

مادختساب Cisco VPN 3000 زكرم نيوكت Microsoft RADIUS

المحتويات

[المقدمة](#)

[المتطلبات الأساسية](#)

[المتطلبات](#)

[المكونات المستخدمة](#)

[الاصطلاحات](#)

[تثبيت خادم RADIUS وتكوينه على Windows 2000 و Windows 2003](#)

[تثبيت خادم RADIUS](#)

[تكوين خادم Microsoft Windows 2000 باستخدام IAS](#)

[تكوين خادم Microsoft Windows 2003 باستخدام IAS](#)

[تكوين مركز Cisco VPN 3000 لمصادقة RADIUS](#)

[التحقق من الصحة](#)

[استكشاف الأخطاء وإصلاحها](#)

[فشل مصادقة WebVPN](#)

[فشل مصادقة المستخدم مقابل Active Directory](#)

[معلومات ذات صلة](#)

المقدمة

خادم مصادقة الإنترنت من Microsoft (IAS) ونظام الإنترنت التجاري من Microsoft (MCIS 2.0) متاحان حالياً. خادم Microsoft RADIUS مناسب لأنه يستخدم Active Directory على وحدة التحكم بالمجال الأساسية لقاعدة بيانات المستخدم الخاصة به. لم تعد بحاجة إلى الاحتفاظ بقاعدة بيانات منفصلة. كما يدعم تشفير 40-بت و 128-بت لاتصالات شبكة VPN لبروتوكول الاتصال النفقي من نقطة إلى نقطة (PPTP). راجع [قائمة التحقق من Microsoft](#): تكوين IAS لوثائق الطلب الهاتفي والوصول إلى VPN للحصول على مزيد من المعلومات.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

لا يقتصر هذا المستند على إصدارات برامج ومكونات مادية معينة.

الاصطلاحات

تثبيت خادم RADIUS وتكوينه على Windows 2000 و Windows 2003

تثبيت خادم RADIUS

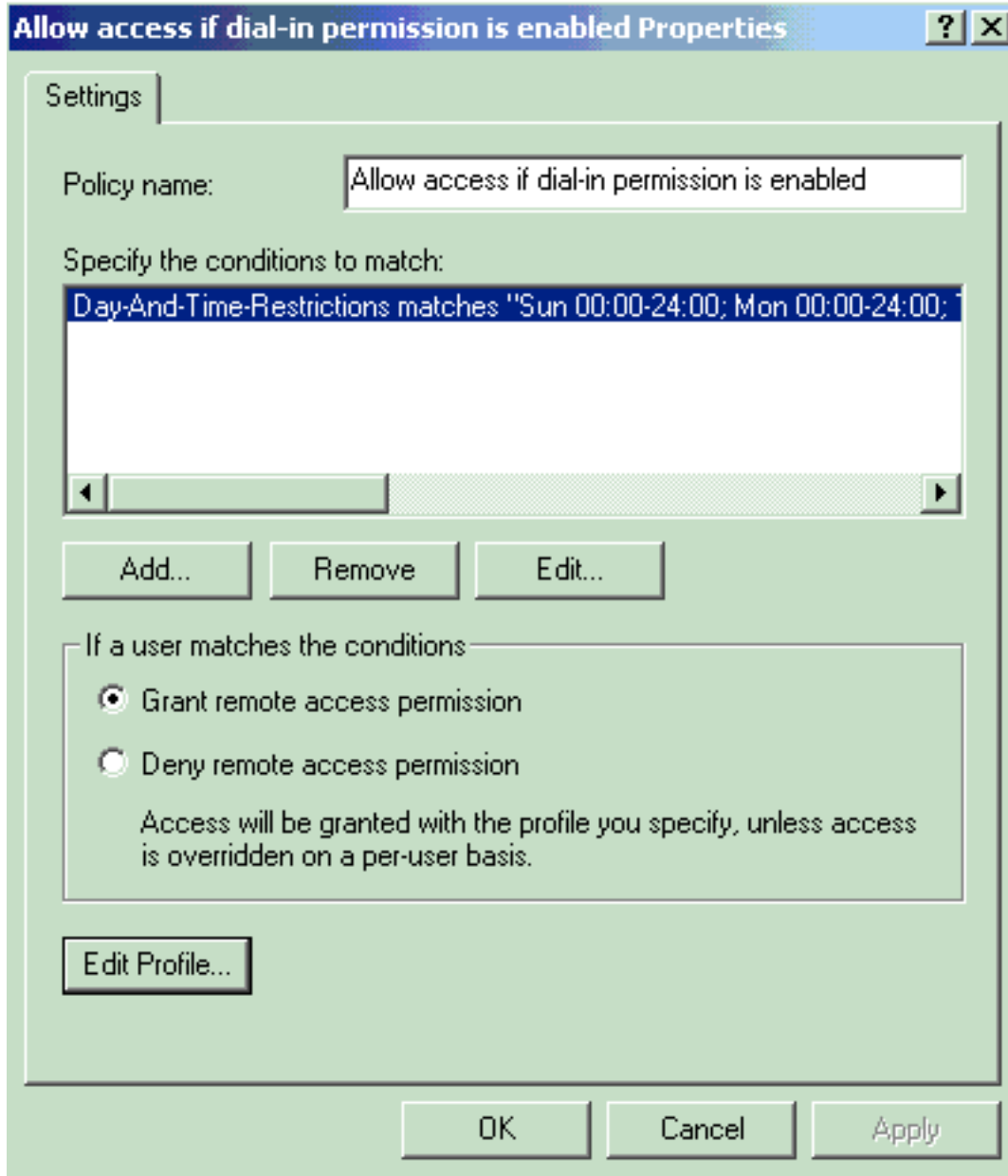
إذا لم يكن خادم (IAS) RADIUS مثبتا بالفعل، فعليك تنفيذ هذه الخطوات للتثبيت. إذا كان خادم RADIUS مثبتا لديك بالفعل، فتابع إلى [خطوات التكوين](#).

1. أدخل القرص المضغوط ل Windows Server وابدأ برنامج الإعداد.
2. انقر على تثبيت مكونات الوظيفة الإضافية، ثم انقر على إضافة/إزالة مكونات Windows.
3. في المكونات، انقر فوق خدمات الشبكة (ولكن لا تحدد أو تمسح خانة الاختيار)، ثم انقر فوق التفاصيل.
4. تحقق من خدمة مصادقة الإنترنت وانقر فوق موافق.
5. انقر فوق Next (التالي).

تكوين خادم Microsoft Windows 2000 باستخدام IAS

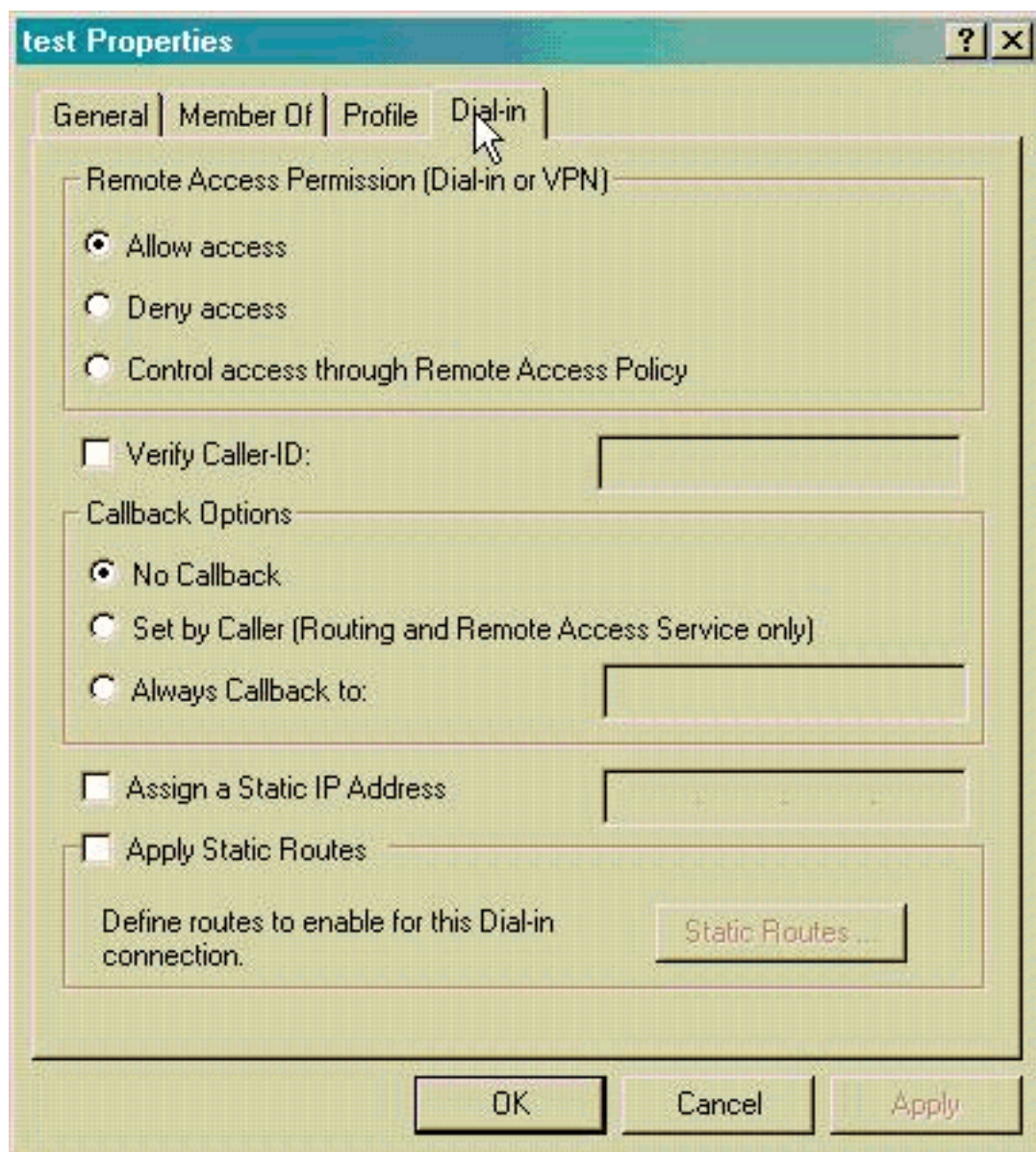
أكمل هذه الخطوات لتكوين خادم (IAS) RADIUS وبدء الخدمة من أجل جعلها متوفرة لمصادقة المستخدمين على مركز VPN.

1. اختر ابدأ < برامج < أدوات إدارية < خدمة مصادقة الإنترنت.
2. انقر بزر الماوس الأيمن فوق خدمة مصادقة الإنترنت، وانقر فوق خصائص من القائمة الفرعية التي تظهر.
3. انتقل إلى علامة التبويب RADIUS لفحص إعدادات المنافذ. إذا اختلفت منافذ مصادقة RADIUS ومنافذ بروتوكول مخطط بيانات المستخدم لمحاسبة (RADIUS (UDP عن القيم الافتراضية المقدمة (1812 و 1645 للمصادقة، 1813 و 1646 للمحاسبة) في المصادقة والمحاسبة، فاكتب إعدادات المنفذ. طقطقت ok عندما أنت إنتهيت. ملاحظة: لا تغير المنافذ الافتراضية. أفضل المنافذ باستخدام الفواصل لاستخدام إعدادات منافذ متعددة لطلبات المصادقة أو المحاسبة.
4. انقر بزر الماوس الأيمن فوق العملاء واختر عميل جديد لإضافة مركز الشبكة الخاصة الظاهرية (VPN) كعميل مصادقة والتحويل والمحاسبة (AAA) إلى خادم (IAS) RADIUS. ملاحظة: إذا تم تكوين التكرار بين مركزي VPN 3000 من Cisco، فيجب أيضا إضافة مركز Cisco VPN 3000 الاحتياطي إلى خادم RADIUS كعميل RADIUS.
5. أدخل اسما مألوف وحدد على هيئة Protocol Radius.
6. قم بتعريف مركز VPN باستخدام عنوان IP أو اسم DNS على الإطار التالي.
7. اختر Cisco من شريط تمرير العميل-المورد.
8. أدخل سر مشترك. ملاحظة: يجب أن تتذكر السر الدقيق الذي تستخدمه. أنت تحتاج هذا معلومة in order to شكلت ال VPN مركز.
9. انقر فوق إنهاء.
10. انقر نقرا مزدوجا فوق نهج الوصول عن بعد وانقر نقرا مزدوجا فوق النهج الذي يظهر في الجانب الأيمن من الإطار. ملاحظة: بعد تثبيت IAS، يجب أن يكون نهج الوصول عن بعد موجودا بالفعل. في Windows 2000، يتم منح التحويل استنادا إلى خصائص الطلب الهاتفي لحساب المستخدم ونهج الوصول عن بعد. سياسات الوصول عن بعد هي مجموعة من الشروط وإعدادات الاتصال التي تمنح مسؤولي الشبكة المزيد من المرونة في التصريح بمحاولات الاتصال. تستخدم كل من خدمة التوجيه والوصول عن بعد في Windows 2000 و IAS Windows 2000 نهج الوصول عن بعد لتحديد ما إذا كان سيتم قبول محاولات الاتصال أو رفضها. في كلتا الحالتين، يتم تخزين سياسات الوصول عن بعد محليا. ارجع إلى وثائق Windows 2000 IAS للحصول على مزيد من المعلومات حول كيفية معالجة محاولات



الاتصال.

11. أختار منح إذن الوصول عن بعد وانقر فوق تحرير ملف التعريف لتكوين خصائص الطلب الهاتفية.
12. حدد البروتوكول المطلوب لإستخدامه للمصادقة في علامة تبويب المصادقة. تحقق من Microsoft Encrypted Authentication الإصدار 2 وقم بإلغاء تحديد جميع بروتوكولات المصادقة الأخرى. ملاحظة: يجب أن تتطابق الإعدادات الموجودة في ملف تعريف الطلب الهاتفية هذا مع الإعدادات الموجودة في تكوين مركز VPN 3000 وعميل الطلب الهاتفية. في هذا المثال، يتم استخدام مصادقة MS-CHAPv2 دون تشفير PPTP.
13. في علامة تبويب التشفير، تحقق من عدم التشفير فقط.
14. انقر على موافق لإغلاق ملف تعريف الطلب الهاتفية، ثم انقر على موافق لإغلاق نافذة نهج الوصول عن بعد.
15. انقر بزر الماوس الأيمن فوق خدمة مصادقة الإنترنت وانقر فوق بدء الخدمة في شجرة وحدة التحكم. ملاحظة: يمكنك أيضا استخدام هذه الوظيفة لإيقاف الخدمة.
16. أكمل هذه الخطوات لتعديل المستخدمين للسماح بالاتصال. أختار وحدة التحكم < إضافة/إزالة الأداة الإضافية. انقر فوق إضافة واختر الأداة الإضافية للمستخدمين المحليين والمجموعات المحلية. انقر فوق إضافة (Add). تأكد من تحديد الكمبيوتر المحلي قطعة إنجاز و ok.
17. قم بتوسيع المستخدم المحلي والمجموعات المحلية وانقر فوق مجلد المستخدمين في الجزء الأيسر. في الجزء الأيمن، انقر نقرا مزدوجا على المستخدم (مستخدم شبكة VPN) الذي تريد السماح بالوصول إليه.
18. انتقل إلى علامة التبويب "الطلب الهاتفية" واختر السماح بالوصول بموجب إذن الوصول عن بعد (الطلب الهاتفية).



أو (VPN).
 19. طقطقة يطبق ok in order to أتمت الإجراء. يمكنك إغلاق نافذة "إدارة وحدة التحكم" وحفظ جلسة العمل، إذا كان ذلك مطلوباً. يمكن للمستخدمين الذين قمت بتعديلهم الآن الوصول إلى مركز الشبكة الخاصة الظاهرية (VPN) باستخدام عميل الشبكة الخاصة الظاهرية (VPN). تذكر أن خادم IAS يقوم بمصادقة معلومات المستخدم فقط. لا يزال مركز الشبكة الخاصة الظاهرية (VPN) يقوم بمصادقة المجموعة.

[تكوين خادم Microsoft Windows 2003 باستخدام IAS](#)

أكمل هذه الخطوات لتكوين خادم Microsoft Windows 2003 باستخدام IAS.

ملاحظة: تفترض هذه الخطوات أن IAS مثبت بالفعل على الجهاز المحلي. وإذا لم تكن هناك مساحة، فقم بإضافة هذا من خلال لوحة التحكم < إضافة/إزالة البرامج.

1. اختر أدوات إدارية < خدمة مصادقة الإنترنت وانقر بزر الماوس الأيمن على عميل RADIUS لإضافة عميل RADIUS جديد. بعد كتابة معلومات العميل، انقر فوق موافق.
2. أدخل اسماً مألوفاً.
3. قم بتعريف مركز VPN باستخدام عنوان IP أو اسم DNS على الإطار التالي.
4. اختر Cisco من شريط تمرير العميل-المورد.
5. أدخل سر مشترك. **ملاحظة:** يجب أن تذكر السر الدقيق الذي تستخدمه. أنت تحتاج هذا معلومة in order to شكلت ال VPN مركز.
6. طقطقة ok أن يستكمل.

7. انتقل إلى نهج الوصول عن بعد، وانقر بزر الماوس الأيمن فوق الاتصالات بخوادم الوصول الأخرى، واختر الخصائص.

8. أختَر منح إذن الوصول عن بعد وانقر فوق تحرير ملف التعريف لتكوين خصائص الطلب الهاتفية.

9. حدد البروتوكول المطلوب إستخدامه للمصادقة في علامة تبويب المصادقة. تحقق من Microsoft Encrypted

Authentication الإصدار 2 وقم بإلغاء تحديد جميع بروتوكولات المصادقة الأخرى. ملاحظة: يجب أن تتطابق

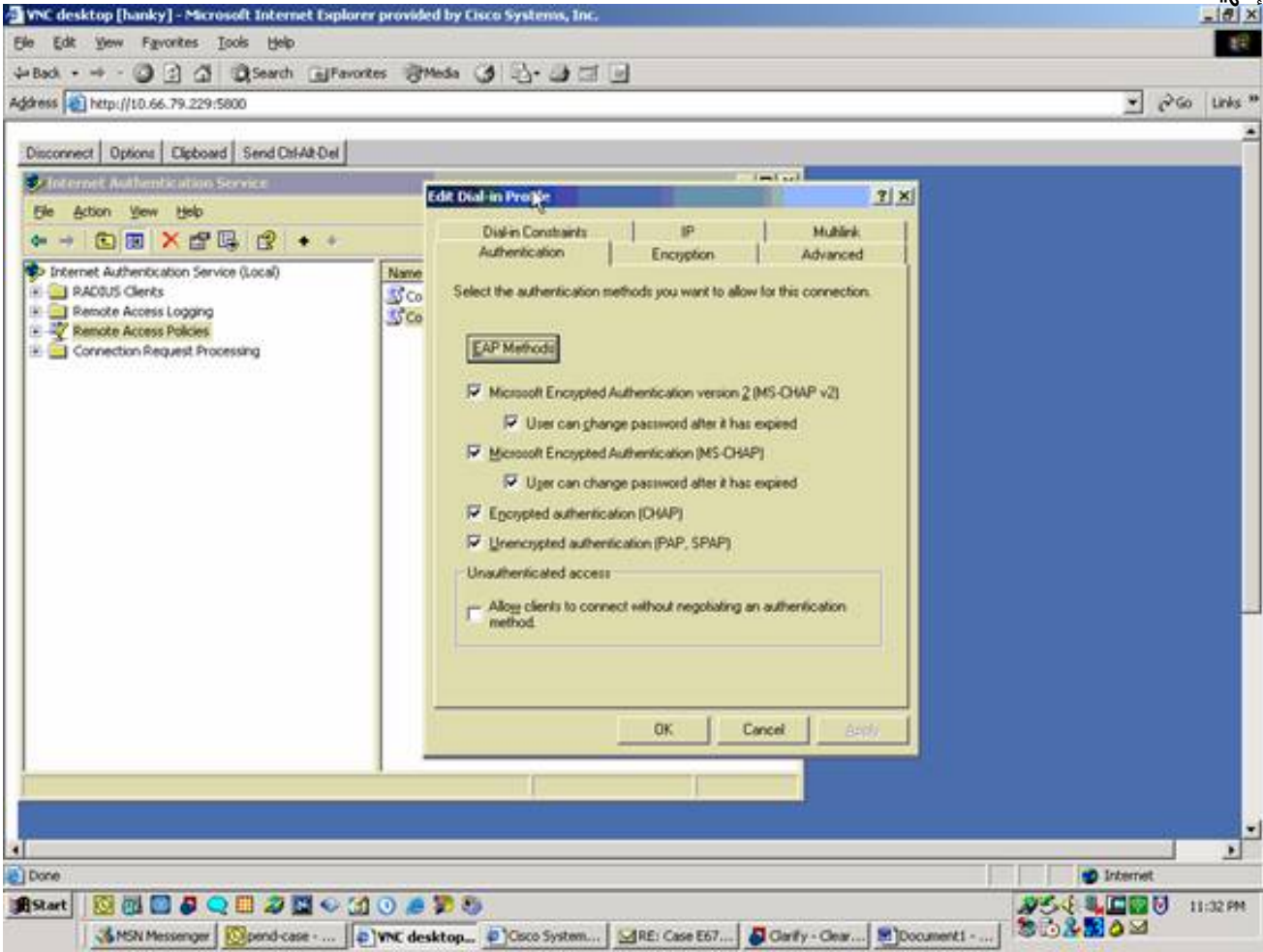
الإعدادات الموجودة في ملف تعريف الطلب الهاتفية هذا مع الإعدادات الموجودة في تكوين مركز VPN 3000

وعميل الطلب الهاتفية. في هذا المثال، يتم إستخدام مصادقة MS-CHAPv2 دون تشفير PPTP.

10. في علامة تبويب التشفير، تحقق من عدم التشفير فقط.

11. طقطقت ok عندما أنت

إنتهيت.



12. انقر بزر الماوس الأيمن فوق خدمة مصادقة الإنترنت وانقر فوق بدء الخدمة في شجرة وحدة التحكم. ملاحظة: يمكنك أيضا إستخدام هذه الوظيفة لإيقاف الخدمة.

13. أختَر أدوات إدارية < إدارة الكمبيوتر > أدوات النظام < المستخدمون المحليون والمجموعات المحلية، وانقر بزر

الماوس الأيمن فوق المستخدمين واختر المستخدمين الجدد لإضافة مستخدم إلى حساب الكمبيوتر المحلي.

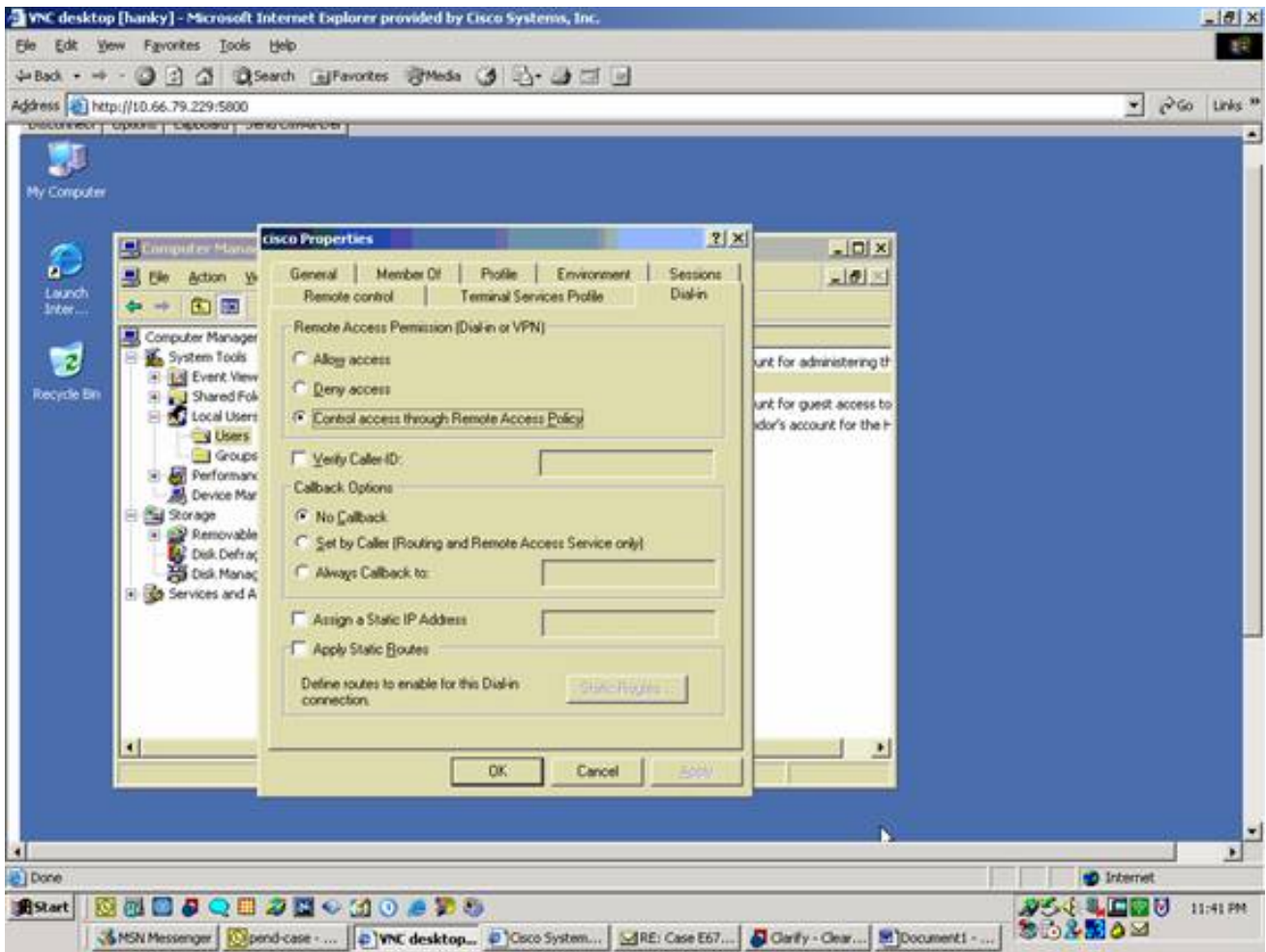
14. أضفت مستعمل مع cisco كلمة "vpnpassword" وفحصت هذا توصيف معلومة. على علامة التبويب "عام"،

تأكد من تحديد خيار كلمة المرور التي لا تنتهي صلاحيتها أبدا بدلا من الخيار الخاص ب المستخدم الذي يجب

عليه تغيير كلمة المرور. في علامة التبويب "الطلب الهاتفية"، أختَر الخيار ل السماح بالوصول (أو أترك الإعداد

الافتراضي ل Control Access من خلال نهج الوصول عن بعد). طقطقت ok عندما أنت

إنتهيت.



تكوين مركز Cisco VPN 3000 لمصادقة RADIUS


أتمت هذا steps in order to شكلت ال VPN 3000 مركز ل RADIUS صحة هوية.

1. قم بالاتصال بمركز الشبكة الخاصة الظاهرية (VPN) باستخدام مستعرض الويب الخاص بك، واختر التكوين < النظام < الخوادم < المصادقة من قائمة الإطارات اليسرى.

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

You should have a properly configured RADIUS, NT Domain, SDI or Kerberos/Active Directory 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
— Empty —	Add 
	Modify
	Delete
	Move Up
	Move Down
	Test

2. قطعة يضيف ويشكل هذا عملية إعداد. نوع الخادم = RADIUS خادم المصادقة = عنوان IP أو اسم المضيف
 خادم (RADIUS (IAS منفذ الخادم = 0 (default=1645=0) سر الخادم = نفسه الموجود في الخطوة 8 في
 القسم الموجود على [تكوين خادم RADIUS](#)

[RADIUS](#)

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. If you are using RADIUS authentication or do not require an additional authorization check, do not configure an authorization server.
Authentication Server	<input type="text" value="msradius.company.com"/>	Enter IP address or hostname.
Used For	<input type="text" value="User Authentication"/>	Select the operation(s) for which this RADIUS server will be used.
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"/>		

3. انقر فوق إضافة لإضافة التغييرات إلى التكوين الجاري تشغيله.

4. انقر فوق إضافة، واختر الخادم الداخلي لنوع الخادم، وانقر فوق تطبيق. تحتاج إلى هذا لاحقاً لتكوين مجموعة IPsec (تحتاج فقط إلى نوع الخادم = خادم داخلي).

Configure and add a user authentication server.

Server Type Selecting *Internal Server* will let you add users to the internal user database.

5. قم بتكوين مركز VPN لمستخدمي PPTP أو لمستخدمي عميل PPTP. VPN. تمت هذا steps in order to شكلت لمستخدمي PPTP. اختر تكوين < إدارة المستخدم > مجموعة أساسية، وانقر فوق علامة التبويب PPTP/L2TP. اختر MSCHAPv2 وألغى تحديد بروتوكولات المصادقة الأخرى في قسم بروتوكولات مصادقة PPTP.

PPTP/L2TP Parameters

Attribute	Value	Description
Use Client Address	<input type="checkbox"/>	Check to accept and use an IP address received from the client.
PPTP Authentication Protocols	<input type="checkbox"/> PAP <input type="checkbox"/> CHAP <input type="checkbox"/> MSCHAPv1 <input checked="" type="checkbox"/> MSCHAPv2 <input type="checkbox"/> EAP Proxy	Check the authentication protocols allowed. Refer to the online help for authentication protocol dependencies. Unchecking all options means that no authentication is required.
PPTP Encryption	<input type="checkbox"/> Required <input type="checkbox"/> Require Stateless <input checked="" type="checkbox"/> 40-bit <input checked="" type="checkbox"/> 128-bit	Select the allowed encryption methods for PPTP connections for this group.
PPTP Compression	<input type="checkbox"/>	Check to enable MPCC compression for PPTP connections for this group.
L2TP Authentication Protocols	<input type="checkbox"/> PAP <input checked="" type="checkbox"/> CHAP <input checked="" type="checkbox"/> MSCHAPv1 <input type="checkbox"/> MSCHAPv2 <input type="checkbox"/> EAP Proxy	Check the authentication protocols allowed. Refer to the online help for authentication protocol dependencies. Unchecking all options means that no authentication is required.
L2TP Encryption	<input type="checkbox"/> Required <input type="checkbox"/> Require Stateless <input checked="" type="checkbox"/> 40-bit <input checked="" type="checkbox"/> 128-bit	Select the allowed encryption methods for L2TP connections for this group.
L2TP Compression	<input type="checkbox"/>	Check to enable MPCC compression for L2TP connections for this group.

انقر فوق تطبيق في أسفل الصفحة لإضافة التغييرات إلى التكوين الجاري تشغيله. والآن عندما يتصل مستخدمو PPTP، تتم مصادقتهم بواسطة خادم (IAS) RADIUS. عميل شبكة VPN. تمت هذا steps in order to شكلت ل VPN زبون مستخدم. اخترت تشكيل < مستعمل إدارة > مجموعة وطققة يضيف in order to أضفت مجموعة جديد.

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, select a group and click the appropriate button.

Actions	Current Groups	Modify
<input type="button" value="Add Group"/> <input type="button" value="Modify Group"/> <input type="button" value="Delete Group"/>	<div style="border: 1px solid gray; padding: 5px;"> — Empty — </div>	<input type="button" value="Authentication Servers"/> <input type="button" value="Authorization Servers"/> <input type="button" value="Accounting Servers"/> <input type="button" value="Address Pools"/> <input type="button" value="Client Update"/> <input type="button" value="Bandwidth Assignment"/> <input type="button" value="WebVPN Servers and URLs"/> <input type="button" value="WebVPN Port Forwarding"/>

اكتب اسم مجموعة (على سبيل المثال، IPsecUsers) وكلمة مرور.

This section lets you add a group. 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 Parameters		
Attribute	Value	Description
Group Name	<input type="text" value="IPSecUsers"/>	Enter a unique name for the group.
Password	<input type="password" value="••••••••"/>	Enter the password for the group.
Verify	<input type="password" value="••••••••"/>	Verify the group's password.
Type	<input type="text" value="Internal"/>	<i>External groups</i> are configured on an external authentication server (e.g. RADIUS). <i>Internal groups</i> are configured on the VPN 3000 Concentrator's Internal Database.
<input type="button" value="Add"/> <input type="button" value="Cancel"/>		

يتم استخدام كلمة المرور هذه كمفتاح مشترك مسبقا لمفاوضات النفق. انتقل إلى علامة التبويب IPsec واضبط المصادقة على RADIUS.

Configuration Administration Monitoring		
		below as needed.
Remote Access Parameters		
Group Lock	<input type="checkbox"/>	<input checked="" type="checkbox"/> Lock users into this group.
Authentication	RADIUS	<input type="checkbox"/> Select the authentication method for members of this group. This parameter does not apply to Individual User Authentication .
Authorization Type	None	<input checked="" type="checkbox"/> If members of this group need authorization in addition to authentication, select an authorization method. If you configure this field, you must also configure an Authorization Server.
Authorization Required	<input type="checkbox"/>	<input checked="" type="checkbox"/> Check to require successful authorization.
DN Field	CN otherwise OU	<input checked="" type="checkbox"/> For certificate-based users, select the subject Distinguished Name (DN) field that is used as the username. This field is used for user Authorization.
IPComp	None	<input checked="" type="checkbox"/> Select the method of IP Compression 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.
		Permit or deny VPN Clients according to

وهذا يسمح بمصادقة عملاء IPsec عبر خادم مصادقة RADIUS. انقر فوق إضافة في أسفل الصفحة لإضافة التغييرات إلى التكوين الجاري تشغيله. الآن عند اتصال عملاء IPsec بالمجموعة التي قمت بتكوينها واستخدامها، تم مصادقتهم بواسطة خادم RADIUS.

[التحقق من الصحة](#)

لا يوجد حالياً إجراء للتحقق من صحة هذا التكوين.

[استكشاف الأخطاء وإصلاحها](#)

[فشل مصادقة WebVPN](#)

توفر هذه الأقسام معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

- **المشكلة:** لا يمكن لمستخدمي WebVPN المصادقة مقابل خادم RADIUS ولكن يمكن مصادقتهم بنجاح مع قاعدة البيانات المحلية الخاصة بموجه VPN. يتلقون أخطاء مثل "فشل تسجيل الدخول" وهذه



الرسالة. السبب: تحدث هذه الأنواع من المشاكل عادة عند استخدام أي قاعدة بيانات أخرى غير قاعدة البيانات الداخلية ل مركز التركيز. يؤثر مستخدمو

WebVPN على المجموعة الأساسية عند توصيلهم أولاً بالمكثف ويجب عليهم استخدام طريقة المصادقة الافتراضية. غالباً ما يتم ضبط هذه الطريقة على قاعدة البيانات الداخلية لـ Concentrator ولا تكون نصف قطر مكون أو خادم آخر. الحل: عندما يقوم مستخدم WebVPN بالمصادقة، يتحقق المكثف من قائمة الخوادم المحددة في التكوين < النظام < الخوادم > المصادقة ويستخدم الخادم الأعلى. تأكد من نقل الخادم الذي تريد من مستخدم WebVPN المصادقة عليه إلى أعلى هذه القائمة. على سبيل المثال، إذا كان يجب أن يكون RADIUS طريقة مصادقة، فأنت بحاجة لنقل خادم RADIUS إلى أعلى القائمة لدفع المصادقة إليه. ملاحظة: لا يعني مجرد أن مستخدم شبكة WebVPN قاموا في البداية بضرب المجموعة الأساسية أنهم محصورون في المجموعة الأساسية. يمكن تكوين مجموعات WebVPN إضافية على مركز التركيز، ويمكن تخصيص المستخدمين لهم بواسطة خادم RADIUS مع تعداد السمة 25 مع `OU=groupName`. راجع [قفل المستخدمين في مجموعة مركز VPN 3000 باستخدام خادم RADIUS](#) للحصول على شرح أكثر تفصيلاً.

فشل مصادقة المستخدم مقابل Active Directory

في خادم Active Directory، من علامة التبويب "حساب" الخاصة بخصائص المستخدم الذي تعرض للفشل، يمكنك مشاهدة خانة الاختيار هذه:

[X] لا تتطلب مصادقة مسبقة

إذا تم إلغاء تحديد خانة الاختيار هذه، فتتحقق منها، وحاول المصادقة مرة أخرى مع هذا المستخدم.

معلومات ذات صلة

- [مركزات Cisco VPN 3000 Series](#)
- [أجهزة Cisco VPN 3002 العملية](#)
- [مفاوضة IPsec/بروتوكولات IKE](#)
- [صفحة دعم RADIUS \(خدمة مصادقة طلب اتصال المستخدم البعيد\)](#)
- [خدمة مصادقة طلب اتصال المستخدم البعيد \(RADIUS\)](#)
- [الدعم التقني والمستندات - Cisco Systems](#)

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة مادختساب دن تسمل اذة Cisco تمةرت
ملاعلاء انء مء مء نء مء دختسمل معد و تمة مء دقتل ةر شبل او
امك ةق قء نوك ت نل ةللأل ةمچرت لصف أن ةظحال مء ءء. ةصاأل مء تءل ب
Cisco ةلخت. فرتمة مچرت مء مء قء ةل ةل ةفارتحال ةمچرتل عم لالحل وه
ىل إأمءءاد ءوچرلاب ةصوء و تامةرتل هذه ةقء نء اهءل وئس م Cisco
Systems (رفوتم طبارل) ةلصلأل ةزىلچن إل دن تسمل