

Настройка концентраторов серии Cisco VPN 3000 на поддержку функции истечения срока действия пароля NT с RADIUS Server

Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Схема сети](#)

[Настройка концентратора VPN 3000](#)

[Конфигурация группы](#)

[Конфигурация RADIUS](#)

[Конфигурирование сервера безопасности сервиса удаленной аутентификации по телефонной линии \(RADIUS\) Cisco](#)

[Настройка записи для концентратора VPN 3000](#)

[Настройка политики для неизвестного пользователя для аутентификации в домене NT](#)

[Тестирование функции окончания срока действия пароля NT/RADIUS](#)

[Тестирование аутентификации RADIUS](#)

[Фактическая аутентификация в домене NT использует прокси-сервер RADIUS для тестирования функции истечения срока действия пароля](#)

[Дополнительные сведения](#)

Введение

Этот документ включает пошаговые инструкции о том, как настроить концентраторы Cisco VPN серии 3000 для поддержки Характеристики истечение срока действия пароля NT с помощью сервера RADIUS.

См. [RADIUS VPN 3000 с Характеристикой проверки срока действия Использование Сервера аутентификации Microsoft Internet Authentication Server](#) для узнавания больше о том же сценарии с Internet Authentication Server (IAS).

Предварительные условия

Требования

- Если ваш сервер RADIUS и сервер Аутентификации в домене NT находятся на двух отдельных компьютерах, удостоверьтесь, что вы установили возможность подключения с помощью IP-адреса между этими двумя машинами.

- Удостоверьтесь, что вы установили возможность подключения с помощью IP-адреса от концентратора до сервера RADIUS. Если сервер RADIUS находится к открытому интерфейсу, не забывайте открывать POPT RADIUS на Общем фильтре.
- Гарантируйте, что можно соединиться с концентратором от клиента VPN, использующего Базу данных Внутреннего пользователя. Если это не настроено см. [IPSec Настройки - Клиент VPN Cisco 3000 к VPN 3000 Concentrator](#).

Примечание: Характеристика истечение срока действия пароля не может использоваться с веб-VPN или VPN-клиентами SSL (SVC).

Используемые компоненты

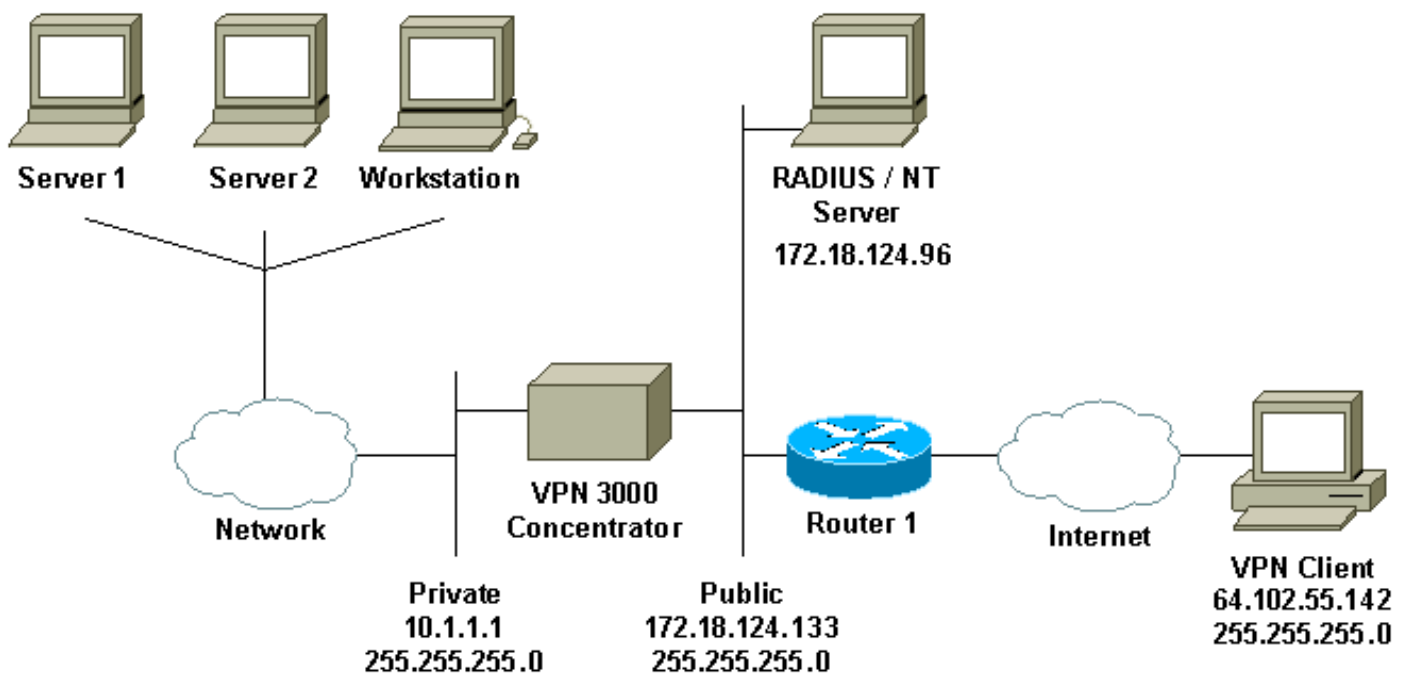
При разработке и тестировании этой конфигурации использовались следующие версии программного и аппаратного обеспечения.

- Версия программного обеспечения 4.7 VPN 3000 Concentrator
- Выпуск 3.5 клиента VPN
- Cisco Secure для NT (CSNT) Сервер Active Directory Microsoft Windows 2000 версии 3.0 для Проверки подлинности пользователя

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Схема сети

В настоящем документе используется следующая схема сети:



Примечания к диаграмме

1. Сервер RADIUS в этой конфигурации находится на открытом интерфейсе. Если это верно, с вашей определенной настройкой, создайте два правила в своем общем фильтре, чтобы позволить Трафику сервера RADIUS вводить и оставлять

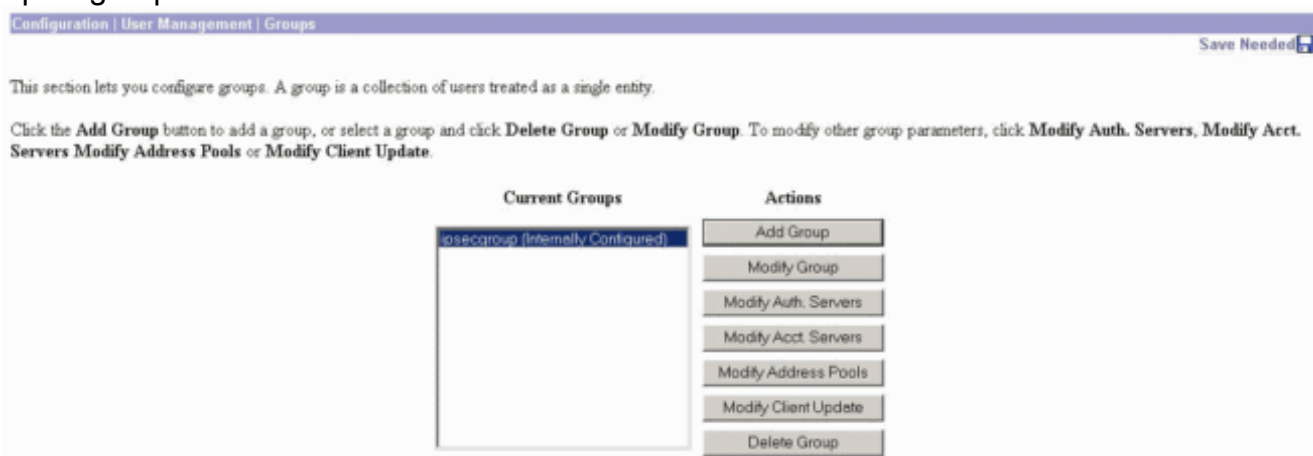
концентратор.

- Эта конфигурация показывает программное обеспечение CSNT и NT Domain Authentication Services, работающая на той же машине. Эти элементы могут быть выполнены на двух отдельных компьютерах при необходимости вашей конфигурацией.

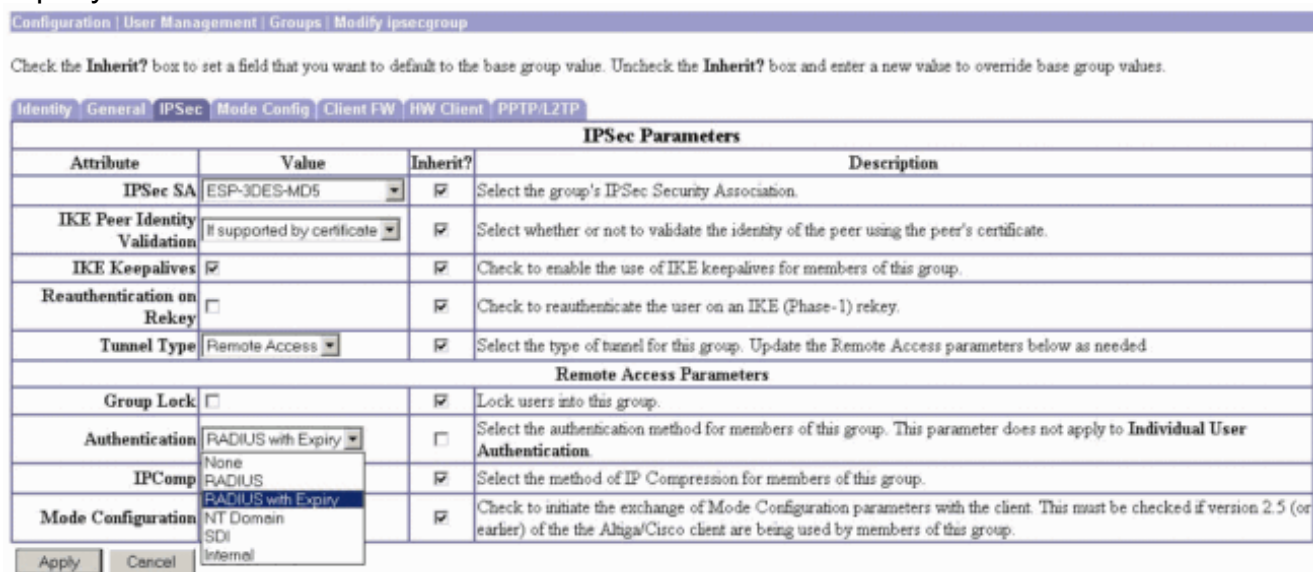
Настройка концентратора VPN 3000

Конфигурация группы

- Для настройки группы для принятия Параметров Истечения срока действия пароля NT от сервера RADIUS перейдите к **Configuration > User Management > Groups**, выберите группу из списка и нажмите **Modify Group**. Пример ниже показов, как модифицировать группу, названную "ipsecgroup".



- Перейдите к вкладке **IPSec**, удостоверьтесь, что **RADIUS с Истечением** выбран для **Опознавательного** атрибута.



- Если вы хотите, чтобы эта функция была включена на аппаратных клиентах VPN 3002, перешла к вкладке **HW Client**, удостоверьтесь, что **Require Interactive Hardware Client Authentication**, включен, то нажмите **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

Конфигурация RADIUS

- Для настройки параметров настройки сервера RADIUS на концентраторе перейдите к **Configuration> System> Servers> Authentication>**, **Добавляют.**

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)	<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"/>

- На экране **Add** введите в значениях, которые соответствуют серверу RADIUS и **нажмите Add**. Пример ниже использует следующие значения. 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="text" value="*****"/>	Enter the RADIUS server secret.
Verify	<input type="text" value="*****"/>	Re-enter the secret.

Add Cancel

Конфигурирование сервера безопасности сервиса удаленной аутентификации по телефонной линии (RADIUS) Cisco

Настройка записи для концентратора VPN 3000

1. Войдите в CSNT и нажмите **Network Configuration** в левой панели. На вкладке **AAA Clients** (Клиенты AAA) щелкните **Add Entry** (Добавить запись).

The screenshot shows the Cisco Systems Network Configuration interface. The left sidebar contains navigation options: User Setup, Group Setup, Shared Profile Components, Network Configuration (selected), System Configuration, Interface Configuration, Administration Control, External User Databases, Reports and Activity, and Online Documentation. The main content area is titled "Network Configuration" and has a "Select" header. It displays three sections: "AAA Clients", "AAA Servers", and "Proxy Distribution Table".

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

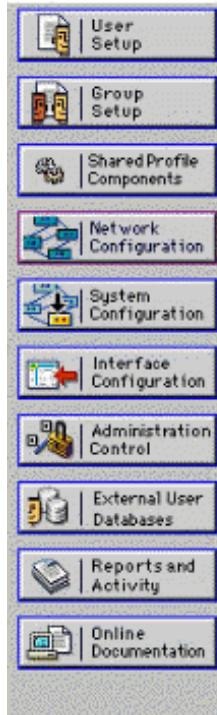
[Add Entry](#) [Sort Entries](#)

2. На экране "Add AAA Client" введите в соответствующих значениях, чтобы добавить концентратор как КЛИЕНТА RADIUS, затем нажать **Submit + Перезапуск**. Пример ниже использует следующие значения. 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

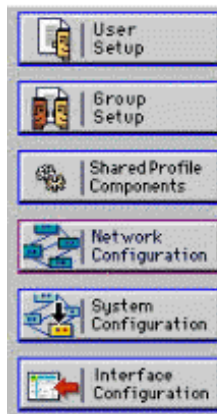
AAA Client Hostname	<input type="text" value="133_3000_conc"/>
AAA Client IP Address	<input type="text" value="172.18.124.133"/>
Key	<input type="text" value="cisco123"/>
Authenticate Using	<input type="text" value="RADIUS (Cisco VPN 3000)"/>
<input type="checkbox"/> Single Connect TACACS+ AAA Client (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	

Запись для ваших 3000 концентраторов появится под разделом "Клиентов AAA".



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)

[Настройка политики для неизвестного пользователя для аутентификации в домене NT](#)

1. Для настройки Проверки подлинности пользователя на сервере RADIUS как часть Неизвестной политики пользователя нажмите **External User Database** в левой панели, затем щелкните по ссылке для **Конфигурации базы данных**.




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

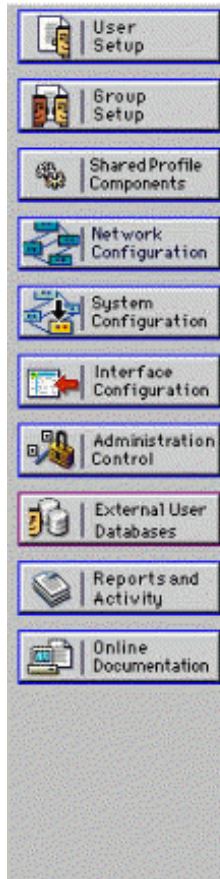
- [Unknown User Policy](#)
- [Database Group Mappings](#)
- [Database Configuration](#)

 [Back to Help](#)

2. Под "Конфигурацией базы данных внешних пользователей" нажмите **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](#)

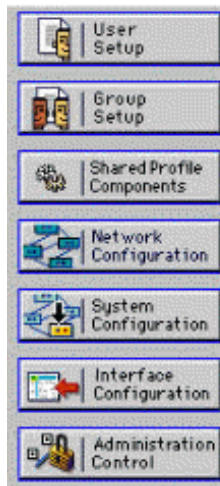
[List all database configurations](#)

Cancel

3. На экране "Database Configuration Creation" нажмите **Create New Configuration**.



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. Когда предложено, введите имя для Аутентификации NT/2000 и нажмите **Submit**. Пример ниже показов название "Истечение срока действия пароля Радиуса/NT".



External User Databases



Edit

Create a new External Database Configuration ?

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

5. Нажмите **Configure** для настройки Доменного имени для Проверки подлинности пользователя.



External User Databases



Edit

External User Database Configuration ?

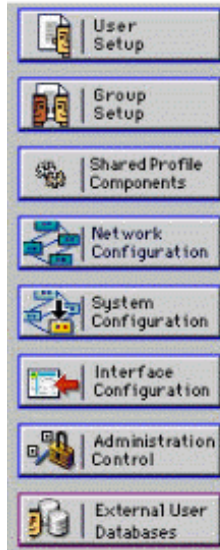
Choose what to do with the Windows NT/2000 database.

6. Выберите свой домен NT от "Доступных Доменов", затем нажмите кнопку стрелки вправо для добавления его к "Списку доменов". При "Параметрах настройки MS-CHAP", гарантируйте, что выбраны опции для **изменений пароля Разрешения с помощью Версии MS-CHAP 1 и версии 2**. По завершении нажмите **Submit**.


7. Нажмите **External User Database** в левой панели, затем щелкните по ссылке для **Сопоставлений групп баз данных** (как замечено в [данном примере](#)). Необходимо видеть запись для ранее настроенной внешней базы данных. Пример ниже показов запись для "Истечения срока действия пароля Радиуса/NT", база данных, которую мы просто настроили.



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


8. На экране "Domain Configurations" нажмите **New configuration** для добавления конфигураций домена.



External User Databases



Edit

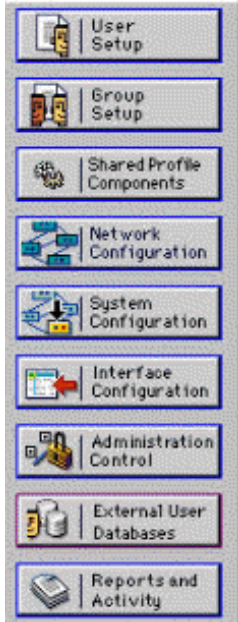
Domain Configurations 

[DEFAULT](#)

9. Выберите свой домен из списка "Обнаруженных Доменов" и нажмите **Submit**. Пример ниже показов домен назвал "JAZIB-ADS".



External User Databases



Edit

Define New Domain Configuration

Detected Domains:

JAZIB-ADS

Clear Selection

Domain:

Submit Cancel

10. Щелкните по своему доменному имени для настройки сопоставлений группы. Данный пример показывает доменный "JAZIB-ADS".



External User Databases



Edit

Domain Configurations

[JAZIB-ADS](#)

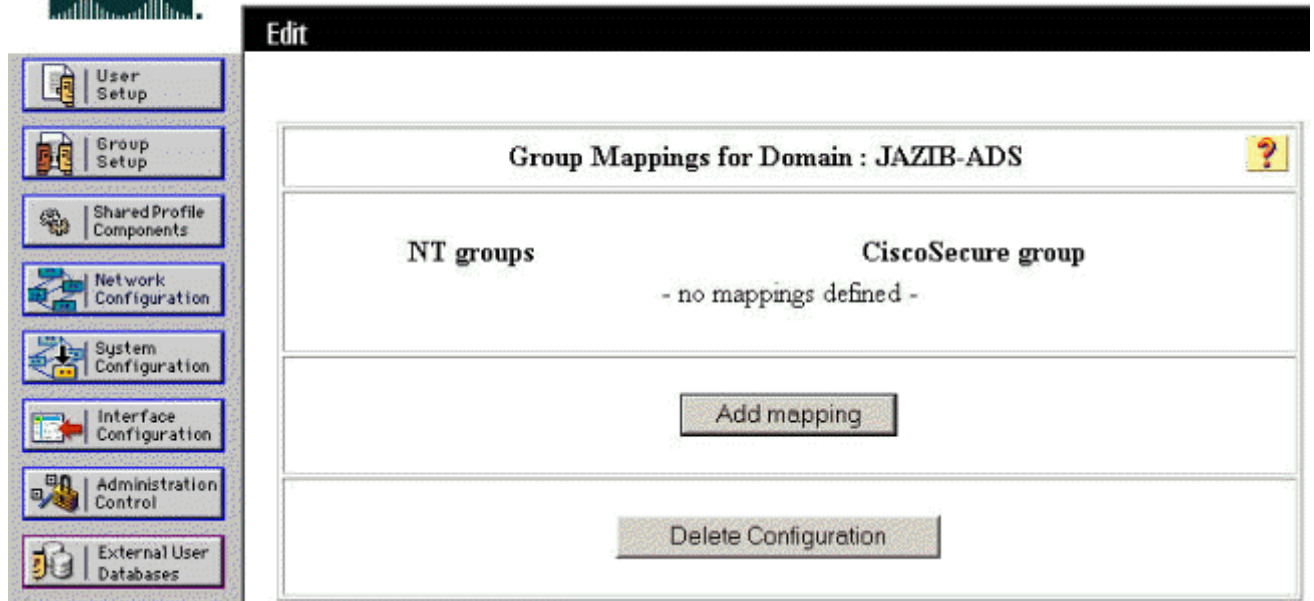
[DEFAULT](#)

New configuration

11. Нажмите Add сопоставление для определения сопоставлений группы.



External User Databases



12. На экране "Create new group mapping" отображите группы домена NT на группы сервера CSNT RADIUS, затем щелкните Submit.. Ниже приведенный пример отображает связь NT группы "Users" с RADIUS группой "Group 1".

Edit

Create new group mapping for Domain : JAZIB-ADS ?

Define NT group set

NT Groups

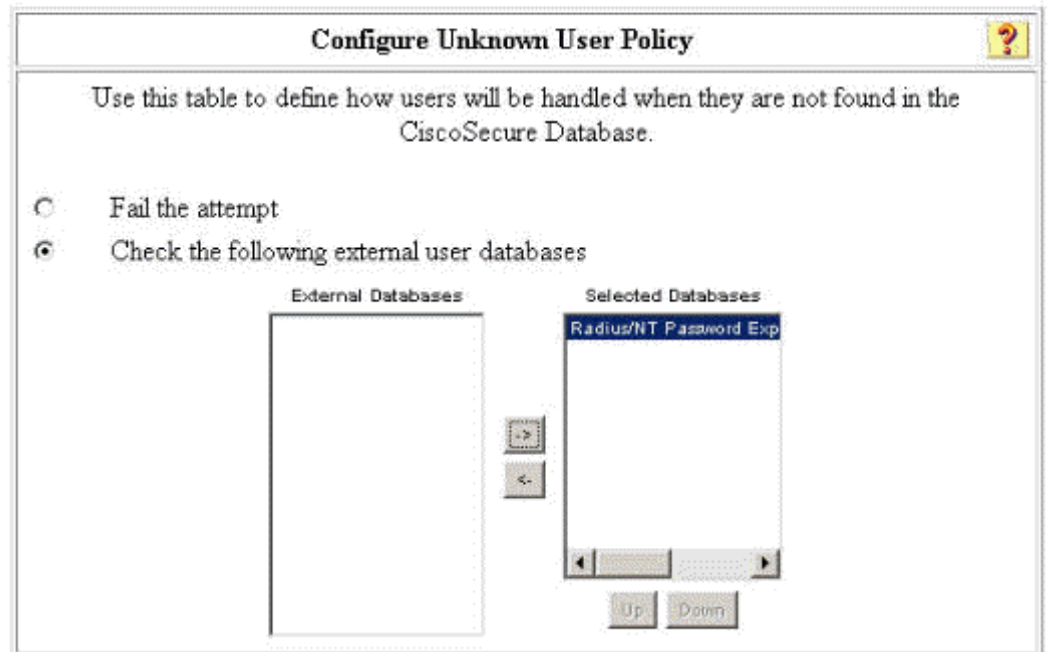
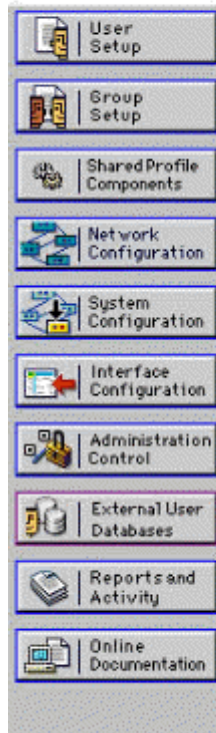
Administrators
Guests
 Backup Operators
 Replicator
 Server Operators
 Account Operators
 Print Operators

Selected

Users

CiscoSecure group:

13. Нажмите **External User Database** в левой панели, затем щелкните по ссылке для **Неизвестной** политики пользователя (как замечено в [данном примере](#)). Удостоверьтесь, что выбрана опция для **Проверки следующие внешние базы данных пользователей**. Нажмите кнопку стрелки вправо для перемещения ранее настроенной внешней базы данных из списка "Внешних баз данных" к списку "Выбранных баз данных".



Тестирование функции окончания срока действия пароля NT/RADIUS

Концентратор предлагает функцию для тестирования Проверки подлинности RADIUS. Для тестирования этой функции должным образом удостоверьтесь, что вы выполняете эти действия тщательно.

Тестирование аутентификации RADIUS

1. Перейдите к **Configuration > System > Servers > Authentication**. Выберите свой сервер RADIUS и нажмите **Test**.



2. Когда предложено, введите свое доменное имя пользователя NT и пароль, и затем нажмите **ОК**. Пример ниже имени пользователя показов "jfracim" настроенный на

сервере домена NT с "cisco123" как пароль.

Configuration | System | Servers | Authentication | Test

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

User Name
Password

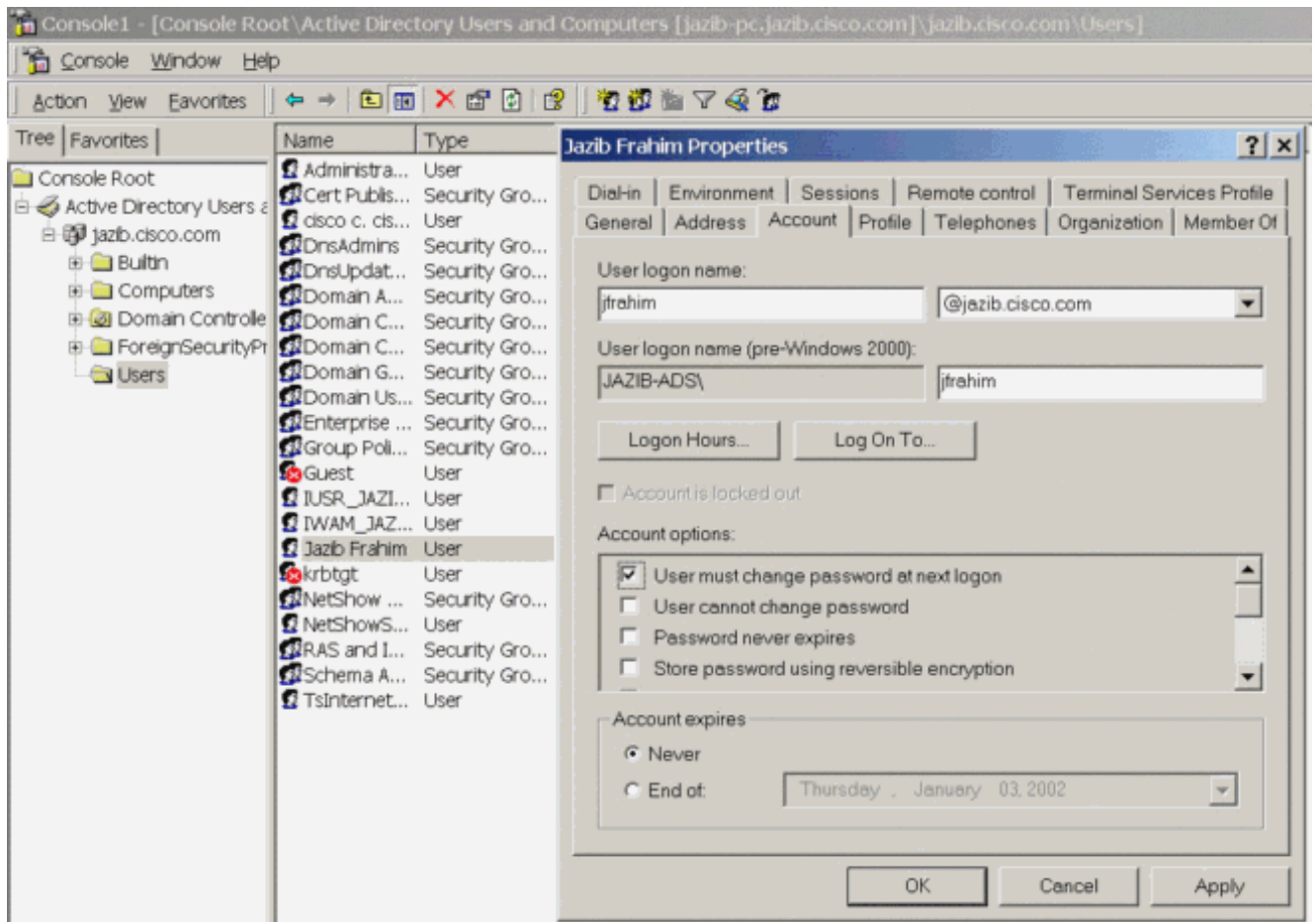
3. Если ваша аутентификация установлена должным образом, необходимо получить сообщение, сообщая "Успешную



Аутентификацию". При получении какого-либо сообщения кроме один показанный выше существует некоторая конфигурация или проблема с подключением. Повторите конфигурацию и шаги тестирования, выделенные в этом документе, чтобы гарантировать, что все настройки были установлены должным образом. Также проверьте возможность подключения с помощью IP-адреса между своими устройствами.

[Фактическая аутентификация в домене NT использует прокси-сервер RADIUS для тестирования функции истечения срока действия пароля](#)

1. Если пользователь уже определен на сервере домена, модифицируйте свойства так, чтобы пользователю предложили изменить пароль при следующем входе в систему. Перейдите к вкладке "Account" диалогового окна со свойствами пользователя, выберите опцию для **Пользователя, должен изменить пароль при следующем входе в систему**, затем нажать **ОК**.

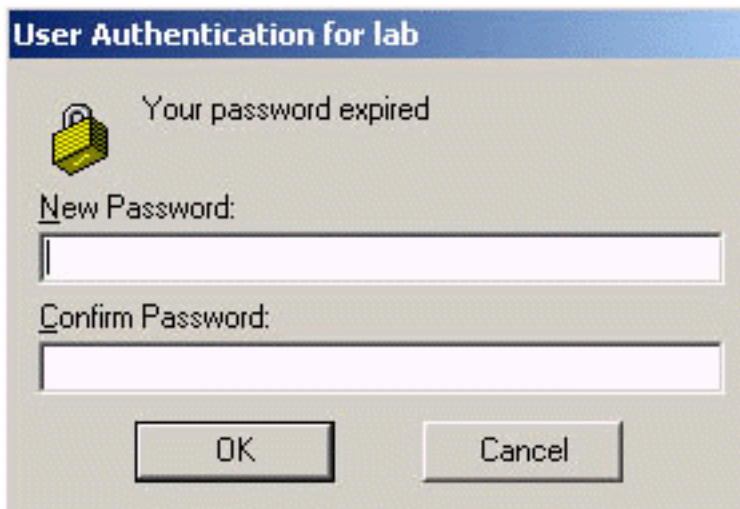


2. Запустите клиент VPN, затем попытайтесь установить туннель к



концентратору.

3. Во время Проверки подлинности пользователя вам нужно предложить изменить



пароль.

[Дополнительные сведения](#)

- [Концентратор серии Cisco VPN 3000](#)
- [IPSec](#)
- [Cisco Secure Access Control Server for Windows](#)
- [RADIUS](#)
- [Запросы комментариев \(RFC\)](#)