

RADIUS サーバを使用して NT のパスワード期限切れ機能をサポートするための Cisco VPN 3000 シリーズ コンセントレータの設定

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[ネットワーク図](#)

[VPN 3000 コンセントレータの設定](#)

[グループの設定](#)

[RADIUSの設定](#)

[Cisco Secure NT RADIUS サーバの設定](#)

[VPN 3000 コンセントレータ用のエントリの設定](#)

[NT ドメイン認証のための未知のユーザのポリシーの設定](#)

[NT/RADIUS パスワード有効期限設定機能のテスト](#)

[RADIUS認証のテスト](#)

[RADIUS プロキシを使用する実際の NT ドメイン認証によるパスワード期限切れ機能のテスト](#)

[関連情報](#)

概要

このドキュメントでは、RADIUS サーバを使用して NT パスワード期限切れ機能をサポートするために、Cisco VPN 3000 シリーズ コンセントレータを設定する方法について段階的に説明します。

Internet Authentication Server(IAS)と同じシナリオについての詳細は、『[Microsoft Internet Authentication Serverを使用したVPN 3000 RADIUSの有効期限機能](#)』を参照してください。

前提条件

要件

- 使用する RADIUS サーバと NT ドメイン認証サーバが別々の 2 台のマシンである場合は、その 2 台のマシン間で IP 接続を確立してください。
- また、コンセントレータから RADIUS サーバへの IP 接続も確立する必要があります。RADIUS サーバがパブリック インターフェイスに接続している場合は、パブリック フィルタの RADIUS ポートを開いておくことを忘れないでください。

- さらに、内部のユーザ データベースを使用して、VPN クライアントからコンセントレータへ接続できることを確認してください。この接続が設定されていない場合は、『[IPSec の設定 - Cisco 3000 VPN クライアントから VPN 3000 コンセントレータへ](#)』を参照してください。

注：パスワードの有効期限機能は、Web VPNまたはSSL VPNクライアントでは使用できません。

使用するコンポーネント

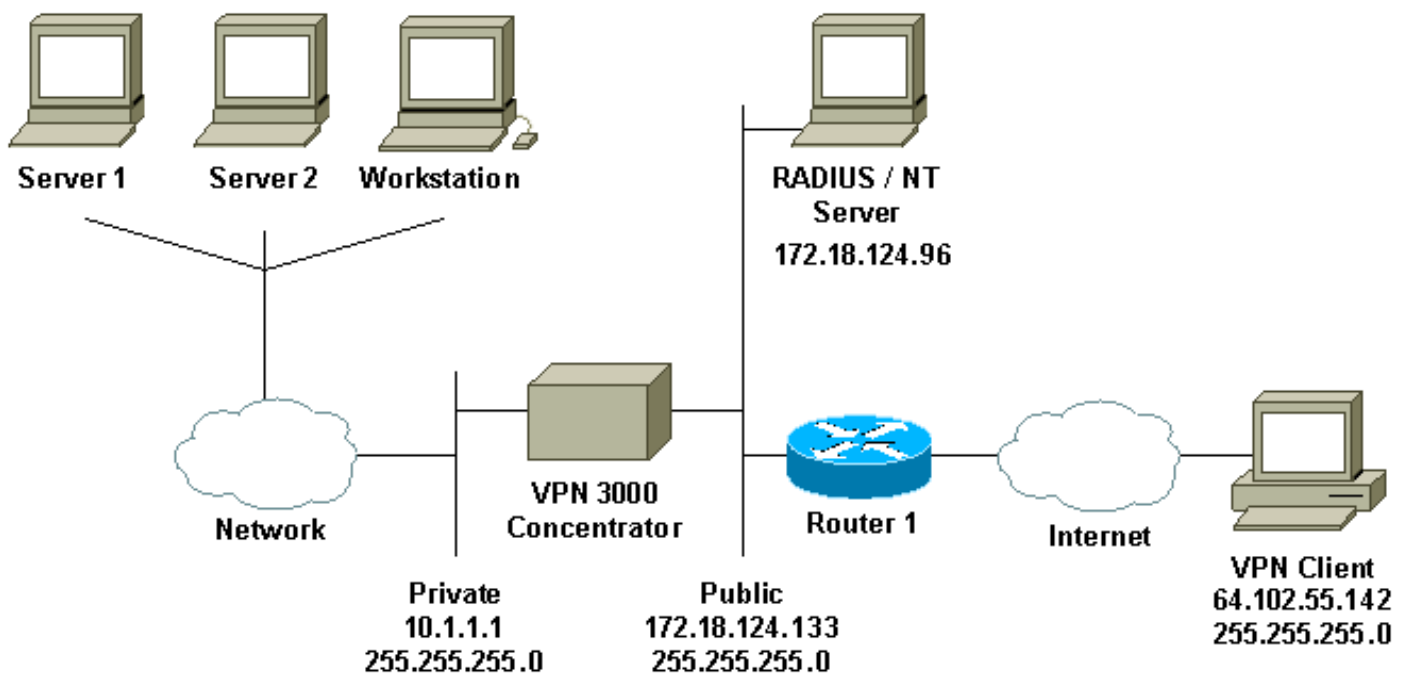
この設定の作成とテストは、次のソフトウェアとハードウェアのバージョンで行われています。

- VPN 3000 コンセントレータ ソフトウェア バージョン 4.7
- VPN クライアント リリース 3.5
- Cisco Secure for NT(CSNT)バージョン3.0 Microsoft Windows 2000 Active Directory Server for User Authentication

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

ネットワーク図

このドキュメントでは、次のネットワーク セットアップを使用します。



ダイアグラムノート

1. この構成での RADIUS サーバは、パブリック インターフェイスに接続されています。使用する設定がこれと同じ場合には、パブリック フィルタに 2 つのルールを作成して、RADIUS サーバのトラフィックがコンセントレータに出入りできるようにしてください。
2. この設定では、CSNT ソフトウェアと NT ドメイン認証サービスが同一のマシン上で実行されています。これらは、必要な場合には別々のマシンで実行することもできます。

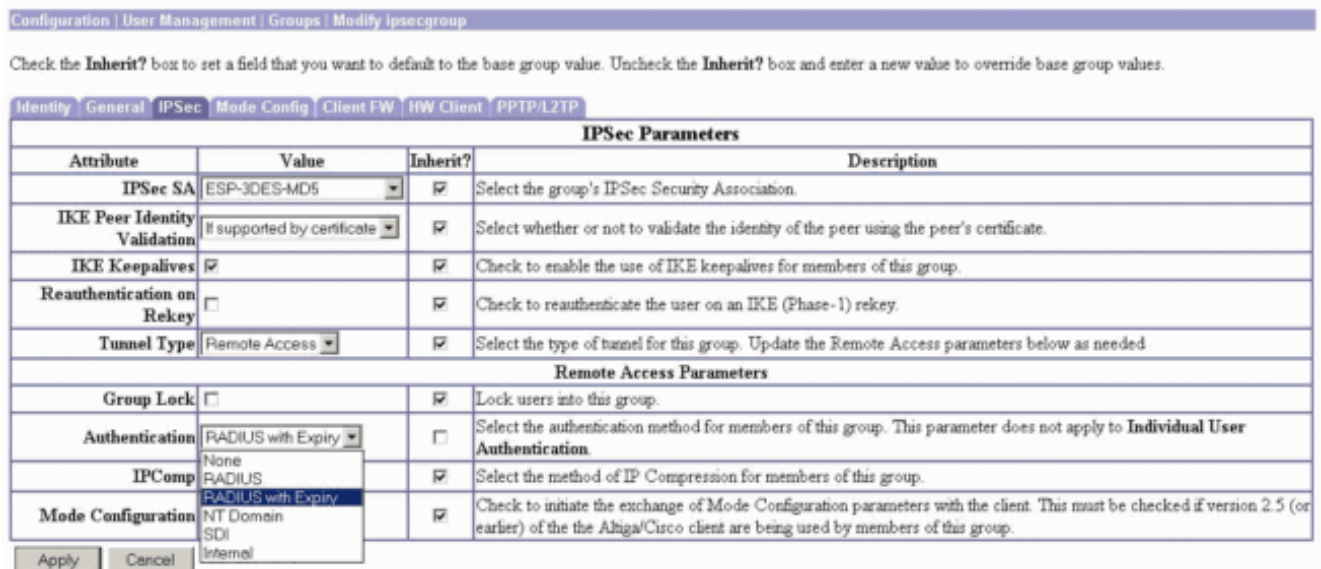
VPN 3000 コンセントレータの設定

グループの設定

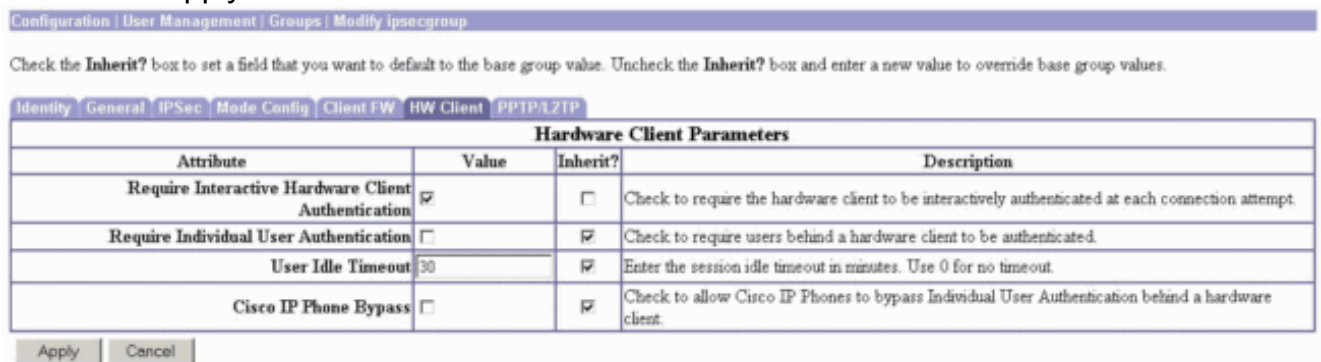
1. RADIUSサーバからNT Password Expiration Parametersを受け入れるようにグループを設定するには、[Configuration] > [User Management] > [Groups]に移動し、リストからグループを選択して、[Modify Group] をクリックします。次の例では、「ipsecgroup」という名前のグループの設定の変更方法について説明します。



2. IPSec タブで、Authentication の属性に RADIUS with Expiry が選択されていることを確認します。

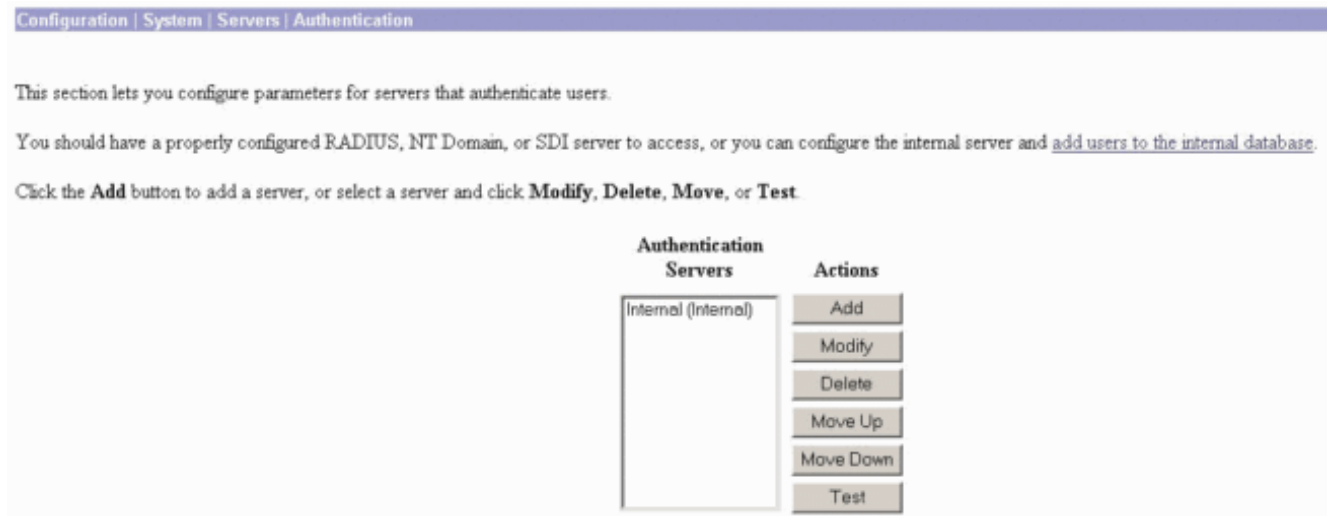


3. この機能を VPN 3002 ハードウェア クライアントでイネーブルにする場合は、HW Client タブで、Require Interactive Hardware Client Authentication がイネーブルにされていることを確認して、Apply をクリックします。



RADIUSの設定

1. コンセントレータでRADIUSサーバの設定を行うには、Configuration > System > Servers > Authentication > Addの順に選択します。



2. Add 画面で、RADIUS サーバに対応する値を入力して、Add をクリックします。下の例では、次の値を使用しています。

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**

Configuration | System | Servers | Authentication | Add

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.
<input type="button" value="Add"/> <input type="button" value="Cancel"/>		

Cisco Secure NT RADIUS サーバの設定

VPN 3000 コンセントレータ用のエントリの設定

1. CSNT にログインして、左側のパネルで Network Configuration をクリックします。「AAA Clients」の下にある Add Entry をクリックします。

The screenshot shows the Cisco Secure Network Configuration interface. On the left is a navigation menu with options like User Setup, Group Setup, Shared Profile Components, Network Configuration, System Configuration, Interface Configuration, Administration Control, External User Databases, Reports and Activity, and Online Documentation. The main area is titled 'Network Configuration' and has a 'Select' dropdown. Below it are three sections: 'AAA Clients', 'AAA Servers', and 'Proxy Distribution Table'. Each section contains a table of configuration entries and an 'Add Entry' button. A red warning message is displayed in the center: 'The current configuration has been changed. Restart ACS in "System Configuration:Service Control" to adopt the new settings.'

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

Add Entry

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

Add Entry Sort Entries

2. 「Add AAA Client」の画面で、適切な値を入力して、コンセントレータを RADIUS クライアントとして追加し、Submit + Restart をクリックします。下の例では、次の値を使用しています。

AAA Client Hostname = **133_3000_conc**

AAA Client IP Address = **172.18.124.133**

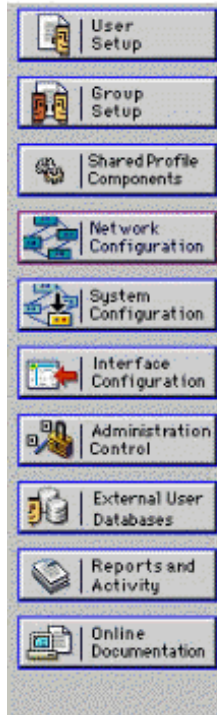
Key = **cisco123**

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	

使用する 3000 コンセントレータのエントリは、「AAA Clients」セクションの下に表示されます。



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)

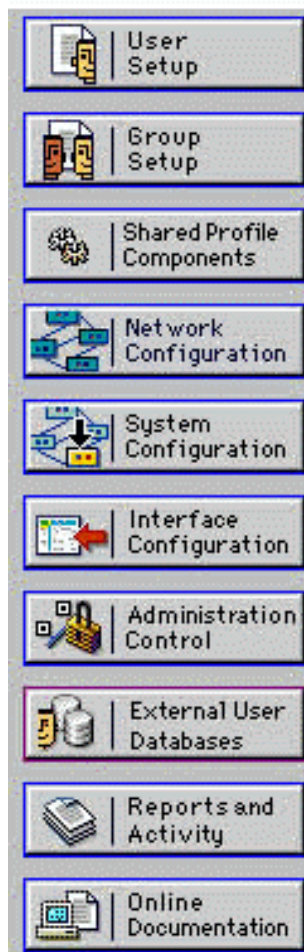
NT ドメイン認証のための未知のユーザのポリシーの設定

1. RADIUS サーバで Unknown User Policy の一部としてユーザ認証を設定する場合は、左側のパネルで External User Database をクリックして、「Database Configuration」へのリンクをクリックします。

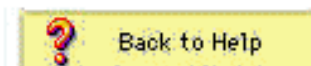


External User Databases

Select



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



2. 「External User Database Configuration」の下にある Windows NT/2000 をクリックします。



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. 「Database Configuration Creation」画面で、Create New Configuration をクリックします。

Database Configuration Creation

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

Create New Configuration

Cancel


4. プロンプトが表示されたら、NT/2000 認証のための名前を入力して、Submit をクリックします。次の例では、「Radius/NT Password Expiration」という名前を使用しています。



External User Databases

Edit



Create a new External Database Configuration 

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


5. Configure をクリックして、ユーザ認証用のドメイン名を設定します。



External User Databases


Edit



External User Database Configuration 

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

6. 「Available Domains」から NT ドメインを選択し、右矢印ボタンをクリックして、これを「Domain List」に追加します。「MS-CHAP Settings」で、Permit password changes using MS-CHAP version 1 と version 2 のオプションが選択されていることを確認します。設定が終了したら、[Submit] をクリックします。



External User Databases

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

Configure Domain List ?


Available Domains		Domain List
	<input type="button" value="→"/> <input type="button" value="←"/>	<div style="background-color: #000080; color: white; padding: 2px;">JAZIB-ADS</div>
		<input type="button" value="Up"/> <input type="button" value="Down"/>

MS-CHAP Settings ?

Permit password changes using MS-CHAP version 1.
 Permit password changes using MS-CHAP version 2.

These settings can be used to enable or disable password changes using the MS-CHAP version 1 or version 2 protocols.

7. 左側のパネルで External User Database をクリックし、次に「Database Group Mappings」へのリンクをクリックします（この例を参照してください）。先に設定した外部データベースのエントリが表示されます。次の例では、先ほど設定したデータベースである「Radius/NT Password Expiration」のエントリが表示されています。



External User Databases

- User Setup
- Group Setup
- Shared Profile Components
- Network Configuration
- System Configuration
- Interface Configuration
- Administration Control
- 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. 「Domain Configurations」画面で、New configuration をクリックして、ドメイン設定を追

加します。



External User Databases



Edit

Domain Configurations ?

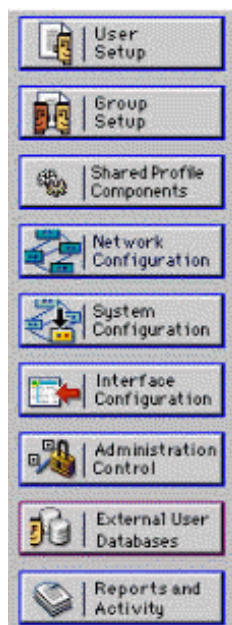
[\DEFAULT](#)

New configuration

9. 「Detected Domains」のリストから使用するドメインを選択して、Submit をクリックします。次の例では、「JAZIB-ADS」という名前のドメインを示しています。



External User Databases



Edit

Define New Domain Configuration ?

Detected Domains:

JAZIB-ADS

Clear Selection

Domain:

Submit Cancel

10. 使用するドメイン名をクリックして、グループのマッピングを設定します。次の例では、ドメイン「JAZIB-ADS」が表示されています。



External User Databases



Edit

Domain Configurations ?

[JAZIB-ADS](#)

[\DEFAULT](#)

New configuration

11. Add mapping をクリックして、グループのマッピングを定義します。



External User Databases

Group Mappings for Domain : JAZIB-ADS

NT groups	CiscoSecure group
	- no mappings defined -

Add mapping

Delete Configuration

12. 「Create new group mapping」画面で、NT ドメイン上のグループを、CSNT RADIUS サーバ上のグループにマップして、Submit をクリックします。次の例では、NT グループ「Users」を RADIUS グループの「Group 1」にマップしています。



External User Databases

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

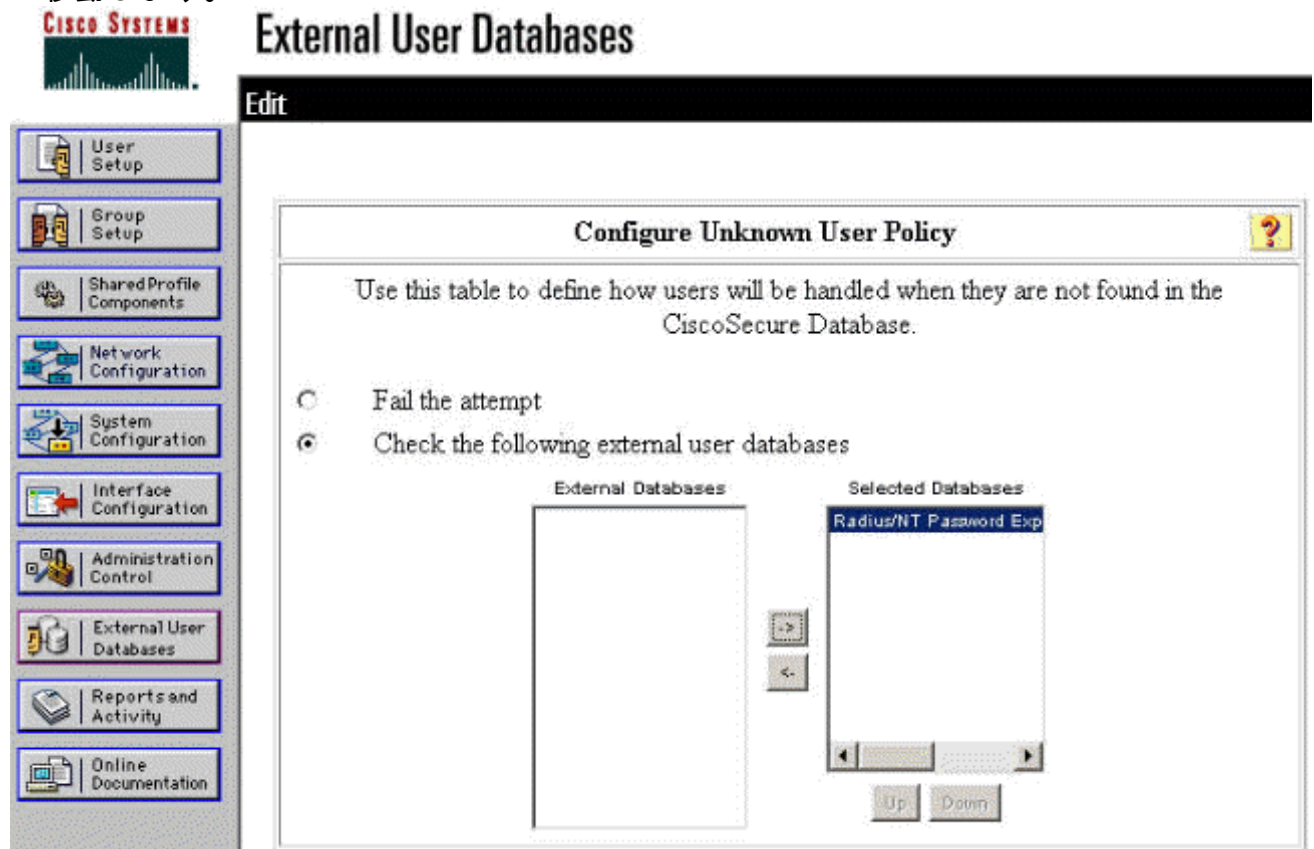
Up Down

CiscoSecure group: Group 1

Submit Cancel

13. 左側のパネルで External User Database をクリックし、次に「Unknown User Policy」へのリンクをクリックします（この例を参照してください）。Check the following external

user databases のオプションを選択します。右矢印ボタンをクリックして、先に設定した外部データベースを「External Databases」のリストから「Selected Databases」のリストへ移動します。



NT/RADIUS パスワード有効期限設定機能のテスト

コンセントレータには、RADIUS 認証をテストする機能があります。この機能を正しく使用するには、次の手順を慎重に行ってください。

RADIUS認証のテスト

1. [Configuration] > [System] > [Servers] > [Authentication] に移動します。使用する RADIUS サーバを選択して、Test をクリックします。



2. プロンプトが表示されたら、NT ドメインのユーザ名とパスワードを入力して、OK をクリックします。次の例では、パスワード「cisco123」を使用している、NT ドメイン サーバで

設定されたユーザ名「jbrahim」を表示しています。


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. 認証が正しく設定されると、「Authentication Successful」というメッセージが表示されま

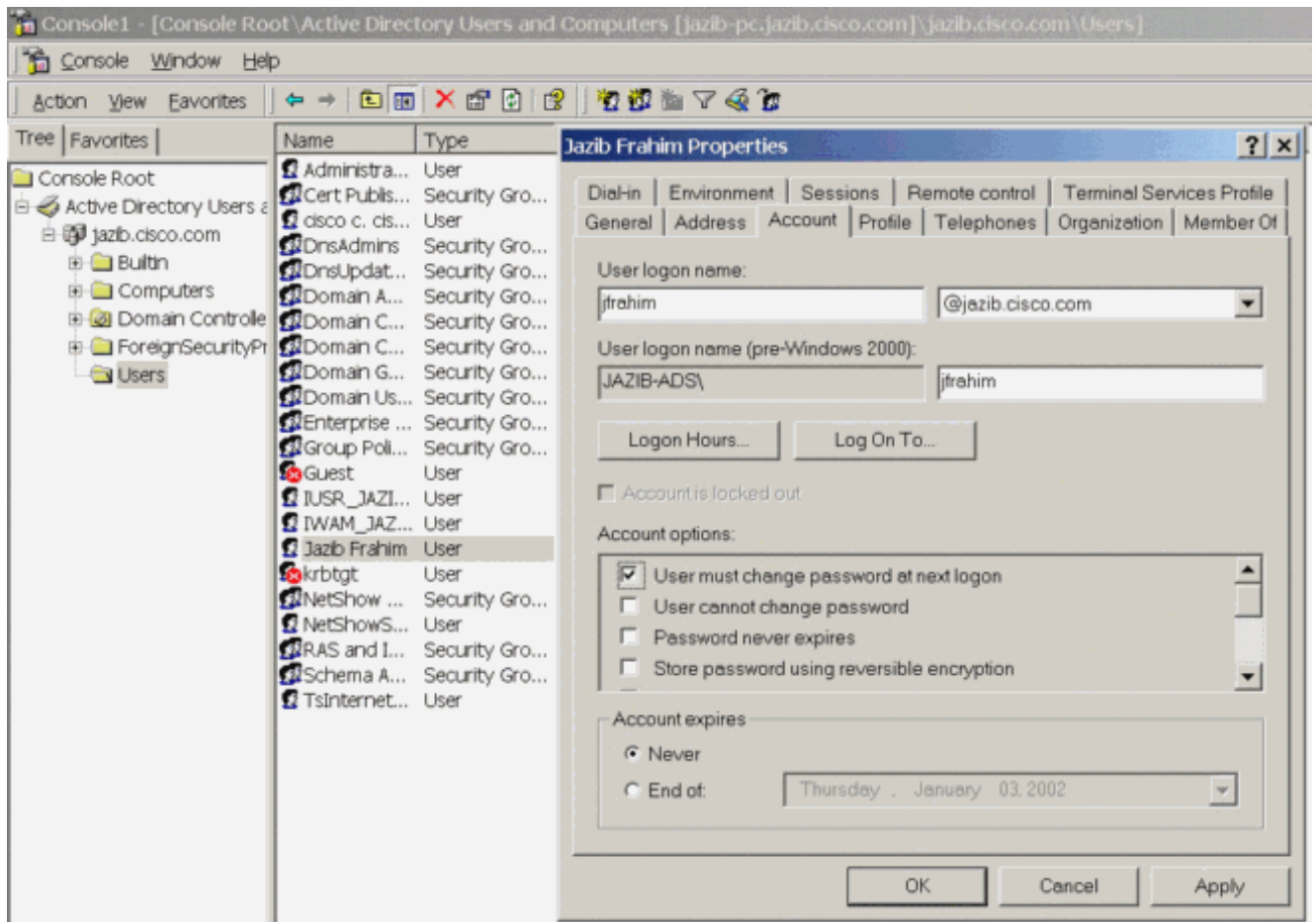
Success

 Authentication Successful

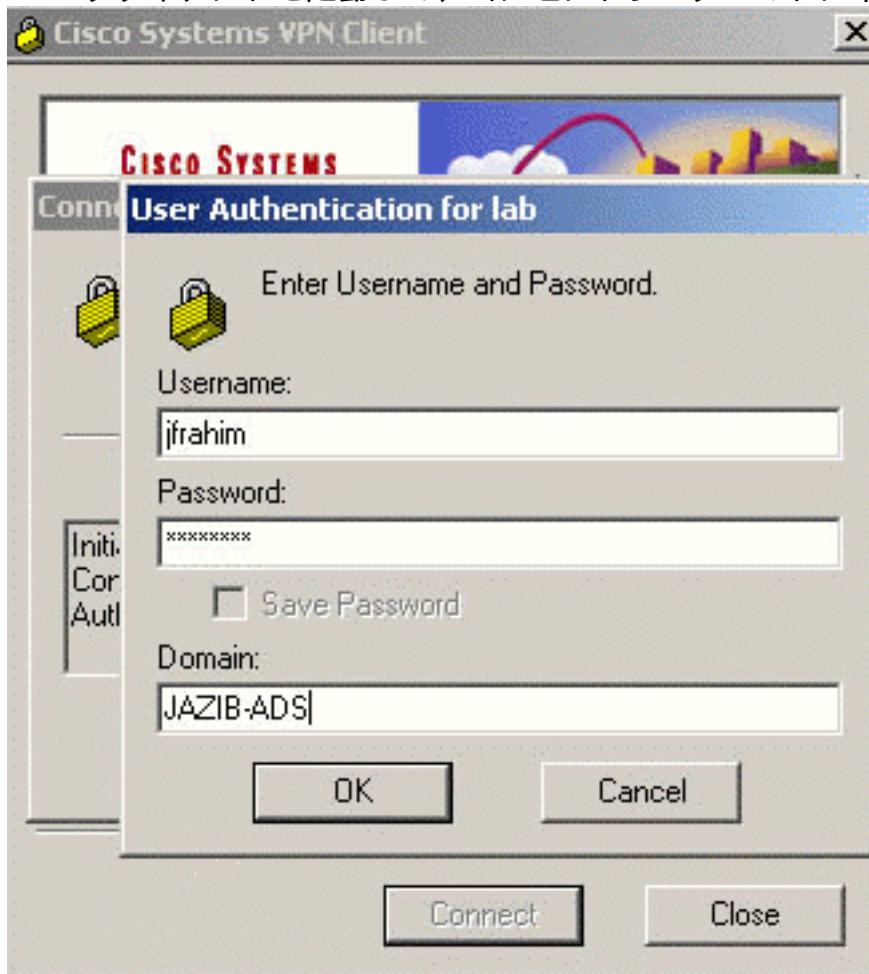
す。上記以外のメッセージが表示された場合は、設定や接続に問題があります。このドキュメントで説明されている設定手順やテスト手順を繰り返して、すべての設定が正しく行われていることを確認してください。また、デバイス間の IP 接続も確認してください。

[RADIUS プロキシを使用する実際の NT ドメイン認証によるパスワード期限切れ機能のテスト](#)

1. ドメイン サーバ上にユーザがすでに定義されている場合は、そのプロパティを変更して、そのユーザが次にログオンするときにパスワードを変更するメッセージが表示されるようにします。ユーザのプロパティのダイアログ ボックスの「Account」タブを表示して、User must change password at next logon のオプションを選択し、OK をクリックします。



2. VPN クライアントを起動して、コンセントレータへのトンネルの確立を試みます。



3. ユーザ認証の際に、パスワードの変更が要求されます。



[関連情報](#)

- [Cisco VPN 3000 シリーズ コンセントレータ](#)
- [IPSec](#)
- [Cisco Secure Access Control Server for Windows](#)
- [RADIUS](#)
- [Requests for Comments \(RFCs\)](#)