Cisco Secure Services Client com autenticação EAP-FAST

Índice

Introdução

Este original descreve como configurar o Cisco Secure Services Client (CSSC) com o software dos controladores do Wireless LAN, do® do Microsoft Windows 2000, e o Serviço de controle de acesso Cisco Secure (ACS) 4.0 com EAP-FAST. Este documento introduz a arquitetura EAP-FAST e fornece exemplos de implementação e configuração. CSSC é o componente de software do cliente que fornece a comunicação de credenciais do usuário à infraestrutura para autenticar um usuário para a rede e atribuir o acesso apropriado.

Estes são algumas das vantagens da solução CSSC de acordo com este original:

- Autenticação de cada usuário (ou de dispositivo) antes da permissão de acesso ao

WLAN/LAN com Extensible Authentication Protocol (EAP)
- Solução fim-a-fim da Segurança de WLAN com server, autenticador, e componentes de cliente
- Solução comum para a autenticação prendida e sem fio
- Dinâmico, pelas chaves de criptografia do usuário derivadas no processo de autenticação
- Nenhuma exigência para o Public Key Infrastructure (PKI) ou os Certificados (verificação de certificado opcional)
- Atribuição da política de acesso e/ou estrutura NAC-permitida EAP

Nota: Refira a segurança do Cisco que o modelo sem fio para obter informações sobre do desenvolvimento de fixa o Sem fio.

O framework de autenticação do 802.1x foi incorporado como parte (Segurança para LAN Wireless) do padrão 802.11i para permitir funções baseadas camada 2 do autenticação, autorização e relatório em uma rede de Wireless LAN do 802.11. Hoje, há diversos protocolos EAP disponíveis para o desenvolvimento no prendido e redes Wireless. Os protocolos geralmente distribuídos EAP incluem o PULO, o PEAP, e o EAP-TLS. Além do que estes protocolos, Cisco definiu e autenticação flexível executada EAP com o protocolo (EAP-FAST) fixado do túnel como um protocolo padrão-baseado EAP disponível para o desenvolvimento no prendido e redes de Wireless LAN. A especificação de protocolo EAP-FAST está publicamente - disponível no site IETF .

Como com alguns outros protocolos EAP, EAP-FAST é uma arquitetura de segurança do servidor cliente que cifre transações EAP dentro de um túnel TLS. Quando similar ao PEAP ou ao EAP-TTLS a este respeito, difere que o estabelecimento de túnel EAP-FAST está baseado nas chaves secretas compartilhadas fortes que são originais a cada usuário contra PEAP/EAP-TTLS (que usam um certificado do server X.509 para proteger a sessão da autenticação). Estas chaves secretas compartilhadas são chamadas as credenciais protegidas do acesso (PAC) e podem ser distribuídas automaticamente (abastecimento automático ou da Em-faixa) ou manualmente (abastecimento manual ou fora da banda) aos dispositivos do cliente. Porque os apertos de mão baseados em segredos compartilhados são mais eficiente do que os apertos de mão baseados em uma infraestrutura PKI, EAP-FAST é menos dos recursos intensivos de processador EAP tipo o mais rápido e daqueles que fornecem trocas protegidas da autenticação. EAP-FAST é projetado igualmente para a simplicidade do desenvolvimento desde que não exige um certificado no cliente do Wireless LAN ou na infraestrutura do RAIO contudo incorpora um mecanismo incorporado do abastecimento.

Estes são algumas das capacidades principais do protocolo EAP-FAST:

- Escolha sinal-em (SSO) com username de Windows/senha
- Apoio para a execução do script do início de uma sessão
- Apoio do Wi-Fi Protected Access (WPA) sem suplicante da terceira parte (Windows 2000 e XP somente)
- Desenvolvimento simples sem a exigência para a infraestrutura PKI
- Envelhecimento da senha do Windows (isto é, apoio para a expiração de senha server-baseada)
- Integração com Cisco Trust Agent para o controle de admissão de rede com software do cliente apropriado

Pré-requisitos

Exigência

Há uma suposição que o instalador tem a instalação de Windows 2003 do conhecimento do gerenciamento de recursos básicos e a instalação de Cisco WLC desde que este original cobre somente as configurações específicas para facilitar os testes.

Para a instalação inicial e a informação de configuração para os controladores do Cisco 4400 Series, refira o guia de início rápido: Controladores de LAN sem fio Cisco série 4400. Para a instalação inicial e a informação de configuração para os controladores do Cisco 2000 Series, refira o guia de início rápido: Controladores de LAN sem fio Cisco série 2000.

Antes que você comece, instale o Microsoft Windows server 2000 com o software o mais atrasado do pacote de serviços. Instale os controladores e o Lightweight Access Points (regaços) e assegure-se de que as atualizações de software mais recente estejam configuradas.

Componentes Utilizados

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

- Controlador do Cisco ou? Series que corridas 4.0.155.5
- Cisco 1242 LWAPP AP
- Windows 2000 com diretório ativo
- Cisco Catalyst 3750G Switch
- Windows XP com placa de adaptadores CB21AG e versão 4.05 do Cisco Secure Services Client

Convenções

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

Parâmetros de projeto

Base de dados

Quando você distribui uma rede de WLAN e procura um protocolo de autenticação, deseja-se geralmente usar um base de dados atual para a autenticação do usuário/máquina. Os bases de dados típicos que podem ser usados são diretório ativo de Windows, LDAP, ou um base de dados da senha de uma vez (OTP) (isto é, RSA ou SecureID). Todos estes bases de dados são compatíveis com o protocolo EAP-FAST, mas quando você planeia para o desenvolvimento, há alguns requisitos de compatibilidade que devem ser considerados. A distribuição inicial de um arquivo PAC aos clientes é realizada com o auto-abastecimento anônimo, o abastecimento autenticado (através do certificado atual do cliente X.509), ou o abastecimento manual. Com a finalidade deste original, o auto-abastecimento anônimo e o abastecimento manual são considerados.

O abastecimento automático PAC usa o protocolo autenticado do acordo da chave diffie-hellman (ADHP) para estabelecer um túnel seguro. O túnel seguro pode ser estabelecido anonimamente ou através de um mecanismo de autenticação de servidor. Dentro da conexão do túnel estabelecido, MS-CHAPv2 é usado para autenticar o cliente e, em cima da autenticação bem

sucedida, para distribuir o arquivo PAC ao cliente. Depois que o PAC provisioned com sucesso, o arquivo PAC pode ser usado para iniciar uma sessão EAP-FAST nova da autenticação a fim ganhar o acesso de rede seguro.

O abastecimento automático PAC é relevante ao base de dados no uso porque, desde que o mecanismo do auto-abastecimento confia no MSCHAPv2, o base de dados usado para autenticar usuários deve ser compatível com este formato da senha. Se você usa EAP-FAST com um base de dados que não apoie o formato MSCHAPv2 (tal como o OTP, o Novell, ou o LDAP), exige-se empregar algum outro mecanismo (isto é, abastecimento manual ou abastecimento autenticado) para distribuir arquivos do usuário PAC. Este original dá um exemplo do auto abastecimento com uma base de dados de usuário de Windows.

Criptografia

A autenticação EAP-FAST não exige o uso um tipo de criptografia específico WLAN. O tipo de criptografia WLAN a ser usado é determinado pelas capacidades do cartão do cliente NIC. Recomenda-se empregar a criptografia WPA2 (AES-CCM) ou WPA(TKIP), dependente das capacidades do cartão NIC no desenvolvimento específico. Note que a solução de Cisco WLAN permite a coexistência do WPA2 e dos dispositivos do cliente de WPA em um SSID comum.

Se os dispositivos do cliente não apoiam o WPA2 ou o WPA, é possível distribuir a autenticação do 802.1X com as chaves de WEP dinâmicas, mas, devido às façanhas conhecidas contra chaves de WEP, este mecanismo de criptografia WLAN não é recomendado. Se se exige para apoiar os clientes WEP-somente, recomenda-se empregar um intervalo do sessão-intervalo, que exija que os clientes derivam uma chave de WEP nova em um intervalo frequente. Trinta minutos são o intervalo recomendado da sessão para taxas de dados típicas WLAN.

Escolha Sinal-em e credenciais da máquina

Escolha Sinal-em refere a capacidade de um usuário único sinal-em ou de uma entrada das credenciais de autenticação para ser usado para alcançar aplicativos múltiplos ou dispositivos múltiplos. Para fins deste original, único Sinal-em refere o uso das credenciais que são usadas para entrar a um PC para a autenticação ao WLAN.

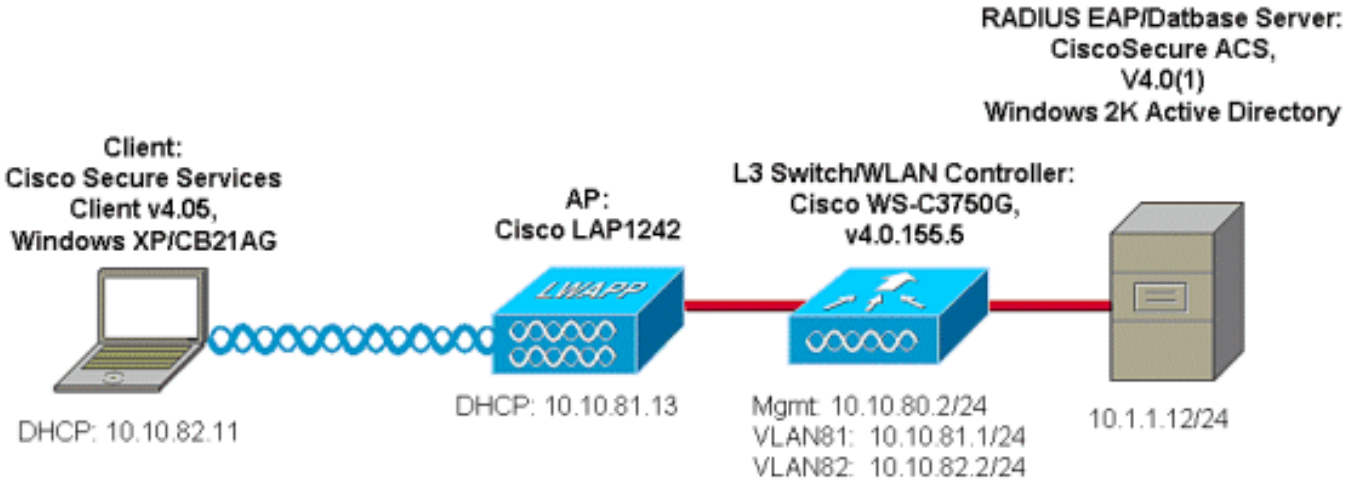
Com o Cisco Secure Services Client, é possível usar as credenciais de logon de um usuário para autenticar igualmente à rede de WLAN. Se se deseja autenticar um PC à rede antes do fazer logon do usuário ao PC, exige-se para usar as credenciais armazenadas do usuário ou as credenciais amarradas a um perfil da máquina. Qualquer um destes métodos é útil nos casos de onde se deseja executar scripts de logon ou movimentações do mapa quando as botas do PC acima, ao contrário quando um usuário entra.

Diagrama de Rede

Este é o diagrama da rede usado neste original. Nesta rede, há quatro sub-redes usadas. Note que não é necessário segmentar estes dispositivos em redes diferentes, mas este tem recursos para a maioria de flexibilidade para a integração com redes reais. O controlador integrado 3750G do Wireless LAN do catalizador fornece a potência sobre switchports dos Ethernet (PoE), interruptor L3, e capacidade do controlador de WLAN em um chassi comum.

1. A rede 10.1.1.0 é a rede de servidor onde o ACS reside.
2. A rede 10.10.80.0 é a rede de gerenciamento usada pelo controlador de WLAN.

3. A rede 10.10.81.0 é a rede onde os APs residem.
4. A rede 10.10.82.0 é usada para os clientes de WLAN.



Configurar o Access Control Server (ACS)

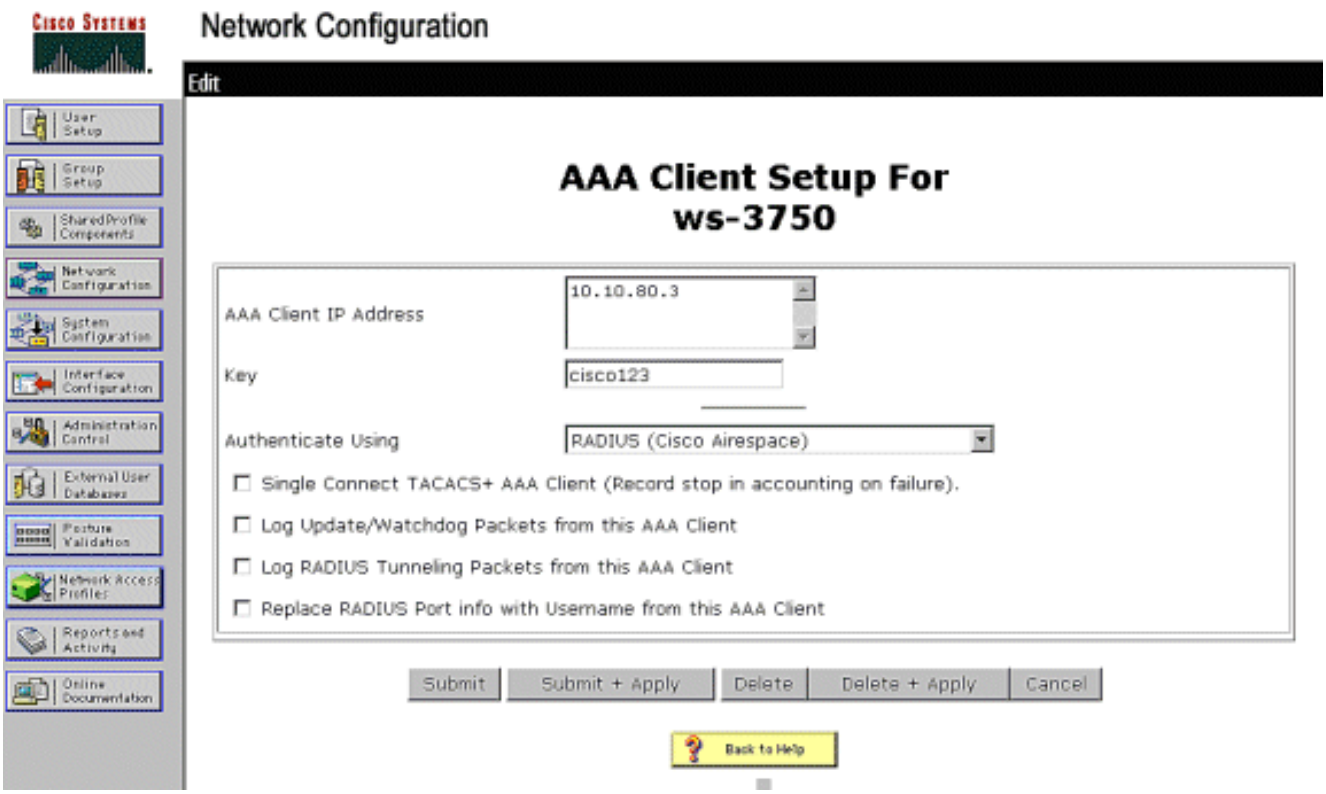
Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Nota: Use a ferramenta Command Lookup Tool (apenas para clientes registrados) para obter mais informações sobre os comandos usados neste documento.

Adicionar o Access point como o cliente de AAA (NAS) em ACS

Esta seção descreve como configurar ACS para EAP-FAST com abastecimento da em-faixa PAC com diretório ativo de Windows como o base de dados externo.

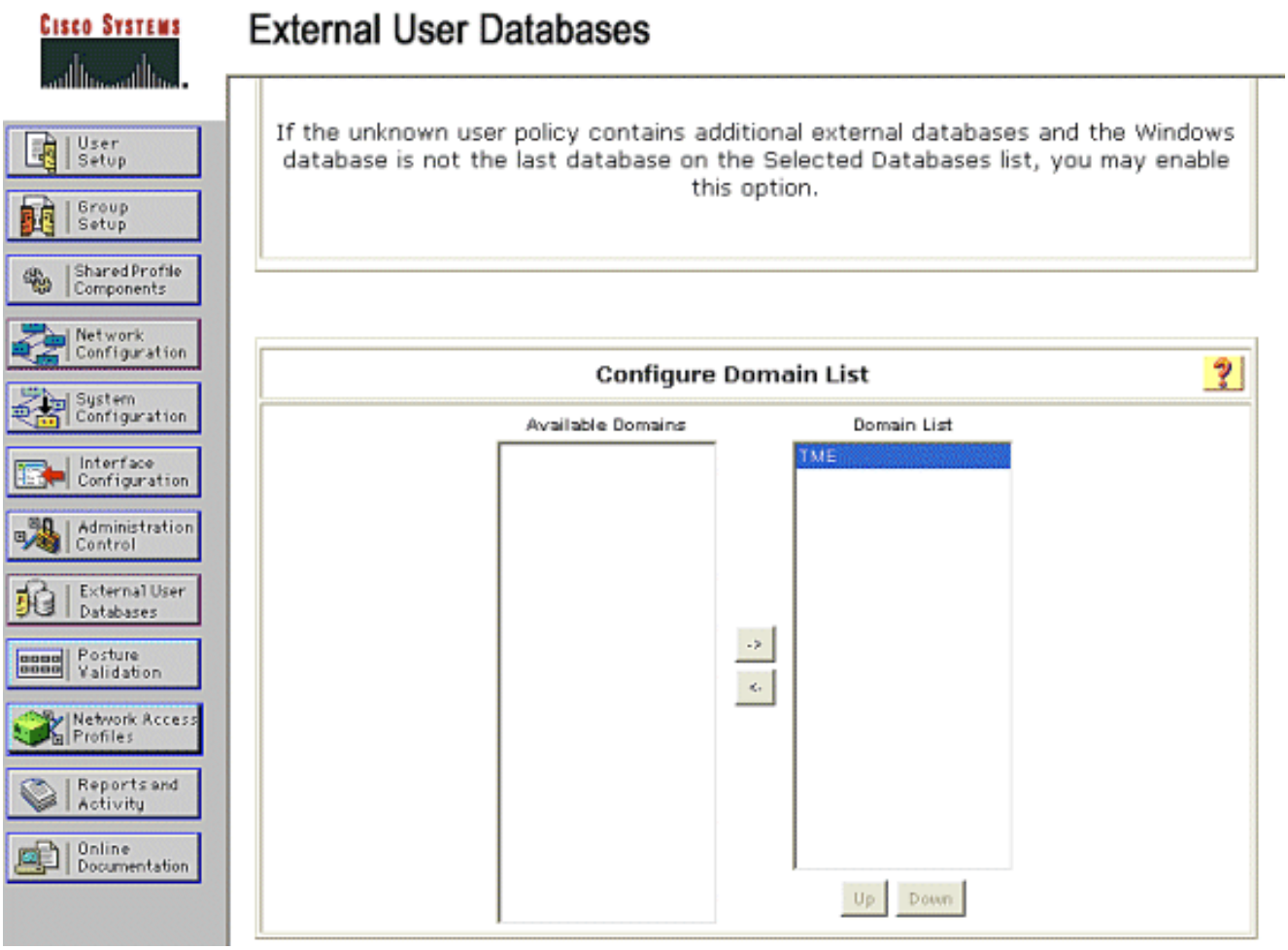
1. O fazer logon a **ACS > configuração de rede** e clique **adiciona a entrada**.
2. Preencha o nome do controlador de WLAN, IP address, chave secreta compartilhada, e abaixo autentique-o usando-se, escolha-o o RAIO (Cisco Airespace), que igualmente inclui atributos do RAIO IETF.**Nota:** Se os grupos de dispositivo de rede (NDG) são permitidos, primeiramente escolha o NDG apropriado e adicionar-lhe o controlador de WLAN. Refira o guia de configuração ACS para detalhes sobre o NDG.
3. **Reinício do** clique **Submit+**.



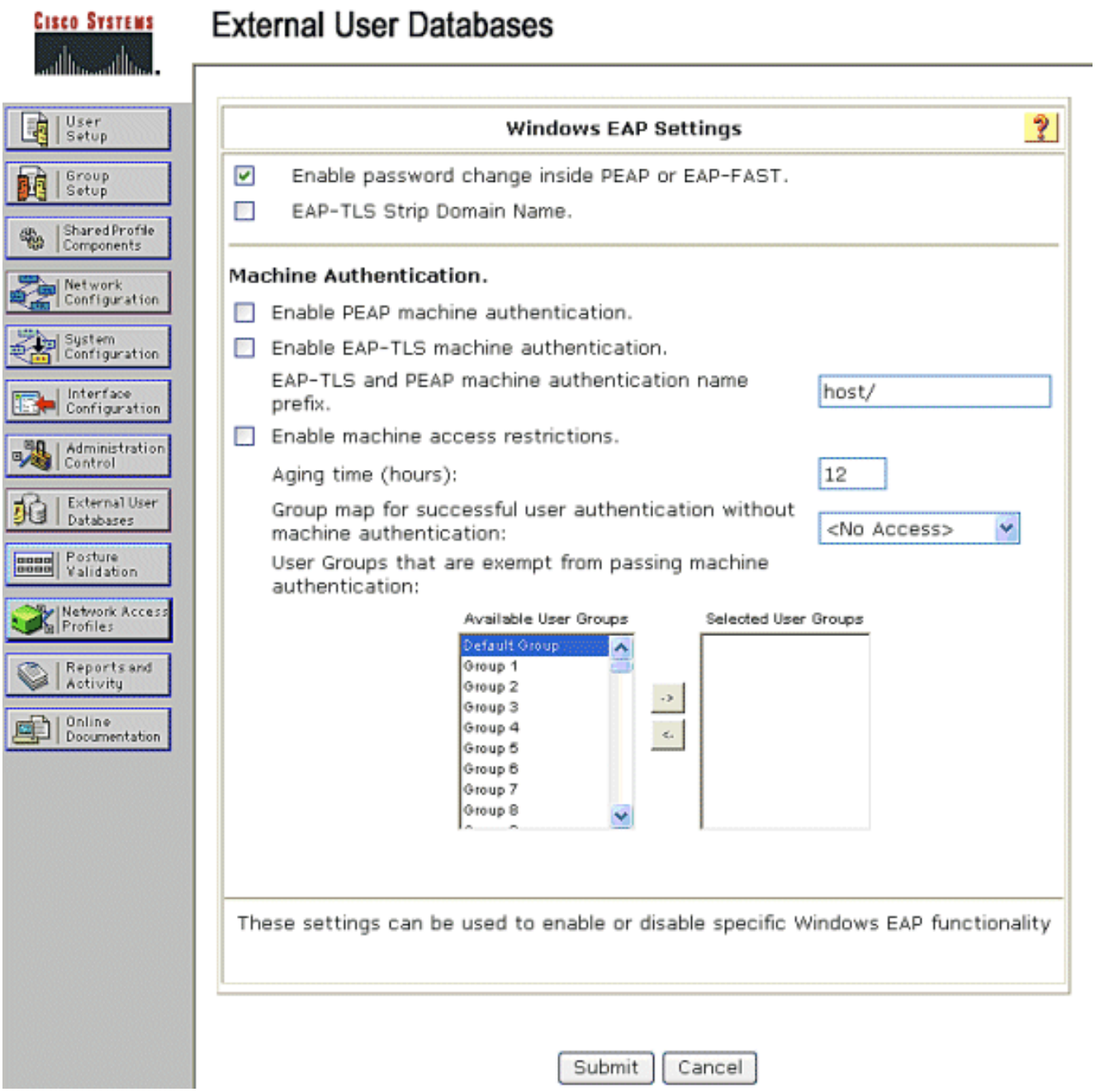
Configurar ACS a fim perguntar o base de dados externo

Esta seção descreve como configurar o ACS a fim perguntar o base de dados externo.

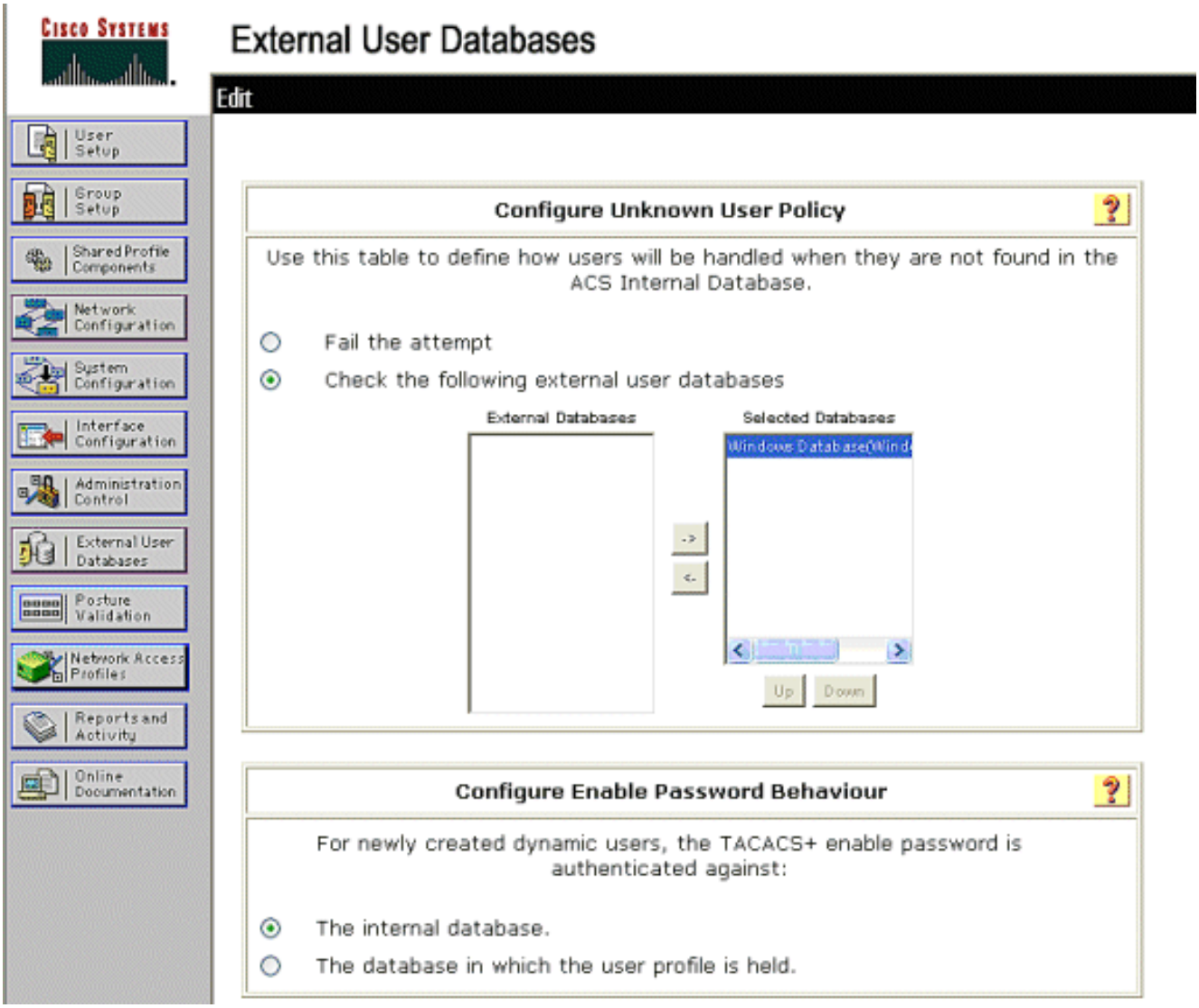
1. **A base de dados de usuário externo > a configuração do base de dados > o base de dados do Windows do** clique **> configuram**.
2. Sob configurar a lista de domínios, **domínios do** movimento dos domínios disponíveis à lista de domínios.**Nota:** O server que executa o ACS deve ter o conhecimento destes domínios para que o aplicativo ACS detecte e use aquelas finalidades dos domínios para autenticação.



3. Sob os ajustes de Windows EAP, configurar a opção para permitir a mudança da senha dentro do PEAP ou da sessão EAP-FAST. Refira o manual de configuração para o Cisco Secure ACS 4.1 a fim obter mais detalhes sobre o envelhecimento EAP-FAST e da senha do Windows.
4. Clique em Submit.**Nota:** Você pode igualmente permitir a característica da permissão de discagem para EAP-FAST sob a configuração de base de dados de usuário de Windows a fim permitir o base de dados externo de Windows controlar a permissão de acesso. Os ajustes MS-CHAP para a mudança da senha na página de configuração do base de dados do Windows são somente aplicáveis à autenticação NON-EAP MS-CHAP. A fim permitir a senha mude conjuntamente com EAP-FAST, ele é necessário para permitir a mudança da senha sob os ajustes de Windows
EAP.



5. Clique a **base de dados de usuário externo > a política de usuário desconhecida** e escolha a **verificação o seguinte** botão de rádio das **bases de dados de usuário externo**.
6. Mova o base de dados do Windows dos **bases de dados externos** para **bases de dados selecionado**.
7. Clique em Submit.**Nota:** A partir daqui, o ACS verifica Windows DB. Se o usuário não é encontrado no base de dados local ACS, coloca o usuário no grupo padrão ACS. Refira a documentação ACS para mais detalhes sobre mapeamentos de grupo de base de dados.**Nota:** Porque o ACS pergunta o base de dados do microsoft ative directory para verificar credenciais do usuário, os ajustes adicionais dos direitos de acesso precisam de ser configurados em Windows. Refira o Guia de Instalação para o server do Cisco Secure ACS for Windows para
detalhes.



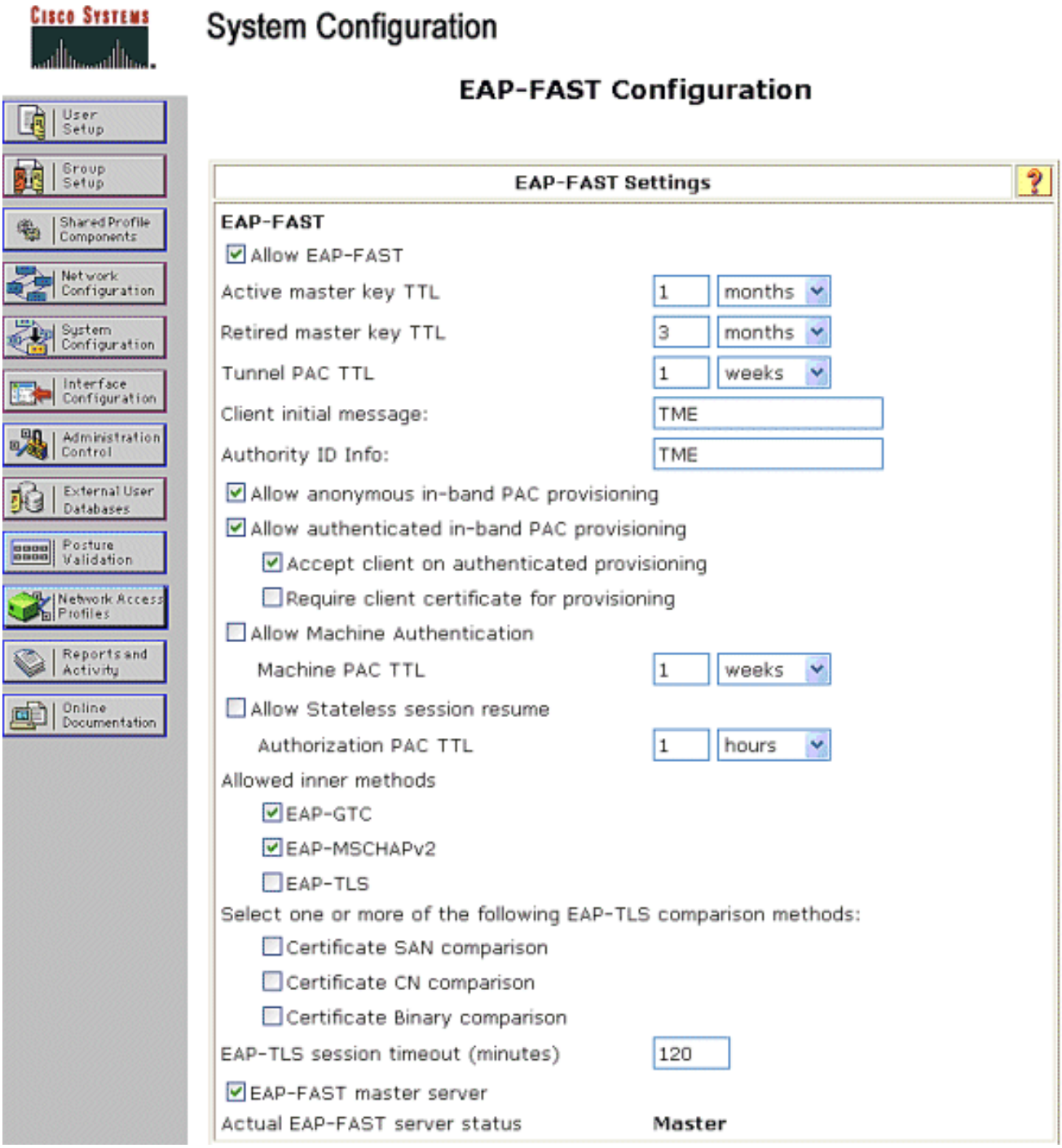
Permita o apoio EAP-FAST no ACS

Esta seção descreve como permitir o apoio EAP-FAST no ACS.

1. Vai à **configuração de sistema > a autenticação global Setup > configuração EAP-FAST**.
2. Escolha **permitem EAP-FAST**.
3. Configurar estas recomendações: Chave mestre aposentado TTL/TTL/PAC TTL do chave mestre. Estes ajustes são configurados à revelia no Cisco Secure ACS:Mês do chave mestre TTL:1TTL chave aposentado: 3 mesesPAC TTL: 1 semana
4. Complete o campo de **informação de ID da autoridade**. Este texto é mostrado em algum software do cliente EAP-FAST onde a seleção da autoridade PAC é o controlador.**Nota:** O Cisco Secure Services Client não emprega este texto descritivo para a autoridade PAC.
5. Escolha o campo do **abastecimento da em-faixa PAC reservar**. Este campo permite o abastecimento automático PAC para clientes EAP-FAST apropriado-permitidos. Para este exemplo, o auto-abastecimento é empregado.
6. Escolha **métodos internos permitidos**: EAP-GTC e EAP-MSCHAP2. Isto permite a operação de v1 EAP-FAST e de clientes EAP-FAST v1a. (O Cisco Secure Services Client apoia v1a EAP-FAST.) Se não é necessário apoiar os clientes v1 EAP-FAST, é somente necessário permitir o EAP-MSCHAPv2 como um método interno.
7. Escolha a caixa de seleção **mestra EAP-FAST do server** permitir este server EAP-FAST como o mestre. Isto permite outros servidores ACS utilizar este server como a autoridade do

mestre PAC para evitar a disposição de chaves originais para cada ACS em uma rede. Refira o guia de configuração ACS para detalhes.

8. Clique **Submit+Restart**.



Controlador de WLAN de Cisco

Para fins deste guia de distribuição, Cisco WS3750G o controlador integrado do Wireless LAN (WLC) é usado com Cisco AP1240 APs de pouco peso (REGAÇO) para fornecer a infraestrutura WLAN para testes CSSC. A configuração é aplicável para todo o controlador de WLAN de Cisco. A versão de software empregada é 4.0.155.5.

Configurar o controlador do Wireless LAN

Operação básica e registro do REGAÇO ao controlador

Use o assistente da configuração de inicialização no comando line interface(cli) a fim configurar o WLC para a operação básica. Alternativamente, você pode usar o GUI a fim configurar o WLC. Este original explica a configuração no WLC com o assistente da configuração de inicialização no CLI.

Após as botas WLC pela primeira vez, participa no assistente da configuração de inicialização. Use o wizard de configuração para configurar configurações básicas. Você pode alcançar o assistente com o CLI ou o GUI. Esta saída mostra um exemplo do assistente da configuração de inicialização no CLI:

```
Welcome to the Cisco Wizard Configuration Tool
Use the '-' character to backup
System Name [Cisco_33:84:a0]: ws-3750
Enter Administrative User Name (24 characters max): admin
Enter Administrative Password (24 characters max): *****
Management Interface IP Address: 10.10.80.3
Management Interface Netmask: 255.255.255.0
Management Interface Default Router: 10.10.80.2
Management Interface VLAN Identifier (0 = untagged):
Management Interface DHCP Server IP Address: 10.10.80.2
AP Manager Interface IP Address: 10.10.80.4
AP-Manager is on Management subnet, using same values
AP Manager Interface DHCP Server (172.16.1.1):
Virtual Gateway IP Address: 1.1.1.1
Mobility/RF Group Name: Security
Network Name (SSID): Enterprise
Allow Static IP Addresses [YES][no]: yes
Configure a RADIUS Server now? [YES][no]: no
Warning! The default WLAN security policy requires a RADIUS server.
Please see documentation for more details.
Enter Country Code (enter 'help' for a list of countries) [US]:
Enable 802.11b Network [YES][no]: yes
Enable 802.11a Network [YES][no]: yes
Enable 802.11g Network [YES][no]: yes
Enable Auto-RF [YES][no]: yes

Configuration saved!
Resetting system with new configuration.
```

Estes parâmetros estabelecem o WLC para a operação básica. Neste exemplo de configuração, o WLC usa **10.10.80.3** como o IP address da interface de gerenciamento e **10.10.80.4** como o IP address da relação do gerenciador AP.

Antes que todos os outros recursos possam ser configurados no WLCs, os regaços têm que registrar-se com o WLC. Este original supõe que o REGAÇO está registrado ao WLC. Refira o registro ao AP de pouco peso à seção de WLCs do Failover do controlador de WLAN para o exemplo de configuração do Lightweight Access Points para obter informações sobre de como os APs de pouco peso se registram com o WLC. Para a referência com este exemplo de configuração, os AP1240s são distribuídos em uma sub-rede separada (10.10.81.0/24) do controlador de WLAN (10.10.80.0/24), e a opção de DHCP 43 é usada prever a descoberta do controlador.

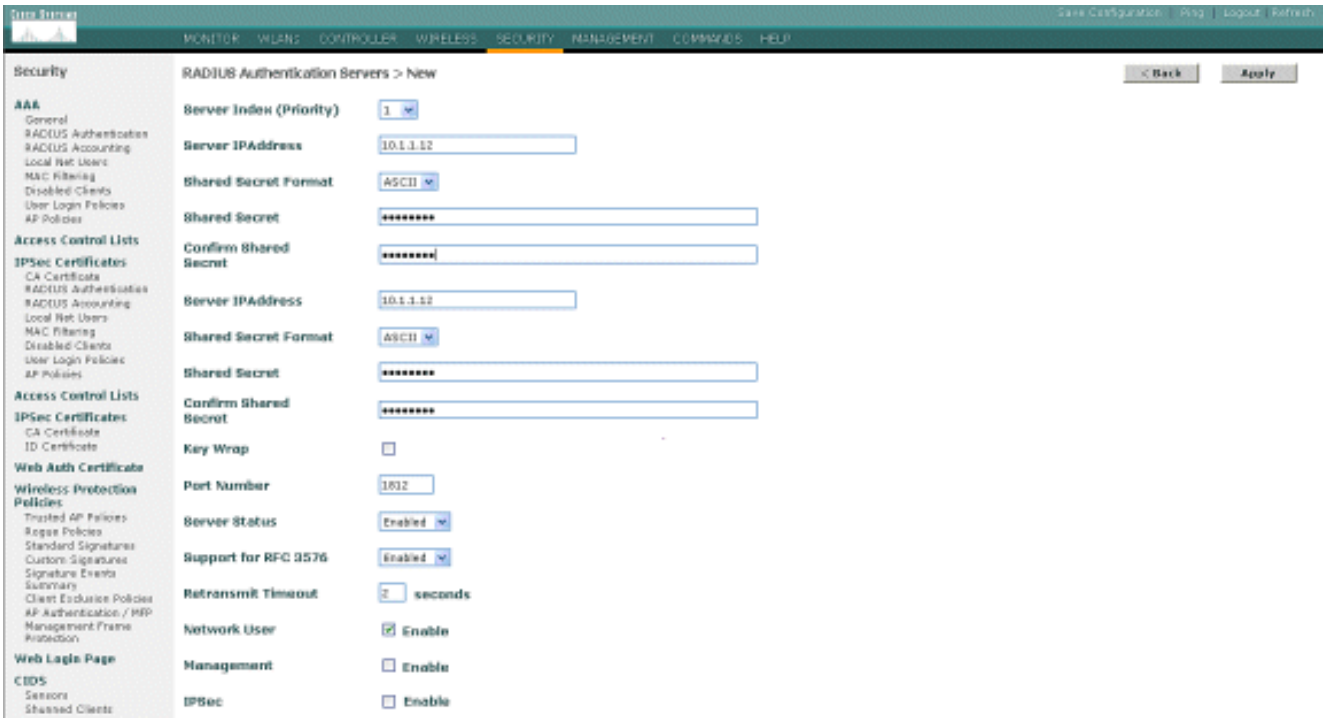
Autenticação RADIUS com o Cisco Secure ACS

O WLC precisa de ser configurado para enviar as credenciais do usuário ao server do Cisco Secure ACS. O servidor ACS então valida as credenciais do usuário (através do base de dados do Windows configurado) e fornece o acesso aos clientes Wireless.

Termine estas etapas para configurar o WLC para uma comunicação ao servidor ACS:

1. Clique a **Segurança** e a **autenticação RADIUS do** controlador GUI para indicar a página dos servidores de autenticação RADIUS. Clique então **novo** para definir o servidor ACS.

2. Defina os parâmetros do servidor ACS nos servidores de autenticação RADIUS > página nova. Estes parâmetros incluem o IP address ACS, o segredo compartilhado, o número de porta, e o status de servidor.**Nota:** Os números de porta 1645 ou 1812 são compatíveis com o ACS para a autenticação RADIUS.O usuário de rede e as caixas de verificação de gerenciamento determinam se a autenticação Raio-baseada se aplica para usuários de rede (por exemplo, clientes de WLAN) e Gerenciamento (isto é, usuários administrativos). O exemplo de configuração usa o Cisco Secure ACS como o servidor Radius com endereço IP 10.1.1.12:



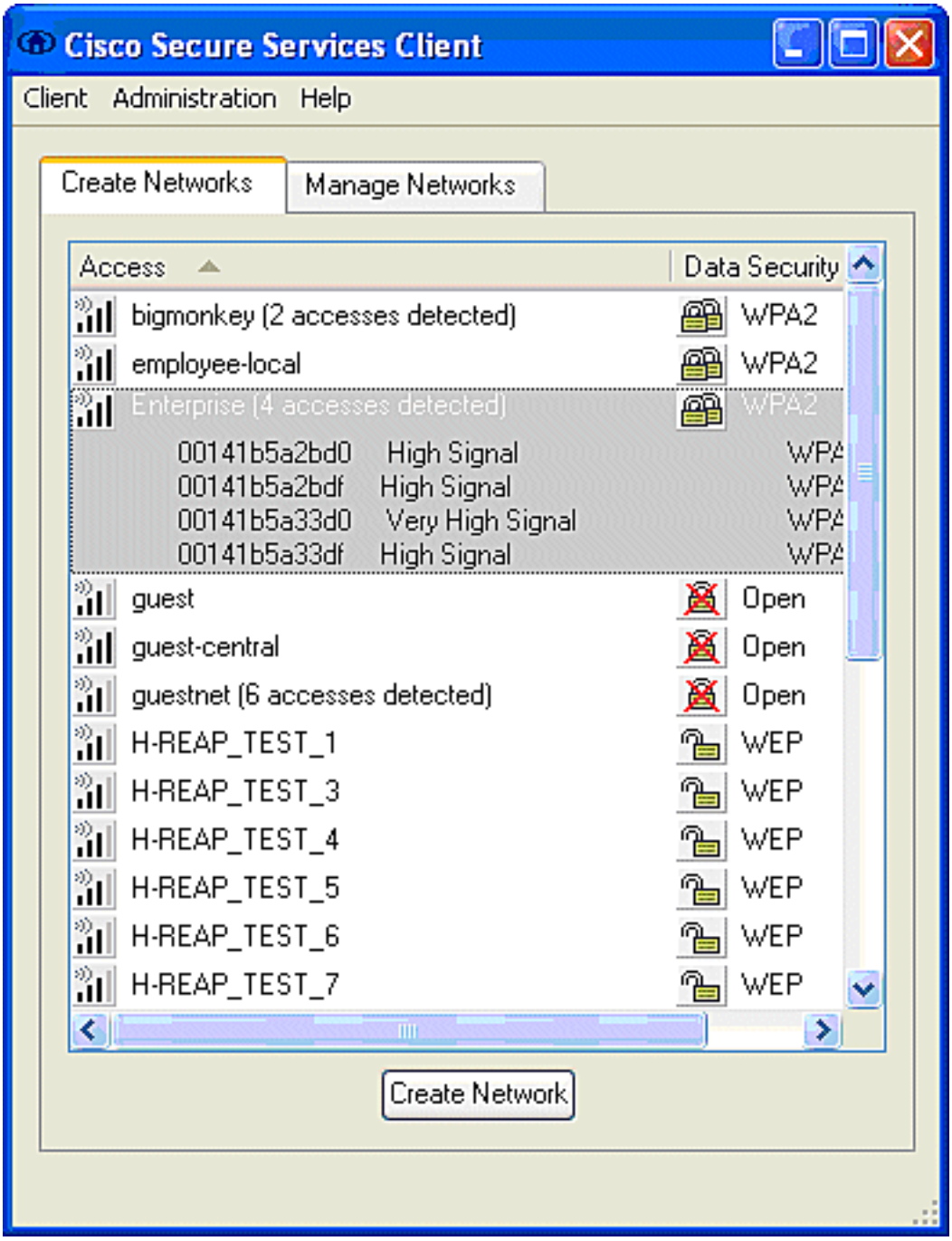
Configuração dos parâmetros WLAN

Esta seção descreve a configuração do Cisco Secure Services Client. Neste exemplo, CSSC v4.0.5.4783 é usado com um adaptador cliente de Cisco CB21AG. Antes da instalação do software CSSC, verifique que somente os direcionadores para o CB21AG estão instalados, não o utilitário de desktop de Aironet (ADU).

Uma vez que o software é instalado e é executado como um serviço, faz a varredura para redes disponíveis e indica aqueles disponíveis.

Nota: CSSC desabilita Windows zero configurações.

Nota: Somente aquele o SSID que é permitido para a transmissão é visível.



Nota: O controlador de WLAN, à revelia, transmite o SSID, assim que mostra-se na lista das redes da criação de SSID feitos a varredura. A fim criar um perfil da rede, você pode simplesmente clicar o **SSID na** lista (empresa) e no botão de rádio da **rede da criação**.

Se a infraestrutura WLAN é configurada com transmissão SSID desabilitada, você deve manualmente adicionar o SSID; clique o botão de rádio **adicionar** sob dispositivos de acesso e incorpore manualmente o **SSID** apropriado (por exemplo, empresa). Configurar o comportamento ativo da ponta de prova para o cliente, isto é, onde o cliente sonda ativamente para seu SSID configurado; especifique **ativamente a busca para este dispositivo de acesso** depois que você incorpora o SSID no indicador do dispositivo de acesso adicionar.

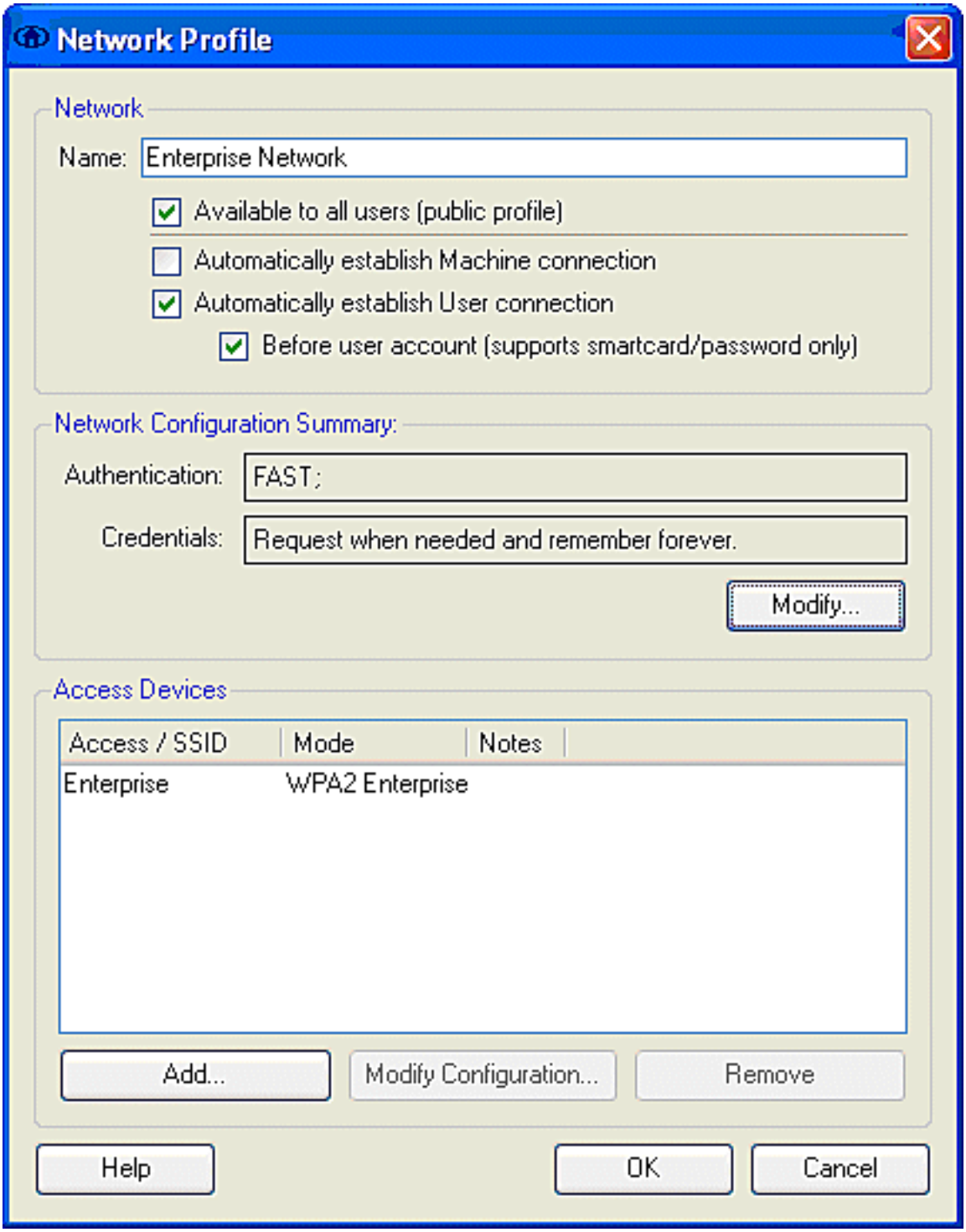
Nota: As configurações de porta não permitem modos de empreendimento (802.1X) se os ajustes da autenticação de EAP não são primeiros configurados para o perfil.

O botão de rádio da **rede da criação** lança o indicador do perfil da rede, que o permite associar (ou configurado) o SSID escolhido com um mecanismo da autenticação. Atribua um nome descritivo para o perfil.

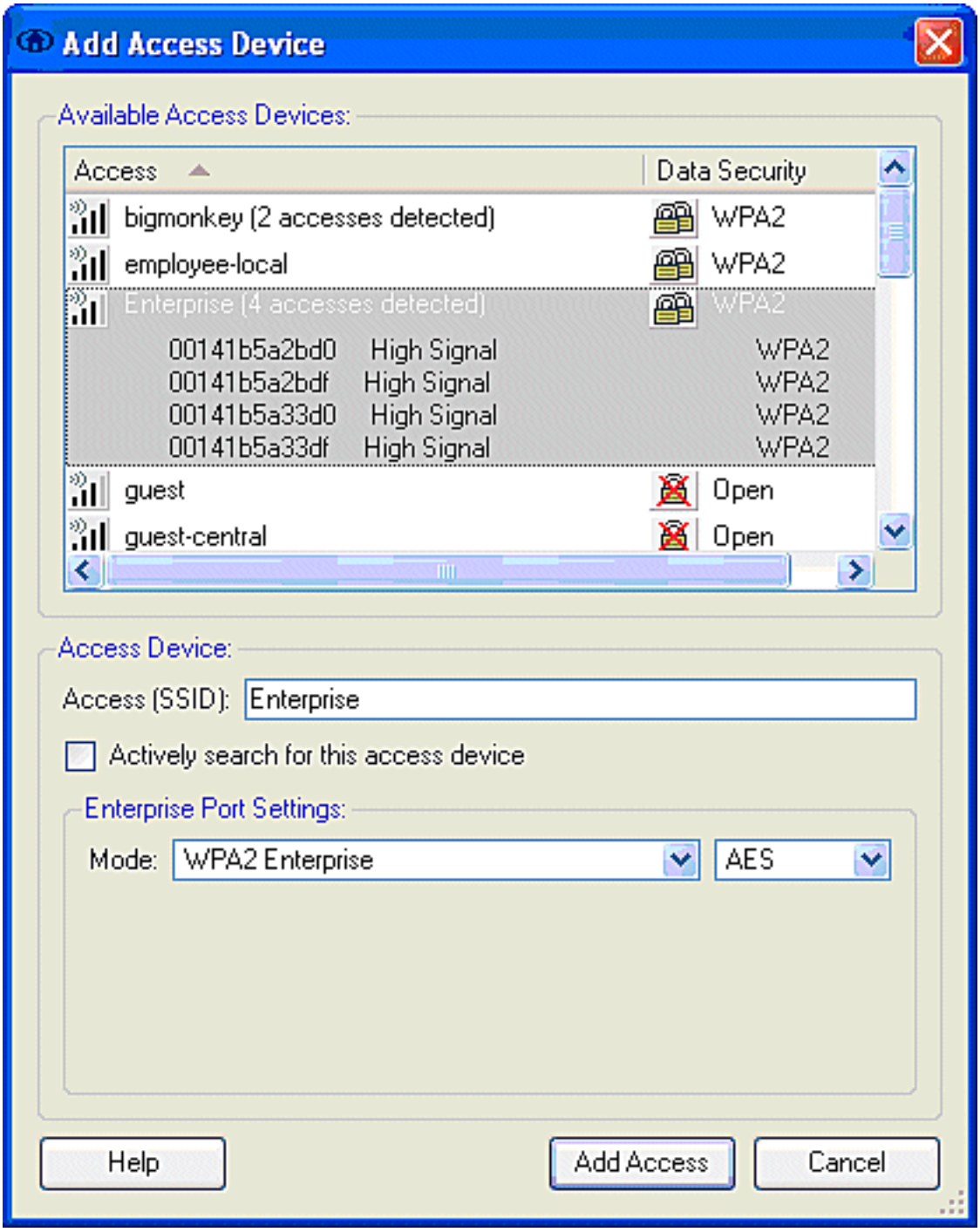
Nota: Os tipos múltiplos da Segurança de WLAN e/ou os SSID podem ser associados sob este perfil da autenticação.

A fim ter o cliente a conectar automaticamente à rede quando na escala de cobertura RF, escolha **estabelecem automaticamente a conexão do usuário**. Uncheck **disponível a todos os usuários** se não é desejável usar este perfil com outras contas de usuário na máquina. Se **estabeleça automaticamente** não é escolhido, é necessário que o usuário abrir o indicador CSSC e inicie manualmente a conexão WLAN com o botão de rádio da **conexão**.

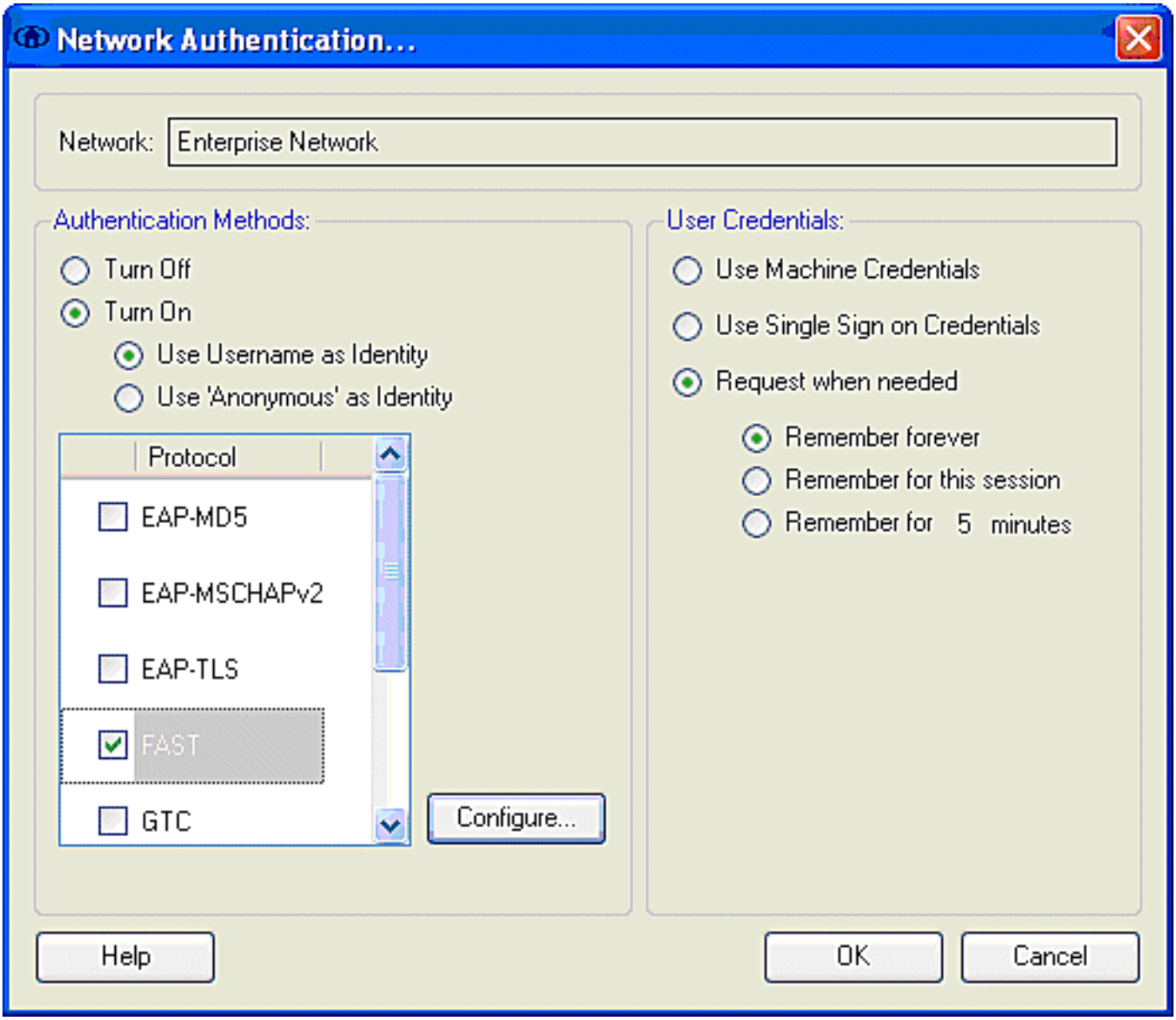
Se se deseja iniciar a conexão WLAN antes do fazer logon do usuário, escolha **antes da conta de usuário**. Isto permite Único-Sinal-na operação com as credenciais salvar do usuário (senha ou certificado/Smartcard quando você usa o TLS dentro de EAP-FAST).



Nota: Para a operação WPA/TKIP com o adaptador cliente do Cisco Aironet série 350, é necessário desabilitar a validação do aperto de mão WPA desde que há atualmente uma incompatibilidade entre o cliente CSSC e 350 direcionadores no que diz respeito ao aperto de mão WPA pique a validação. Isto é desabilitado sob o **cliente > ajustes > validação avançados do aperto de mão WPA/WPA2**. A validação deficiente do aperto de mão ainda permite os recursos de segurança inerentes em WPA (fechar e Message Integrity Check do pacote per. TKIP), mas desabilita a autenticação de chave inicial WPA.



Sob o sumário da configuração de rede, o clique **altera** para configurar o EAP/ajustes das credenciais. Especifique **gerenciem sobre a** autenticação, escolhem-na **RAPIDAMENTE** sob o protocolo, e escolhem-nos **"anônimo" como a identidade** (a fim não usar nenhum username no pedido inicial EAP). É possível usar o **username do uso como Identityas a** identidade exterior EAP, mas muitos clientes não desejam expor o usuário - ids no pedido unencrypted inicial EAP. Especifique o **único sinal do uso em credenciais** usar credenciais de logon para a autenticação de rede. O clique **configura** para estabelecer parâmetros EAP-FAST.



Sob ajustes RÁPIDOS, é possível especificar **valida o certificado de servidor**, que permite o cliente validar o certificado EAP-FAST do server (ACS) antes do estabelecimento de uma sessão EAP-FAST. Isto fornece a proteção para os dispositivos do cliente da conexão a um server EAP-FAST do desconhecido ou do rogue e da submissão inadvertida de suas credenciais de autenticação a uma fonte não confiável. Isto exige que o servidor ACS tem um certificado instalado e o cliente igualmente tem o certificado correspondente do Certificate Authority da raiz instalado. Neste exemplo, a validação do certificado de servidor não é permitida.

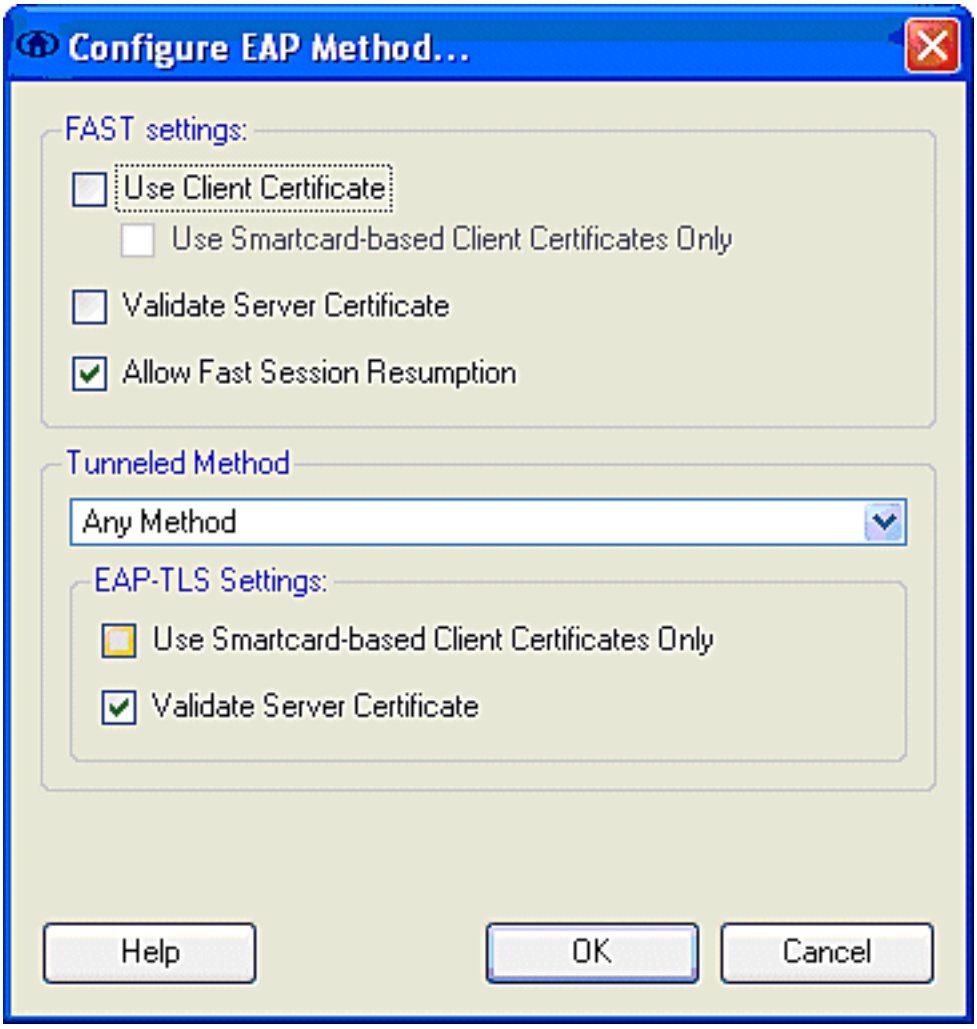
Sob ajustes RÁPIDOS, é possível especificar **permite a ressunção rápida da sessão**, que permite a ressunção de uma sessão EAP-FAST baseada na informação do túnel (sessão TLS) um pouco do que a exigência de um reauthentication EAP-FAST completo. Se o server e o cliente EAP-FAST têm o sabido por todos da informação de sessão TLS negociada dentro da troca EAP-FAST inicial da autenticação, a ressunção da sessão pode ocorrer.

Nota: O server EAP-FAST e o cliente devem ser configurados para o resumo EAP-FAST da sessão.

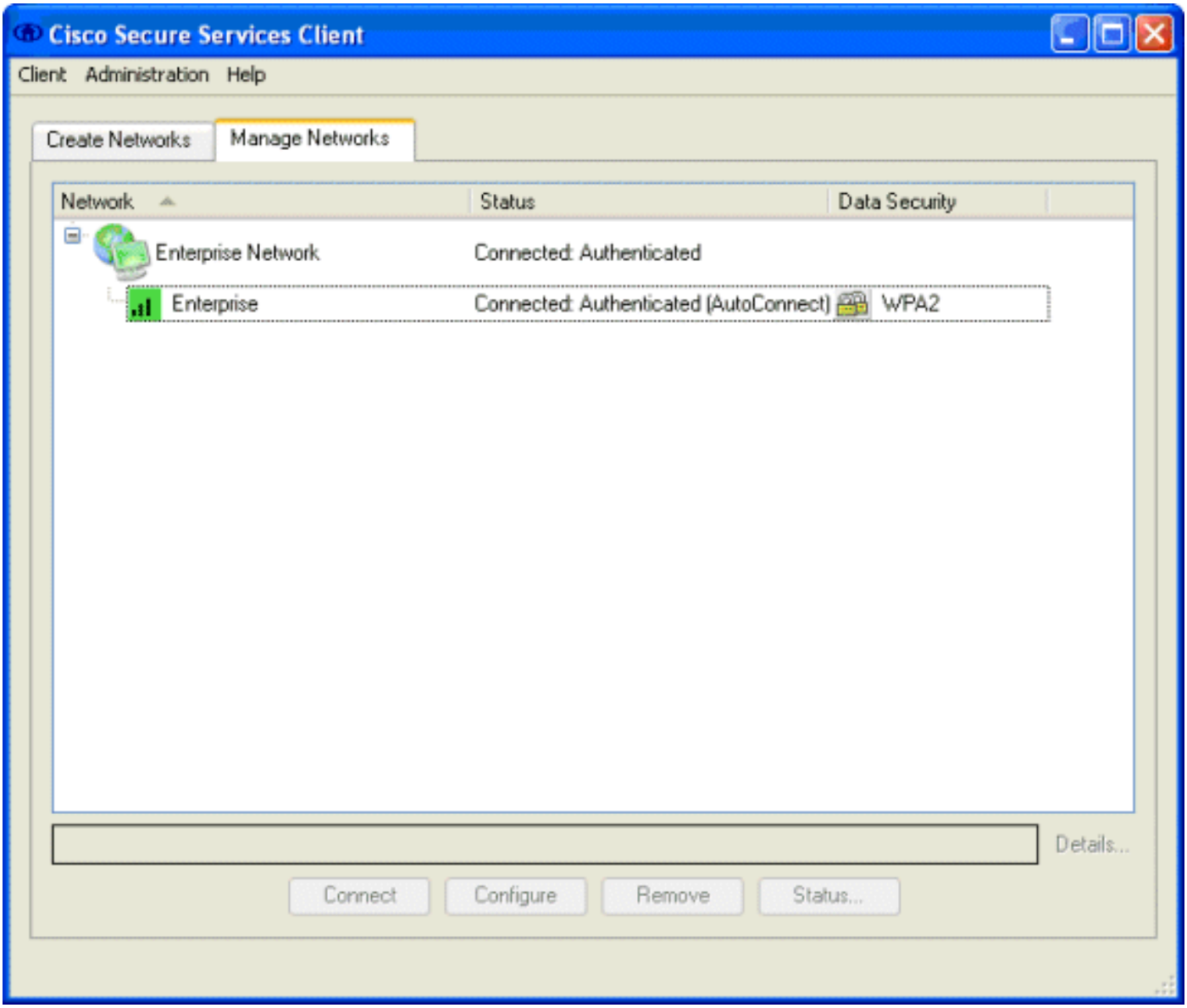
Sob o método em túnel > os ajustes do EAP-TLS, especifique **todo o método** para permitir o EAP-MSCHAPv2 para a auto-disposição PAC e o EAP-GTC para a autenticação. Se você usa um base de dados do Microsoft-formato, tal como o diretório ativo, e se se não apoia nenhuns clientes v1 EAP-FAST na rede, você pode igualmente especificar o uso somente do **MSCHAPv2**

como o método em túnel.

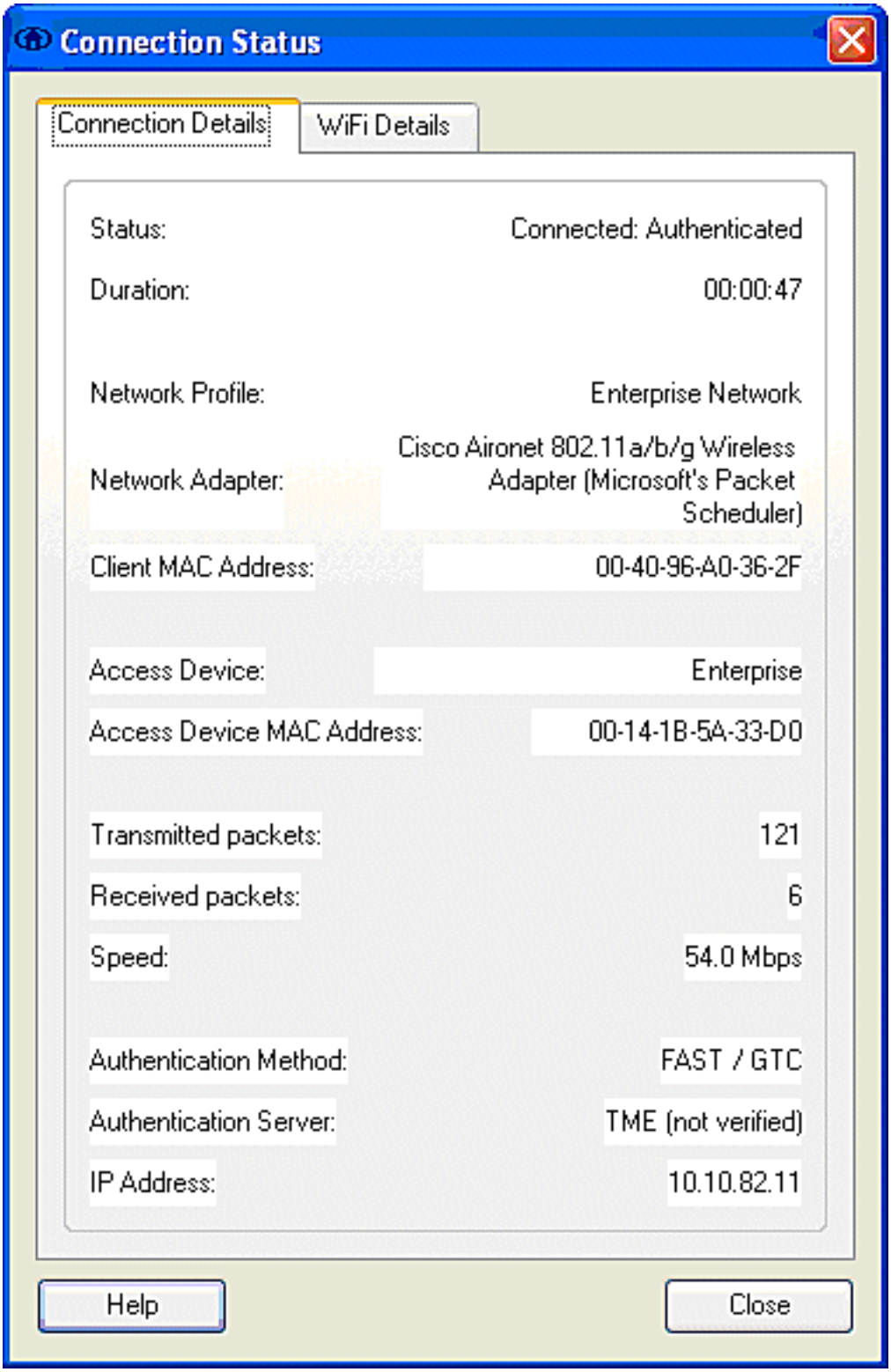
Nota: Valide o certificado de servidor é permitido à revelia sob os ajustes do EAP-TLS neste indicador. Desde que o exemplo não usa o EAP-TLS como o método de autenticação interno, este campo não é aplicável. Se este campo é permitido, permite o cliente de validar o certificado de servidor além do que a validação do server do certificado de cliente dentro do EAP-TLS.

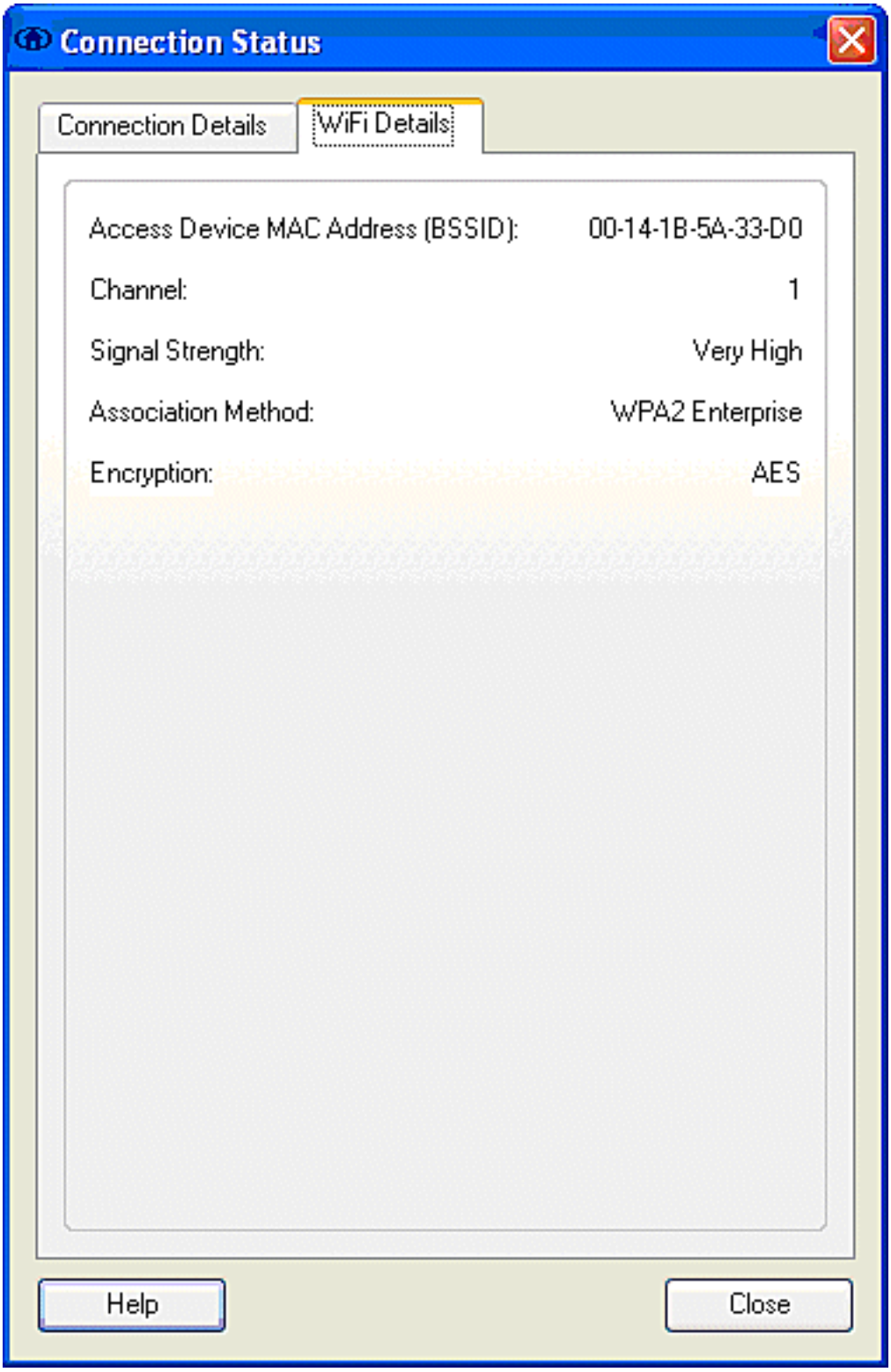


APROVAÇÃO do clique para salvar os ajustes EAP-FAST. Desde que o cliente é configurado para “automaticamente estabeleça” sob o perfil, ele inicia automaticamente a associação/autenticação com a rede. Da aba das redes do controlo, os campos da rede, do estado, e de segurança de dados indicam o status de conexão do cliente. Do exemplo, vê-se que a rede de empreendimento do perfil está no uso, e o dispositivo do acesso de rede é a empresa SSID, que indica conectado: Autenticado e os usos Autoconnect. O campo de segurança de dados indica o tipo de criptografia do 802.11 que é empregado, que, para este exemplo, é WPA2.



Depois que o cliente autentica, escolha o **SSID** sob o perfil na aba das redes do controlo e clique o **estado** para perguntar detalhes da conexão. O indicador dos detalhes da conexão fornece a informação no dispositivo do cliente, o status de conexão e as estatísticas, e o método de autenticação. A aba dos detalhes de WiFi fornece detalhes no status de conexão do 802.11, que inclui o RSSI, o canal do 802.11, e a autenticação/criptografia.


Connection Status
Connection Details
WiFi Details
Status:
Connected: Authenticated
Duration:
00:00:47
Network Profile:
Enterprise Network
Network Adapter:
Cisco Aironet 802.11a/b/g Wireless Adapter (Microsoft's Packet Scheduler)
Client MAC Address:
00-40-96-A0-36-2F
Access Device:
Enterprise
Access Device MAC Address:
00-14-1B-5A-33-D0
Transmitted packets:
121
Received packets:
6
Speed:
54.0 Mbps
Authentication Method:
FAST / GTC
Authentication Server:
TME (not verified)
IP Address:
10.10.82.11
Help
Close



Como um administrador de sistema, você é autorizado à utilidade diagnóstica, o relatório do sistema do Cisco Secure Services Client, que está disponível com a distribuição do padrão CSSC. Esta utilidade é desde o início menu disponível ou do diretório CSSC. A fim obter dados, o clique **recolhe dados > cópia à prancheta > encontra o arquivo de relatório**. Isto dirige uma janela do Explorer do arquivo de Microsoft ao diretório com o arquivo de relatório fechado. Dentro do arquivo fechado, a maioria de dados úteis são ficados situados sob o log (log_current).

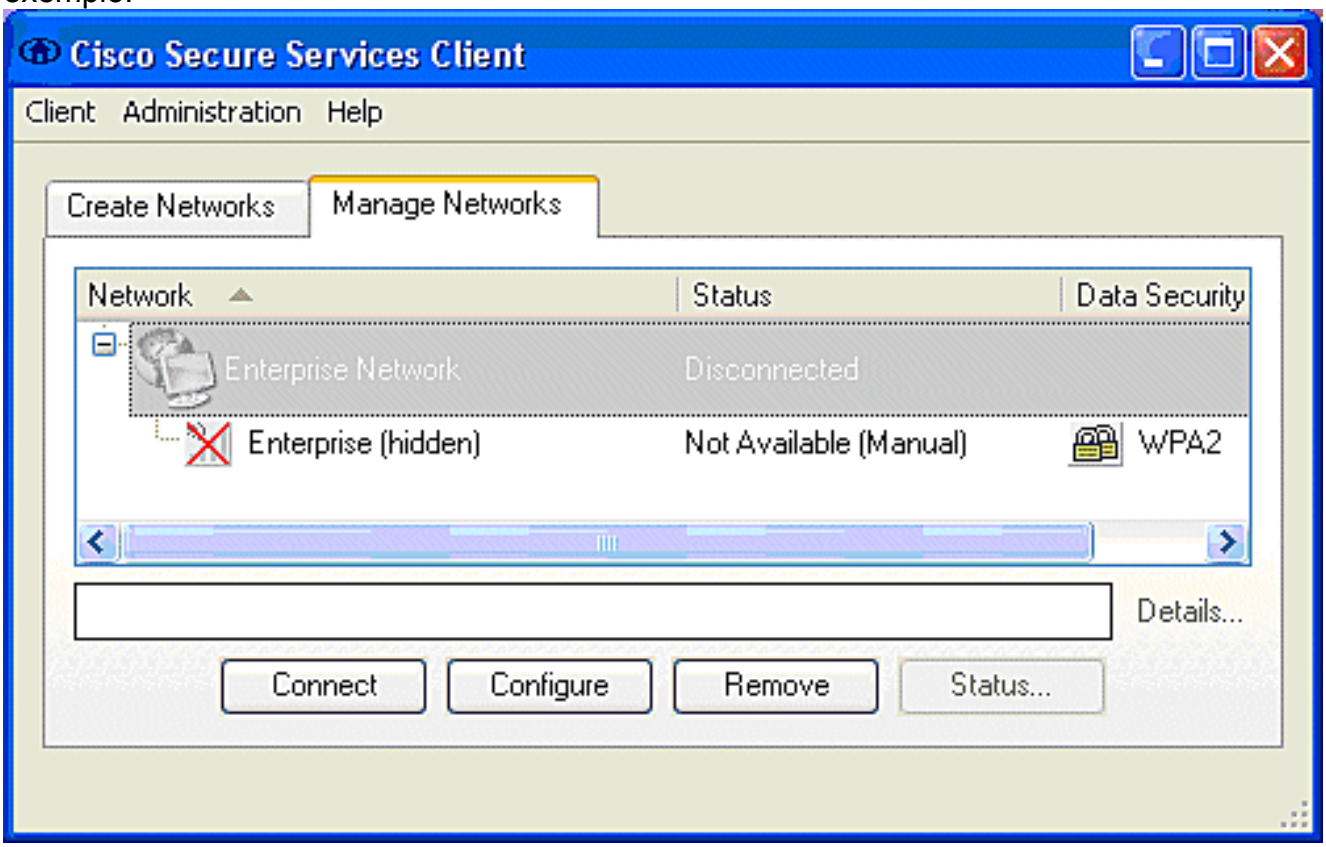
A utilidade dá o status atual de CSSC, relação, e detalhes do direcionador, junto com a informação WLAN (SSID detectado, status de associação, etc.). Isto pode ser útil, especialmente diagnosticar problemas de conectividade entre CSSC e o adaptador de WLAN.

Verifique a operação

Após a configuração do server do Cisco Secure ACS, do controlador de WLAN, do cliente CSSC, e da população presumivelmente correta da configuração e do base de dados, a rede de WLAN é configurada para a autenticação EAP-FAST e uma comunicação cliente segura. Há os pontos numerosos que podem ser monitorados para verificar o progresso/erros para ver se há uma sessão segura.

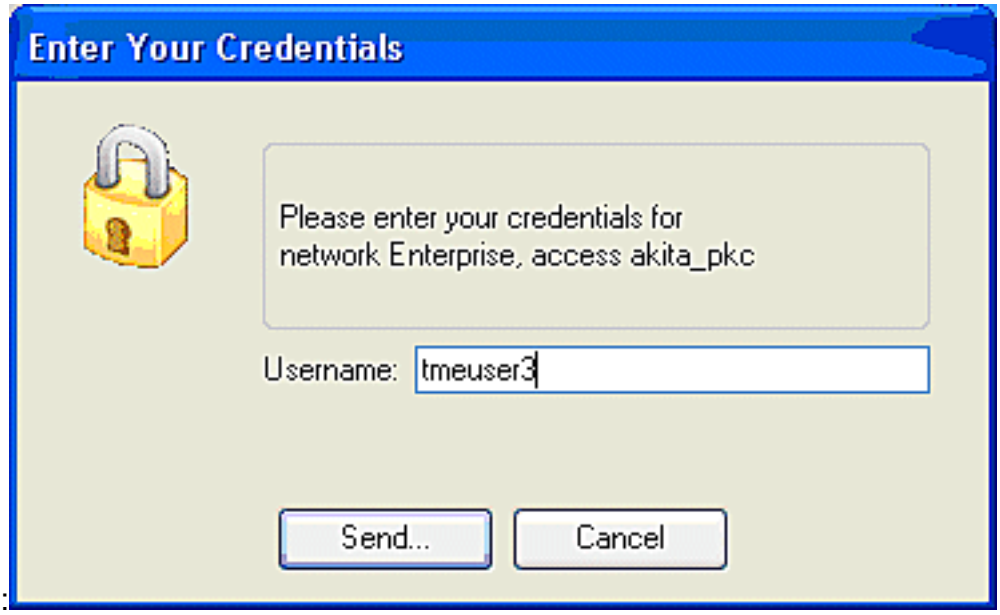
A fim testar a configuração, tente associar um cliente Wireless com o controlador de WLAN com autenticação EAP-FAST.

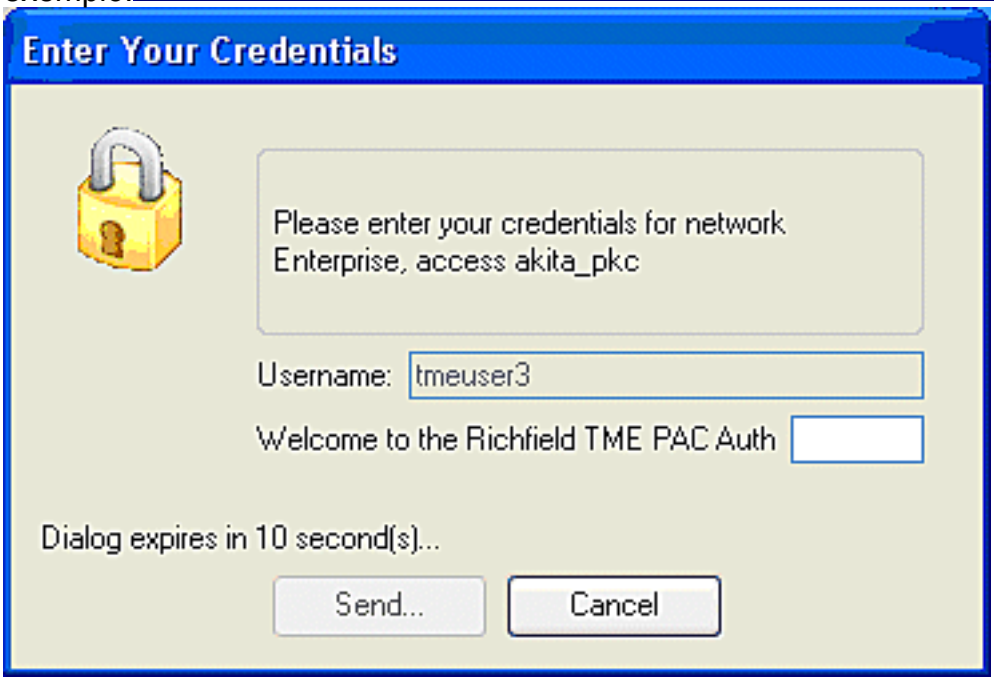
1. Se CSSC é configurado para a Auto-conexão, o cliente tenta esta conexão automaticamente. Se não é configurado para a Auto-conexão e escolhe Sinal-na operação, o usuário deve iniciar a conexão WLAN através do botão de rádio da **conexão**. Isto inicia o processo de associação do 802.11 sobre que a autenticação de EAP ocorre.Este é um exemplo:



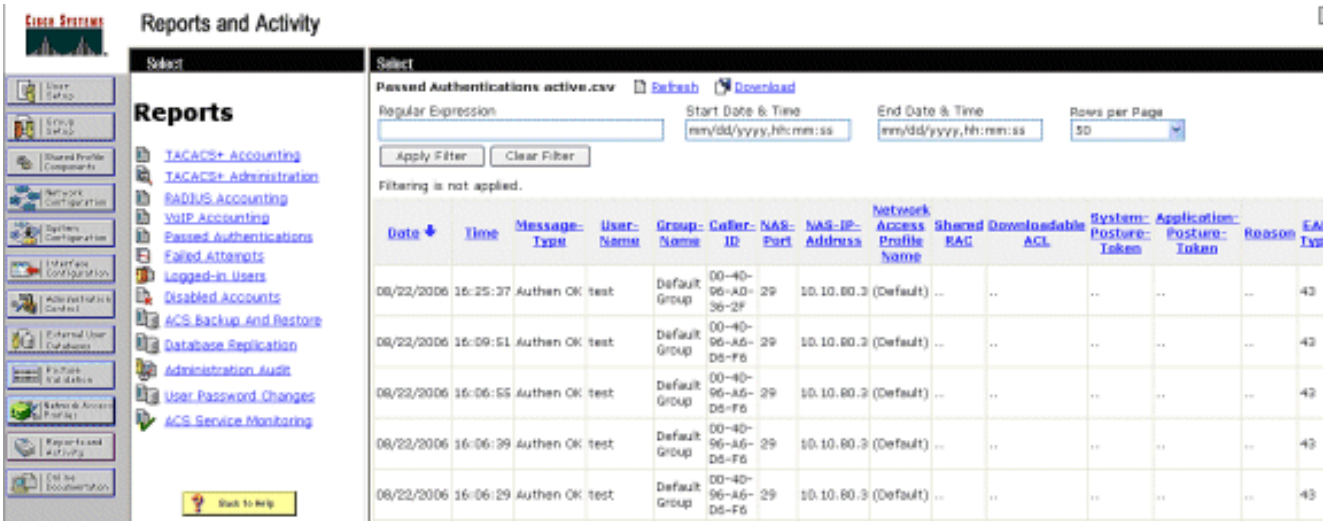
2. O usuário é alertado subseqüentemente fornecer o username e então a senha para a autenticação EAP-FAST (da autoridade PAC ou do ACS EAP-FAST).Este é um

exemplo:

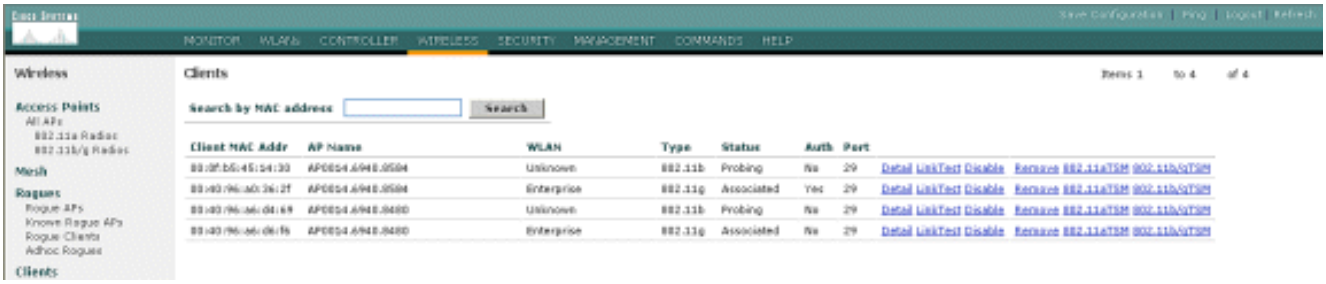




3. O cliente CSSC, pelo WLC, passa então as credenciais do usuário ao servidor Radius (Cisco Secure ACS) a fim validar as credenciais. ACS verifica as credenciais do usuário com uma comparação dos dados e do base de dados configurado (no exemplo de configuração, o base de dados externo é diretório ativo de Windows) e fornece o acesso ao cliente Wireless sempre que as credenciais do usuário são válidas. O relatório passado das autenticações no servidor ACS mostra que o cliente passou a autenticação RADIUS/EAP.Este é um
   exemplo:



4. Em cima da autenticação bem sucedida RADIUS/EAP, o cliente Wireless (00:40:96:ab:36:2f neste exemplo) é autenticado com o controlador de WLAN AP/.



Appendix

Além do que o diagnóstico e a informação de status, que está disponível no Cisco Secure ACS e no controlador de WLAN de Cisco, há os pontos adicionais que podem ser usados para diagnosticar a autenticação EAP-FAST. Embora a maioria de edições da autenticação possa ser diagnosticada sem o uso de um sniffer ou de debugar WLAN trocas EAP no controlador de WLAN, este material de referência é incluído para ajudar a pesquisar defeitos.

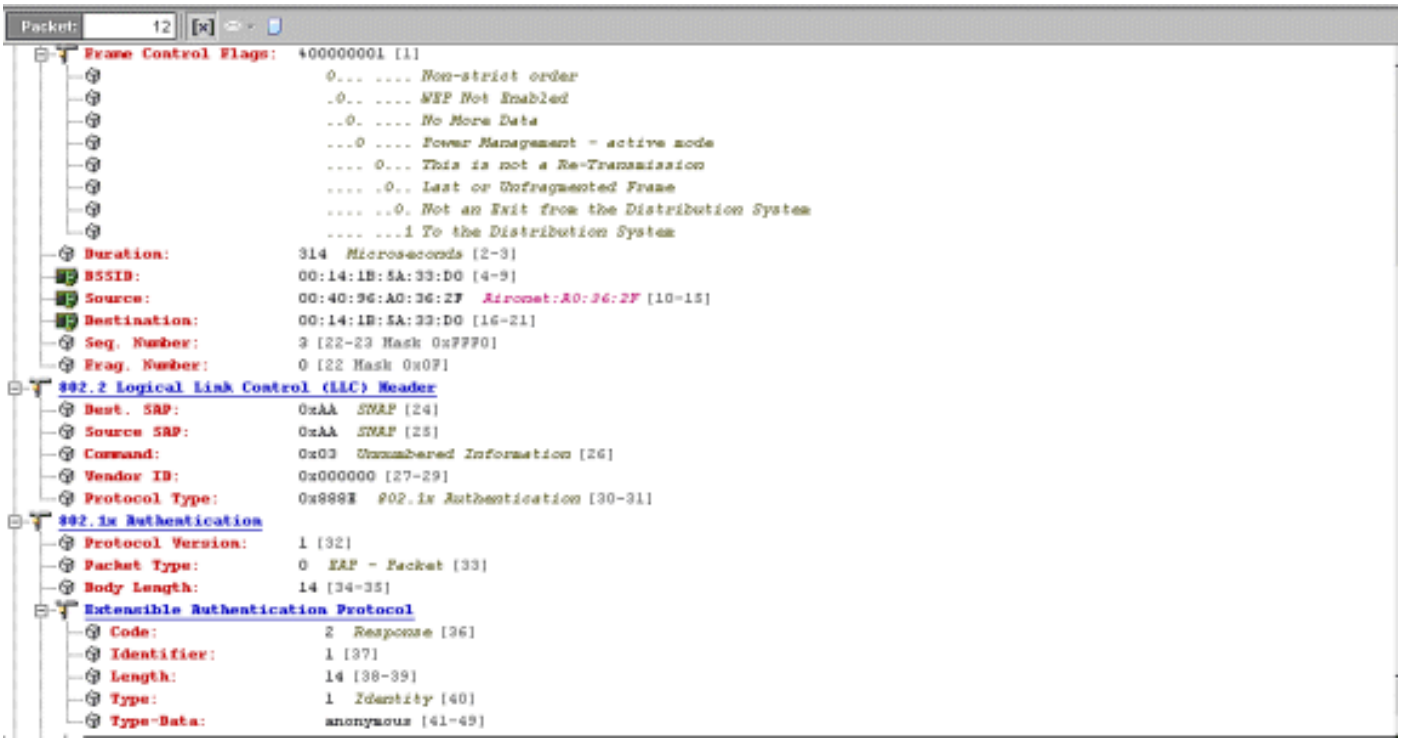
Captação do sniffer para a troca EAP-FAST

Esta captação do sniffer do 802.11 mostra a troca da autenticação.

Source	Flags	Channel	Signal	Data Rate	Size	Relative Time	Protocol	Summary
00:14:1B:5A:33:D0	*	11	68%	36.0	101	00.033877	802.11 Assoc Rsp	FC=...R....,SN=2867,FN= 0,Status...
00:14:1B:5A:33:D0	*	11	70%	24.0	101	00.036453	802.11 Assoc Rsp	FC=...R....,SN=2867,FN= 0,Status...
00:14:1B:5A:33:D0		11	71%	54.0	90	00.036494	802.1x	FC=.F......,SN=2868,FN= 0
Aironet:A0:36:2F		11	54%	1.0	82	00.123205	EAP Response	FC=T.......,SN= 3,FN= 0
00:14:1B:5A:33:D0	#	11	71%	1.0	14	00.123517	802.11 Ack	FC=.....
00:14:1B:5A:33:D0		11	67%	54.0	65	00.165611	802.1x	FC=.F......,SN=2870,FN= 0
Aironet:A0:36:2F		11	55%	1.0	82	00.173920	EAP Response	FC=T.......,SN= 4,FN= 0
00:14:1B:5A:33:D0	#	11	70%	1.0	14	00.174228	802.11 Ack	FC=.....
00:14:1B:5A:33:D0		11	68%	54.0	66	00.178863	802.1x	FC=.F......,SN=2871,FN= 0
Aironet:A0:36:2F		11	58%	1.0	282	00.200632	EAP Response	FC=T.......,SN= 5,FN= 0
Aironet:A0:36:2F		11	58%	1.0	282	00.203340	EAP Response	FC=T..R....,SN= 5,FN= 0
00:14:1B:5A:33:D0	#	11	71%	1.0	14	00.203639	802.11 Ack	FC=.....
00:14:1B:5A:33:D0		11	70%	54.0	188	00.207634	802.1x	FC=.F......,SN=2872,FN= 0
Aironet:A0:36:2F		11	55%	1.0	105	00.216295	EAP Response	FC=T.......,SN= 6,FN= 0
Aironet:A0:36:2F		11	57%	1.0	105	00.217444	EAP Response	FC=T..R....,SN= 6,FN= 0
00:14:1B:5A:33:D0	#	11	70%	1.0	14	00.217754	802.11 Ack	FC=.....
00:14:1B:5A:33:D0		11	67%	54.0	99	00.222799	802.1x	FC=.F......,SN=2874,FN= 0
Aironet:A0:36:2F		11	55%	1.0	152	00.254189	EAP Response	FC=T.......,SN= 7,FN= 0
00:14:1B:5A:33:D0	#	11	68%	1.0	14	00.254499	802.11 Ack	FC=.....
00:14:1B:5A:33:D0		11	64%	54.0	147	00.288950	802.1x	FC=.F.R....,SN=2875,FN= 0
Aironet:A0:36:2F		11	55%	1.0	232	00.318087	EAP Response	FC=T.......,SN= 8,FN= 0
00:14:1B:5A:33:D0	#	11	70%	1.0	14	00.318383	802.11 Ack	FC=.....
00:14:1B:5A:33:D0		11	68%	54.0	44	00.326833	802.1x	FC=.F......,SN=2877,FN= 0
00:14:1B:5A:33:D0		11	65%	54.0	44	00.326882	802.1x	FC=.F.R....,SN=2877,FN= 0
00:14:1B:5A:33:D0		11	67%	48.0	44	00.326922	802.1x	FC=.F.R....,SN=2877,FN= 0
00:14:1B:5A:33:D0		11	67%	54.0	157	00.326964	802.1x	FC=.F......,SN=2878,FN= 0
Aironet:A0:36:2F		11	57%	1.0	157	00.333742	EAP01-Key	FC=T.......,SN= 9,FN= 0
00:14:1B:5A:33:D0	#	11	70%	1.0	14	00.334019	802.11 Ack	FC=.....
00:14:1B:5A:33:D0		11	65%	54.0	207	00.340467	802.1x	FC=.F......,SN=2879,FN= 0
00:14:1B:5A:33:D0		11	67%	54.0	207	00.341130	802.1x	FC=.F.R....,SN=2879,FN= 0
Aironet:A0:36:2F		11	57%	1.0	135	00.342542	EAP01-Key	FC=T.......,SN= 10,FN= 0

Este pacote mostra a resposta EAP-FAST inicial EAP.

Nota: Como configurado no cliente CSSC, anônimo é usado como a identidade exterior EAP na resposta inicial EAP.



Debugar no controlador de WLAN

Estes comandos debug podem ser empregados no controlador de WLAN para monitorar o progresso da troca da autenticação:

- **debugar eventos aaa permitem**
- **debugar o detalhe aaa permitem**

- debugar eventos do dot1x permitem
- debugar estados do dot1x permitem

Este é um exemplo do começo de uma transação da autenticação entre o cliente CSSC e o ACS como monitorado no controlador de WLAN com debuga:

```
Welcome to the Cisco Wizard Configuration Tool
Use the '-' character to backup
System Name [Cisco_33:84:a0]: ws-3750
Enter Administrative User Name (24 characters max): admin
Enter Administrative Password (24 characters max): *****
Management Interface IP Address: 10.10.80.3
Management Interface Netmask: 255.255.255.0
Management Interface Default Router: 10.10.80.2
Management Interface VLAN Identifier (0 = untagged):
Management Interface DHCP Server IP Address: 10.10.80.2
AP Manager Interface IP Address: 10.10.80.4
AP-Manager is on Management subnet, using same values
AP Manager Interface DHCP Server (172.16.1.1):
Virtual Gateway IP Address: 1.1.1.1
Mobility/RF Group Name: Security
Network Name (SSID): Enterprise
Allow Static IP Addresses [YES][no]: yes
Configure a RADIUS Server now? [YES][no]: no
Warning! The default WLAN security policy requires a RADIUS server.
Please see documentation for more details.
Enter Country Code (enter 'help' for a list of countries) [US]:
Enable 802.11b Network [YES][no]: yes
Enable 802.11a Network [YES][no]: yes
Enable 802.11g Network [YES][no]: yes
Enable Auto-RF [YES][no]: yes

Configuration saved!
Resetting system with new configuration.
```

Esta é a conclusão bem sucedida da troca EAP do controlador debuga (com autenticação WPA2):

```
Welcome to the Cisco Wizard Configuration Tool
Use the '-' character to backup
System Name [Cisco_33:84:a0]: ws-3750
Enter Administrative User Name (24 characters max): admin
Enter Administrative Password (24 characters max): *****
Management Interface IP Address: 10.10.80.3
Management Interface Netmask: 255.255.255.0
Management Interface Default Router: 10.10.80.2
Management Interface VLAN Identifier (0 = untagged):
Management Interface DHCP Server IP Address: 10.10.80.2
AP Manager Interface IP Address: 10.10.80.4
AP-Manager is on Management subnet, using same values
AP Manager Interface DHCP Server (172.16.1.1):
Virtual Gateway IP Address: 1.1.1.1
Mobility/RF Group Name: Security
Network Name (SSID): Enterprise
Allow Static IP Addresses [YES][no]: yes
Configure a RADIUS Server now? [YES][no]: no
Warning! The default WLAN security policy requires a RADIUS server.
Please see documentation for more details.
Enter Country Code (enter 'help' for a list of countries) [US]:
Enable 802.11b Network [YES][no]: yes
Enable 802.11a Network [YES][no]: yes
```

```
Enable 802.11g Network [YES][no]: yes
Enable Auto-RF [YES][no]: yes

Configuration saved!
Resetting system with new configuration.
```

Informações Relacionadas

- Guia de Instalação para o server do Cisco Secure ACS for Windows
- Manual de configuração para o Cisco Secure ACS 4.1
- Restrinja o acesso WLAN baseado no SSID com WLC e exemplo de configuração do Cisco Secure ACS
- EAP-TLS sob a rede Wireless unificada com ACS 4.0 e Windows 2003
- Exemplo de configuração de atribuição da VLAN dinâmica com servidor RADIUS e Wireless LAN Controller
- Suporte Técnico e Documentação - Cisco Systems