

Configuration des concentrateurs de la gamme Cisco VPN 3000 pour une prise en charge de la fonction NT Password Expiration avec le serveur RADIUS

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Diagramme du réseau](#)

[Configuration du concentrateur VPN 3000](#)

[Configuration de groupe](#)

[Configuration RADIUS](#)

[Configuration du serveur Cisco Secure NT RADIUS](#)

[Configuration d'une entrée pour le concentrateur VPN 3000](#)

[Configuration de la stratégie d'utilisateur inconnu pour l'authentification de domaine NT](#)

[Test de la fonction d'expiration du mot de passe NT/RADIUS](#)

[Test de l'authentification RADIUS](#)

[Authentification de domaine NT réelle à l'aide du proxy RADIUS pour tester la fonction d'expiration du mot de passe](#)

[Informations connexes](#)

[Introduction](#)

Ce document inclut des instructions détaillées sur la façon de configurer les concentrateurs de la gamme Cisco VPN 3000 pour prendre en charge la fonctionnalité d'expiration de mot de passe NT à l'aide du serveur RADIUS.

Référez-vous à [VPN 3000 RADIUS avec fonctionnalité d'expiration utilisant Microsoft Internet Authentication Server](#) afin d'en savoir plus sur le même paysage avec Internet Authentication Server (IAS).

[Conditions préalables](#)

[Conditions requises](#)

- Si votre serveur RADIUS et votre serveur d'authentification de domaine NT se trouvent sur deux machines distinctes, vérifiez que vous avez établi une connectivité IP entre les deux

machines.

- Vérifiez que vous avez établi la connectivité IP du concentrateur au serveur RADIUS. Si le serveur RADIUS se trouve vers l'interface publique, n'oubliez pas d'ouvrir le port RADIUS sur le filtre public.
- Assurez-vous que vous pouvez vous connecter au concentrateur à partir du client VPN à l'aide de la base de données utilisateur interne. Si ce n'est pas configuré, reportez-vous à [Configuration d'IPSec - Client VPN Cisco 3000 vers concentrateur VPN 3000](#).

Remarque : La fonction d'expiration du mot de passe ne peut pas être utilisée avec des clients VPN Web ou VPN SSL.

Components Used

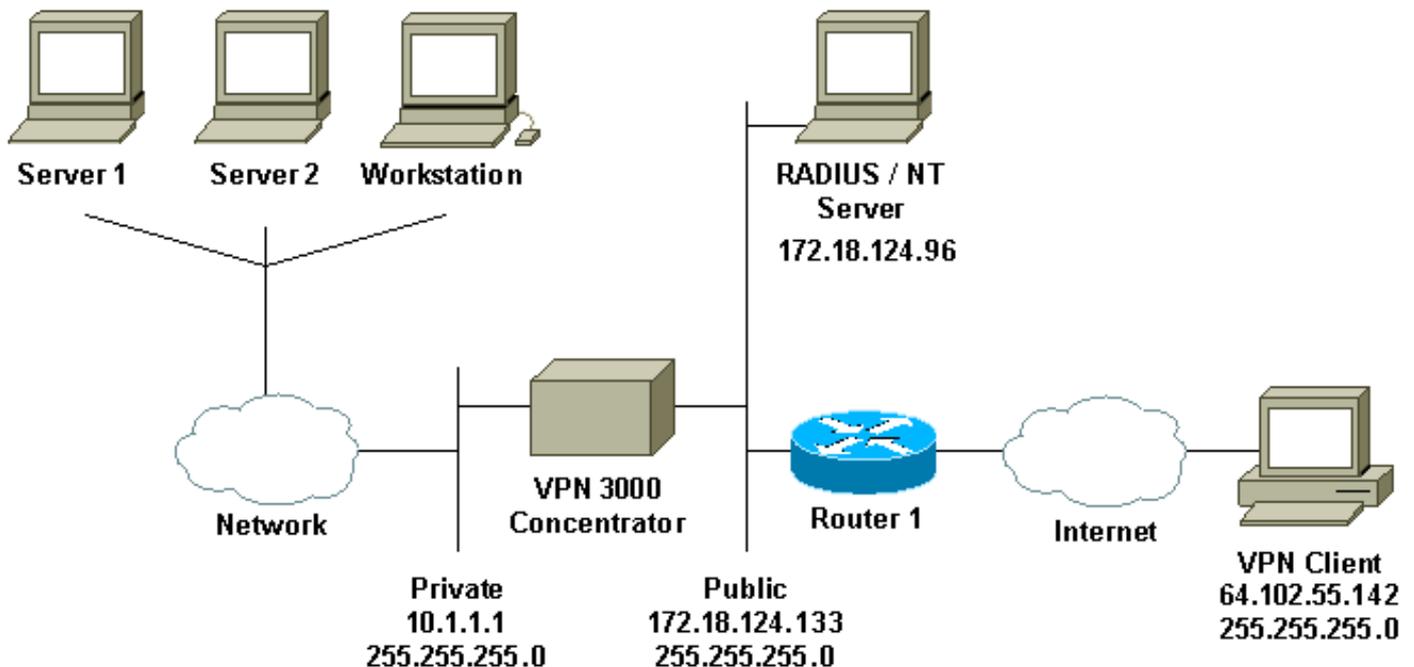
Cette configuration a été développée et testée à l'aide des versions logicielle et matérielle ci-dessous.

- Logiciel du concentrateur VPN 3000 version 4.7
- Client VPN version 3.5
- Cisco Secure pour NT (CSNT) version 3.0 Microsoft Windows 2000 Active Directory Server for User Authentication

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.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Notes de diagramme

1. Le serveur RADIUS dans cette configuration se trouve sur l'interface publique. Si tel est le cas avec votre configuration spécifique, créez deux règles dans votre filtre public pour autoriser le trafic RADIUS à entrer et à quitter le concentrateur.

2. Cette configuration montre le logiciel CSNT et les services d'authentification de domaine NT exécutés sur la même machine. Ces éléments peuvent être exécutés sur deux machines distinctes si votre configuration l'exige.

Configuration du concentrateur VPN 3000

Configuration de groupe

1. Pour configurer le groupe pour qu'il accepte les paramètres d'expiration de mot de passe NT à partir du serveur RADIUS, accédez à **Configuration > User Management > Groups**, sélectionnez votre groupe dans la liste, puis cliquez sur **Modify Group**. L'exemple ci-dessous montre comment modifier un groupe nommé « ipsecgroup ».

2. Accédez à l'onglet **IPSec**, vérifiez que **RADIUS avec expiration** est sélectionné pour l'attribut **Authentication**.

 Select the group's IPSec Security Association. |
IKE Peer Identity Validation
 If supported by certificate | | Select whether or not to validate the identity of the peer using the peer's certificate. |
IKE Keepalives
 | | Check to enable the use of IKE keepalives for members of this group. |
Reauthentication on Rekey
 | | Check to reauthenticate the user on an IKE (Phase-1) rekey. |
Tunnel Type
 Remote Access | | Select the type of tunnel for this group. Update the Remote Access parameters below as needed. |
Group Lock
 | | Lock users into this group. |
Authentication
 RADIUS with Expiry | | Select the authentication method for members of this group. This parameter does not apply to Individual User Authentication. |
IPComp
 RADIUS | | Select the method of IP Compression for members of this group. |
Mode Configuration
 RADIUS with Expiry | | Check to initiate the exchange of Mode Configuration parameters with the client. This must be checked if version 2.5 (or earlier) of the the Aliga/Cisco client are being used by members of this group. |

3. Si vous voulez que cette fonctionnalité soit activée sur les clients matériels VPN 3002, accédez à l'onglet **Client matériel**, assurez-vous que l'option **Exiger une authentification client matériel interactive** est activée, puis cliquez sur **Appliquer**.

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

Configuration RADIUS

1. Pour configurer les paramètres du serveur RADIUS sur le concentrateur, accédez à 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)	<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"/>

2. Dans l'écran **Ajouter**, saisissez les valeurs qui correspondent au serveur RADIUS et cliquez sur **Ajouter**. L'exemple ci-dessous utilise les valeurs suivantes.

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

[Configuration du serveur Cisco Secure NT RADIUS](#)

[Configuration d'une entrée pour le concentrateur VPN 3000](#)

1. Connectez-vous à CSNT et cliquez sur **Configuration réseau** dans le panneau de gauche. Sous « Clients AAA », cliquez sur **Ajouter une entrée**.

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. Dans l'écran « Ajouter un client AAA », saisissez les valeurs appropriées pour ajouter le concentrateur en tant que client RADIUS, puis cliquez sur **Soumettre + Redémarrer**. L'exemple ci-dessous utilise les valeurs suivantes.

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

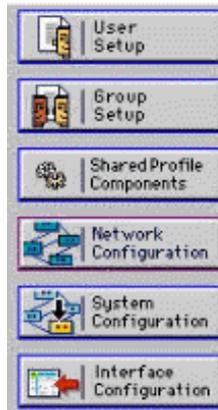
AAA Client Hostname	<input type="text" value="133_3000_conc"/>
AAA Client IP Address	<input type="text" value="172.18.124.133"/>
Key	<input type="text" value="cisco123"/>
Authenticate Using	<input type="text" value="RADIUS (Cisco VPN 3000)"/>
<input type="checkbox"/> Single Connect TACACS+ AAA Client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

Une entrée pour votre concentrateur 3000 apparaîtra sous la section "Clients 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)

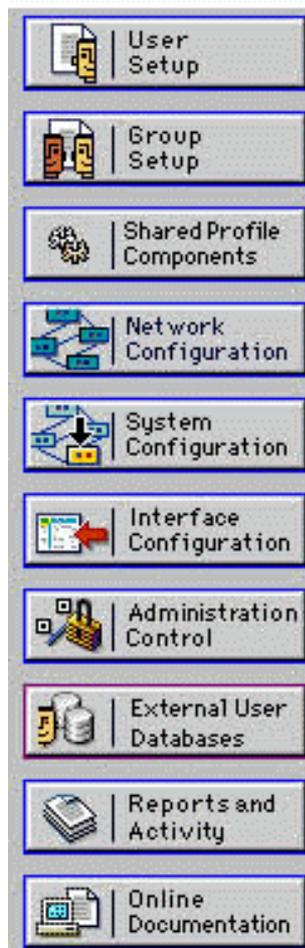
[Configuration de la stratégie d'utilisateur inconnu pour l'authentification de domaine NT](#)

1. Pour configurer l'authentification utilisateur sur le serveur RADIUS dans le cadre de la stratégie utilisateur inconnu, cliquez sur **Base de données utilisateur externe** dans le panneau de gauche, puis cliquez sur le lien pour **Configuration de base de données**.

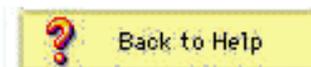


External User Databases

Select



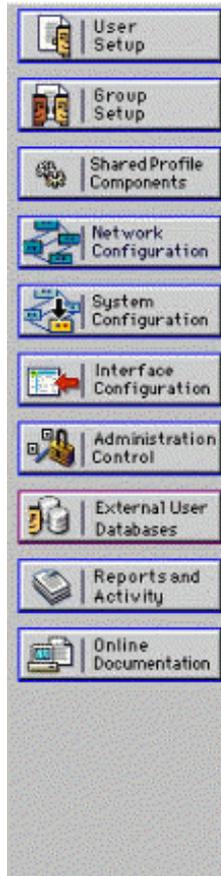
- [Unknown User Policy](#)
- [Database Group Mappings](#)
- [Database Configuration](#)



2. Sous Configuration de base de données utilisateur externe, cliquez sur **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](#)

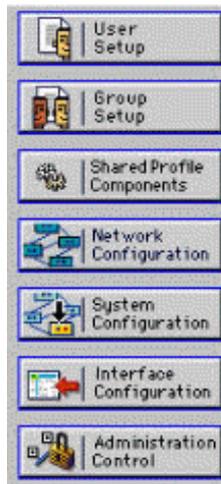
[List all database configurations](#)

Cancel

3. Dans l'écran Création de la configuration de base de données, cliquez sur **Créer une 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. Lorsque vous y êtes invité, tapez un nom pour l'authentification NT/2000 et cliquez sur **Submit**. L'exemple ci-dessous montre le nom « Radius/NT Password Expiration.

»



External User Databases



Edit

Create a new External Database Configuration ?

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

5. Cliquez sur **Configurer** pour configurer le nom de domaine pour l'authentification utilisateur.



External User Databases



Edit

External User Database Configuration ?

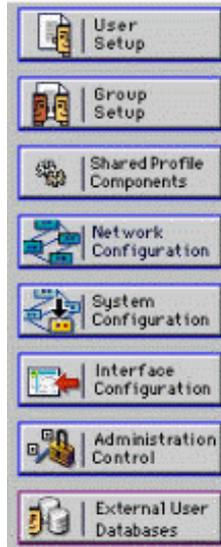
Choose what to do with the Windows NT/2000 database.

6. Sélectionnez votre domaine NT dans la zone « Domaines disponibles », puis cliquez sur la flèche droite pour l'ajouter à la liste de domaines. Sous « Paramètres MS-CHAP », assurez-vous que les options **Permit password change en utilisant MS-CHAP version 1 et version 2** sont sélectionnées. Cliquez sur **Submit** lorsque vous avez terminé.

7. Cliquez sur **Base de données d'utilisateurs externes** dans le panneau de gauche, puis cliquez sur le lien correspondant aux **mappages de groupes de bases de données** (comme dans cet [exemple](#)). Vous devriez voir une entrée pour votre base de données externe précédemment configurée. L'exemple ci-dessous montre une entrée pour « Radius/NT Password Expiration », la base de données que nous venons de configurer.



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. Dans l'écran « Configurations de domaine », cliquez sur **Nouvelle configuration** pour ajouter les configurations de domaine.



External User Databases



Edit

Domain Configurations 

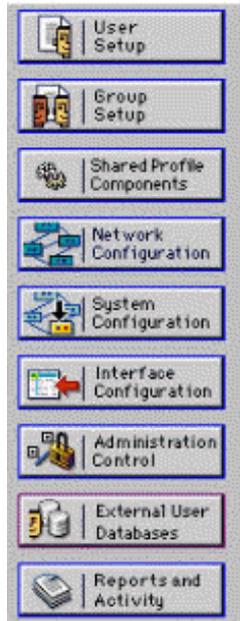
[DEFAULT](#)

9. Sélectionnez votre domaine dans la liste des domaines détectés et cliquez sur **Soumettre**. L'exemple ci-dessous montre un domaine nommé « JAZIB-ADS.

»



External User Databases



Edit

Define New Domain Configuration

Detected Domains:

JAZIB-ADS

Clear Selection

Domain:

Submit Cancel

10. Cliquez sur votre nom de domaine pour configurer les mappages de groupe. Cet exemple montre le domaine « JAZIB-ADS ».

»



External User Databases



Edit

Domain Configurations

[JAZIB-ADS](#)

[DEFAULT](#)

New configuration

11. Cliquez sur **Ajouter un mappage** pour définir les mappages de groupe.



External User Databases

Edit

Group Mappings for Domain : JAZIB-ADS

NT groups	CiscoSecure group
	- no mappings defined -

Add mapping

Delete Configuration

12. Dans l'écran « Créer un nouveau mappage de groupe », mappez le groupe sur le domaine NT à un groupe sur le serveur RADIUS CSNT, puis cliquez sur **Soumettre**. L'exemple ci-dessous mappe le groupe NT « Users » au groupe RADIUS « Group 1 ».

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

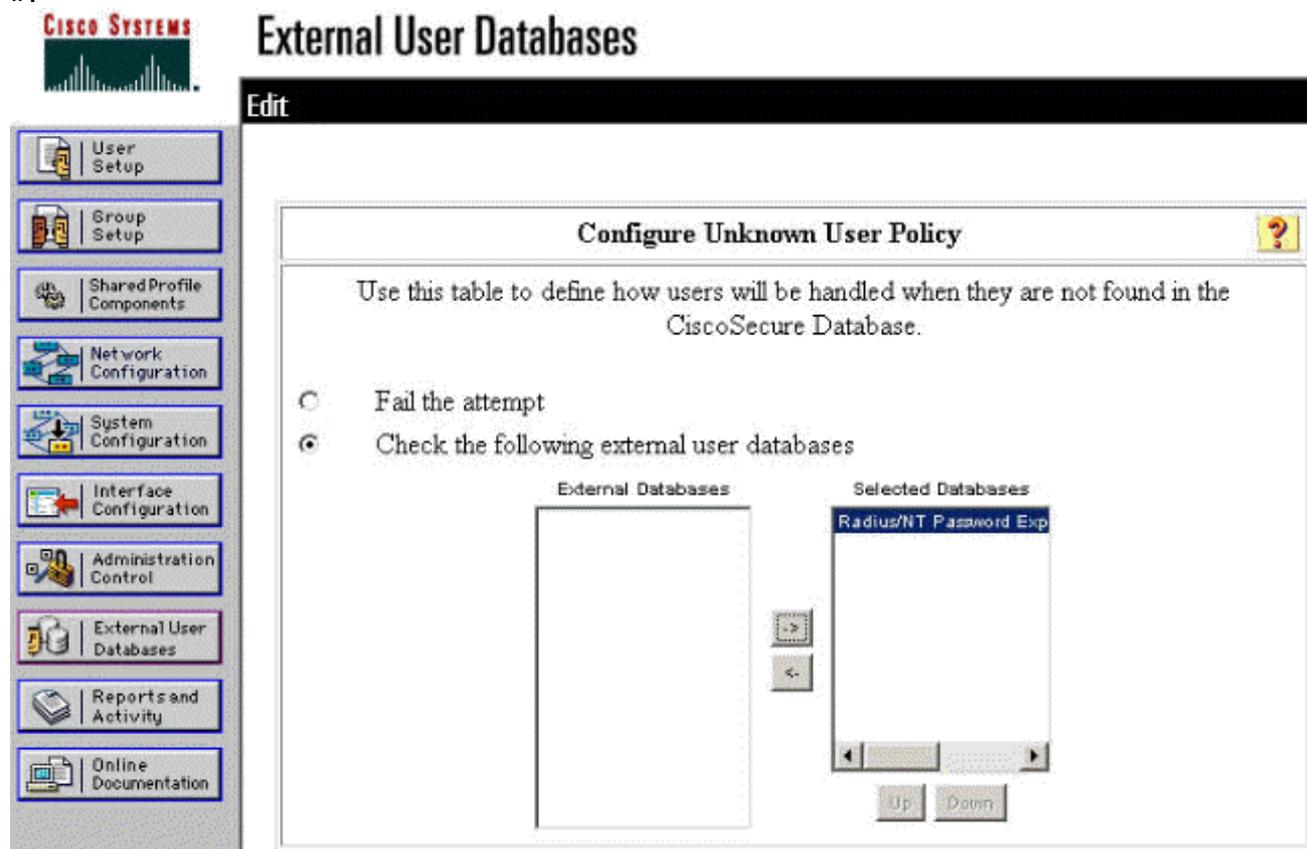
CiscoSecure group: Group 1

Submit Cancel

13. Cliquez sur **Base de données utilisateur externe** dans le panneau de gauche, puis cliquez

sur le lien **Stratégie utilisateur inconnu** (comme dans cet [exemple](#)). Assurez-vous que l'option **Vérifier les bases de données utilisateur externes suivantes** est sélectionnée. Cliquez sur la flèche droite pour déplacer la base de données externe précédemment configurée de la liste des « bases de données externes » vers la liste des « bases de données sélectionnées »

».



[Test de la fonction d'expiration du mot de passe NT/RADIUS](#)

Le concentrateur offre une fonction pour tester l'authentification RADIUS. Pour tester correctement cette fonctionnalité, veillez à suivre attentivement ces étapes.

[Test de l'authentification RADIUS](#)

1. Accédez à **Configuration > System > Servers > Authentication**. Sélectionnez votre serveur RADIUS et cliquez sur **Test**.

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

- Lorsque vous y êtes invité, tapez votre nom d'utilisateur et votre mot de passe de domaine NT, puis cliquez sur **OK**. L'exemple ci-dessous montre le nom d'utilisateur « jfracim » configuré sur le serveur de domaine NT avec « cisco123 » comme mot de passe.

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

User Name

Password

- Si votre authentification est configurée correctement, vous devez recevoir un message indiquant « Authentication Success

Success

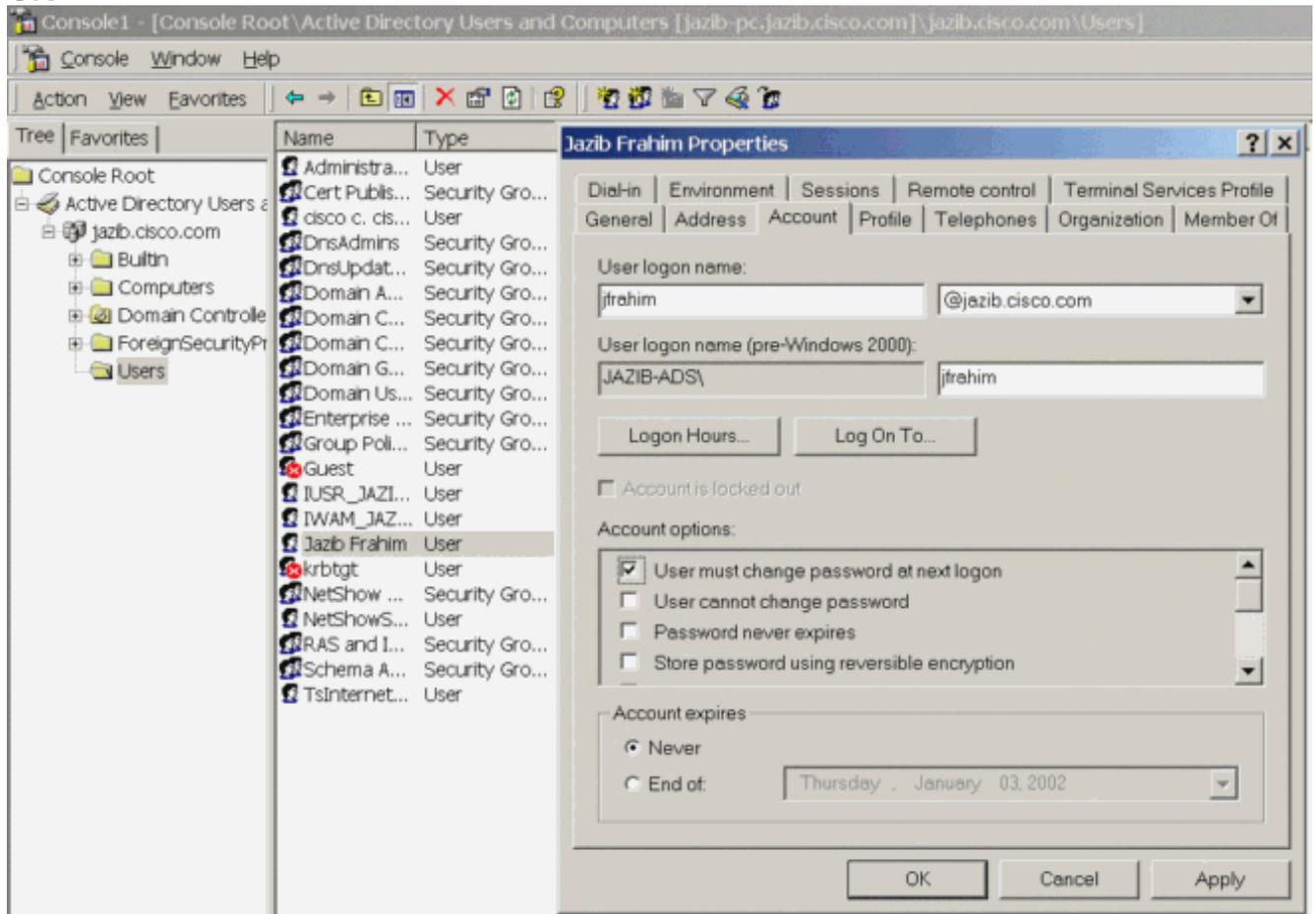
 Authentication Successful

». Si vous recevez un message autre que celui présenté ci-dessus, il y a un problème de configuration ou de connexion. Répétez les étapes de configuration et de test décrites dans ce document pour vous assurer que tous les paramètres ont été correctement définis. Vérifiez également la connectivité IP entre vos périphériques.

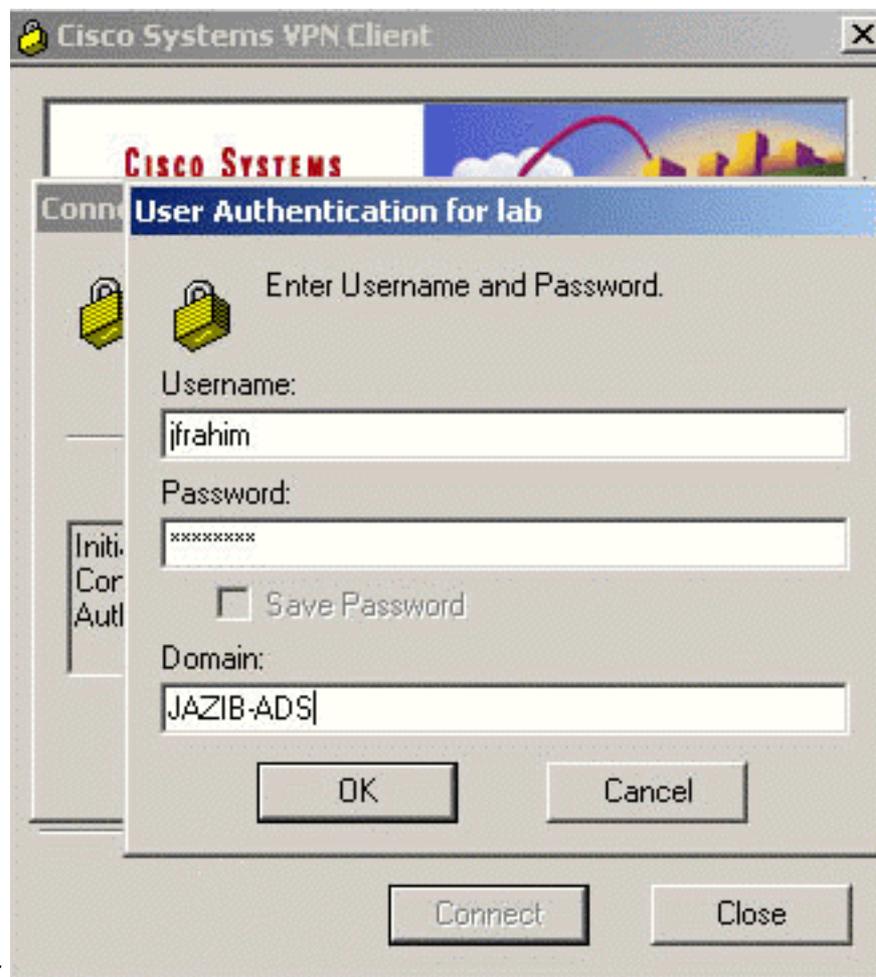
[Authentification de domaine NT réelle à l'aide du proxy RADIUS pour tester la fonction d'expiration du mot de passe](#)

- Si l'utilisateur est déjà défini sur le serveur de domaine, modifiez les propriétés afin que l'utilisateur soit invité à modifier le mot de passe lors de la prochaine connexion. Accédez à l'onglet « Compte » de la boîte de dialogue des propriétés de l'utilisateur, sélectionnez

l'option pour l'utilisateur doit changer de mot de passe lors de la prochaine ouverture de session, puis cliquez sur OK.

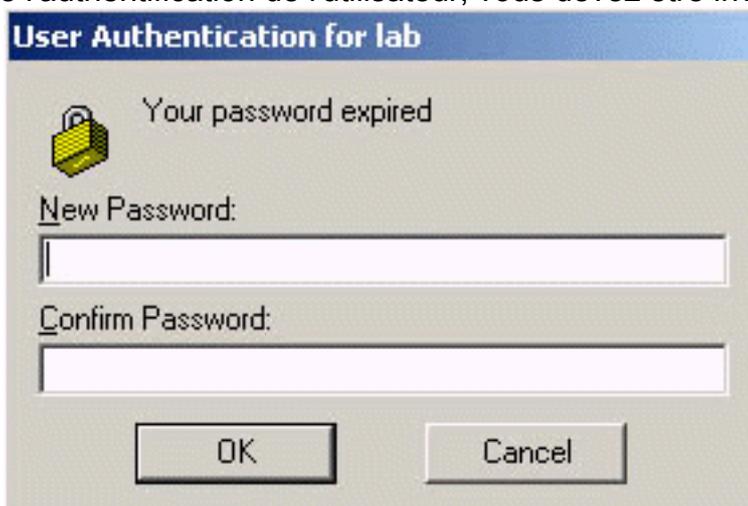


2. Lancez le client VPN, puis essayez d'établir le tunnel vers le



concentrateur.

3. Lors de l'authentification de l'utilisateur, vous devez être invité à modifier le mot de



passee.

[Informations connexes](#)

- [Concentrateur de la gamme Cisco VPN 3000](#)
- [IPsec](#)
- [Cisco Secure Access Control Server pour Windows](#)
- [RADIUS](#)
- [Demandes de commentaires \(RFC\)](#)