

Configure os Cisco VPN 3000 Series Concentrators para suportar o recurso de expiração de senha NT com o servidor RADIUS

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Diagrama de Rede](#)

[Configurando o VPN 3000 Concentrator](#)

[Configuração de grupo](#)

[Configuração de RADIUS](#)

[Configurando o servidor NT RADIUS do Cisco Secure](#)

[Configurando uma entrada para o VPN 3000 Concentrator](#)

[Configurando a política de usuário desconhecido para a autenticação de domínio NT](#)

[Testando o recurso de expiração de senha NT/RADIUS](#)

[Testando a autenticação RADIUS](#)

[Autenticação do domínio NT real utilizando o proxy RADIUS para testar o recurso de expiração de senha](#)

[Informações Relacionadas](#)

Introduction

Este documento inclui instruções passo a passo sobre como configurar os Cisco VPN 3000 Series Concentrators para suportar o recurso NT Password Expiration usando o servidor RADIUS.

Consulte [RADIUS VPN 3000 com recurso de expiração usando o Microsoft Internet Authentication Server](#) para saber mais sobre o mesmo cenário com o Internet Authentication Server (IAS).

Prerequisites

Requirements

- Se o servidor RADIUS e o servidor NT Domain Authentication estiverem em duas máquinas separadas, certifique-se de ter estabelecido a conectividade IP entre as duas máquinas.
- Verifique se você estabeleceu a conectividade IP do concentrador para o servidor RADIUS. Se o servidor RADIUS estiver em direção à interface pública, não se esqueça de abrir a porta

RADIUS no filtro público.

- Certifique-se de que você pode se conectar ao concentrador do cliente VPN usando o banco de dados de usuário interno. Se isso não estiver configurado, consulte [Configuração do IPSec - Cisco 3000 VPN Client para VPN 3000 Concentrator](#).

Observação: o recurso de expiração de senha não pode ser usado com clientes VPN da Web ou VPN SSL.

Componentes Utilizados

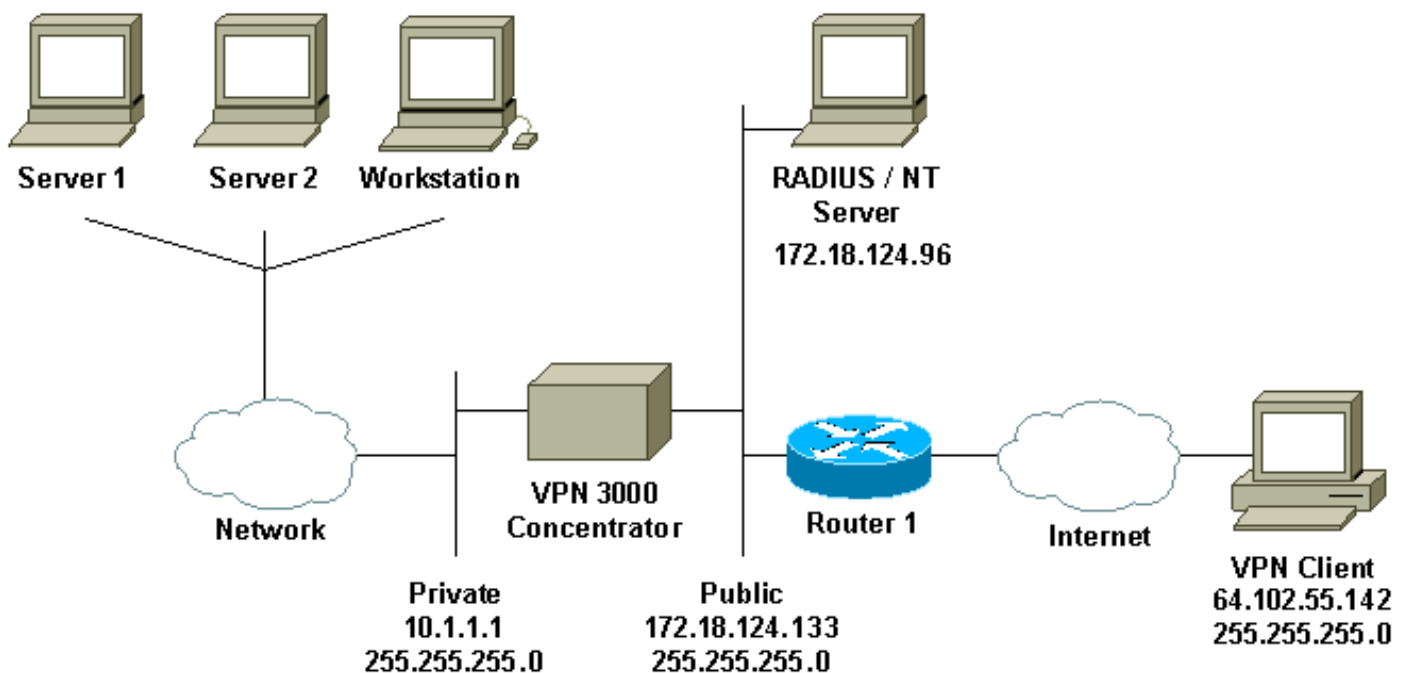
Esta configuração foi desenvolvida e testada utilizando as versões de software e hardware abaixo.

- Software VPN 3000 Concentrator versão 4.7
- VPN Client versão 3.5
- Cisco Secure para NT (CSNT) versão 3.0 Microsoft Windows 2000 Active Directory Server para autenticação de usuário

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.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Notas de diagrama

1. O servidor RADIUS nessa configuração está na interface pública. Se for esse o caso da configuração específica, crie duas regras no filtro público para permitir que o tráfego RADIUS entre e saia do concentrador.
2. Esta configuração mostra o software CSNT e os Serviços de Autenticação de Domínio NT sendo executados na mesma máquina. Esses elementos podem ser executados em duas máquinas separadas, se exigido pela sua configuração.

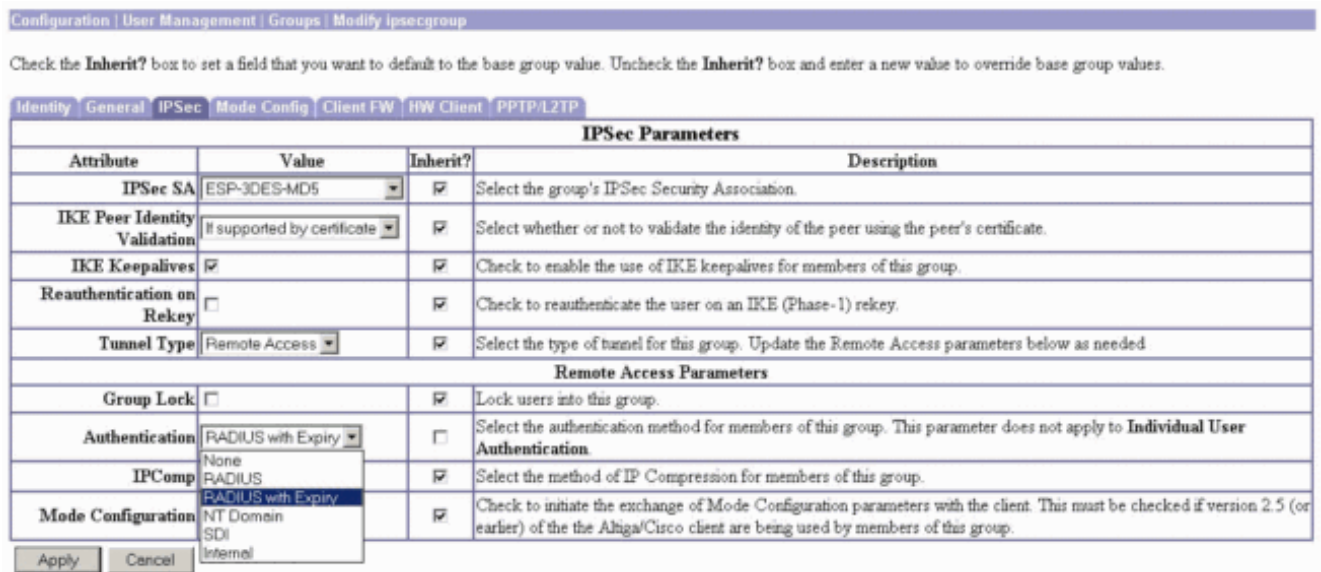
Configurando o VPN 3000 Concentrator

Configuração de grupo

1. Para configurar o grupo para aceitar os Parâmetros de Expiração de Senha NT do Servidor RADIUS, vá para **Configuration > User Management > Groups**, selecione seu grupo na lista e clique em **Modify Group**. O exemplo abaixo mostra como modificar um grupo chamado "ipsecgroup".



2. Vá para a guia **IPSec**, verifique se **RADIUS com vencimento** está selecionado para o atributo **Authentication**.



3. Se quiser que este recurso seja ativado nos VPN 3002 Hardware Clients, vá para a guia **HW Client**, verifique se **Require Interactive Hardware Client Authentication** está ativado e clique em **Apply**.

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.

| Hardware Client Parameters | | | |
|--|-------------------------------------|-------------------------------------|--|
| Attribute | Value | Inherit? | Description |
| Require Interactive Hardware Client Authentication | <input checked="" type="checkbox"/> | <input type="checkbox"/> | Check to require the hardware client to be interactively authenticated at each connection attempt. |
| Require Individual User Authentication | <input type="checkbox"/> | <input checked="" type="checkbox"/> | Check to require users behind a hardware client to be authenticated. |
| User Idle Timeout | 30 | <input checked="" type="checkbox"/> | Enter the session idle timeout in minutes. Use 0 for no timeout. |
| Cisco IP Phone Bypass | <input type="checkbox"/> | <input checked="" type="checkbox"/> | Check to allow Cisco IP Phones to bypass Individual User Authentication behind a hardware client. |

Apply Cancel

Configuração de RADIUS

1. Para definir as configurações do servidor RADIUS no concentrador, vá para Configuration > System > Servers > Authentication > Add.

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

You should have a properly configured RADIUS, NT Domain, or SDI server to access, or you can 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 **Test**.

| Authentication Servers | Actions |
|------------------------|-----------|
| Internal (Internal) | Add |
| | Modify |
| | Delete |
| | Move Up |
| | Move Down |
| | Test |

2. Na tela **Add**, digite os valores que correspondem ao servidor RADIUS e clique em **Add**.O exemplo abaixo usa os seguintes valores.

Server Type: **RADIUS**

Authentication Server: **172.18.124.96**

Server Port = **0** (for default of 1645)

Timeout = **4**

Retries = **2**

Server Secret = **cisco123**

Verify: **cisco123**

Configure and add a user authentication server.

| | | |
|------------------------------|--|--|
| Server Type | <input type="text" value="RADIUS"/> | Selecting <i>Internal Server</i> will let you add users to the internal user database. |
| Authentication Server | <input type="text" value="172.18.124.96"/> | Enter IP address or hostname. |
| Server Port | <input type="text" value="0"/> | Enter 0 for default port (1645). |
| Timeout | <input type="text" value="4"/> | Enter the timeout for this server (seconds). |
| Retries | <input type="text" value="2"/> | Enter the number of retries for this server. |
| Server Secret | <input type="password" value="*****"/> | Enter the RADIUS server secret. |
| Verify | <input type="password" value="*****"/> | Re-enter the secret. |

[Configurando o servidor NT RADIUS do Cisco Secure](#)

[Configurando uma entrada para o VPN 3000 Concentrator](#)

1. Faça login no CSNT e clique em **Network Configuration** no painel esquerdo. Em "AAA Clients" (Clientes AAA), clique em **Add Entry (Adicionar entrada)**.

CISCO SYSTEMS Network Configuration

Select

AAA Clients

| AAA Client Hostname | AAA Client IP Address | Authenticate Using |
|-----------------------|-----------------------|------------------------|
| nsite | 172.18.141.40 | RADIUS (Cisco IOS/PIX) |

Add Entry

The current configuration has been changed. Restart ACS in "System Configuration:Service Control" to adopt the new settings.

AAA Servers

| AAA Server Name | AAA Server IP Address | AAA Server Type |
|--------------------------|-----------------------|-------------------------------------|
| jazib-pc | 172.18.124.96 | CiscoSecure ACS for Windows 2000/NT |

Add Entry

Proxy Distribution Table

| Character String | AAA Servers | Strip | Account |
|---------------------------|-------------|-------|---------|
| (Default) | jazib-pc | No | Local |

Add Entry Sort Entries

2. Na tela "Add AAA Client" (Adicionar cliente AAA), digite os valores apropriados para adicionar o concentrador como o cliente RADIUS e clique em **Submit + Restart (Enviar + Reiniciar)**. O exemplo abaixo usa os seguintes valores.

AAA Client Hostname = **133_3000_conc**

AAA Client IP Address = **172.18.124.133**

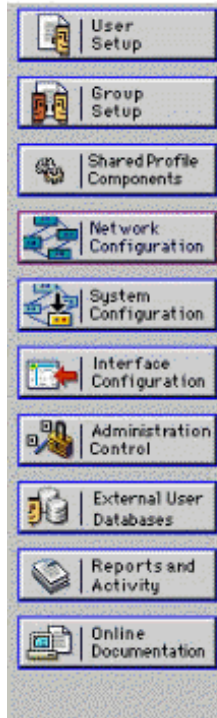
Key = **cisco123**

Authenticate using = **RADIUS (Cisco VPN 3000)**



Network Configuration

Edit



Add AAA Client

| | |
|--|--|
| AAA Client Hostname | <input type="text" value="133_3000_conc"/> |
| AAA Client IP Address | <input type="text" value="172.18.124.133"/> |
| Key | <input type="text" value="cisco123"/> |
| Authenticate Using | <input type="text" value="RADIUS (Cisco VPN 3000)"/> |
| <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 | |

Uma entrada para o seu concentrador 3000 será exibida na seção "AAA Clients".



Network Configuration

Select



| AAA Clients | | |
|-------------------------------|-----------------------|-------------------------|
| AAA Client Hostname | AAA Client IP Address | Authenticate Using |
| 133_3000_conc | 172.18.124.133 | RADIUS (Cisco VPN 3000) |
| nsite | 172.18.141.40 | RADIUS (Cisco IOS/PIX) |

[Configurando a política de usuário desconhecido para a autenticação de domínio NT](#)

1. Para configurar Autenticação de usuário no servidor RADIUS como parte da Política de usuário desconhecida, clique em **Banco de dados de usuário externo** no painel esquerdo e clique no link **Configuração do banco de dados**.




External User Databases

Select

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

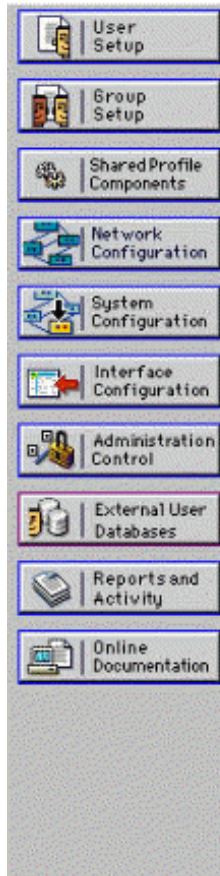
- [Unknown User Policy](#)
- [Database Group Mappings](#)
- [Database Configuration](#)

 [Back to Help](#)

2. Em "External User Database Configuration", clique em **Windows NT/2000**.



External User Databases



Select

External User Database Configuration

Choose which external user database type to configure.

- [NIS/NIS+](#)
- [LEAP Proxy RADIUS Server](#)
- [Windows NT/2000](#)
- [Novell NDS](#)
- [Generic LDAP](#)
- [External ODBC Database](#)
- [RADIUS Token Server](#)
- [AXENT Token Server](#)
- [CRYPTOCARD Token Server](#)
- [SafeWord Token Server](#)
- [SDI SecurID Token Server](#)

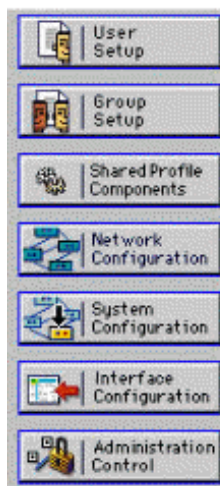
[List all database configurations](#)

Cancel

3. Na tela "Database Configuration Creation" (Criação de configuração de banco de dados), clique em **Create New Configuration** (Criar nova configuração).



External User Databases



Edit

Database Configuration Creation

Click here to create a new configuration for the Windows NT/2000 database.

[Create New Configuration](#)

Cancel

4. Quando solicitado, digite um nome para a Autenticação NT/2000 e clique em **Enviar**. O exemplo abaixo mostra o nome "Radius/NT Password Expiration" (Expiração da senha Radius/NT).



External User Databases



Edit

Create a new External Database Configuration ?

Enter a name for the new configuration for Windows NT/2000

5. Clique em **Configurar** para configurar o nome de domínio para autenticação de usuário.



External User Databases



Edit

External User Database Configuration ?

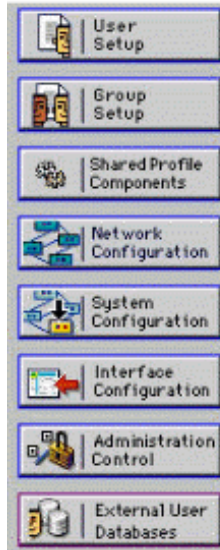
Choose what to do with the Windows NT/2000 database.

6. Selecione o domínio NT em "Domínios disponíveis" e clique no botão de seta para a direita para adicioná-lo à "Lista de domínios". Em "MS-CHAP Settings" (Configurações MS-CHAP), certifique-se de que as opções para **permitir alterações de senha usando MS-CHAP versão 1 e versão 2** estejam selecionadas. Clique em **Enviar** quando terminar.

7. Clique em **External User Database** no painel esquerdo e, em seguida, clique no link para **Database Group Mappings** (Mapeamentos de grupos de bancos de dados). Você deve ver uma entrada para seu banco de dados externo configurado anteriormente. O exemplo abaixo mostra uma entrada para "Radius/NT Password Expiration" (Expiração de senha do Radius/NT), o banco de dados que acabamos de configurar.



External User Databases



Select

Unknown User Group Mappings ?

Choose the External User Database for which you want to configure the group mappings.

| Name | Type |
|---|-----------------|
| Radius/NT Password Expiration | Windows NT/2000 |

Cancel

8. Na tela "Configurações de domínio", clique em **Nova configuração** para adicionar as configurações de domínio.



External User Databases



Edit

Domain Configurations ?

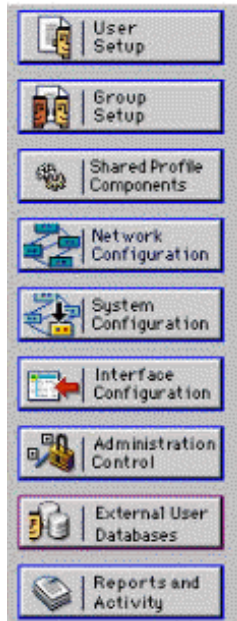
[DEFAULT](#)

New configuration

9. Selecione o seu domínio na lista de "Domínios detectados" e clique em **Enviar**. O exemplo abaixo mostra um domínio chamado "JAZIB-ADS."



External User Databases



Edit

Define New Domain Configuration

Detected Domains:

JAZIB-ADS

Clear Selection

Domain:

Submit Cancel

10. Clique no seu nome de domínio para configurar os mapeamentos de grupo. Este exemplo mostra o domínio "JAZIB-ADS".



External User Databases



Edit

Domain Configurations

[JAZIB-ADS](#)
[DEFAULT](#)

New configuration

11. Clique em **Adicionar mapeamento** para definir os mapeamentos de grupo.



External User Databases

Edit

Group Mappings for Domain : JAZIB-ADS

| NT groups | CiscoSecure group |
|-----------|-------------------------|
| | - no mappings defined - |

Add mapping

Delete Configuration

12. Na tela "Criar novo mapeamento de grupo", mapeie o grupo no domínio NT para um grupo no servidor CSNT RADIUS e clique em **Enviar**. O exemplo abaixo mapeia o grupo NT "Users" para o grupo RADIUS "Group 1".

11.

CISCO SYSTEMS

External User Databases

Edit

Create new group mapping for Domain : JAZIB-ADS

Define NT group set

NT Groups

- Administrators
- Guests
- Backup Operators
- Replicator
- Server Operators
- Account Operators
- Print Operators

Add to selected Remove from selected

Selected

- Users

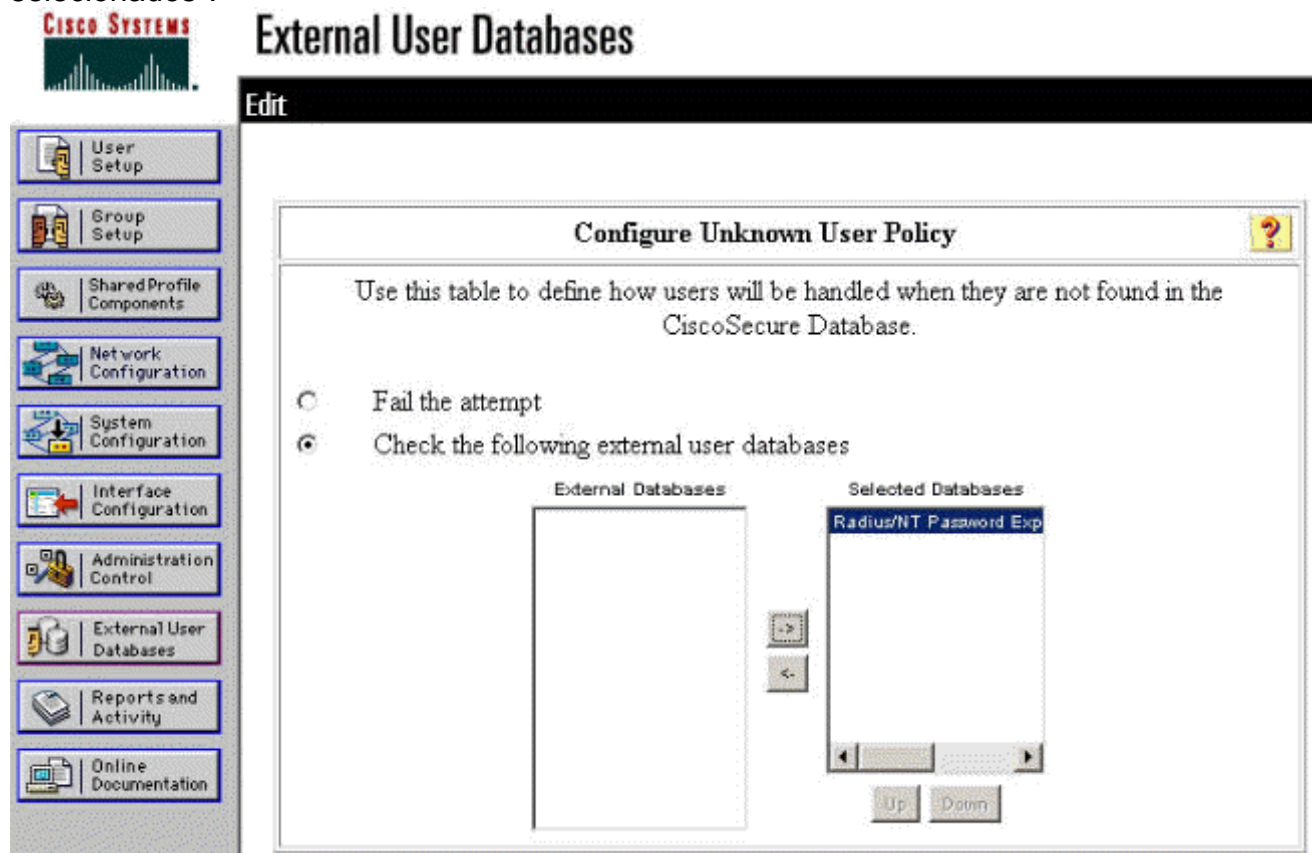
Up Down

CiscoSecure group: Group 1

Submit Cancel

13. Clique em **External User Database** no painel esquerdo e, em seguida, clique no link

Unknown User Policy (Política de usuário desconhecida) (como visto neste [exemplo](#)). Certifique-se de que a opção **Verificar os seguintes bancos de dados de usuário externo** está selecionada. Clique no botão de seta para a direita para mover o banco de dados externo configurado anteriormente da lista de "Bancos de dados externos" para a lista de "Bancos de dados selecionados".



[Testando o recurso de expiração de senha NT/RADIUS](#)

O concentrador oferece uma função para testar a autenticação RADIUS. Para testar este recurso corretamente, siga estas etapas cuidadosamente.

[Testando a autenticação RADIUS](#)

1. Vá para **Configuration > System > Servers > Authentication**. Selecione o servidor RADIUS e clique em **Testar**.

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

You should have a properly configured RADIUS, NT Domain, or SDI server to access, or you can 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 **Test**.

| Authentication Servers | Actions |
|------------------------|-----------|
| Internal (Internal) | Add |
| 172.18.124.96 (Radius) | Modify |
| | Delete |
| | Move Up |
| | Move Down |
| | Test |

- Quando solicitado, digite seu nome de usuário e senha do domínio NT e clique em **OK**. O exemplo abaixo mostra o nome de usuário "jbrahim" configurado no servidor de domínio NT com "cisco123" como a senha.

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

User Name

Password

- Se a autenticação estiver configurada corretamente, você deverá receber uma mensagem indicando "Authentication Successful" (Autenticação bem-

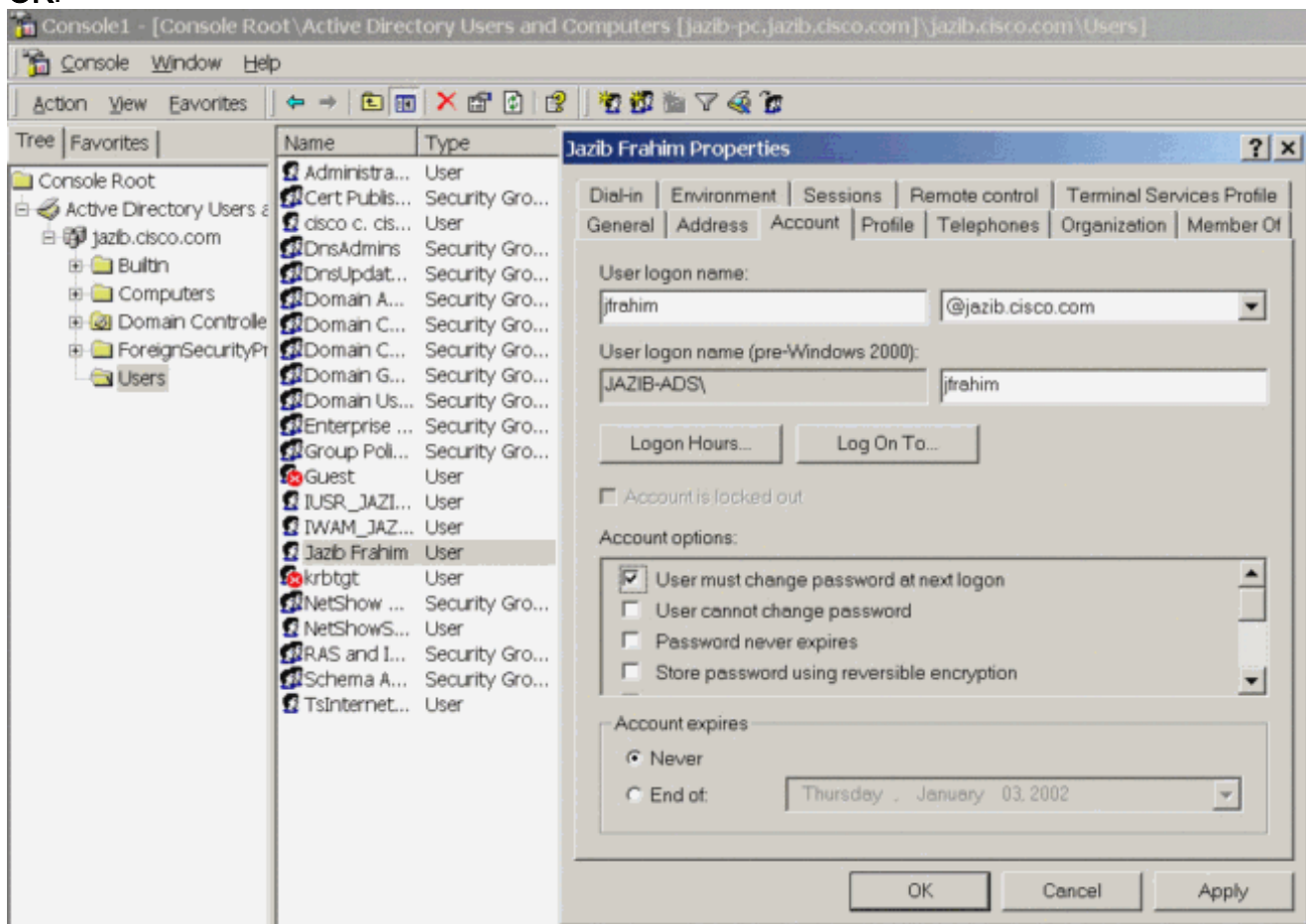


sucedida). Se você receber uma mensagem diferente da mostrada acima, há algum problema de configuração ou conexão. Repita as etapas de configuração e teste descritas neste documento para garantir que todas as configurações foram feitas corretamente. Verifique também a conectividade IP entre seus dispositivos.

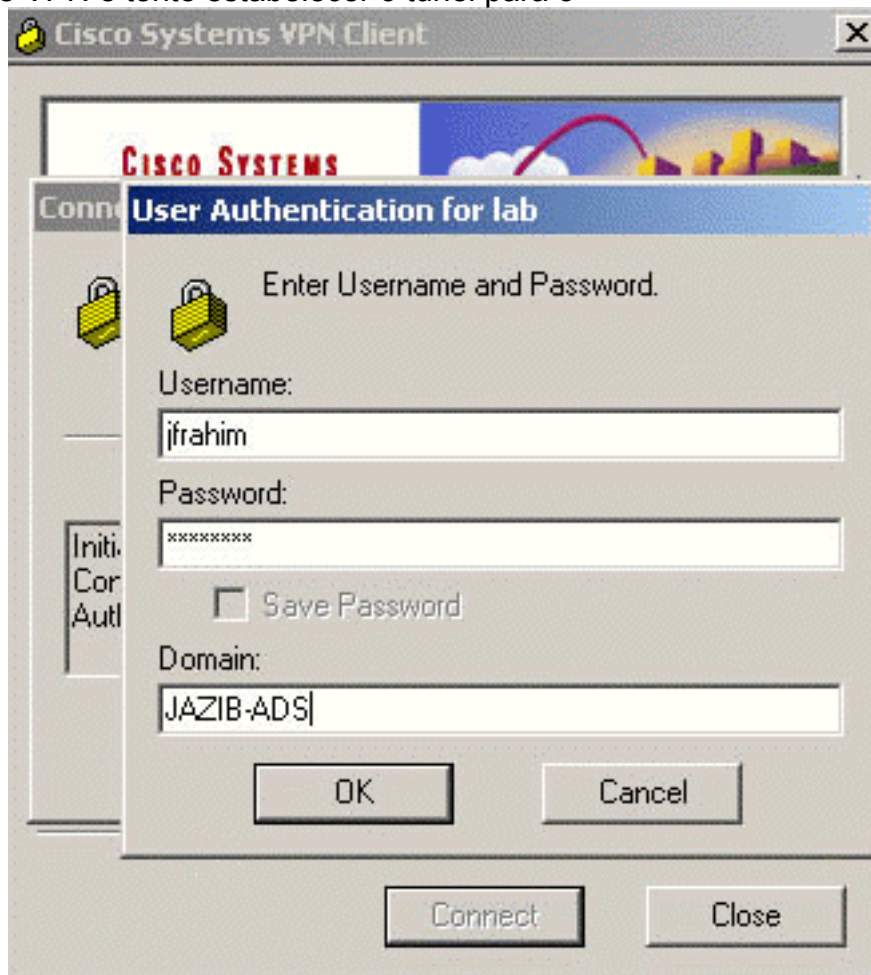
[Autenticação do domínio NT real utilizando o proxy RADIUS para testar o recurso de expiração de senha](#)

- Se o usuário já estiver definido no servidor de domínio, modifique as propriedades para que o usuário seja solicitado a alterar a senha no próximo logon. Vá para a guia "Conta" da caixa de diálogo de propriedades do usuário, selecione a opção para **Usuário deve alterar a senha**

no próximo logon e clique em OK.



2. Inicie o cliente VPN e tente estabelecer o túnel para o



concentrador.

3. Durante a autenticação do usuário, você deve ser solicitado a alterar a



senha.

[Informações Relacionadas](#)

- [Concentrador do Cisco VPN 3000 Series](#)
- [IPSec](#)
- [Cisco Secure Access Control Server for Windows](#)
- [RADIUS](#)
- [Solicitações de Comentários \(RFCs\)](#)