Restrinja o acesso WLAN baseado no SSID com WLC e exemplo de configuração do Cisco Secure ACS

Índice

Introdução

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

Pré-requisitos

Requisitos

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

- Conhecimento de como configurar o controlador do Wireless LAN (WLC) e o Access point de pouco peso (REGAÇO) para a operação básica
- Conhecimento básico em como configurar o Serviço de controle de acesso Cisco Secure (ACS)
- Conhecimento de métodos de pouco peso do protocolo (LWAPP) e da segurança Wireless do Access point

Componentes Utilizados

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

- Cisco 2000 Series WLC que executa o firmware 4.0
- REGAÇO do Cisco 1000 Series
- Versão de servidor 3.2 do Cisco Secure ACS
- Adaptador de cliente Wireless de Cisco 802.11a/b/g que executa o firmware 2.6
- Versão 2.6 do utilitário de desktop do Cisco Aironet (ADU)

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

Convenções

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

Informações de Apoio

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

1. Autenticação de EAP
2. Autenticação SSID baseada nas limitações do acesso de rede (NAR) no Cisco Secure ACS

Se o EAP e a autenticação SSID-baseada são bem sucedidos, está permitido ao usuário alcançar o WLAN ou então o usuário é dissociado.

O Cisco Secure ACS usa a característica NAR para restringir o acesso de usuário baseado no SSID. Um NAR é uma definição, que você faça no Cisco Secure ACS, das circunstâncias adicionais que devem ser estadas conformes antes que um usuário possa alcançar a rede. O Cisco Secure ACS aplica estas circunstâncias usando a informação dos atributos enviados por seus clientes de AAA. Embora haja diversas maneiras que você pode estabelecer NAR, todos são baseados na informação de atributos de harmonização enviada pelo cliente de AAA. Consequentemente, você deve compreender que o formato e o índice dos atributos que seus clientes de AAA enviam se você quer empregar NAR eficazes.

Quando você estabelece um NAR, você pode escolher se o filtro se opera positivamente ou negativamente. Isto é, no NAR você especifica se ao acesso de rede do permit or deny, com base em uma comparação da informação enviada dos clientes de AAA à informação armazenada no NAR. Contudo, se um NAR não encontra a informação suficiente para se operar, opta o acesso negado.

Você pode definir um NAR para, e aplica ao, a um usuário ou um grupo de usuário específico. Refira o White Paper das limitações do acesso de rede para mais informação.

O Cisco Secure ACS apoia dois tipos de filtros NAR:

1. **Filtros com base em IP** — O NAR com base em IP filtra o acesso do limite baseado nos IP address do cliente do utilizador final e do cliente de AAA. Refira filtros aproximadamente

com base em IP NAR para obter mais informações sobre deste tipo de filtro NAR.

2. **filtros NON-IP-baseados** — o NAR NON-IP-baseado filtra o acesso do limite baseado na comparação de série simples de um valor enviado do cliente de AAA. O valor pode ser o número identificação da linha de chamada (CLI), o número do Dialed Number Identification Service (DNIS), o MAC address, ou o outro valor que origina do cliente. Para este tipo de NAR a operar-se, o valor na descrição NAR deve exatamente combinar o que é enviada do cliente, incluindo o que formato é usado. Por exemplo, o (217) 555-4534 não combina 217-555-4534. Refira filtros aproximadamente NON-IP-baseados NAR para obter mais informações sobre deste tipo de filtro NAR.

Este original usa os filtros NON-IP-baseados para fazer a autenticação SSID-baseada. Um filtro NON-IP-baseado NAR (isto é, um filtro DNIS/CLI-based NAR) é uma lista de permitido ou o Denied Calling/Point of Access Locations que você pode usar na limitação de um cliente de AAA quando você não tem uma conexão com base em IP estabelecida. A característica NON-IP-baseada NAR usa geralmente o número CLI e o número DNIS. Há umas exceções no uso dos campos DNIS/CLI. Você pode dar entrada com o nome SSID no campo DNIS e faz autenticação SSID-baseada. Isto é porque o WLC envia no atributo DNIS, o nome SSID, ao servidor Radius. Assim se você constrói DNIS NAR no usuário ou no grupo, você pode criar limitações por-USER SSID.

Se você usa o RAIO, os campos NAR alistados aqui usam estes valores:

- **Cliente de AAA** — O Nas-ip-address (atributo 4) ou, se o Nas-ip-address não existe, o NAS-identificador (atributo RADIUS 32) são usados.
- **Porta** — A NAS-porta (atributo 5) ou, se a NAS-porta não existe, o nas-port-id (atributo 87) são usados.
- **CLI** — A chamar-estação-identificação (atributo 31) é usada.
- **DNIS** — A chamar-estação-identificação (atributo 30) é usada.

Refira limitações do acesso de rede para obter mais informações sobre do uso do NAR.

Desde que o WLC envia no atributo DNIS e no nome SSID, você pode criar limitações por-USER SSID. No caso do WLC, os campos NAR têm estes valores:

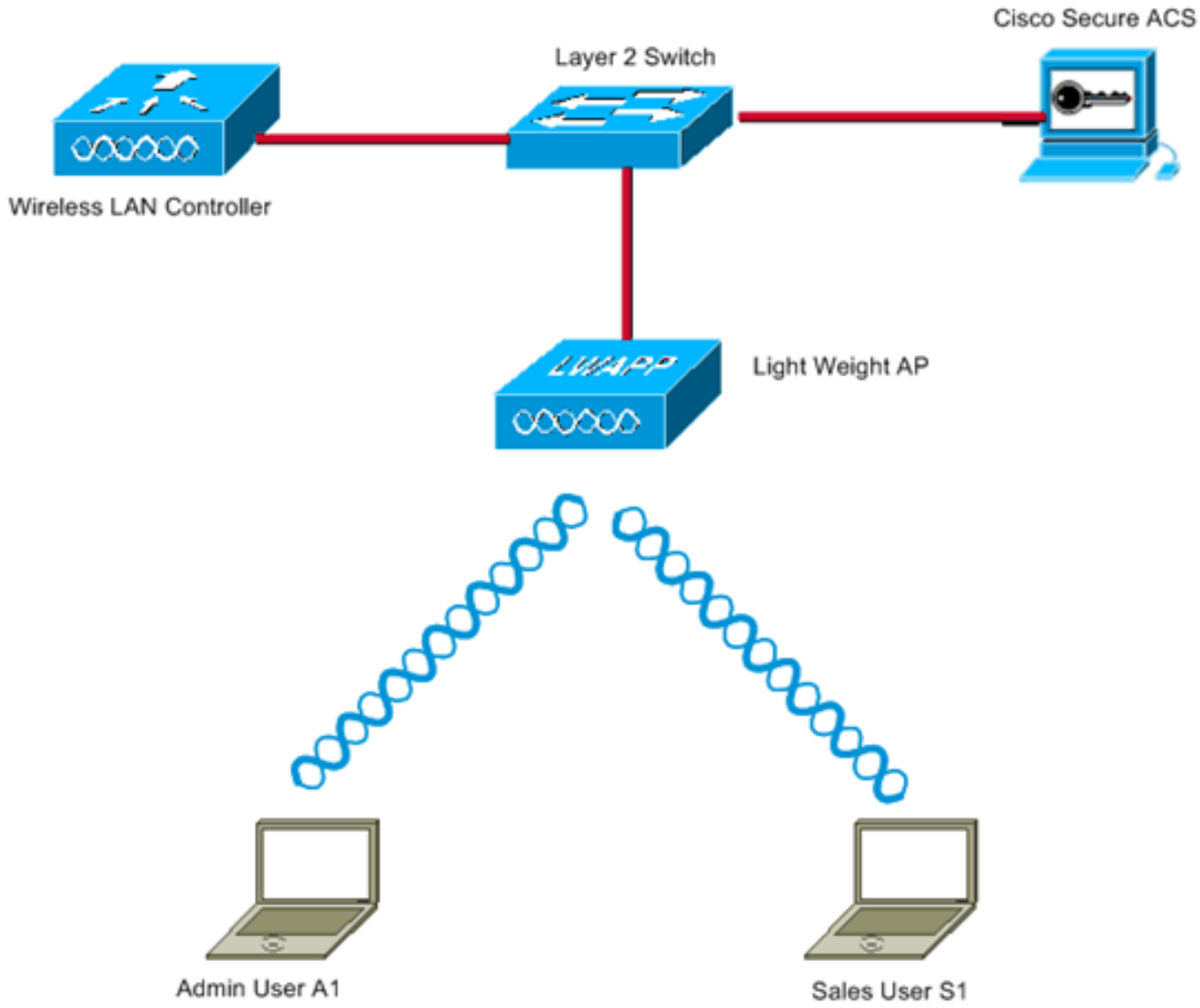
- **Cliente de AAA** — IP address WLC
- **porta** — *
- **CLI** — *
- **DNIS** — *ssidname

O restante deste documento fornece um exemplo de configuração em como realizar isto.

Instalação de rede

Nesta instalação do exemplo, WLC é registrado ao REGAÇO. Dois WLAN são usados. Um WLAN é para os usuários do departamento administrativo e o outro WLAN é para os usuários do departamento de vendas. O cliente Wireless A1 (usuário admin) e S1 (usuário das vendas) conecta à rede Wireless. Você precisa de configurar o WLC e o servidor Radius de tal maneira que o usuário admin A1 pode alcançar somente o WLAN **Admin** e é acesso restrito às **vendas** WLAN e ao usuário S1 das vendas deve poder alcançar as **vendas** WLAN e deve ter o acesso restrito ao WLAN **Admin**. Todos os usuários usam a autenticação de leap como um método de autenticação da camada 2.

Nota: Este original supõe que o WLC está registrado ao controlador. Se você é novo a WLC e não sabe configurar o WLC para a operação básica, refere o registro de pouco peso AP (REGAÇO) a um controlador do Wireless LAN (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

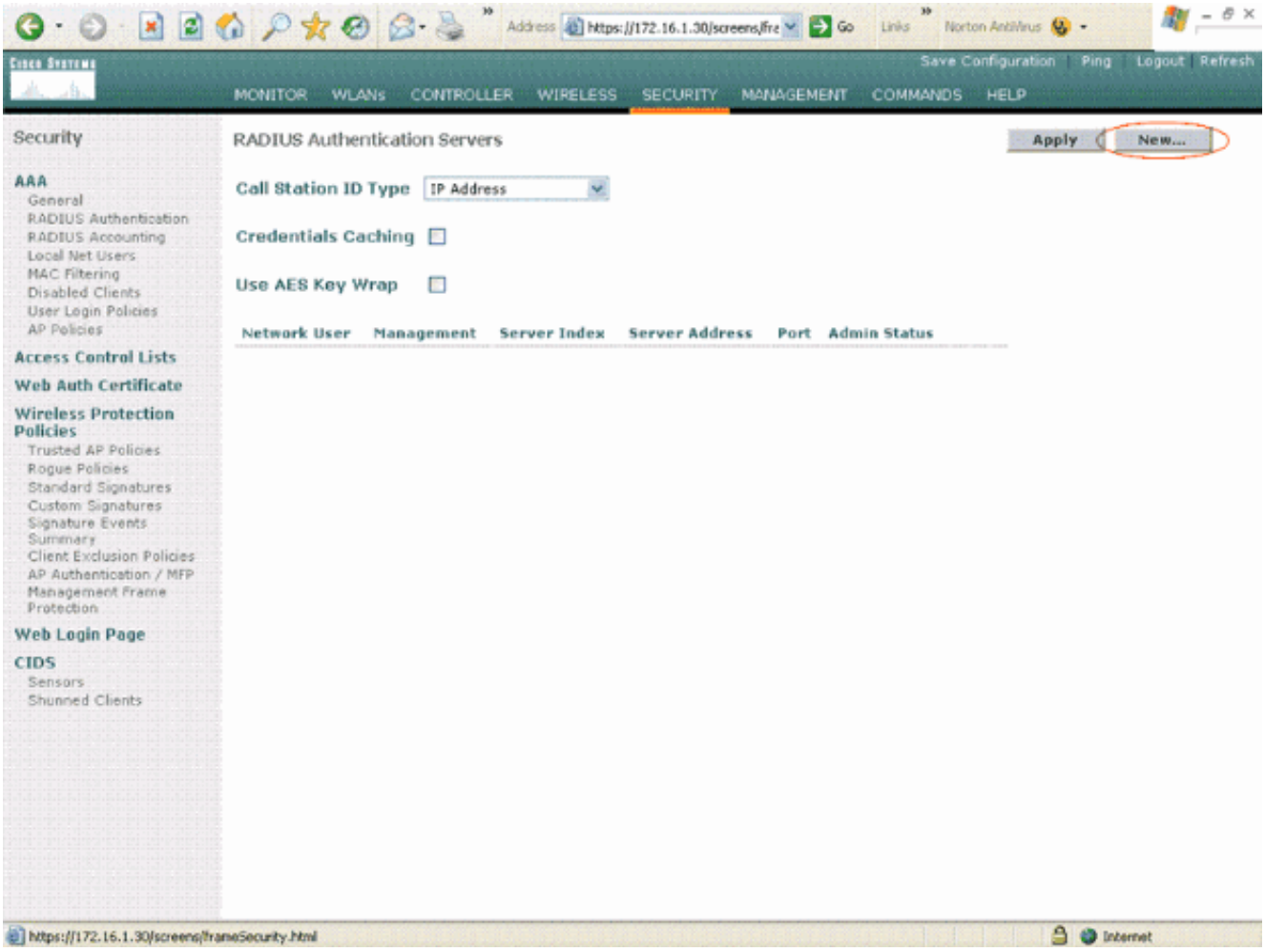
A fim configurar os dispositivos para esta instalação, você precisa:

1. Configurar o WLC para os dois WLAN e servidores Radius.
2. Configurar o Cisco Secure ACS.
3. Configurar os clientes Wireless e verifique-os.

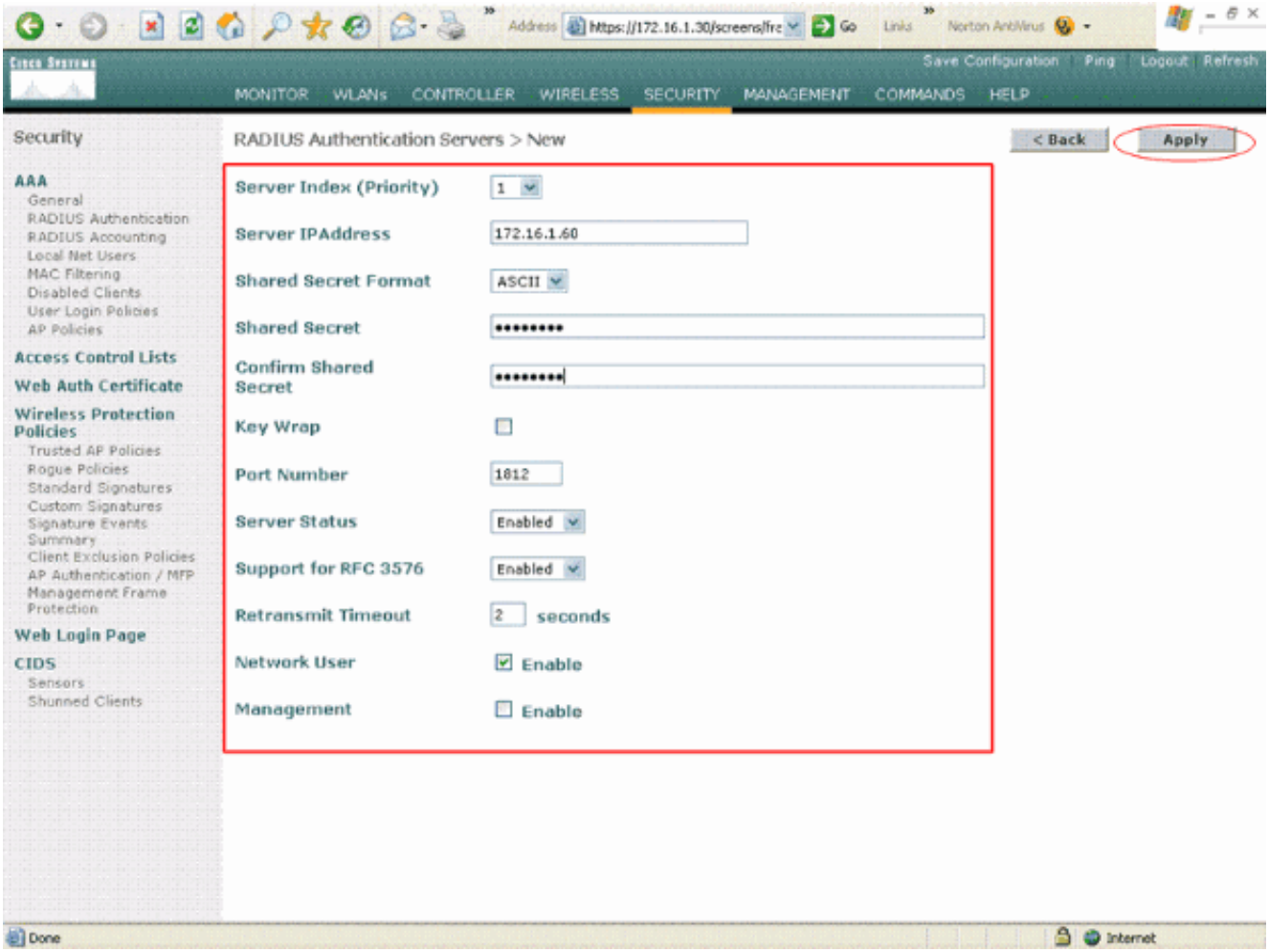
Configurar o WLC

Termine estas etapas a fim configurar o WLC para esta instalação:

1. O WLC precisa de ser configurado para enviar as credenciais do usuário a um servidor de raio externo. O servidor de raio externo (Cisco Secure ACS neste caso) então valida as credenciais do usuário e fornece o acesso aos clientes Wireless. Conclua estes passos:Escolha a **Segurança** > a **autenticação RADIUS do** controlador GUI a fim indicar a página dos servidores de autenticação
RADIUS.

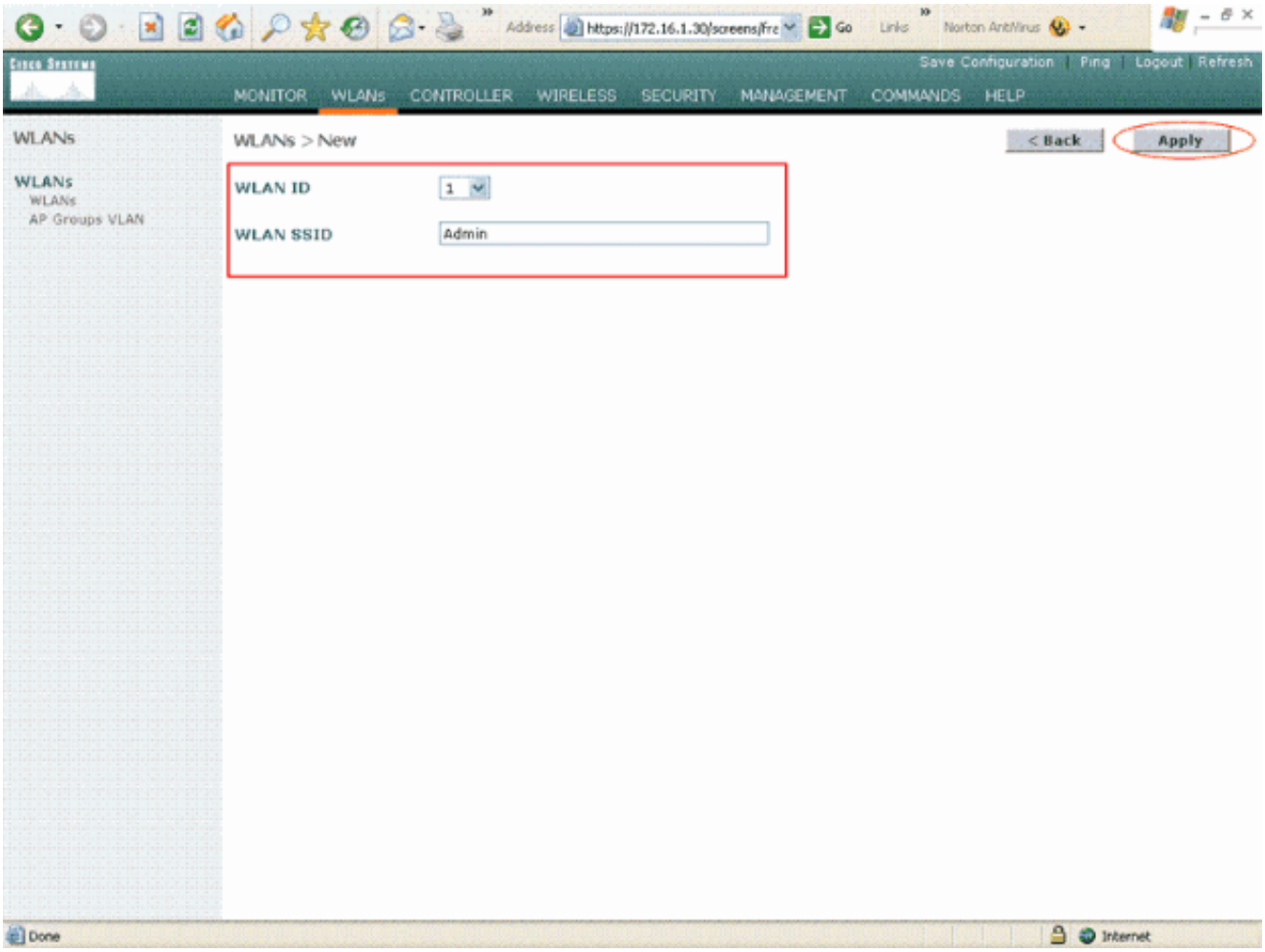


Clique **novo** a fim definir os parâmetros do servidor Radius.Estes parâmetros incluem o IP address do servidor Radius, o segredo compartilhado, o número de porta, e o status de servidor. O usuário de rede e as caixas de verificação de gerenciamento determinam se a autenticação Raio-baseada se aplica para o Gerenciamento e os usuários de rede. Este exemplo usa o Cisco Secure ACS como o servidor Radius com endereço IP 172.16.1.60.

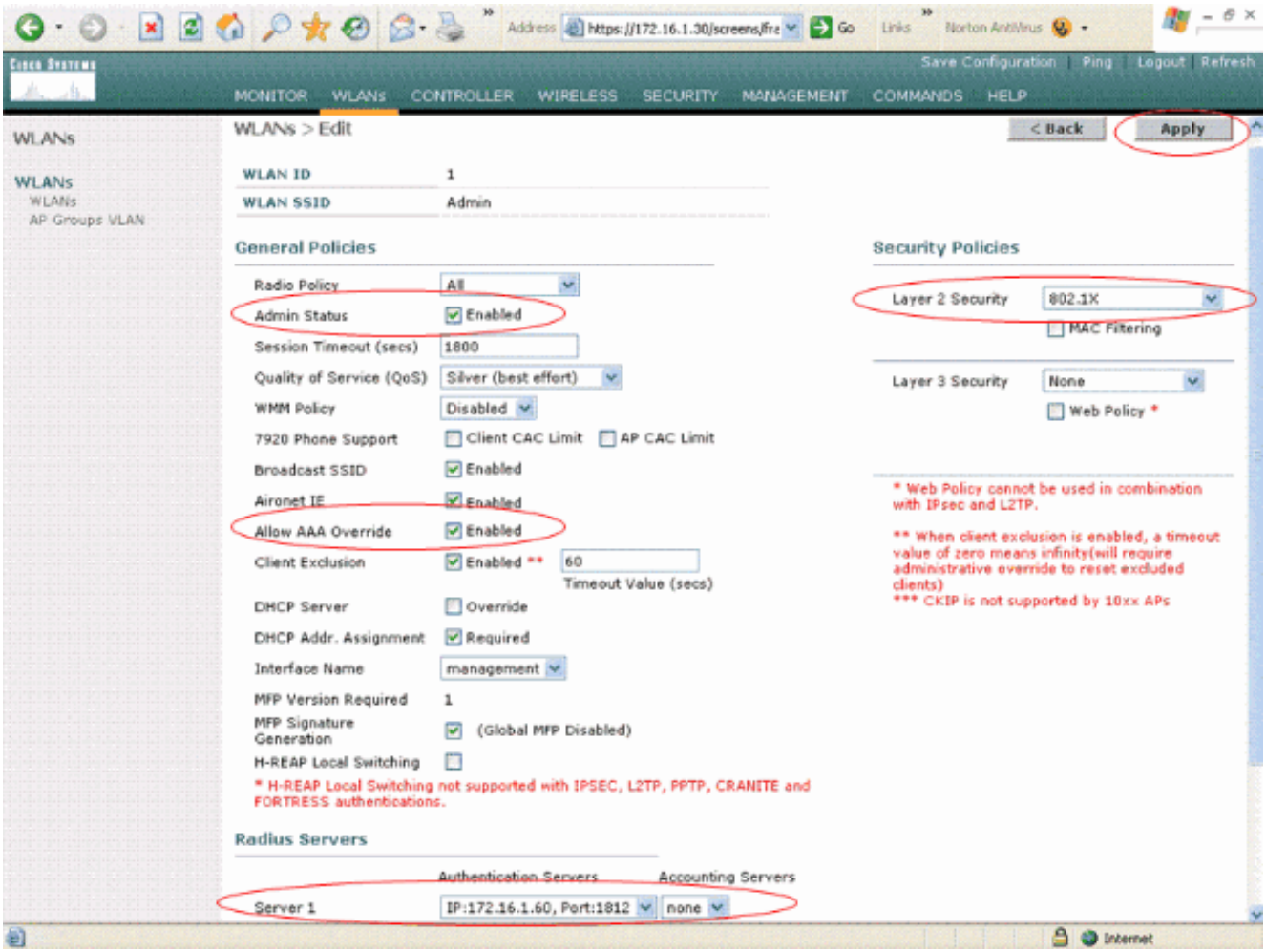


Clique em Apply.

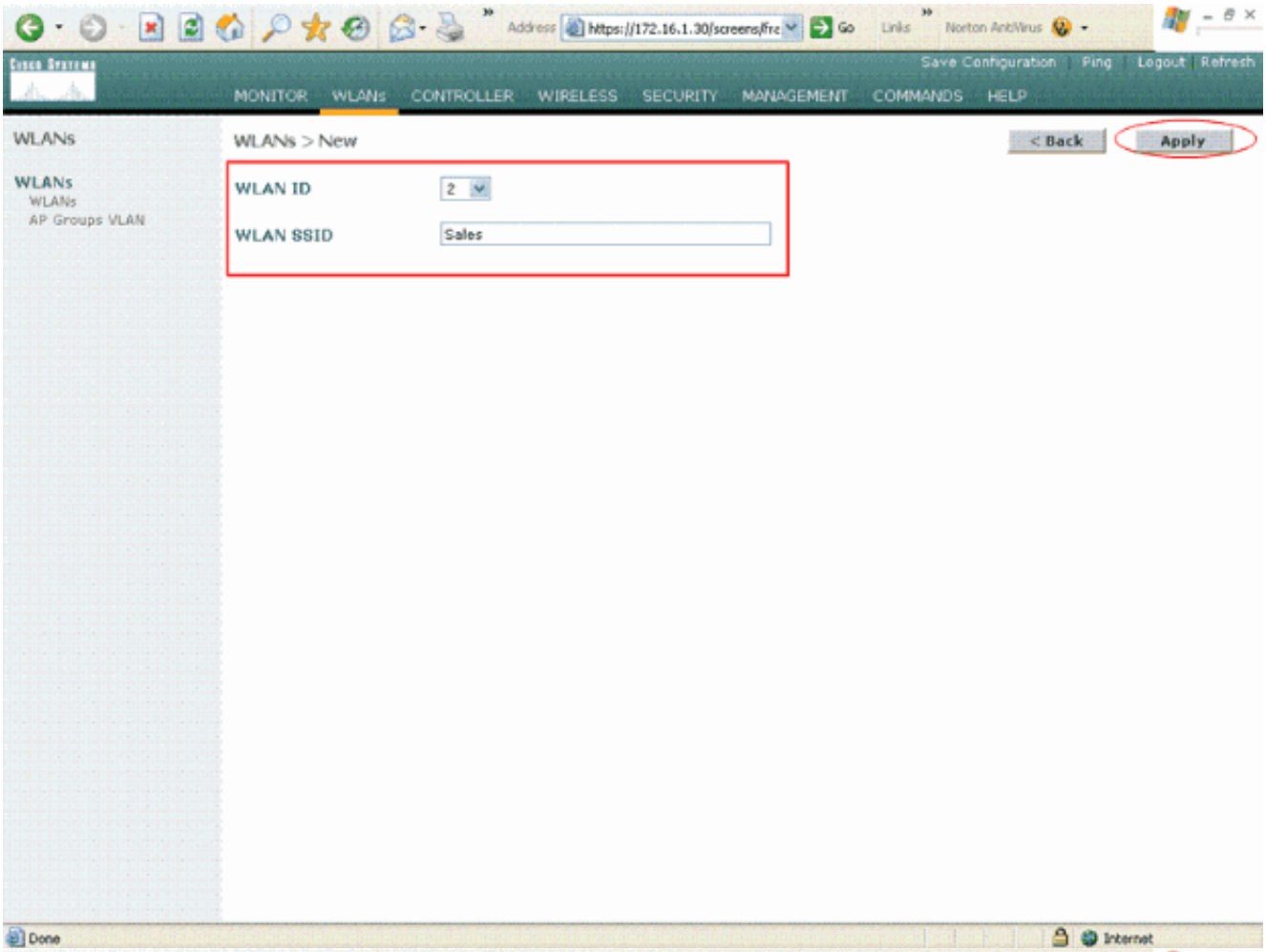
2. Configurar um WLAN para o departamento administrativo com SSID **Admin** e o outro WLAN para o departamento de vendas com **vendas** SSID. Termine estas etapas a fim fazer isto:Clique **WLAN do** controlador GUI a fim criar um WLAN. A janela WLANs aparece. Este indicador alista os WLAN configurados no controlador.Clique **novo** a fim configurar um WLAN novo.Este exemplo cria um **Admin** nomeado WLAN para o departamento administrativo e o ID de WLAN é **1.** cliques **aplica-se**.

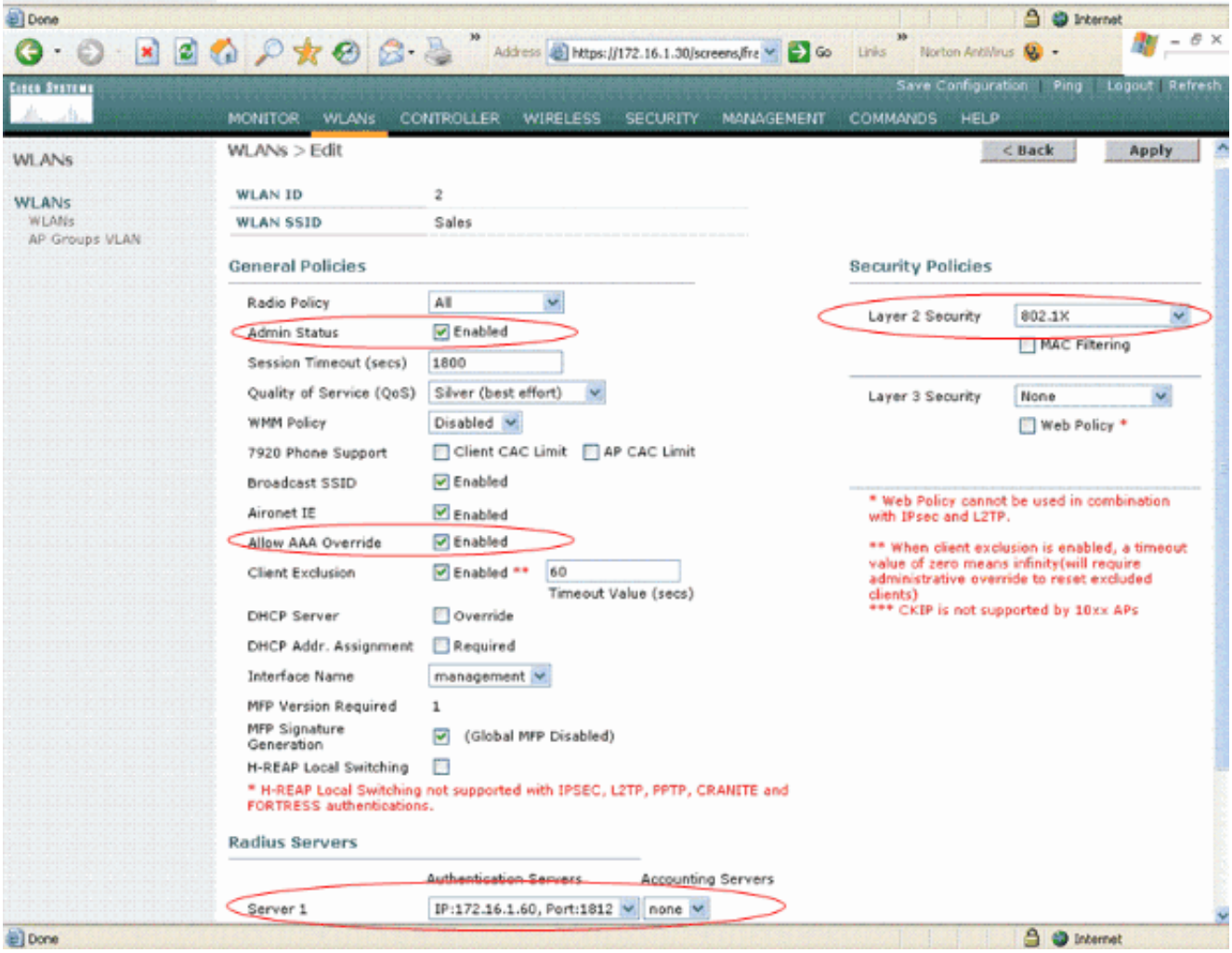


No o **WLAN > edita o** indicador, define os parâmetros específicos ao WLAN:Do menu de destruição da Segurança da camada 2, selecione o **802.1x**. À revelia, a opção de segurança da camada 2 é 802.1x. Isto permite a autenticação 802.1x/EAP para o WLAN.Sob políticas gerais, verifique a caixa da **ultrapassagem AAA**. Quando a ultrapassagem AAA está permitida, e um cliente tem parâmetros de autenticação de oposição AAA e de controlador WLAN, a authenticação do cliente está executada pelo servidor AAA.Selecione o servidor Radius apropriado do menu de destruição sob servidores Radius. Os outros parâmetros podem ser alterados basearam na exigência da rede de WLAN. Clique em Apply.



Similarmente, a fim criar um WLAN para o departamento de vendas, repita as etapas b e C. Estão aqui os
screenshots.


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

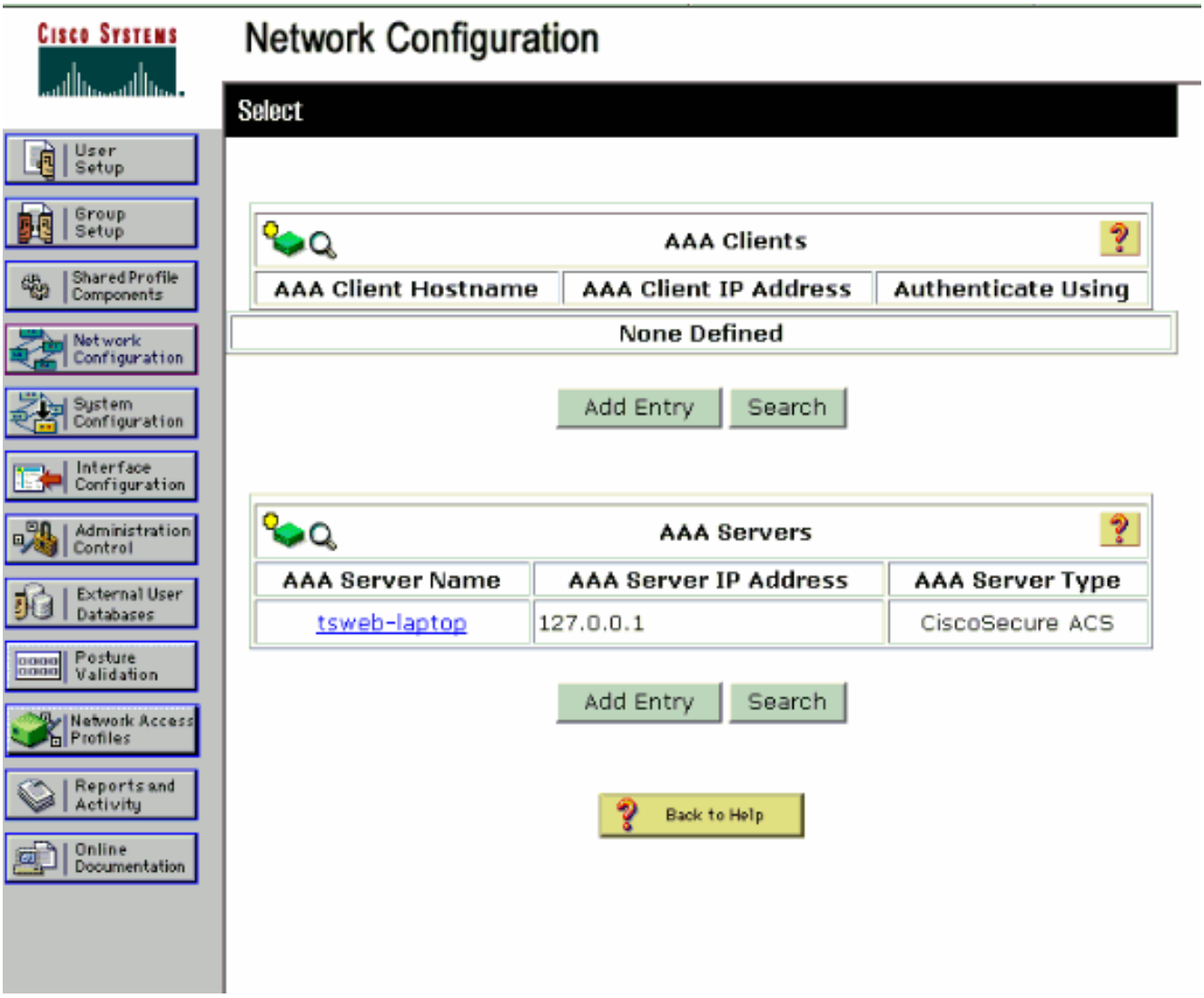
Configurar o Cisco Secure ACS

No server do Cisco Secure ACS você precisa:

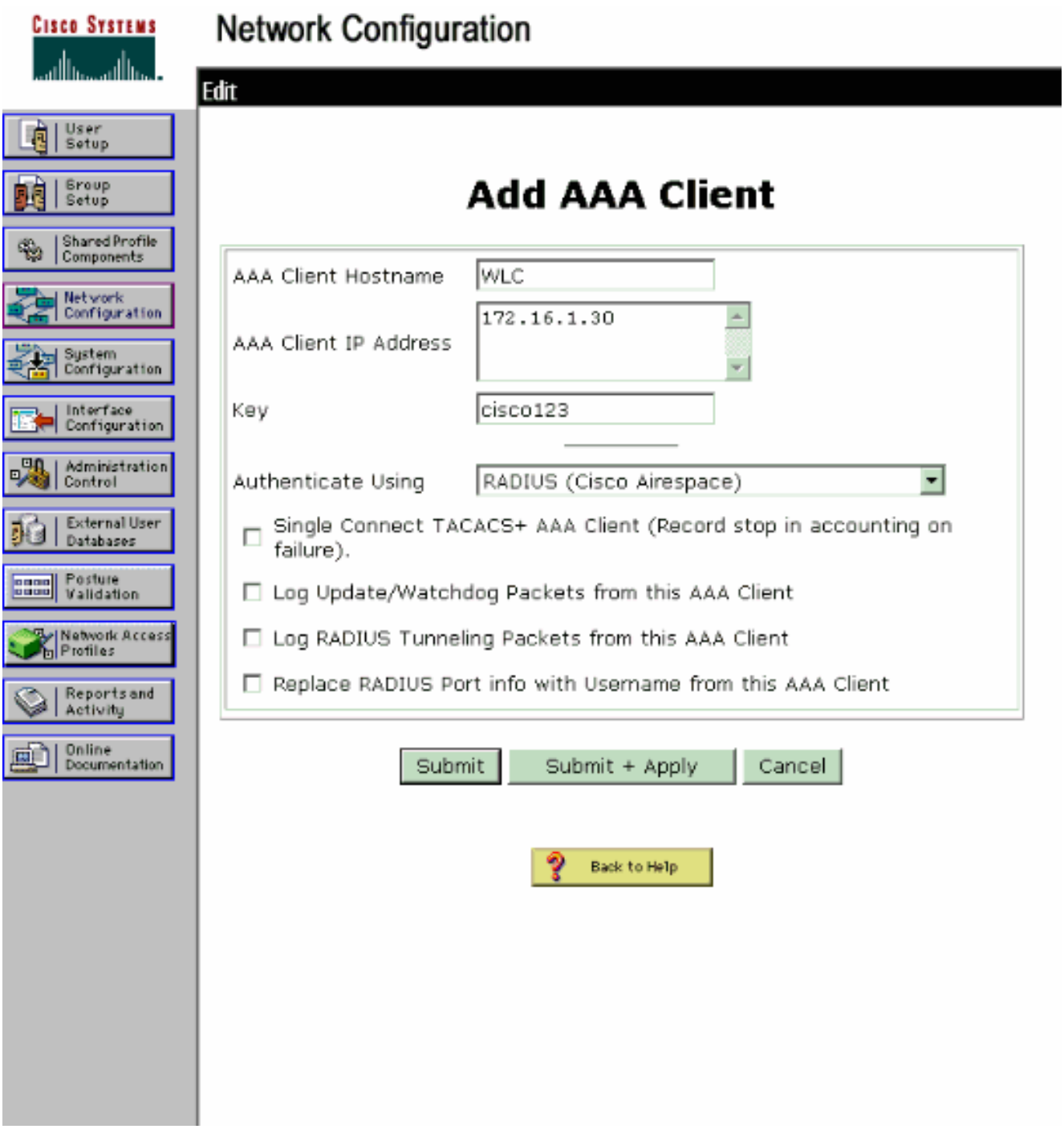
1. Configurar o WLC como um cliente de AAA.
2. Crie a base de dados de usuário e defina o NAR para a autenticação SSID-baseada.
3. Permita a autenticação de EAP.

Termine estas etapas no Cisco Secure ACS:

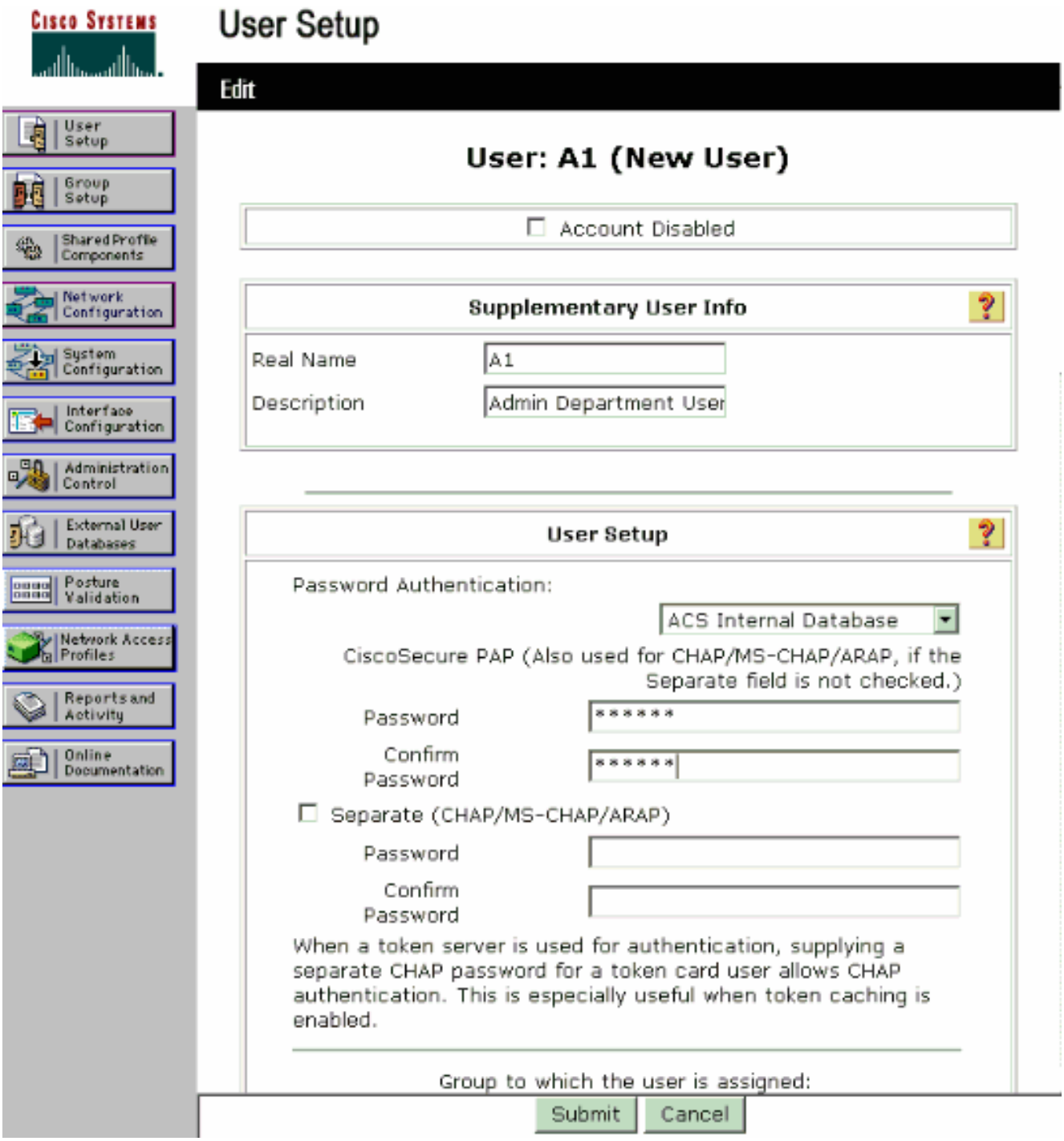
1. A fim definir o controlador como um cliente de AAA no servidor ACS, clique a **configuração de rede do** ACS GUI. Sob clientes de AAA clique sobre a **entrada Add**.



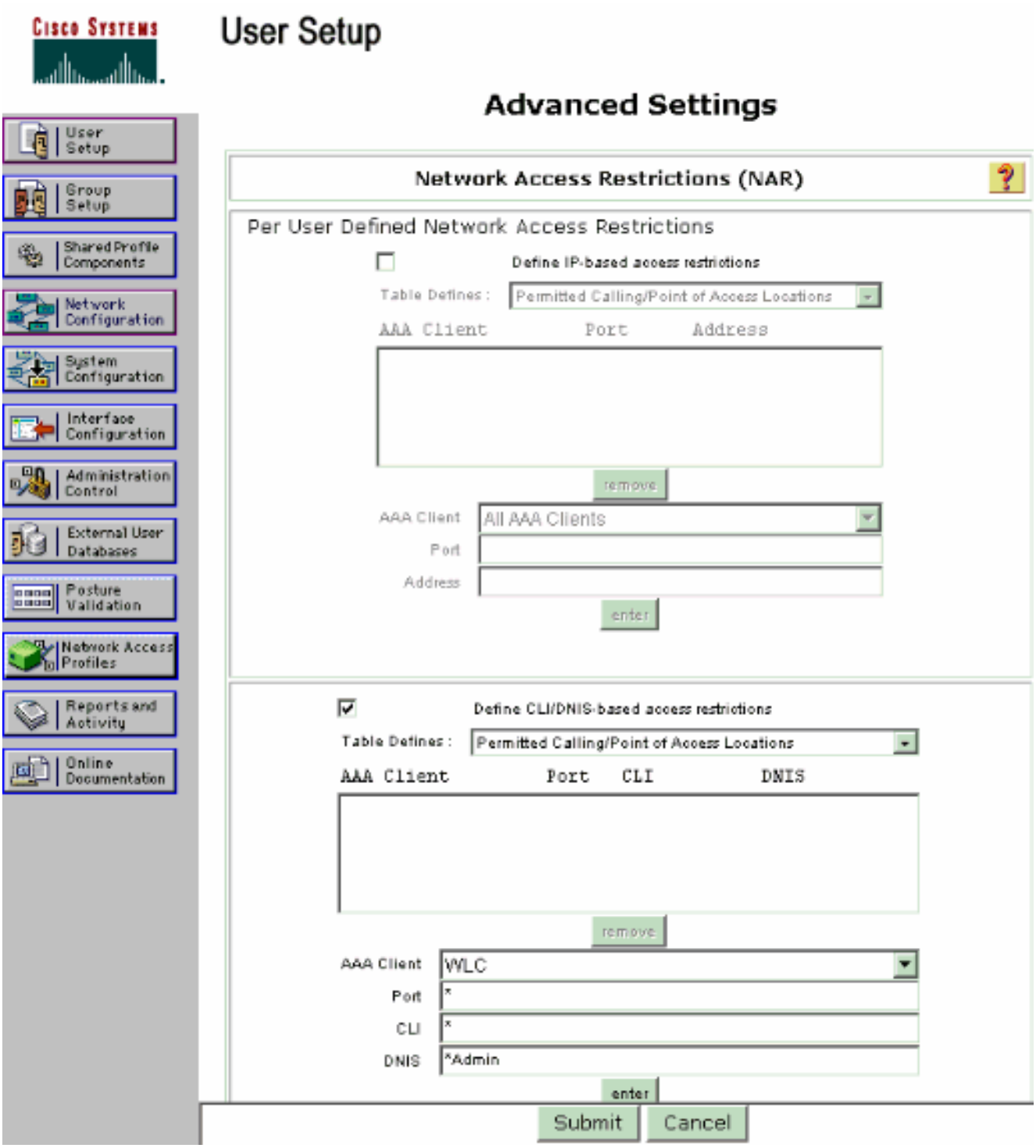
2. Quando a página da configuração de rede se publica, defina o nome do WLC, do IP address, do segredo compartilhado e do método de autenticação (RAIO Cisco Airespace).



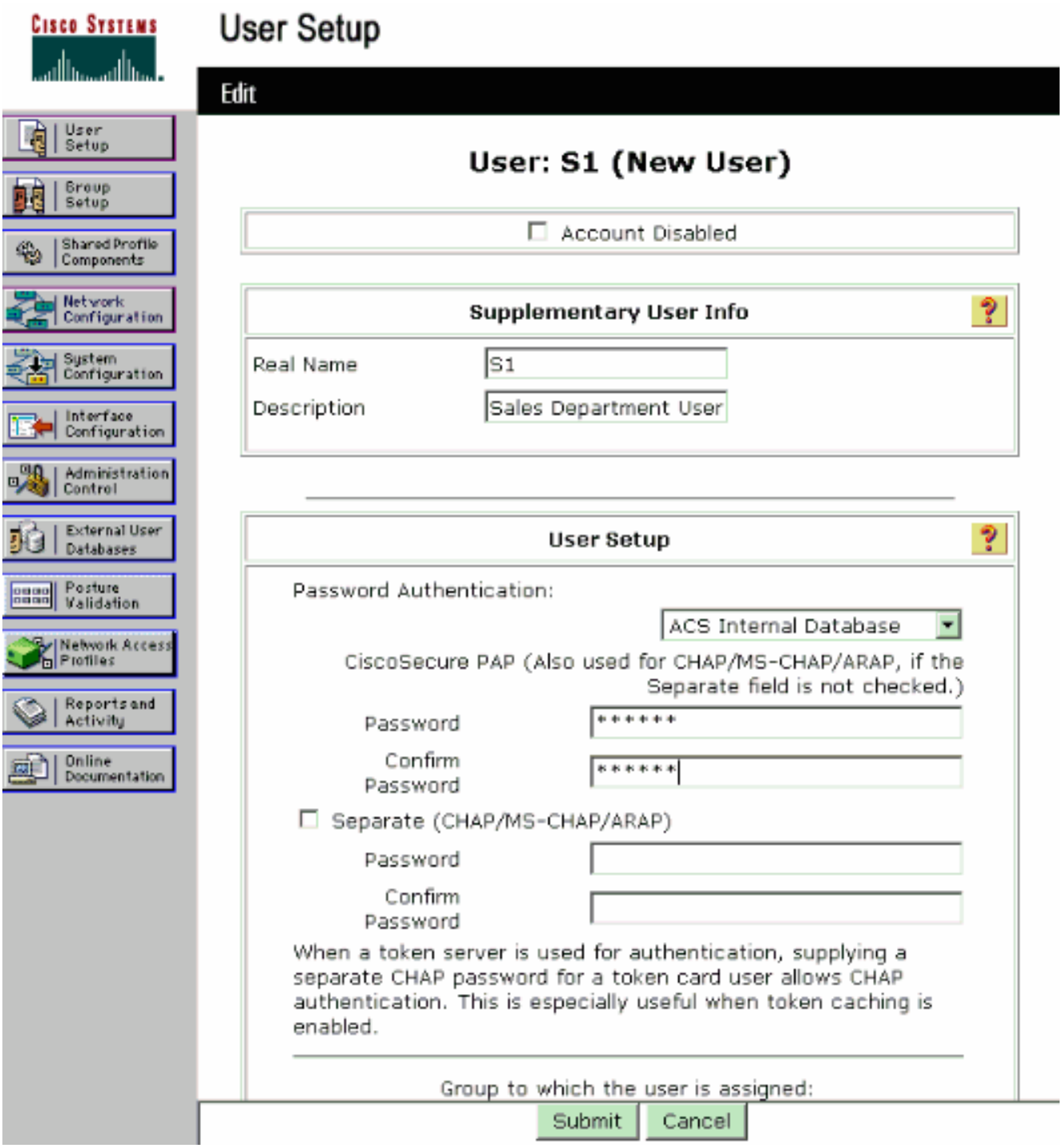
3. Clique a **instalação de usuário do** ACS GUI, incorpore o username, e o clique **adiciona/edita**. Neste exemplo o usuário é A1.
4. Quando a página da instalação de usuário se publica, defina todos os parâmetros específicos ao usuário. Neste exemplo o username, a senha e a informação de usuário suplementar são configurados porque você precisa estes parâmetros para a autenticação de leap.

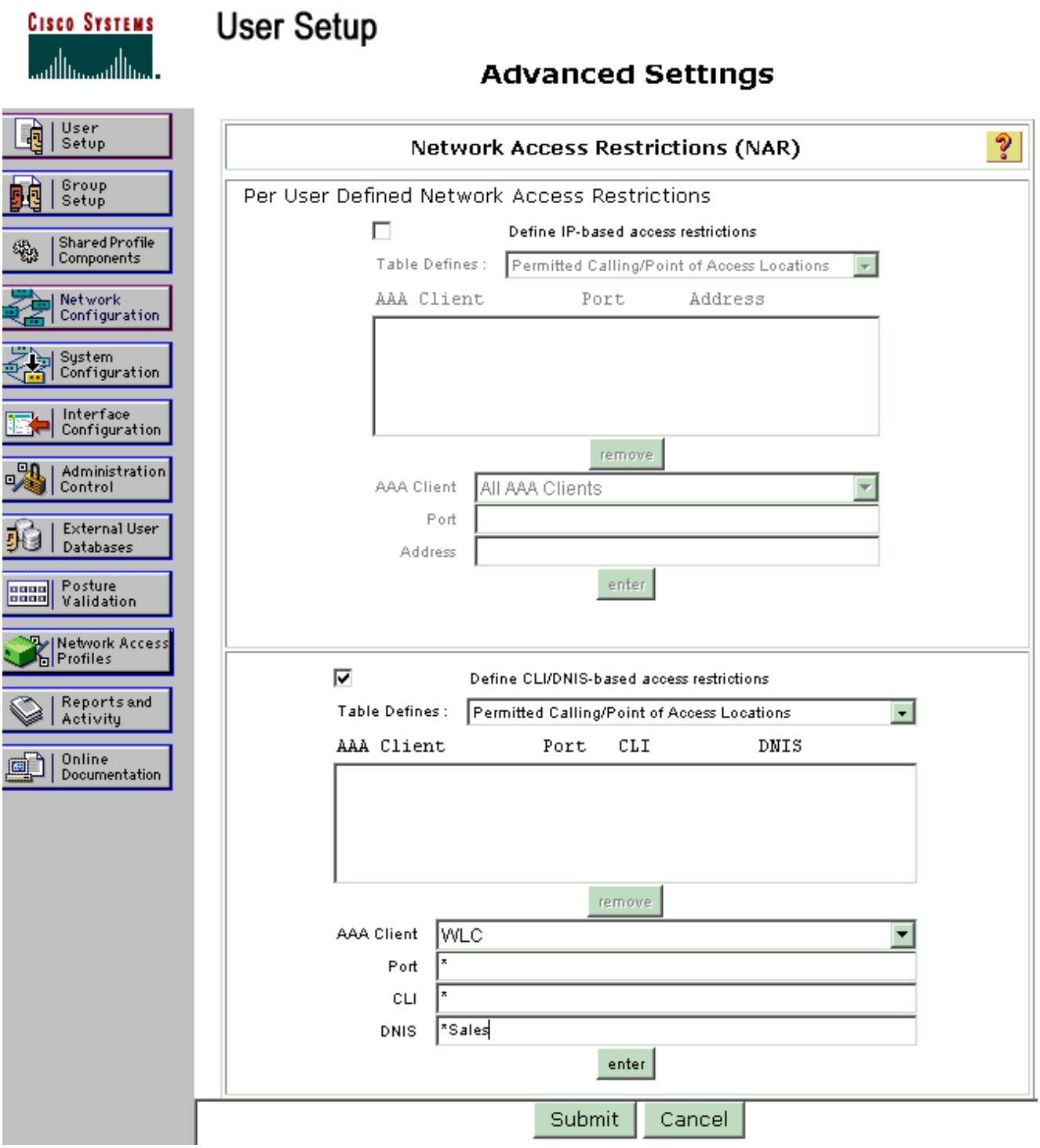


5. Enrole para baixo a página da instalação de usuário, até que você ver a seção das limitações do acesso de rede. Sob a interface do utilizador da restrição de acesso DNIS/CLI, o **Permitted Calling/Point of Access Locations** seleto e define estes parâmetros:**Cliente de AAA** — IP address WLC (172.16.1.30 em nosso exemplo)**Porta** — ***CLI** — ***DNIS** — *ssidname
6. O atributo DNIS define o SSID que é permitido ao usuário alcançar. O WLC envia o SSID no atributo DNIS ao servidor Radius.Se o usuário precisa de alcançar somente o Admin nomeado WLAN, entre no ***Admin** para o campo DNIS. Isto assegura-se de que o usuário tenha o acesso somente ao Admin nomeado WLAN. O clique **entra**.**Nota:** O SSID deve sempre ser precedido com ***.** É
imperativo.

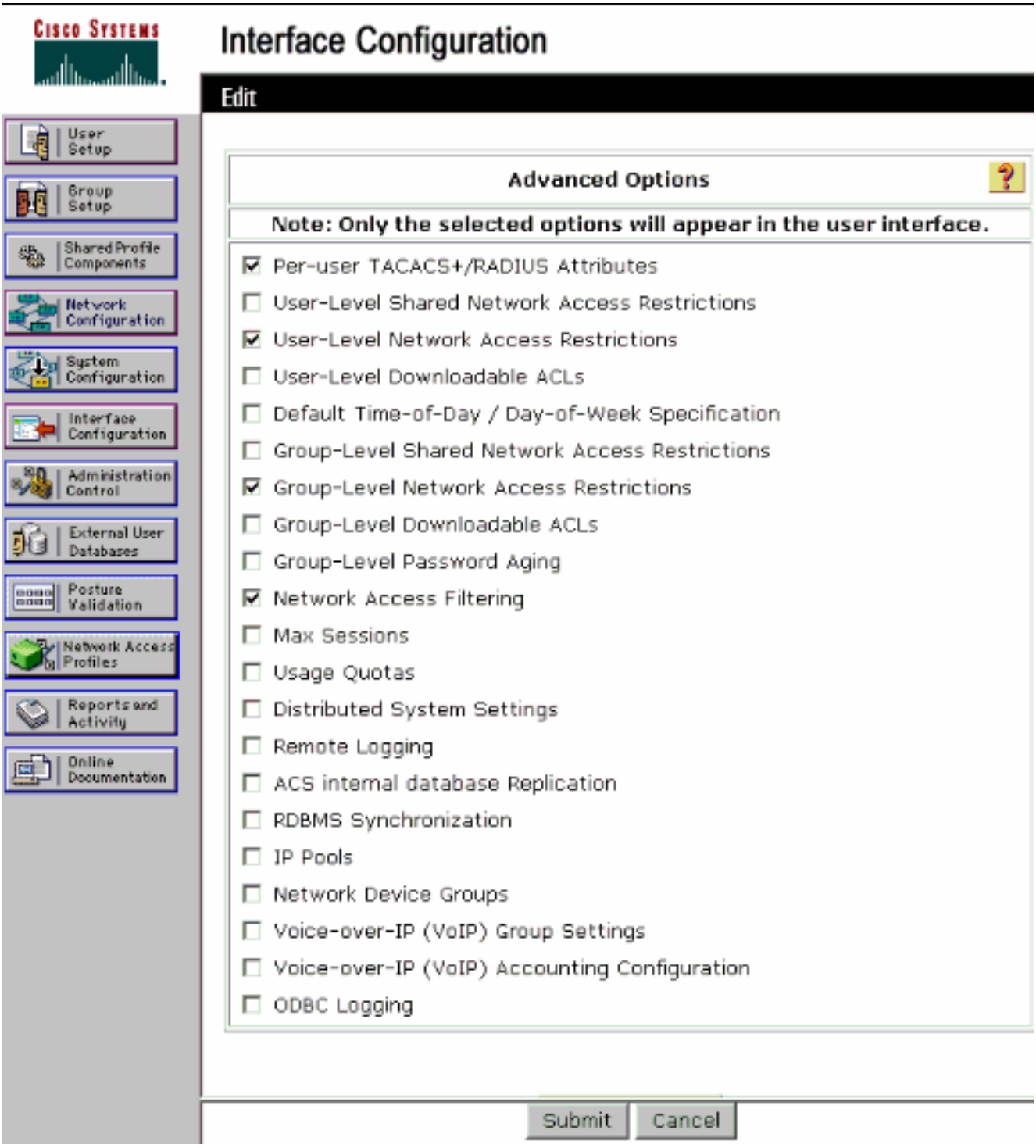


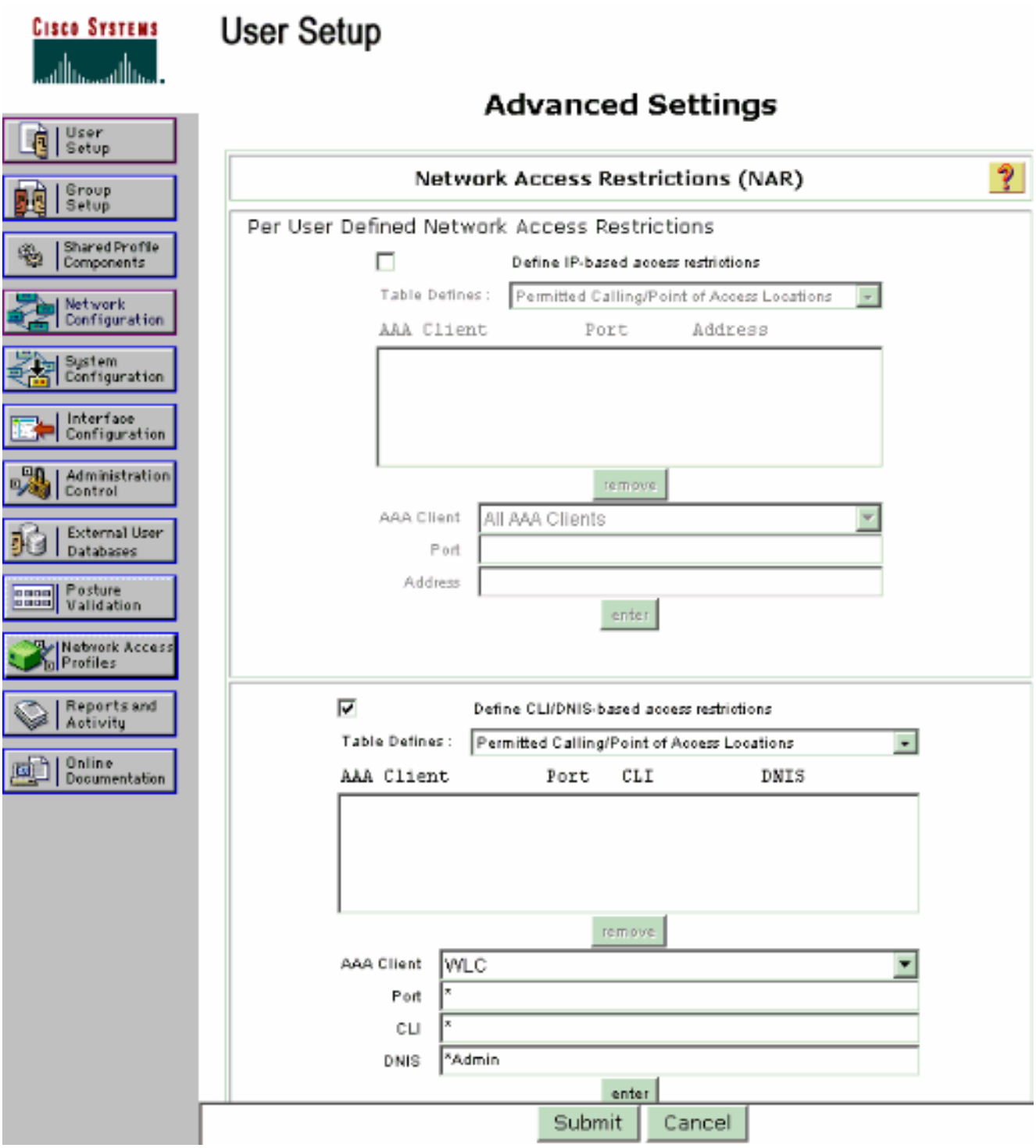
7. Clique em Submit.
8. Similarmente, crie um usuário para o usuário do departamento de vendas. Estão aqui os screenshots.


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

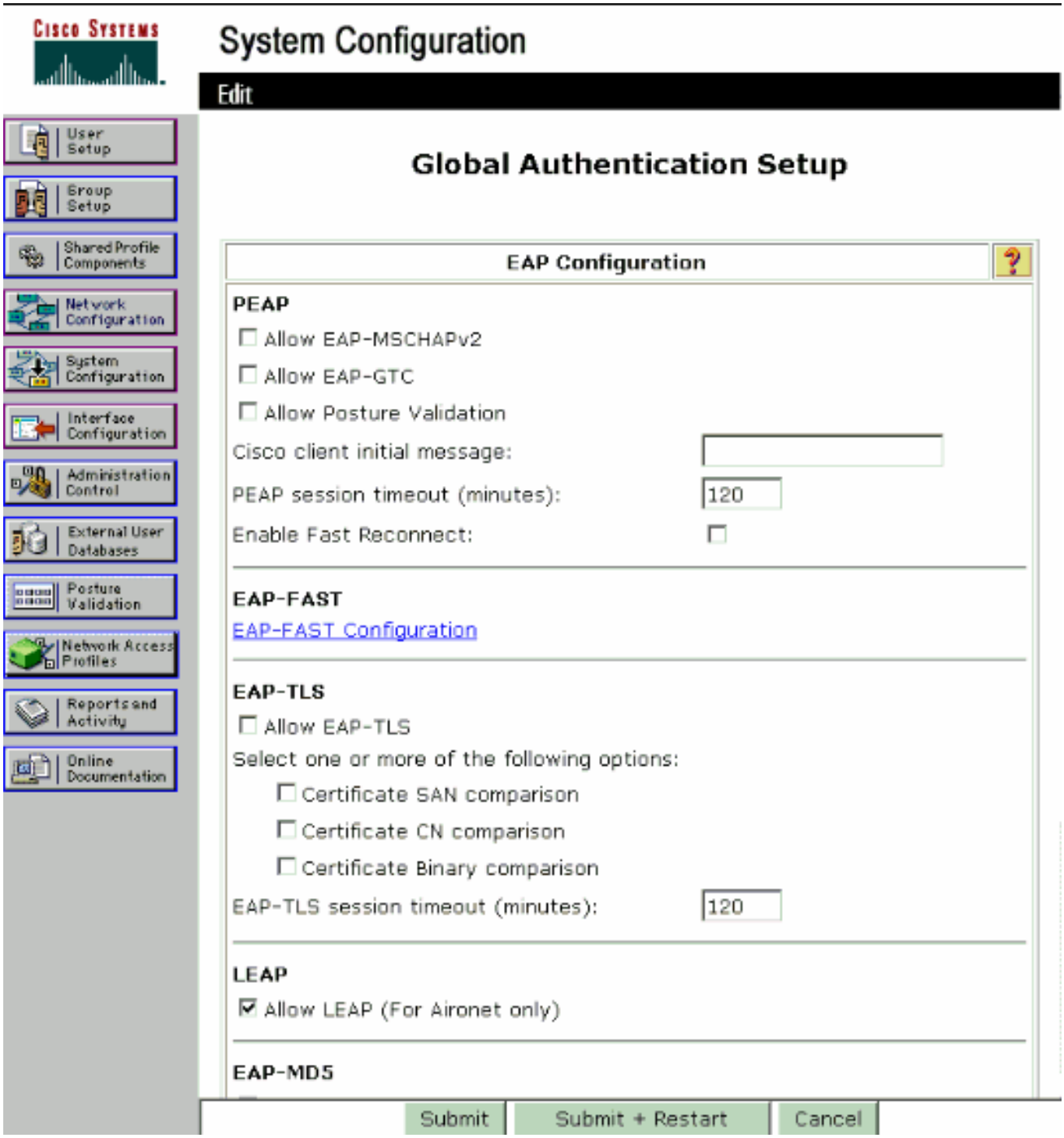


9. Repita o mesmo processo para adicionar mais usuários ao base de dados.**Nota:** Todos os usuários são agrupados à revelia sob o grupo padrão. Se você quer atribuir usuários específicos aos grupos diferentes, refira a seção de gerenciamento do grupo de usuário do Guia do Usuário para o server 3.2 do Cisco Secure ACS for Windows.**Nota:** Se você não vê a seção das limitações do acesso de rede no indicador da instalação de usuário, pôde ser porque não é permitido. A fim permitir as limitações do acesso de rede para usuários, para escolher **relações > avançou opções do** ACS GUI, **limitações** seletas do **acesso de rede do nível de usuário** e o clique **submete-se**. Isto permite o NAR e aparece no indicador da instalação de
usuário.


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. A fim permitir a autenticação de EAP, a **configuração de sistema do** clique e a **autenticação global Setup** a fim assegurar-se de que o Authentication Server esteja configurado para executar o método de autenticação de EAP desejado.Sob o EAP os ajustes de configuração selecionam o método de EAP apropriado. Este exemplo usa a autenticação de leap. O clique **submete-se** quando você é feito.

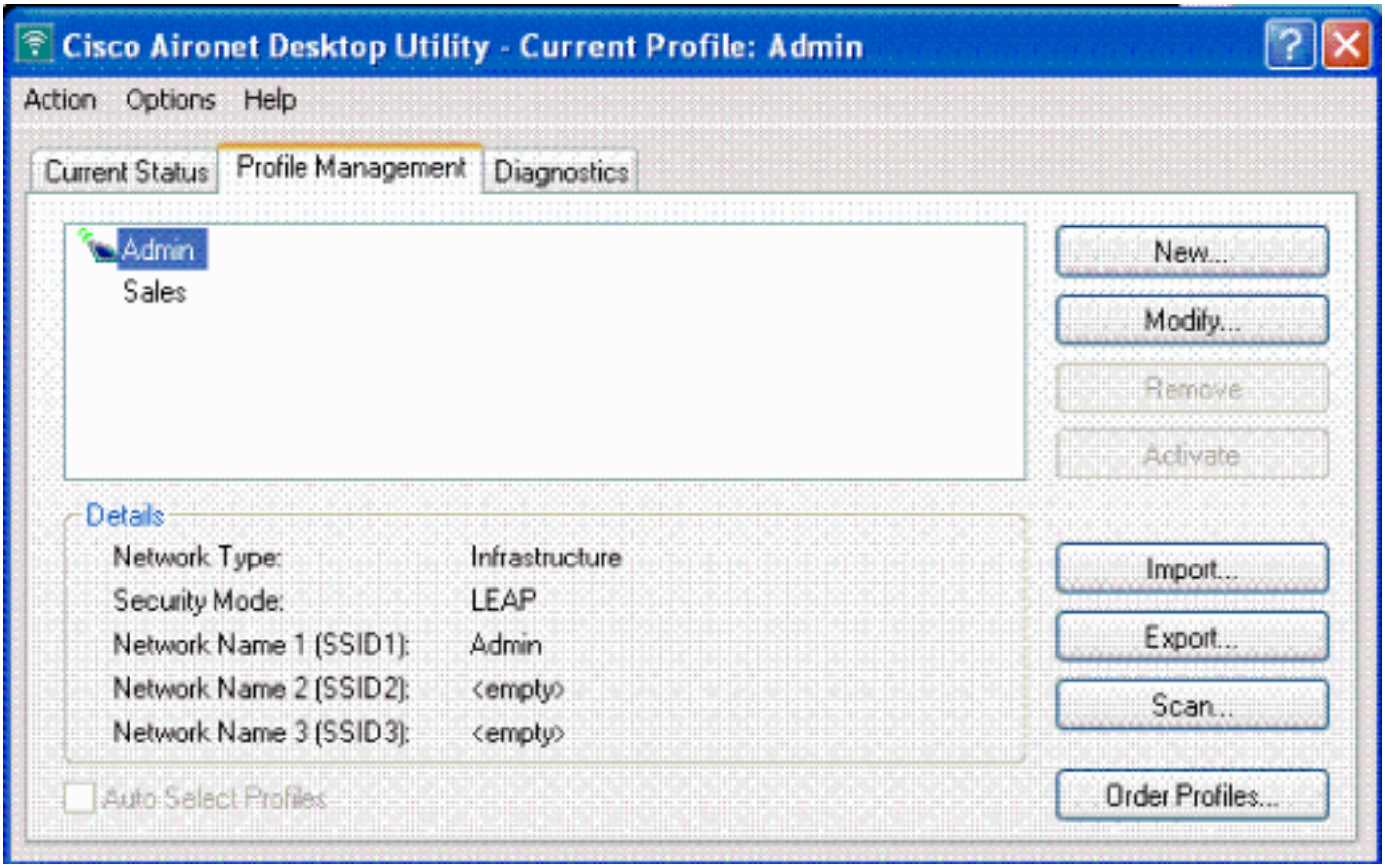


Configurar o cliente Wireless e verifique-o

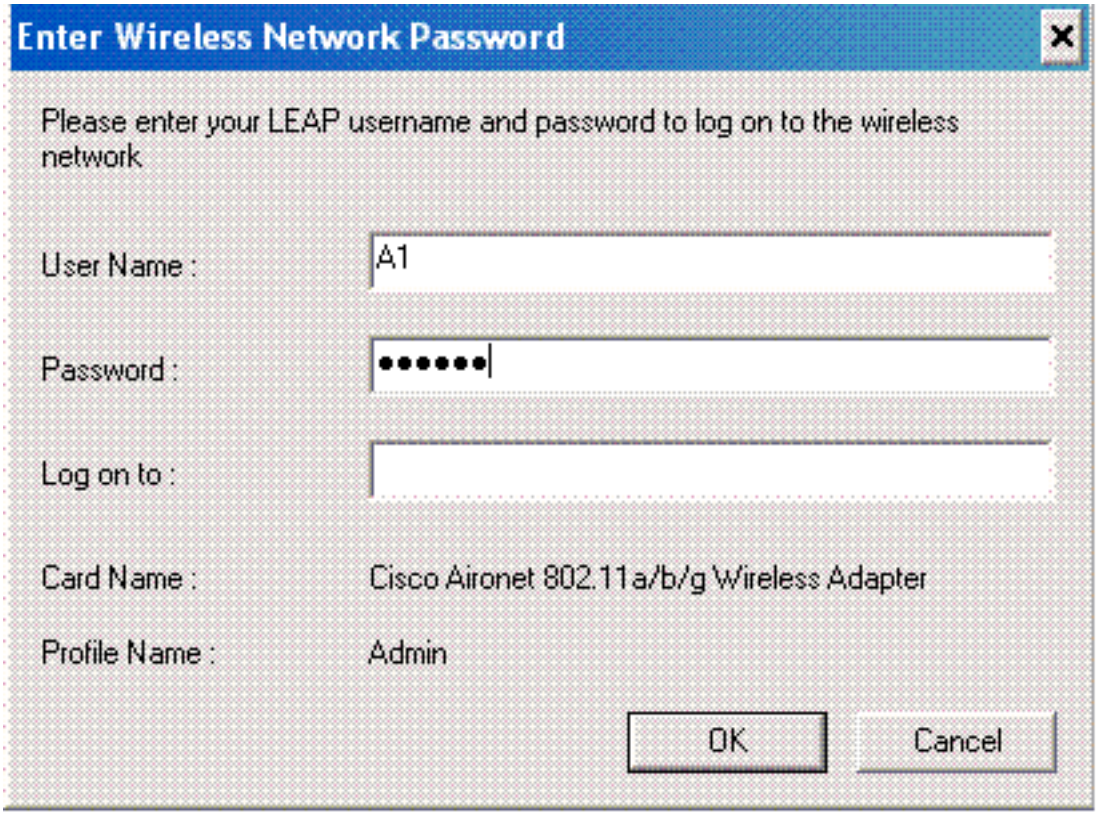
Use esta seção para confirmar se a sua configuração funciona corretamente. Tente associar um cliente Wireless com o REGAÇO usando a autenticação de leap para verificar se a configuração trabalha como esperado.

Nota: Este original supõe que o perfil do cliente está configurado para a autenticação de leap. Refira a utilização da autenticação de EAP para obter informações sobre de como configurar o adaptador de cliente Wireless do a/b/g do 802.11 para a autenticação de leap.

Nota: Do ADU você vê que você configurou dois perfis do cliente. Um para os usuários do departamento administrativo com SSID **Admin** e o outro perfil para os usuários do departamento de vendas com **vendas** SSID. Ambos os perfis são configurados para a autenticação de leap.



Quando o perfil para o usuário Wireless do departamento administrativo é ativado, o usuário está pedido para fornecer o username/senha para a autenticação de leap. Aqui está um exemplo:

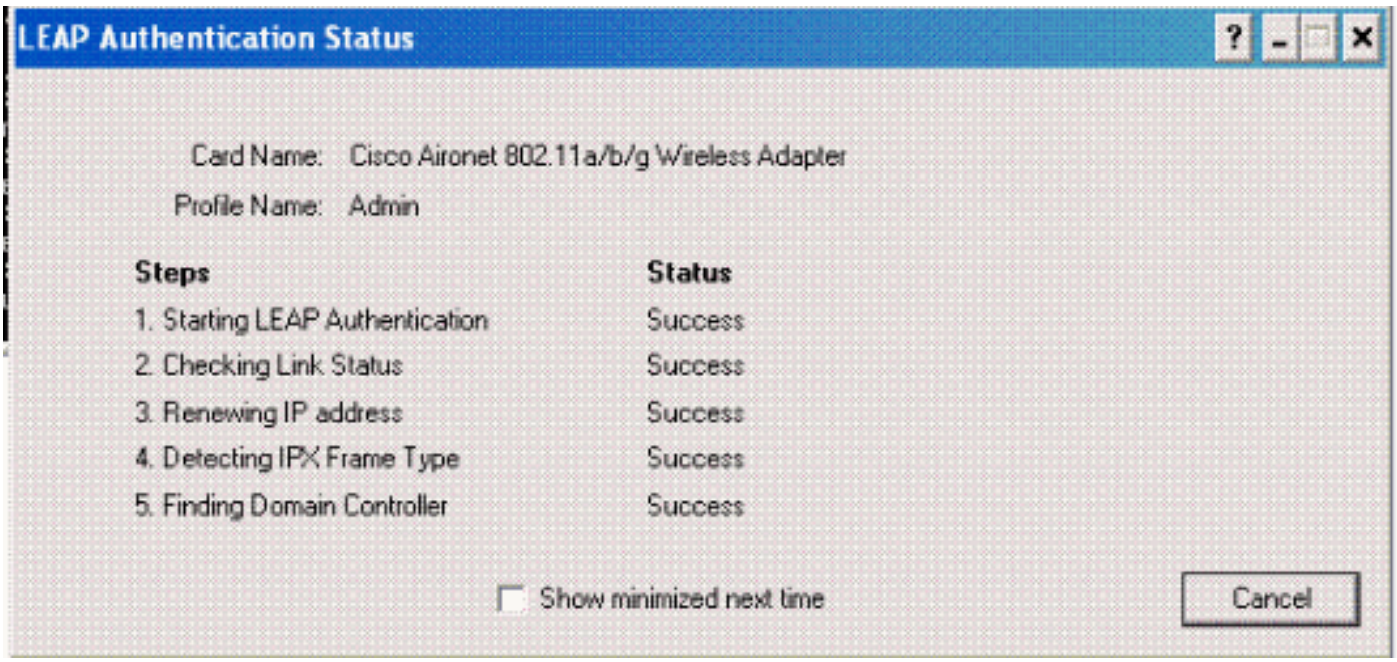


O REGAÇO e então o WLC passa sobre as credenciais do usuário ao servidor de raio externo (Cisco Secure ACS) para validar as credenciais. O WLC passa sobre as credenciais que incluem o atributo DNIS (nome SSID) ao servidor Radius para a validação.

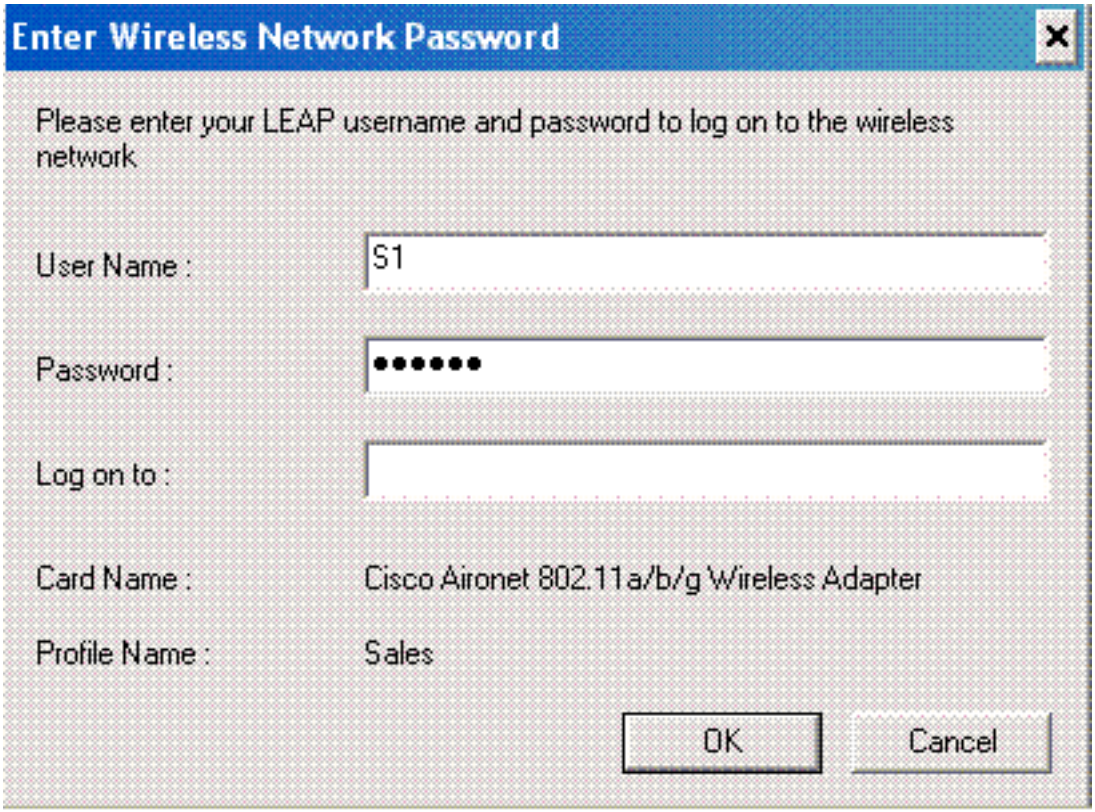
O servidor Radius verifica as credenciais do usuário comparando os dados com a base de dados

de usuário (e os NAR) e fornece o acesso ao cliente Wireless sempre que as credenciais do usuário são válidas.

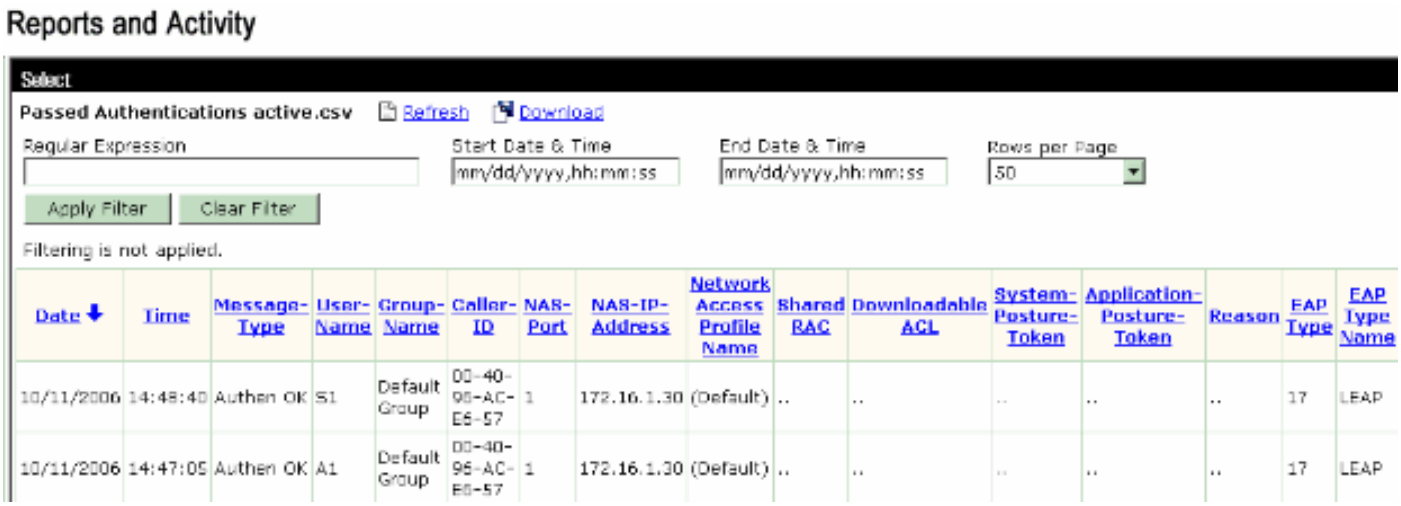
Em cima da autenticação RADIUS bem sucedida o cliente Wireless associa com o REGAÇO.



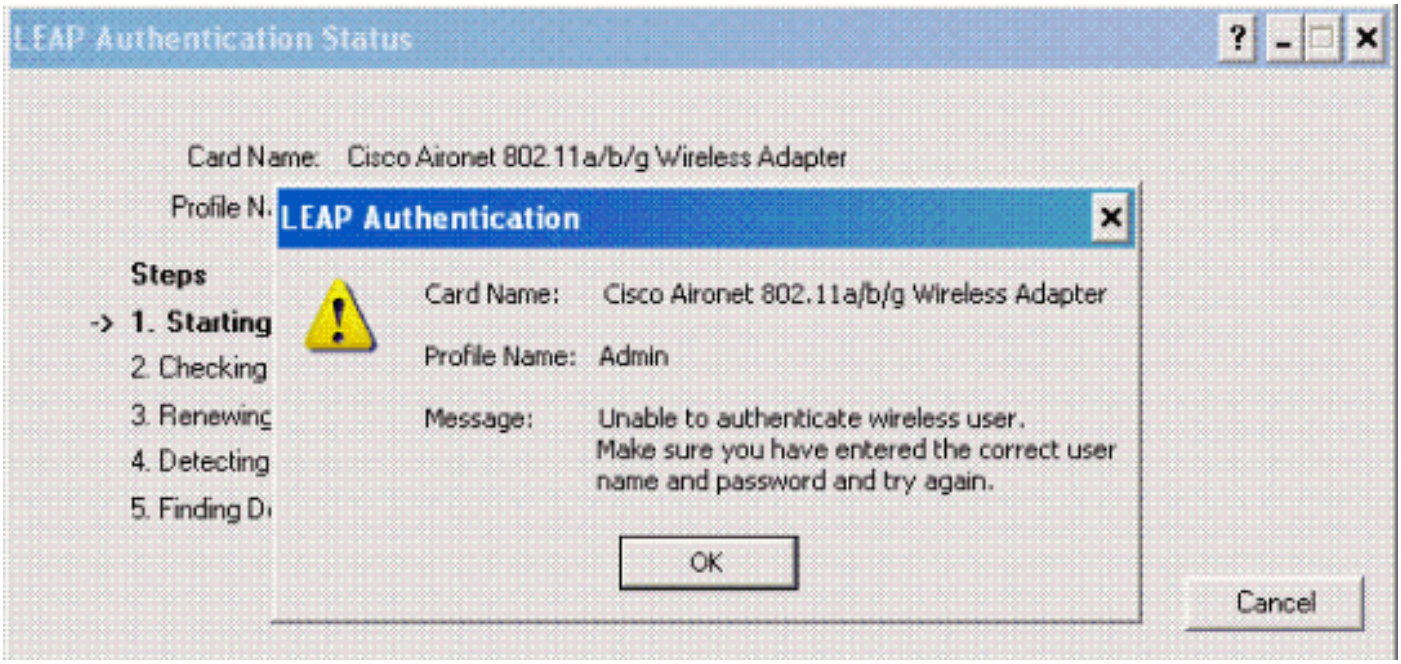
Similarmente quando um usuário do departamento de vendas ativa o perfil das vendas, o usuário é autenticado pelo servidor Radius baseado no username do PULO/senha e no SSID.



O relatório passado da autenticação no servidor ACS mostra que o cliente passou a autenticação RADIUS (autenticação de EAP e autenticação SSID). Aqui está um exemplo:



Agora, se o usuário das vendas tenta alcançar o **Admin** SSID, o servidor Radius nega o acesso de usuário ao WLAN. Aqui está um exemplo:



Esta maneira que os usuários podem ser acesso restrito baseou no SSID. Em um ambiente de empreendimento, todos os usuários que caem em um departamento específico podem ser agrupados em um únicos grupo e acesso ao WLAN podem ser fornecidos basearam no SSID que se usam como explicado neste original.

Troubleshooting

Comandos para Troubleshooting

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

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

- **debugar o dot1x aaa permitem** — Permite debugar de interações do 802.1x AAA.
- **debugar o pacote do dot1x permitem** — Permite debugar de todos os pacotes do dot1x.

- **debugar o aaa que todos permitem** — Configura debugar de todos os mensagens AAA.

Você pode igualmente usar o relatório passado da autenticação e o relatório da autenticação falha no server do Cisco Secure ACS a fim pesquisar defeitos a configuração. Estes relatórios estão sob os **relatórios e a janela de atividade no** ACS GUI.

Informações Relacionadas

- Autenticação de EAP com exemplo de configuração dos controladores de WLAN (WLC)
- Exemplo de configuração de autenticação da Web para o controlador da LAN sem fio
- Grupo VLAN AP com exemplo de configuração dos controladores do Wireless LAN
- Página de Suporte Wireless
- Suporte Técnico e Documentação - Cisco Systems