

Konfigurieren des Cisco VPN 300 Concentrator mit Microsoft RADIUS

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konventionen](#)

[Installieren und Konfigurieren des RADIUS-Servers unter Windows 2000 und Windows 2003](#)

[Installation des RADIUS-Servers](#)

[Konfigurieren des Microsoft Windows 2000-Servers mit IAS](#)

[Konfigurieren des Microsoft Windows 2003-Servers mit IAS](#)

[Konfigurieren des Cisco VPN 3000 Concentrator für die RADIUS-Authentifizierung](#)

[Überprüfen](#)

[Fehlerbehebung](#)

[WebVPN-Authentifizierung schlägt fehl](#)

[Die Benutzerauthentifizierung schlägt mit dem Active Directory fehl](#)

[Zugehörige Informationen](#)

Einführung

Microsoft Internet Authentication Server (IAS) und Microsoft Commercial Internet System (MCIS 2.0) sind derzeit verfügbar. Der Microsoft RADIUS-Server ist benutzerfreundlich, da er das Active Directory auf dem primären Domänen-Controller für seine Benutzerdatenbank verwendet. Sie müssen keine separate Datenbank mehr verwalten. Darüber hinaus unterstützt es die 40-Bit- und 128-Bit-Verschlüsselung für PPTP-VPN-Verbindungen (Point-to-Point Tunneling Protocol). Weitere Informationen finden Sie in der [Microsoft Checkliste: Konfiguration der IAS für die Dokumentation für Einwahl- und VPN-Zugriff](#) .

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den [Cisco Technical Tips Conventions](#) (Technische Tipps zu Konventionen von Cisco).

Installieren und Konfigurieren des RADIUS-Servers unter Windows 2000 und Windows 2003

Installation des RADIUS-Servers

Wenn der RADIUS-Server (IAS) nicht bereits installiert ist, führen Sie die folgenden Schritte aus, um die Installation durchzuführen. Wenn Sie den RADIUS-Server bereits installiert haben, fahren Sie mit den [Konfigurationsschritten fort](#).

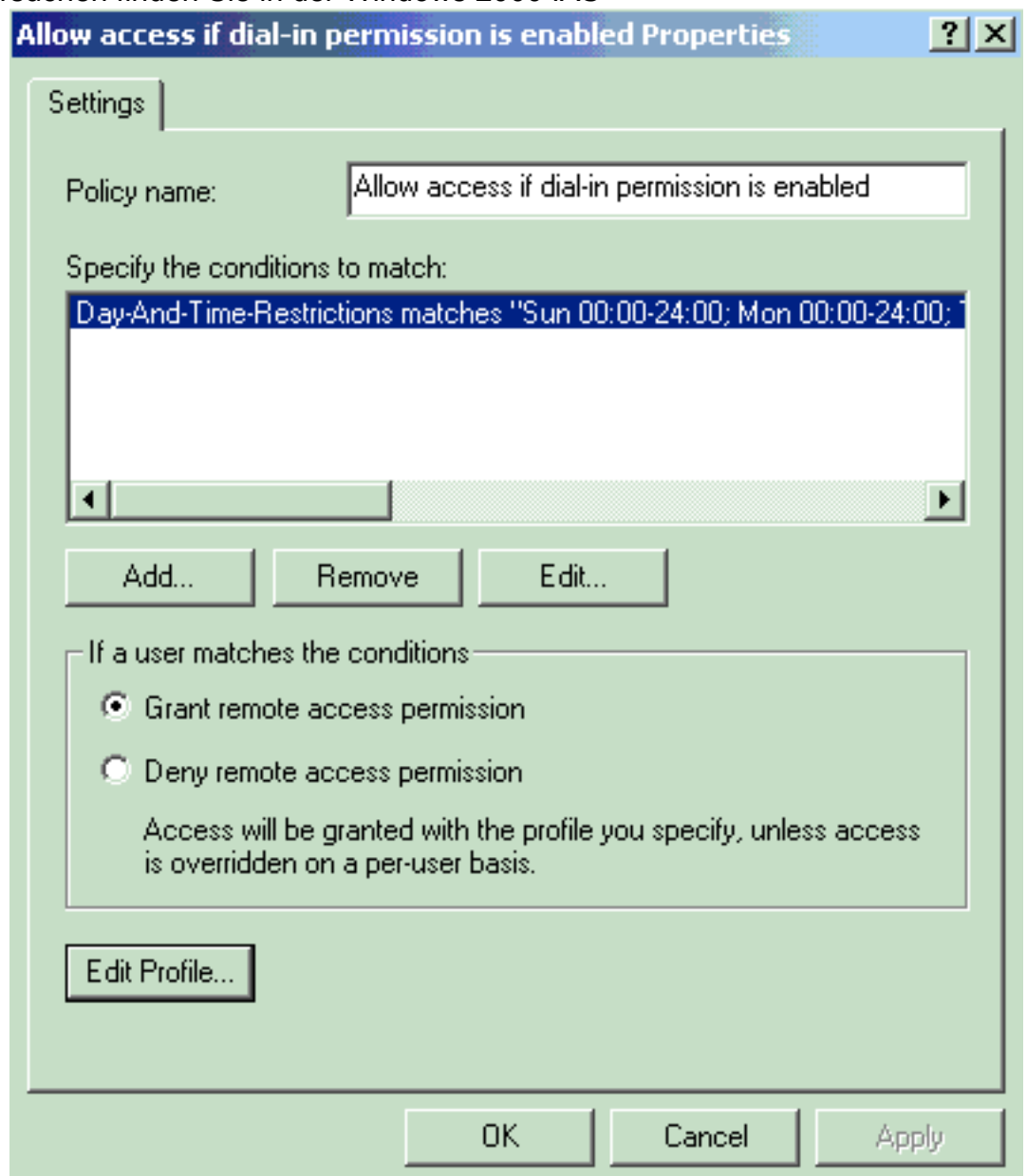
1. Legen Sie die Windows Server-CD ein, und starten Sie das Setup-Programm.
2. Klicken Sie auf **Add-On-Komponenten installieren** und dann auf **Windows-Komponenten hinzufügen/entfernen**.
3. Klicken Sie unter Komponenten auf **Netzwerkdienste** (aktivieren oder deaktivieren Sie jedoch nicht das Kontrollkästchen), und klicken Sie dann auf **Details**.
4. Aktivieren Sie **Internet Authentication Service** und klicken Sie auf **OK**.
5. Klicken Sie auf **Weiter**.

Konfigurieren des Microsoft Windows 2000-Servers mit IAS

Führen Sie diese Schritte aus, um den RADIUS-Server (IAS) zu konfigurieren und den Dienst zu starten, um ihn für die Authentifizierung von Benutzern im VPN-Konzentrator verfügbar zu machen.

1. Wählen Sie **Start > Programme > Verwaltung > Internetauthentifizierungsdienst** aus.
2. Klicken Sie mit der rechten Maustaste auf den **Internetauthentifizierungsdienst**, und klicken Sie im angezeigten Untermenü auf **Eigenschaften**.
3. Wechseln Sie zur Registerkarte RADIUS, um die Einstellungen für Ports zu überprüfen. Wenn sich die Ports für die RADIUS-Authentifizierung und die RADIUS Accounting User Datagram Protocol (UDP)-Accounting-Ports von den Standardwerten (1812 und 1645 für die Authentifizierung, 1813 und 1646 für die Accounting) in Authentication and Accounting unterscheiden, geben Sie Ihre Porteeinstellungen ein. Klicken Sie abschließend auf **OK**. **Hinweis:** Ändern Sie die Standardports nicht. Trennen Sie die Ports, indem Sie Kommas verwenden, um mehrere Porteeinstellungen für Authentifizierungs- oder Accounting-Anforderungen zu verwenden.
4. Klicken Sie mit der rechten Maustaste auf **Clients**, und wählen Sie **New Client** aus, um den VPN Concentrator als AAA-Client (Authentication, Authorization, Accounting) zum RADIUS-Server (IAS) hinzuzufügen. **Hinweis:** Wenn zwischen zwei Cisco VPN 3000-Concentrators Redundanz konfiguriert wird, muss der Cisco VPN 3000-Backup-Concentrator auch dem RADIUS-Server als RADIUS-Client hinzugefügt werden.
5. Geben Sie einen benutzerfreundlichen Namen ein, und wählen Sie als **Protokoll Radius** aus.
6. Definieren Sie im nächsten Fenster den VPN Concentrator mit einer IP-Adresse oder einem DNS-Namen.

7. Wählen Sie **Cisco** aus der Client-Vendor-Bildlaufleiste aus.
8. Geben Sie einen gemeinsamen geheimen Schlüssel ein.**Hinweis:** Sie müssen sich an das *genaue* Geheimnis erinnern, das Sie verwenden. Sie benötigen diese Informationen, um den VPN-Konzentrator zu konfigurieren.
9. Klicken Sie auf **Fertig stellen**.
10. Doppelklicken Sie auf **Remote Access Policies (Remote-Zugriffsrichtlinien)**, und doppelklicken Sie auf die Richtlinie, die rechts im Fenster angezeigt wird.**Hinweis:** Nachdem Sie IAS installiert haben, sollte bereits eine Richtlinie für den Remote-Zugriff existieren. In Windows 2000 wird die Autorisierung basierend auf den Einwahleigenschaften eines Benutzerkontos und den Richtlinien für den Remotezugriff gewährt. Richtlinien für den Remote-Zugriff sind eine Reihe von Bedingungen und Verbindungseinstellungen, die Netzwerkadministratoren mehr Flexibilität bei der Autorisierung von Verbindungsversuchen bieten. Sowohl der Dienst Windows 2000 Routing und Remote Access als auch der Windows 2000 IAS verwenden Remote-Zugriffsrichtlinien, um zu bestimmen, ob Verbindungsversuche akzeptiert oder abgelehnt werden. In beiden Fällen werden die Remote-Zugriffsrichtlinien lokal gespeichert. Weitere Informationen zur Verarbeitung von Verbindungsversuchen finden Sie in der Windows 2000 IAS-

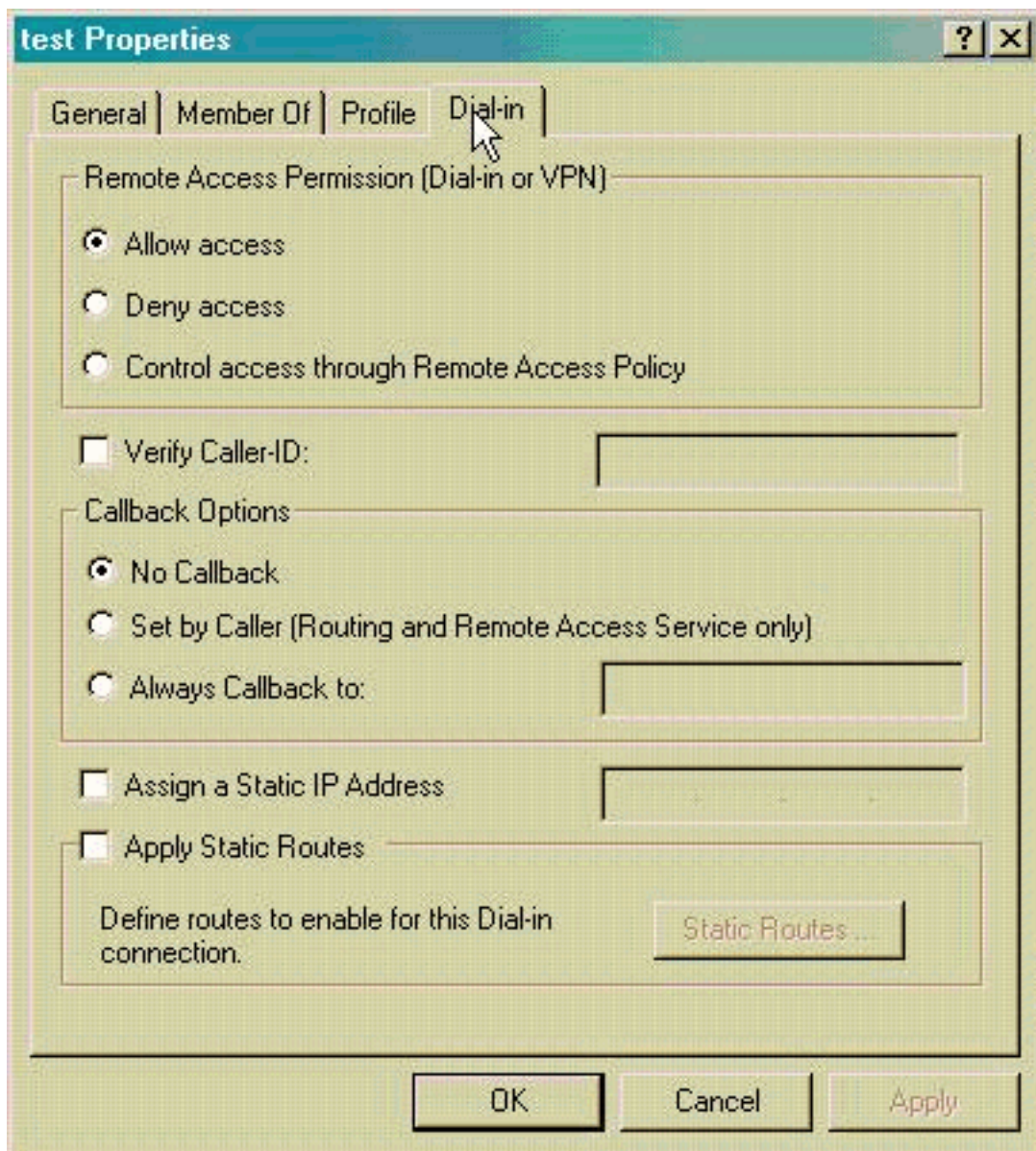


Dokumentation.

11. Wählen Sie **Remotezugriffsberechtigung erteilen aus**, und klicken Sie auf **Profil bearbeiten**,

um die Einwahleigenschaften zu konfigurieren.

12. Wählen Sie auf der Registerkarte Authentifizierung das Protokoll für die Authentifizierung aus. Aktivieren Sie **Microsoft Encrypted Authentication Version 2**, und deaktivieren Sie alle anderen Authentifizierungsprotokolle. **Hinweis:** Die Einstellungen in diesem Einwahlprofil müssen mit den Einstellungen in der Konfiguration des VPN 3000-Concentrators und dem Einwahlclient übereinstimmen. In diesem Beispiel wird die MS-CHAPv2-Authentifizierung ohne PPTP-Verschlüsselung verwendet.
13. Aktivieren Sie auf der Registerkarte Verschlüsselung die Option **Nur Verschlüsselung**.
14. Klicken Sie auf **OK**, um das Einwahlprofil zu schließen, und klicken Sie dann auf **OK**, um das Fenster mit den Richtlinien für den Remote-Zugriff zu schließen.
15. Klicken Sie mit der rechten Maustaste auf den **Internetauthentifizierungsdienst**, und klicken Sie in der Konsolenstruktur auf **Dienst starten**. **Hinweis:** Sie können diese Funktion auch verwenden, um den Dienst zu beenden.
16. Führen Sie diese Schritte aus, um die Benutzer so zu modifizieren, dass sie die Verbindung zulassen. Wählen Sie **Console > Snap-In hinzufügen/entfernen aus**. Klicken Sie auf **Hinzufügen**, und wählen Sie **Snap-In Lokale Benutzer und Gruppen aus**. Klicken Sie auf **Hinzufügen**. Stellen Sie sicher, dass Sie **Lokaler Computer** auswählen. Klicken Sie auf **Fertig stellen** und **OK**.
17. Erweitern Sie **Lokale Benutzer und Gruppen**, und klicken Sie im linken Bereich auf den Ordner **Benutzer**. Doppelklicken Sie im rechten Teilfenster auf den Benutzer (VPN-Benutzer), dem der Zugriff gewährt werden soll.
18. Wechseln Sie zur Registerkarte Dial-in (Einwählen), und wählen Sie **Allow Access** (Zugriff **zulassen** unter Remote-Zugriffsberechtigung (Einwahl oder VPN)



aus.

19. Klicken Sie auf **Übernehmen** und **OK**, um den Vorgang abzuschließen. Sie können das Fenster Konsolenverwaltung schließen und die Sitzung bei Bedarf speichern. Die von Ihnen geänderten Benutzer können nun über den VPN-Client auf den VPN-Concentrator zugreifen. Beachten Sie, dass der IAS-Server nur die Benutzerinformationen authentifiziert. Der VPN Concentrator führt die Gruppenauthentifizierung weiterhin aus.

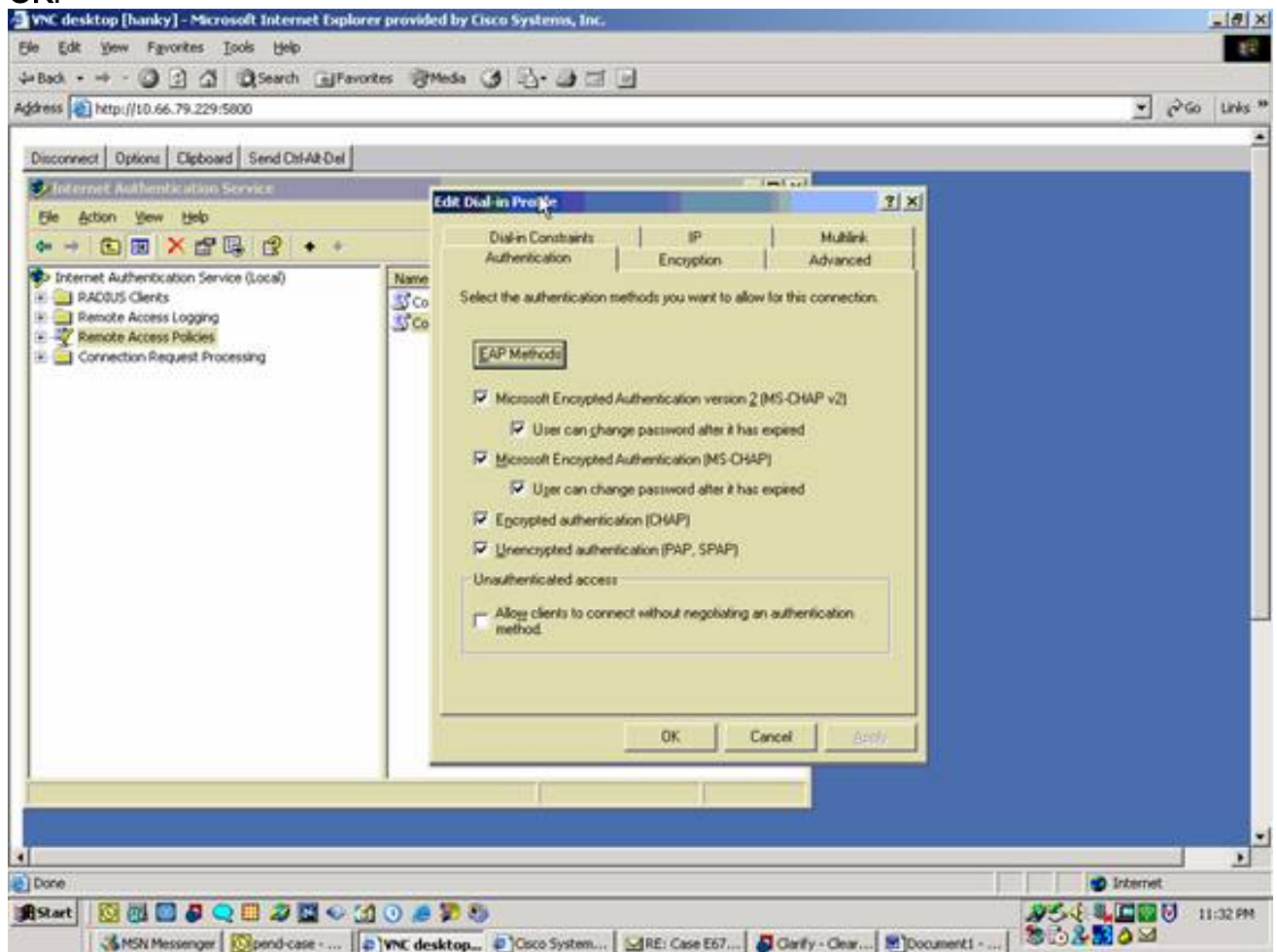
[Konfigurieren des Microsoft Windows 2003-Servers mit IAS](#)

Führen Sie diese Schritte aus, um den Microsoft Windows 2003-Server mit IAS zu konfigurieren.

Hinweis: Bei diesen Schritten wird davon ausgegangen, dass IAS bereits auf dem lokalen Computer installiert ist. Falls nicht, fügen Sie dies über **Systemsteuerung > Software** hinzu.

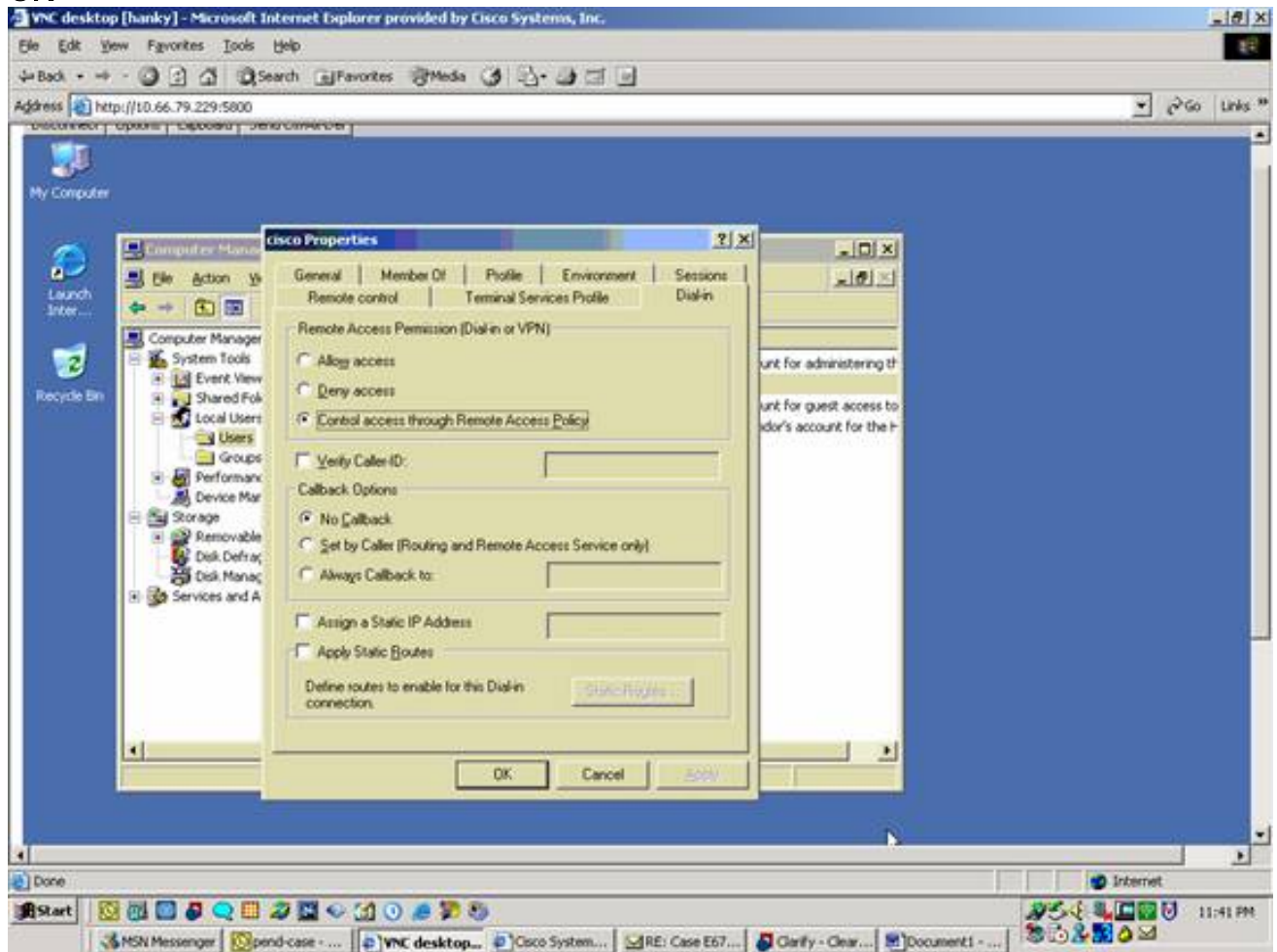
1. Wählen Sie **Verwaltung > Internet Authentication Service** und klicken Sie mit der rechten Maustaste auf **RADIUS Client**, um einen neuen RADIUS-Client hinzuzufügen. Nachdem Sie die Clientinformationen eingegeben haben, klicken Sie auf **OK**.
2. Geben Sie einen benutzerfreundlichen Namen ein.
3. Definieren Sie im nächsten Fenster den VPN Concentrator mit einer IP-Adresse oder einem DNS-Namen.
4. Wählen Sie **Cisco** aus der Client-Vendor-Bildlaufleiste aus.

5. Geben Sie einen gemeinsamen geheimen Schlüssel ein.**Hinweis:** Sie müssen sich an das *genaue* Geheimnis erinnern, das Sie verwenden. Sie benötigen diese Informationen, um den VPN-Konzentrator zu konfigurieren.
6. Klicken Sie zum Abschließen auf **OK**.
7. Gehen Sie zu **Remotezugriffsrichtlinien**, klicken Sie mit der rechten Maustaste auf **Verbindungen zu anderen Zugriffsservern**, und wählen Sie **Eigenschaften** aus.
8. Wählen Sie **Remotezugriffsberechtigung erteilen aus**, und klicken Sie auf **Profil bearbeiten**, um die Einwahleigenschaften zu konfigurieren.
9. Wählen Sie auf der Registerkarte Authentifizierung das Protokoll für die Authentifizierung aus. Aktivieren Sie **Microsoft Encrypted Authentication Version 2**, und deaktivieren Sie alle anderen Authentifizierungsprotokolle.**Hinweis:** Die Einstellungen in diesem Einwahlprofil müssen mit den Einstellungen in der Konfiguration des VPN 3000-Concentrators und dem Einwahlclient übereinstimmen. In diesem Beispiel wird die MS-CHAPv2-Authentifizierung ohne PPTP-Verschlüsselung verwendet.
10. Aktivieren Sie auf der Registerkarte Verschlüsselung die Option **Nur Verschlüsselung**.
11. Klicken Sie abschließend auf **OK**.



12. Klicken Sie mit der rechten Maustaste auf den **Internetauthentifizierungsdienst**, und klicken Sie in der Konsolenstruktur auf **Dienst starten**.**Hinweis:** Sie können diese Funktion auch verwenden, um den Dienst zu beenden.
13. Wählen Sie **Verwaltung > Computerverwaltung > Systemprogramme > Lokale Benutzer und Gruppen**, klicken Sie mit der rechten Maustaste auf **Benutzer** und wählen Sie **Neue Benutzer**, um dem lokalen Computerkonto einen Benutzer hinzuzufügen.
14. Fügen Sie den Benutzer mit dem Cisco Kennwort "vpnpassword" hinzu, und überprüfen Sie diese Profilinformationen. Stellen Sie auf der Registerkarte Allgemein sicher, dass die

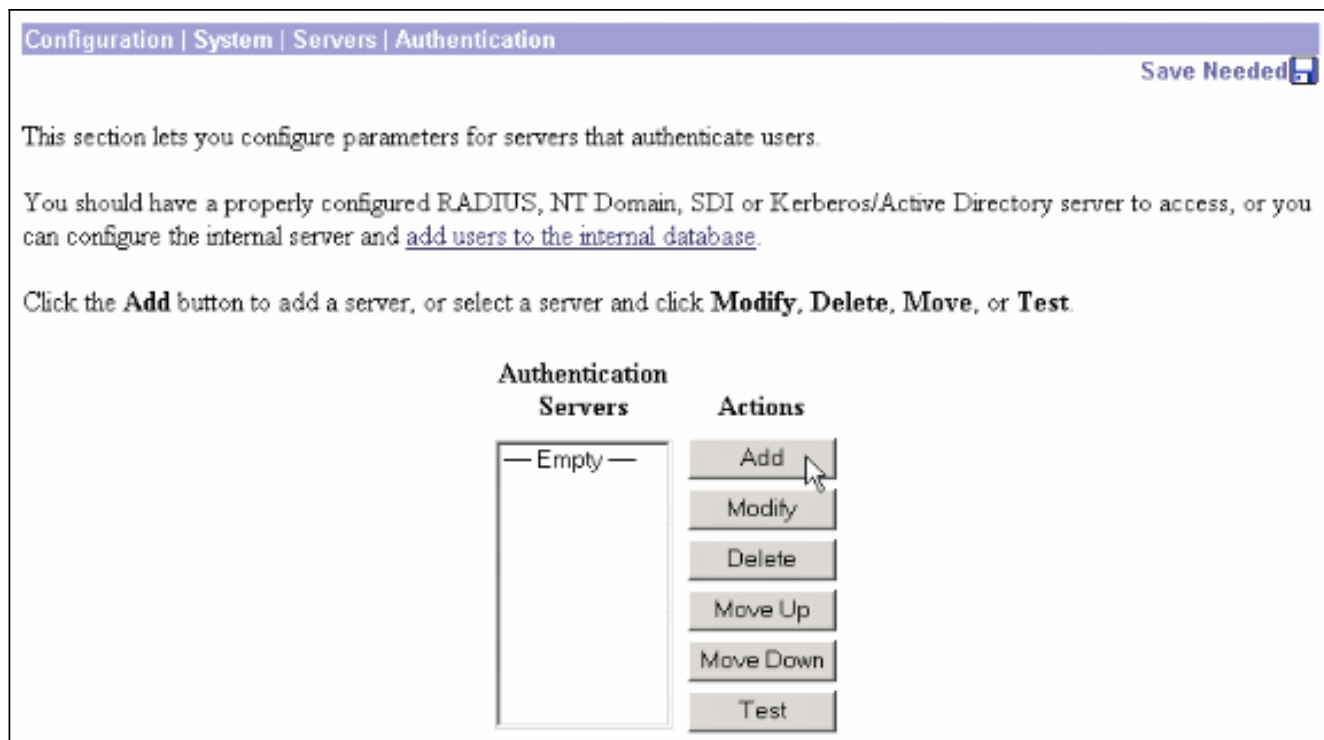
Option **Kennwort nie abgelaufen** anstelle der Option Kennwort ändern muss aktiviert ist. Wählen Sie auf der Registerkarte Dial-in (Einwählen) die Option **Allow access (Zugriff zulassen)** (oder belassen Sie die Standardeinstellung Control Access (Zugriffssteuerung über Remote-Zugriffsrichtlinie). Klicken Sie abschließend auf **OK**.



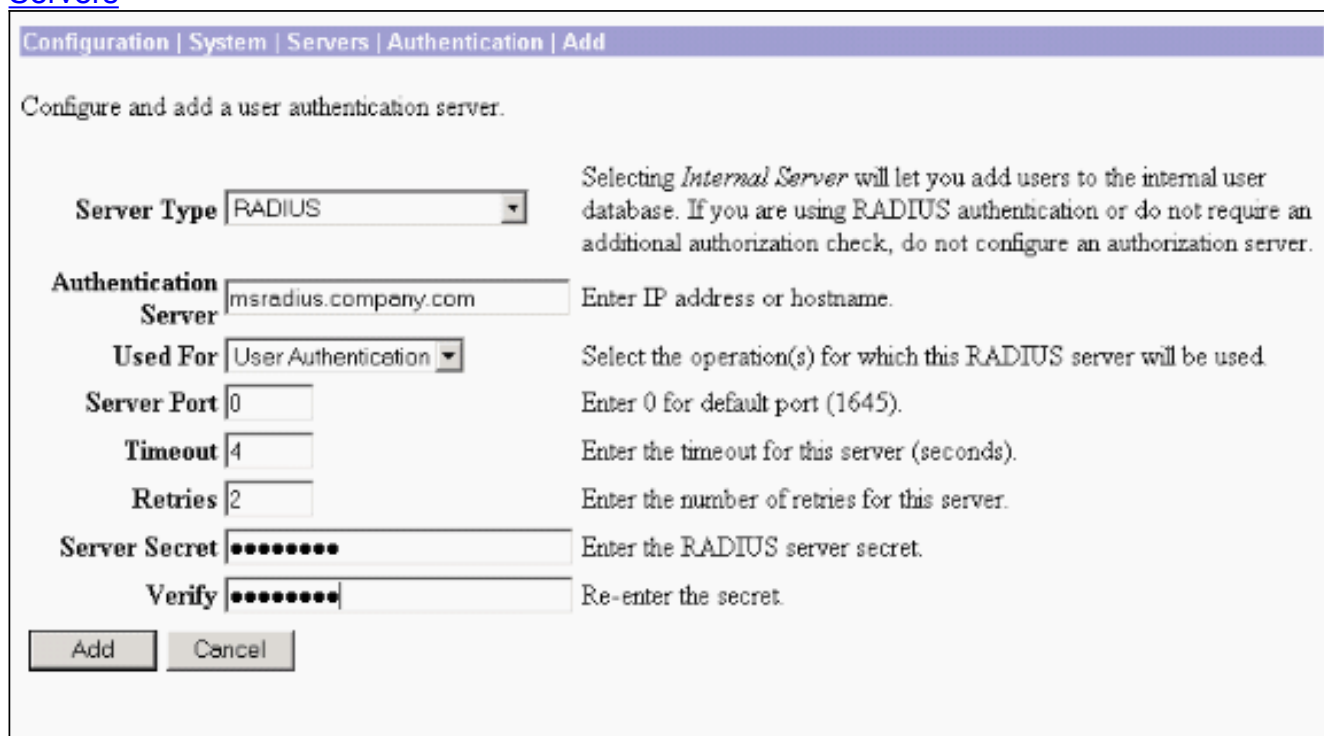
Konfigurieren des Cisco VPN 3000 Concentrator für die RADIUS-Authentifizierung

Führen Sie diese Schritte aus, um den Cisco VPN 3000 Concentrator für die RADIUS-Authentifizierung zu konfigurieren.

1. Stellen Sie über Ihren Webbrowser eine Verbindung zum VPN Concentrator her, und wählen Sie im linken Frame-Menü **Configuration > System > Servers > Authentication** aus.



- Klicken Sie auf **Hinzufügen** und konfigurieren Sie diese Einstellungen. Servertyp = RADIUS
 Authentifizierungsserver = IP-Adresse oder Hostname des RADIUS-Servers (IAS)
 Server-Port = 0 (0=Standard=1645)
 Servergeheimnis = identisch mit Schritt 8 im Abschnitt [Konfigurieren des RADIUS-Servers](#)



- Klicken Sie auf **Hinzufügen**, um die Änderungen zur aktuellen Konfiguration hinzuzufügen.
- Klicken Sie auf **Hinzufügen**, wählen Sie **Interner Server** als Servertyp aus, und klicken Sie auf **Übernehmen**. Sie benötigen dies später, um eine IPsec-Gruppe zu konfigurieren (Sie benötigen nur Servertyp = Interner Server).

Configuration | System | Servers | Authentication | Add

Configure and add a user authentication server.

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

5. Konfigurieren Sie den VPN Concentrator für PPTP-Benutzer oder für VPN-Client-Benutzer. **PPTP**Führen Sie diese Schritte aus, um PPTP-Benutzer zu konfigurieren. Wählen Sie **Konfiguration > Benutzerverwaltung > Basisgruppe**, und klicken Sie auf die Registerkarte **PPTP/L2TP**. Wählen Sie **MSCHAPv2** aus, und deaktivieren Sie andere Authentifizierungsprotokolle im Abschnitt PPTP-Authentifizierungsprotokolle.


Configuration | User Management | Base Group

General | IPsec | Client Config | Client FW | HW Client | **PPTP/L2TP** | WebVPN | NAC

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 MPPC 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 MPPC compression for L2TP connections for this group.

Klicken Sie unten auf der Seite auf **Apply** (Übernehmen), um die Änderungen zur aktuellen Konfiguration hinzuzufügen. Wenn PPTP-Benutzer jetzt eine Verbindung herstellen, werden sie vom RADIUS-Server (IAS) authentifiziert. **VPN-Client**Führen Sie diese Schritte aus, um die Konfiguration für VPN-Client-Benutzer durchzuführen. Wählen Sie **Konfiguration > Benutzerverwaltung > Gruppen** und klicken Sie auf **Hinzufügen**, um eine neue Gruppe hinzuzufügen.

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, select a group and click the appropriate button.

Actions

Add Group

Modify Group

Delete Group

Current Groups

— Empty —

Modify

Authentication Servers

Authorization Servers

Accounting Servers

Address Pools

Client Update

Bandwidth Assignment

WebVPN Servers and URLs

WebVPN Port Forwarding

Geben Sie einen Gruppennamen (z. B. IPsecUsers) und ein Kennwort ein.

Configuration | User Management | Groups | Add

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 | General | IPsec | Client Config | Client FW | HW Client | PPTP/L2TP | WebVPN | NAC

Identity Parameters

Attribute	Value	Description
Group Name	IPSecUsers	Enter a unique name for the group.
Password	••••••••	Enter the password for the group.
Verify	••••••••	Verify the group's password.
Type	Internal	<i>External groups are configured on an external authentication server (e.g. RADIUS). Internal groups are configured on the VPN 3000 Concentrator's Internal Database.</i>

Add Cancel

Dieses Kennwort wird als vorinstallierter Schlüssel für die Tunnelverhandlung verwendet. Wechseln Sie zur Registerkarte IPsec, und legen Sie für die Authentifizierung **RADIUS** fest.

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

Dadurch können IPsec-Clients über den RADIUS-Authentifizierungsserver authentifiziert werden. Klicken Sie unten auf der Seite auf **Hinzufügen**, um die Änderungen zur aktuellen Konfiguration hinzuzufügen. Wenn IPsec-Clients jetzt eine Verbindung herstellen und die von Ihnen konfigurierte Gruppe verwenden, werden sie vom RADIUS-Server authentifiziert.

Überprüfen

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

WebVPN-Authentifizierung schlägt fehl

In diesen Abschnitten finden Sie Informationen zur Fehlerbehebung in Ihrer Konfiguration.

- **Problem:** Die WebVPN-Benutzer können sich nicht über den RADIUS-Server authentifizieren, sondern können sich erfolgreich über die lokale Datenbank des VPN Concentrator authentifizieren. Sie erhalten Fehler wie "Anmeldung fehlgeschlagen" und diese



Meldung.

Ursache: Diese

Probleme treten häufig auf, wenn eine andere Datenbank als die interne Datenbank des Concentrators verwendet wird. WebVPN-Benutzer drücken bei der ersten Verbindung mit dem Concentrator die Basisgruppe und müssen die Standardauthentifizierungsmethode verwenden. Oft ist diese Methode auf die interne Datenbank des Concentrators festgelegt und ist kein konfigurierter RADIUS- oder anderer Server. **Lösung:** Bei der Authentifizierung eines WebVPN-Benutzers überprüft der Concentrator die Liste der unter **Configuration > System > Servers > Authentication** definierten Server und verwendet die höchste Serverliste. Stellen Sie sicher, dass Sie den Server, mit dem Sie WebVPN-Benutzer authentifizieren möchten, an die Spitze dieser Liste verschieben. Wenn beispielsweise RADIUS die Authentifizierungsmethode sein soll, müssen Sie den RADIUS-Server an die Spitze der Liste verschieben, um die Authentifizierung an diesen Server zu übertragen. **Hinweis:** Nur weil WebVPN-Benutzer anfänglich die Basisgruppe treffen, bedeutet dies nicht, dass sie auf die Basisgruppe beschränkt sind. Zusätzliche WebVPN-Gruppen können im Concentrator konfiguriert werden, und Benutzer können ihnen vom RADIUS-Server mit der Auflistung des Attributs 25 mit **OU=gruppenname** zugewiesen werden. Detailliertere Erklärungen erhalten Sie [unter Locken von Benutzern in eine VPN 3000-Concentrator-Gruppe mithilfe eines RADIUS-Servers](#).

[Die Benutzerauthentifizierung schlägt mit dem Active Directory fehl](#)

Im Active Directory-Server auf der Registerkarte "Account" (Konto) der Benutzereigenschaften des ausgefallenen Benutzers wird dieses Kontrollkästchen angezeigt:

Keine Vorauthentifizierung erforderlich

Wenn dieses Kontrollkästchen deaktiviert ist, **aktivieren Sie es**, und versuchen Sie, sich erneut bei diesem Benutzer zu authentifizieren.

[Zugehörige Informationen](#)

- [Cisco VPN Concentrators der Serie 3000](#)
- [Cisco VPN 3002 Hardware-Clients](#)
- [IPsec-Aushandlung/IKE-Protokolle](#)
- [Support-Seite für RADIUS \(Remote Authentication Dial-In User Service\)](#)
- [RADIUS \(Remote Authentication Dial-In User Service\)](#)
- [Technischer Support und Dokumentation - Cisco Systems](#)