Configuração dos serviços do domínio sem fio

Contents

Introduction

Este documento introduz o conceito de serviços de domínio sem fio (WDS). O documento também descreve como configurar um ponto de acesso (AP) ou o Wireless LAN Services Module (WLSM) como o WDS e pelo menos um outro como um AP de infraestrutura. O procedimento neste documento fornece orientações sobre um WDS que é funcional e permite que clientes associem ao WDS AP ou a um AP de infraestrutura. Este documento pretende estabelecer uma base a partir da qual você pode configurar o Fast Secure Roaming ou introduzir um Wireless LAN Solutions Engine (WLSE) na rede, para que você possa usar os recursos.

Prerequisites

Requirements

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

- Tenha um conhecimento profundo das redes LAN sem fio e dos problemas de segurança sem fio.
- Ter conhecimento dos métodos de segurança atuais do Extensible Authentication Protocol (EAP).

Componentes Utilizados

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

- APs com o software Cisco IOS®
- Software Cisco IOS versão 12.3(2)JA2 ou posterior
- Módulo de serviços de LAN sem fio Catalyst 6500 Series

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos usados neste documento começaram com uma configuração limpa (padrão) e um endereço IP na interface BVI1, de modo que a unidade é acessível a partir da GUI do software Cisco IOS ou da interface de linha de comando (CLI). Se você trabalha em uma rede ativa, certifique-se de entender o impacto potencial de qualquer comando.

Conventions

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

Serviços de domínio sem fio

O WDS é um novo recurso para APs no Cisco IOS Software e a base do Catalyst 6500 Series WLSM. O WDS é uma função central que permite outros recursos como estes:

- Roaming seguro rápido
- interação WLSE
- Gerenciamento de rádio

Você deve estabelecer relações entre os APs que participam do WDS e do WLSM, antes que qualquer outro recurso baseado em WDS funcione. Uma das finalidades do WDS é eliminar a necessidade de validação de credenciais de usuário pelo servidor de autenticação e reduzir o tempo necessário para as autenticações de cliente.

Para usar o WDS, você deve designar um AP ou o WLSM como o WDS. Um AP WDS deve usar um nome de usuário e senha WDS para estabelecer uma relação com um servidor de autenticação. O servidor de autenticação pode ser um servidor RADIUS externo ou o recurso Local RADIUS Server no AP WDS. O WLSM deve ter uma relação com o servidor de autenticação, mesmo que o WLSM não precise se autenticar no servidor.

Outros APs, chamados de APs de infraestrutura, comunicam-se com o WDS. Antes do registro, os APs de infraestrutura devem se autenticar no WDS. Um grupo de servidores de infraestrutura no WDS define essa autenticação de infraestrutura.

Um ou mais grupos de servidores clientes no WDS definem a autenticação de clientes.

Quando um cliente tenta se associar a um AP de infraestrutura, o AP de infraestrutura passa as credenciais do usuário para o WDS para validação. Se o WDS vir as credenciais pela primeira vez, o WDS volta para o servidor de autenticação para validar as credenciais. Em seguida, o WDS coloca em cache as credenciais, para eliminar a necessidade de voltar ao servidor de autenticação quando o mesmo utilizador tentar novamente a autenticação. Exemplos de reautenticação incluem:

- Nova chaveamento
- Roaming
- Quando o usuário inicia o dispositivo cliente

Qualquer protocolo de autenticação EAP baseado em RADIUS pode ser encapsulado por meio de WDS como:

- EAP leve (LEAP)
- PEAP (EAP Protegido)
- EAP-Transport Layer Security (EAP-TLS)
- Autenticação EAP-Flexível através do Secure Tunneling (EAP-FAST)

A autenticação de endereço MAC também pode fazer o túnel para um servidor de autenticação externo ou em uma lista local para um AP WDS. O WLSM não suporta autenticação de endereço MAC.

O WDS e os APs de infraestrutura comunicam-se através de um protocolo multicast chamado WLAN Context Control Protocol (WLCCP). Essas mensagens multicast não podem ser roteadas, portanto, um WDS e os APs de infraestrutura associados devem estar na mesma sub-rede IP e no mesmo segmento de LAN. Entre o WDS e o WLSE, o WLCCP usa TCP e o User Datagram Protocol (UDP) na porta 2887. Quando o WDS e o WLSE estão em sub-redes diferentes, um protocolo como a Network Address Translation (NAT) não pode converter os pacotes.

Um AP configurado como dispositivo WDS suporta até 60 APs participantes. Um Integrated Services Router (ISR) configurado como dispositivos WDS suporta até 100 APs participantes. E um switch equipado com WLSM suporta até 600 APs participantes e até 240 grupos de mobilidade. Um único AP suporta até 16 grupos de mobilidade.

Observação: a Cisco recomenda que os APs de infraestrutura executem a mesma versão do IOS que o dispositivo WDS. Se você usar uma versão mais antiga do IOS, os APs podem falhar na autenticação para o dispositivo WDS. Além disso, a Cisco recomenda que você use a versão mais recente do IOS. Você pode encontrar a versão mais recente do IOS na página Downloads sem fio.

Função do dispositivo WDS

O dispositivo WDS executa várias tarefas na sua LAN sem fios:

- Anuncia sua capacidade WDS e participa da escolha do melhor dispositivo WDS para sua LAN sem fio. Ao configurar sua LAN sem fio para WDS, você configura um dispositivo como o principal candidato WDS e um ou mais dispositivos adicionais como candidatos WDS de backup. Se o dispositivo WDS principal ficar offline, um dos dispositivos WDS de backup ocupará seu lugar.
- Autentica todos os APs na sub-rede e estabelece um canal de comunicação seguro com cada um deles.
- Coleta dados de rádio de APs na sub-rede, agrega os dados e os encaminha para o dispositivo WLSE na sua rede.
- Funciona como uma passagem para todos os dispositivos cliente autenticados 802.1x associados aos APs participantes.
- Registra todos os dispositivos clientes na sub-rede que usam chaveamento dinâmico, estabelece chaves de sessão para eles e armazena em cache suas credenciais de

segurança. Quando um cliente faz roaming para outro AP, o dispositivo WDS encaminha as credenciais de segurança do cliente para o novo AP.

Função dos pontos de acesso usando o dispositivo WDS

Os APs em sua LAN sem fio interagem com o dispositivo WDS nestas atividades:

- Descubra e rastreie o dispositivo WDS atual e retransmita os anúncios WDS para a LAN sem fio.
- Autentique com o dispositivo WDS e estabeleça um canal de comunicação seguro para o dispositivo WDS.
- Registre os dispositivos de cliente associados com o dispositivo WDS.
- Informar os dados de rádio para o dispositivo WDS.

Configuração

O WDS apresenta a configuração de forma ordenada e modular. Cada conceito baseia-se no conceito que precede. O WDS omite outros itens de configuração, como senhas, acesso remoto e configurações de rádio para esclarecer e focar no assunto principal.

Esta seção apresenta as informações necessárias para configurar os recursos descritos neste documento.

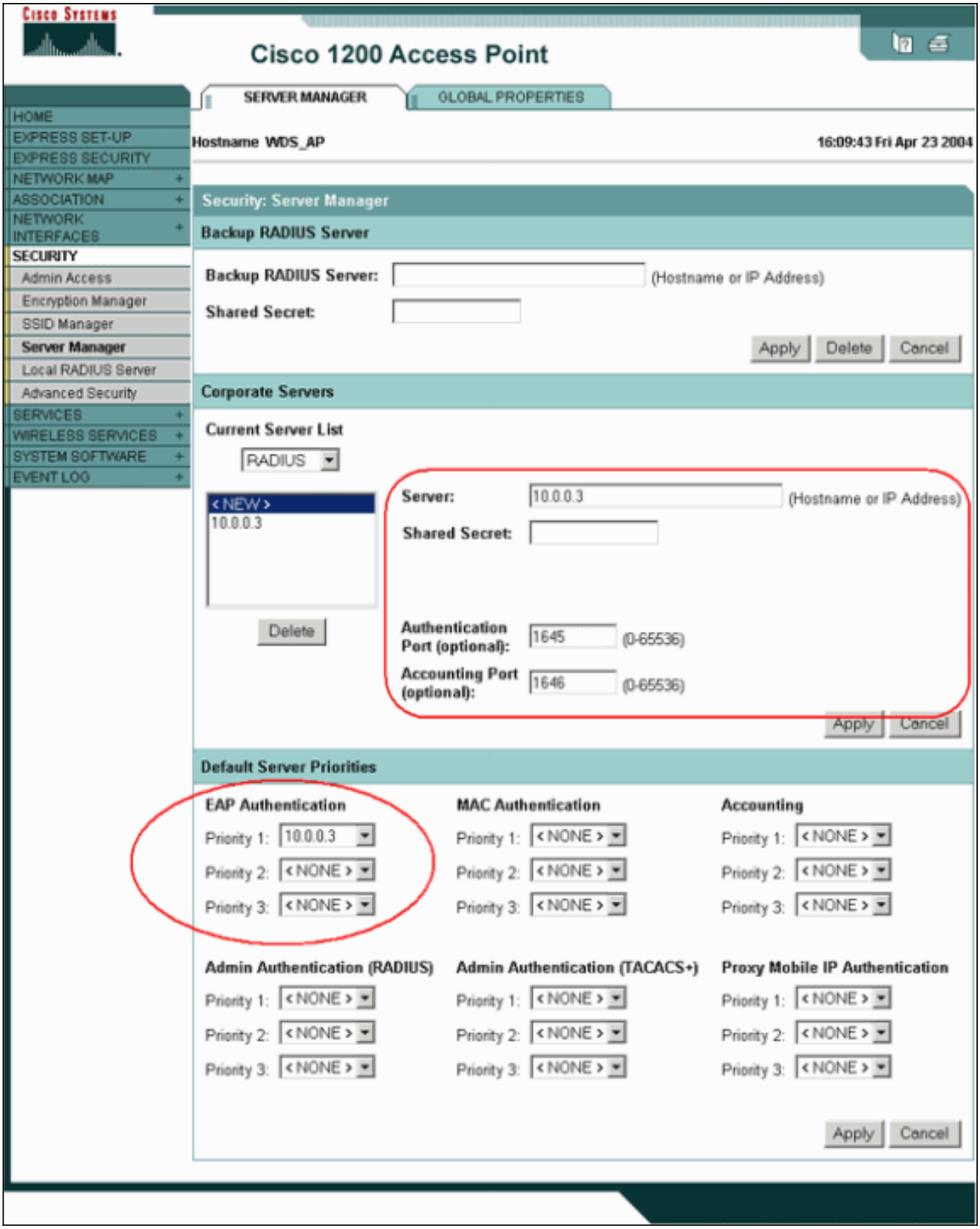
Nota: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Designar um AP como WDS

A primeira etapa é designar um AP como o WDS. O AP WDS é o único que se comunica com o servidor de autenticação.

Conclua estes passos para designar um AP como WDS:

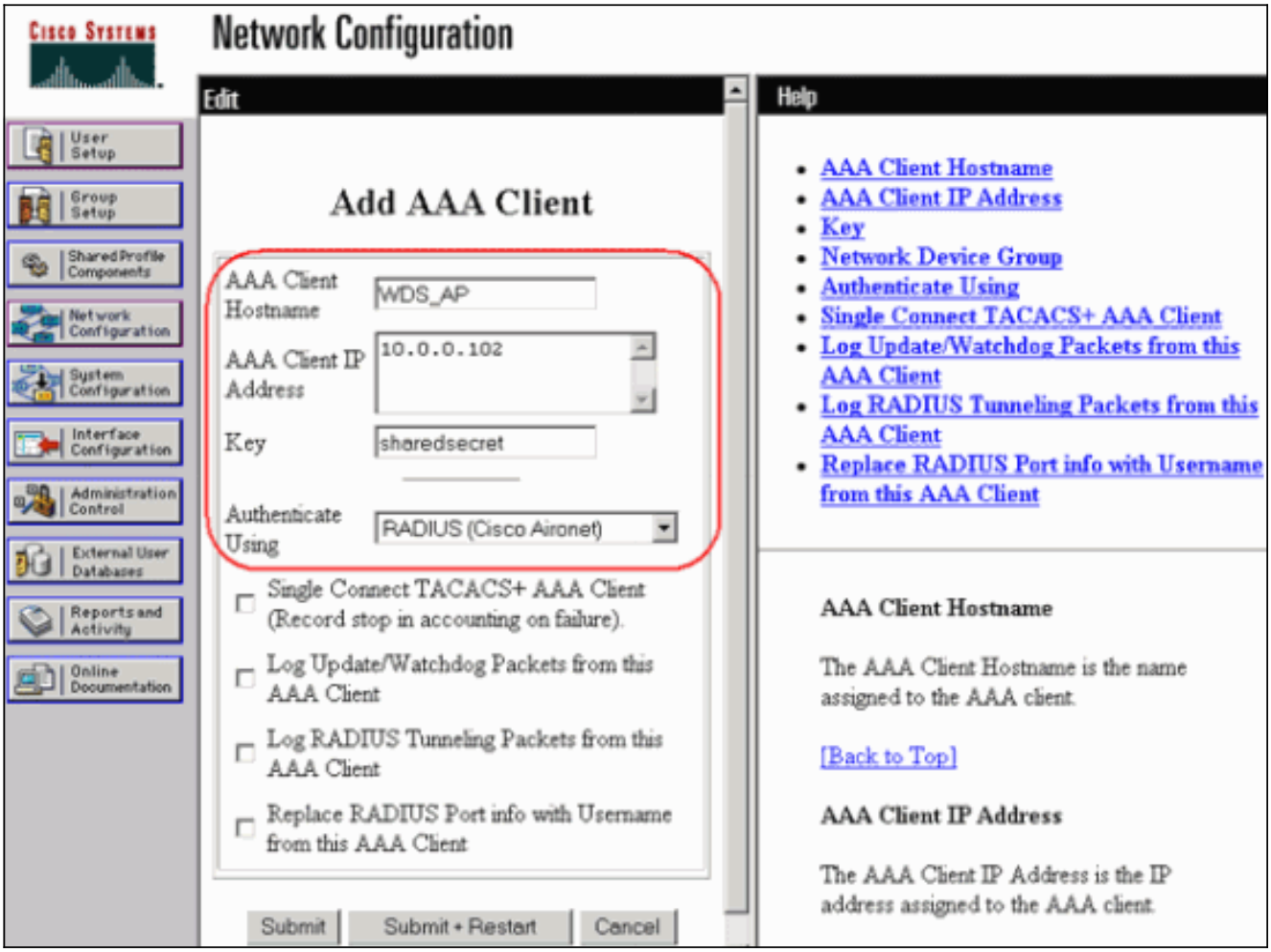
1. Para configurar o servidor de autenticação no AP WDS, escolha **Security > Server Manager** para ir para a guia Server Manager:Em Servidores Corporativos, digite o endereço IP do servidor de autenticação no campo Servidor.Especifique o segredo compartilhado e as portas.Em Prioridades de servidor padrão, defina o campo Prioridade 1 para esse endereço IP do servidor sob o tipo de autenticação apropriado.



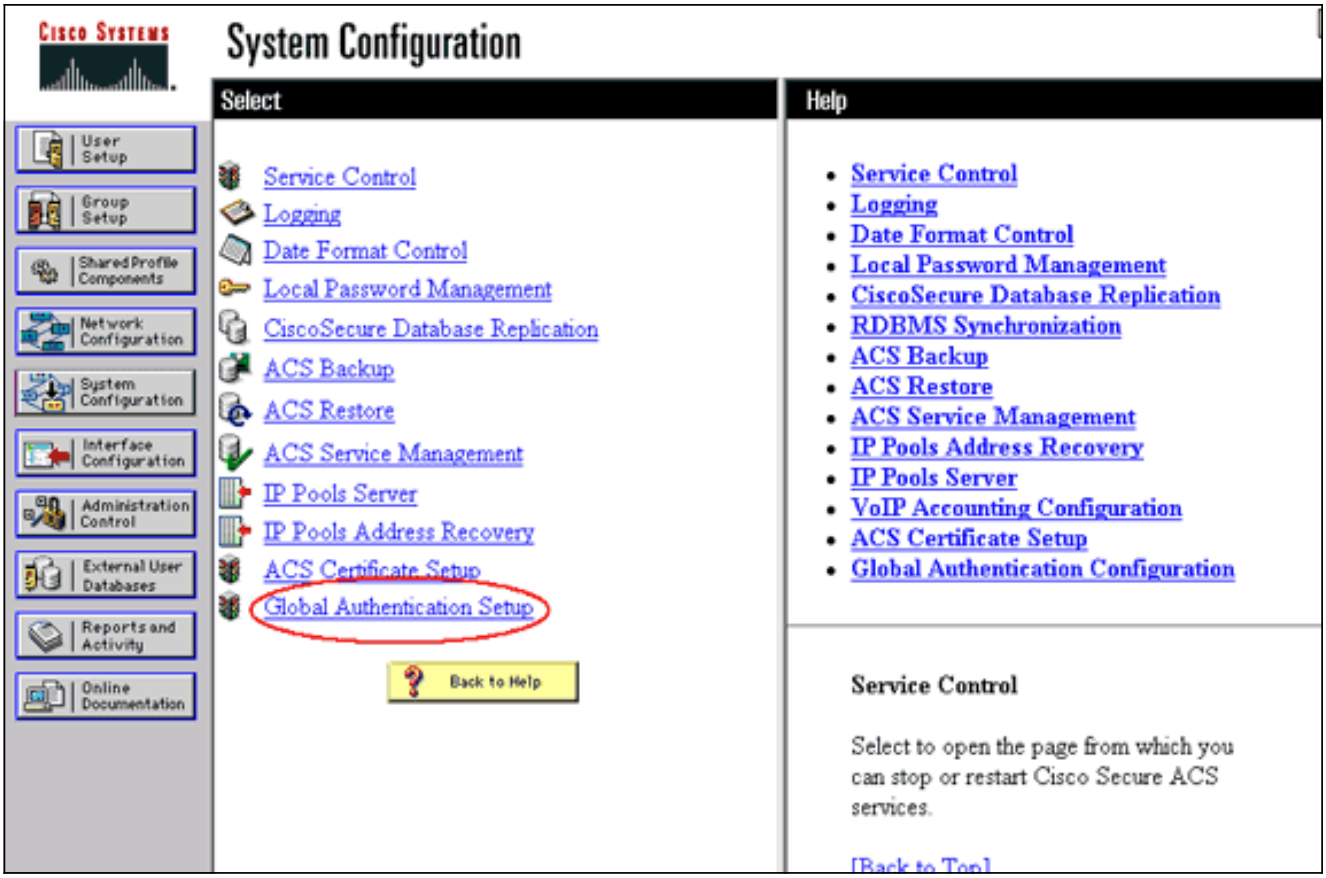
Como alternativa, emita estes comandos da CLI:

2. A próxima etapa é configurar o AP WDS no servidor de autenticação como um cliente de autenticação, autorização e contabilização (AAA). Para isso, você precisa adicionar o AP WDS como um cliente AAA. Conclua estes passos:**Observação:** este documento usa o servidor Cisco Secure ACS como o servidor de autenticação.No Cisco Secure Access Control Server (ACS), isso ocorre na página Network Configuration onde você define estes atributos para o AP WDS:NomeEndereço IPShared secretMétodo de autenticaçãoRADIUS Cisco AironetInternet Engineering Task Force [IETF] de RADIUSClique em **Enviar**.Para outros servidores de autenticação não-ACS, consulte a documentação do

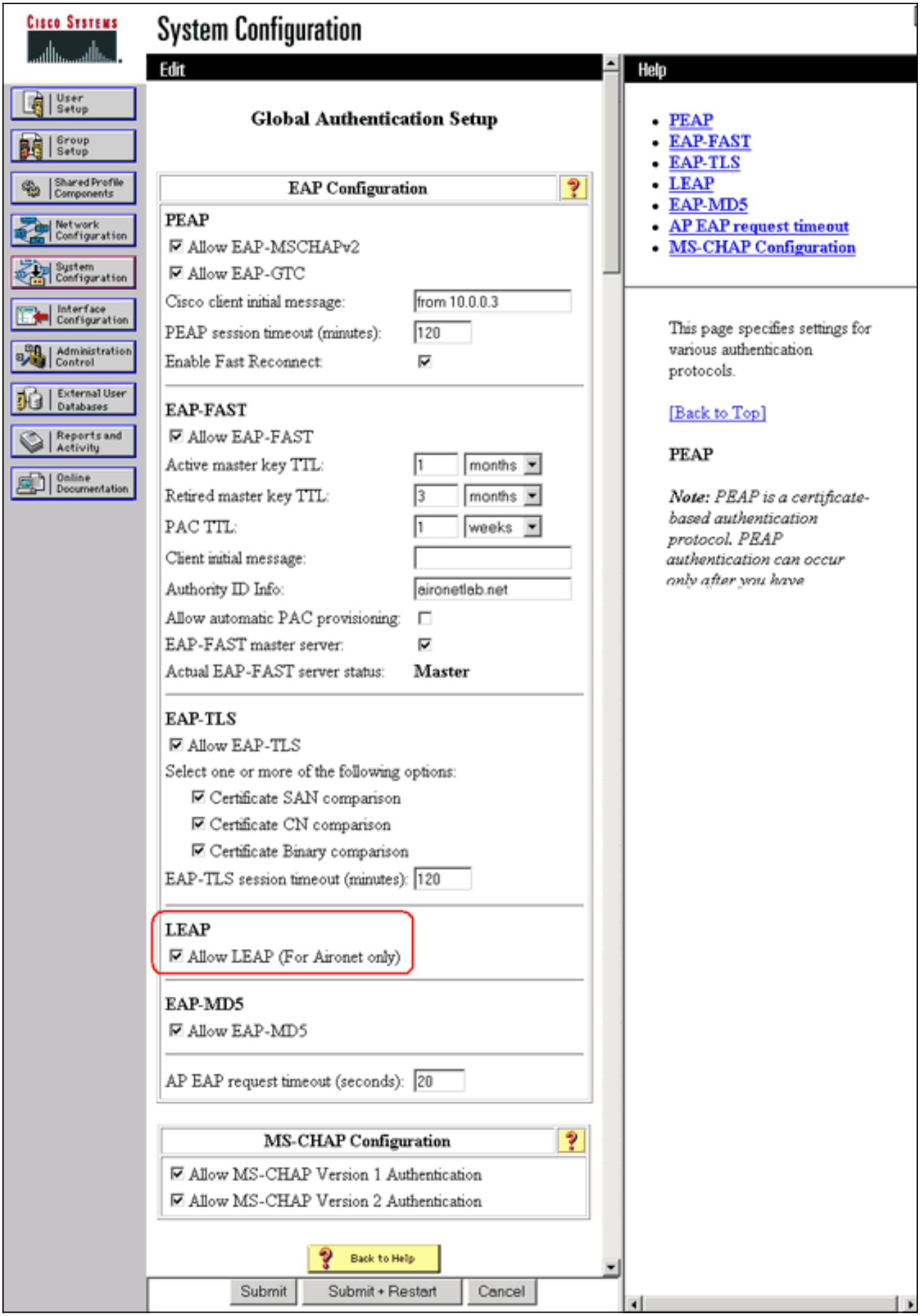
fabricante.



Além disso, no Cisco Secure ACS, certifique-se de configurar o ACS para executar a autenticação LEAP na página System Configuration - Global Authentication Setup. Primeiro, clique em **Configuração do sistema** e, em seguida, clique em **Configuração de autenticação global**.

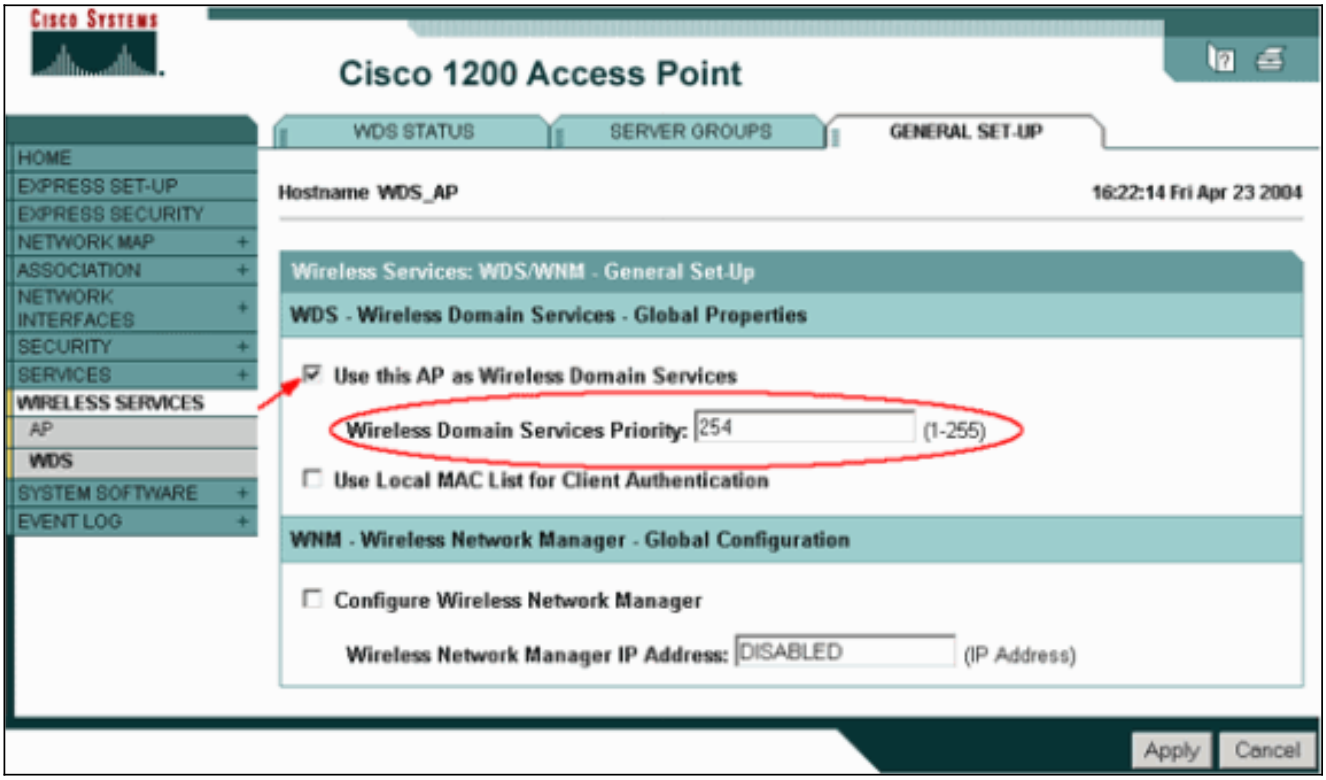


Role a página para baixo até a configuração LEAP. Quando a caixa é marcada, o ACS autentica o
LEAP.



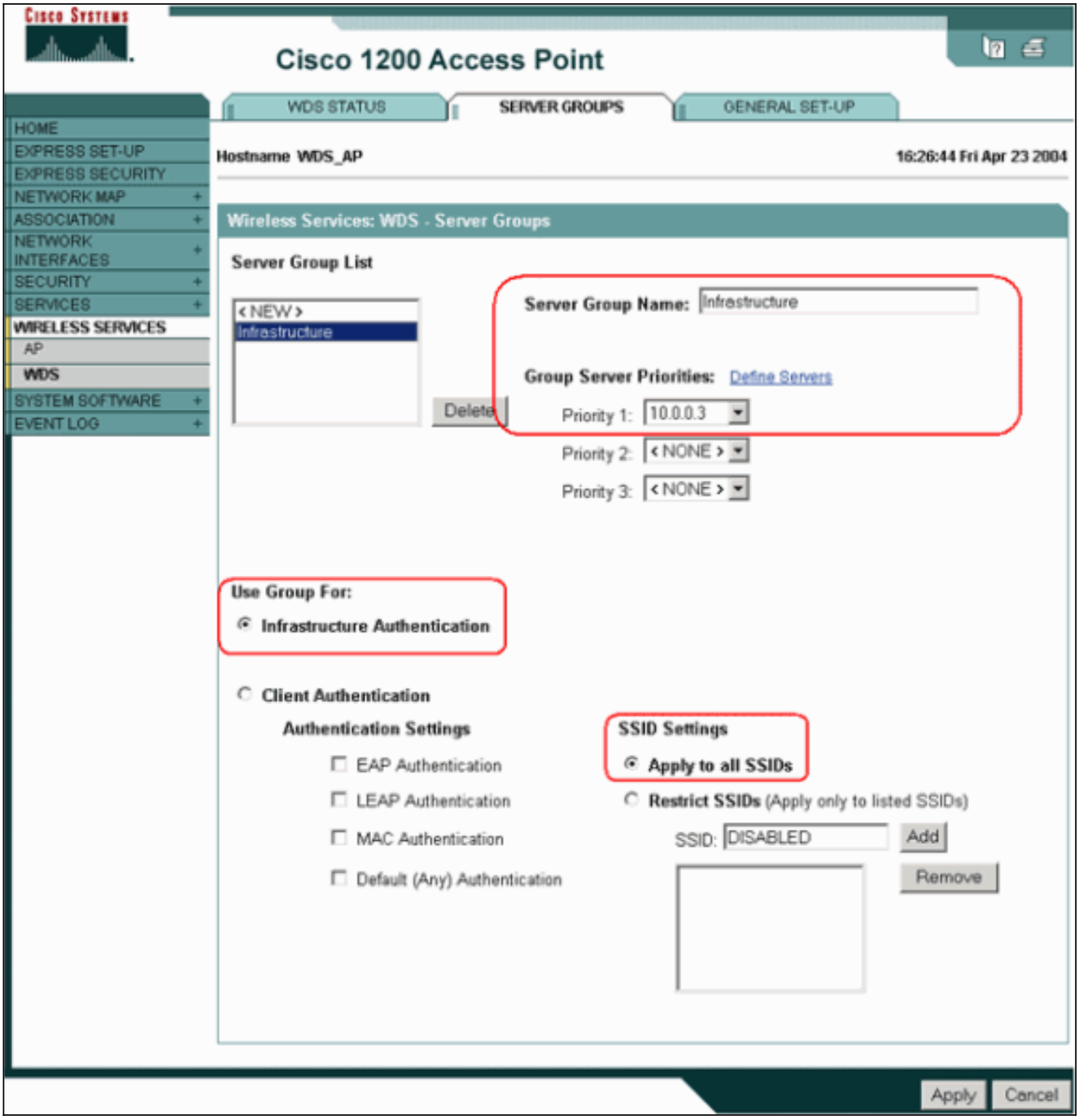
3. Para configurar as configurações WDS no AP WDS, escolha **Serviços sem fio > WDS** no AP WDS e clique na guia **Configuração geral**. Execute estas etapas:Em WDS-Wireless Domain Services - Global Properties, marque **Use this AP as Wireless Domain Services**.Defina o

valor do campo Wireless Domain Services Priority como um valor de aproximadamente **254**, pois este é o primeiro. Você pode configurar um ou mais APs ou switches como candidatos para fornecer WDS. O dispositivo com a maior prioridade fornece
WDS.



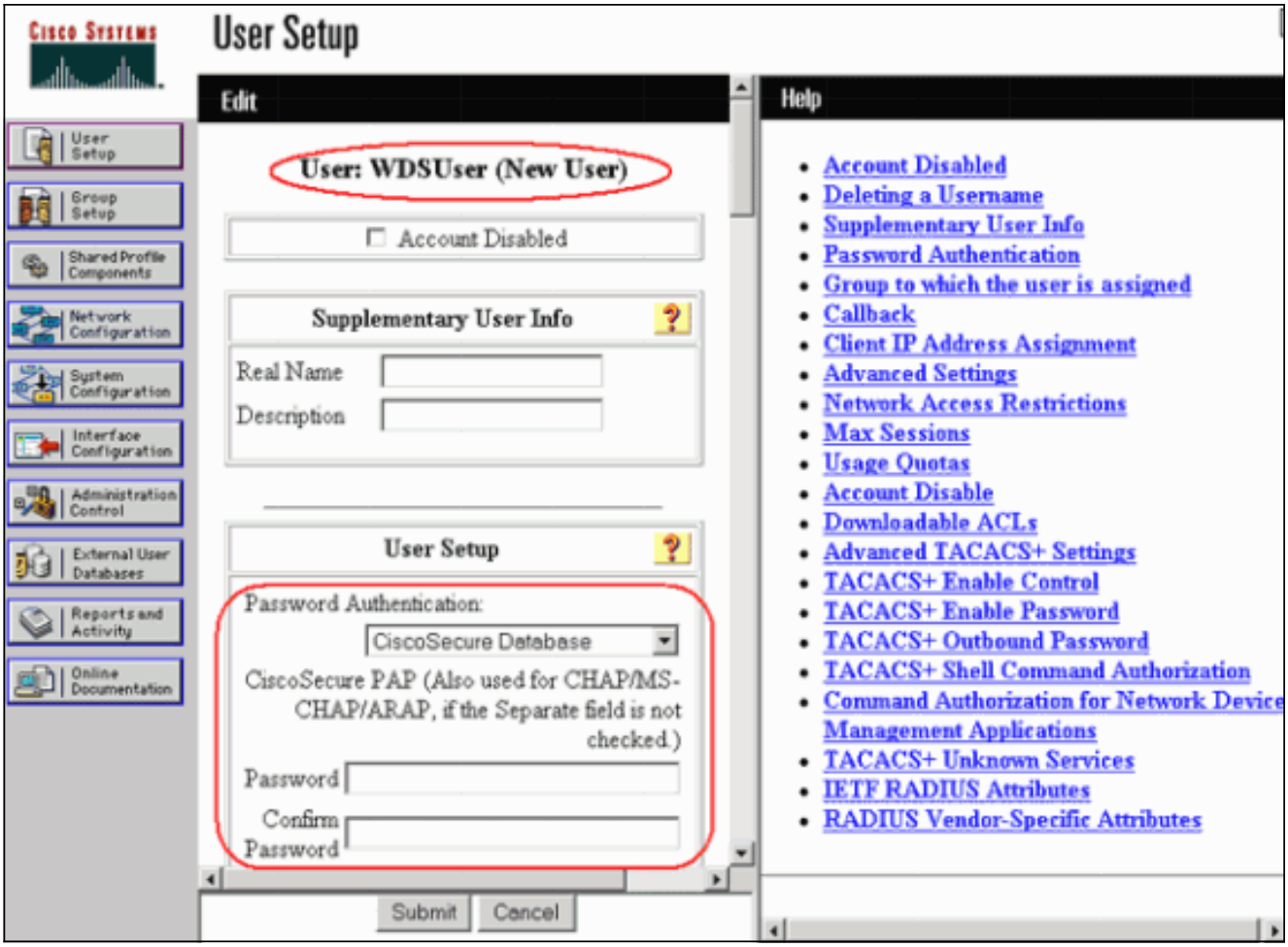
Como alternativa, emita estes comandos da CLI:

4. Escolha **Wireless Services > WDS** e vá para a guia **Server Groups**:Defina um Nome do Grupo de Servidores que autentica os outros APs, um grupo de Infraestrutura.Defina a prioridade 1 para o servidor de autenticação configurado anteriormente.Clique em **Usar grupo para:** Botão de opção **Infrastructure Authentication**.Aplique as configurações aos SSIDs
relevantes.



Como alternativa, emita estes comandos da CLI:

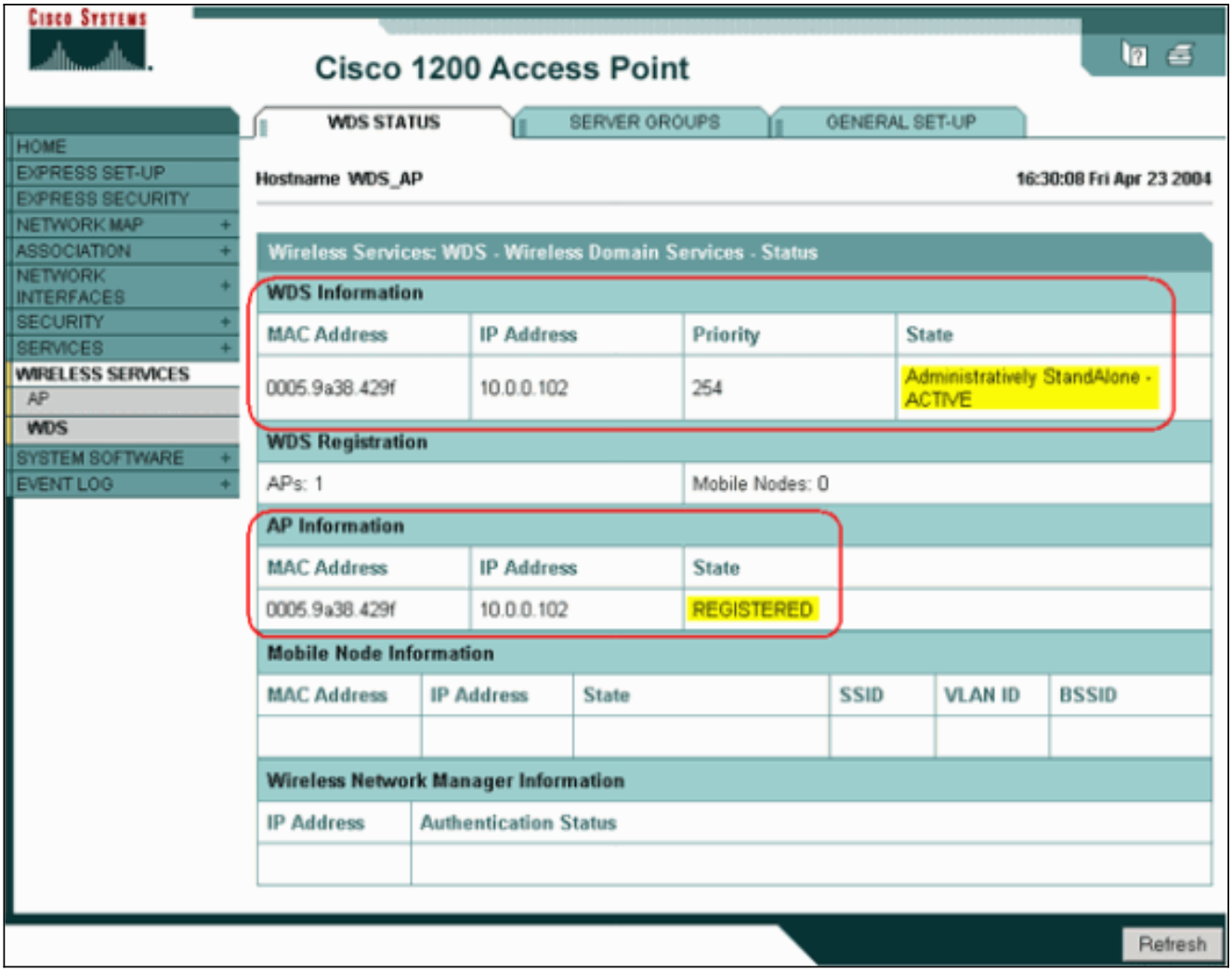
5. Configure o nome de usuário e a senha WDS como um usuário no servidor de autenticação.No Cisco Secure ACS, isso ocorre na página User Setup, onde você define o nome de usuário e a senha do WDS. Para outros servidores de autenticação não-ACS, consulte a documentação do fabricante.**Observação:** não coloque o usuário WDS em um grupo que recebe muitos direitos e privilégios — o WDS requer apenas autenticação limitada.



6. Escolha **Wireless Services > AP** e clique em **Enable** para a opção Participate in SWAN infrastructure. Em seguida, digite o nome de usuário e a senha WDS.Você deve definir um nome de usuário e uma senha WDS no servidor de autenticação para todos os diapositivos que designam membros do
WDS.

Como alternativa, emita estes comandos da CLI:

7. Escolha **Wireless Services > WDS**. Na guia Status WDS AP WDS, verifique se o AP WDS aparece na área Informações do WDS, no estado ATIVO. O AP também deve aparecer na área AP Information, com State como REGISTERED.Se o AP não for exibido REGISTERED ou ATIVE, verifique se há erros no servidor de autenticação ou tentativas de autenticação com falha.Quando o AP se registrar adequadamente, adicione um AP de infraestrutura para usar os serviços do
WDS.



Como alternativa, emita estes comandos da CLI:**Nota:** Não é possível testar associações de clientes porque a autenticação de clientes ainda não tem provisões.

Designar um WLSM como WDS

Esta seção explica como configurar um WLSM como um WDS. O WDS é o único dispositivo que se comunica com o servidor de autenticação.

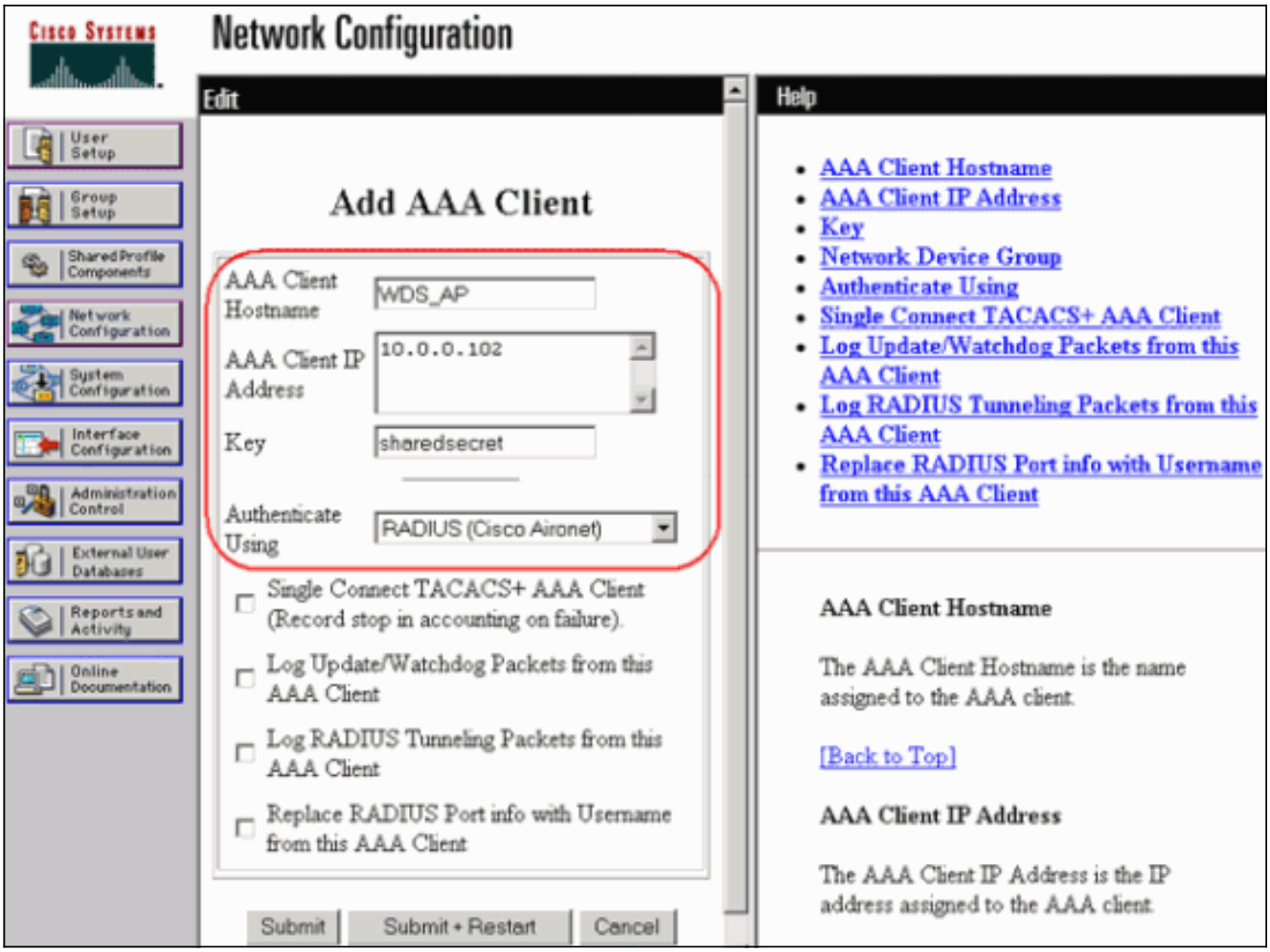
Observação: emita esses comandos no prompt de comando `enable` do WLSM, não do Supervisor Engine 720. Para chegar ao prompt de comando do WLSM, emita esses comandos em um prompt de comando `enable` no Supervisor Engine 720:

```
c6506#session slot x proc 1
!--- In this command, x is the slot number where the
WLSM resides. The default escape character is Ctrl-^,
then x. You can also type 'exit' at the remote prompt to
end the session Trying 127.0.0.51 ... Open User Access
Verification Username: <username> Password: <password>
wlan>enable
Password: <enable password>
wlan#
```

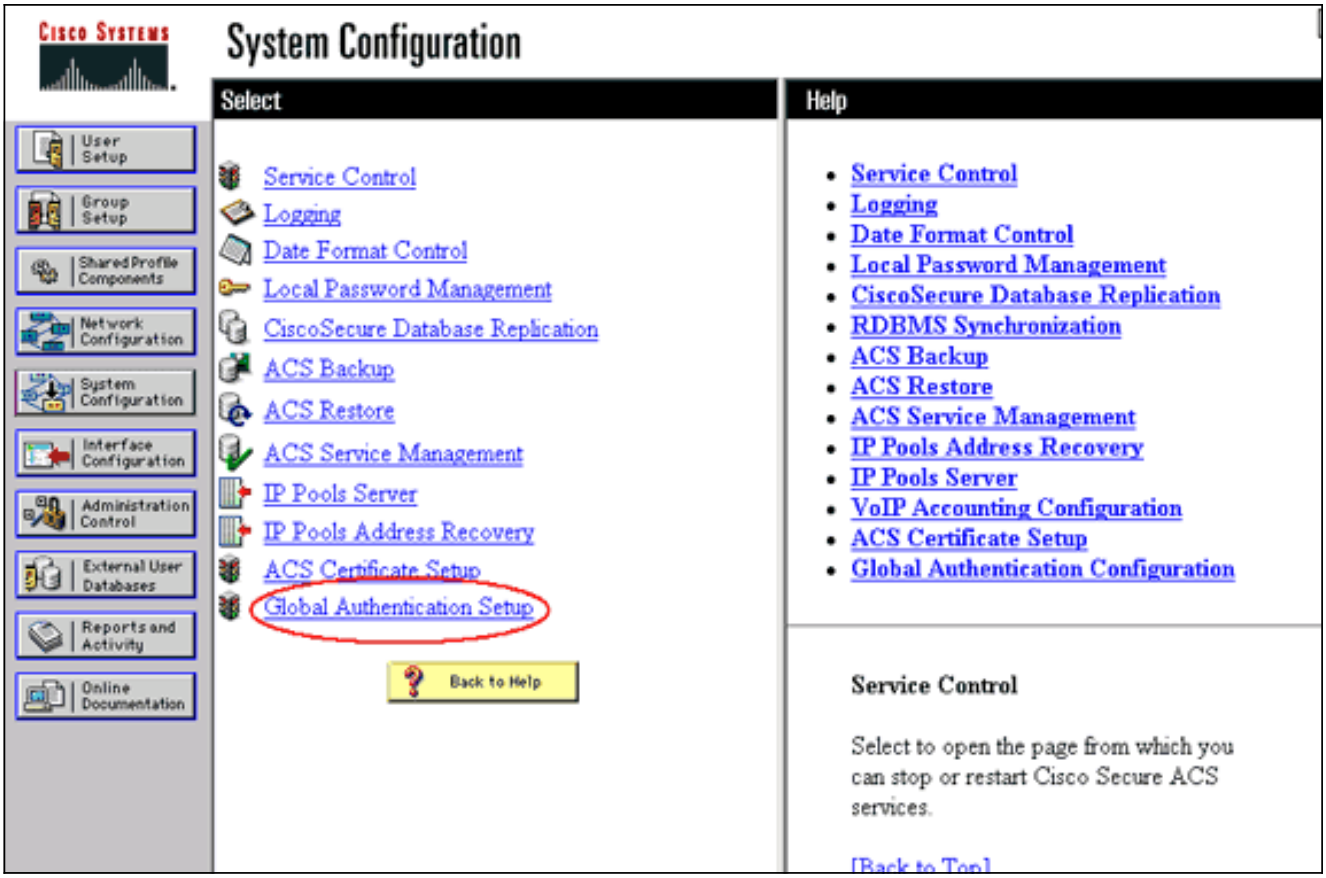
Observação: para solucionar problemas e manter seu WLSM mais facilmente, configure o acesso remoto Telnet ao WLSM. Consulte a Configuração de Acesso Remoto de Telnet.

Para designar um WLSM como WDS:

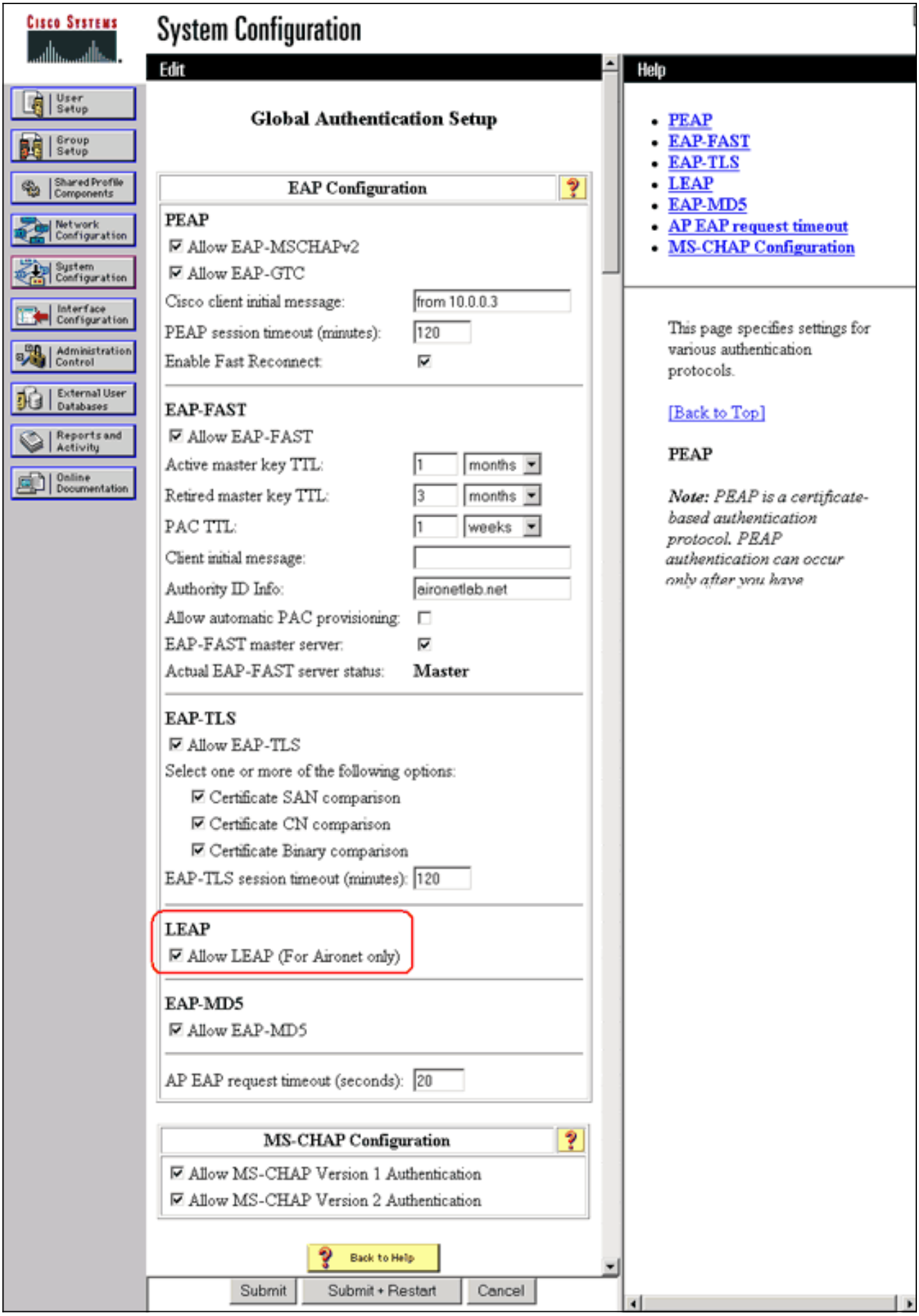
1. Na CLI do WLSM, emita estes comandos e estabeleça uma relação com o servidor de autenticação:**Observação:** não há controle de prioridade no WLSM. Se a rede contiver vários módulos WLSM, o WLSM usará configuração de redundância para determinar o módulo principal.
2. Configure o WLSM no servidor de autenticação como um cliente AAA.No Cisco Secure ACS, isso ocorre na página Network Configuration onde você define estes atributos para o WLSM:NomeEndereço IPShared secretMétodo de autenticaçãoRADIUS Cisco AironetIETF RADIUSPara outros servidores de autenticação não-ACS, consulte a documentação do fabricante.



Além disso, no Cisco Secure ACS, configure o ACS para executar a autenticação LEAP na página System Configuration - Global Authentication Setup. Primeiro, clique em **Configuração do sistema** e, em seguida, clique em **Configuração de autenticação global**.



Role a página para baixo até a configuração LEAP. Quando a caixa é marcada, o ACS autentica o
LEAP.



3. No WLSM, defina um método que autentique os outros APs (um grupo de servidores de infraestrutura).
4. No WLSM, defina um método que autentica os dispositivos do cliente (um grupo de

servidores cliente) e os tipos de EAP que esses clientes usam.**Observação:** esta etapa elimina a necessidade do processo Definir Método de Autenticação de Cliente.

5. Defina uma VLAN exclusiva entre o Supervisor Engine 720 e o WLSM para permitir que o WLSM se comunique com entidades externas, como APs e servidores de autenticação. Esta VLAN não está sendo usada em nenhum outro lugar ou para qualquer outra finalidade na rede. Crie primeiro a VLAN no Supervisor Engine 720 e, em seguida, emita estes comandos:No Supervisor Engine 720:No WLSM:
6. Verifique a função do WLSM com esses comandos:No WLSM:No Supervisor Engine 720:

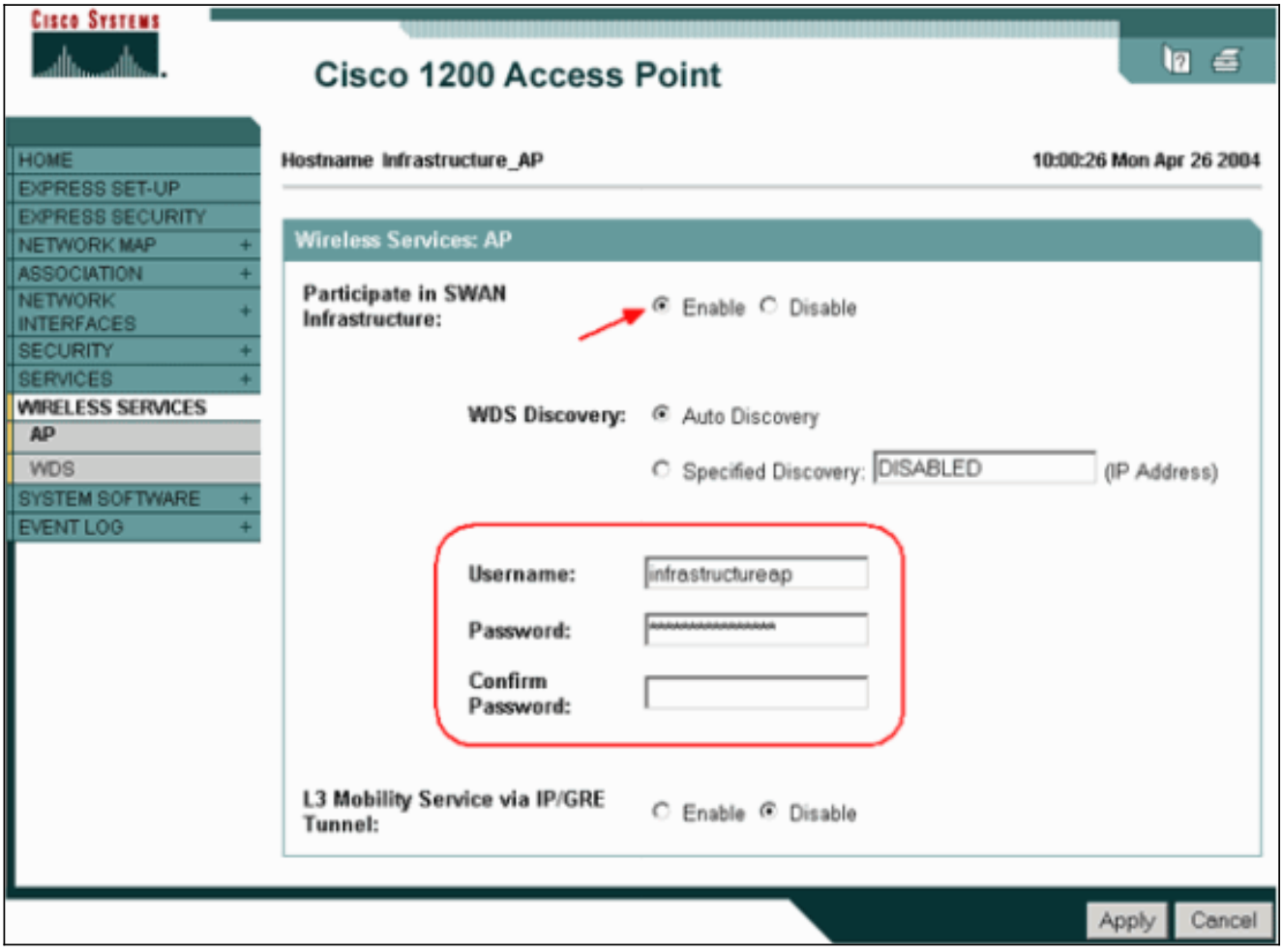
Designar um AP como dispositivo de infraestrutura

Em seguida, você deve designar pelo menos um AP de infraestrutura e relacionar o AP ao WDS. Os clientes se associam aos APs de infraestrutura. Os APs de infraestrutura solicitam que o WDS AP ou WLSM execute a autenticação para eles.

Conclua estes passos para adicionar um AP de infraestrutura que use os serviços do WDS:

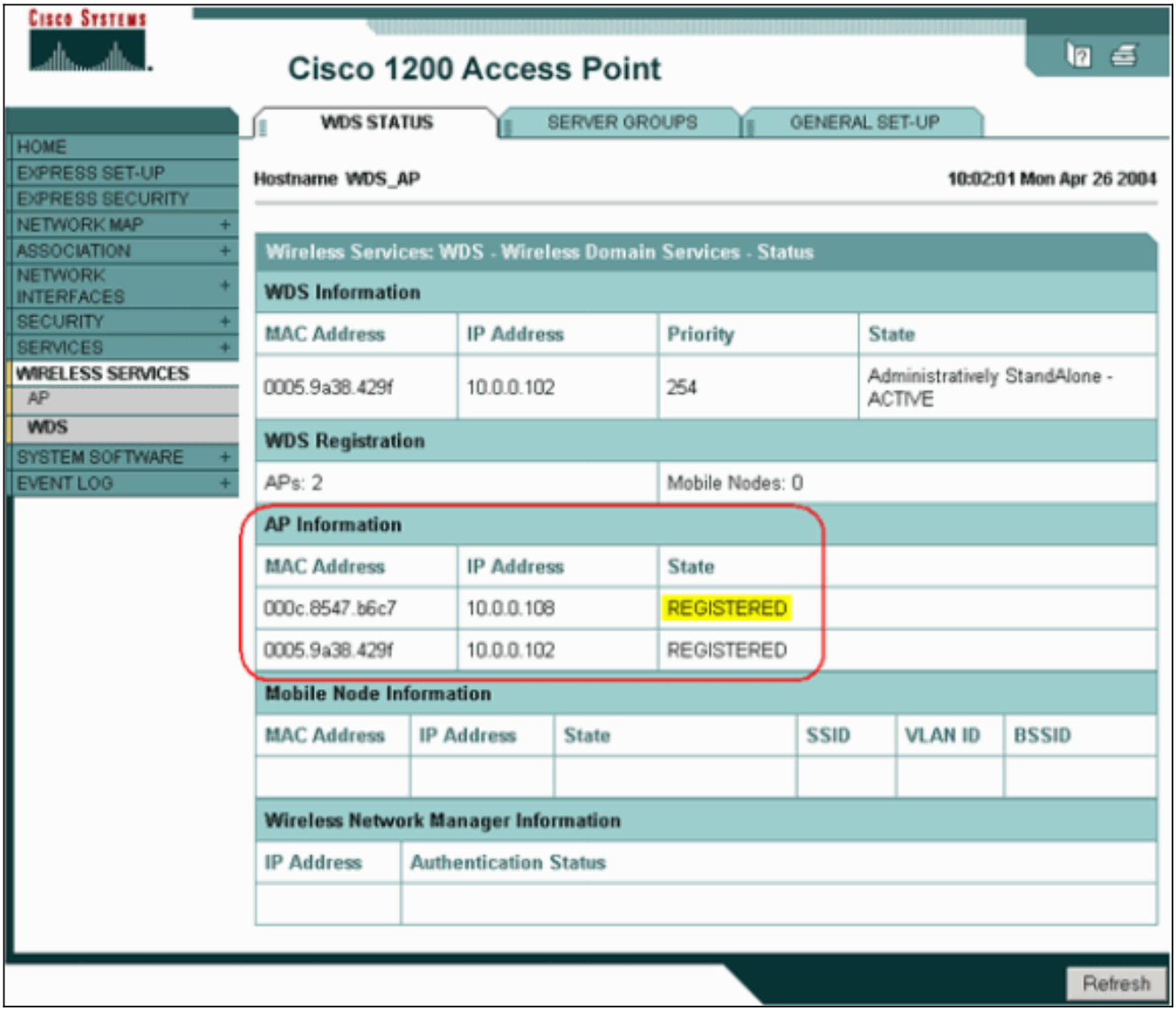
Observação: essa configuração se aplica somente aos APs de infraestrutura e não ao AP WDS.

1. Escolha **Wireless Services > AP**. No AP da infraestrutura, selecione **Enable** para a opção Wireless Services. Em seguida, digite o nome de usuário e a senha WDS.Você deve definir um nome de usuário e uma senha de WDS no servidor de autenticação para todos os dispositivos que serão membros do
WDS.



Como alternativa, emita estes comandos da CLI:

2. Escolha **Wireless Services > WDS**. Na guia Status WDS AP WDS, o novo AP de infraestrutura aparece na área Informações do WDS, com Estado como ATIVO, e na área Informações do AP, com Estado como REGISTRADO.Se o AP não for exibido ATIVE e/ou REGISTERED, verifique se há erros no servidor de autenticação ou tentativas de autenticação com falha.Depois que o AP aparecer ATIVE e/ou REGISTERED, adicione um método de autenticação de cliente ao
WDS.



Como alternativa, emita este comando da CLI:Como alternativa, emita este comando do WLSM:Em seguida, emita este comando no AP de infraestrutura:**Nota:** Não é possível testar associações de clientes porque a autenticação de clientes ainda não tem provisões.

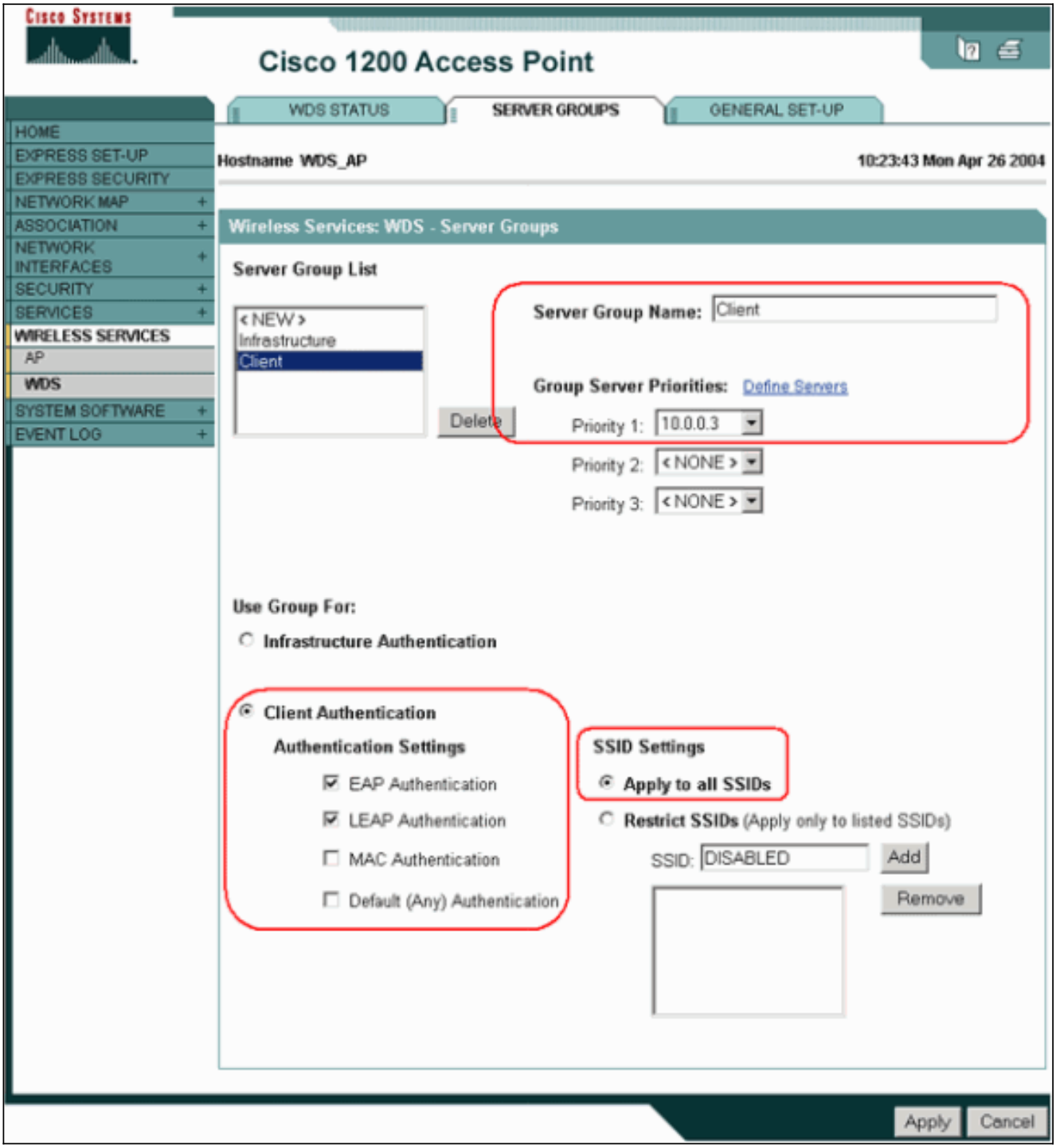
Definir Método de Autenticação do Cliente

Finalmente, defina um método de autenticação de cliente.

Conclua estes passos para adicionar um método de autenticação de cliente:

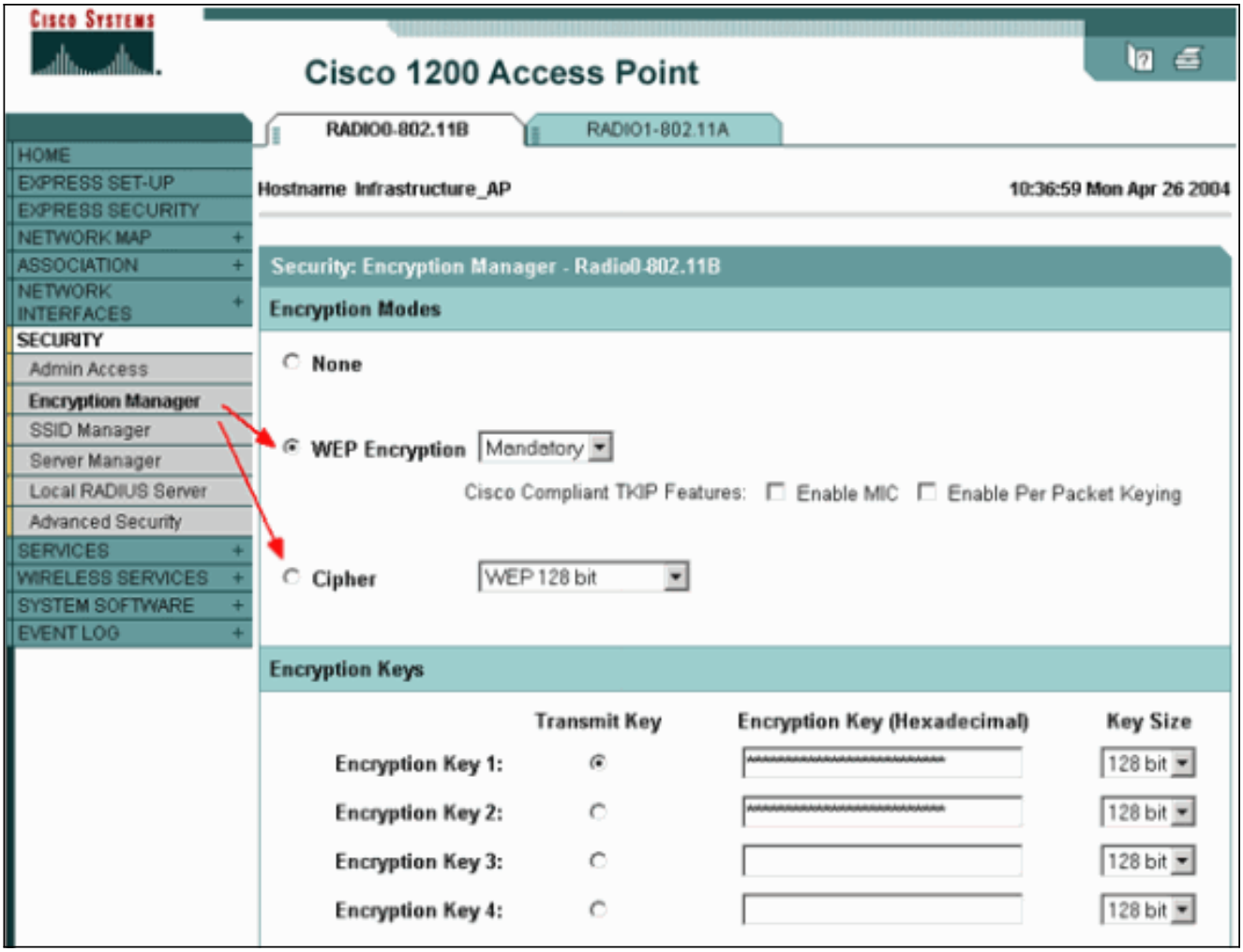
1. Escolha **Wireless Services > WDS**. Execute estas etapas na guia Grupos de servidores AP WDS:Defina um grupo de servidores que autentica clientes (um grupo de clientes).Defina a prioridade 1 para o servidor de autenticação configurado anteriormente.Defina o tipo de autenticação aplicável (LEAP, EAP, MAC, etc.).Aplique as configurações aos SSIDs

relevantes.

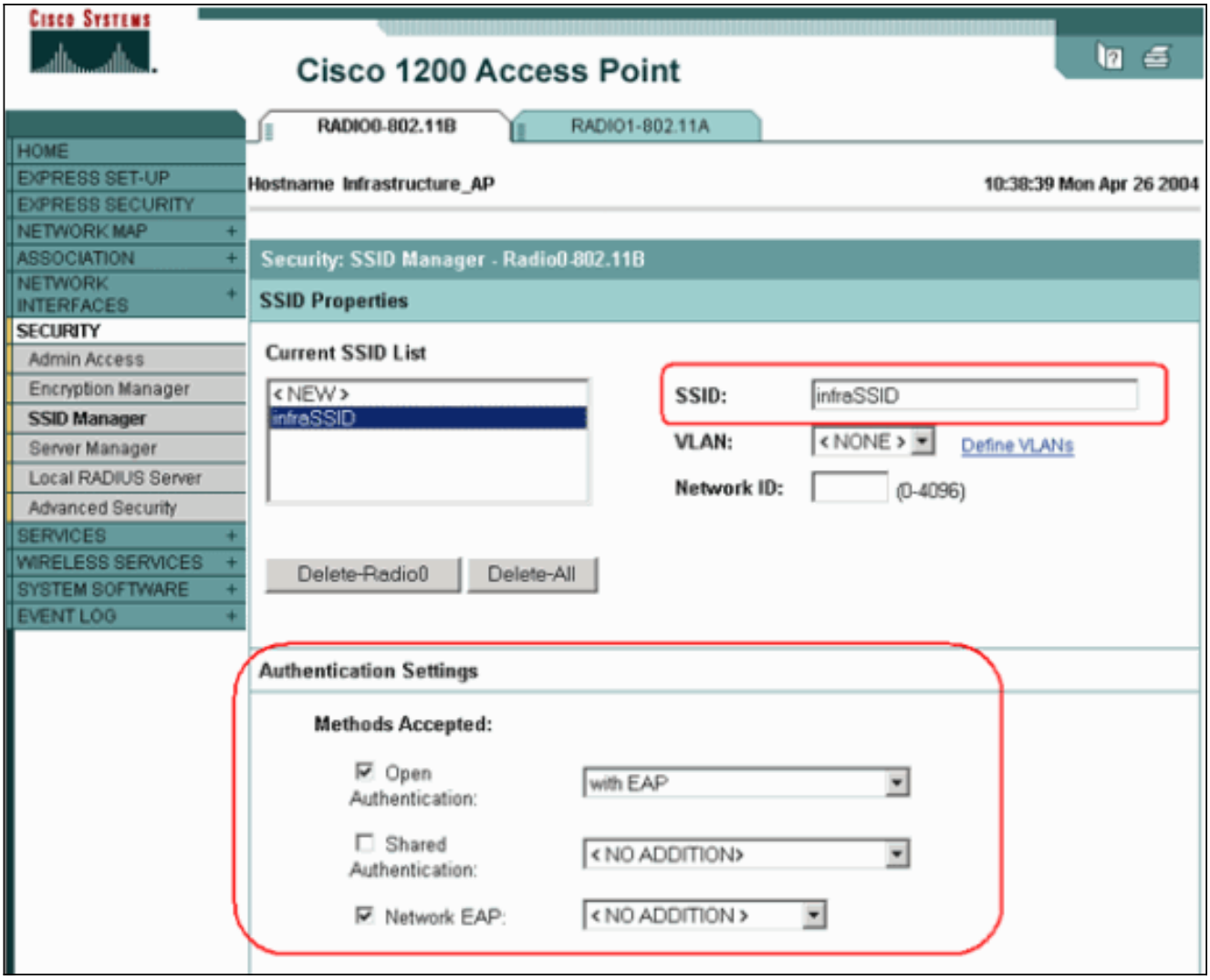


Como alternativa, emita estes comandos da CLI:**Observação:** o AP WDS de exemplo é dedicado e não aceita associações de clientes.**Observação:** não configure nos APs de infraestrutura para grupos de servidores porque os APs de infraestrutura encaminham quaisquer solicitações ao WDS para serem processados.

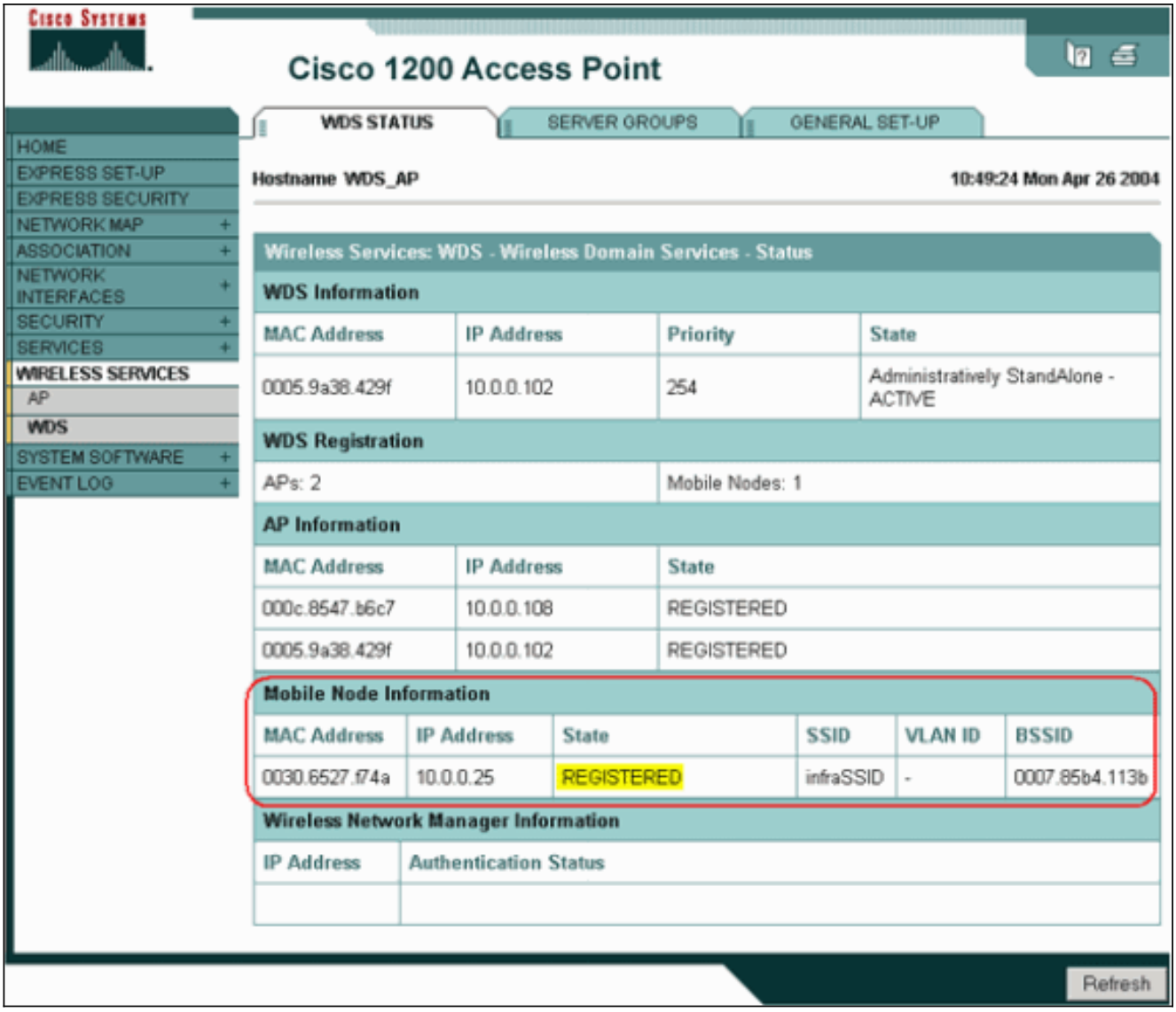
2. No AP ou APs da infraestrutura:No item de menu **Security > Encryption Manager**, clique em **WEP Encryption** ou **Cipher**, conforme exigido pelo protocolo de autenticação usado.



No item de menu **Security > SSID Manager (Segurança > Gerenciador de SSID)**, selecione métodos de autenticação conforme exigido pelo protocolo de autenticação usado.



3. Agora você pode testar com êxito se os clientes se autenticam em APs de infraestrutura. O AP do WDS na guia Status do WDS (sob o item de menu **Serviços sem fio > WDS**) indica que o cliente aparece na área Informações do nó móvel e tem um Estado REGISTRADO.Se o cliente não for exibido, verifique se há erros no servidor de autenticação ou tentativas de autenticação com falha por parte dos
clientes.



Como alternativa, emita estes comandos da CLI:**Observação:** se você precisar depurar a autenticação, certifique-se de depurar no AP WDS, pois o AP WDS é o dispositivo que se comunica com o servidor de autenticação.

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshoot

Esta seção fornece informações que você pode utilizar para fazer troubleshooting de configuração. Esta lista mostra algumas das perguntas comuns relacionadas ao comando WDS para esclarecer ainda mais a utilidade destes comandos:

- **Pergunta: No AP WDS, quais são as configurações recomendadas para esses itens?radius-server timeoutradius-server deadtimeTempo de Retenção da Falha da Verificação de Integridade da Mensagem da Chave Temporal (TKIP - Temporal Key Integrity Protocol)Tempo de Retenção do ClienteIntervalo de reautenticação EAP ou MACTempo limite do cliente EAP (opcional)Resposta:** Sugere-se que você mantenha a configuração com as configurações padrão relativas a essas configurações especiais e use-as somente quando

houver um problema com relação à temporização.Estas são as configurações recomendadas para o AP WDS:Desative o **tempo limite do servidor radius**. Esse é o número de segundos que um AP espera por uma resposta a uma solicitação RADIUS antes de reenviar a solicitação. O padrão é 5 segundos.Desative o **tempo de inatividade do servidor radius**. O RADIUS é ignorado por solicitações adicionais durante os minutos, a menos que todos os servidores sejam marcados como inativos.Por padrão, o tempo de espera da falha do TKIP MIC está ativado para 60 segundos. Se você habilitar o tempo de holdoff, poderá inserir o intervalo em segundos. Se o AP detectar duas falhas de MIC em 60 segundos, ele bloqueia todos os clientes TKIP nessa interface durante o período de tempo de holdoff especificado aqui.O tempo de espera do cliente deve ser desativado por padrão. Se você habilitar o holdoff, insira o número de segundos que o AP deve esperar após uma falha de autenticação antes que uma solicitação de autenticação subsequente seja processada.O EAP ou o Intervalo de reautenticação MAC está desativado por padrão. Se você habilitar a reautenticação, poderá especificar o intervalo ou aceitar o intervalo fornecido pelo servidor de autenticação. Se você optar por especificar o intervalo, insira o intervalo em segundos que o AP espera antes de forçar um cliente autenticado a reautenticar.O tempo limite do cliente EAP (opcional) é de 120 segundos por padrão. Digite o tempo que o AP deve esperar para que os clientes sem fio respondam às solicitações de autenticação EAP.

- **Pergunta: No que diz respeito ao tempo de espera do TKIP, li que este deve ser definido como 100 ms e não 60 segundos. Presumo que esteja definido para um segundo no navegador porque esse é o número mais baixo que você pode selecionar?Resposta:** Não há recomendação específica para defini-la como 100 ms, a menos que haja uma falha reportada em que a única solução é aumentar esse tempo. Um segundo é a configuração mais baixa.
- **Pergunta: Esses dois comandos ajudam a autenticação do cliente de alguma forma e são necessários no WDS ou AP de infraestrutura?radius-server attribute 6 on-for-login-authradius-server attribute 6 support-multipleResposta:** Esses comandos não ajudam no processo de autenticação e não são necessários no WDS ou no AP.
- **Pergunta: No AP de infraestrutura, suponho que nenhuma das configurações do Gerenciador de servidores e Propriedades globais seja necessária porque o AP recebe informações do WDS. Algum desses comandos específicos é necessário para o AP de infraestrutura?radius-server attribute 6 on-for-login-authradius-server attribute 6 support-multipleradius-server timeoutradius-server deadtimeResposta:** Não há necessidade de ter o Server Manager e as propriedades globais para os APs de infraestrutura. O WDS cuida dessa tarefa e não há necessidade de ter estas configurações:**radius-server attribute 6 on-for-login-authradius-server attribute 6 support-multipleradius-server timeoutradius-server deadtime**A configuração **radius-server attribute 32 include-in-access-req format %h** permanece por padrão e é necessária.

Um AP é um dispositivo da Camada 2. Portanto, o AP não oferece suporte à mobilidade da camada 3 quando o AP é configurado para atuar como um dispositivo WDS. Você pode alcançar a mobilidade da camada 3 somente quando configura o WLSM como o dispositivo WDS. Consulte a seção *Arquitetura de Mobilidade de Camada 3 do* Cisco Catalyst 6500 Series Wireless LAN Services Module: White Paper para obter mais informações.

Portanto, ao configurar um AP como um dispositivo WDS, não use o comando **mobility network-id**. Esse comando se aplica à mobilidade da camada 3 e você precisa ter um WLSM como seu dispositivo WDS para configurar corretamente a mobilidade da camada 3. Se você usar o comando **mobility network-id** incorretamente, poderá ver alguns destes sintomas:

- Os clientes Wireless não podem se associar ao AP.

- Os clientes sem fio podem se associar ao AP, mas não recebem um endereço IP do servidor DHCP.
- Um telefone sem fio não é autenticado quando você tem uma implantação de voz sobre WLAN.
- A autenticação EAP não ocorre. Com a **identificação da rede de mobilidade** configurada, o AP tenta criar um túnel GRE (Generic Routing Encapsulation) para encaminhar pacotes EAP. Se nenhum túnel for estabelecido, os pacotes não irão a lugar nenhum.
- Um AP configurado como um dispositivo WDS não funciona como esperado e a configuração do WDS não funciona.**Observação:** você não pode configurar o Cisco Aironet 1300 AP/Bridge como um WDS mestre. O 1300 AP/Bridge não suporta esta funcionalidade. O 1300 AP/Bridge pode participar de uma rede WDS como um dispositivo de infraestrutura no qual outro AP ou WLSM é configurado como um WDS mestre.

Comandos para Troubleshooting

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.

Nota:Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos debug.

- **debug dot11 aaa authenticator all** — Mostra as várias negociações pelas quais um cliente passa enquanto o cliente associa e autentica através do processo 802.1x ou EAP. Esta depuração foi introduzida no Cisco IOS Software Release 12.2(15)JA. Esse comando torna obsoleto debug dot11 aaa dot1x all nesta versão e em versões posteriores.
- **debug aaa authentication** —Mostra o processo de autenticação de uma perspectiva genérica de AAA.
- **debug wlccp ap** —Mostra as negociações WLCCP envolvidas quando um AP se une a um WDS.
- **debug wlccp packet** — Mostra as informações detalhadas sobre as negociações do WLCCP.
- **debug wlccp leap-client** — Mostra os detalhes quando um dispositivo de infraestrutura se une a um WDS.

Informações Relacionadas

- Configuração de WDS, roaming rápido e seguro e gerenciamento de rádio
- Nota de configuração do módulo de serviços de LAN sem fio do Catalyst 6500 Series
- Configurando conjuntos de cifras e o WEP
- Configurando tipos de autenticação
- Páginas de Suporte de Wireless LAN
- Suporte Técnico e Documentação - Cisco Systems