

Cisco VPN 3000 Series تازكرم نيوكتب مق NT رورم ةملك ةيحالص ءاهتنا ةزي م عدل RADIUS مداخ مادختساب

المحتويات

- [المقدمة](#)
- [المتطلبات الأساسية](#)
- [المتطلبات](#)
- [المكونات المستخدمة](#)
- [الرسم التخطيطي للشبكة](#)
- [تكوين مركز VPN 3000](#)
- [تكوين المجموعة](#)
- [تهيئة RADIUS](#)
- [تكوين خادم Cisco Secure NT RADIUS](#)
- [تكوين إدخال لمركز VPN 3000](#)
- [تكوين نهج مستخدم غير معروف لمصادقة مجال NT](#)
- [إختبار ميزة انتهاء صلاحية كلمة مرور NT/RADIUS](#)
- [إختبار مصادقة RADIUS](#)
- [مصادقة مجال NT الفعلية باستخدام وكيل RADIUS لإختبار ميزة انتهاء صلاحية كلمة المرور](#)
- [معلومات ذات صلة](#)

المقدمة

يتضمن هذا المستند إرشادات خطوة بخطوة حول كيفية تكوين مراكز Cisco VPN 3000 Series لدعم ميزة انتهاء صلاحية كلمة مرور NT باستخدام خادم RADIUS.

ارجع إلى [VPN 3000 RADIUS مع ميزة انتهاء الصلاحية باستخدام خادم مصادقة الإنترنت من Microsoft](#) لمعرفة المزيد حول نفس السيناريو مع خادم مصادقة الإنترنت (IAS).

المتطلبات الأساسية

المتطلبات

- إذا كان خادم RADIUS وخادم مصادقة مجال NT على جهازين منفصلين، فتأكد من إنشاء اتصال IP بين الجهازين.
- تأكد من تحديد اتصال IP من مركز التركيز إلى خادم RADIUS. إذا كان خادم RADIUS باتجاه الواجهة العامة، فلا تتس فتح منفذ RADIUS على المرشح العام.
- ضمنت أن أنت يستطيع ربطت إلى مركز من ال VPN زبون يستعمل ال داخلي مستعمل قاعدة معطيات. إذا لم يتم تكوين هذا الأمر، فيرجى الرجوع إلى [تكوين IPsec - عمل Cisco 3000 VPN إلى مركز VPN 3000](#).

ملاحظة: لا يمكن إستخدام ميزة انتهاء صلاحية كلمة المرور مع عملاء Web VPN أو SSL VPN.

المكونات المستخدمة

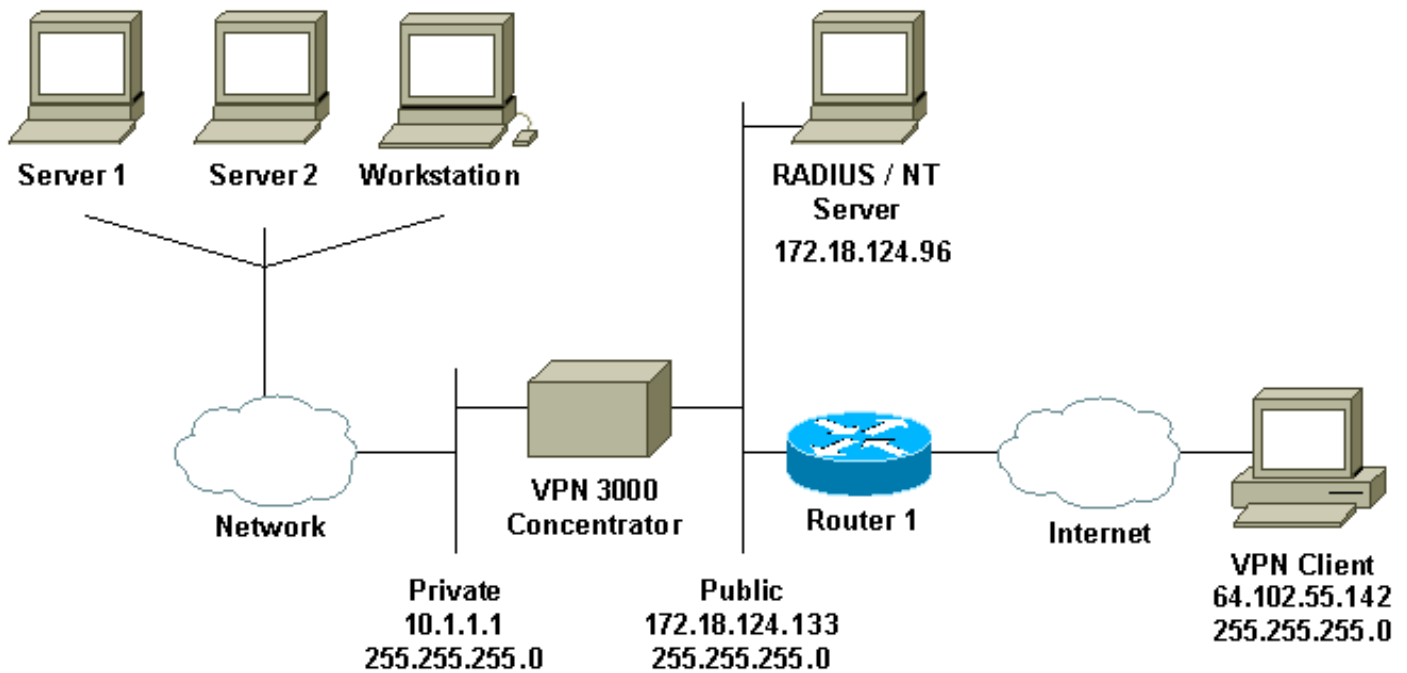
تم تطوير هذه التهيئة واختبارها باستخدام إصدارات البرامج والمكونات المادية الواردة أدناه.

- برنامج VPN 3000 Concentrator، الإصدار 4.7
- عميل شبكة VPN، الإصدار 3.5
- الإصدار Microsoft Windows 2000 Active Directory Server 3.0 (Cisco Secure for NT (CSNT لمصادقة المستخدم

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:



ملاحظات المخطط

1. يكون خادم RADIUS الموجود في هذا التكوين على الواجهة العامة. إذا كان هذا هو الحال مع الإعداد المحدد، يرجى إنشاء قاعدتين في مرشح عام للسماح لحركة مرور RADIUS بإدخال وترك المركز.
2. يوضح هذا التكوين خدمات مصادقة مجال CSNT و NT التي تعمل على نفس الجهاز. يمكن تشغيل هذه العناصر على جهازين منفصلين إذا تطلب التكوين الخاص بك ذلك.

تكوين مركز VPN 3000

تكوين المجموعة

1. لتكوين المجموعة لقبول معلمات انتهاء صلاحية كلمة مرور NT من خادم RADIUS، انتقل إلى التكوين <إدارة المستخدم> المجموعات، وحدد مجموعتك من القائمة، وانقر فوق تعديل المجموعة. يوضح المثال التالي كيفية

تعديل مجموعة تسمى "ipsecgroup".

Configuration | User Management | Groups Save Needed

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 other group parameters, click **Modify Auth. Servers**, **Modify Acct. Servers**, **Modify Address Pools** or **Modify Client Update**.

Current Groups

ipsecgroup (Internally Configured)

Actions

Add Group

Modify Group

Modify Auth. Servers

Modify Acct. Servers

Modify Address Pools

Modify Client Update

Delete Group

2. انتقل إلى علامة التبويب IPsec، وتأكد من تحديد RADIUS مع انتهاء الصلاحية للسمة المصادقة.

Configuration | User Management | Groups | Modify ipsecgroup

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 | Mode Config | Client FW | HW Client | PPTP/L2TP

| 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 of the peer using the peer's certificate. |
| IKE Keepalives | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Check to enable the use of IKE keepalives for members of this group. |
| Reauthentication on Rekey | <input type="checkbox"/> | <input checked="" type="checkbox"/> | Check to reauthenticate the user on an IKE (Phase-1) rekey. |
| Tunnel Type | Remote Access | <input checked="" type="checkbox"/> | Select the type of tunnel for this group. Update the Remote Access parameters below as needed. |
| Remote Access Parameters | | | |
| Group Lock | <input type="checkbox"/> | <input checked="" type="checkbox"/> | Lock users into this group. |
| Authentication | RADIUS with Expiry | <input type="checkbox"/> | Select the authentication method for members of this group. This parameter does not apply to Individual User Authentication . |
| IPComp | None | <input checked="" type="checkbox"/> | Select the method of IP Compression for members of this group. |
| Mode Configuration | RADIUS with Expiry | <input checked="" type="checkbox"/> | 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 Ahiga/Cisco client are being used by members of this group. |

Apply Cancel

3. إذا كنت تريد تمكين هذه الميزة على أجهزة VPN 3002 العميلة، فانتقل إلى علامة التبويب عميل HW، وتأكد من تمكين متطلبات مصادقة عميل الجهاز التفاعلية، ثم انقر فوق تطبيق.

Configuration | User Management | Groups | Modify ipsecgroup

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 | Mode Config | Client FW | HW Client | PPTP/L2TP

| 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

تهيئة RADIUS

1. لتكوين إعدادات خادم RADIUS على مركز التركيز، انتقل إلى التكوين < النظام > الخوادم < المصادقة > إضافة.

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 |

على الشاشة إضافة، اكتب القيم التي تترادف خادم RADIUS وانقر إضافة. يستخدم المثال التالي القيم التالية. 2.
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. |
| <input type="button" value="Add"/> <input type="button" value="Cancel"/> | | |

[تكوين خادم Cisco Secure NT RADIUS](#)

[تكوين إدخال لمركز VPN 3000](#)

1. قم بتسجيل الدخول إلى CSNT وانقر فوق تكوين الشبكة في اللوحة اليسرى. تحت "عملاء AAA"، انقر فوق إضافة إدخال.

The screenshot shows the Cisco Systems 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 content area is titled 'Select' and contains three sections:

- AAA Clients:** A table with columns 'AAA Client Hostname', 'AAA Client IP Address', and 'Authenticate Using'. It contains one entry with hostname 'nsize', IP '172.18.141.40', and authentication 'RADIUS (Cisco IOS/PIX)'. Below the table is an 'Add Entry' button.
- AAA Servers:** A table with columns 'AAA Server Name', 'AAA Server IP Address', and 'AAA Server Type'. It contains one entry with name 'jazib-pc', IP '172.18.124.96', and type 'CiscoSecure ACS for Windows 2000/NT'. Below the table is an 'Add Entry' button.
- Proxy Distribution Table:** A table with columns 'Character String', 'AAA Servers', 'Strip', and 'Account'. It contains one entry with character string '(Default)', AAA Servers 'jazib-pc', Strip 'No', and Account 'Local'. Below the table are 'Add Entry' and 'Sort Entries' buttons.

A red message box in the center states: "The current configuration has been changed. Restart ACS in "System Configuration:Service Control" to adopt the new settings."

في شاشة "إضافة عميل AAA"، اكتب القيم المناسبة لإضافة مركز كعميل RADIUS، ثم انقر فوق إرسال + 2. إعادة تشغيل. يستخدم المثال التالي القيم التالية.

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

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

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 | |

سوف يظهر مدخل لمركز تركيزك 3000 ضمن قسم عملاء "AAA".



Network Configuration

Select

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

| 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) |

تكوين نهج مستخدم غير معروف لمصادقة مجال NT

1. لتكوين مصادقة المستخدم على خادم RADIUS كجزء من نهج المستخدم غير المعروف، انقر فوق قاعدة بيانات المستخدم الخارجي في اللوحة اليسرى، ثم انقر فوق الارتباط لتكوين قاعدة البيانات.



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](#)

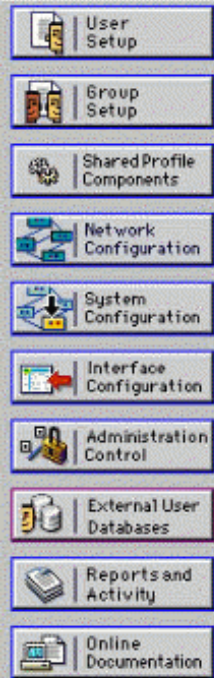
[Back to Help](#)

2. تحت "تكوين قاعدة بيانات المستخدم الخارجي"، انقر فوق 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](#)

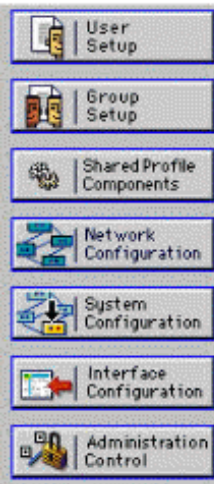
Cancel

3. في الشاشة "إنشاء تكوين قاعدة البيانات"، انقر فوق إنشاء تكوين جديد.



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. عندما يطلب منك، اكتب اسم لمصادقة NT/2000 وانقر إرسال. يوضح المثال التالي اسم "انتهاء صلاحية كلمة مرور RADIUS/NT".



External User Databases

Edit



Create a new External Database Configuration 

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


5. انقر على تكوين لتكوين اسم المجال لمصادقة المستخدم.



External User Databases

Edit



External User Database Configuration 

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

6. حدد مجال NT الخاص بك من "المجالات المتاحة"، ثم انقر فوق زر السهم الأيمن لإضافته إلى "قائمة المجالات". تحت "إعدادات MS-CHAP"، تأكد من تحديد خيارات السماح بتغييرات كلمة المرور باستخدام MS-CHAP الإصدار 1 والإصدار 2. انقر فوق إرسال عند الانتهاء.



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

JAZIB-ADS

Up 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. انقر فوق قاعدة بيانات المستخدم الخارجي في اللوحة اليسرى، ثم انقر فوق الارتباط الخاص بتعيينات مجموعة قواعد البيانات (كما يظهر في هذا المثال). يجب أن ترى إدخالاً لقاعدة البيانات الخارجية التي تم تكوينها مسبقاً. يوضح المثال التالي إدخال "انتهاء صلاحية كلمة مرور RADIUS/NT"، قاعدة البيانات التي قمنا بتكوينها للتو.



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 |

Cancel

8. في الشاشة "تكوينات المجال"، انقر فوق تكوين جديد لإضافة تكوينات



External User Databases

Edit



Domain Configurations ?

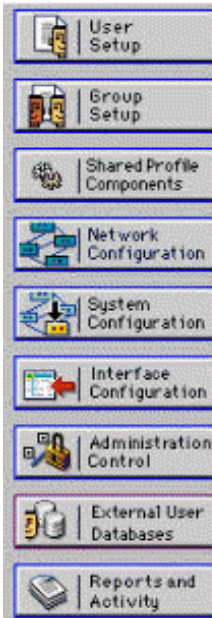
[\DEFAULT](#)

9. حدد مجالك من قائمة "المجالات التي تم الكشف عنها" وانقر فوق إرسال. المثال التالي يوضح مجال يسمى JAZIB-"
".ADS



External User Databases

Edit



Define New Domain Configuration ?

Detected Domains:

JAZIB-ADS

Domain :

10. انقر فوق اسم المجال لتكوين تعيينات المجموعة. هذا المثال يوضح المجال JAZIB-"
".ADS



External User Databases

Edit



Domain Configurations ?

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

11. انقر فوق إضافة تخطيط لتحديد تعيينات المجموعة.



External User Databases

Edit

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

12. في الشاشة "إنشاء تعيين مجموعة جديد"، قم بتعيين المجموعة الموجودة في مجال NT إلى مجموعة على خادم CSNT RADIUS، ثم انقر فوق إرسال. يوضح المثال التالي مجموعة "Users" NT إلى مجموعة "RADIUS Group".

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

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:

Submit Cancel

13. انقر فوق قاعدة بيانات المستخدم الخارجي في اللوحة اليسرى، ثم انقر فوق الارتباط الخاص ب نهج المستخدم غير المعروف (كما يظهر في هذا [المثال](#)). تأكد من تحديد خيار التحقق من قواعد بيانات المستخدم الخارجية التالية. انقر فوق الزر الأيمن لنقل قاعدة البيانات الخارجية التي تم تكوينها مسبقا من قائمة "قواعد البيانات الخارجية" إلى قائمة "قواعد البيانات المحددة".

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

Configure Unknown User Policy

Use this table to define how users will be handled when they are not found in the CiscoSecure Database.

Fail the attempt
 Check the following external user databases

| External Databases | | Selected Databases |
|--------------------|--|--|
| | <input type="button" value="→"/> <input type="button" value="←"/> | <div style="background-color: #e0e0e0; padding: 2px;">Radius/NT Password Exp</div> |
| | <input type="button" value="Up"/> <input type="button" value="Down"/> | |

إختبار ميزة انتهاء صلاحية كلمة مرور NT/RADIUS

ويوفر مركز التركيز وظيفة لاختبار مصادقة RADIUS. لاختبار هذه الميزة بشكل صحيح، تأكد من أنك تتبع هذه الخطوات بعناية.

إختبار مصادقة RADIUS

1. انتقل إلى التكوين > النظام > الخوادم > المصادقة. حدد خادم RADIUS وانقر فوق إختبار.

Configuration | System | Servers | Authentication

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"/> |
| 172.18.124.96 (Radius) | |

2. عندما يطلب منك، اكتب اسم مستخدم وكلمة مرور مجال NT، ثم انقر على موافق. يوضح المثال التالي اسم المستخدم "jfracim" الذي تم تكوينه على خادم مجال NT مع "Cisco123" ككلمة المرور.

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

User Name

Password

3. في حالة إعداد المصادقة بشكل صحيح، يجب أن تحصل على رسالة تذكر "نجاح"

Success

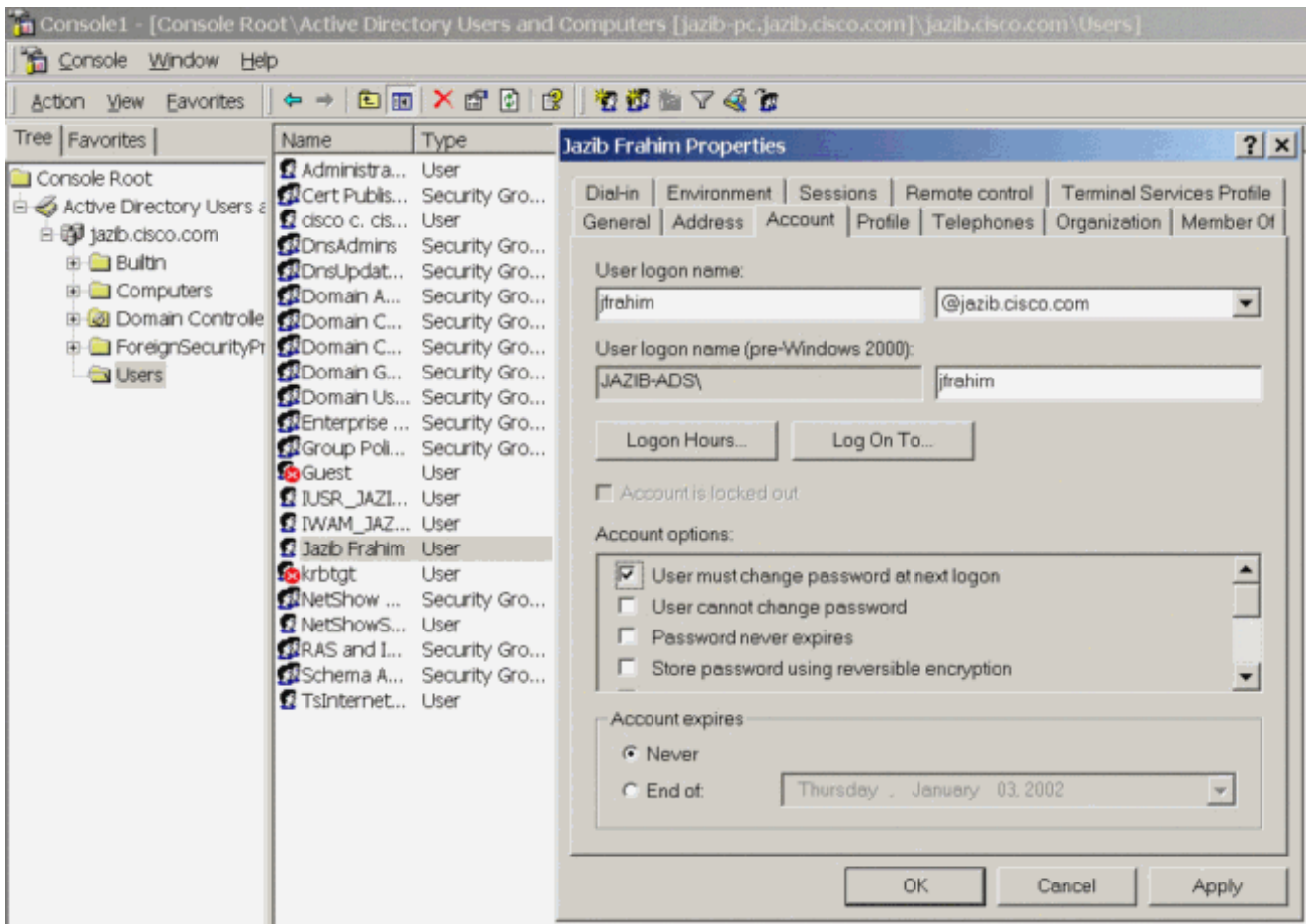


Authentication Successful

المصادقة." إذا ظهرت لديك أي رسالة أخرى غير الرسالة الموضحة أعلاه، فهذا يعني وجود مشكلة في التكوين أو الاتصال. يرجى تكرار خطوات التكوين والاختبار الموضحة في هذا المستند لضمان إجراء جميع الإعدادات بشكل صحيح. تحقق أيضا من اتصال IP بين أجهزتك.

مصادقة مجال NT الفعلية باستخدام وكيل RADIUS لاختبار ميزة انتهاء صلاحية كلمة المرور

1. إذا تم تعريف المستخدم بالفعل على خادم المجال، فقم بتعديل الخصائص بحيث تتم مطالبة المستخدم بتغيير كلمة المرور عند تسجيل الدخول التالي. انتقل إلى علامة التبويب "حساب" في مربع الحوار "خصائص" المستخدم، وحدد الخيار الذي يجب أن يقوم المستخدم بتغيير كلمة المرور عند تسجيل الدخول التالي، ثم انقر فوق موافق.



2. قم بتشغيل عميل الشبكة الخاصة الظاهرية (VPN)، ثم حاول إنشاء النفق إلى مركز



التركيز.

3. أثناء مصادقة المستخدم، يجب مطالبتك بتغيير كلمة



المرو.

معلومات ذات صلة

- [مركز Cisco VPN 3000 Series](#)
- [IPsec](#)
- [خادم التحكم في الوصول الآمن من Cisco لأنظمة التشغيل Windows](#)
- [RADIUS](#)
- [طلبات التعليقات \(RFCs\)](#)

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة مادختساب دن تسمل اذة Cisco تمةرت
ملاعلاء انء مء مء نمة دختسمل معد و تمة مء دقتل ةر شبل او
امك ةق قء نوك ت نل ةللأل ةمچرت لصف أن ةظحال مء ءرء. ةصاأل مء تءل ب
Cisco ةللخت. فرتمة مچرت مء مء دقء ةللأل ةل فارتحال ةمچرتل عم لاعل او
ىل إأمءءاد ءوچرلاب ةصوءو تاملرتل هذه ةقء نء اهءل وئس م Cisco
Systems (رفوتم طبارل) ةلصلأل ةزءل ءنل اءل دن تسمل