

Cisco Secure Services Client com autenticação EAP-FAST

Contents

[Introduction](#)

[Prerequisites](#)

[Requisito](#)

[Componentes Utilizados](#)

[Conventions](#)

[Parâmetros de design](#)

[Banco de dados](#)

[Criptografia](#)

[Credenciais para login único e máquina](#)

[Diagrama de Rede](#)

[Configurar o Access Control Server \(ACS\)](#)

[Adicionar ponto de acesso como cliente AAA \(NAS\) no ACS](#)

[Configurar o ACS para consultar o banco de dados externo](#)

[Ativar o suporte EAP-FAST no ACS](#)

[Controlador Cisco WLAN](#)

[Configurar o controlador de LAN sem fio](#)

[Operação básica e registro do LAP no controlador](#)

[Autenticação RADIUS através do Cisco Secure ACS](#)

[Configuração dos parâmetros da WLAN](#)

[Verificar a operação](#)

[Appendix](#)

[Captura de farejador para EAP-FAST Exchange](#)

[Depuração no controlador de WLAN](#)

[Informações Relacionadas](#)

Introduction

Este documento descreve como configurar o Cisco Secure Services Client (CSSC) com os controladores de LAN Wireless, o software Microsoft Windows 2000[®] e o Cisco Secure Access Control Server (ACS) 4.0 através do 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.

Estas são algumas das vantagens da solução CSSC conforme descrito neste documento:

- Autenticação de cada usuário (ou dispositivo) antes da permissão de acesso à WLAN/LAN

- com EAP (Extensible Authentication Protocol)
- Solução de segurança WLAN de ponta a ponta com componentes de servidor, autenticador e cliente
- Solução comum para autenticação com e sem fio
- Chaves de criptografia dinâmicas por usuário derivadas do processo de autenticação
- Sem requisitos para a infraestrutura de chave pública (PKI) ou certificados (verificação de certificado opcional)
- Atribuição de política de acesso e/ou estrutura EAP habilitada para NAC

Nota: Consulte Apresentação de Redes Wireless Cisco SAFE para obter informações sobre a implementação de redes wireless seguras.

A estrutura de autenticação 802.1x foi incorporada como parte do padrão 802.11i (Wireless LAN Security) para ativar as funções de autenticação, autorização e contabilização baseadas na camada 2 em uma rede LAN sem fio 802.11. Atualmente, há vários protocolos EAP disponíveis para implantação em redes com e sem fio. Os protocolos EAP geralmente implantados incluem LEAP, PEAP e EAP-TLS. Além desses protocolos, a Cisco definiu e implementou o protocolo EAP Flexible Authentication por meio do Secure Tunnel (EAP-FAST) como um protocolo EAP baseado em padrões disponível para implantação em redes LAN com e sem fio. A especificação do protocolo EAP-FAST está disponível publicamente no [site da IETF](#).

Como em alguns outros protocolos EAP, o EAP-FAST é uma arquitetura de segurança cliente-servidor que criptografa transações EAP em um túnel TLS. Embora semelhante ao PEAP ou EAP-TTLS a este respeito, difere no fato de o estabelecimento do túnel EAP-FAST se basear em chaves secretas compartilhadas fortes que são exclusivas para cada usuário versus PEAP/EAP-TTLS (que usam um certificado X.509 do servidor para proteger a sessão de autenticação). Essas chaves secretas compartilhadas são chamadas de PACs (Protected Access Credentials) e podem ser distribuídas automaticamente (Automatic ou In-band Provisioning) ou manualmente (Manual ou Out-of-band Provisioning) para dispositivos clientes. Como os handshakes baseados em segredos compartilhados são mais eficientes do que os handshakes baseados em uma infraestrutura de PKI, o EAP-FAST é o tipo de EAP mais rápido e com menos uso intensivo de processador daqueles que fornecem trocas de autenticação protegidas. O EAP-FAST também foi projetado para simplicidade de implantação, pois não requer um certificado no cliente LAN sem fio ou na infraestrutura RADIUS, mas incorpora um mecanismo de provisionamento integrado.

Estes são alguns dos principais recursos do protocolo EAP-FAST:

- Login único (SSO) com nome de usuário/senha do Windows
- Suporte para execução de script de login
- Suporte a WPA (Wi-Fi Protected Access) sem requerente de terceiros (somente Windows 2000 e XP)
- Implantação simples sem necessidade de infraestrutura de PKI
- Envelhecimento da senha do Windows (ou seja, suporte para expiração de senha baseada em servidor)
- Integração com o Cisco Trust Agent para Network Admission Control com o software cliente apropriado

Prerequisites

Requisito

Há uma suposição de que o instalador tem conhecimento da instalação básica do Windows 2003 e da instalação do Cisco WLC, já que este documento abrange apenas as configurações específicas para facilitar os testes.

Para obter informações sobre instalação e configuração iniciais dos Cisco 4400 Series Controllers, consulte o [Guia de início rápido: Cisco 4400 Series Wireless LAN Controllers](#). Para obter informações sobre instalação e configuração iniciais dos Cisco 2000 Series Controllers, consulte o [Guia de início rápido: Cisco 2000 Series Wireless LAN Controllers](#).

Antes de começar, instale o Microsoft Windows Server 2000 com o software de service pack mais recente. Instale os controladores e os LAPs (Lightweight Access Points, pontos de acesso leves) e verifique se as atualizações de software mais recentes estão configuradas.

Componentes Utilizados

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

- Controlador Cisco 2006 ou 4400 Series que executa 4.0.155.5
- AP LWAPP Cisco 1242
- Windows 2000 com Active Directory
- Switch Cisco Catalyst 3750G
- Windows XP com placa de adaptador CB21AG e Cisco Secure Services Client versão 4.05

Conventions

Consulte as [Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos](#).

Parâmetros de design

Banco de dados

Quando você implanta uma rede WLAN e busca um protocolo de autenticação, geralmente se deseja usar um banco de dados atual para autenticação de usuário/máquina. Os bancos de dados típicos que podem ser usados são o Windows Active Directory, LDAP ou um banco de dados OTP (One Time Password, Senha única) (ou seja, RSA ou SecureID). Todos esses bancos de dados são compatíveis com o protocolo EAP-FAST, mas quando você planeja a implantação, há alguns requisitos de compatibilidade que devem ser considerados. A implantação inicial de um arquivo PAC para os clientes é realizada por meio do provisionamento automático anônimo, provisionamento autenticado (através do certificado X.509 atual do cliente) ou provisionamento manual. Para a finalidade deste documento, o provisionamento automático anônimo e o provisionamento manual são considerados.

O provisionamento automático de PAC usa o Authenticated Diffie-Hellman Key Agreement Protocol (ADHP) para estabelecer um túnel seguro. O túnel seguro pode ser estabelecido anonimamente ou por meio de um mecanismo de autenticação de servidor. Dentro da conexão de túnel estabelecida, o MS-CHAPv2 é usado para autenticar o cliente e, na autenticação bem-sucedida, para distribuir o arquivo PAC ao cliente. Depois que a PAC tiver sido provisionada com êxito, o arquivo PAC pode ser usado para iniciar uma nova sessão de autenticação EAP-FAST para obter acesso seguro à rede.

O provisionamento automático de PAC é relevante para o banco de dados em uso porque, como o mecanismo de provisionamento automático depende do MSCHAPv2, o banco de dados usado para autenticar usuários deve ser compatível com esse formato de senha. Se você usa o EAP-FAST com um banco de dados que não oferece suporte ao formato MSCHAPv2 (como OTP, Novell ou LDAP), é necessário empregar algum outro mecanismo (ou seja, provisionamento manual ou provisionamento autenticado) para implantar arquivos PAC do usuário. Este documento fornece um exemplo de provisionamento automático com um banco de dados de usuários do Windows.

Criptografia

A autenticação EAP-FAST não exige o uso de um tipo de criptografia WLAN específico. O tipo de criptografia WLAN a ser usado é determinado pelos recursos da placa de rede do cliente. É recomendável empregar a criptografia WPA2 (AES-CCM) ou WPA(TKIP), dependendo dos recursos da placa NIC na implantação específica. Observe que a solução Cisco WLAN permite a coexistência de dispositivos clientes WPA2 e WPA em um SSID comum.

Se os dispositivos clientes não suportam WPA2 ou WPA, é possível implantar a autenticação 802.1X com chaves WEP dinâmicas, mas, devido às bem conhecidas explorações contra chaves WEP, esse mecanismo de criptografia WLAN não é recomendado. Se for necessário oferecer suporte a clientes somente WEP, é recomendável empregar um intervalo de tempo limite de sessão, o que exige que os clientes derivem uma nova chave WEP em um intervalo frequente. Trinta minutos é o intervalo de sessão recomendado para taxas de dados típicas da WLAN.

Credenciais para login único e máquina

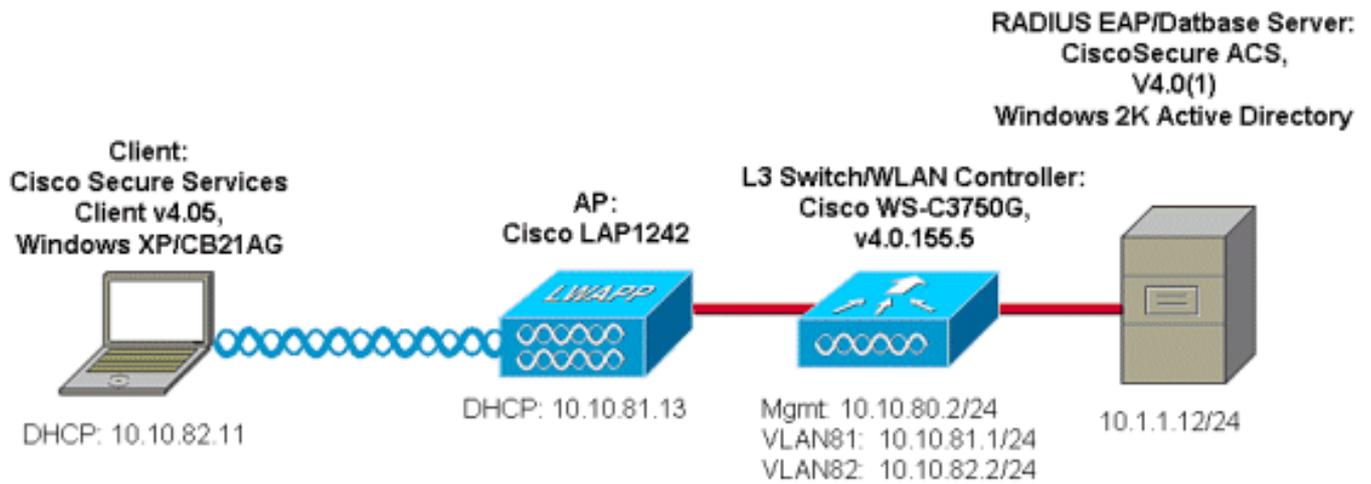
Logon único refere-se à capacidade de um único usuário fazer logon ou inserir credenciais de autenticação para ser usado para acessar vários aplicativos ou vários dispositivos. Para os fins deste documento, Logon único refere-se ao uso das credenciais usadas para fazer logon em um PC para autenticação na WLAN.

Com o Cisco Secure Services Client, é possível usar as credenciais de login de um usuário para autenticar também na rede WLAN. Se você deseja autenticar um PC na rede antes do login do usuário no PC, é necessário usar credenciais de usuário armazenadas ou credenciais vinculadas a um perfil de máquina. Qualquer um desses métodos é útil nos casos em que se deseja executar scripts de login ou mapear unidades quando o PC é inicializado, ao contrário de quando um usuário faz logon.

Diagrama de Rede

Este é o diagrama de rede usado neste documento. Nesta rede, há quatro sub-redes usadas. Observe que não é necessário segmentar esses dispositivos em redes diferentes, mas isso oferece a maior flexibilidade para integração com redes reais. O Controlador de LAN sem fio integrado Catalyst 3750G fornece comutação Power Over Ethernet (POE), comutação L3 e capacidade de controlador WLAN em um chassi comum.

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



[Configurar o Access Control Server \(ACS\)](#)

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

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

[Adicionar ponto de acesso como cliente AAA \(NAS\) no ACS](#)

Esta seção descreve como configurar o ACS para EAP-FAST com provisionamento de PAC em banda com o Windows Active Directory como o banco de dados externo.

1. Faça login no **ACS > Network Configuration** e clique em **Add Entry**.
2. Preencha o nome da controladora WLAN, o endereço IP, a chave secreta compartilhada e, em **Authenticate Using**, escolha **RADIUS (Cisco Airespace)**, que também inclui atributos **RADIUS IETF**. **Observação:** se o **Network Device Groups (NDG)** estiver habilitado, primeiro escolha o NDG apropriado e adicione o controlador de WLAN a ele. Consulte o Guia de Configuração do ACS para obter detalhes sobre o NDG.
3. Clique em **Enviar+**
Reiniciar.



AAA Client Setup For ws-3750

AAA Client IP Address	<input type="text" value="10.10.80.3"/>
Key	<input type="text" value="cisco123"/>
Authenticate Using	<input type="text" value="RADIUS (Cisco Airespace)"/>
<input type="checkbox"/> Single Connect TACACS+ AAA Client (Record stop in accounting on failure).	
<input type="checkbox"/> Log Update/Watchdog Packets from this AAA Client	
<input type="checkbox"/> Log RADIUS Tunneling Packets from this AAA Client	
<input type="checkbox"/> Replace RADIUS Port info with Username from this AAA Client	

[Back to Help](#)

[Configurar o ACS para consultar o banco de dados externo](#)

Esta seção descreve como configurar o ACS para consultar o banco de dados externo.

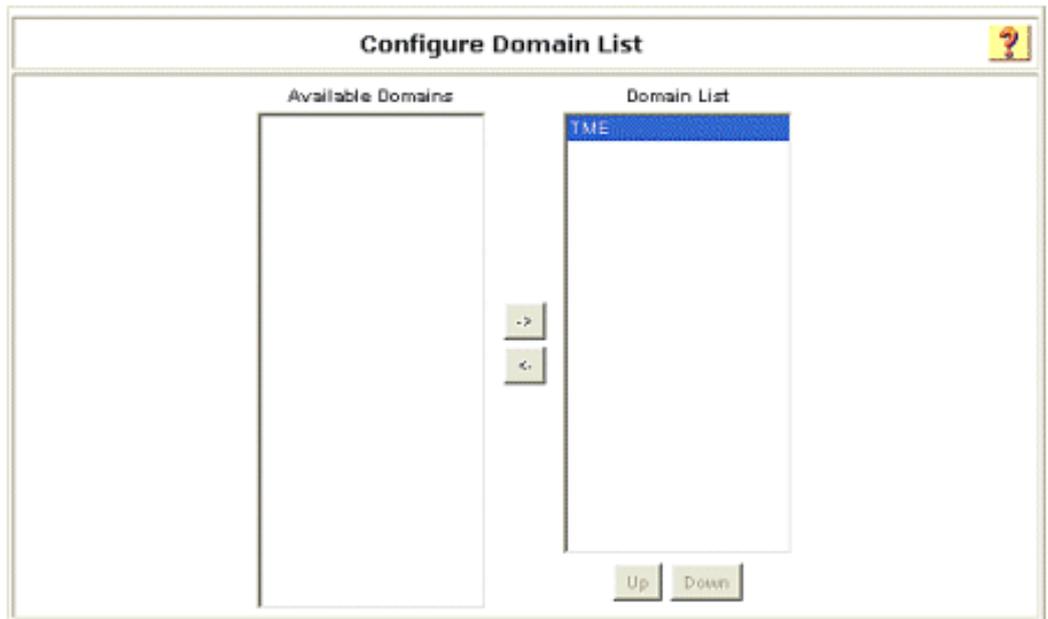
1. Clique em **External User Database > Database Configuration > Windows Database > Configure**.
2. Em Configurar lista de domínio, mova domínios de domínios disponíveis para a lista de domínios. **Nota:** O servidor que executa o ACS deve conhecer esses domínios para que o aplicativo do ACS detecte e use esses domínios com fins de autenticação.



External User Databases



If the unknown user policy contains additional external databases and the Windows database is not the last database on the Selected Databases list, you may enable this option.



3. Em Configurações EAP do Windows, configure a opção para permitir a alteração de senha na sessão PEAP ou EAP-FAST. Consulte o [Guia de Configuração do Cisco Secure ACS 4.1](#) para obter mais detalhes sobre o EAP-FAST e a validade de senhas do Windows.
4. Clique em Submit. **Nota:** Você também pode habilitar o recurso **Dialin Permission para EAP-FAST em Windows User Database Configuration** de forma a permitir que o banco de dados externo do Windows controle as permissões de acesso. As Configurações MS-CHAP para alteração de senha na página de configuração do banco de dados do Windows só se aplicam à autenticação MS-CHAP não EAP. Para permitir a alteração de senha em conjunto com EAP-FAST, é necessário ativar a alteração de senha em Configurações EAP do Windows.

- User Setup
- Group Setup
- Shared Profile Components
- Network Configuration
- System Configuration
- Interface Configuration
- Administration Control
- External User Databases
- Posture Validation
- Network Access Profiles
- Reports and Activity
- Online Documentation

Windows EAP Settings ?

Enable password change inside PEAP or EAP-FAST.
 EAP-TLS Strip Domain Name.

Machine Authentication.

Enable PEAP machine authentication.
 Enable EAP-TLS machine authentication.
 EAP-TLS and PEAP machine authentication name prefix:

Enable machine access restrictions.
 Aging time (hours):
 Group map for successful user authentication without machine authentication:

User Groups that are exempt from passing machine authentication:

Available User Groups		Selected User Groups
Default Group	->	
Group 1	->	
Group 2	->	
Group 3	->	
Group 4	->	
Group 5	->	
Group 6	->	
Group 7	->	
Group 8	->	

These settings can be used to enable or disable specific Windows EAP functionality

5. Clique em **External User Database > Unknown User Policy** e escolha o botão de opção **Check the following external user database.**
6. Mova o Banco de Dados do Windows de **External Databases** para **Selected Databases.**
7. Clique em **Submit.** **Nota:** A partir desse ponto, o ACS verificará o banco de dados do **Windows.** Se o usuário não for encontrado no banco de dados local do ACS, ele colocará o usuário no grupo padrão do ACS. Consulte a documentação do ACS para obter mais detalhes sobre Mapeamentos de grupos de bancos de dados. **Nota:** Como o ACS consulta o banco de dados do Microsoft Active Directory para verificar credenciais de usuários, configurações de direitos de acesso adicionais precisam ser definidas no Windows. Consulte o [Guia de Instalação do Cisco Secure ACS para Windows Server](#) para obter detalhes.

External User Databases

Edit

Configure Unknown User Policy

Use this table to define how users will be handled when they are not found in the ACS Internal Database.

Fail the attempt
 Check the following external user databases

External Databases	Selected Databases
	Windows DatabaseWind

For newly created dynamic users, the TACACS+ enable password is authenticated against:
 The internal database.
 The database in which the user profile is held.

[Ativar o suporte EAP-FAST no ACS](#)

Esta seção descreve como ativar o suporte EAP-FAST no ACS.

1. Vá para **System Configuration > Global Authentication Setup > EAP-FAST Configuration**.
2. Escolha **Permitir EAP-FAST**.
3. Configure estas recomendações: Chave mestre TTL/ Chave mestre aposentada TTL/ PAC TTL. Essas configurações são definidas por padrão no Cisco Secure ACS: TTL de chave mestra: 1 mês TTL de chave aposentada: 3 meses TTL PAC: 1 semana
4. Preencha o campo **Informações da ID da Autoridade**. Este texto é mostrado em algum software cliente EAP-FAST onde a seleção da Autoridade PAC é o controlador. **Nota: O Cisco Secure Services Client não emprega esse texto descritivo para a autoridade de PAC.**
5. Escolha o campo **Permitir provisionamento de PAC em banda**. Este campo ativa o Provisionamento Automático de PAC para clientes EAP-FAST habilitados corretamente. Para este exemplo, o provisionamento automático é empregado.
6. Escolha **Métodos internos permitidos**: EAP-GTC e EAP-MSCHAP2. Isso permite a operação de clientes EAP-FAST v1 e EAP-FAST v1a. (O Cisco Secure Services Client oferece suporte a EAP-FAST v1a.) Se não for necessário oferecer suporte a clientes EAP-FAST v1, somente EAP-MSCHAPv2 precisa ser habilitado como um método interno.
7. Escolha a caixa de verificação **EAP-FAST Master Server** para ativar este servidor EAP-FAST como mestre. Isso permite que outros servidores ACS utilizem esse servidor como

autoridade PAC mestre para evitar o fornecimento de chaves exclusivas para cada ACS em uma rede. Consulte o Guia de configuração do ACS para obter detalhes.

8. Clique em **Enviar+Reiniciar**.

The screenshot displays the Cisco System Configuration web interface. On the left is a navigation sidebar with icons and labels for various configuration areas: User Setup, Group Setup, Shared Profile Components, Network Configuration, System Configuration, Interface Configuration, Administration Control, External User Databases, Posture Validation, Network Access Profiles, Reports and Activity, and Online Documentation. The main content area is titled "System Configuration" and "EAP-FAST Configuration". A window titled "EAP-FAST Settings" is open, showing the following configuration options:

- Allow EAP-FAST
- Active master key TTL: 1 months
- Retired master key TTL: 3 months
- Tunnel PAC TTL: 1 weeks
- Client initial message: TME
- Authority ID Info: TME
- Allow anonymous in-band PAC provisioning
- Allow authenticated in-band PAC provisioning
 - Accept client on authenticated provisioning
 - Require client certificate for provisioning
- Allow Machine Authentication
 - Machine PAC TTL: 1 weeks
- Allow Stateless session resume
 - Authorization PAC TTL: 1 hours
- Allowed inner methods:
 - EAP-GTC
 - EAP-MSCHAPv2
 - EAP-TLS
- Select one or more of the following EAP-TLS comparison methods:
 - Certificate SAN comparison
 - Certificate CN comparison
 - Certificate Binary comparison
- EAP-TLS session timeout (minutes): 120
- EAP-FAST master server
- Actual EAP-FAST server status: **Master**

[Controlador Cisco WLAN](#)

Para os fins deste Guia de Implantação, um Cisco WS3750G Integrated Wireless LAN Controller (WLC) é usado com os APs Lightweight Cisco AP1240 (LAP) para fornecer a infraestrutura de WLAN para testes CSSC. A configuração é aplicável para qualquer controlador de WLAN da Cisco. A versão do software utilizada é 4.0.155.5.

[Configurar o controlador de LAN sem fio](#)

Operação básica e registro do LAP no controlador

Use o assistente de configuração de inicialização na interface de linha de comando (CLI) para configurar a WLC para a operação básica. Como alternativa, você pode usar a GUI para configurar a WLC. Este documento explica a configuração na WLC com o assistente de configuração de inicialização na CLI.

Depois que a WLC é inicializada pela primeira vez, ela entra no assistente de configuração de inicialização. Use o assistente de configuração para definir as configurações básicas. Você pode acessar o assistente por meio da CLI ou da GUI. Esta saída mostra um exemplo do assistente de configuração de inicialização na 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.
```

Esses parâmetros configuram a WLC para a operação básica. Neste exemplo de configuração, a WLC usa **10.10.80.3** como o endereço IP da interface de gerenciamento e **10.10.80.4** como o endereço IP da interface do gerenciador de AP.

Antes que qualquer outro recurso possa ser configurado nas WLCs, os LAPs devem se registrar na WLC. Este documento pressupõe que o LAP está registrado no WLC. Consulte a seção [Registro de AP Lightweight nos WLCs](#) de [Exemplo de Configuração de Failover de Controlador de WLAN para Pontos de Acesso Lightweight](#) para obter informações sobre o registro de APs Lightweight no WLC. Para referência a este exemplo de configuração, os AP1240s são implantados 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 para fornecer a descoberta do controlador.

Autenticação RADIUS através do Cisco Secure ACS

A WLC precisa ser configurada para encaminhar as credenciais do usuário ao servidor Cisco

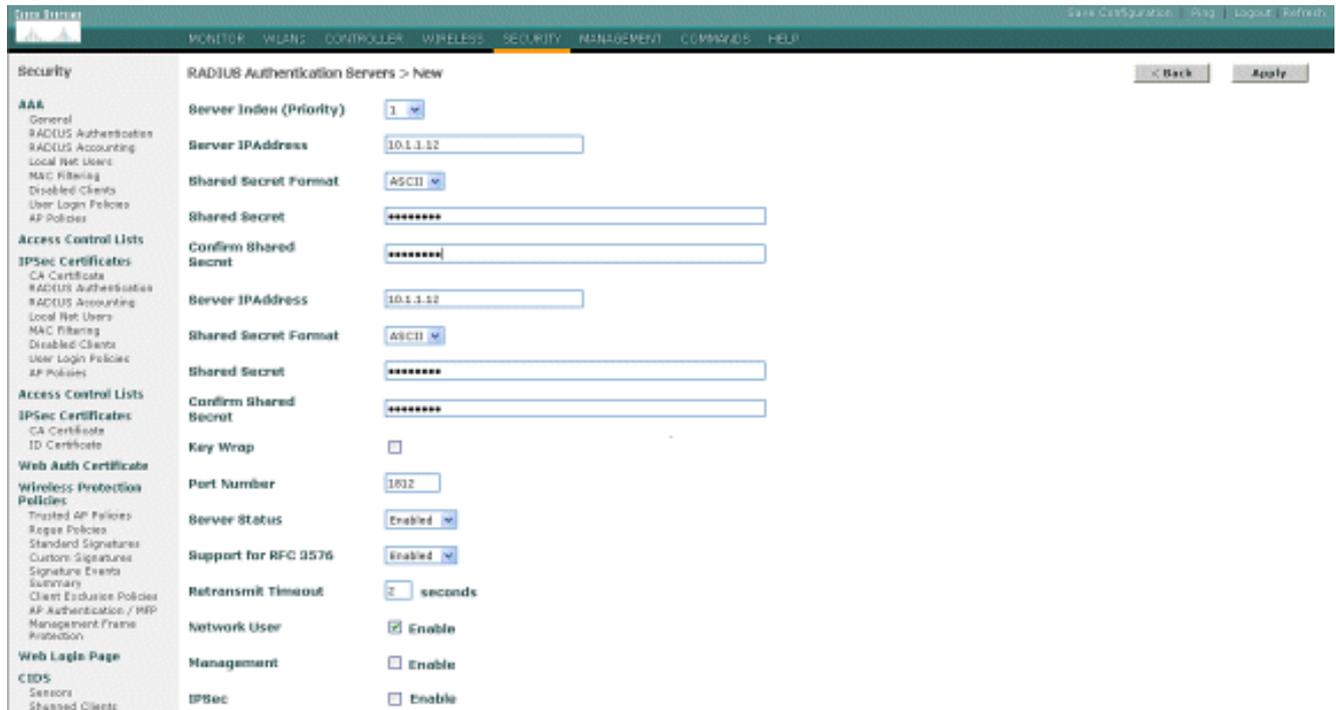
Secure ACS. O servidor ACS valida as credenciais do usuário (através do banco de dados configurado do Windows) e fornece acesso aos clientes sem fio.

Conclua estes passos para configurar a WLC para comunicação com o servidor ACS:

1. Clique em **Segurança e Autenticação RADIUS** na GUI do controlador para exibir a página Servidores de Autenticação RADIUS. Em seguida, clique em **New** para definir o servidor ACS.



2. Defina os parâmetros do servidor ACS na página RADIUS Authentication Servers > New. Esses parâmetros incluem o endereço IP ACS, o segredo compartilhado, o número da porta e o status do servidor. **Nota: Os números de portas 1645 ou 1812 são compatíveis com o ACS para autenticação RADIUS.** As caixas de seleção Network User and Management determinam se a autenticação baseada em RADIUS se aplica a usuários de rede (por exemplo, clientes WLAN) e gerenciamento (ou seja, usuários administrativos). O exemplo de configuração usa o Cisco Secure ACS como o servidor RADIUS com o endereço IP 10.1.1.12:



[Configuração dos parâmetros da WLAN](#)

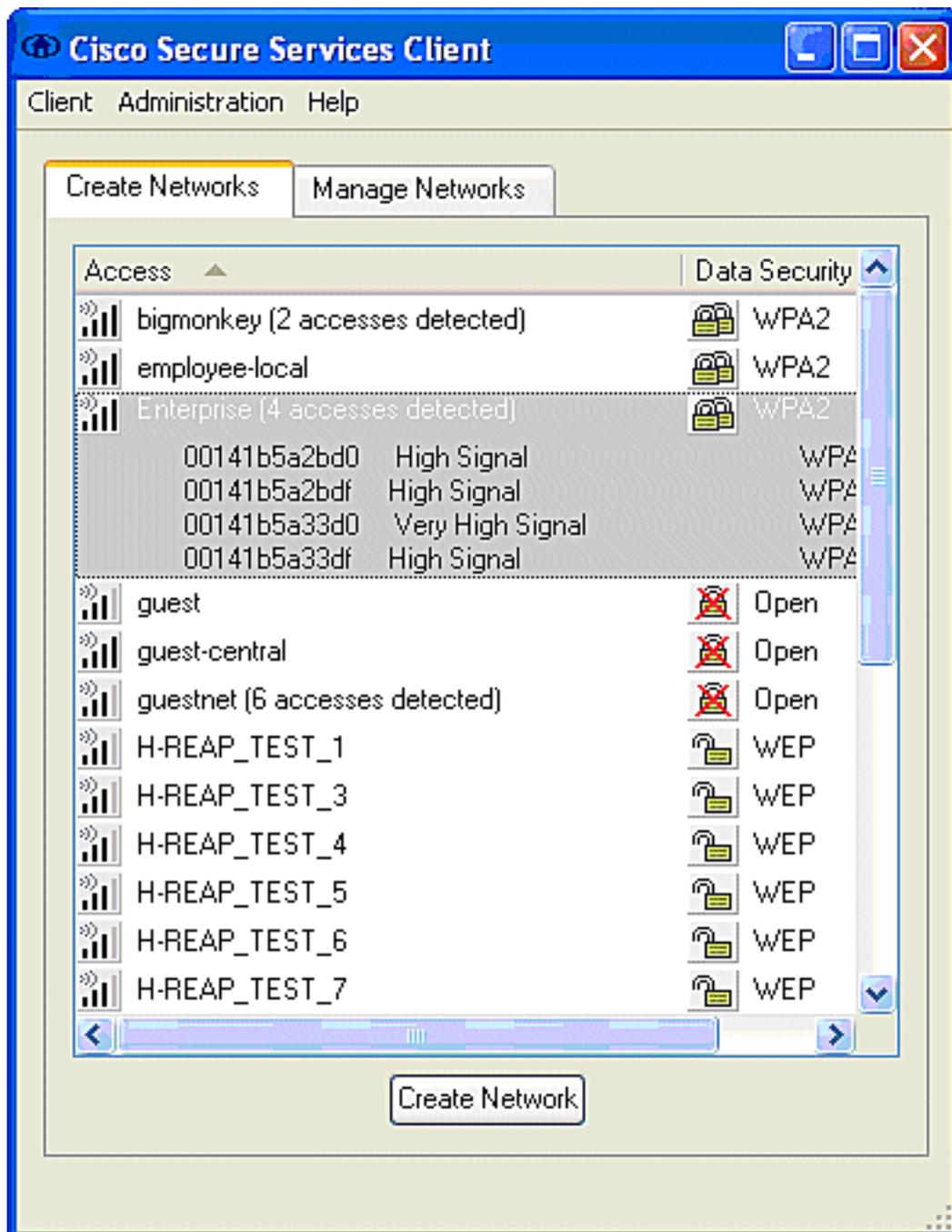
Esta seção descreve a configuração do Cisco Secure Services Client. Neste exemplo, o CSSC v4.0.5.4783 é usado com um adaptador cliente Cisco CB21AG. Antes da instalação do software CSSC, verifique se apenas os drivers para o CB21AG estão instalados, não o Aironet Desktop Utility (ADU).

Depois que o software é instalado e executado como um serviço, ele verifica as redes disponíveis

e exibe as disponíveis.

Nota:O CSSC desativa o Windows Zero Config.

Nota:Somente os SSIDs habilitados para broadcast são visíveis.



Nota:O Controlador de WLAN, por padrão, difunde o SSID, de forma que ele seja mostrado na lista Create Networks de SSIDs verificados. Para criar um perfil de rede, basta clicar no SSID na lista (Empresa) e no botão de opção Criar rede.

Se a infraestrutura da WLAN estiver configurada com o SSID de broadcast desabilitado, você deverá adicionar manualmente o SSID; clique no botão de opção Add em Access Devices (Dispositivos de acesso) e insira manualmente o SSID apropriado (por exemplo, Enterprise). Configure o comportamento de prova ativo para o cliente, ou seja, onde o cliente procura ativamente seu SSID configurado; especifique **Actively search for this access device** depois de inserir o SSID na janela Add Access Device.

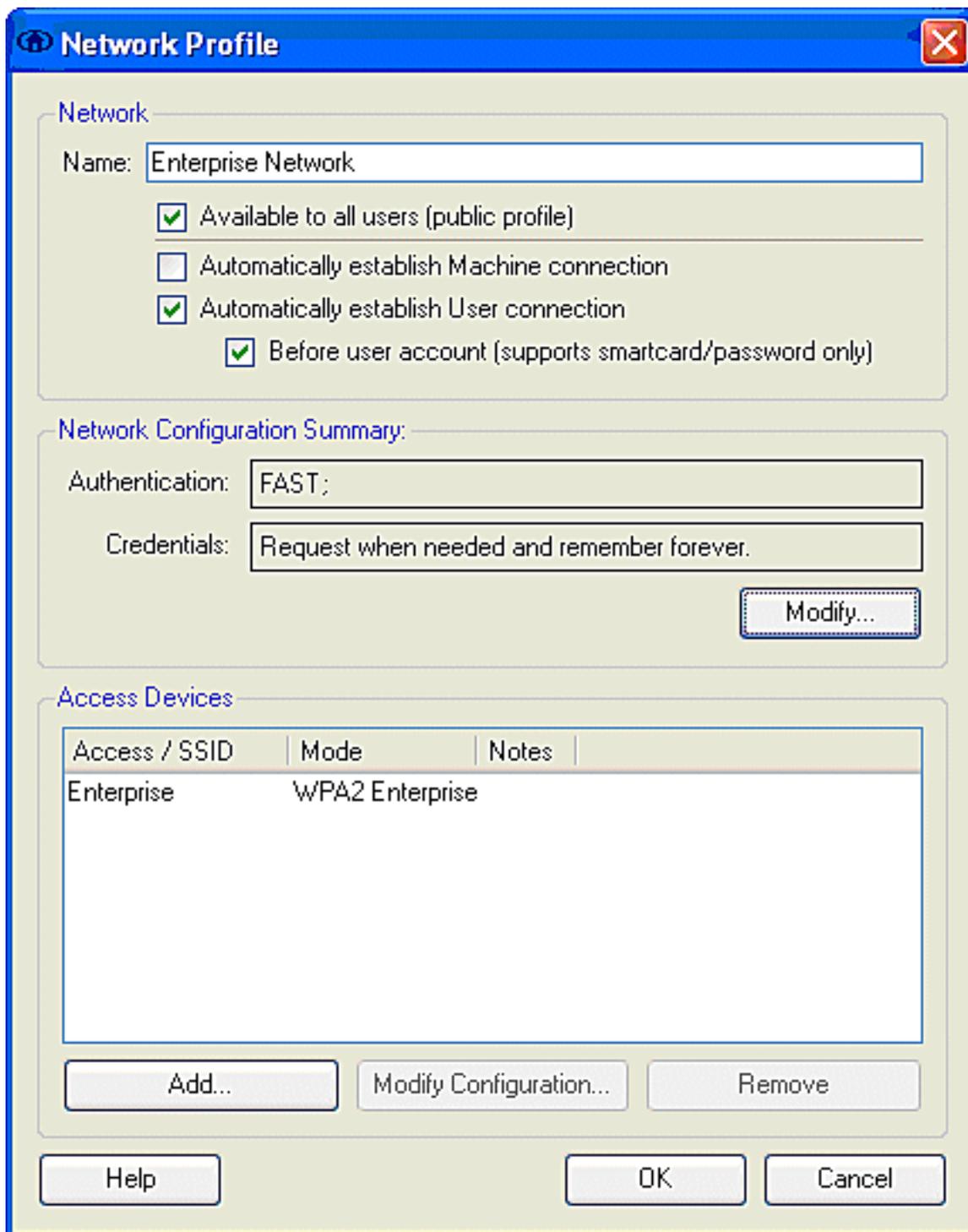
Nota:As configurações de porta não permitirão modos corporativos (802.1X) se as configurações de autenticação EAP não forem primeiro configuradas para o perfil.

O botão de opção **Create Network** inicia a janela Network Profile, que permite associar o SSID escolhido (ou configurado) a um mecanismo de autenticação. Atribua um nome descritivo para o perfil.

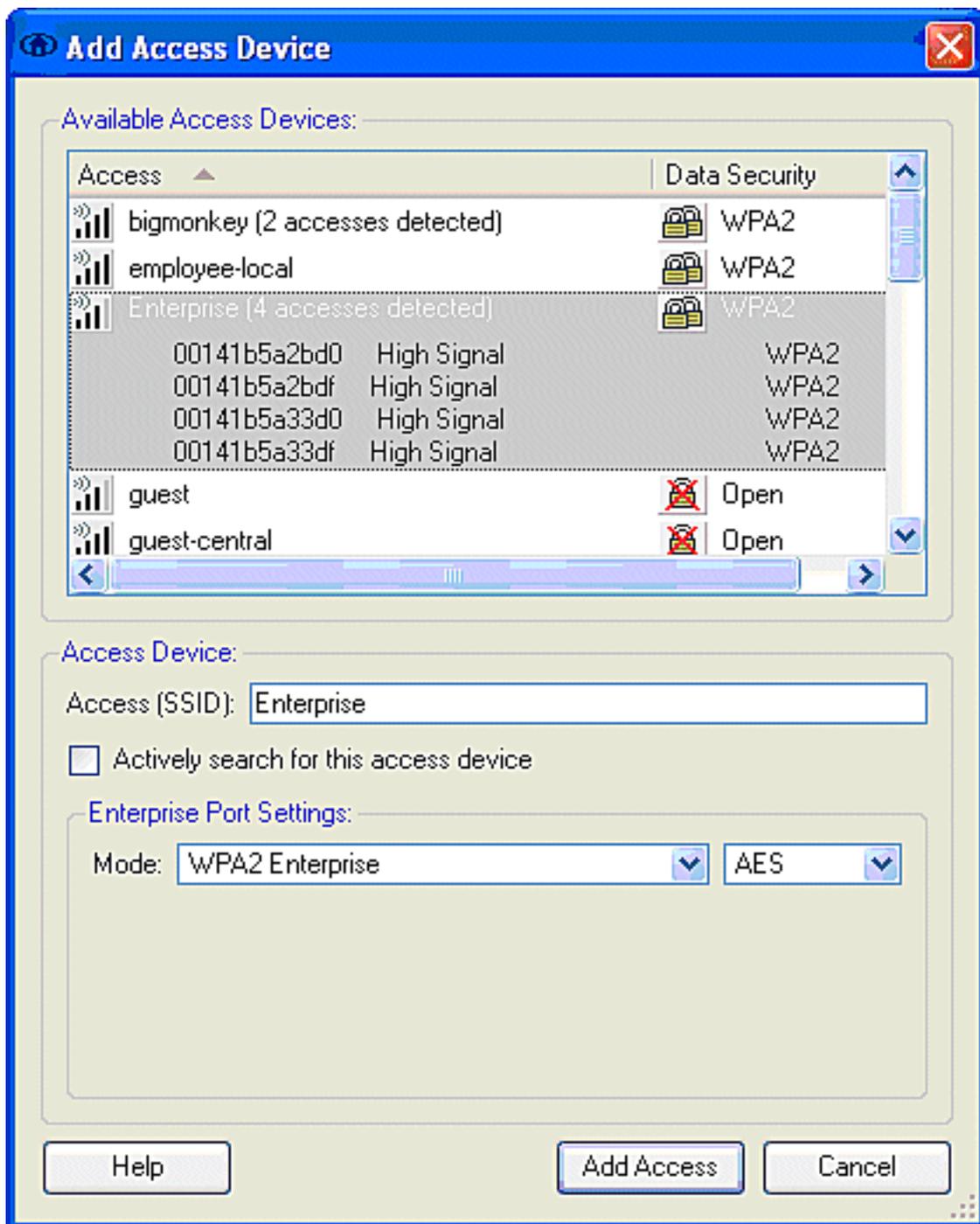
Nota:Vários tipos de segurança de WLAN e/ou SSIDs podem ser associados neste perfil de autenticação.

Para que o cliente se conecte automaticamente à rede quando estiver no intervalo de cobertura de RF, escolha **Estabelecer automaticamente a conexão do usuário**. Desmarque **Disponível para todos os usuários** se não for desejável usar esse perfil com outras contas de usuário na máquina. Se a opção **Automatically establish** não for escolhida, o usuário deverá abrir a janela do CSSC e iniciar manualmente a conexão de WLAN com o botão de opção **Connect**.

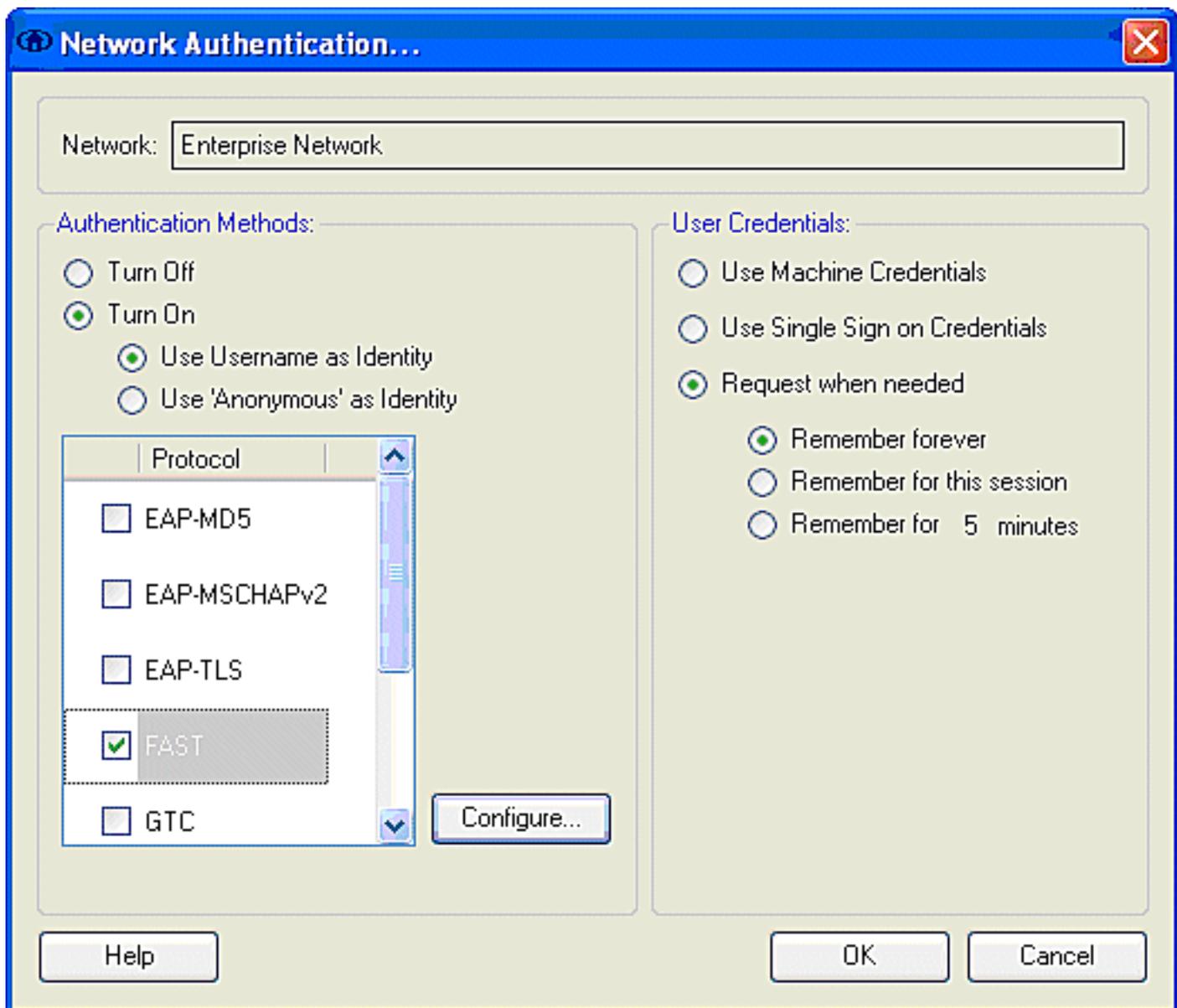
Se desejar iniciar a conexão WLAN antes do login do usuário, escolha **Antes da conta do usuário**. Isso permite uma operação de login único com credenciais de usuário salvas (senha ou certificado/Smartcard quando você usa TLS no EAP-FAST).



Observação: para a operação WPA/TKIP com o Cisco Aironet 350 Series Client Adapter, é necessário desativar a validação do handshake WPA, pois há atualmente uma incompatibilidade entre o cliente CSSC e os drivers 350 com relação à validação do hash do handshake WPA. Isso é desativado em **Client > Advanced Settings > WPA/WPA2 Handshake Validation**. A validação do handshake desabilitado ainda permite os recursos de segurança inerentes à WPA (TKIP per packet keying e Message Integrity Check), mas desabilita a autenticação inicial da chave WPA.



Em Network Configuration Summary (Resumo da configuração da rede), clique em **Modify (Modificar)** para definir as configurações de EAP/credenciais. Especifique **Turn On Authentication**, escolha **FAST** em Protocol e **'Anonymous' as Identity** (para não usar nome de usuário na solicitação EAP inicial). É possível usar o **Nome de usuário como Identificador** como a identidade EAP externa, mas muitos clientes não desejam expor as IDs de usuário na solicitação EAP não criptografada inicial. Especifique **Utilizar Credenciais de Início de Sessão Único** para utilizar credenciais de início de sessão para autenticação de rede. Clique em **Configurar** para configurar parâmetros EAP-FAST.



Nas configurações FAST, é possível especificar **Validate Server Certificate**, que permite que o cliente valide o certificado do servidor EAP-FAST (ACS) antes do estabelecimento de uma sessão EAP-FAST. Isso fornece proteção para os dispositivos clientes da conexão com um servidor EAP-FAST desconhecido ou invasor e envio inadvertido de suas credenciais de autenticação para uma fonte não confiável. Isso exige que o servidor ACS tenha um certificado instalado e que o cliente também tenha o certificado correspondente de autoridade de certificação raiz instalado. Neste exemplo, a validação do certificado do servidor não está ativada.

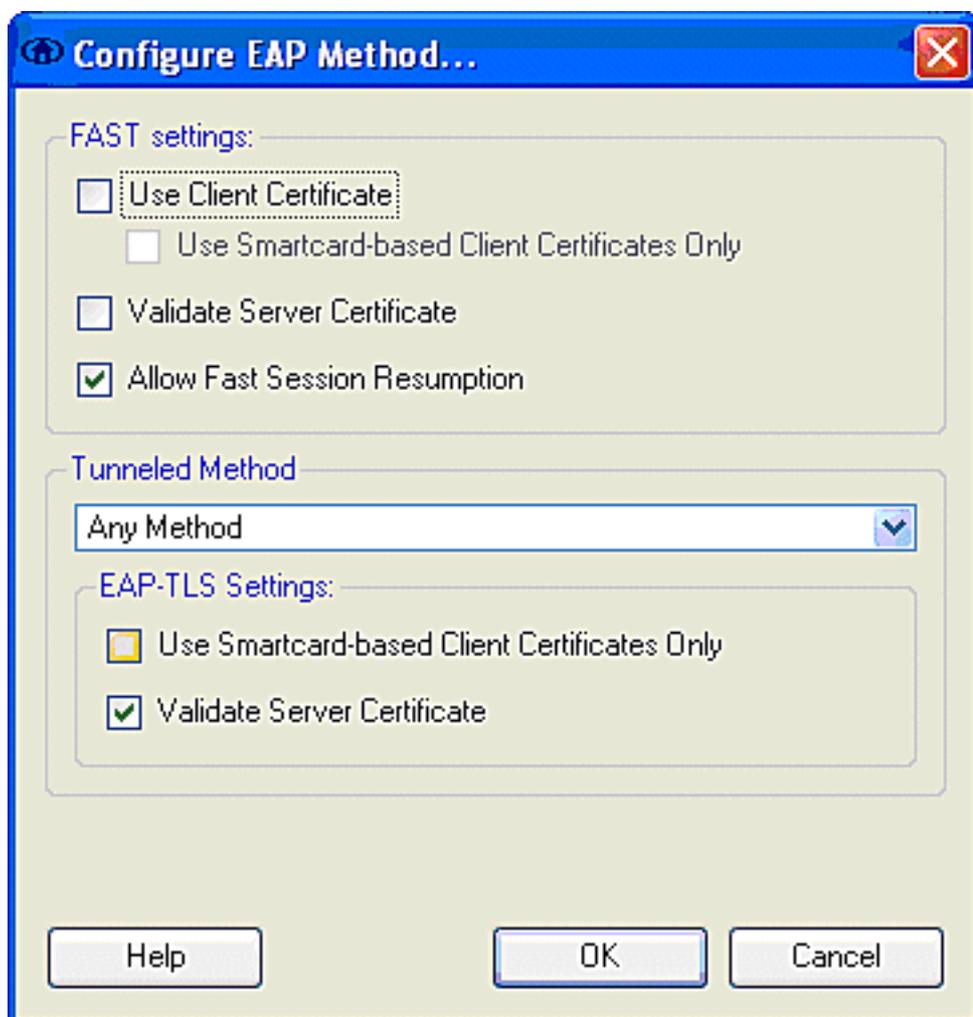
Nas configurações FAST, é possível especificar **Permitir reinicialização rápida da sessão**, o que permite a retomada de uma sessão EAP-FAST com base nas informações do túnel (sessão TLS), em vez do requisito de uma reautenticação EAP-FAST completa. Se o servidor e o cliente EAP-FAST tiverem conhecimento comum das informações da sessão TLS negociadas na troca de autenticação EAP-FAST inicial, poderá ocorrer a retomada da sessão.

Nota: Ambos o servidor e o cliente EAP-FAST devem estar configurados para que a sessão EAP-FAST continue.

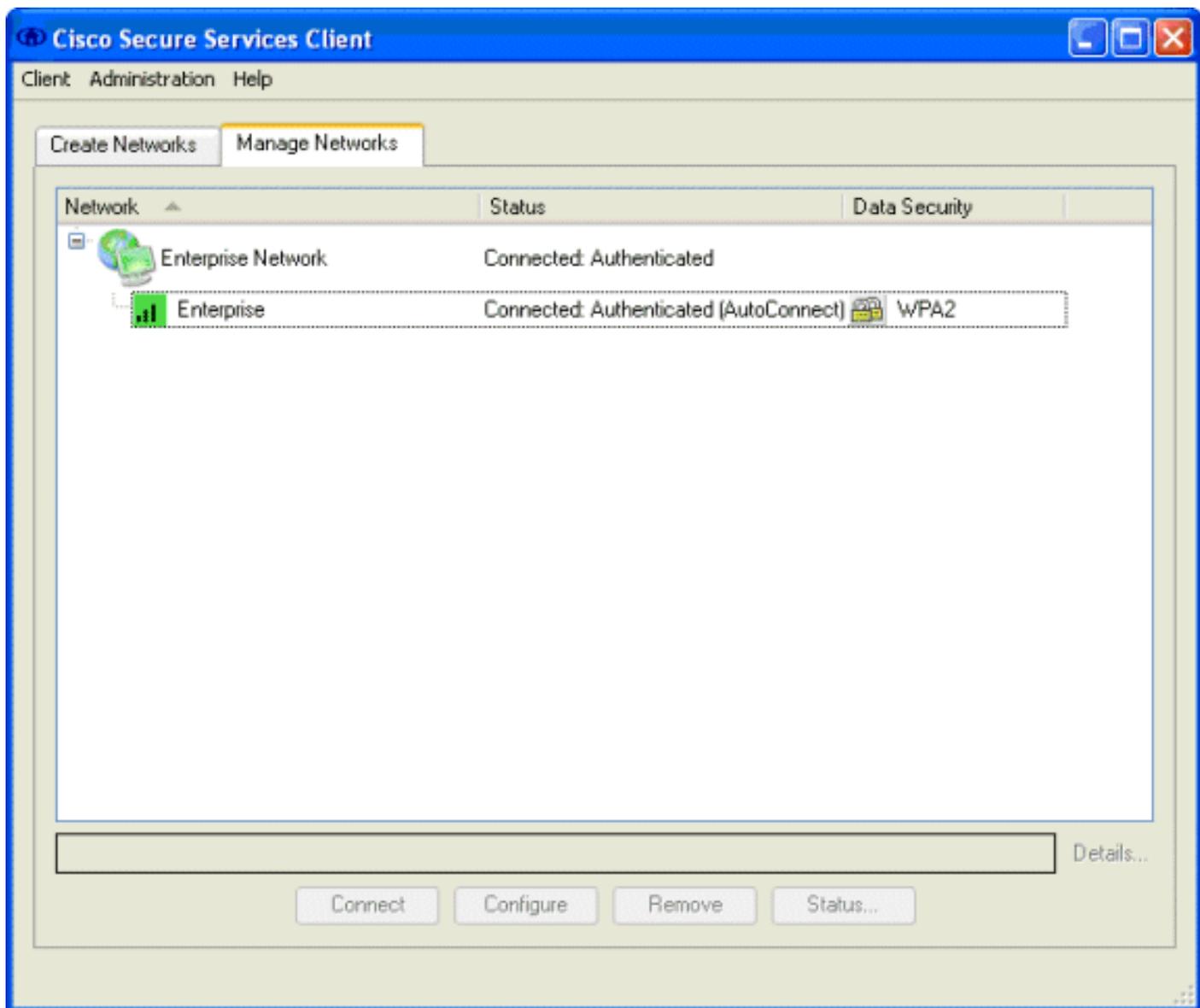
Em Tunneled Method > EAP-TLS Settings, especifique **Any Method** para permitir o EAP-MSCHAPv2 para o provisionamento automático PAC e EAP-GTC para autenticação. Se você usar um banco de dados em formato Microsoft, como o Active Directory, e se não oferecer suporte a nenhum cliente EAP-FAST v1 na rede, você também poderá especificar o uso de apenas

MSCHAPv2 como o Método em túnel.

Nota:A opção **Validate Server Certificate** está habilitada por padrão nas configurações EAP-TLS desta janela. Como o exemplo não usa EAP-TLS como método de autenticação interna, esse campo não é aplicável. Se esse campo estiver ativado, ele permitirá que o cliente valide o certificado do servidor além da validação do servidor do certificado do cliente no EAP-TLS.



Clique em **OK** para salvar as configurações EAP-FAST. Como o cliente está configurado para "estabelecer automaticamente" no perfil, ele inicia automaticamente a associação/authenticação com a rede. Na guia Gerenciar redes, os campos Rede, Status e Segurança de dados indicam o status da conexão do cliente. No exemplo, a Rede Corporativa do Perfil é exibida como em uso, e o Dispositivo de Acesso à Rede é a Empresa do SSID, que indica Connected:Authenticated e usa Autoconnect. O campo Segurança de dados indica o tipo de criptografia 802.11 empregado, que, por exemplo, é WPA2.



Depois que o cliente autentica, escolha **SSID** na guia Profile (Perfil) na guia Manage Networks (Gerenciar redes) e clique em **Status** para consultar os detalhes da conexão. A janela Detalhes da conexão fornece informações sobre o dispositivo cliente, status e estatísticas da conexão e método de autenticação. A guia Detalhes do WiFi fornece detalhes sobre o status da conexão 802.11, que inclui o RSSI, o canal 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 802.11 a/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

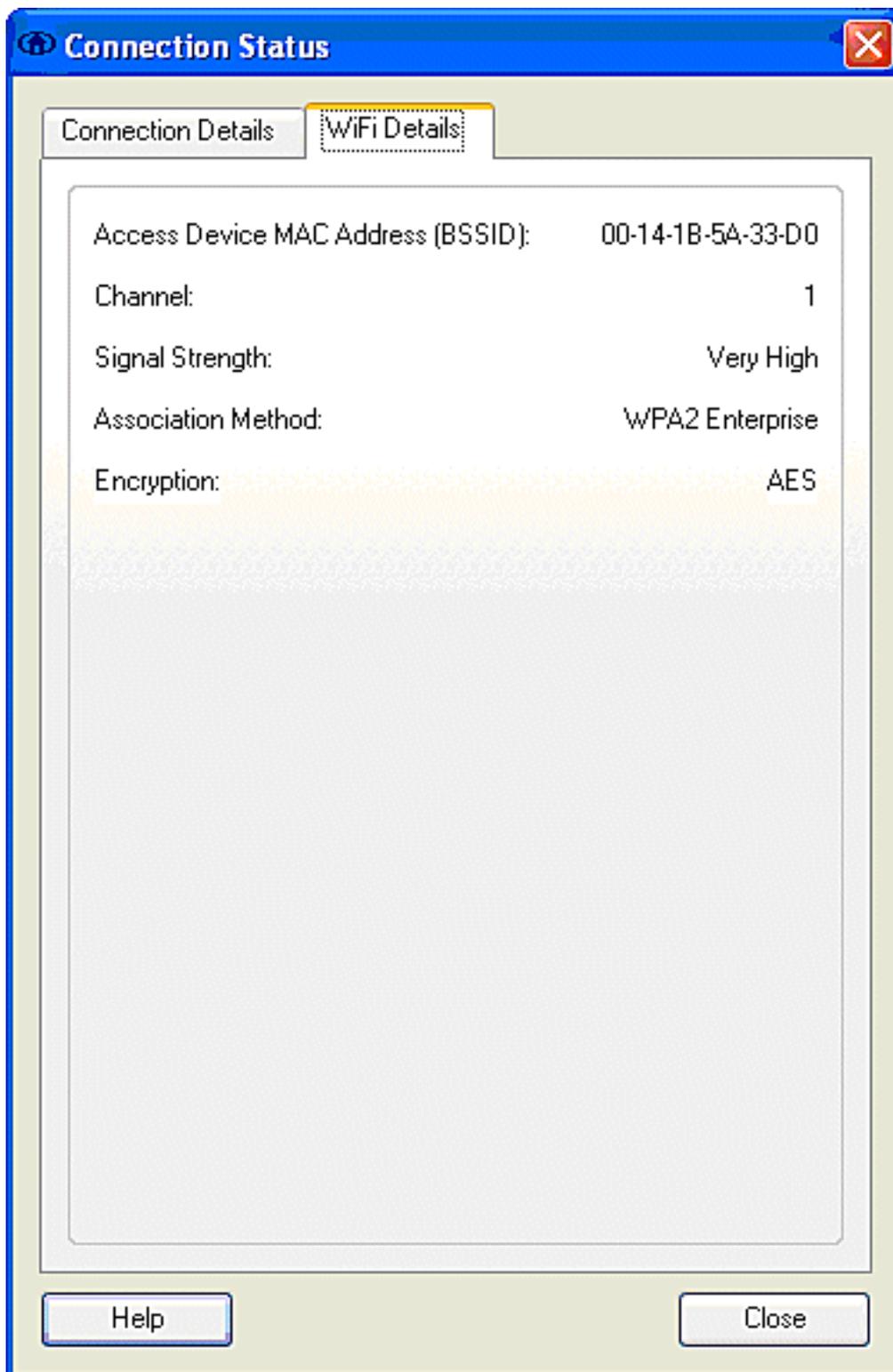
Authentication Method: FAST / GTC

Authentication Server: TME (not verified)

IP Address: 10.10.82.11

Help

Close



Como administrador do sistema, você tem direito ao utilitário de diagnóstico, o Cisco Secure Services Client System Report, que está disponível com a distribuição CSSC padrão. Este utilitário está disponível no menu Iniciar ou no diretório CSSC. Para obter dados, clique em **Coletar Dados > Copiar para Área de Transferência > Localizar Arquivo de Relatório**. Isso direciona uma janela do Microsoft File Explorer para o diretório com o arquivo de relatório zipado. No arquivo zipado, os dados mais úteis estão localizados em log (log_current).

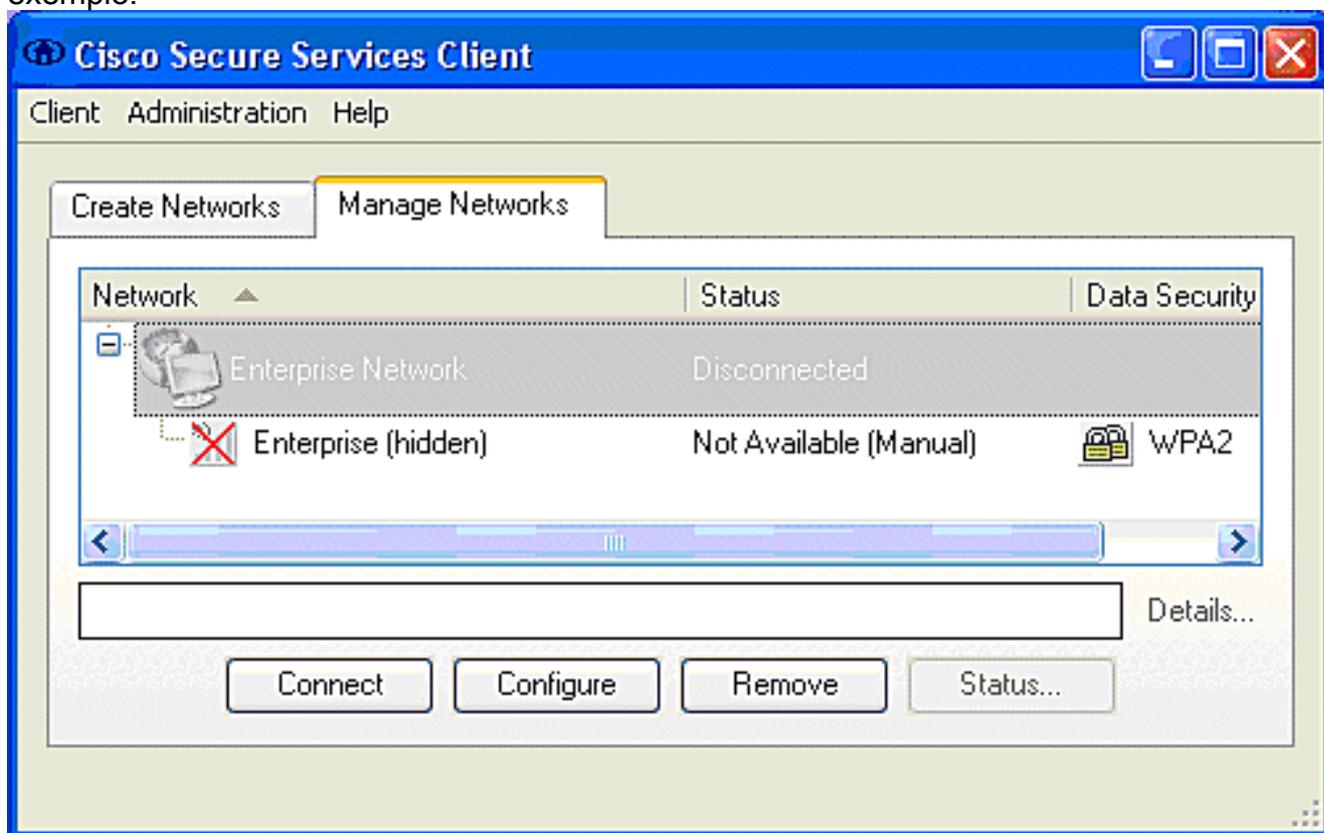
O utilitário fornece o status atual do CSSC, da interface e dos detalhes do driver, juntamente com as informações da WLAN (SSID detectado, status da associação, etc.). Isso pode ser útil, especialmente para diagnosticar problemas de conectividade entre o CSSC e o adaptador WLAN.

Verificar a operação

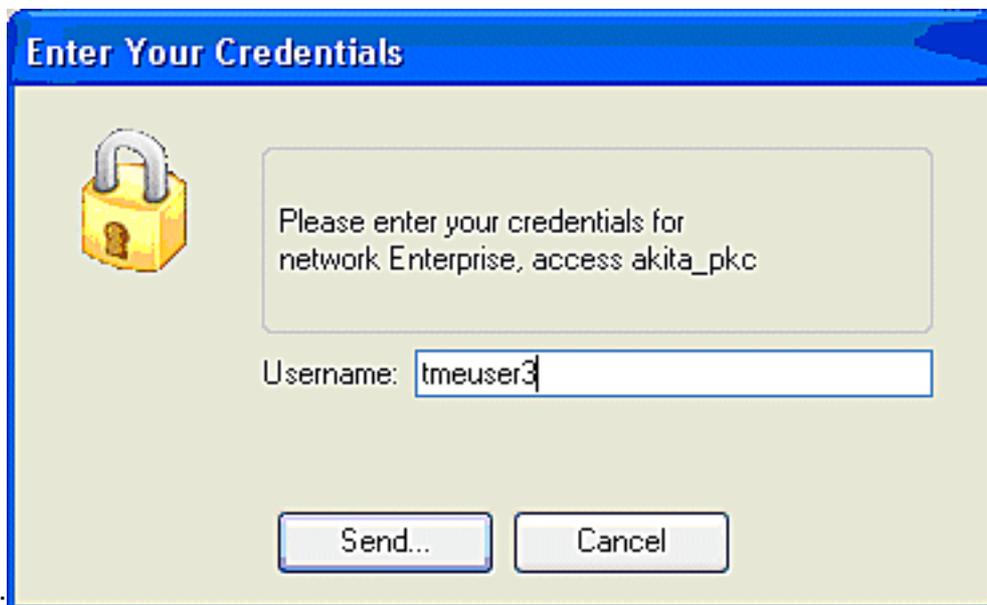
Após a configuração do servidor Cisco Secure ACS, controlador WLAN, cliente CSSC e presumivelmente a configuração correta e a população do banco de dados, a rede WLAN é configurada para autenticação EAP-FAST e comunicação segura com o cliente. Há vários pontos que podem ser monitorados para verificar o progresso/erros de uma sessão segura.

Para testar a configuração, tente associar um cliente sem fio ao controlador de WLAN com a autenticação EAP-FAST.

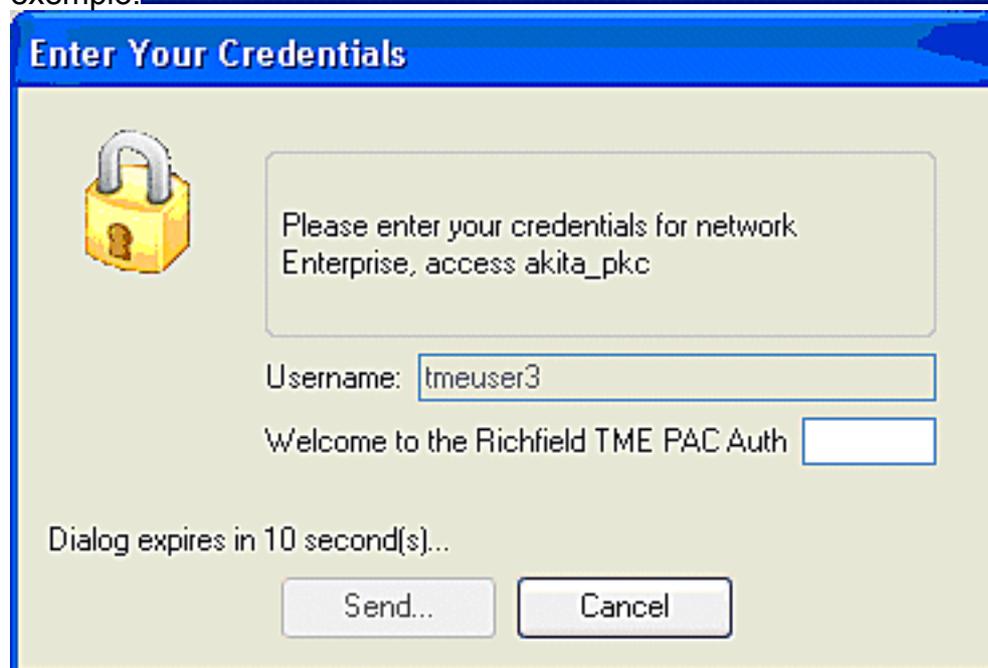
1. Se o CSSC estiver configurado para Conexão automática, o cliente tentará essa conexão automaticamente. Se não estiver configurado para a operação Conexão automática e Logon único, o usuário deverá iniciar a conexão WLAN por meio do botão de opção **Connect**. Isso inicia o processo de associação 802.11 sobre o qual ocorre a autenticação EAP. Este é um exemplo:



2. Em seguida, é solicitado ao usuário que forneça o nome de usuário e a senha para a autenticação EAP-FAST (da EAP-FAST PAC Authority ou ACS). Este é um



exemplo:



3. O cliente CSSC, por meio da WLC, passa as credenciais do usuário ao servidor RADIUS (Cisco Secure ACS) para validar as credenciais. O ACS verifica as credenciais do usuário com uma comparação dos dados e do banco de dados configurado (no exemplo de configuração, o banco de dados externo é o Windows Ative Directory) e fornece acesso ao cliente sem fio sempre que as credenciais do usuário são válidas. O relatório Autenticações aprovadas no servidor ACS mostra que o cliente passou na autenticação RADIUS/EAP. Este é um exemplo:

Reports and Activity

Reports

- TACACS+ Accounting
- TACACS+ Administration
- RADIUS Accounting
- WAP Accounting
- Passed Authentications
- Failed Authentications
- Logged-in Users
- Disabled Accounts
- ACS Backup And Restore
- Database Replication
- Administration Audit
- User Password Changes
- ACS Service Monitoring

Passed Authentications active.csv Refresh Download

Regular Expression: Start Date & Time: End Date & Time: Rows per Page: 50

Filtering is not applied.

Date	Time	Message- Type	User- Name	Group- Name	CoRr- ID	NAS- Port	NAS- IP- Address	Network Access Profile Name	Shared BAC	Downloadable ACL	System- Posture- Token	Application- Posture- Token	Reason	EA Typ
08/22/2006	16:25:37	Authn OK	test	Default Group	00-40-96-A0-36-2F	29	10.10.80.3	(Default)	43
08/22/2006	16:09:51	Authn OK	test	Default Group	00-40-96-A5-D5-F6	29	10.10.80.3	(Default)	43
08/22/2006	16:06:55	Authn OK	test	Default Group	00-40-96-A5-D5-F6	29	10.10.80.3	(Default)	43
08/22/2006	16:06:29	Authn OK	test	Default Group	00-40-96-A5-D5-F6	29	10.10.80.3	(Default)	43
08/22/2006	16:06:29	Authn OK	test	Default Group	00-40-96-A6-D5-F6	29	10.10.80.3	(Default)	43

4. Após a autenticação RADIUS/EAP bem-sucedida, o cliente sem fio (00:40:96:ab:36:2f neste exemplo) é autenticado com o controlador AP/WLAN.

Client List

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP

Wireless

Access Points

- 802.11a Radios
- 802.11b/g Radios

Mesh

Rogues

- Rogue APs
- Known Rogue APs
- Rogue Clients
- Adhoc Rogue

Clients

Search by NWE address: Search

Client MAC Addr	AP Name	WLAN	Type	Status	Auth Port	Detail	LinkTest	Disable	Remove
88:0F:D5:45:54:30	AP0504/898.9584	Unknown	882.11b	Probing	No 29	Detail	LinkTest	Disable	Remove 882.11aTSM 802.11b/gTSM
88:03:96:ab:36:2f	AP0504/898.9584	Enterprise	882.11g	Associated	Yes 29	Detail	LinkTest	Disable	Remove 882.11aTSM 802.11b/gTSM
88:03:96:ab:01:89	AP0504/898.9480	Unknown	882.11b	Probing	No 29	Detail	LinkTest	Disable	Remove 882.11aTSM 802.11b/gTSM
88:03:96:ab:06:5b	AP0504/898.9480	Enterprise	882.11g	Associated	No 29	Detail	LinkTest	Disable	Remove 882.11aTSM 802.11b/gTSM

Appendix

Além das informações de diagnóstico e status, disponíveis no Cisco Secure ACS e no Cisco WLAN Controller, há pontos adicionais que podem ser usados para diagnosticar a autenticação EAP-FAST. Embora a maioria dos problemas de autenticação possa ser diagnosticada sem o uso de um sniffer de WLAN ou a depuração de trocas EAP no controlador de WLAN, este material de referência é incluído para ajudar a solucionar problemas.

Captura de farejador para EAP-FAST Exchange

Esta captura de farejador 802.11 mostra a troca de 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 Req	FC=...R...,SN=2867,FM= 0,Status...
00:14:1B:5A:33:D0	*	11	70%	24.0	101	00.036453	802.11 Assoc Req	FC=...R...,SN=2867,FM= 0,Status...
00:14:1B:5A:33:D0		11	71%	54.0	90	00.036494	802.1x	FC=.F...,SN=2868,FM= 0
Aironet:A0:36:2F		11	54%	1.0	82	00.123205	EAP Response	FC=T...,SN= 3,FM= 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,FM= 0
Aironet:A0:36:2F		11	55%	1.0	82	00.173920	EAP Response	FC=T...,SN= 4,FM= 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,FM= 0
Aironet:A0:36:2F		11	58%	1.0	282	00.200632	EAP Response	FC=T...,SN= 5,FM= 0
Aironet:A0:36:2F		11	58%	1.0	282	00.203340	EAP Response	FC=T...,SN= 5,FM= 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,FM= 0
Aironet:A0:36:2F		11	55%	1.0	105	00.216295	EAP Response	FC=T...,SN= 6,FM= 0
Aironet:A0:36:2F		11	57%	1.0	105	00.217444	EAP Response	FC=T...,SN= 6,FM= 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,FM= 0
Aironet:A0:36:2F		11	55%	1.0	152	00.254189	EAP Response	FC=T...,SN= 7,FM= 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,FM= 0
Aironet:A0:36:2F		11	55%	1.0	232	00.318087	EAP Response	FC=T...,SN= 8,FM= 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,FM= 0
00:14:1B:5A:33:D0		11	65%	54.0	44	00.326882	802.1x	FC=.F.R...,SN=2877,FM= 0
00:14:1B:5A:33:D0		11	67%	48.0	44	00.326922	802.1x	FC=.F.R...,SN=2877,FM= 0
00:14:1B:5A:33:D0		11	67%	54.0	157	00.326964	802.1x	FC=.F...,SN=2878,FM= 0
Aironet:A0:36:2F		11	57%	1.0	157	00.333742	EAP01-Key	FC=T...,SN= 9,FM= 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,FM= 0
00:14:1B:5A:33:D0		11	67%	54.0	207	00.341130	802.1x	FC=.F.R...,SN=2879,FM= 0
Aironet:A0:36:2F		11	57%	1.0	135	00.342542	EAP01-Key	FC=T...,SN= 10,FM= 0

Este pacote mostra a resposta EAP-FAST EAP inicial.

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

Packet: 12

Frame Control Flags: 00000001 [11]

- 0... .. Non-strict order
- .0... .. WEP Not Enabled
- ..0... .. No More Data
-0... .. Power Management - active mode
-0... .. This is not a Re-Transmission
-0... .. Last or Unfragmented Frame
-0... .. Not an Exit from the Distribution System
-1... .. To the Distribution System

Duration: 314 Microseconds [2-3]

BSSID: 00:14:1B:5A:33:D0 [4-9]

Source: 00:40:96:A0:36:2F Aironet:A0:36:2F [10-15]

Destination: 00:14:1B:5A:33:D0 [16-21]

Seq. Number: 3 [22-23 Hash 0x7770]

Frag. Number: 0 [22 Hash 0x07]

IEEE 802.2 Logical Link Control (LLC) Header

- Dest. SRP: 0xAA SNAP [24]
- Source SRP: 0xAA SNAP [25]
- Command: 0x03 Unnumbered Information [26]
- Vendor ID: 0x000000 [27-29]
- Protocol Type: 0x888E 802.1x Authentication [30-31]

IEEE 802.1x Authentication

- Protocol Version: 1 [32]
- Packet Type: 0 EAP - Packet [33]
- Body Length: 14 [34-35]

Extensible Authentication Protocol

- Code: 2 Response [36]
- Identifier: 1 [37]
- Length: 14 [38-39]
- Type: 1 Identity [40]
- Type-Data: anonymous [41-49]

Depuração no controlador de WLAN

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

- debug aaa events enable
- debug aaa detail enable

- debug dot1x events enable
- debug dot1x states enable

Este é um exemplo do início de uma transação de autenticação entre o cliente CSSC e o ACS conforme monitorado no controlador WLAN com as depurações:

```
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Processing RSN IE type 48,
length 20 for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Received RSN IE with
0 PMKIDs from mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f dot1x -
moving mobile 00:40:96:a0:36:2f into Connecting state
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Sending EAP-
Request/Identity to mobile 00:40:96:a0:36:2f (EAP Id 1)
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Received Identity Response
(count=1) from mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f EAP State update from
Connecting to Authenticating for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f dot1x - moving mobile
00:40:96:a0:36:2f into Authenticating state
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Entering Backend Auth
Response state for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: AuthenticationRequest: 0x138dd764
Thu Aug 24 18:20:54 2006: Callback.....0x10372764
Thu Aug 24 18:20:54 2006: protocolType...0x00040001
Thu Aug 24 18:20:54 2006: proxyState.....00:40:96:A0:36:2F-11:00
Thu Aug 24 18:20:54 2006: Packet contains 15 AVPs (not shown)
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Successful transmission of
Authentication Packet (id 84) to 10.1.1.12:1812, proxy state0
Thu Aug 24 18:20:54 2006: ****Enter processIncomingMessages: response code=11
Thu Aug 24 18:20:54 2006: ****Enter processRadiusResponse: response code=11
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Access-Challenge received from
RADIUS server 10.1.1.12 for mobile 00:40:96:a0:36:2f rec7
Thu Aug 24 18:20:54 2006: AuthorizationResponse: 0x11c8a394
Thu Aug 24 18:20:54 2006: structureSize..147
Thu Aug 24 18:20:54 2006: resultCode.....255
Thu Aug 24 18:20:54 2006: protocolUsed...0x00000001
Thu Aug 24 18:20:54 2006: proxyState.....00:40:96:A0:36:2F-11:00
Thu Aug 24 18:20:54 2006: Packet contains 4 AVPs (not shown)
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Processing Access-Challenge
for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Entering Backend Auth Req state
(id=249) for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f WARNING:
updated EAP-Identifer 1 ==> 249 for STA 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Sending EAP Request from
AAA to mobile 00:40:96:a0:36:2f (EAP Id 249)
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Received EAP Response from
mobile 00:40:96:a0:36:2f (EAP Id 249, EAP Type 3)
```

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

```
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Processing Access-
Accept for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Applying new AAA
override for station 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Override values for station
```

00:40:96:a0:36:2f source: 4, valid bits: 0x0
qosLevel: -1, dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout:
-1 dataAvgC: -1, rTAVgC: -1, dataBurstC: -1, r1'
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Unable to apply override
policy for station 00:40:96:a0:36:2f - VapAllowRadiusOverride E
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Creating a new PMK Cache Entry
for station 00:40:96:a0:36:2f (RSN 2)
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Adding BSSID
00:14:1b:5a:33:d0 to PMKID cache for station 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: New PMKID: (16)
Thu Aug 24 18:20:54 2006: [0000] a6 c0 02 95 66 e8 ed 9b 1c 65 9b
72 1f 3f 5f 5b
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Sending EAP-Success
to mobile 00:40:96:a0:36:2f (EAP Id 0)
Thu Aug 24 18:20:54 2006: Including PMKID in M1 (16)
Thu Aug 24 18:20:54 2006:
[0000] a6 c0 02 95 66 e8 ed 9b 1c 65 9b 72 1f 3f 5f 5b
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Sending EAPOL-Key Message to
mobile 00:40:96:a0:36:2f state INITPMK (message 1), repl0
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Entering Backend
Auth Success state (id=0) for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Received Auth Success
while in Authenticating state for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f dot1x -
moving mobile 00:40:96:a0:36:2f into Authenticated state
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Received EAPOL-
Key from mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Invalid EAPOL version
(1) in EAPOL-key message from mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Received EAPOL-key
in PKT_START state (message 2) from mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Stopping retransmission
timer for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Sending EAPOL-Key Message
to mobile 00:40:96:a0:36:2f state PTKINITNEGOTIATING (messal
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Received
EAPOL-Key from mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Invalid EAPOL version (1)
in EAPOL-key message from mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Received EAPOL-key in
PTKINITNEGOTIATING state (message 4) from mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: AccountingMessage
Accounting Interim: 0x138dd764
Thu Aug 24 18:20:54 2006: Packet contains 20 AVPs:
Thu Aug 24 18:20:54 2006:
AVP[01] User-Name.....enterprise (10 bytes)
Thu Aug 24 18:20:54 2006: AVP[02]
Nas-Port.....0x0000001d (29) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[03]
Nas-Ip-Address.....0x0a0a5003 (168448003) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[04]
Class.....CACs:0/28b5/a0a5003/29 (22 bytes)
Thu Aug 24 18:20:54 2006: AVP[05]
NAS-Identifier.....ws-3750 (7 bytes)
Thu Aug 24 18:20:54 2006: AVP[06]
Airespace / WLAN-Identifier.....0x00000001 (1) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[07]
Acct-Session-Id.....44ede3b0/00:40:
96:a0:36:2f/14 (29 bytes)
Thu Aug 24 18:20:54 2006: AVP[08]
Acct-Authentic.....0x00000001 (1) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[09]
Tunnel-Type.....0x0000000d (13) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[10]

```
Tunnel-Medium-Type.....0x00000006 (6) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[11]
Tunnel-Group-Id.....0x3832 (14386) (2 bytes)
Thu Aug 24 18:20:54 2006: AVP[12]
Acct-Status-Type.....0x00000003 (3) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[13]
Acct-Input-Octets.....0x000b99a6 (760230) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[14]
Acct-Output-Octets.....0x00043a27 (277031) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[15]
Acct-Input-Packets.....0x0000444b (17483) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[16]
Acct-Output-Packets.....0x0000099b (2459) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[17]
Acct-Session-Time.....0x00000a57 (2647) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[18]
Acct-Delay-Time.....0x00000000 (0) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[19]
Calling-Station-Id.....10.10.82.11 (11 bytes)
Thu Aug 24 18:20:54 2006: AVP[20]
Called-Station-Id.....10.10.80.3 (10 bytes)
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f
Stopping retransmission timer for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:57 2006: User admin authenticated
```

[Informações Relacionadas](#)

- [Guia de instalação do Cisco Secure ACS para Windows Server](#)
- [Guia de configuração do Cisco Secure ACS 4.1](#)
- [Restringir o acesso à WLAN com base no SSID com WLC e o exemplo de configuração do Cisco Secure ACS](#)
- [EAP-TLS em Redes Wireless Unificadas com o ACS 4.0 e o Windows 2003](#)
- ["Atribuição da VLAN dinâmica com um exemplo de configuração do servidor RADIUS e do controlador LAN sem fio](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)