable**, você vê:`(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
```

Pré-requisitos

Requisitos

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

- O WLC não contém SSC que a utilidade da elevação gerou.
- Os AP contêm SSC.
- O telnet é permitido no WLC e no AP.
- A versão mínima do código de software PRE-LWAPP Cisco IOS® está no AP a ser promovido.

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 instalou
- 1230 Series AP do Cisco Aironet com SSC

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

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

Informações de Apoio

Em Cisco a arquitetura de WLAN centralizada, AP opera-se no modo leve. Os AP associam a Cisco WLC com o uso do LWAPP. O LWAPP é um protocolo de esboço do Internet Engineering Task Force (IETF) que defina a Mensagem do controle para operações da instalação e da autenticação e do tempo de execução do trajeto. O LWAPP também define o mecanismo de tunelamento para o tráfego de dados.

Um AP de pouco peso (REGAÇO) descobre um WLC com uso de mecanismos da descoberta LWAPP. O REGAÇO envia então o WLC que um LWAPP se junta ao pedido. O WLC envia o REGAÇO que um LWAPP se junta à resposta que permite que o REGAÇO se junte ao WLC. Quando o REGAÇO é juntado ao WLC, o REGAÇO transfere o software WLC se as revisões no REGAÇO e no WLC não combinam. Subseqüentemente, o REGAÇO está completamente sob o controle do WLC.

O LWAPP fixa a comunicação do controle entre o AP e o WLC por meio de uma distribuição chave segura. A distribuição chave segura exige os Certificados digitais X.509 já fornecida no REGAÇO e no WLC. Os certificados na fábrica são conhecidos pelo termo “MIC”, que é um acrônimo em inglês para Certificado Instalado na Fábrica. Aironet AP que enviou antes de julho 18, 2005, não tem MIC. Assim estes AP criam SSC quando são convertidos para se operar no modo leve. As controladoras são programadas para aceitar SSCs para a autenticação de APs específicos.

Este é o processo de upgrade:

1. O usuário executa uma utilidade da elevação que aceite um arquivo de entrada com uma lista de AP e de seus endereços IP de Um ou Mais Servidores Cisco ICM NT, além do que suas credenciais do início de uma sessão.
2. A utilidade estabelece sessões de Telnet com os AP e envia uma série de comandos do Cisco IOS Software no arquivo de entrada a fim preparar o AP para a elevação. Estes comandos include os comandos criar o SSCs. Também, a utilidade estabelece uma sessão de Telnet com o WLC a fim programar o dispositivo para permitir a autorização de SSC específico AP.
3. A utilidade carrega então o Cisco IOS Software Release 12.3(7)JX no AP de modo que o AP possa se juntar ao WLC.
4. Depois que o AP se junta ao WLC, o AP transfere uma versão de Cisco IOS Software completa do WLC. A utilidade da elevação gerencie um arquivo de saída que inclua a lista de AP e de valores correspondentes da chave-mistura de SSC que podem ser importados no software de gestão wireless do sistema de controle (WCS).
5. O WCS pode então enviar esta informação a outros WLC na rede.

Depois que um AP se junta a um WLC, você pode atribuir novamente o AP a todo o WLC em sua rede, caso necessário.

Encontre a mistura da chave SHA1

Se o computador que executou a conversão AP está disponível, você pode obter a mistura da chave do algoritmo de mistura segura 1 (SHA1) do arquivo .csv que está no diretório da ferramenta de upgrade de Cisco. Se o arquivo .csv é não disponível, você pode emitir um **comando debug no** WLC a fim recuperar a mistura da chave SHA1.

Conclua estes passos:

1. Gire sobre o AP e conecte-o à rede.
2. Permita a eliminação de erros no comando line interface(cli) WLC.O comando é **debuga o pki pm permite**.(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**

Adicionar SSC ao WLC

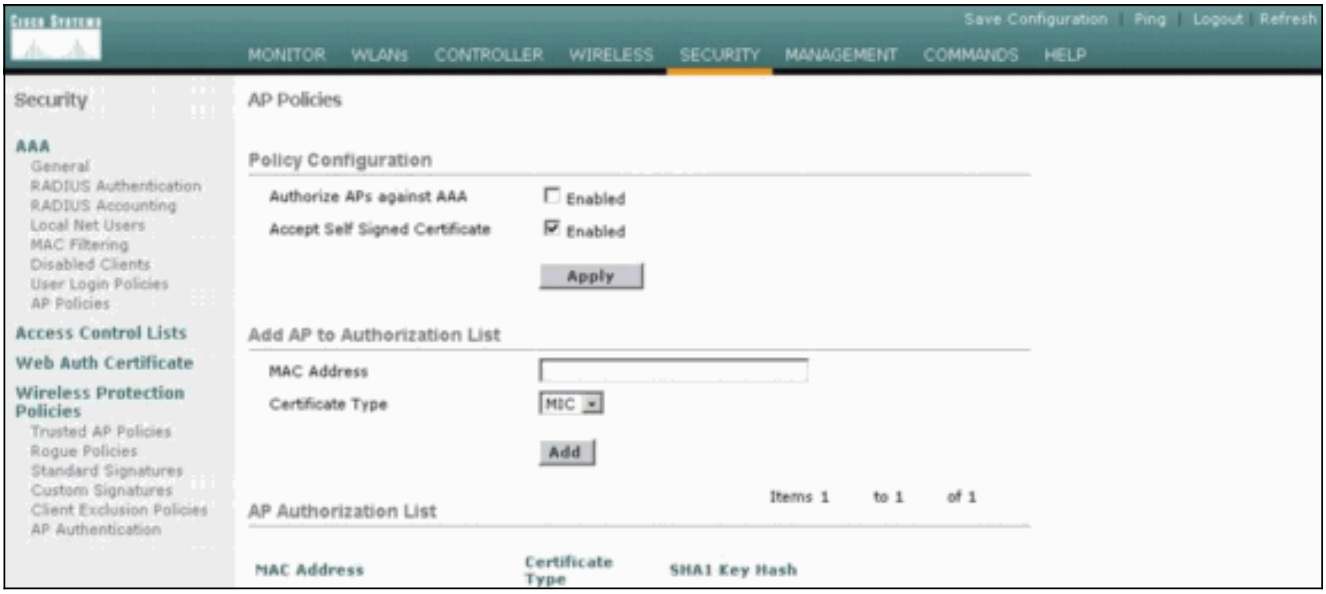
Tarefa

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

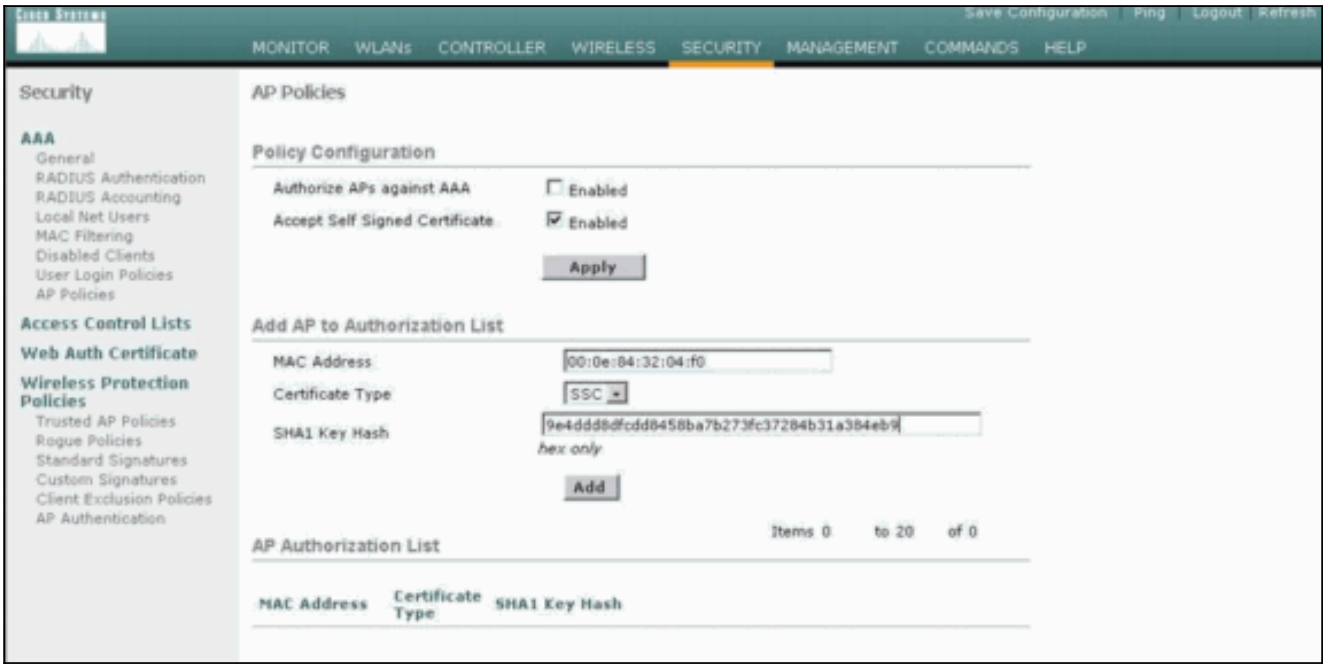
Configuração de GUI

Termine estas etapas do GUI:

1. Escolha a **Segurança > as políticas AP** e o clique **permitido** ao lado aceita o certificado assinado do
auto.



2. Selecione **SSC do** tipo menu suspenso do certificado.



3. Incorpore o MAC address do AP e da chave da mistura, e o clique **adiciona**.

Configuração de CLI

Termine estas etapas do CLI:

1. Permita aceitam o certificado assinado do auto no WLC.O comando é **ssc da ap-política da autêntico-lista da configuração permite**.`(Cisco Controller) >`**`config auth-list ap-policy ssc enable`**
2. Adicionar o MAC address AP e a chave da mistura à lista da autorização.O comando é autêntico-**lista da configuração adiciona o 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.`*

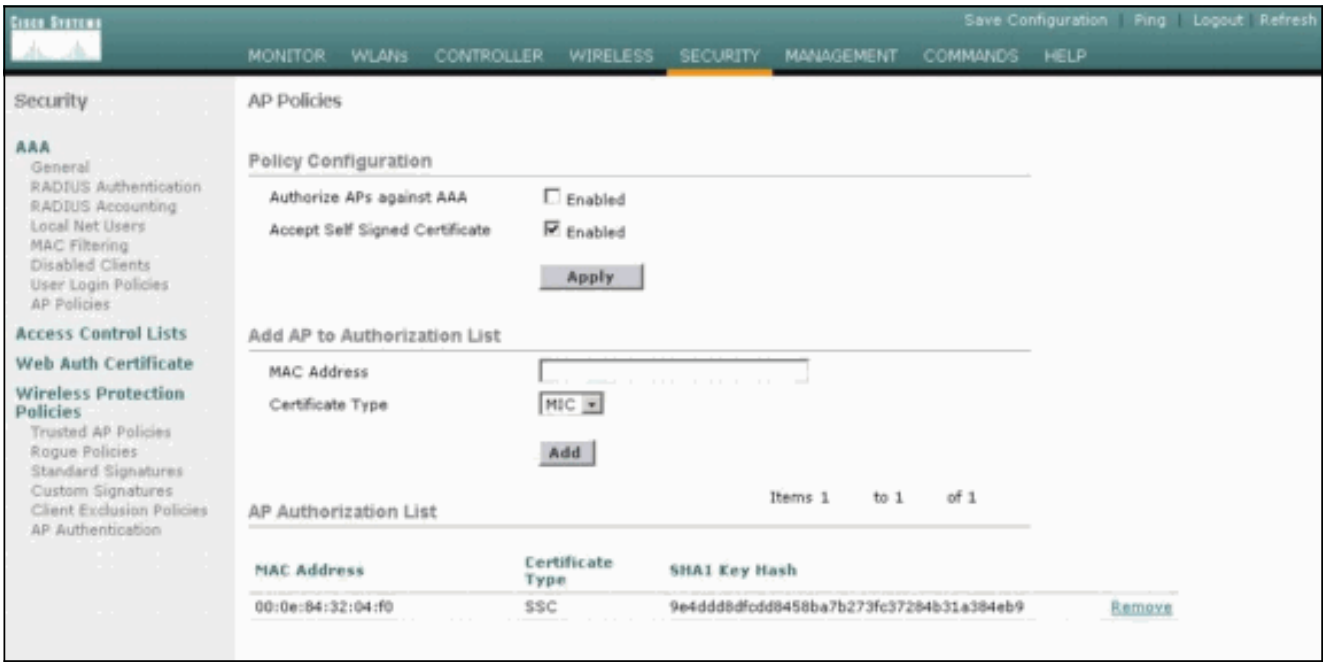
Verificar

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

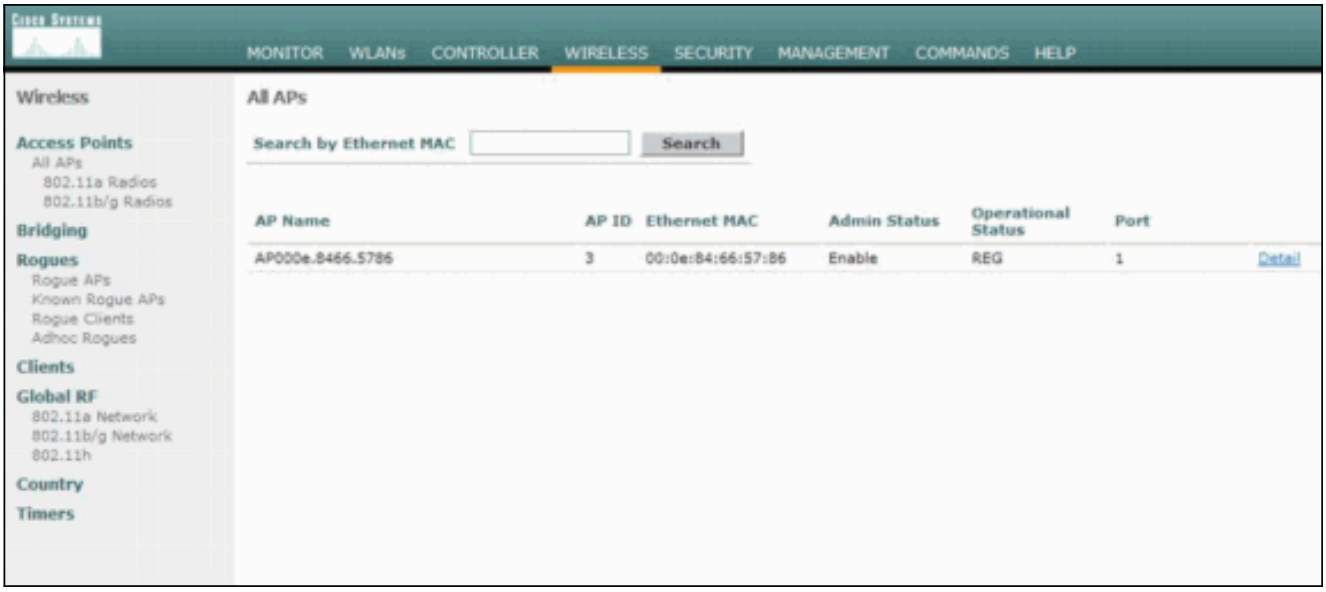
Verificação GUI

Conclua estes passos:

1. Na janela de políticas AP, verifique que o MAC address AP e a mistura SHA1 chave aparecem na área da lista da autorização AP.



2. Em toda a janela APS, verifique que todos os AP estão registrados com o WLC.



Verificação CLI

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

- **autêntico-lista da mostra** — Indica a lista da autorização AP.
- **mostre o sumário ap** — Indica um sumário de todos os AP conectados.

Troubleshooting

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 de Controladoras de Wireless LAN e Pontos de Acesso Lightweight
- Suporte Técnico e Documentação - Cisco Systems