

# Verwalten von VPN-Benutzern und Konfigurieren von Quick VPN auf den VPN-Routern RV016, RV042, RV042G und RV082

## Ziel

Ein Virtual Private Network (VPN) ist eine Möglichkeit, Endpunkte in verschiedenen Netzwerken über ein öffentliches Netzwerk wie das Internet miteinander zu verbinden. Eine nützliche Anwendung von VPNs ist, dass ein Remote-Benutzer mit VPN-Client-Software sicher auf Informationen in einem privaten Netzwerk zugreifen kann, solange er Zugriff auf das Internet hat. Die VPN-Router der Serie RV0xx können so konfiguriert werden, dass Benutzer mit QuickVPN einen VPN-Tunnel mit dem Router erstellen können. Cisco QuickVPN ist eine Software, die für den Remote-Zugriff auf ein Virtual Private Network (VPN) entwickelt wurde.

Ein VPN-Zertifikat ist eine Möglichkeit, die Sicherheit im VPN-Tunnel zu erhöhen. Zertifikate werden vom Router generiert und verwendet, um die Sicherheit sowohl des Routers als auch des QuickVPN-Benutzers zu gewährleisten. Vom Router aus können Sie das Zertifikat exportieren, das vom QuickVPN-Client verwendet werden kann.

In diesem Artikel wird erläutert, wie Sie einen VPN-Benutzer konfigurieren und die VPN-Zertifikate auf VPN-Routern der Serie RV0xx verwalten.

**Hinweis:** Sie müssen den VPN-Tunnel konfigurieren, bevor Sie VPN-Benutzer konfigurieren. Weitere Informationen zur Konfiguration von Gateway zu Gateway-VPN finden Sie unter *Konfiguration von Gateway zu Gateway-VPN auf RV016-, RV042-, RV042G- und RV082-VPN-Routern*. Weitere Informationen zum Konfigurieren von Client zu Gateway-VPN finden Sie unter *Richten Sie einen Remote-Zugriffstunnel (Client zu Gateway) für VPN-Clients auf RV016-, RV042-, RV042G- und RV082-VPN-Routern ein*. Nach der Konfiguration der VPN-Benutzer müssen Sie Quick VPN auf dem PC des Benutzers einrichten, um auf den VPN-Tunnel zuzugreifen.

## Unterstützte Geräte

RV016  
RV042  
RV042G  
RV082

## Software-Version

v4.2.2.08 [VPN-Router der RV-Serie]  
1.4.2.1 [Cisco QuickVPN]

## VPN-Benutzer konfigurieren

Schritt 1: Melden Sie sich beim Router-Konfigurationsprogramm an, und wählen Sie **VPN > VPN Client Access**. Die Seite *VPN Client Access* wird geöffnet:

## VPN Client Access

Username :

New Password :

Confirm New Password :

Allow Password Change :  Yes  No

Active :

--

## Certificate Management

Generate New Certificate :

Export Certificate for Administrator :

Export Certificate for Client :

Import Certificate :  No file chosen

Existing Certificate : RV042G\_0101\_0000.pem

### VPN Client Access

Username :	<input type="text" value="user_1"/>
New Password :	<input type="password" value="...."/>
Confirm New Password :	<input type="password" value="...."/>
Allow Password Change :	<input type="radio"/> Yes <input checked="" type="radio"/> No
Active :	<input checked="" type="checkbox"/>

Schritt 2: Geben Sie den Benutzernamen für den VPN-Client in das Feld "Username" (Benutzername) ein.

Schritt 3: Geben Sie das Kennwort für den Benutzer in das Feld "New Password" (Neues Kennwort) ein.

Schritt 4: Geben Sie das Kennwort erneut ein, um es im Feld Neues Kennwort bestätigen zu bestätigen.

Schritt 5: (Optional) Klicken Sie auf das Optionsfeld **Ja**, um dem Benutzer das Ändern seines Kennworts zu ermöglichen.

Schritt 6: Aktivieren Sie das Kontrollkästchen **Aktiv**, um den VPN-Benutzer zu aktivieren.

Schritt 7. Klicken Sie auf **Zur Liste hinzufügen**, um den Benutzer zur Tabelle hinzuzufügen.

### VPN Client Access

Username :

New Password :

Confirm New Password :

Allow Password Change :  Yes  No

Active :

user_1=>Active
----------------

### VPN Client Access

Username :

New Password :

Confirm New Password :

Allow Password Change :  Yes  No

Active :

user_1=>Active
user_2=>Active

Schritt 8: (Optional) Um Informationen über einen Benutzer zu bearbeiten, klicken Sie auf den entsprechenden Benutzer in der Tabelle. Bearbeiten Sie die erforderlichen Informationen, und klicken Sie dann auf **Aktualisieren**. Sie können den Benutzernamen nicht bearbeiten.

Schritt 9: (Optional) Um einen Benutzer aus der Tabelle zu löschen, klicken Sie auf den entsprechenden Benutzer in der Tabelle und anschließend auf **Löschen**.

Schritt 10: (Optional) Um einen neuen VPN-Benutzer hinzuzufügen, klicken Sie auf **Add New (Neu hinzufügen)**, und befolgen Sie die Schritte [1](#) bis 7.

Schritt 11. Klicken Sie auf **Speichern**, um die Einstellungen zu speichern.

## Zertifikatsverwaltung

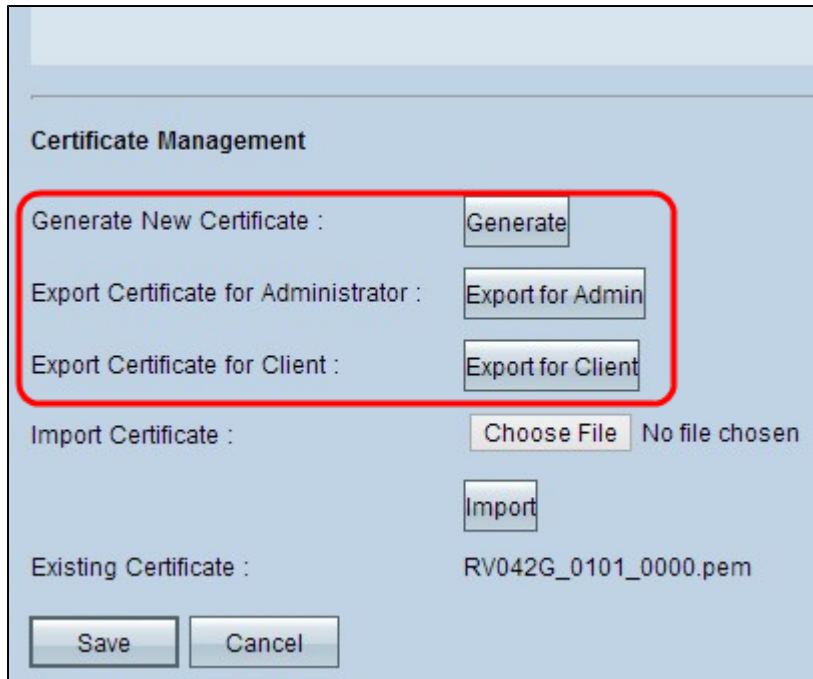
**Hinweis:** Es ist möglich, eine VPN-Verbindung ohne Zertifikat auf dem PC zu haben. Ein Zertifikat erhöht jedoch die Sicherheit des VPN.

Schritt 1: Melden Sie sich beim Router-Konfigurationsprogramm an, und wählen Sie **VPN > VPN Client Access aus**. Die Seite "VPN Client Access" wird geöffnet. Blättern Sie nach unten zum Bereich Zertifikatsverwaltung.

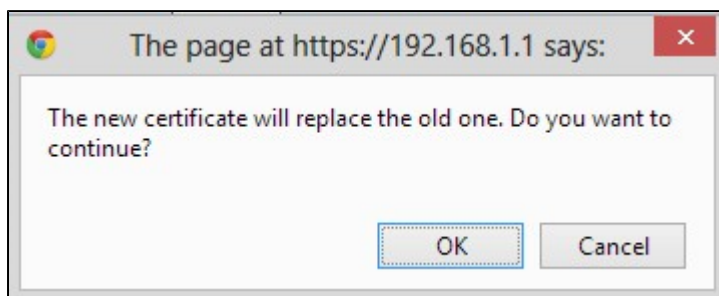
The screenshot displays the "VPN Client Access" configuration interface. At the top, there are input fields for "Username", "New Password", and "Confirm New Password", along with radio buttons for "Allow Password Change" (Yes/No) and a checkbox for "Active". Below these is a list of users: "user\_1=>Active", "user\_2=>Active", "user23=>Active", and "user\_3=>Active". An "Add to list" button is located to the right of the list. At the bottom of the page, the "Certificate Management" section is highlighted with a red box. It contains buttons for "Generate New Certificate" (Generate), "Export Certificate for Administrator" (Export for Admin), "Export Certificate for Client" (Export for Client), "Import Certificate" (Choose File, No file chosen, Import), and "Existing Certificate" (RV042G\_0101\_0000.pem). "Save" and "Cancel" buttons are at the bottom left of the Certificate Management section.

Das aktuelle Zertifikat wird im Feld Vorhandenes Zertifikat angezeigt. Wenn Sie ein Zertifikat auf Ihren PC exportieren möchten, wechseln Sie zum Abschnitt [Zertifikat exportieren](#). Wenn Sie ein Zertifikat von Ihrem PC auf den Router importieren möchten, wechseln Sie zum Abschnitt [Zertifikat importieren](#).

### Zertifikat exportieren



Schritt 1: (Optional) Klicken Sie auf **Generate (Erstellen)**, um ein neues Zertifikat für den Router zu generieren. Dadurch wird das vorherige Zertifikat durch das neue ersetzt. Ein Warnmeldungsfenster wird angezeigt:



Schritt 2: Klicken Sie auf **OK**, um mit einem neuen Zertifikat fortzufahren und das alte Zertifikat durch das neue zu ersetzen.

Schritt 3. (Optional) Um ein Zertifikat als Backup auf Ihrem PC herunterzuladen und zu speichern, klicken Sie auf **Als Administrator exportieren**. Ein Administratorzertifikat enthält den privaten Schlüssel und wird als Sicherung beim Zurücksetzen auf die Werkseinstellungen verwendet.

Schritt 4: Klicken Sie auf **Exportieren für Client**, um ein Clientzertifikat herunterzuladen und auf Ihrem PC zu speichern. Er wird verwendet, während der Benutzer auf den VPN-Tunnel zugreift. Der Router speichert eine PEM-Datei auf Ihrem Computer.

**Hinweis:** Um eine PEM-Datei im Zertifikatspeicher von Windows zu speichern, muss sie in eine PFX- oder P12-Datei konvertiert werden.

## Zertifikat importieren

**Certificate Management**

Generate New Certificate :

Export Certificate for Administrator :

Export Certificate for Client :

Import Certificate :  LICENSE

Existing Certificate : RV042G\_0101\_0000.pem

Schritt 1: Klicken Sie auf **Choose File** (Datei auswählen), und wählen Sie das Zertifikat aus, das Sie importieren möchten. Der Dateityp sollte ".pem" sein.

Schritt 2: Klicken Sie auf **Importieren**, um das Zertifikat zu importieren.

Schritt 3: Klicken Sie auf **Speichern**, um die Einstellungen zu speichern.

## Cisco QuickVPN-Einrichtung

**Hinweis:** Diese Software wird nur für Windows-Betriebssysteme unterstützt. Sie können diese Software auf der offiziellen Cisco Website ([www.cisco.com](http://www.cisco.com)) herunterladen.

Schritt 1: Öffnen Sie Cisco QuickVPN.

Small Business  
**cisco QuickVPN Client**

Profile Name :

User Name :

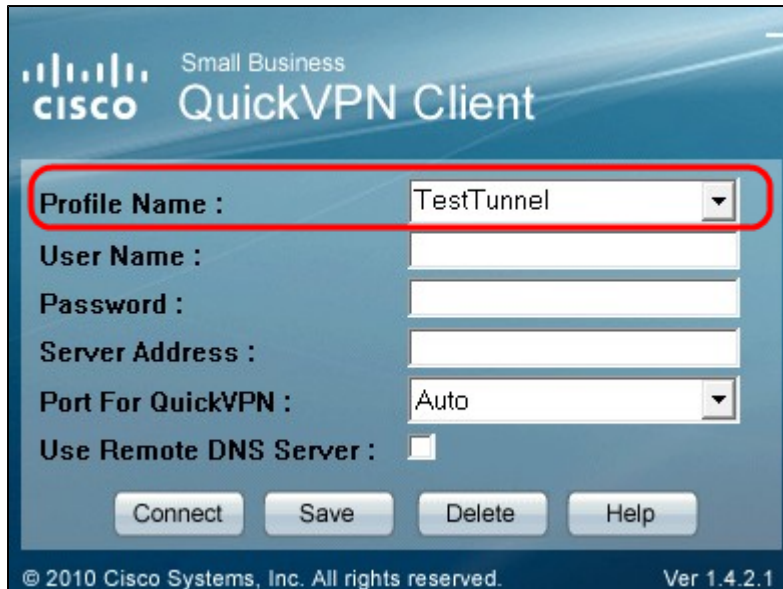
Password :

Server Address :

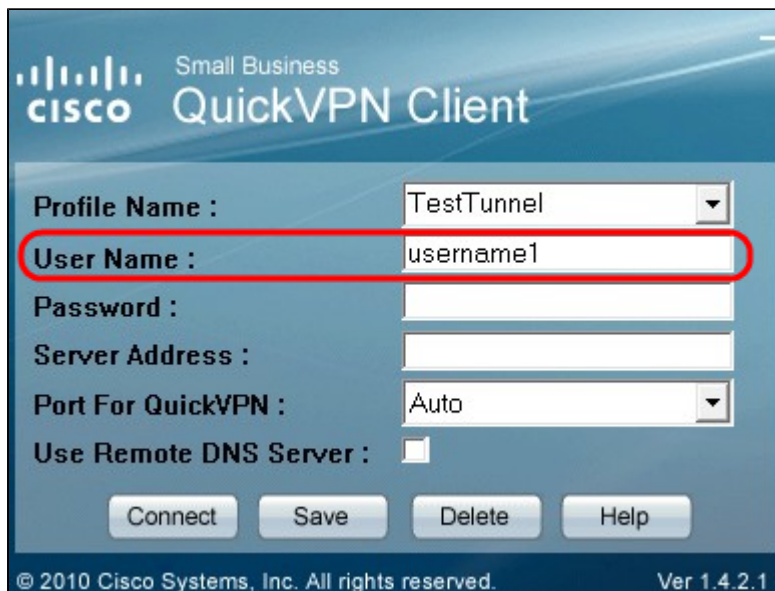
Port For QuickVPN : Auto

Use Remote DNS Server :

© 2010 Cisco Systems, Inc. All rights reserved. Ver 1.4.2.1

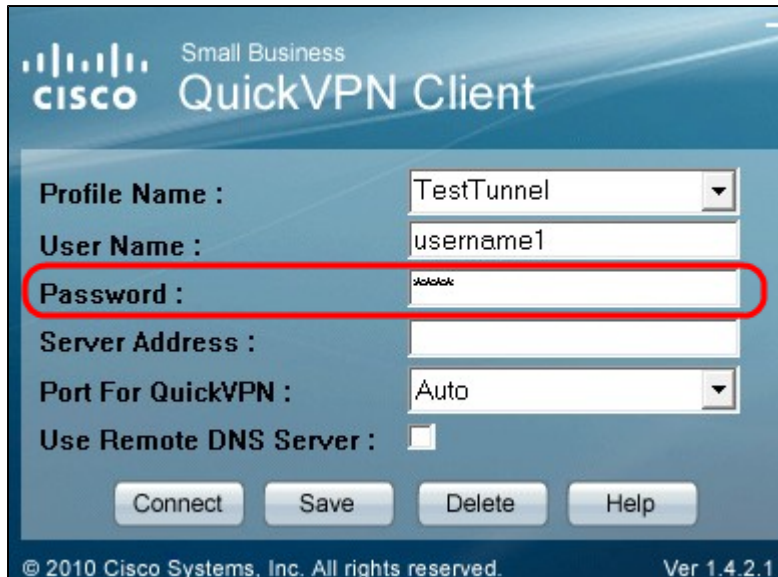


Schritt 2: Geben Sie im Feld Profile Name (Profilname) den Namen des VPN-Tunnels ein, der auf dem kabelgebundenen RV-Router erstellt wurde.

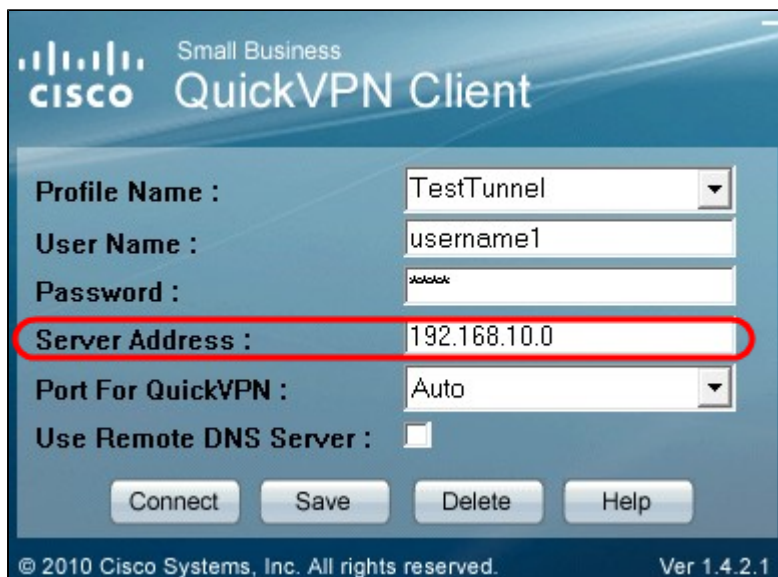


Schritt 3: Geben Sie im Feld User Name (Benutzername) den Benutzernamen ein, der dem Router zugewiesen wurde.





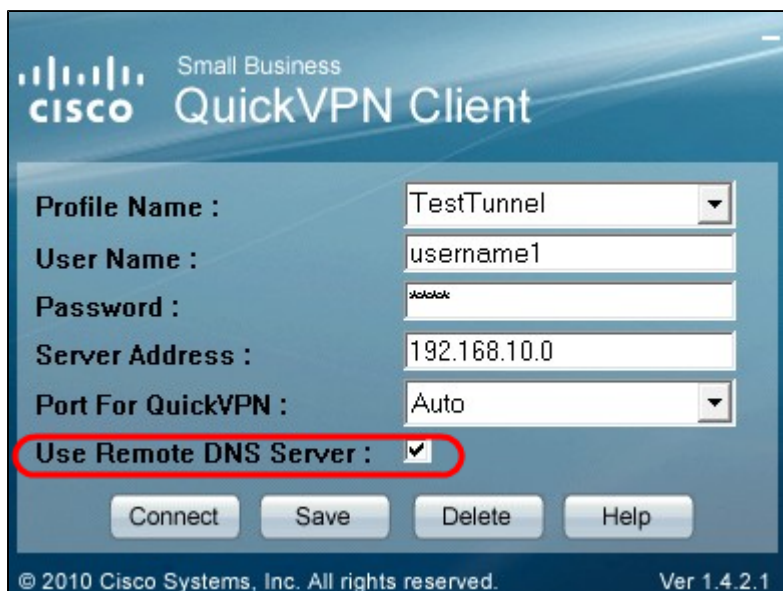
Schritt 4: Geben Sie im Feld Password (Kennwort) das Kennwort ein, das dem Router zugewiesen wurde.



Schritt 5: Geben Sie im Feld Server Address (Serveradresse) die IP-Adresse des Routers ein, der für VPN verwendet wird.



Schritt 6: Wählen Sie in der Dropdown-Liste "Use Remote DNS Server" (Remote-DNS-Server verwenden) die entsprechende Anschlussnummer aus. Auto (Automatisch) ist der Standardwert, der die Portnummer basierend auf den VPN-Einstellungen automatisch auswählt.



Schritt 7. Aktivieren Sie das Kontrollkästchen **Remote-DNS-Server verwenden**, wenn Sie einen DNS-Server haben, der Domännennamen auflösen kann. Andernfalls deaktivieren Sie ihn, und verwenden Sie die VPN-Netzwerkeinstellungen.



Schritt 8: Klicken Sie auf **Verbinden**, um auf das VPN zuzugreifen.

Schritt 9: Klicken Sie auf "**Speichern**", um die Konfiguration zu speichern.

Schritt 10: (Optional) Klicken Sie auf **Löschen**, um eine gespeicherte Konfiguration zu löschen.

## Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.