Restringir o acesso à WLAN com base no SSID com WLC e o exemplo de configuração do Cisco Secure ACS

Contents

[Introduction](#)
[Prerequisites](#)
[Requirements](#)
[Componentes Utilizados](#)
[Conventions](#)
[Informações de Apoio](#)
[Instalação de rede](#)
[Configurar](#)
[Configurar o WLC](#)
[Configurar o Cisco Secure ACS](#)
[Configurar o cliente sem fio e verificar](#)
[Troubleshoot](#)
[Comandos para Troubleshooting](#)
[Informações Relacionadas](#)

Introduction

Este documento fornece um exemplo de configuração para restringir o acesso por usuário a uma WLAN com base no Service Set Identifier (SSID).

Prerequisites

Requirements

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

- Conhecimento de como configurar o Wireless LAN Controller (WLC) e o Lightweight Access Point (LAP) para operação básica
- Conhecimento básico sobre como configurar o Cisco Secure Access Control Server (ACS)
- Conhecimento de Lightweight Access Point Protocol (LWAPP) e métodos de segurança sem fio

Componentes Utilizados

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

- Cisco 2000 Series WLC que executa o firmware 4.0
- LAP Cisco 1000 Series
- Cisco Secure ACS Server versão 3.2
- Adaptador de cliente sem fio Cisco 802.11a/b/g que executa o firmware 2.6
- Cisco Aironet Desktop Utility (ADU) versão 2.6

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

Conventions

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

Informações de Apoio

Com o uso do acesso à WLAN baseado em SSID, os usuários podem ser autenticados com base no SSID que usam para se conectar à WLAN. O servidor Cisco Secure ACS é usado para autenticar os usuários. A autenticação acontece em duas etapas no Cisco Secure ACS:

1. autenticação EAP
2. Autenticação de SSID com base em Network Access Restrictions (NARs) no Cisco Secure ACS

Se a autenticação baseada em EAP e SSID for bem-sucedida, o usuário poderá acessar a WLAN ou então o usuário será desassociado.

O Cisco Secure ACS usa o recurso NARs para restringir o acesso do usuário com base no SSID. Um NAR é uma definição, que você faz no Cisco Secure ACS, de condições adicionais que devem ser atendidas antes que um usuário possa acessar a rede. O Cisco Secure ACS aplica essas condições usando informações de atributos enviados por seus clientes AAA. Embora haja várias maneiras de configurar NARs, todos eles se baseiam em informações de atributo correspondentes enviadas pelo cliente AAA. Portanto, você deve entender o formato e o conteúdo dos atributos que seus clientes AAA enviam se quiser empregar NARs eficazes.

Quando você configura um NAR, você pode escolher se o filtro funciona de forma positiva ou negativa. Ou seja, no NAR você especifica se permite ou nega o acesso à rede, com base em uma comparação de informações enviadas de clientes AAA às informações armazenadas no NAR. No entanto, se um NAR não encontrar informações suficientes para operar, o padrão será o acesso negado.

Você pode definir um NAR para um usuário específico ou grupo de usuários e aplicá-lo a ele. Consulte o white paper Restrições de acesso à rede para obter mais informações.

O Cisco Secure ACS suporta dois tipos de filtros NAR:

1. **Filtros baseados em IP** — os filtros NAR baseados em IP limitam o acesso com base nos endereços IP do cliente do usuário final e do cliente AAA. Consulte Sobre filtros NAR baseados em IP para obter mais informações sobre esse tipo de filtro NAR.

2. **Filtros não baseados em IP** — Os filtros NAR não baseados em IP limitam o acesso com base na simples comparação de cadeia de caracteres de um valor enviado do cliente AAA. O valor pode ser o número da ID da linha chamadora (CLI), o número do serviço de identificação do número discado (DNIS), o endereço MAC ou outro valor originado do cliente. Para que esse tipo de NAR funcione, o valor na descrição do NAR deve corresponder exatamente ao que é enviado do cliente, incluindo qualquer formato usado. Por exemplo, (217) 555-4534 não corresponde a 217-555-4534. Consulte Sobre os filtros NAR não baseados em IP para obter mais informações sobre esse tipo de filtro NAR.

Este documento usa os filtros não baseados em IP para fazer autenticação baseada em SSID. Um filtro NAR não baseado em IP (ou seja, um filtro NAR baseado em DNIS/CLI) é uma lista de locais de chamada/ponto de acesso permitidos ou negados que você pode usar na restrição de um cliente AAA quando você não tem uma conexão baseada em IP estabelecida. O recurso NAR não baseado em IP geralmente usa o número CLI e o número DNIS. Há exceções no uso dos campos DNIS/CLI. Você pode inserir o nome SSID no campo DNIS e fazer a autenticação baseada em SSID. Isso ocorre porque a WLC envia o atributo DNIS, o nome SSID, para o servidor RADIUS. Assim, se você criar o NAR do DNIS no usuário ou no grupo, poderá criar restrições de SSID por usuário.

Se você usa RADIUS, os campos NAR listados aqui usam estes valores:

- **AAA client** —O NAS-IP-address (atributo 4) ou, se NAS-IP-address não existir, NAS-identifier (atributo 32 RADIUS) é usado.
- **Porta** —A porta NAS (atributo 5) ou, se a porta NAS não existir, NAS-port-ID (atributo 87) é usada.
- **CLI** —A ID da estação chamadora (atributo 31) é usada.
- **DNIS** — O ID da estação chamada (atributo 30) é usado.

Consulte Restrições de Acesso à Rede para obter mais informações sobre o uso do NAR.

Como a WLC envia o atributo DNIS e o nome SSID, você pode criar restrições de SSID por usuário. No caso da WLC, os campos NAR têm estes valores:

- **Cliente AAA** — endereço IP WLC
- **porta**—*
- **CLI** —*
- **DNIS** —*ssidname

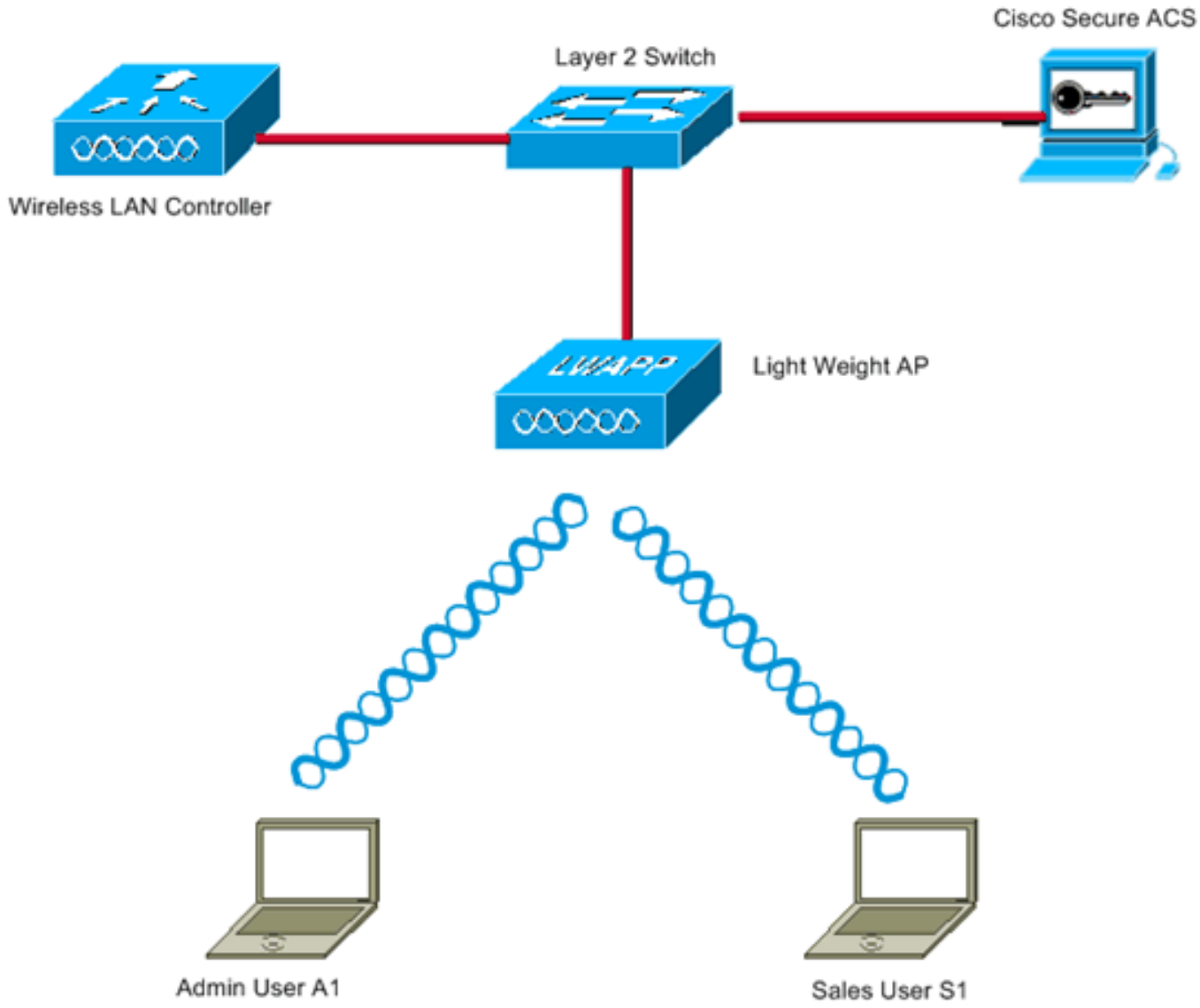
O restante deste documento fornece um exemplo de configuração sobre como fazer isso.

Instalação de rede

Neste exemplo de configuração, a WLC está registrada no LAP. Duas WLANs são usadas. Uma WLAN é para os usuários do departamento administrativo e a outra WLAN é para os usuários do departamento de vendas. O cliente sem fio A1 (usuário Admin) e S1 (usuário Sales) se conectam à rede sem fio. Você precisa configurar o WLC e o servidor RADIUS de forma que o usuário Admin A1 possa acessar somente o **Admin** da WLAN e tenha acesso restrito às **Vendas** da WLAN e o usuário de Vendas S1 possa acessar as **Vendas** da WLAN e tenha acesso restrito ao **Admin** da **WLAN**. Todos os usuários usam a autenticação LEAP como um método de autenticação de Camada 2.

Observação: este documento pressupõe que a WLC está registrada no controlador. Se você for

novo na WLC e não souber como configurar a WLC para a operação básica, consulte Lightweight AP (LAP) Registration to a Wireless LAN Controller (WLC).



WLC Management Interface IP address : 172.16.1.30/16
WLC AP-Manager Interface IP address: 172.16.1.31/16
Cisco Secure ACS server IP address: 172.16.1.60/16

SSID for the Admin department users : Admin
SSID for Sales department users: Sales

Configurar

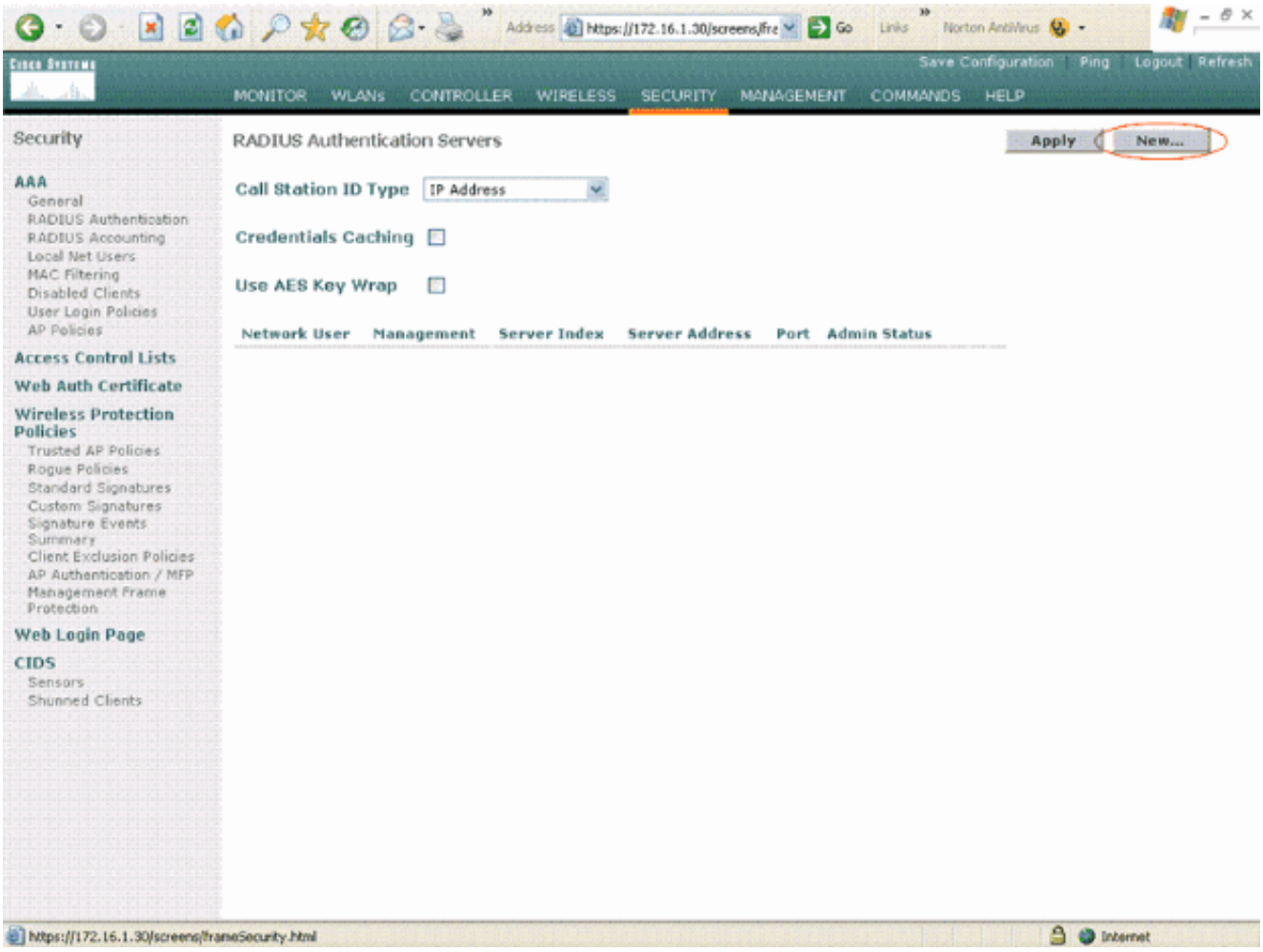
Para configurar os dispositivos para esta configuração, você precisa:

1. Configure a WLC para as duas WLANs e o servidor RADIUS.
2. Configure o Cisco Secure ACS.
3. Configure os clientes sem fio e verifique.

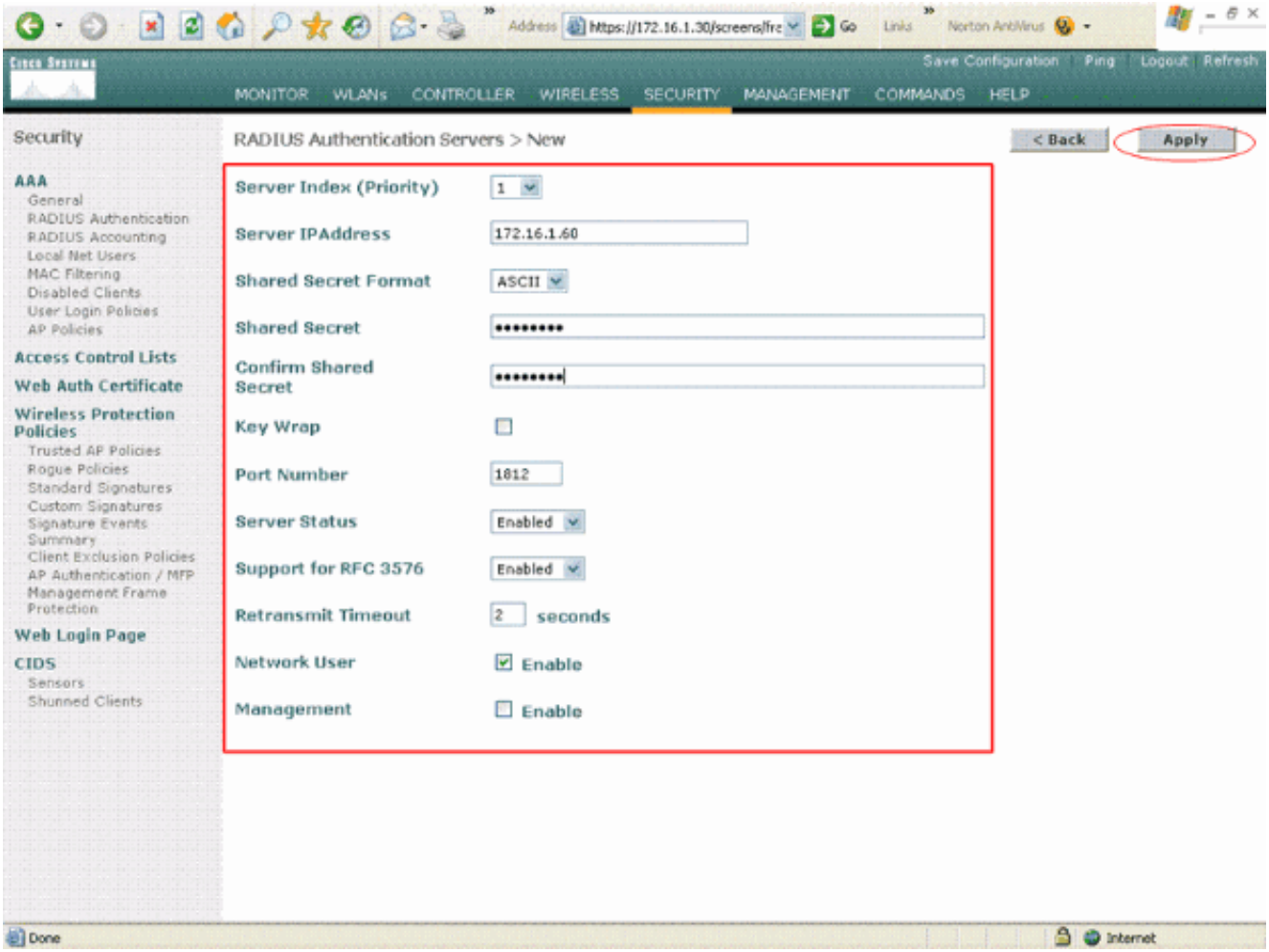
Configurar o WLC

Conclua estes passos para configurar a WLC para esta configuração:

1. A WLC precisa ser configurada para encaminhar as credenciais do usuário a um servidor RADIUS externo. O servidor RADIUS externo (Cisco Secure ACS, neste caso) valida as credenciais do usuário e fornece acesso aos clientes sem fio. Conclua estes passos:Escolha **Security > RADIUS Authentication** na GUI do controlador para exibir a página RADIUS Authentication
   Servers.

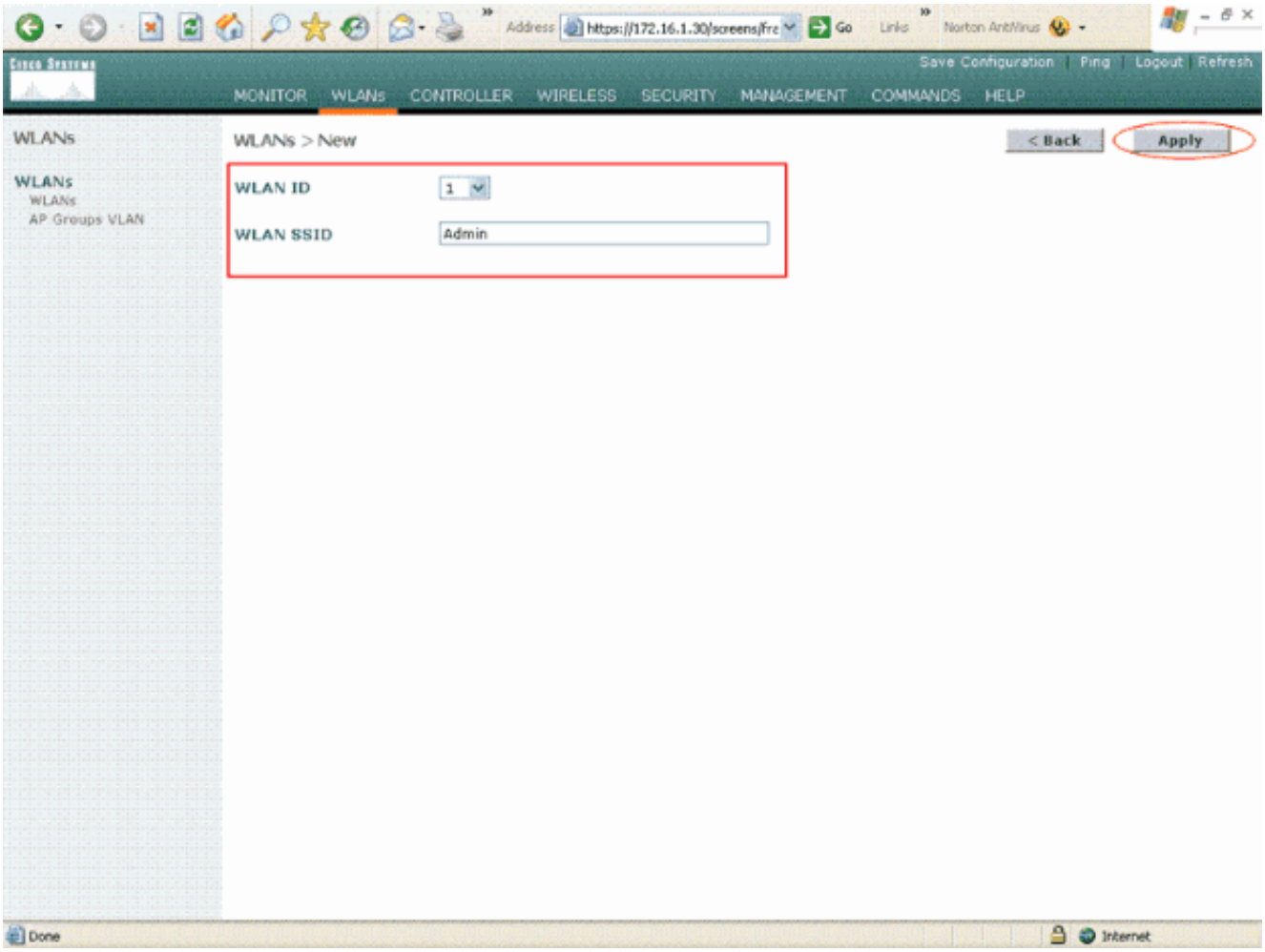


   Clique em **New** para definir os parâmetros do servidor RADIUS.Esses parâmetros incluem o endereço IP do servidor RADIUS, o segredo compartilhado, o número da porta e o status do servidor. As caixas de seleção Network User and Management determinam se a autenticação baseada em RADIUS se aplica a usuários de gerenciamento e rede. Este exemplo usa o Cisco Secure ACS como o servidor RADIUS com endereço IP 172.16.1.60.

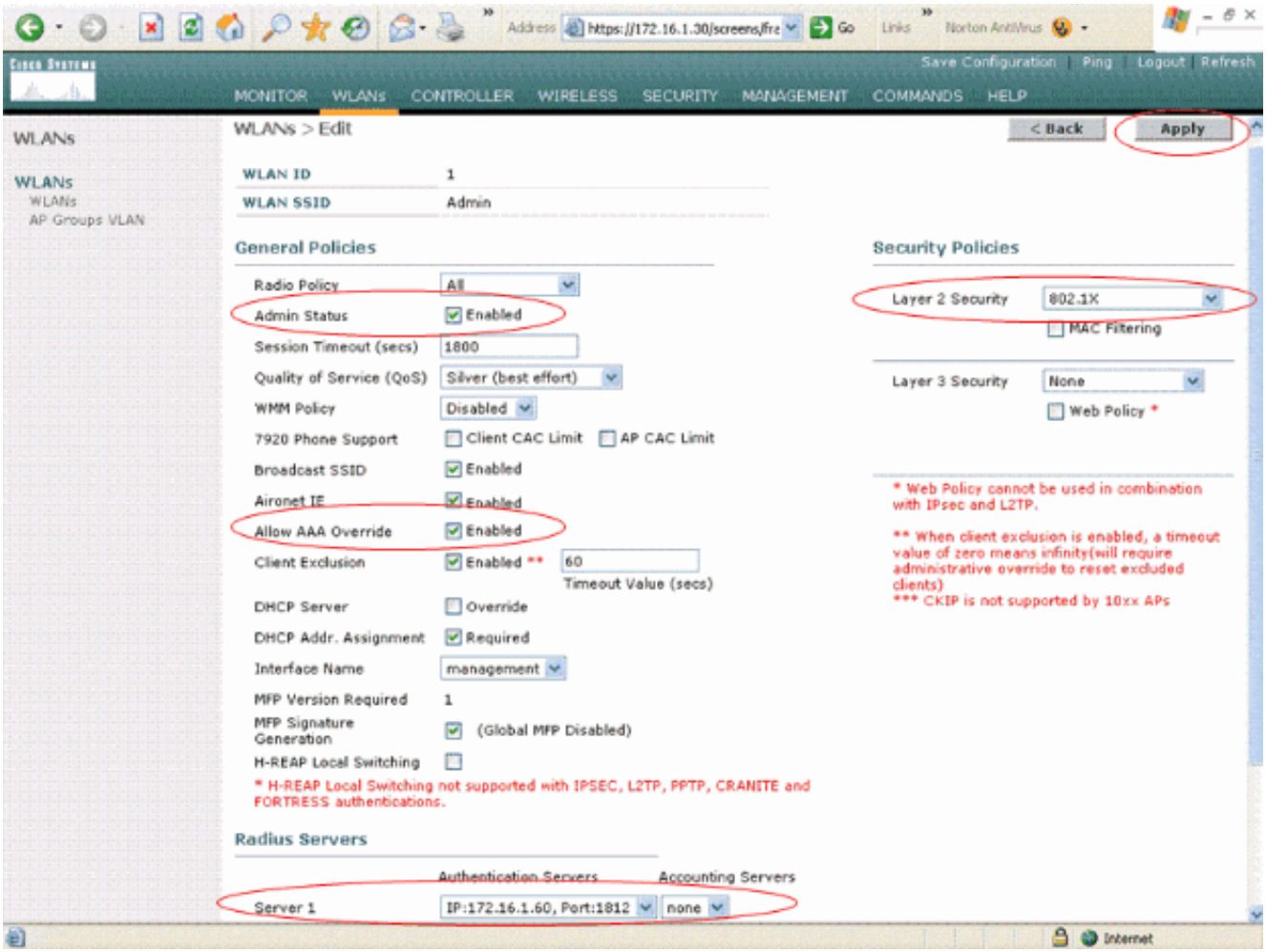


Clique em Apply.

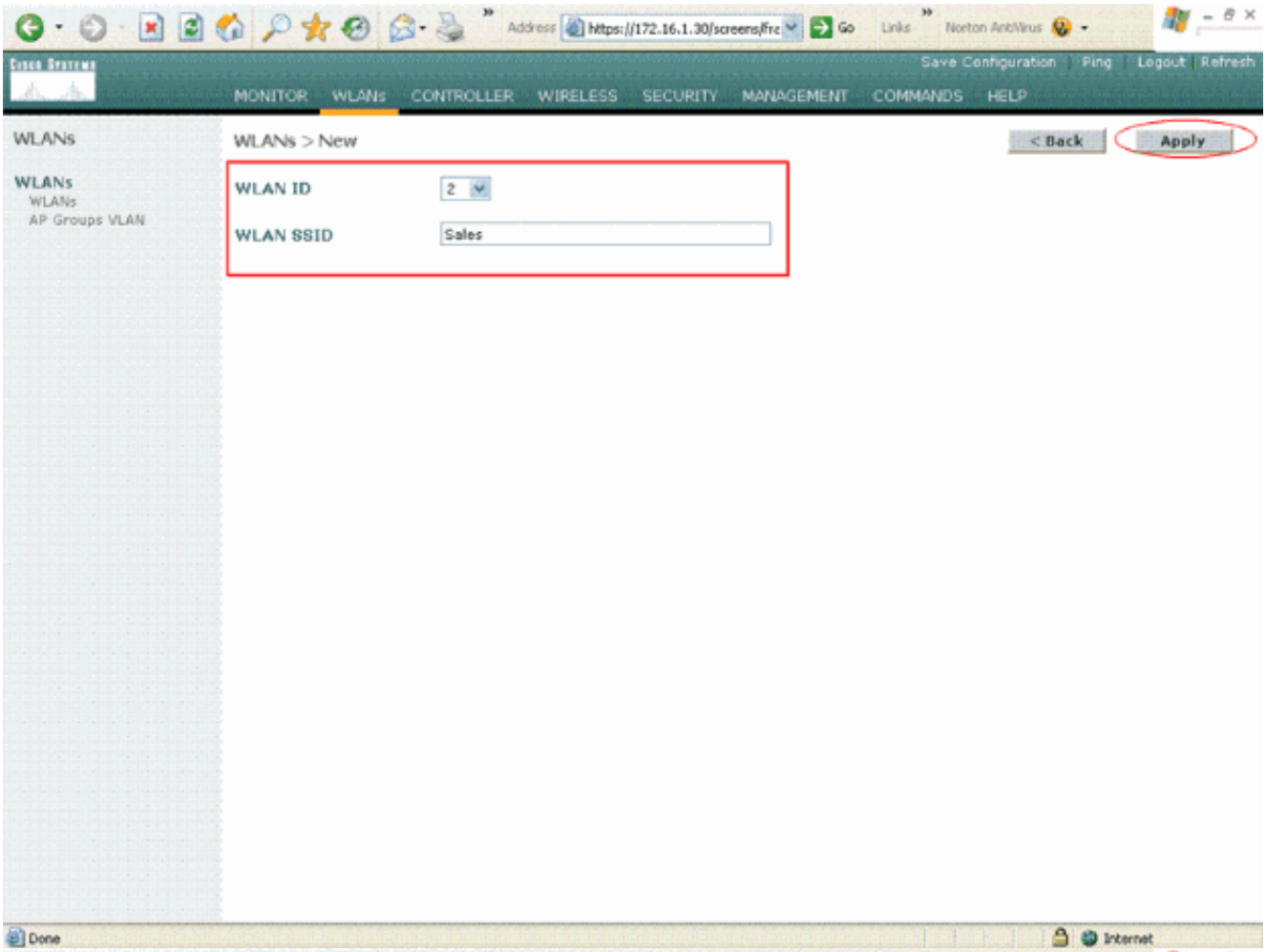
2. Configure uma WLAN para o departamento Admin com SSID **Admin** e outra WLAN para o departamento de vendas com SSID **Sales**. Conclua estes passos para fazer isso:Clique em **WLANs na GUI do controlador para criar uma WLAN.** A janela WLANs será exibida. Essa janela lista as WLANs configuradas no controlador.Clique em **Novo para configurar uma nova WLAN.**Este exemplo cria uma WLAN chamada **Admin** para o departamento Admin e a ID da WLAN é **1**. Clique em
Apply.

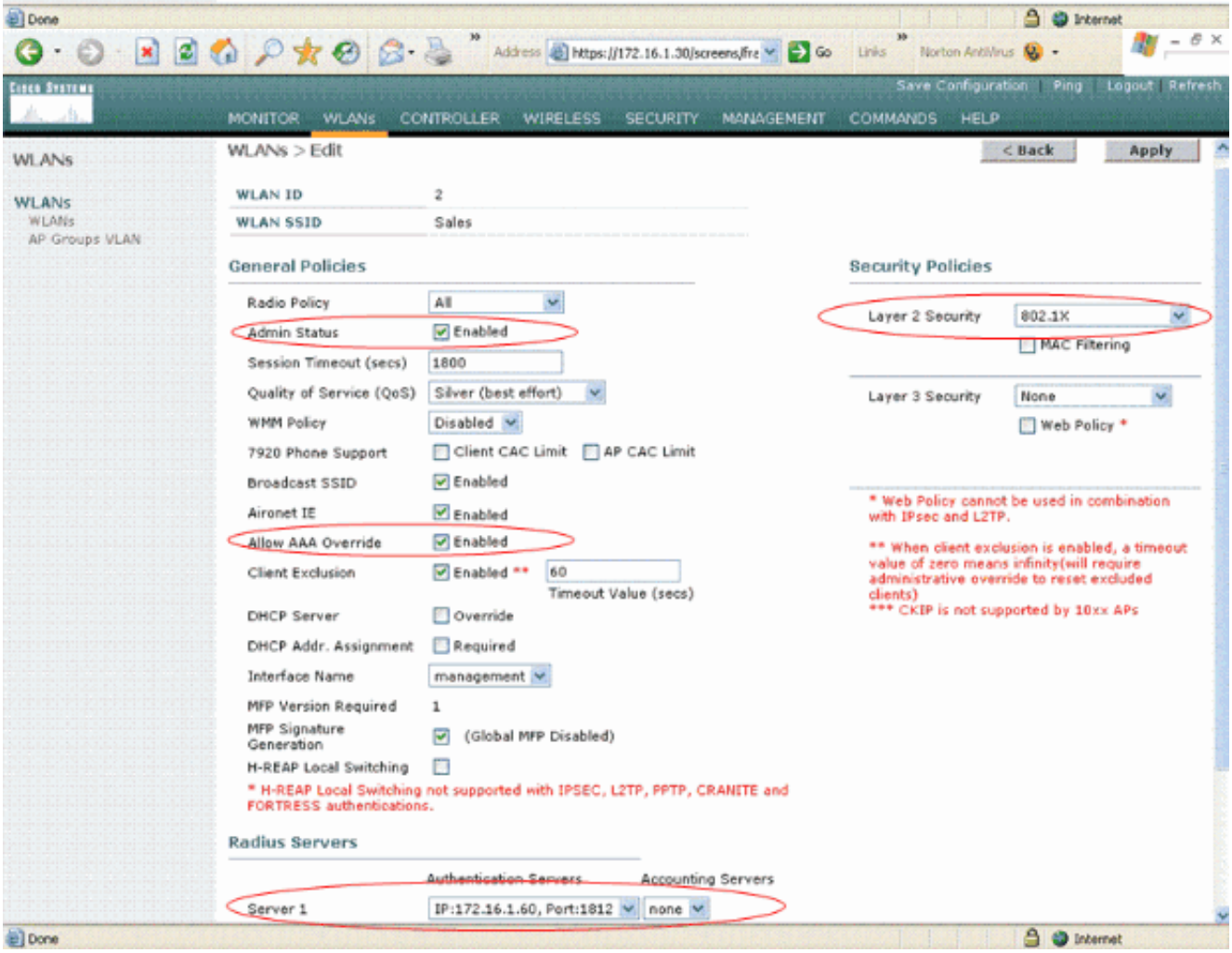


Na janela WLAN > Editar, defina os parâmetros específicos para a WLAN:No menu suspenso Layer 2 Security, selecione **802.1x**. Por padrão, a opção Layer 2 Security é 802.1x. Isso habilita a autenticação 802.1x/EAP para a WLAN.Em políticas gerais, marque a caixa **de substituição AAA**. Quando a Substituição AAA está habilitada e um cliente tem parâmetros conflitantes de autenticação AAA e WLAN do controlador, a autenticação do cliente é executada pelo servidor AAA.Selecione o servidor RADIUS apropriado no menu suspenso em Servidores RADIUS. Os outros parâmetros podem ser modificados com base no requisito da rede WLAN. Clique em
Apply.



Da mesma forma, para criar uma WLAN para o departamento de vendas, repita as etapas b e c. Aqui estão as capturas de
tela.


Address https://172.16.1.30/screens/fra
Go
Links
Norton AntiVirus
Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
WLANs
WLANs
WLANs
AP Groups VLAN
WLANs > New
< Back
Apply
WLAN ID
2
WLAN SSID
Sales


Done
Internet
Address https://172.16.1.30/screens/fra
Go
Links
Norton AntiVirus
Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
WLANs
WLANs
WLANs
AP Groups VLAN
WLANs > Edit
< Back
Apply
WLAN ID 2
WLAN SSID Sales
General Policies
Radio Policy All
Admin Status Enabled
Session Timeout (secs) 1800
Quality of Service (QoS) Silver (best effort)
WMM Policy Disabled
7920 Phone Support Client CAC Limit AP CAC Limit
Broadcast SSID Enabled
Aironet IE Enabled
Allow AAA Override Enabled
Client Exclusion Enabled ** 60
Timeout Value (secs)
DHCP Server Override
DHCP Addr. Assignment Required
Interface Name management
MFP Version Required 1
MFP Signature Generation (Global MFP Disabled)
H-REAP Local Switching
* H-REAP Local Switching not supported with IPSEC, L2TP, PPTP, CRANITE and FORTRESS authentications.
Security Policies
Layer 2 Security 802.1X
MAC Filtering
Layer 3 Security None
Web Policy *
* Web Policy cannot be used in combination with IPsec and L2TP.
** When client exclusion is enabled, a timeout value of zero means infinity(will require administrative override to reset excluded clients)
*** CKIP is not supported by 10xx APs
Radius Servers
Authentication Servers
Accounting Servers
Server 1 IP:172.16.1.60, Port:1812 none
Done
Internet

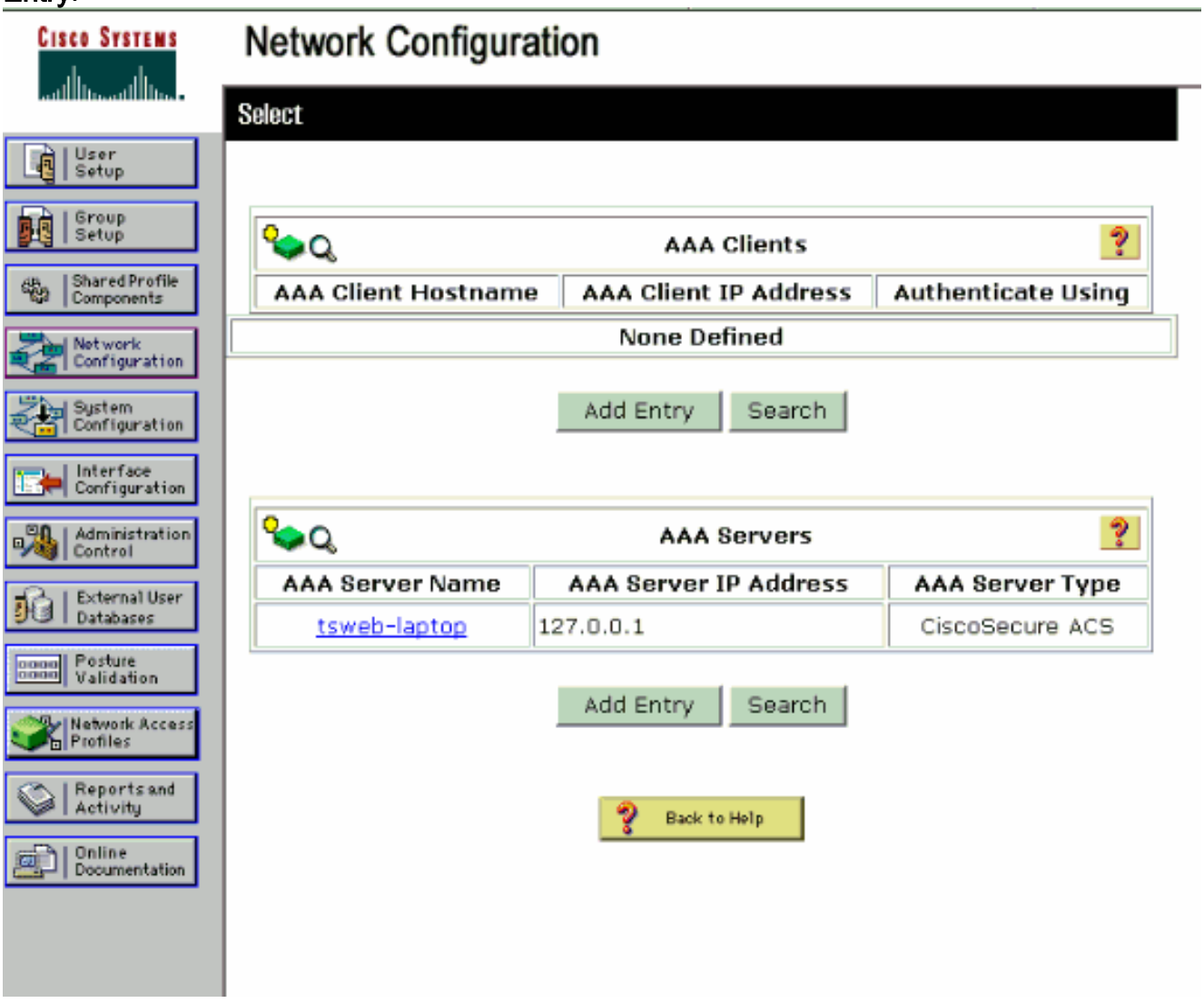
Configurar o Cisco Secure ACS

No servidor Cisco Secure ACS você precisa:

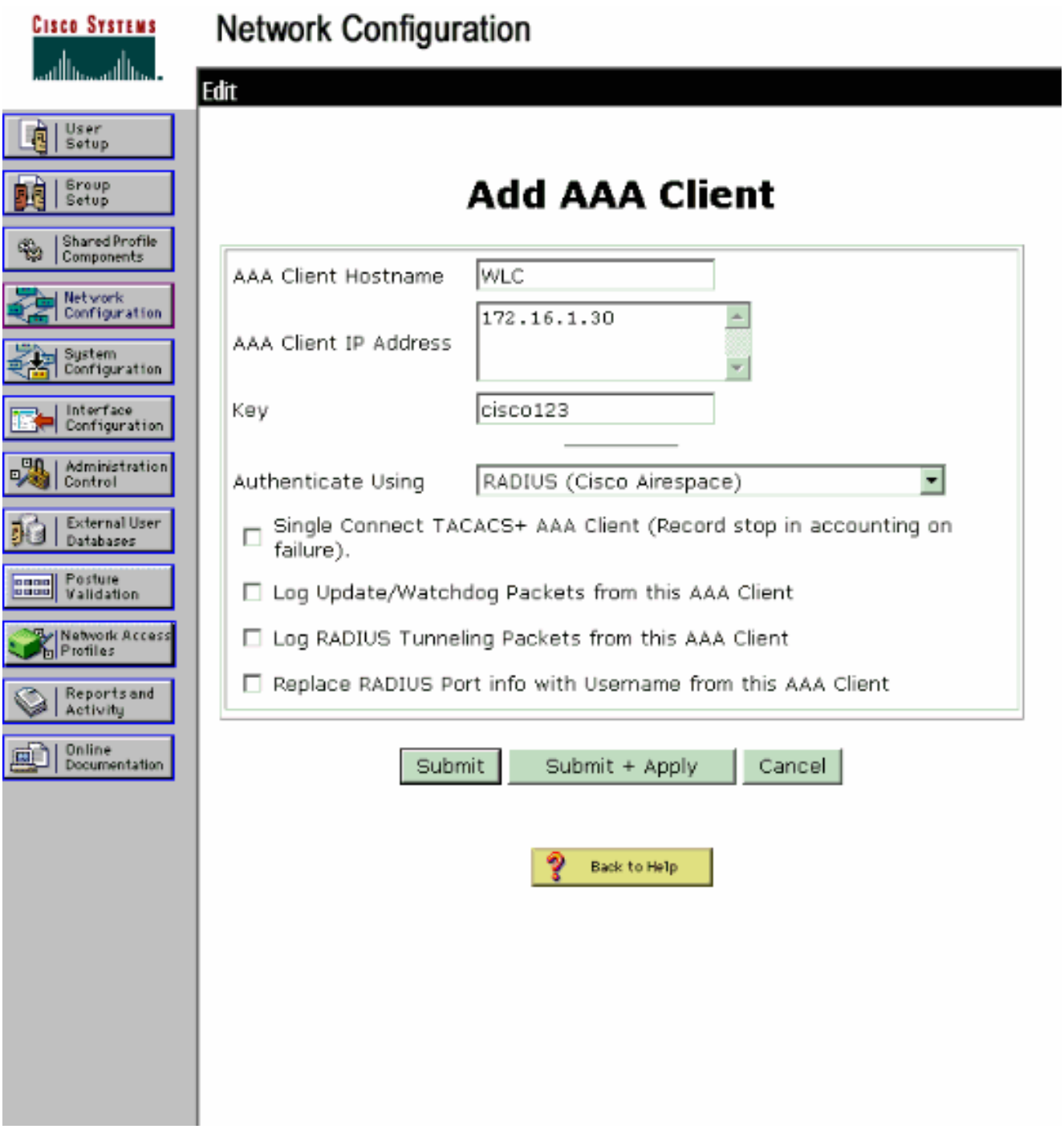
1. Configure a WLC como um cliente AAA.
2. Crie o banco de dados do usuário e defina o NAR para autenticação baseada em SSID.
3. Ative a autenticação EAP.

Conclua estes passos no Cisco Secure ACS:

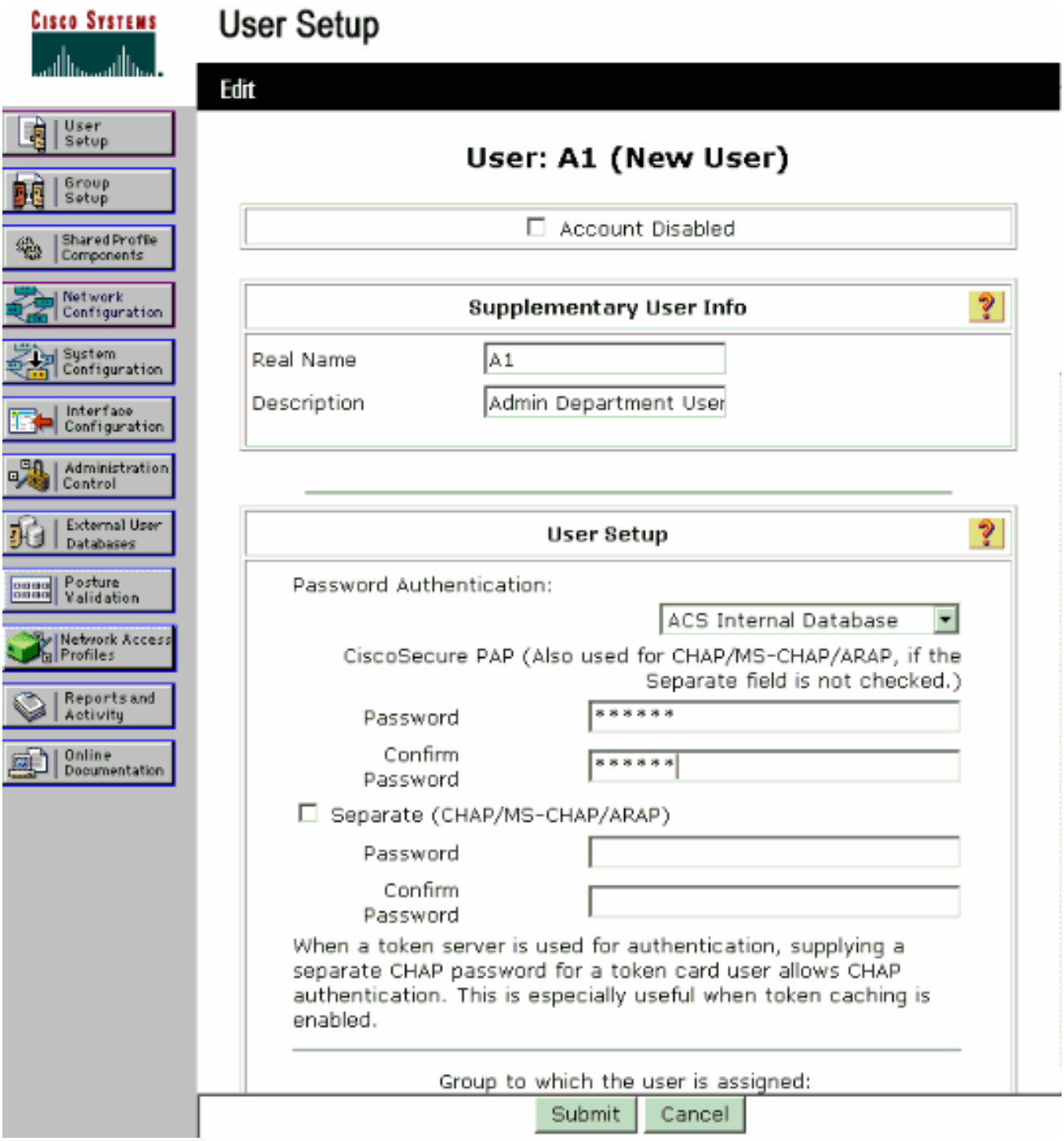
1. Para definir o controlador como um cliente AAA no servidor ACS, clique em **Network Configuration** na GUI do ACS. Em AAA clients, clique em **Add Entry**.



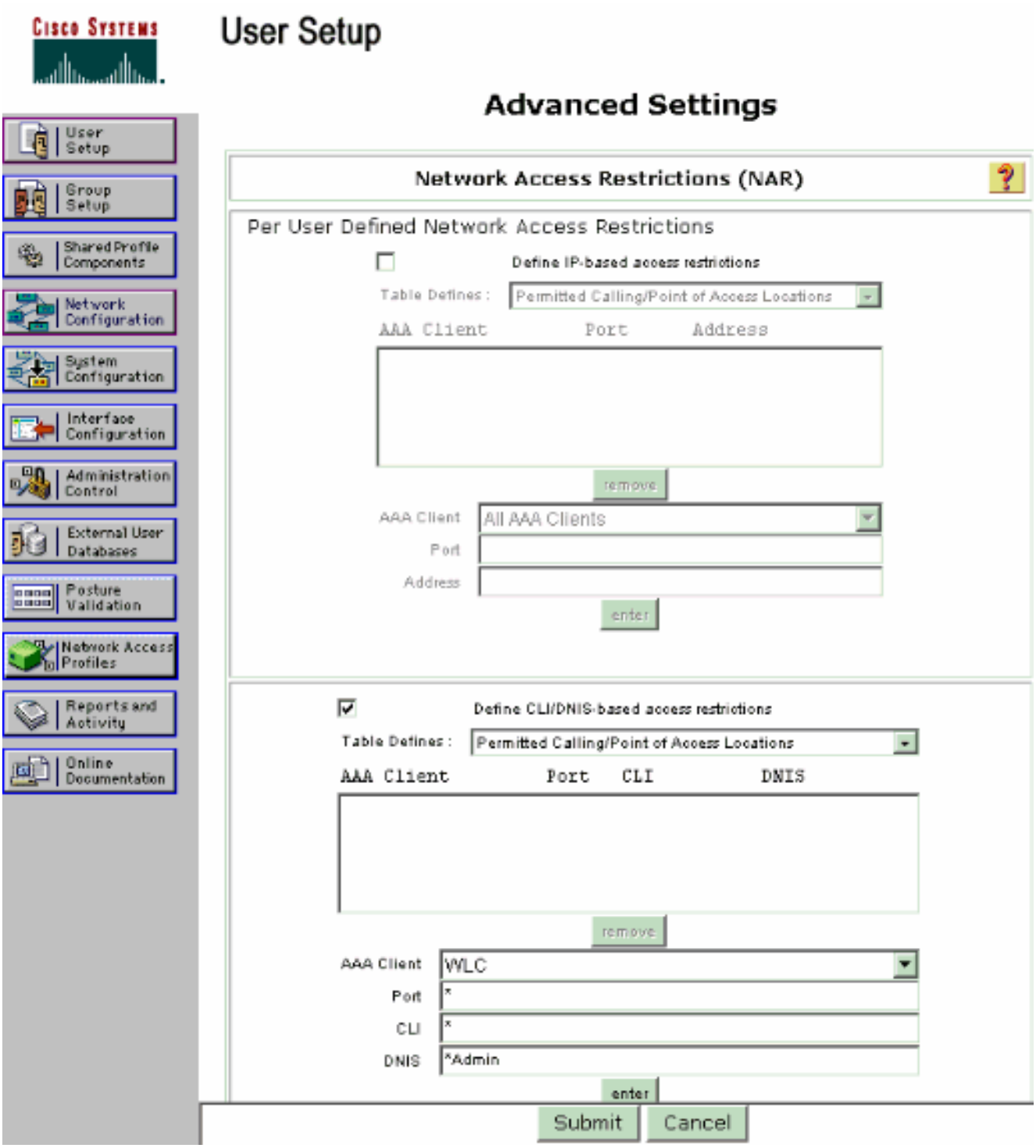
2. Quando a página Configuração de rede for exibida, defina o nome da WLC, do endereço IP, do segredo compartilhado e do método de autenticação (RADIUS Cisco Airespace).



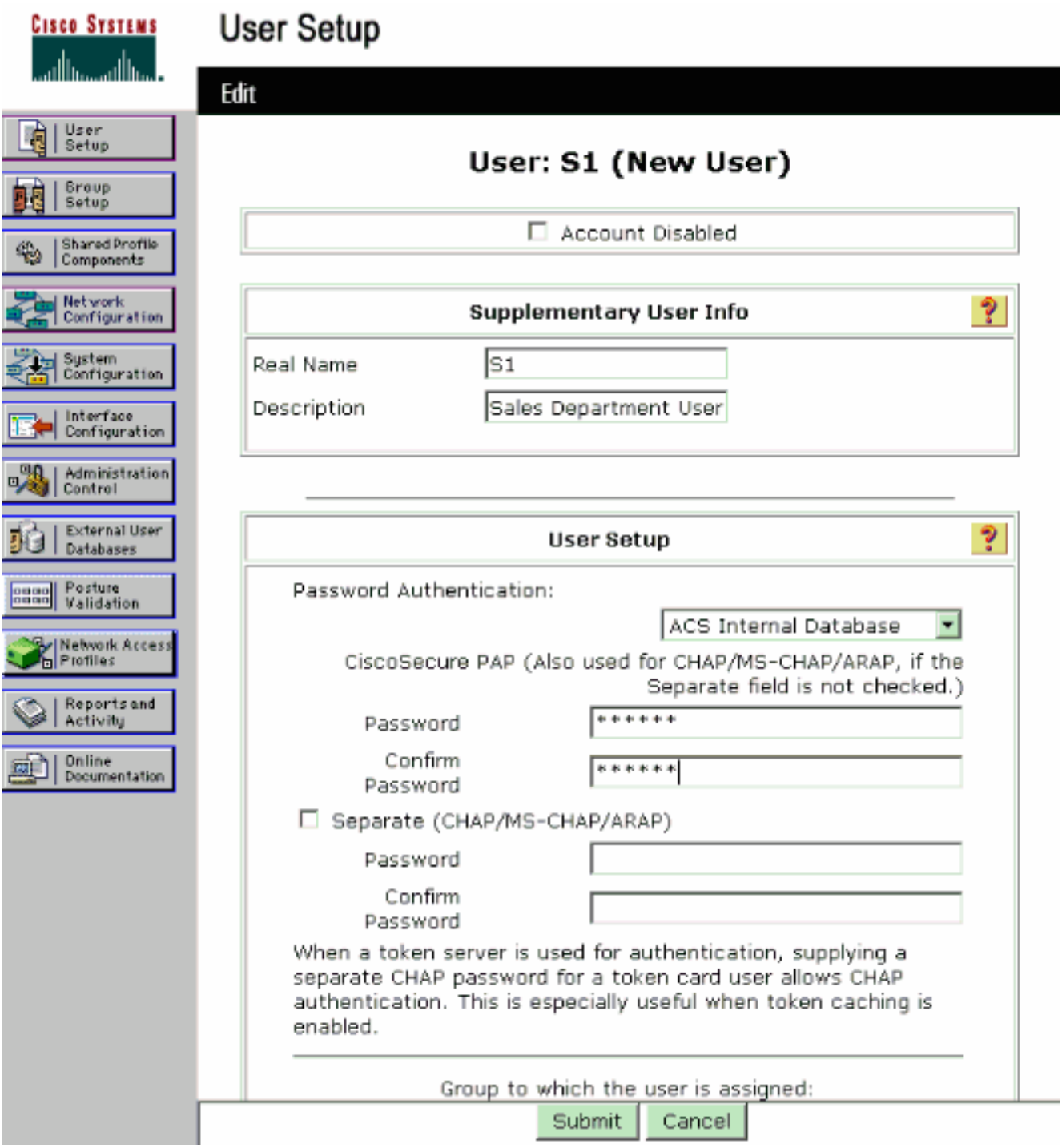
3. Clique em **User Setup** na GUI do ACS, digite o nome de usuário e clique em **Add/Edit**. Neste exemplo, o usuário é A1.
4. Quando a página User Setup for exibida, defina todos os parâmetros específicos do usuário. Neste exemplo, o nome de usuário, a senha e as Informações de usuário suplementares são configurados porque você precisa desses parâmetros para a autenticação LEAP.

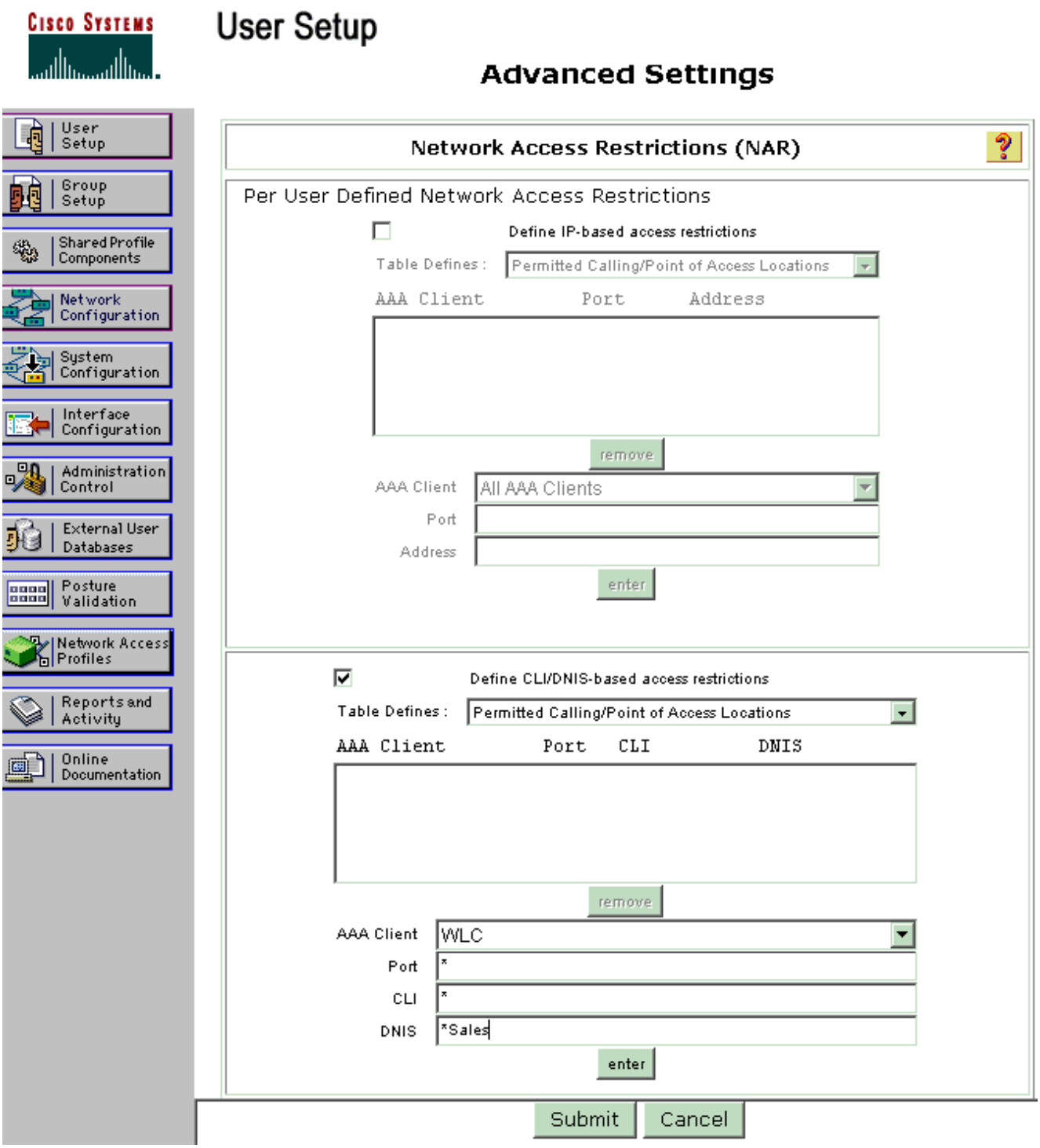


5. Role para baixo na página User Setup (Configuração do usuário) até ver a seção Network Access Restrictions (Restrições de acesso à rede). Na Interface de Usuário da Restrição de Acesso DNIS/CLI, selecione **Chamada Permitida/Ponto de Acesso Locais** e defina estes parâmetros:**Cliente AAA** — endereço IP WLC (172.16.1.30 em nosso exemplo)**Porta**—***CLI**—***DNIS** —*ssidname
6. O atributo DNIS define o SSID que o usuário pode acessar. A WLC envia o SSID no atributo DNIS para o servidor RADIUS.Se o usuário precisar acessar apenas a WLAN chamada Admin, insira ***Admin** para o campo DNIS. Isso garante que o usuário tenha acesso apenas à WLAN chamada Admin. Clique em **Enter**.**Observação:** o SSID deve ser sempre precedido por *. É
obrigatório.

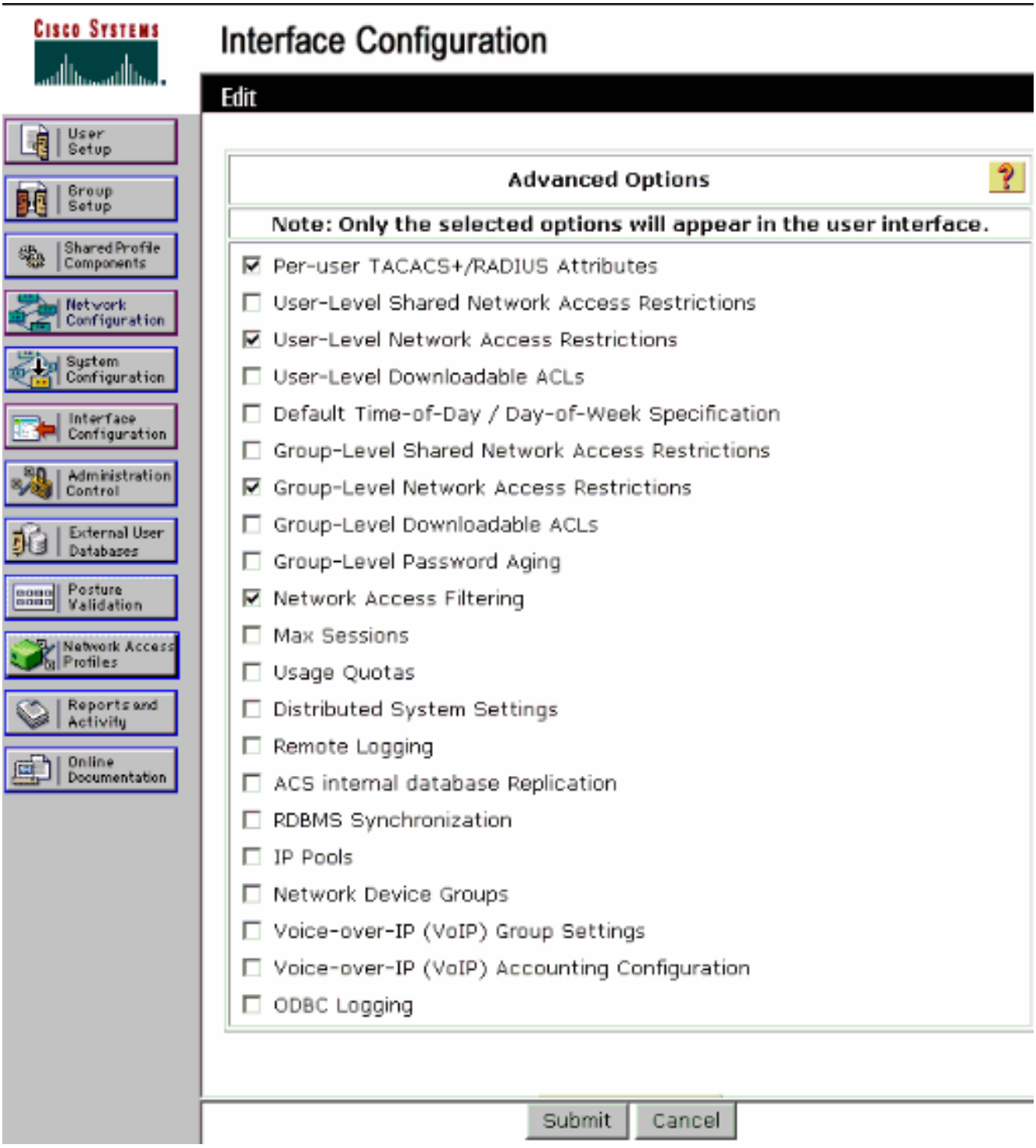


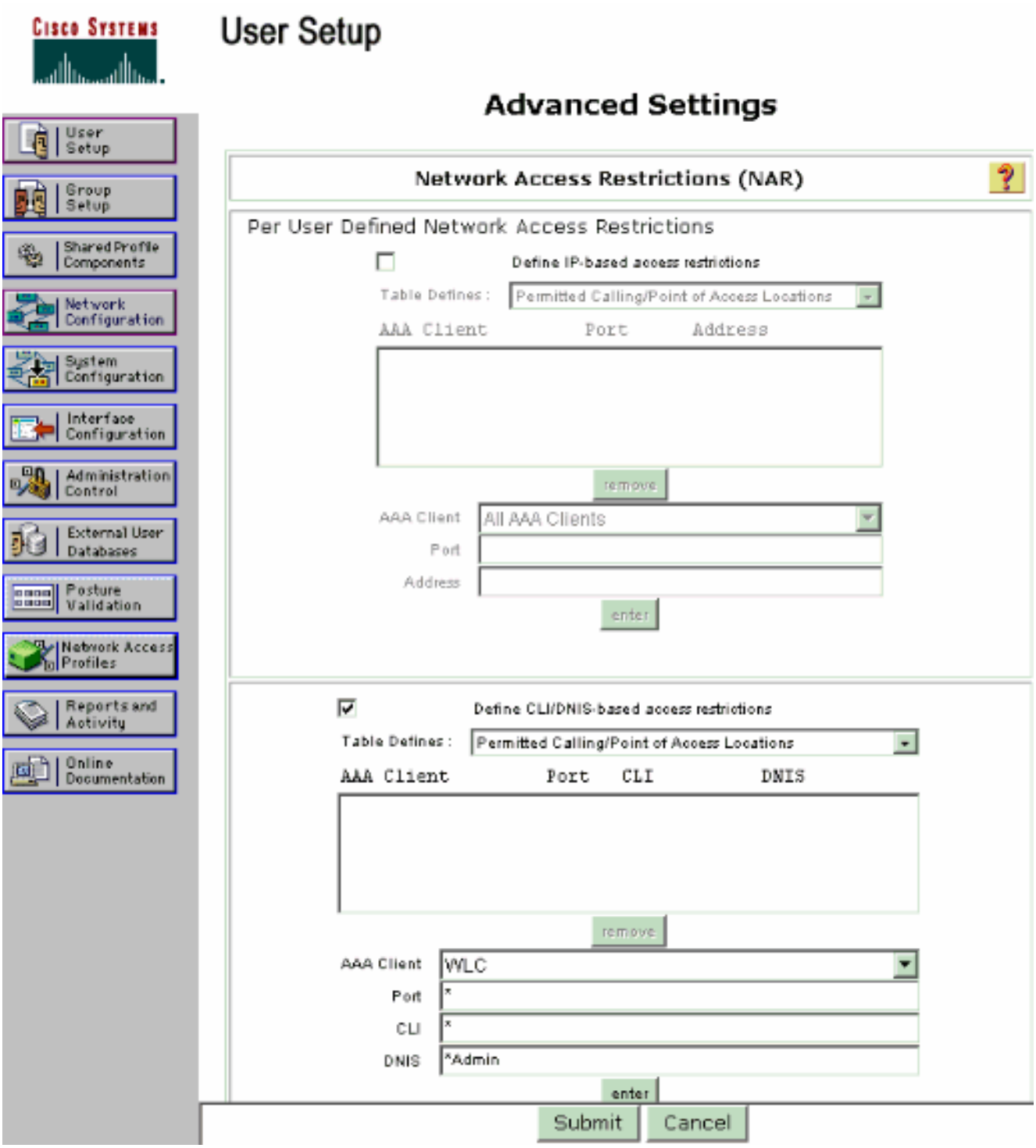
7. Clique em Submit.
8. Da mesma forma, crie um usuário para o usuário do departamento de Vendas. Aqui estão as capturas de
   tela.


Cisco Systems
User Setup
Edit
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
User: S1 (New User)
Account Disabled
Supplementary User Info
Real Name
S1
Description
Sales Department User
User Setup
Password Authentication:
ACS Internal Database
CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)
Password
******
Confirm Password
******
Separate (CHAP/MS-CHAP/ARAP)
Password
Confirm Password
When a token server is used for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication. This is especially useful when token caching is enabled.
Group to which the user is assigned:
Submit
Cancel

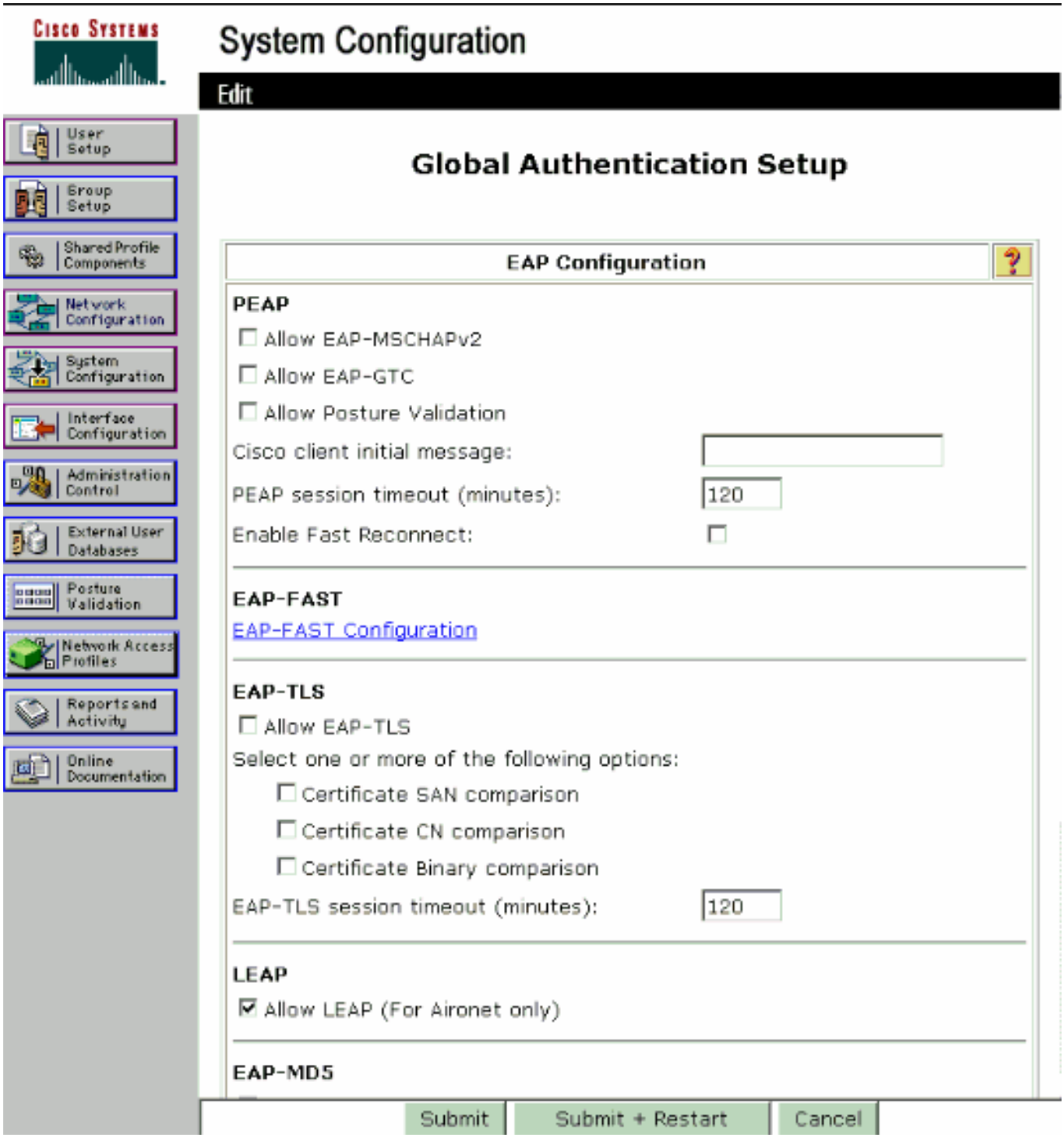


9. Repita o mesmo processo para adicionar mais usuários ao banco de dados.**Observação:** por padrão, todos os usuários são agrupados no grupo padrão. Se quiser atribuir usuários específicos a diferentes grupos, consulte a seção Gerenciamento de grupo de usuários do Guia do usuário do Cisco Secure ACS for Windows Server 3.2.**Observação:** se a seção Network Access Restrictions (Restrições de Acesso à Rede) não for exibida na janela User Setup (Configuração do usuário), isso pode ser porque ela não está habilitada. Para habilitar as Restrições de Acesso à Rede para usuários, escolha **Interfaces > Advanced Options** na GUI do ACS, selecione **User-Level Network Access Restrictions** e clique em **Submit**. Isso ativa o NAR e é exibido na janela User
Setup.


Cisco Systems
Interface Configuration
Edit
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
Advanced Options
Note: Only the selected options will appear in the user interface.
Per-user TACACS+/RADIUS Attributes
User-Level Shared Network Access Restrictions
User-Level Network Access Restrictions
User-Level Downloadable ACLs
Default Time-of-Day / Day-of-Week Specification
Group-Level Shared Network Access Restrictions
Group-Level Network Access Restrictions
Group-Level Downloadable ACLs
Group-Level Password Aging
Network Access Filtering
Max Sessions
Usage Quotas
Distributed System Settings
Remote Logging
ACS internal database Replication
RDBMS Synchronization
IP Pools
Network Device Groups
Voice-over-IP (VoIP) Group Settings
Voice-over-IP (VoIP) Accounting Configuration
ODBC Logging
Submit
Cancel



10. Para habilitar a autenticação EAP, clique em **Configuração do sistema** e **Configuração de autenticação global** para garantir que o servidor de autenticação esteja configurado para executar o método de autenticação EAP desejado.Nas definições de configuração do EAP, selecione o método EAP apropriado. Este exemplo usa autenticação LEAP. Clique em **Enviar** quando
terminar.

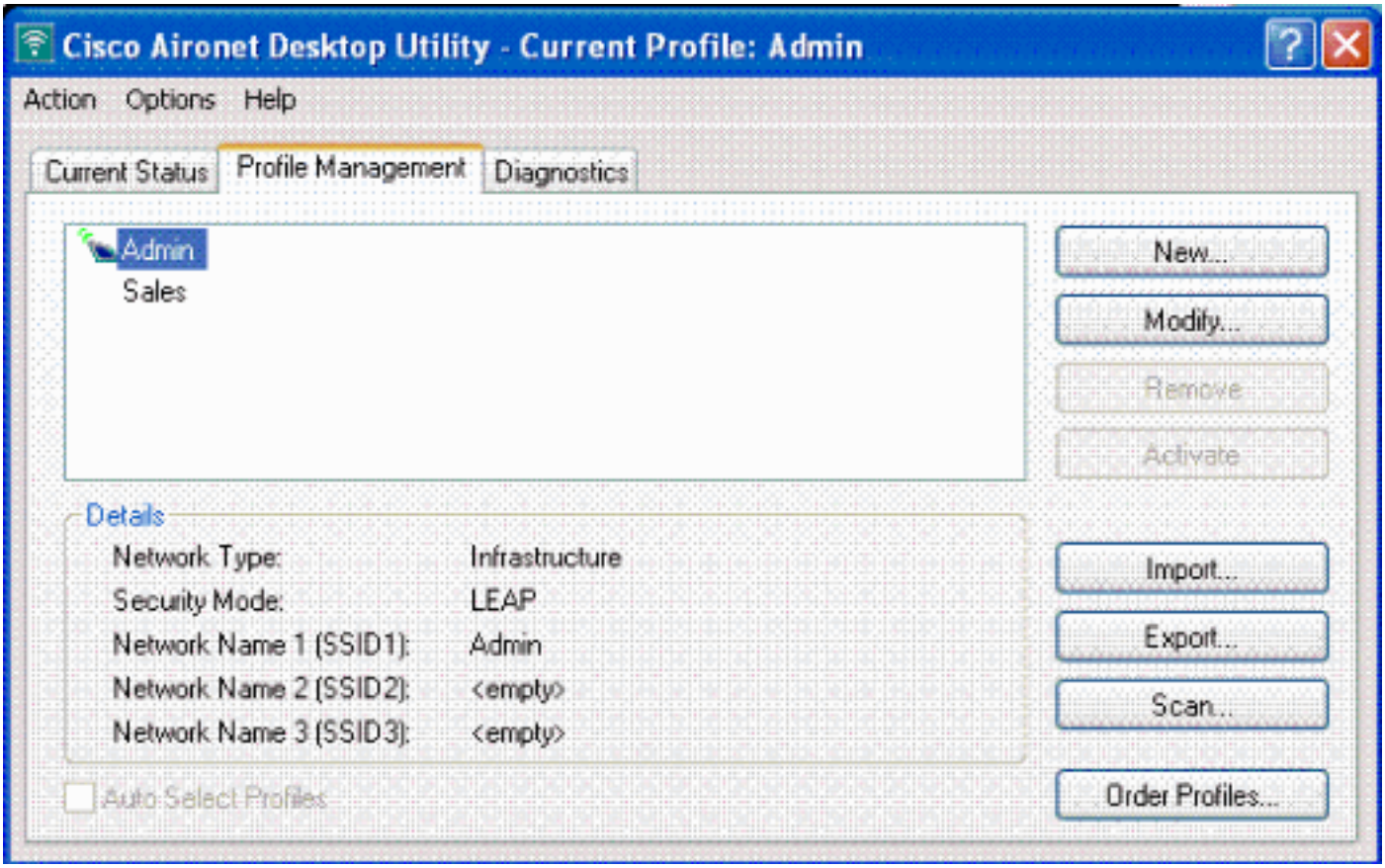


Configurar o cliente sem fio e verificar

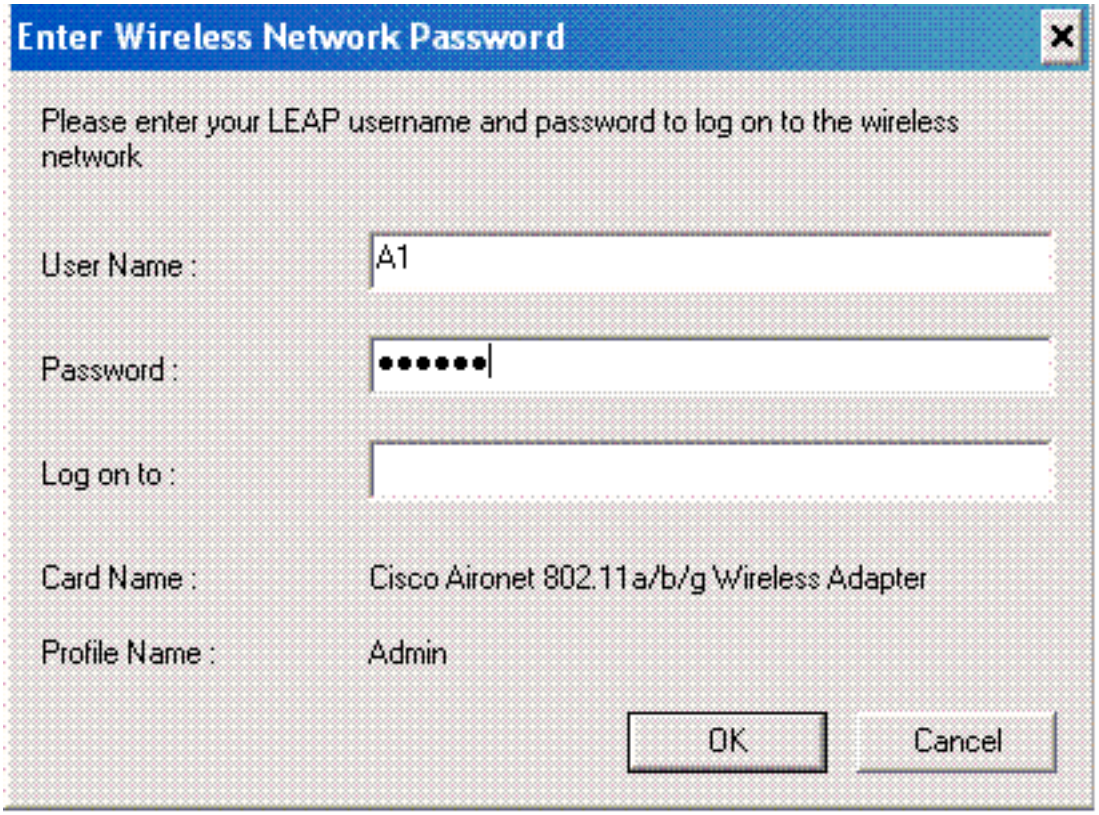
Use esta seção para confirmar se a sua configuração funciona corretamente. Tente associar um cliente sem fio ao LAP usando a autenticação LEAP para verificar se a configuração funciona como esperado.

Observação: este documento pressupõe que o perfil do cliente está configurado para autenticação LEAP. Consulte Utilização da Autenticação EAP para obter informações sobre como configurar o Adaptador de Cliente Wireless 802.11 a/b/g para autenticação LEAP.

Observação: no ADU você vê que configurou dois perfis de cliente. Um para os usuários do departamento Admin com **Admin** SSID e outro para os usuários do departamento de vendas com **Vendas** SSID. Ambos os perfis estão configurados para autenticação LEAP.



Quando o perfil do usuário sem fio do departamento Admin é ativado, o usuário é solicitado a fornecer o nome de usuário/senha para a autenticação LEAP. Aqui está um exemplo:

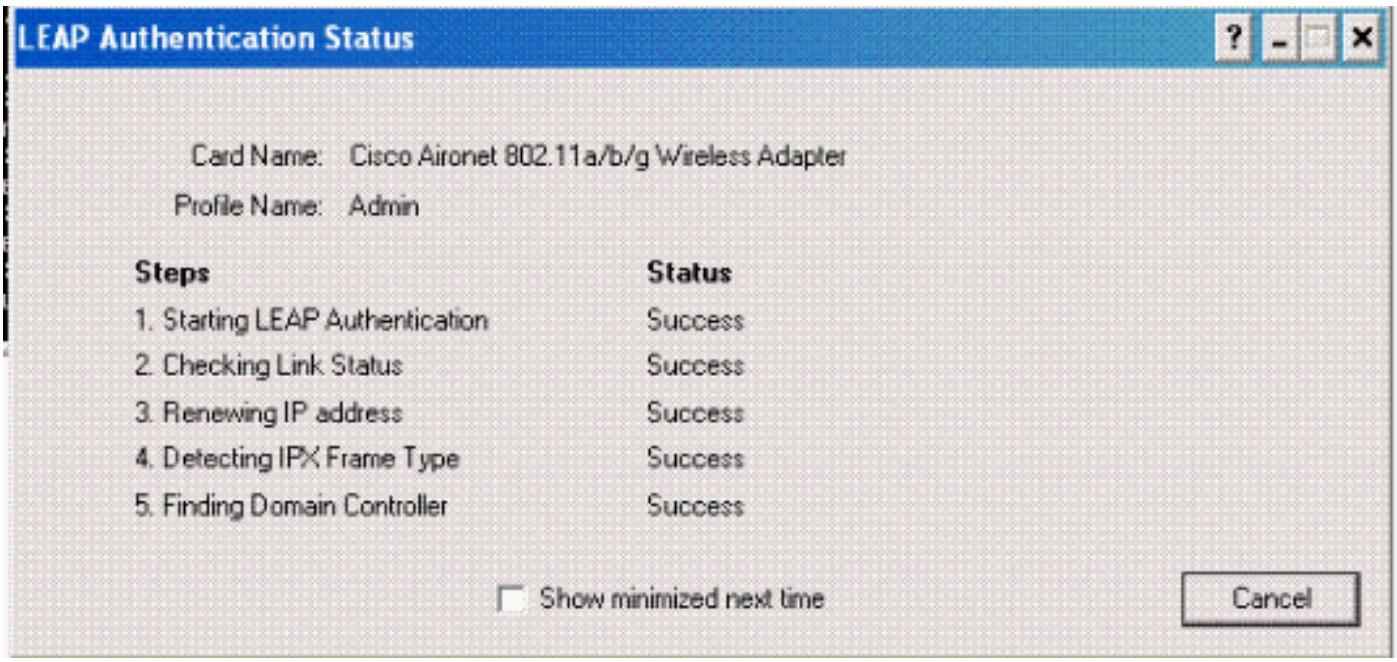


O LAP e, em seguida, a WLC passam as credenciais do usuário para o servidor RADIUS externo (Cisco Secure ACS) para validar as credenciais. A WLC passa as credenciais, incluindo o atributo DNIS (nome SSID) para o servidor RADIUS para validação.

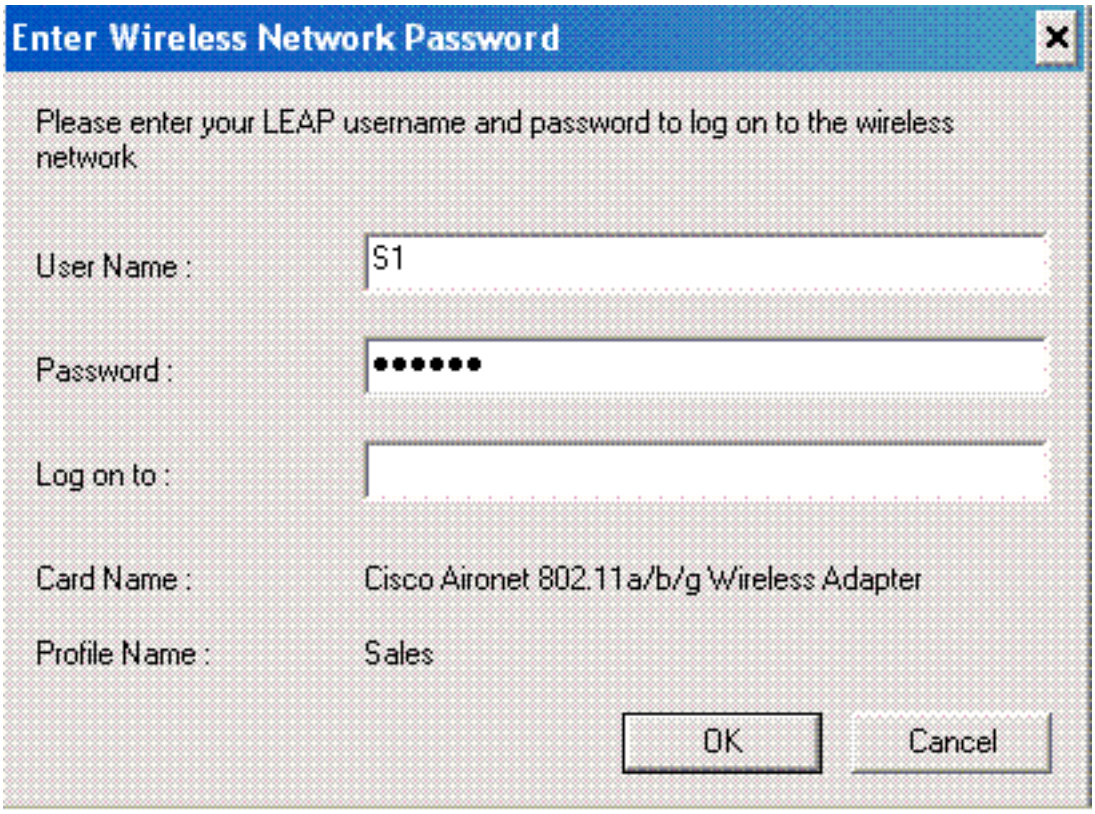
O servidor RADIUS verifica as credenciais do usuário comparando os dados com o banco de

dados do usuário (e os NARs) e fornece acesso ao cliente sem fio sempre que as credenciais do usuário são válidas.

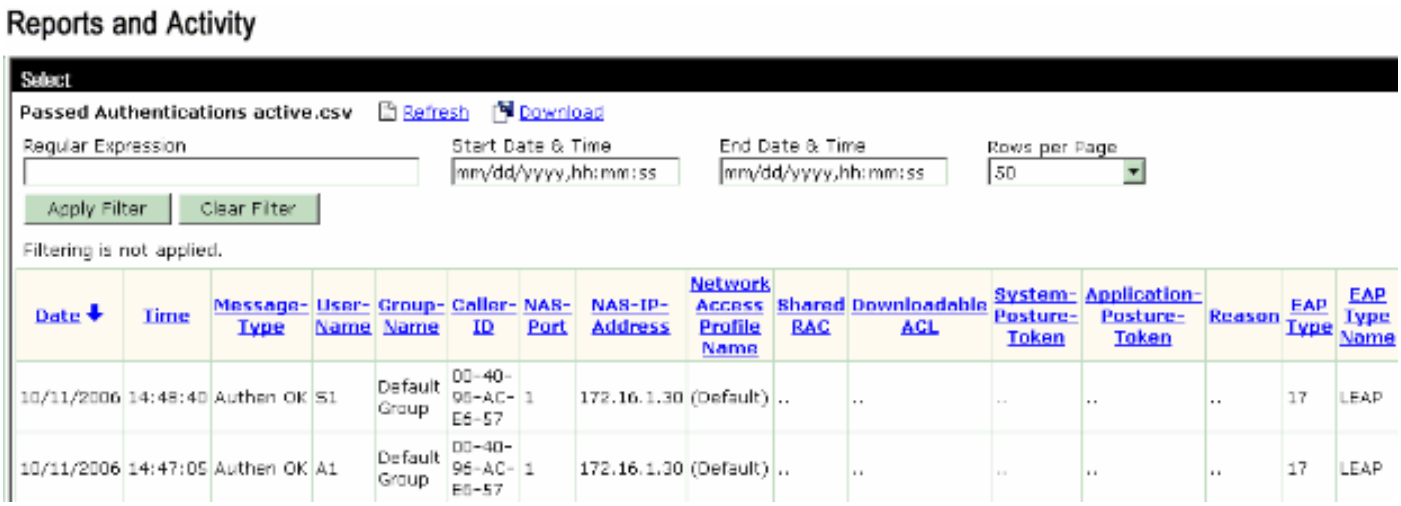
Após a autenticação RADIUS bem-sucedida, o cliente sem fio associa-se ao LAP.



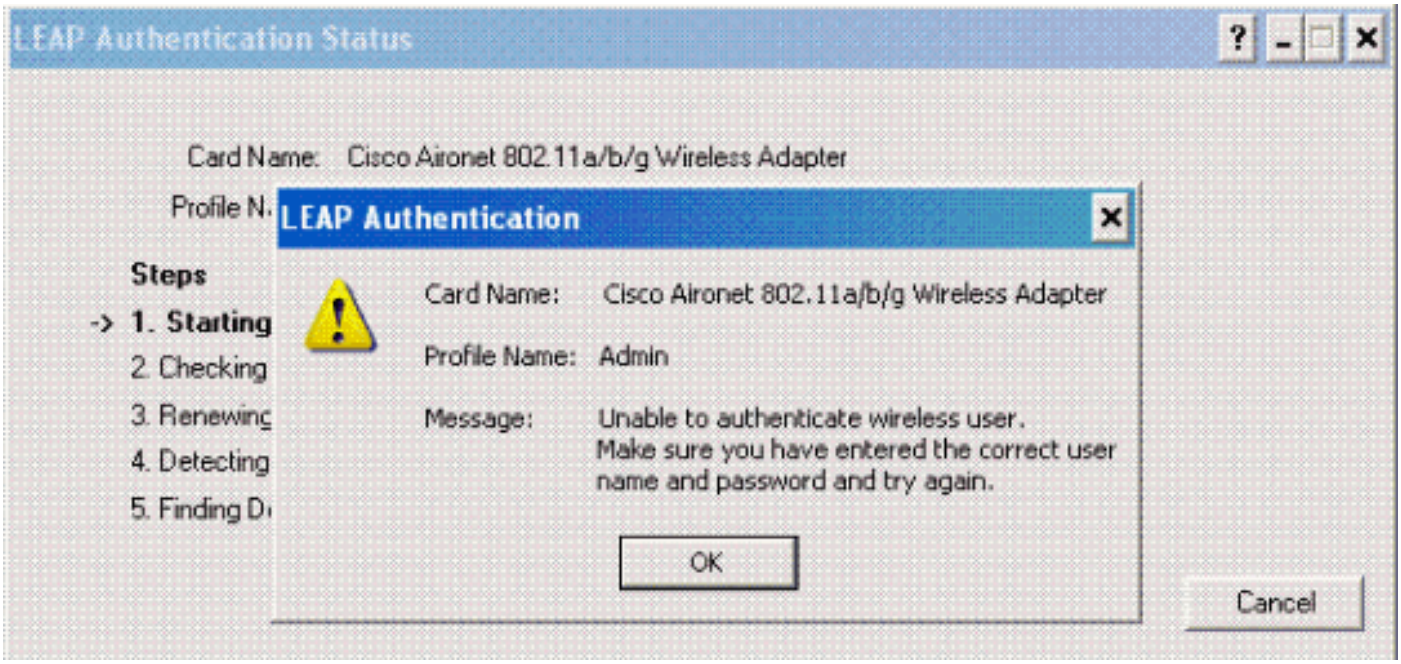
Da mesma forma, quando um usuário do departamento de Vendas ativa o perfil de Vendas, o usuário é autenticado pelo servidor RADIUS com base no nome de usuário/senha LEAP e no SSID.



O relatório Autenticação aprovada no servidor ACS mostra que o cliente passou na autenticação RADIUS (autenticação EAP e autenticação SSID). Aqui está um exemplo:



Agora, se o usuário de vendas tentar acessar o SSID **Admin**, o servidor RADIUS negará o acesso do usuário à WLAN. Aqui está um exemplo:



Dessa forma, os usuários podem ter acesso restrito com base no SSID. Em um ambiente corporativo, todos os usuários que se enquadram em um departamento específico podem ser agrupados em um único grupo e o acesso à WLAN pode ser fornecido com base no SSID que usam, conforme explicado neste documento.

Troubleshoot

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 dot1x aaa enable** —Habilita a depuração de interações AAA 802.1x.
- **debug dot1x packet enable**—Habilita a depuração de todos os pacotes dot1x.

- **debug aaa all enable** — Configura a depuração de todas as mensagens AAA.

Você também pode usar o relatório Autenticação Passada e o relatório Falha de Autenticação no servidor Cisco Secure ACS para solucionar problemas de configuração. Esses relatórios estão na janela **Relatórios e atividade** na GUI do ACS.

Informações Relacionadas

- Exemplo de Configuração de Autenticação EAP com Controladores WLAN (WLC)
- Exemplo de configuração de autenticação da Web para o controlador da LAN sem fio
- Exemplo de configuração de VLANs de grupo de AP com Wireless LAN Controllers
- Página de Suporte Wireless
- Suporte Técnico e Documentação - Cisco Systems