

# IPsec entre um VPN 3000 Concentrator e um VPN Client 4.x para Windows usando RADIUS para autenticação de usuário e exemplo de configuração de contabilidade

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Conventions](#)

[Configurar](#)

[Diagrama de Rede](#)

[Usar grupos no VPN 3000 Concentrator](#)

[Como o VPN 3000 Concentrator usa os atributos de grupo e de usuário](#)

[Configuração do VPN 3000 Series Concentrator](#)

[Configuração de servidor RADIUS](#)

[Atribuir um endereço IP estático ao usuário do cliente VPN](#)

[Configuração de cliente de VPN](#)

[Adicionar relatório](#)

[Verificar](#)

[Verificar o VPN Concentrator](#)

[Verificar o VPN Client](#)

[Troubleshoot](#)

[Solucionar problemas do VPN Client 4.8 para Windows](#)

[Informações Relacionadas](#)

## [Introduction](#)

Este documento descreve como estabelecer um túnel IPsec entre um Cisco VPN 3000 Concentrator e um Cisco VPN Client 4.x para Microsoft Windows que usa RADIUS para autenticação e tarifação do usuário. Este documento recomenda o Cisco Secure Access Control Server (ACS) para Windows para uma configuração RADIUS mais fácil para autenticar usuários que se conectam a um VPN 3000 Concentrator. Um grupo em um VPN 3000 Concentrator é uma coleção de usuários tratados como uma única entidade. A configuração de grupos, ao contrário de usuários individuais, pode simplificar o gerenciamento do sistema e simplificar as tarefas de configuração.

Consulte [Exemplo de Configuração de Autenticação do PIX/ASA 7.x e Cisco VPN Client 4.x para Windows com Microsoft Windows 2003 IAS RADIUS](#) para configurar a conexão VPN de acesso

remoto entre um Cisco VPN Client (4.x para Windows) e o PIX 500 Series Security Appliance 7.x que usa um Serviço de Autenticação de Internet do Microsoft Windows 20003 (IAS) Servidor RADIUS.

Consulte [Configurando o IPsec entre um Cisco IOS Router e um Cisco VPN Client 4.x para Windows usando RADIUS para autenticação de usuário](#) para configurar uma conexão entre um roteador e o Cisco VPN Client 4.x que usa RADIUS para autenticação de usuário.

## Prerequisites

### Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- O Cisco Secure ACS para Windows RADIUS está instalado e opera corretamente com outros dispositivos.
- O Cisco VPN 3000 Concentrator é configurado e pode ser gerenciado com a interface HTML.

### Componentes Utilizados

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

- Cisco Secure ACS para Windows com versão 4.0
- Cisco VPN 3000 Series Concentrator com arquivo de imagem 4.7.2.B
- Cisco VPN Client 4.x

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](#).

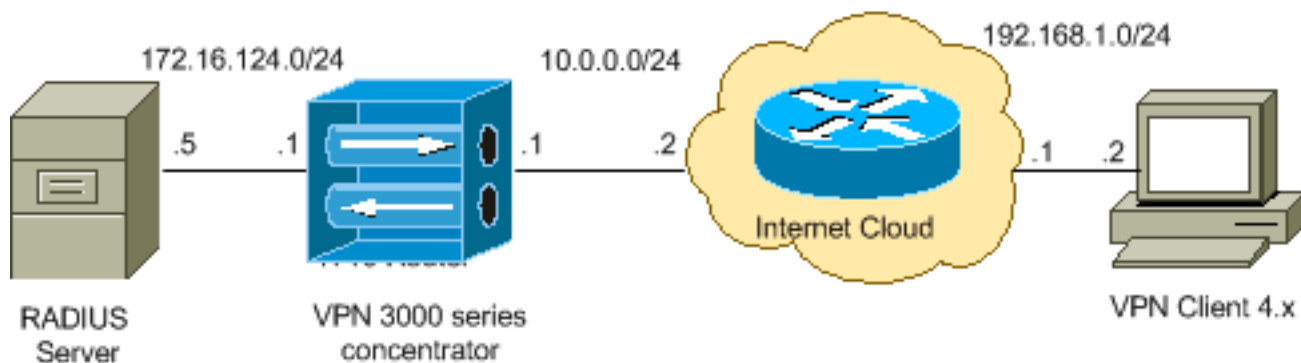
## Configurar

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 nesta seção.

### Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



**Observação:** os esquemas de endereçamento IP usados nesta configuração não são legalmente roteáveis na Internet. São endereços [RFC 1918](#) que foram usados em um ambiente de laboratório.

## Usar grupos no VPN 3000 Concentrator

Os grupos podem ser definidos para o Cisco Secure ACS for Windows e para o VPN 3000 Concentrator, mas usam grupos de forma um pouco diferente. Execute estas tarefas para simplificar as coisas:

- **Configure um único grupo no VPN 3000 Concentrator** para quando você estabelecer o túnel inicial. Isso é frequentemente chamado de Grupo de Túnel e é usado para estabelecer uma sessão criptografada do Internet Key Exchange (IKE) para o VPN 3000 Concentrator usando uma chave pré-compartilhada (a senha do grupo). Esse é o mesmo nome de grupo e senha que devem ser configurados em todos os Cisco VPN Clients que desejam se conectar ao VPN Concentrator.
- **Configure grupos no servidor Cisco Secure ACS for Windows** que usam atributos RADIUS padrão e atributos específicos do fornecedor (VSAs) para gerenciamento de políticas. Os VSAs que devem ser usados com o VPN 3000 Concentrator são os atributos RADIUS (VPN 3000).
- **Configure os usuários no servidor Cisco Secure ACS for Windows RADIUS e atribua-os a um dos grupos** configurados no mesmo servidor. Os usuários herdam atributos definidos para seu grupo e o Cisco Secure ACS for Windows envia esses atributos ao VPN Concentrator quando o usuário é autenticado.

## Como o VPN 3000 Concentrator usa os atributos de grupo e de usuário

Depois que o VPN 3000 Concentrator autentica o Grupo de Túneis com o VPN Concentrator e o usuário com RADIUS, ele deve organizar os atributos que recebeu. O VPN Concentrator usa os atributos nessa ordem de preferência, seja a autenticação feita no VPN Concentrator ou com RADIUS:

1. **Atributos do usuário** — esses atributos sempre têm precedência sobre quaisquer outros.
2. **Atributos do Grupo de Túneis** — Todos os atributos não retornados quando o usuário foi autenticado são preenchidos pelos atributos do Grupo de Túneis.
3. **Atributos do grupo base** — Todos os atributos ausentes dos atributos do usuário ou do grupo de túnel são preenchidos pelos atributos do grupo base do concentrador VPN.

## Configuração do VPN 3000 Series Concentrator

Conclua o procedimento nesta seção para configurar um Cisco VPN 3000 Concentrator para os parâmetros necessários para a conexão IPsec, bem como o cliente AAA para que o usuário VPN autentique com o servidor RADIUS.

Nesta configuração de laboratório, o VPN Concentrator é acessado primeiro através da porta de console e uma configuração mínima é adicionada como esta saída mostra:

```
Login: admin
!--- The password must be "admin". Password:***** Welcome to Cisco Systems VPN 3000 Concentrator
Series Command Line Interface Copyright (C) 1998-2005 Cisco Systems, Inc. 1) Configuration 2)
Administration 3) Monitoring 4) Save changes to Config file 5) Help Information 6) Exit Main ->
1 1) Interface Configuration 2) System Management 3) User Management 4) Policy Management 5)
Tunneling and Security 6) Back Config -> 1 This table shows current IP addresses. Intf Status IP
Address/Subnet Mask MAC Address -----
----- Ether1-Pri| DOWN | 10.1.1.1/255.255.255.0 | 00.03.A0.89.BF.D0 Ether2-Pub|Not
Configured| 0.0.0.0/0.0.0.0 | Ether3-Ext|Not Configured| 0.0.0.0/0.0.0.0 | -----
----- DNS Server(s): DNS Server Not
Configured DNS Domain Name: Default Gateway: Default Gateway Not Configured 1) Configure
Ethernet #1 (Private) 2) Configure Ethernet #2 (Public) 3) Configure Ethernet #3 (External) 4)
Configure Power Supplies 5) Back Interfaces -> 1 1) Interface Setting (Disable, DHCP or Static
IP) 2) Set Public Interface 3) Select IP Filter 4) Select Ethernet Speed 5) Select Duplex 6) Set
MTU 7) Set Port Routing Config 8) Set Bandwidth Management 9) Set Public Interface IPsec
Fragmentation Policy 10) Set Interface WebVPN Parameters 11) Back Ethernet Interface 1 -> 1 1)
Disable 2) Enable using DHCP Client 3) Enable using Static IP Addressing Ethernet Interface 1 ->
[ ] 3 This table shows current IP addresses. Intf Status IP Address/Subnet Mask MAC Address ----
----- Ether1-Pri| DOWN |
10.1.1.1/255.255.255.0 | 00.03.A0.89.BF.D0 Ether2-Pub|Not Configured| 0.0.0.0/0.0.0.0 | Ether3-
Ext|Not Configured| 0.0.0.0/0.0.0.0 | -----
----- DNS Server(s): DNS Server Not Configured DNS Domain Name: Default Gateway:
Default Gateway Not Configured > Enter IP Address Ethernet Interface 1 -> [ 10.1.1.1 ]
172.16.124.1 20 02/14/2007 09:50:18.830 SEV=3 IP/2 RPT=3 IP Interface 1 status changed to Link
Down. 21 02/14/2007 09:50:18.830 SEV=3 IP/1 RPT=3 IP Interface 1 status changed to Link Up. 22
02/14/2007 09:50:18.950 SEV=3 IP/1 RPT=4 IP Interface 1 status changed to Link Up. > Enter
Subnet Mask 23 02/14/2007 09:50:19.460 SEV=3 IP/2 RPT=4 IP Interface 1 status changed to Link
Down. Ethernet Interface 1 -> [ 255.255.255.0 ] 1) Interface Setting (Disable, DHCP or Static
IP) 2) Set Public Interface 3) Select IP Filter 4) Select Ethernet Speed 5) Select Duplex 6) Set
MTU 7) Set Port Routing Config 8) Set Bandwidth Management 9) Set Public Interface IPsec
Fragmentation Policy 10) Set Interface WebVPN Parameters 11) Back Ethernet Interface 1 -> 11
This table shows current IP addresses. Intf Status IP Address/Subnet Mask MAC Address -----
----- Ether1-Pri| Up |
172.16.124.1/255.255.255.0 | 00.03.A0.89.BF.D0 Ether2-Pub|Not Configured| 0.0.0.0/0.0.0.0 |
Ether3-Ext|Not Configured| 0.0.0.0/0.0.0.0 | -----
----- DNS Server(s): DNS Server Not Configured DNS Domain Name: Default
Gateway: Default Gateway Not Configured 1) Configure Ethernet #1 (Private) 2) Configure Ethernet
#2 (Public) 3) Configure Ethernet #3 (External) 4) Configure Power Supplies 5) Back Interfaces -
>
```

O VPN Concentrator é exibido em Quick Configuration e esses itens são configurados.

- Hora/Data
- Interfaces/Masks in Configuration > Interfaces (public=10.0.0.1/24, private=172.16.124.1/24)
- Gateway padrão em Configuration > System > IP routing > Default\_Gateway (10.0.0.2)

Neste ponto, o VPN Concentrator é acessível por meio de HTML da rede interna.

**Observação:** se o VPN Concentrator for gerenciado de fora, você também executará estas etapas:

1. Escolha **Configuration > 1-Interfaces > 2-Public > 4-Select IP Filter > 1. Privado (Padrão).**
2. Escolha **Administration > 7-Access Rights > 2-Access Control List > 1-Add Manager**

**Workstation** para adicionar o endereço IP do gerenciador externo.

Essas etapas só são necessárias se você gerenciar o VPN Concentrador de fora.

Depois de concluir essas duas etapas, o restante da configuração pode ser feito através da GUI usando um navegador da Web e conectando-se ao IP da interface que você acabou de configurar. Neste exemplo e neste ponto, o VPN Concentrador é acessível por meio de HTML da rede interna:

1. Escolha **Configuration > Interfaces** para verificar novamente as interfaces depois de ativar a GUI.

Interface	Status	IP Address	Subnet Mask	MAC Address	Default Gateway
<a href="#">Ethernet 1 (Private)</a>	UP	172.16.124.1	255.255.255.0	00.03.A0.89.BF.D0	
<a href="#">Ethernet 2 (Public)</a>	UP	10.0.0.1	255.255.255.0	00.03.A0.89.BF.D1	10.0.0.2
<a href="#">Ethernet 3 (External)</a>	Not Configured	0.0.0.0	0.0.0.0		
<a href="#">DNS Server(s)</a>	DNS Server Not Configured				
<a href="#">DNS Domain Name</a>					

2. Conclua estes passos para adicionar o servidor Cisco Secure ACS for Windows RADIUS à configuração do VPN 3000 Concentrador. Escolha **Configuration > System > Servers > Authentication** e clique em **Add** no menu à esquerda.

Configure and add a user authentication server.

**Server Type**  Selecting *Internal Server* will let you add users to database. If you are using RADIUS authenticator additional authorization check, do not configure at

**Authentication Server**  Enter IP address or hostname.

**Used For**  Select the operation(s) for which this RADIUS se

**Server Port**  Enter 0 for default port (1645).

**Timeout**  Enter the timeout for this server (seconds).

**Retries**  Enter the number of retries for this server.

**Server Secret**  Enter the RADIUS server secret.

**Verify**  Re-enter the secret.

Escolha o tipo de servidor **RADIUS** e adicione esses parâmetros ao servidor Cisco Secure ACS for Windows RADIUS. Deixe todos os outros parâmetros em seu estado padrão. **Authentication Server** — Insira o endereço IP do servidor Cisco Secure ACS for

Windows RADIUS.**Server Secret** — Insira o segredo do servidor RADIUS. Esse deve ser o mesmo segredo que você usa ao configurar o VPN 3000 Concentrator na configuração do Cisco Secure ACS for Windows.**Verify** — (Verificar) Insira novamente a senha para verificação. Isso adiciona o servidor de autenticação na configuração global do VPN 3000 Concentrator. Este servidor é usado por todos os grupos, exceto quando um servidor de autenticação foi especificamente definido. Se um servidor de autenticação não estiver configurado para um grupo, ele será revertido para o servidor de autenticação global.

### 3. Conclua estes passos para configurar o Grupo de Túneis no VPN 3000

Concentrator. Escolha **Configuration > User Management > Groups** no menu esquerdo e clique em **Add**. Altere ou adicione esses parâmetros nas guias Configuração. Não clique em Aplicar até que você altere todos estes parâmetros: **Observação:** esses parâmetros são o mínimo necessário para conexões VPN de acesso remoto. Esses parâmetros também presumem que as configurações padrão no grupo base no VPN 3000 Concentrator não foram

alteradas. **Identidade**

Configuration | User Management | Groups | Add

This section lets you add a group. Check the **Inherit?** box to set a field that you want to default to the base group value. Uncheck the **Inherit?** box and enter a new value to override base group values.

Identity | General | IPsec | Client Config | Client FW | HW Client | PPTP/L2TP | WebVPN | NAC

Identity Parameters		
Attribute	Value	Description
Group Name	<input type="text" value="ipsecgroup"/>	Enter a unique name for the group.
Password	<input type="password"/>	Enter the password for the group.
Verify	<input type="password"/>	Verify the group's password.
Type	<input type="text" value="Internal"/>	<i>External</i> groups are configured on an external authentication server (e.g. RADIUS). <i>Internal</i> groups are configured on the VPN 3000 Concentrator's Internal Database.

**Nome do grupo** — Digite um nome de grupo. Por exemplo, IPsecUsers. **Senha** — Insira uma senha para o grupo. Esta é a chave pré-compartilhada para a sessão IKE. **Verify** — (Verificar) Insira novamente a senha para verificação. **Tipo** — Deixe isso como padrão: Interno. **IPsec**



Check the **Inherit?** box to set a field that you want to default to the base group value. Uncheck the **Inherit?** box and enter

IPSec Parameters			
Attribute	Value	Inherit?	Description
IPSec SA	ESP-3DES-MD5	<input checked="" type="checkbox"/>	Select the group's IPSec Security Association.
IKE Peer Identity Validation	If supported by certificate	<input checked="" type="checkbox"/>	Select whether or not to validate the identity.
IKE Keepalives	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Check to enable the use of IKE keepalives.
Confidence Interval	300	<input checked="" type="checkbox"/>	(seconds) Enter how long a peer is permitted to remain idle before the peer is checked to see if it is still connected.
Tunnel Type	Remote Access	<input checked="" type="checkbox"/>	Select the type of tunnel for this group. Updates are needed.
Remote Access Parameters			
Group Lock	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Lock users into this group.
Authentication	RADIUS	<input type="checkbox"/>	Select the authentication method for members. This method does not apply to <b>Individual User Authentication</b> .
Authorization Type	None	<input checked="" type="checkbox"/>	If members of this group need authorization, select the authorization method. If you configure this method, you must also configure an Authorization Server.

**Tipo de túnel**—Escolha **Acesso Remoto**. **Autenticação** — RADIUS. Isso informa ao VPN Concentrador qual método usar para autenticar usuários. **Mode Config** — Check **Mode Config**. Clique em **Apply**.

- Conclua estes passos para configurar vários servidores de autenticação no VPN 3000 Concentrador. Depois que o grupo for definido, realce esse grupo e clique em **Authentication Servers (Servidores de autenticação)** na coluna **Modify (Modificar)**. Os servidores de autenticação individuais podem ser definidos para cada grupo, mesmo que esses servidores não existam nos servidores globais.

This section lets you configure groups. A group is a collection of users treated as a single entity.

Click the **Add Group** button to add a group, or select a group and click **Delete Group** or **Modify Group**. To modify group parameters, select a group and click the appropriate button.

Actions	Current Groups	Modify
<p>Add Group</p> <p>Modify Group</p> <p>Delete Group</p>	<p>ipsecgroup (Internally Configured)</p>	<p>Authentication Servers</p> <p>Authorization Servers</p> <p>Accounting Servers</p> <p>Address Pools</p> <p>Client Update</p> <p>Bandwidth Assignment</p> <p>WebVPN Servers and URLs</p> <p>WebVPN Port Forwarding</p>

Escolha o tipo de servidor **RADIUS** e adicione esses parâmetros ao servidor Cisco Secure ACS for Windows RADIUS. Deixe todos os outros parâmetros em seu estado padrão. **Authentication Server** — Insira o endereço IP do servidor Cisco Secure ACS for Windows RADIUS. **Server Secret** — Insira o segredo do servidor RADIUS. Esse deve ser o mesmo segredo que você usa ao configurar o VPN 3000 Concentrador na configuração do Cisco Secure ACS for Windows. **Verify** — (Verificar) Insira novamente a senha para verificação.

5. Escolha **Configuration > System > Address Management > Assignment** e marque **Use Address from Authentication Server** para atribuir o endereço IP aos VPN Clients do pool de IPs criado no servidor RADIUS quando o cliente for autenticado.

The screenshot shows the 'Assignment' configuration page in the Cisco Secure ACS for Windows web interface. The breadcrumb navigation at the top reads 'Configuration | System | Address Management | Assignment'. Below the breadcrumb, a descriptive text states: 'This section presents Address Assignment options. Each of the following methods are tried, in order, until an address is found.' The configuration options are as follows:

- Use Client Address**  Check to use the IP address supplied by the client. This can be overridden by user/group configuration.
- Use Address from Authentication Server**  Check to use an IP address retrieved from an authentication server for the client.
- Use DHCP**  Check to use DHCP to obtain an IP address for the client.
- Use Address Pools**  Check to use internal address pool configuration to obtain an IP address for the client.

Below these options is the **IP Reuse Delay** field, which is a text input box containing the number '0'. To its right, the text reads: 'Enter the length of time in minutes (0-480) that a released internal address pool IP address will be held before being reassigned.' At the bottom of the configuration area, there are two buttons: 'Apply' and 'Cancel'.

## [Configuração de servidor RADIUS](#)

Esta seção do documento descreve o procedimento necessário para configurar o Cisco Secure ACS como um servidor RADIUS para autenticação de usuário do VPN Client encaminhada pelo Cisco VPN 3000 Series Concentrador - cliente AAA.

Clique duas vezes no ícone **ACS Admin** para iniciar a sessão de administração no PC que executa o servidor Cisco Secure ACS for Windows RADIUS. Faça login com o nome de usuário e a senha corretos, se necessário.

1. Conclua estes passos para adicionar o VPN 3000 Concentrador à configuração do servidor Cisco Secure ACS for Windows. Escolha **Network Configuration** e clique em **Add Entry** para adicionar um cliente AAA ao servidor RADIUS.





## Network Configuration

- User Setup
- Group Setup
- Shared Profile Components
- Network Configuration
- System Configuration
- Interface Configuration

Select

AAA Clients		
AAA Client Hostname	AAA Client IP Address	Authenticate Using
<a href="#">nm-wlc</a>	192.168.11.24	RADIUS (Cisco Aironet)
<a href="#">WLC</a>	172.16.1.30	RADIUS (Cisco Airespace)

Add Entry

Search

Adicione estes parâmetros ao seu VPN 3000

Concentrator:

## Network Configuration

Edit

### Add AAA Client

AAA Client Hostname

AAA Client IP Address

Key

Authenticate Using

- Single Connect TACACS+ AAA Client (Record stop in accounting on failure).
- Log Update/Watchdog Packets from this AAA Client
- Log RADIUS Tunneling Packets from this AAA Client
- Replace RADIUS Port info with Username from this AAA Client

Submit

Submit + Apply

Cancel

**AAA Client Hostname** — Digite o nome de host do VPN 3000 Concentrator (para resolução de DNS). **AAA Client IP Address** — Insira o endereço IP do VPN 3000 Concentrator. **Key** — (Chave) Insira o segredo do servidor RADIUS. Esse deve ser o mesmo segredo que você configurou ao adicionar o Servidor de autenticação no VPN Concentrator. **Autenticar usando** — Escolha **RADIUS (Cisco VPN 3000/ASA/PIX 7.x+)**. Isso permite que os VPN 3000 VSAs sejam exibidos na janela de configuração do grupo. Clique em Submit. Escolha

Interface Configuration, clique em **RADIUS (Cisco VPN 3000/ASA/PIX 7.x+)** e marque **Group Specific**.

## Interface Configuration

Edit

### RADIUS (Cisco VPN 3000/ASA/PIX 7.x+)

#### User Group

- [026/3076/001] Access-Hours
- [026/3076/002] Simultaneous-Logins
- [026/3076/005] Primary-DNS
- [026/3076/006] Secondary-DNS
- [026/3076/007] Primary-WINS
- [026/3076/008] Secondary-WINS
- [026/3076/009] SEP-Card-Assignment
- [026/3076/011] Tunneling-Protocols
- [026/3076/012] IPSec-Sec-Association
- [026/3076/013] IPSec-Authentication
- [026/3076/015] IPSec-Banner1
- [026/3076/016] IPSec-Allow-Passwd-Store

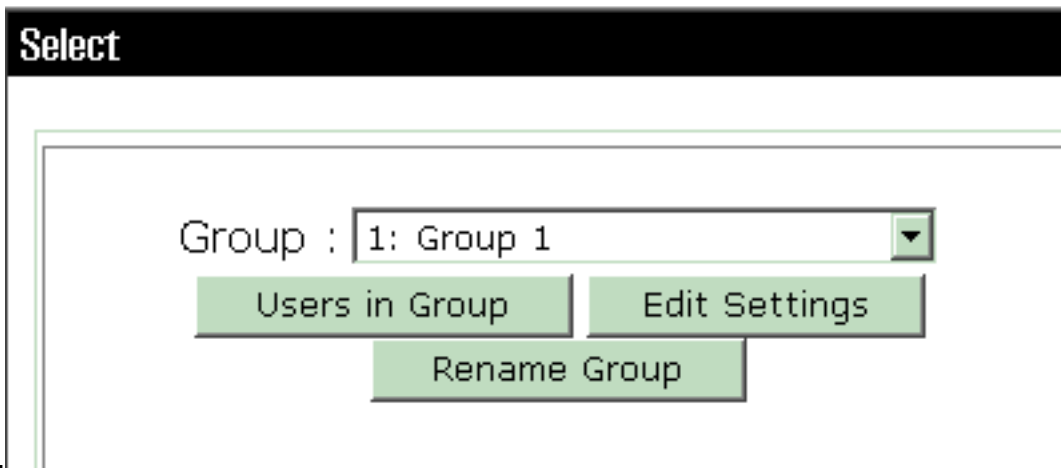
Submit

Cancel

**Observação:** 'atributo RADIUS 26' refere-se a todos os atributos específicos do fornecedor. Por exemplo, escolha **Interface Configuration > RADIUS (Cisco VPN 3000)** e veja se todos os atributos disponíveis começam com 026. Isso mostra que todos esses atributos específicos do fornecedor estão incluídos no padrão IETF RADIUS 26. Por padrão, esses atributos não aparecem na configuração Usuário ou Grupo. Para aparecer na configuração do grupo, crie um cliente AAA (neste caso, o VPN 3000 Concentrator) que autentica com RADIUS na configuração de rede. Em seguida, verifique os atributos que precisam ser exibidos em User Setup, Group Setup ou ambos na configuração da interface. Consulte [Atributos RADIUS](#) para obter mais informações sobre os atributos disponíveis e seu uso. Clique em Submit.

2. Conclua estes passos para adicionar grupos à configuração do Cisco Secure ACS for Windows. Escolha **Group Setup**, selecione um dos grupos de modelos, por exemplo, Group 1 e clique em **Rename**

# Group Setup



**Group.**

Altere o

nome para algo apropriado para sua organização. Por exemplo, ipsecgroup. Como os usuários são adicionados a esses grupos, faça com que o nome do grupo reflita a finalidade real desse grupo. Se todos os usuários forem colocados no mesmo grupo, você poderá chamá-lo de grupo de usuários de VPN. Clique em **Editar configurações** para editar os parâmetros no grupo renomeado recentemente.


# Group Setup

Jump To


## Group Settings : ipsecgroup

---

### Access Restrictions

**Group Disabled** 

Members of this group will be denied access to the network.

**Callback** 

No callback allowed

Dialup client specifies callback number

Use Windows Database callback settings (where possible)

Clique em

**Cisco VPN 3000 RADIUS** e configure estes atributos recomendados. Isso permite que os usuários atribuídos a esse grupo herdem os atributos do Cisco VPN 3000 RADIUS, que permitem centralizar políticas para todos os usuários no Cisco Secure ACS for

# Group Setup

Jump To IP Address Assignment

### Cisco VPN 3000/ASA/PIX v7.x+ RADIUS Attributes

[3076\001] Access-Hours

[3076\002] Simultaneous-Logins

[3076\005] Primary-DNS

[3076\006] Secondary-DNS

[3076\007] Primary-WINS

[3076\008] Secondary-WINS

[3076\009] SEP-Card-Assignment

Windows.

O

**Observação:** tecnicamente, os atributos RADIUS do VPN 3000 não precisam ser configurados desde que o grupo de túnel esteja configurado na etapa 3 da [configuração do VPN 3000 Series Concentrator](#) e o grupo base no VPN Concentrator não mude das configurações padrão originais. **Atributos recomendados do VPN 3000:** **Primary-DNS** — Introduza o endereço IP do servidor DNS primário. **Secondary-DNS** — Insira o endereço IP do servidor DNS secundário. **Primary-WINS** — Insira o endereço IP do servidor WINS primário. **Secondary-WINS** — Digite o endereço IP do servidor WINS secundário. **Tunneling-Protocols** — Escolha **IPsec**. Isso permite *somente* conexões de cliente IPsec. PPTP ou L2TP não são permitidos. **IPsec-Sec-Association** — Digite **ESP-3DES-MD5**. Isso garante que todos os seus clientes IPsec se conectem com a criptografia mais alta disponível. **IPsec-Allow-Password-Store** — Escolha **Disallow** para que os usuários *não tenham* permissão para salvar sua senha no VPN Client. **Banner IPsec** — Insira um banner de mensagem de boas-vindas a ser apresentado ao usuário na conexão. Por exemplo, "Bem-vindo ao acesso VPN do funcionário da MyCompany!" **Domínio padrão IPsec** — Insira o nome de domínio de sua empresa. Por exemplo, "mycompany.com". Este conjunto de atributos não é necessário. Mas

se você não tiver certeza se os atributos do grupo base do VPN 3000 Concentrator foram alterados, a Cisco recomenda que você configure estes atributos:**Logins simultâneos** — Digite o número de vezes que você permite que um usuário faça logon simultaneamente com o mesmo nome de usuário. A recomendação é 1 ou 2.**SEP-Card-Assignment**— Escolha **Any-SEP**.**IPsec-Mode-Config** — Escolha **ON**.**IPsec sobre UDP** — Escolha **OFF**, a menos que você queira que os usuários neste grupo se conectem usando IPsec sobre o protocolo UDP. Se você selecionar **ON**, o VPN Client ainda poderá desativar localmente o IPsec sobre UDP e conectar-se normalmente.**IPsec sobre porta UDP** — Selecione um número de porta UDP no intervalo de 4001 a 49151. Isso é usado somente se IPsec sobre UDP estiver **ATIVADO**. O próximo conjunto de atributos exige que você configure algo no VPN Concentrator antes de poder usá-los. Isso é recomendado apenas para usuários avançados.**Access-Hours** — Isso exige que você configure um intervalo de Horas de Acesso no VPN 3000 Concentrator em **Configuration > Policy Management**. Em vez disso, use o Access Hours disponível no Cisco Secure ACS for Windows para gerenciar esse atributo.**IPsec-Split-Tunnel-List** — Isso exige que você configure uma lista de rede no VPN Concentrator em **Configuration > Policy Management > Traffic Management**. Esta é uma lista de redes enviadas ao cliente que instrui o cliente a criptografar dados somente para aquelas redes na lista. Escolha **Atribuição de IP na configuração do grupo** e marque **Atribuído do pool de servidores AAA** para atribuir os endereços IP aos usuários do VPN Client depois que eles forem

## Group Setup

Jump To IP Address Assignment

### IP Assignment

- No IP address assignment
- Assigned by dialup client
- Assigned from AAA Client pool
- Assigned from AAA server pool

Available Pools

Selected Pools

pool1

->

<-

Up Down

autenticados.


Escolha **Configuração do sistema > Pools de IP** para criar um pool de IPs para usuários do



VPN Client e clique em **Enviar**


## System Configuration

**Edit**

New Pool 	
Name	<input type="text" value="pool1"/>
Start Address	<input type="text" value="10.1.1.1"/>
End Address	<input type="text" value="10.1.1.10"/>

## System Configuration

**Select**

AAA Server IP Pools 			
Pool Name	Start Address	End Address	In Use
<a href="#">pool1</a>	10.1.1.1	10.1.1.10	0%

Escolha

**Submit > Restart** para salvar a configuração e ativar o novo grupo. Repita essas etapas para adicionar mais grupos.

3. **Configurar usuários no Cisco Secure ACS para Windows.** Escolha **User Setup**, insira um nome de usuário e clique em

# User Setup

Select

User:

Find

Add/Edit

List users beginning with letter/number:

[A](#) [B](#) [C](#) [D](#) [E](#) [F](#) [G](#) [H](#) [I](#) [J](#) [K](#) [L](#) [M](#)  
[N](#) [O](#) [P](#) [Q](#) [R](#) [S](#) [T](#) [U](#) [V](#) [W](#) [X](#) [Y](#) [Z](#)  
[0](#) [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#)

List all users

Remove Dynamic Users

Add/Edit.


estes parâmetros na seção de configuração do usuário:

Configure

## User Setup

### User: ipsecuser1 (New User)


Account Disabled

**Supplementary User Info** 


Real Name

Description

---

**User Setup** 

Password Authentication:



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:



**Autenticação de Senha** — Escolha Banco de Dados Interno ACS. Cisco Secure PAP - Senha — Insira uma senha para o usuário. Cisco Secure PAP - Confirmar senha — Insira novamente a senha para o novo usuário. Grupo ao qual o usuário está atribuído — Selecione o nome do grupo criado na etapa anterior. Clique em **Submit** para salvar e ativar as configurações do usuário. Repita essas etapas para adicionar outros usuários.

### [Atribuir um endereço IP estático ao usuário do cliente VPN](#)

Conclua estes passos:

1. Crie um novo grupo de VPN IPSECGRP.
2. Crie um usuário que queira receber o IP estático e escolha IPSECGRP. Escolha **Atribuir endereço IP estático** com o endereço IP estático atribuído em Client IP Address Assignment.

## User Setup

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:

### Callback

- Use group setting
- No callback allowed
- Callback using this number
- Dialup client specifies callback number
- Use Windows Database callback settings

### Client IP Address Assignment

- Use group settings
- No IP address assignment
- Assigned by dialup client
- Assign static IP address
- Assigned by AAA client pool

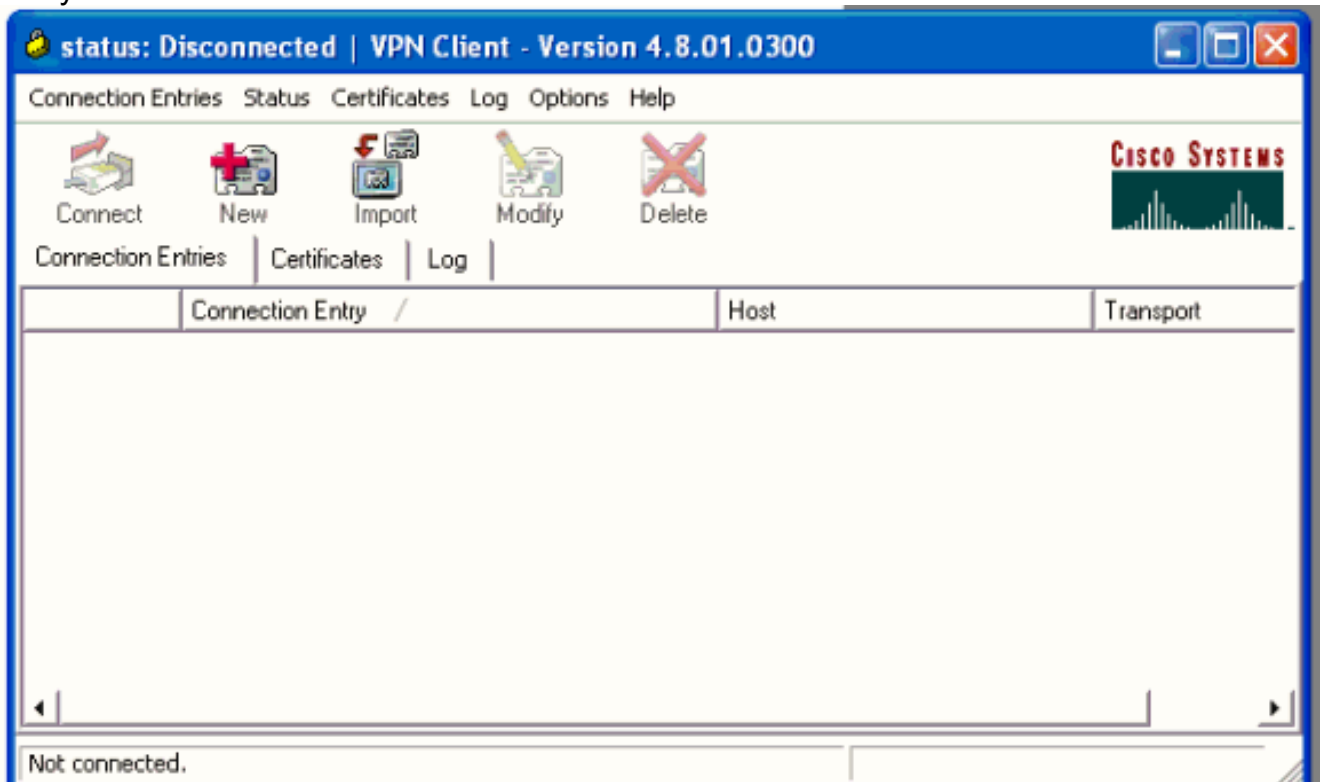
Submit

Delete

Cancel

Esta seção descreve a configuração do lado do VPN Client.

1. Escolha **Iniciar > Programas > Cisco Systems VPN Client > VPN Client**.
2. Clique em **New** para iniciar a janela Create New VPN Connection Entry.



3. Quando solicitado, atribua um nome para sua entrada. Você pode inserir também uma descrição se desejar. Especifique o endereço IP da interface pública do VPN 3000 Concentrator na coluna Host e escolha **Autenticação de grupo**. Em seguida, forneça o nome do grupo e a senha. Clique em **Salvar** para concluir a nova entrada de conexão

VPN Client | Create New VPN Connection Entry

Connection Entry: vpnuser

Description: Headoffice

Host: 10.0.0.1

Authentication | Transport | Backup Servers | Dial-Up

Group Authentication  Mutual Group Authentication

Name: ipsecgroup

Password: \*\*\*\*\*

Confirm Password: \*\*\*\*\*

Certificate Authentication

Name: [dropdown]

Send CA Certificate Chain

Erase User Password Save Cancel

VPN.

Obser

**vação:** certifique-se de que o VPN Client esteja configurado para usar o mesmo nome de grupo e senha configurados no Cisco VPN 3000 Series Concentrator.

### [Adicionar relatório](#)

Depois que a autenticação funcionar, você poderá adicionar a contabilidade.

1. No VPN 3000, escolha **Configuration > System > Servers > Accounting Servers** e adicione o **Cisco Secure ACS for Windows** server.
2. Você pode adicionar servidores de contabilidade individuais a cada grupo ao escolher **Configuration > User Management > Groups**, realçar um grupo e clicar em **Modify Acct. Servidores**. Em seguida, insira o endereço IP do servidor de contabilidade com o segredo do servidor.



Configure and add a RADIUS user accounting server.

**Accounting Server**  Enter IP address or hostname.

**Server Port**  Enter the server UDP port number.

**Timeout**  Enter the timeout for this server (se

**Retries**  Enter the number of retries for this

**Server Secret**  Enter the RADIUS server secret.

**Verify**  Re-enter the server secret.

No Cisco Secure ACS for Windows, os registros de contabilidade são exibidos conforme mostrado na saída:

**Select**

RADIUS Accounting active.csv

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

Filtering is not applied.

Date	Time	User-Name	Group-Name	Calling-Station-Id	Acct-Status-Type	Acct-Session-Id	Acct-Session-Time	Service-Type	Framed-Protocol	Acct-Input-Octets	Acct-Output-Octets	Acct-Input-Packets	Acct-Output-Packets
10/27/2006	18:38:20	ipseuser1	ipsegroup	192.168.1.2	Start	E8700001	..	Framed	PPP	..	..	..	..
10/27/2006	18:38:20	VPN 3000 Concentrator	Default Group	..	Accounting On	..	..	..	..	..	..	..	..
10/27/2006	13:17:10	VPN 3000 Concentrator	Default Group	..	Accounting Off	..	..	..	..	..	..	..	..

## Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

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.

### Verificar o VPN Concentrator

No lado do VPN 3000 Concentrator, escolha **Administration > Administer Sessions** para verificar o estabelecimento do túnel VPN remoto.

## Remote Access Sessions

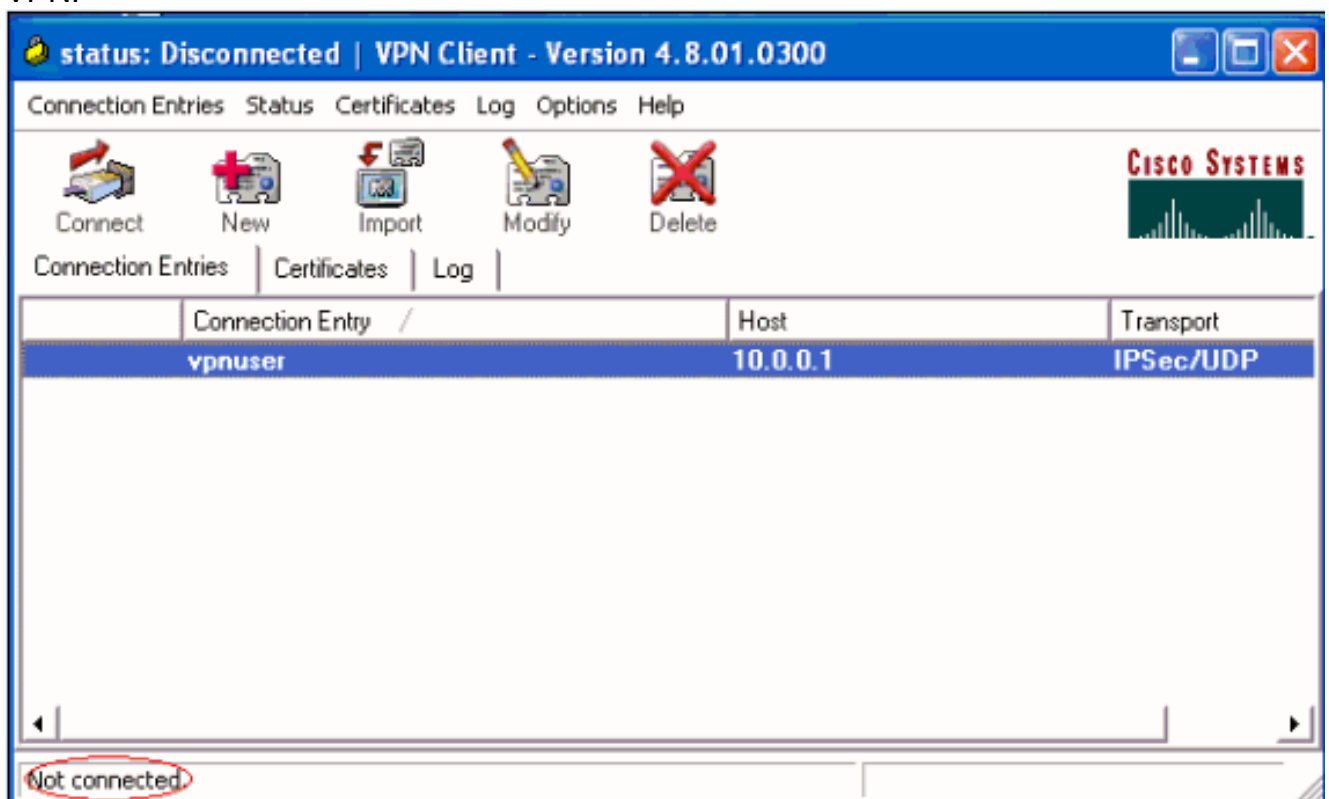
[ [LAN-to-LAN Sessions](#) | [Management Sessions](#) ]

<a href="#">Username</a>	<a href="#">Assigned IP Address</a> <a href="#">Public IP Address</a>	<a href="#">Group</a>	<a href="#">Protocol Encryption</a>	<a href="#">Login Time Duration</a>	<a href="#">Client Type Version</a>	<a href="#">Bytes Tx</a> <a href="#">Bytes Rx</a>	<a href="#">NAC Result Posture Token</a>	<a href="#">Actions</a>
<a href="#">ipsecuser1</a>	10.1.1.9 192.168.1.2	ipsecgroup	IPSec 3DES-168	Oct 27 17:22:14 0:05:11	WinNT 4.8.01.0300	0 8056	N/A	[ <a href="#">Logout</a>   <a href="#">Ping</a> ]

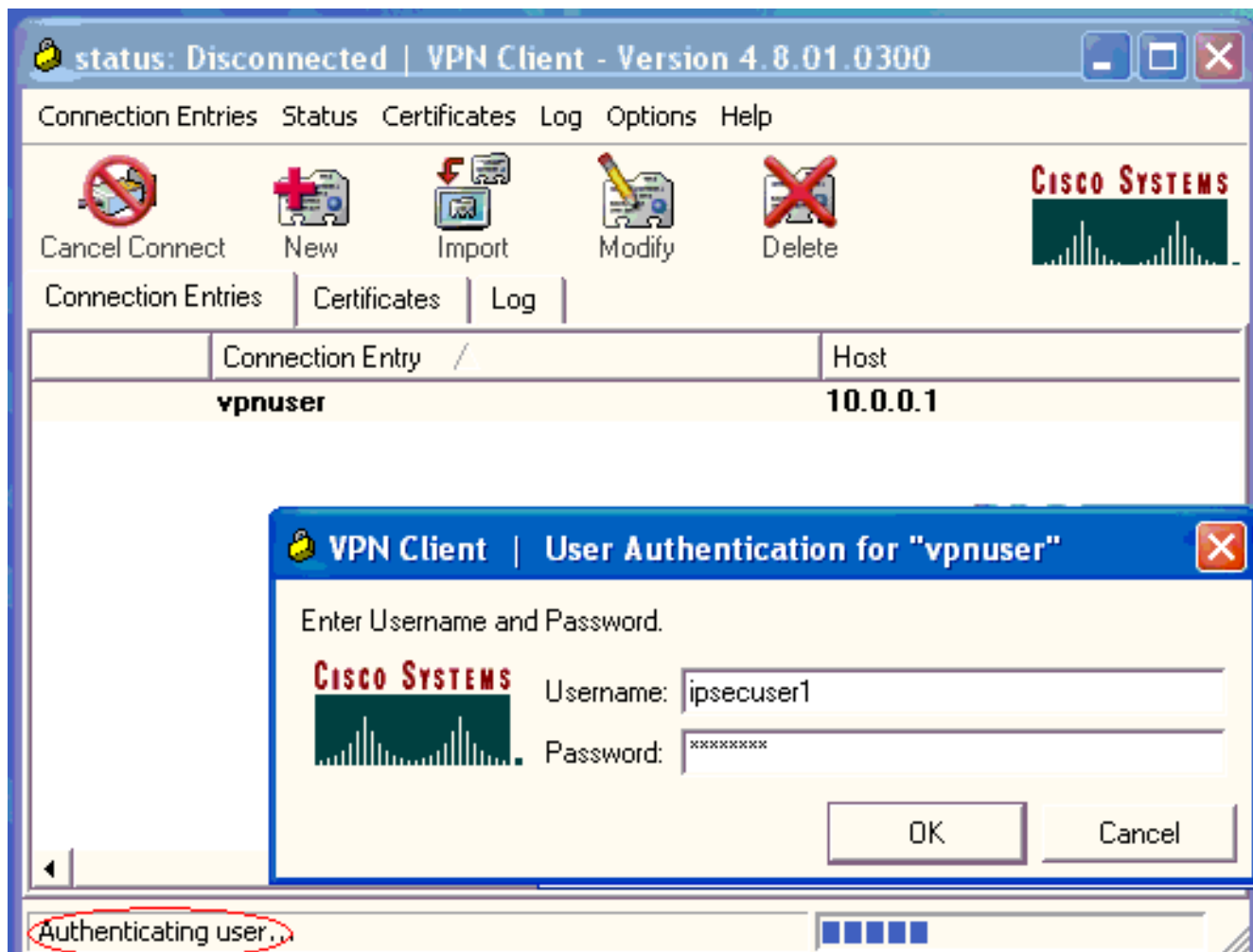
## [Verificar o VPN Client](#)

Conclua estes passos para verificar o VPN Client.

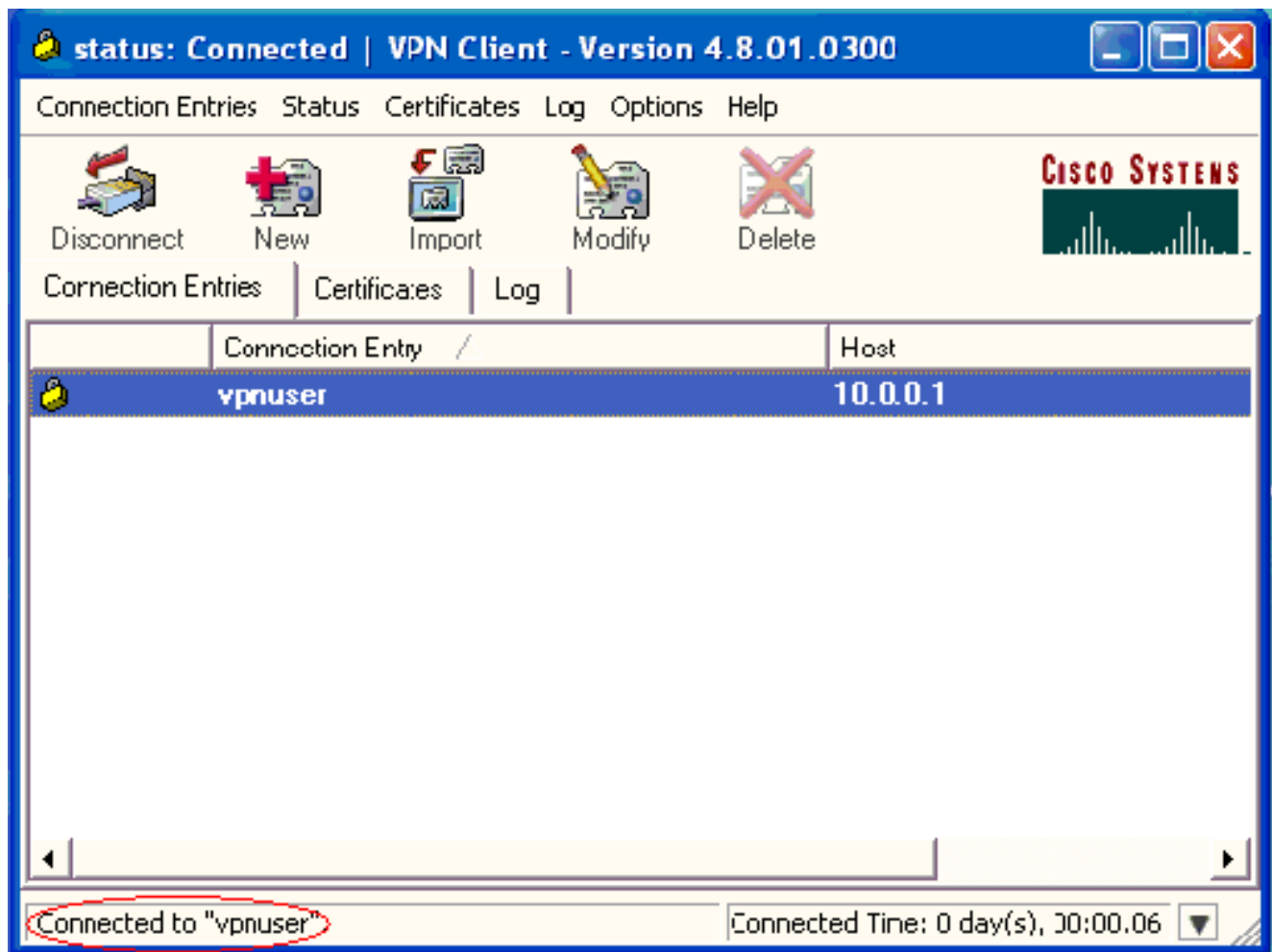
1. Clique em **Connect** para iniciar uma conexão VPN.



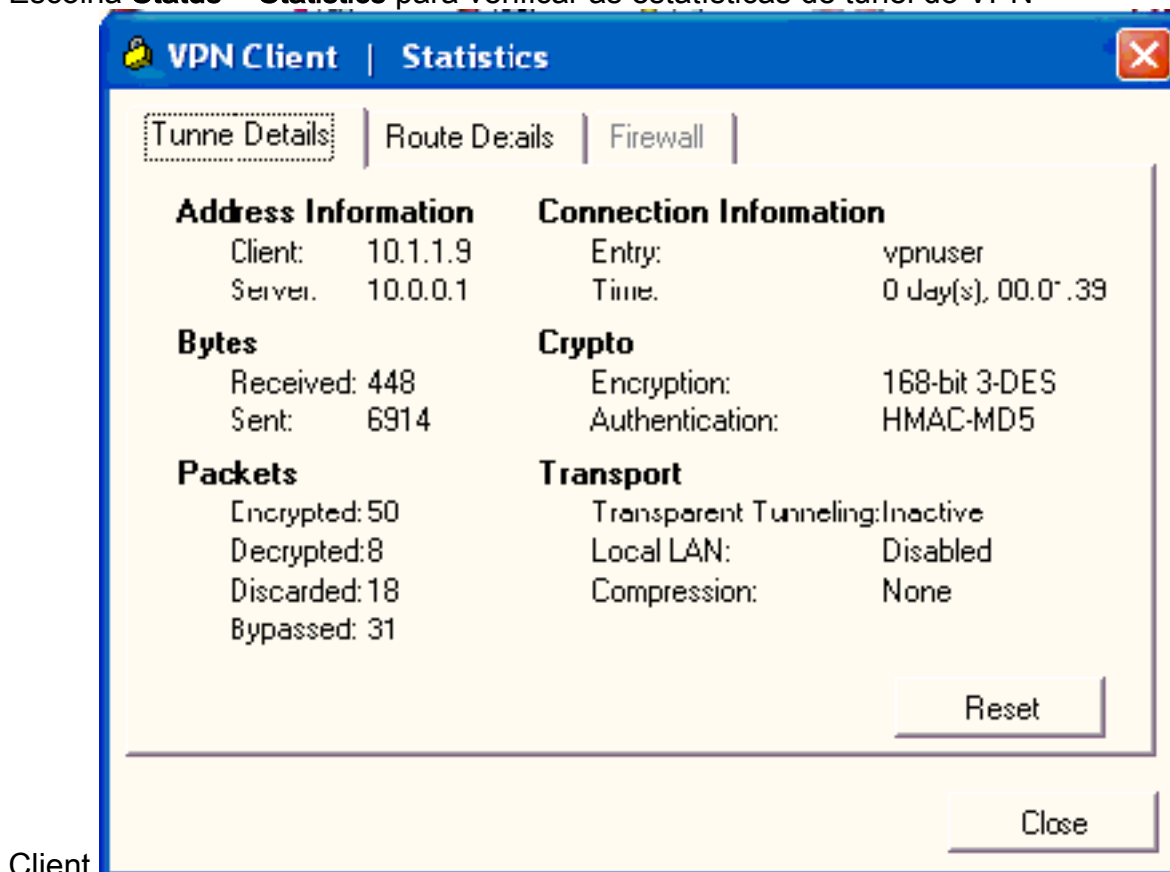
2. Esta janela é exibida para autenticação de usuário. Insira um nome de usuário e uma senha válidos para estabelecer a conexão VPN.



3. O VPN Client é conectado ao VPN 3000 Concentrador no local central.



4. Escolha **Status > Statistics** para verificar as estatísticas de túnel do VPN



Client.

## [Troubleshoot](#)

Execute estes passos para fazer troubleshooting da sua configuração.

1. Escolha **Configuration > System > Servers > Authentication** e conclua estas etapas para testar a conectividade entre o servidor RADIUS e o VPN 3000 Concentrator. Selecione o servidor e clique em **Testar**.

Configuration | System | Servers | Authentication

This section lets you configure parameters for servers that authenticate users.

You should have a properly configured RADIUS, NT Domain, SDI or Kerberos/Active Direct configure the internal server and [add users to the internal database](#).

Click the **Add** button to add a server, or select a server and click **Modify**, **Delete**, **Move**, or

Authentication Servers	Actions
172.16.124.5 (Radius/User Authentication) Internal (Internal)	<input type="button" value="Add"/> <input type="button" value="Modify"/> <input type="button" value="Delete"/> <input type="button" value="Move Up"/> <input type="button" value="Move Down"/> <input type="button" value="Test"/>

Digite o nome de usuário e a senha RADIUS e clique em **OK**.


Configuration | System | Servers | Authentication | Test

Enter a username and password with which to test. **Please wait for the operation**

Username

Password

Success

 Authentication Successful

Uma autenticação bem-sucedida é exibida.

2. Se ele falhar, há um problema de configuração ou um problema de conectividade IP. Verifique se há mensagens relacionadas à falha no registro de tentativas com falha no servidor ACS. Se nenhuma mensagem for exibida neste registro, provavelmente há um problema de conectividade IP. A solicitação RADIUS não chega ao servidor RADIUS. Verifique se os filtros aplicados à interface apropriada do VPN 3000 Concentrator permitem que o RADIUS (1645) entre e saia. Se a autenticação de teste for bem-sucedida, mas os logins no VPN 3000 Concentrator continuarem a falhar, verifique o Filterable Event Log através da porta de console. Se as conexões não funcionarem, você poderá adicionar classes de eventos AUTH, IKE e IPsec ao VPN Concentrator quando selecionar **Configuration > System > Events > Classes > Modify (Severity to Log=1-9, Severity to Console=1-3)**. AUTHDBG, AUTHDECODE, IKEDBG, IKEDECODE, IPSECDBG e IPSECDECODE também estão disponíveis, mas podem fornecer muitas informações. Se forem necessárias informações detalhadas sobre os atributos que são transmitidos do servidor RADIUS, AUTHDECODE, IKEDECODE e IPSECDECODE, forneça isso no nível Severidade para Log=1-13.
3. Recupere o registro de eventos de **Monitoring > Event Log**.

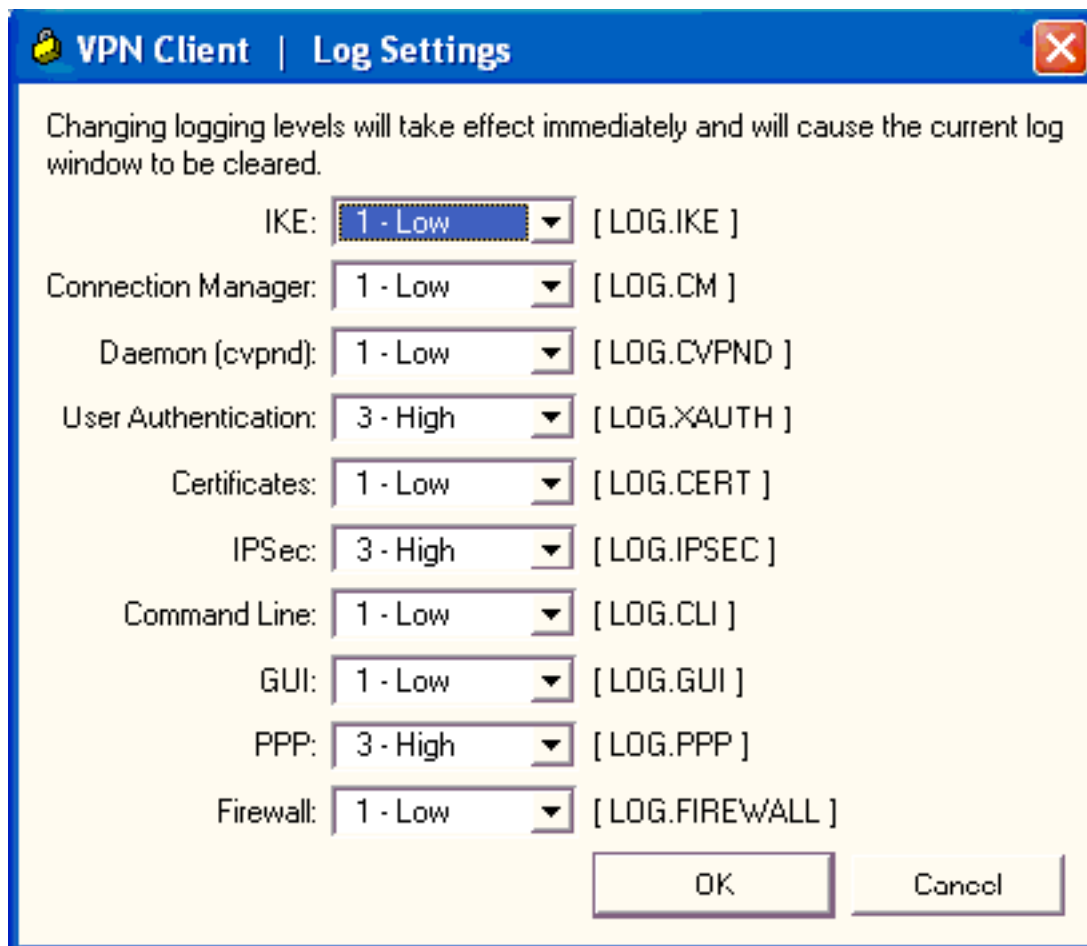


## [Solucionar problemas do VPN Client 4.8 para Windows](#)

Conclua estes passos para solucionar problemas do VPN Client 4.8 para Windows.

1. Escolha **Log > Log settings** para ativar os níveis de log no VPN





Client.

- Escolha **Log > Janela Log** para exibir as entradas de log no VPN Client.

Cisco Systems VPN Client Version 4.8.01.0300  
Copyright (C) 1998-2005 Cisco Systems, Inc. All Rights Reserved.  
Client Type(s): Windows, WinNT  
Running on: 5.1.2600 Service Pack 2  
Config file directory: C:\Program Files\Cisco Systems\VPN Client

1 13:26:29.234 10/31/06 Sev=Warning/2 IKE/0xA3000067  
Received an IPC message during invalid state (IKE\_MAIN:507)

2 13:26:36.109 10/31/06 Sev=Warning/2 CVPND/0xE3400013  
AddRoute failed to add a route: code 87  
Destination 192.168.1.255  
Netmask 255.255.255.255  
Gateway 10.1.1.9  
Interface 10.1.1.9

3 13:26:36.109 10/31/06 Sev=Warning/2 CM/0xA3100024  
Unable to add route. Network: c0a801ff, Netmask: ffffffff, Interface: a010109, Gateway: a010109

Cisco Systems VPN Client Version 4.8.01.0300  
Copyright (C) 1998-2005 Cisco Systems, Inc. All Rights Reserved.  
Client Type(s): Windows, WinNT  
Running on: 5.1.2600 Service Pack 2  
Config file directory: C:\Program Files\Cisco Systems\VPN Client

1 13:27:31.640 10/31/06 Sev=Info/4IPSEC/0x63700019  
Activate outbound key with SPI=0x2c9afd45 for inbound key with SPI=0xc9c1b7d5

2 13:27:42.656 10/31/06 Sev=Info/4IPSEC/0x63700013  
Delete internal key with SPI=0xc9c1b7d5

3 13:27:42.656 10/31/06 Sev=Info/4IPSEC/0x6370000C  
Key deleted by SPI 0xc9c1b7d5

4 13:27:42.656 10/31/06 Sev=Info/4IPSEC/0x63700013  
Delete internal key with SPI=0x2c9afd45

5 13:27:42.656 10/31/06 Sev=Info/4IPSEC/0x6370000C  
Key deleted by SPI 0x2c9afd45

## [Informações Relacionadas](#)

- [Página de suporte do Cisco VPN 3000 Series Concentrator](#)
- [Página de Suporte do Cisco VPN Client](#)
- [Negociação IPsec/Protocolos IKE](#)
- [Cisco Secure ACS para página de suporte do Windows](#)
- [Configurando filtros dinâmicos em um servidor RADIUS](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)