. . . c o n n e c t i n g y o u r b u s i n e s s

LANCOM Advanced VPN Client

- **Handbuch**
- **Manual**

LANCOM
Systems

LANCOM Advanced VPN Client

LANCOM Systems

LANCOM Systems GmbH
Adenauerstr. 20/B2
52146 Würselen
Deutschland

www.lancom.de

Würselen, November 2011

110972/1111

Einleitung

LANCOM Systems bietet mit dem LANCOM Advanced VPN Client eine Software mit umfangreichen Security-Funktionen, die optimal auf die LANCOM-VPN-Gateways abgestimmt ist. Der vorliegende Schnelleinstieg umfasst alle Konfigurationsschritte, die zur VPN-gesicherten RAS-Einwahl eines entfernten Rechners mit LANCOM Advanced VPN Client auf ein LANCOM-VPN-Gateway notwendig sind:

- 'LANCOM Advanced VPN Client installieren, aktivieren und upgraden' > Seite 2
- 'VPN-Zugang auf dem Router mit dem 1-Click-Wizard einrichten' > Seite 7
- 'VPN-Zugang auf dem Router manuell einrichten' > Seite 9
- 'LANCOM Advanced VPN Client konfigurieren' > Seite 11
- 'LANCOM Advanced VPN Client auf Zertifikatsverbindungen einstellen' > Seite 16
- 'Extended Authentication Protocol (XAUTH)' > Seite 18

Hinweise zur Konfiguration des LANCOM Advanced VPN Clients bei der Verwendung von anderen Gateways entnehmen Sie bitte der integrierten Hilfe bzw. dem zugehörigen Handbuch.

Neben dem vorliegenden **Schnelleinsteig** finden Sie in der kompletten Dokumentation zur vorgestellten VPN-Lösung weitere Informationen:

- Das **Benutzerhandbuch zum LANCOM Advanced VPN Client** beschreibt vollständig die umfangreichen Funktionen der VPN-Client-Software mit allen Parametern.
- Das **Benutzerhandbuch zu Ihrem LANCOM-Gerät** enthält alle Informationen, die zur Inbetriebnahme Ihres Gerätes notwendig sind. Außerdem finden Sie hier alle wichtigen technischen Spezifikationen.
- Das **Referenzhandbuch** ergänzt das Benutzerhandbuch und geht ausführlich auf Themen ein, die auch modellübergreifend für das LANCOM-Betriebssystem LCOS gelten.

Benutzer- und Referenzhandbuch befinden sich je nach Modell als Acrobat-Dokument (PDF-Datei) auf der beiliegenden CD. Aktuelle Versionen von Dokumentation und Software finden Sie jederzeit auf www.lancom.de/download.

DE

1 LANCOM Advanced VPN Client installieren, aktivieren und upgraden

Zur Installation des LANCOM Advanced VPN Clients legen Sie bitte die mitgelieferte CD in Ihr CD-ROM-Laufwerk. Sollte das Setup-Programm nach einigen Sekunden nicht automatisch starten, öffnen Sie bitte die Datei „autostart.exe" aus dem Stammverzeichnis der CD. Der folgende Assistent leitet Sie durch die weiteren Schritte der Installation. Wählen Sie dabei die 'Standard-Installation' aus.

Sollte bereits eine frühere Version des Clients vorhanden sein, so wird diese automatisch erkannt und es wird ein Update durchgeführt.

Zur vollständigen Installation ist ein Neustart erforderlich.

Aktivierung

Nach dem Neustart ist der LANCOM Advanced VPN Client bereits vollständig installiert. Sie können den LANCOM Advanced VPN Client vor der Aktivierung 30 Tage lang testen. Nach dem Start des Clients erscheint das Hauptfenster.

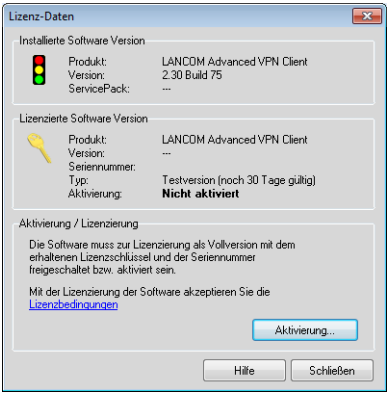
Um nach der 30 Tage-Testphase den vollen Funktionsumfang nutzen zu können ist eine Produktaktivierung notwendig. Hierfür stehen drei mögliche Szenarien zur Verfügung:

- Es handelt sich um eine **Erstinstallation** mit Erwerb einer vollen Lizenz.

- Ein Software- und Lizenz-**Upgrade** von einer früheren Version mit Erwerb einer neuen Lizenz. Hier können alle neuen Funktionen der neuen Version benutzt werden.
- Ein Software-**Update** als reines Bugfixing. Sie behalten Ihre bisherige Lizenz bei. Hierbei wird zwar die neue Client-Version installiert, jedoch steht dem Anwender nur der Funktionsumfang der bisherigen Version zur Verfügung. Der Anwender profitiert hierbei von Fehlerbehebungen gegenüber der bisherigen Version.

In jedem Fall sind folgende Schritte durchzuführen:

1. Klicken Sie im Hauptfenster auf **Aktivierung**. Im Folgenden erscheint ein Dialog, der Ihre aktuelle Versionsnummer und die verwendete Lizenz anzeigt.



Dieser Dialog kann alternativ im Hauptfenster über den Menüpunkt **Hilfe ▶ Lizenzinfo und Aktivierung** aufgerufen werden.

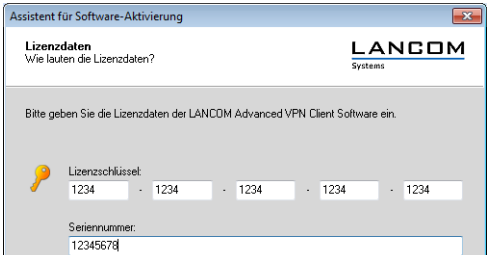
2. Klicken Sie hier erneut auf **Aktivierung**. Sie können die Aktivierung online oder offline vornehmen.

Auch für die „Offline-Aktivierung“ wird ein Zugang zum Internet benötigt.

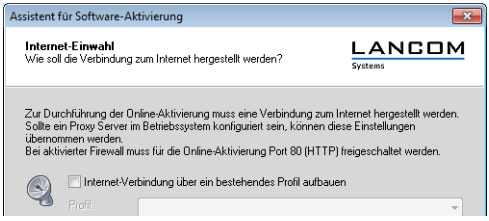
DE

Online-Aktivierung

1. Wenn Sie die Online-Aktivierung wählen, geben Sie in folgendem Dialog Ihre Lizenzdaten ein. Diese haben Sie mit dem Erwerb des LANCOM Advanced VPN Clients erhalten.



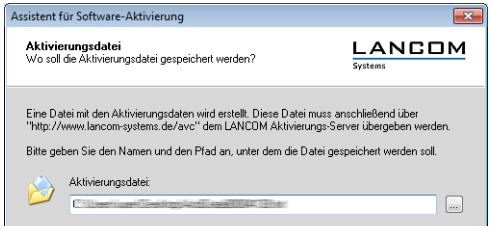
2. Der Client stellt eine Verbindung zum LANCOM-Server her.



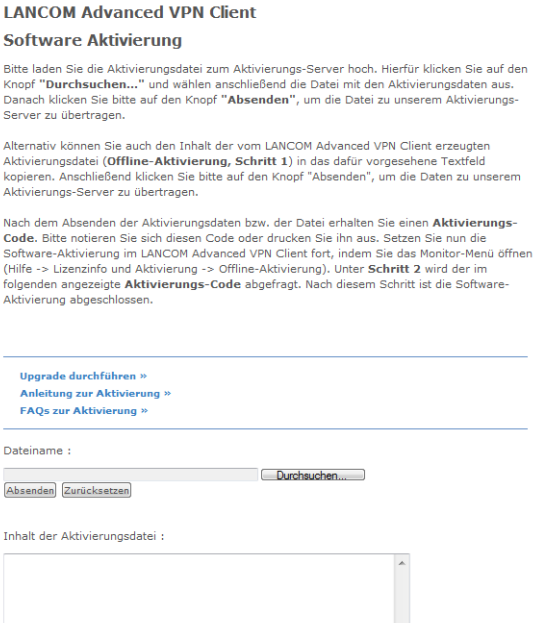
Falls Sie bereits eine ältere Version des LANCOM Advanced VPN Clients benutzen, können Sie ein bereits eingerichtetes VPN-Profil zur Verbindung mit dem Internet verwenden. Sobald der Computer über eine Verbindung mit dem Internet verfügt, verbindet er sich automatisch mit dem Aktivierungs-Server. Die Aktivierung erfolgt automatisch und der Vorgang schließt selbstständig ab.

Offline-Aktivierung

1. Wenn Sie die Offline-Aktivierung gewählt haben, müssen Sie genauso wie bei der Online-Aktivierung zunächst Ihre Lizenzdaten und die Seriennummer eingeben. Diese werden dann überprüft und in einer Datei auf Festplatte gespeichert. Den Dateinamen können Sie frei wählen, es muß sich allerdings um eine Textdatei (.txt) handeln.



2. In dieser Aktivierungsdatei sind Ihre Lizenzdaten enthalten. Zur Aktivierung muß diese Datei dem Aktivierungs-Server übergeben werden. Starten Sie dazu Ihren Browser und öffnen Sie die Seite www.lancom.de/avc/activation.

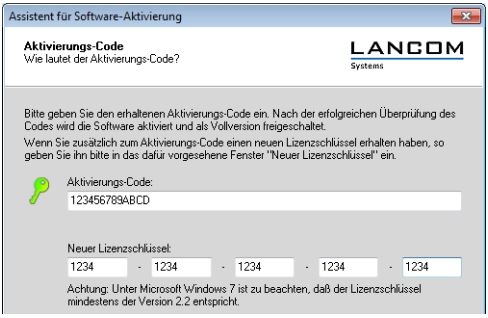


3. Klicken Sie auf **Durchsuchen** und wählen Sie die eben erstellte Aktivierungsdatei aus. Im Anschluss daran klicken Sie auf **Absenden**. Die Akti-

DE

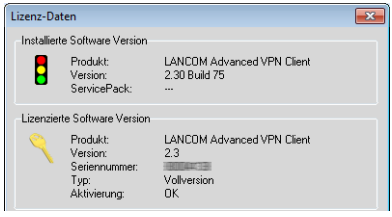
vierungsdatei wird nun vom Aktivierungs-Server bearbeitet. Sie werden auf eine Website weitergeleitet, der Sie Ihren Aktivierungs-Code entnehmen können. Drucken Sie diese Seite aus oder notieren Sie sich den angegebenen Code.

4. Wechseln Sie wieder zum LANCOM Advanced VPN Client und klicken Sie im Hauptfenster auf **Aktivierung**. Geben Sie im folgenden Dialog den Code ein, den Sie ausgedruckt oder notiert haben.



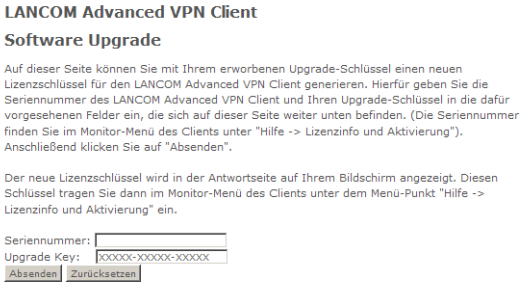
5. Mit der Eingabe des Aktivierungs-Codes ist die Produktaktivierung abgeschlossen und Sie können den LANCOM Advanced VPN Client im Umfang Ihrer Lizenz benutzen.

Abhängig von der von Ihnen erworbenen Lizenz wird nun die Lizenz- und Versions-Nummer angezeigt.



Upgrade

Wenn Sie bereits über eine frühere Version des LANCOM Advanced VPN Clients verfügen und einen Upgrade-Schlüssel auf die aktuelle Version erworben haben, können Sie unter www.lancom.de/avc/upgrade einen neuen Lizenzschlüssel anfordern.



1. Geben Sie die Seriennummer des LANCOM Advanced VPN Clients und Ihren Upgrade-Schlüssel in die dafür vorgesehenen Felder ein. Die Seriennummer finden Sie im Monitor-Menü des Clients unter **Hilfe ▶ Lizenzinfo und Aktivierung**.
2. Anschließend klicken Sie auf **Absenden**. Der neue Lizenzschlüssel wird in der Antwortseite auf Ihrem Bildschirm angezeigt.
3. Diesen Schlüssel tragen Sie dann im Monitor-Menü des Clients unter dem Menü-Punkt **Hilfe ▶ Lizenzinfo und Aktivierung ▶ Lizenzierung** ein.

Nach Eingabe des neuen Lizenzschlüssels startet der Aktivierungsvorgang.

2 VPN-Zugang auf dem Router mit dem 1-Click-Wizard einrichten

Die VPN-Zugänge im LANCOM VPN Router lassen sich sehr einfach mit dem Setup-Assistenten erstellen und in eine Datei exportieren, die vom LANCOM Advanced VPN Client als Profil eingelesen werden kann. Dabei werden die erforderlichen Informationen der aktuellen Konfiguration des LANCOM VPN Router entnommen und mit zufällig ermittelten Werten ergänzt (z.B. für den Preshared Key).

1. Starten Sie über LANconfig den Setup-Assistenten 'Zugang bereitstellen' und wählen Sie die 'VPN-Verbindung'.

2. Aktivieren Sie die Optionen 'LANCOM Advanced VPN Client' und 'Beschleunigen Sie das Konfigurieren mit 1-Click-VPN'.
3. Geben Sie den Namen für diesen Zugang ein und wählen Sie aus, über welche Adresse der Router aus dem Internet erreichbar ist.
4. Im letzten Schritt können Sie wählen, wie die neuen Zugangsdaten ausgegeben werden sollen:
   - ☐ Profil als Importdatei für den LANCOM Advanced VPN Client speichern
   - ☐ Profil per E-Mail versenden
   - ☐ Profil ausdrucken

Das Versenden der Profildatei per E-Mail stellt ein Sicherheitsrisiko dar, weil die E-Mail unterwegs ggf. abgehört werden könnte!

Zum Versenden der Profildatei per E-Mail muss in der Konfiguration des Geräts ein SMTP-Konto mit den erforderlichen Zugangsdaten in dem LANCOM VPN Router eingerichtet sein. Außerdem muss auf dem Konfigurationsrechner ein E-Mail-Programm als Standard-Mail-Anwendung eingerichtet sein, über die auch andere Anwendungen E-Mails versenden dürfen.

Beim Erstellen des VPN-Zugangs werden Einstellungen verwendet, die optimal auf die Verwendung im LANCOM Advanced VPN Client abgestimmt sind, darunter z.B.:

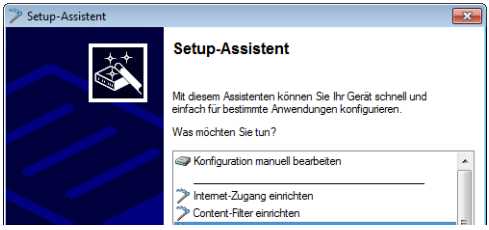
- Gateway: Sofern im LANCOM VPN Router definiert, wird hier ein DynDNS-Name verwendet, ansonsten die IP-Adresse
- FQUN: Kombination aus dem Namen der Verbindung, eine fortlaufenden Nummer und der internen Domäne im LANCOM VPN Router
- Domäne: Sofern im LANCOM VPN Router definiert, wird hier die interne Domäne verwendet, ansonsten ein DynDNS-Name oder die IP-Adresse
- VPN IP-Netze: Alle im Gerät definierten IP-Netzwerke vom Typ 'Intranet'.
- Preshared Key: Zufällig generierter Schlüssel mit einer Länge von 16 ASCII-Zeichen.
- Automatische Medienerkennung als Verbindunsmedium.
- VoIP-Priorisierung: Die VoIP-Priorisierung ist standardmäßig aktiviert.
- Exchange Mode: Als Exchange-Mode wir der 'Aggressive Mode' verwendet.
- Seamless Roaming: Per Default aktiviert.

- IKE-Config-Mode: Der IKE-Config-Mode ist aktiviert, die IP-Adress-Informationen für den LANCOM Advanced VPN Client werden automatisch vom LANCOM VPN Router zugewiesen.

3 VPN-Zugang auf dem Router manuell einrichten

Das Einrichten des VPN-Zugangs für einen LANCOM Advanced VPN Client auf Ihrem LANCOM-Router gelingt schnell und komfortabel mit der Konfigurationssoftware LANconfig unter Windows:

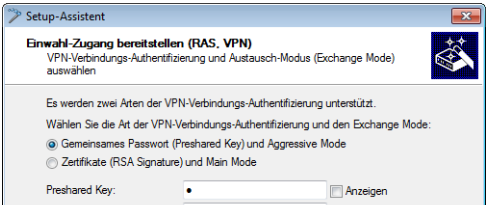
1. Starten Sie LANconfig, klicken Sie mit der rechten Maustaste auf Ihr Gerät und wählen Sie aus dem Kontextmenü den Punkt **Setup Assistent**.
2. Wählen Sie im Setup Assistenten den Eintrag **Zugang bereitstellen (RAS, VPN, IPSec over WLAN)**.



3. Wählen Sie im folgenden Fenster **VPN-Verbindung über das Internet** und im nächsten Schritt den **LANCOM Advanced VPN Client**.
4. Geben Sie einen Benutzernamen für den Benutzer an, der sich in das Netzwerk einwählen soll, z.B. KMUSTERMANN.

DE

5 Geben Sie den **Pre-shared-Key** für Verbindungs-Authentifizierungen nach dem 'Aggressive Mode' ein. Der Pre-shared-Key wird zur Verschlüsselung der Verbindung zwischen Client und Gateway verwendet.



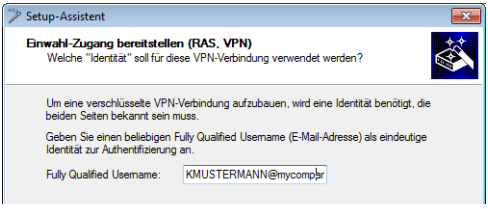
Für jeden Benutzer kann ein eigener Pre-shared-Key verwendet werden. Machen Sie von dieser Möglichkeit Gebrauch, um die Sicherheit der VPN-Verbindungen weiter zu verbessern!

Wählen Sie alternativ die Option **Zertifikate (RSA Signature)**, wenn die Verbindungs-Authentifizierung über den sichereren 'Main Mode' mit Hilfe von digitalen Zertifikaten erfolgen soll.

Bitte beachten Sie, dass in diesem Fall digitale Zertifikate sowohl für den Einwahl-Router als auch für den VPN-Client benötigt werden.

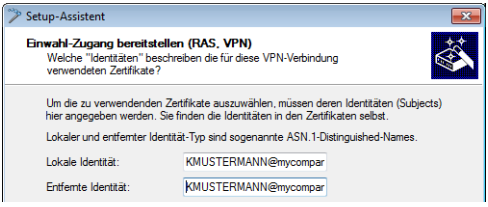
Nur für Aggressive Mode/Preshared Key

6 Geben Sie als **Fully Qualified Username** eine E-Mail-Adresse des Nutzers ein, mit der sich der Client beim VPN-Gateway authentifizieren kann.



Nur für Main Mode/ RSA Signature

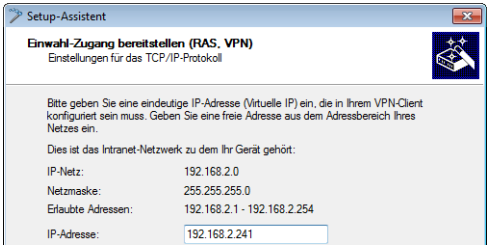
7 Geben Sie die **Lokale Identität** und die **Entfernte Identität** an, um den Verbindungsaufbau über Zertifikate zu ermöglichen.



Lokaler und entfernter Identitäts-Typ sind so genannte „ASN.1.Distinguished Names" und können den Zertifikaten entnommen werden.

8 Zur Einwahl in das LAN muss der VPN-Client über eine gültige IP-Adresse aus dem Adressbereich des LANs verfügen. Tragen Sie im folgenden Dialog eine IP-Adresse ein, die diesem Client bei der Einwahl in das LAN zugewiesen werden soll.

Achten Sie darauf, dass es sich um eine freie IP-Adresse handelt, diese darf z.B. von einem DHCP-Server im LAN nicht an andere Geräte vergeben werden.



9 Im folgenden Fenster können Sie angeben, auf welche Bereiche des lokalen Netzwerkes der Client zugreifen darf. Im Normalfall kann die Voreinstellung **Alle IP-Adressen für den VPN-Client erlauben** beibehalten werden. Soll der Client nur auf ein bestimmtes Subnetz oder einen begrenzten IP-Adressbereich zugreifen dürfen, können Sie dieses nach dem Markieren von **Folgendes IP-Netzwerk soll vom VPN-Client erreicht werden können** mit Hilfe der Angaben für das IP-Netz und die Netzwerkmaske näher bestimmen.

10 Wenn Sie in einem Microsoft Windows Netzwerk arbeiten, lassen Sie die Einstellung **NetBIOS über IP Routing aktivieren** eingeschaltet. Bestätigen Sie mit **Weiter**. Ein Klick auf **Fertig stellen** beendet die Konfiguration.

4 LANCOM Advanced VPN Client konfigurieren

Nach einem Neustart des Computers startet der LANCOM Advanced VPN Client automatisch - diese Funktion kann im LANCOM Advanced VPN Client später unter dem Menüpunkt **Fenster ▶ Autostart ▶ kein Autostart** ausgeschaltet werden. Solange der LANCOM Advanced VPN Client aktiv ist, erscheint in der Symbolleiste in der rechten unteren Bildschirmecke ein Ampel-Symbol.

Sofern noch kein Profil eingerichtet ist, startet mit dem LANCOM Advanced VPN Client automatisch ein Assistent, der Ihnen bei der Erstellung des ersten

DE

Profils behilflich ist. Möchten Sie später zu den bereits bestehenden Profilen ein weiteres Profil hinzufügen, können Sie den Assistenten jederzeit über **Konfiguration ▶ Profile ▶ Neuer Eintrag** starten.

Zur Erstellung eines Profils gehen Sie wie folgt vor:

1. Wählen Sie die Verbindungsmethode **Verbindung zum Firmennetz über IPSec**. Dies gewährleistet, dass die Verbindung verschlüsselt wird.
2. Geben Sie einen aussagekräftigen Namen ein, unter dem das Profil im LANCOM Advanced VPN Client abgelegt werden soll. Eine Möglichkeit ist z.B. der Name der Firma, zu deren Netzwerk eine Verbindung aufgebaut werden soll.
3. Wählen Sie als Verbindungsart **Automatische Medienerkennung**. Aktivieren Sie optional die Checkbox für **Seamless Roaming**.

Wir setzen voraus, dass der Rechner mit dem LANCOM Advanced VPN Client bereits über einen Zugang zum Internet verfügt. Sollte der Internetzugang noch nicht eingerichtet sein, wählen Sie an dieser Stelle die entsprechende Internet-Zugangsart aus. In zusätzlichen Eingabefeldern haben Sie dann die Möglichkeit, die Zugangsdaten zu Ihrem Internetaccount einzutragen (Benutzername, Passwort, Einwahlrufnummer etc.).

4 Im folgenden Fenster geben Sie entweder die IP-Adresse oder alternativ den DNS-Namen des Gateways ein (z.B. vpnserver.musterfirma.de).

Achten Sie darauf, dass es sich bei der IP-Adresse um die öffentliche Adresse des VPN-Gateways des Netzes handeln muss, in das Sie sich einwählen möchten. Wenn Sie die Einstellung **Erweiterte Authentisierung (XAUTH)** aktivieren, kann der Benutzer mit Hilfe von Benutzername und das Passwort authentifiziert werden. Wenn Sie die Felder Benutzername und Passwort frei lassen, wird der Benutzer bei jeder Einwahl zur Eingabe der Login-Daten aufgefordert. Um die Verwendung von XAUTH besonders sicher zu gestalten, sollten Sie nach Möglichkeit anstelle des Preshared-Key-Verfahrens (PSK) die Einwahl über RSA-SIG (Zertifikate) verwenden. Stellen Sie dabei sicher, dass das VPN-Gateway nur das Zertifikat der jeweils richtigen Gegenstelle akzeptiert (und nicht alle von der gleichen CA ausgestellten Zertifikate).

Im Abschnitt 'Extended Authentication Protocol (XAUTH)' > Seite 18 finden Sie weitere Informationen zur Konfiguration des Extended Authentication Protocol XAUTH im VPN-Gateway.

Im Abschnitt 'LANCOM Advanced VPN Client auf Zertifikatsverbindungen einstellen' > Seite 16 finden Sie weitere Informationen zur zertifikatsbasierten Einwahl in einVPN-Gateway.

5 Im nächsten Fenster werden Einstellungen zur Verbindungsherstellung und zur Verschlüsselung der Verbindung abgefragt.

- Wählen Sie als Austausch-Modus die Option **Aggressive Mode**, wenn Sie ausschließlich Pre-Shared-Keys zur Authentifizierung verwenden wollen.

- Wählen Sie den **Main Mode**, wenn Sie für die Authentifizierung digitale Zertifikate verwenden möchten. In diesem Fall müssen Sie nach dem Fertigstellen des Profil-Assistenten das Profil manuell auf die Verwendung der Zertifikate umstellen (‘LANCOM Advanced VPN Client auf Zertifikatsverbindungen einstellen’ > Seite 16).

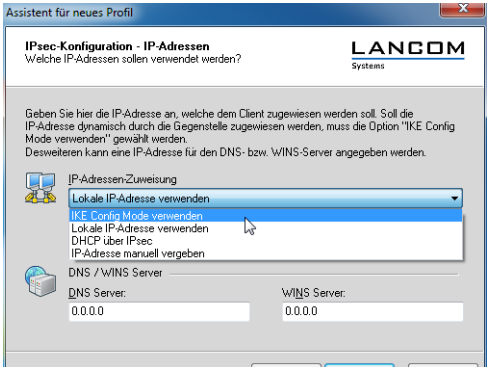
Die Voreinstellungen für die PFS-Gruppe (**DH-Gruppe 2 (1024 Bit)**) können übernommen werden.

6 Tragen Sie im folgenden Dialog in das Feld **Shared Secret** den „Pre-shared-Key“ ein. Als „Lokale Identität“ wählen Sie den Typ **Fully Qualified Username**. Im Feld „ID“ wird die E-Mail-Adresse eingetragen, mit der sich der Client beim VPN-Gateway authentifiziert.

Achten Sie darauf, dass für den „Pre-shared-Key“ und die E-Mail-Adresse exakt die gleichen Werte verwendet werden, die auch im Setup-Assistenten für LANconfig bei der Einrichtung des RAS-Zugangs im VPN-Gateway eingetragen wurden.

7 Im nächsten Fenster wird abgefragt, welche IP-Adresse der Client erhalten soll. Wenn Sie im LANCOM VPN-Gateway eine feste IP-Adresse für den Einwahlzugang vorgeben möchten, können Sie zwischen **lokale IP-**

Adresse verwenden oder **IP-Adresse manuell verwenden** wählen. Sie können aber auch einen Pool von IP-Adressen angeben, aus dem den VPN-Clients dynamisch eine freie IP-Adresse zugewiesen wird (IKE Config Mode). Wenn Sie die Option **IKE Config Mode verwenden** wählen, werden IP-Adressen und DNS Server über das Protokoll IKE-Config Mode zugewiesen. Alternativ zur Verwendung des IKE Config Modes kann auch ein DHCP Server des Gateways genutzt werden mit der Option **DHCP über IPSec**. Dabei wird über den VPN-Tunnel dem Client in einer DHCP-Verhandlung die IP-Adresse zugewiesen.

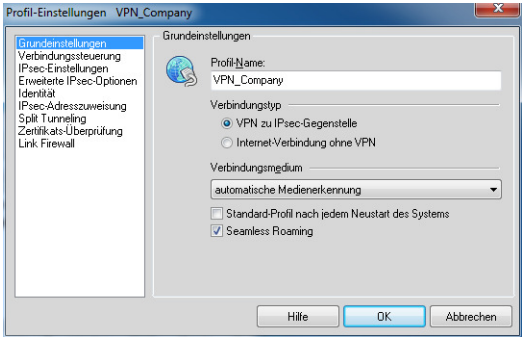


8 Im letzten Fenster der Profil-Konfiguration werden die Netzwerkadressen mit den Netzwerkmasken eingegeben, auf die der Client zugreifen soll. Hier können ggf. verschiedene Teilnetze bzw. Subnetze angegeben werden. Ein Klick auf **Fertigstellen** beendet die Konfiguration.

Nun kann eine Verbindung zum eingestellten Firmennetz hergestellt werden. Hierzu wählen Sie im Hauptfenster des LANCOM Advanced VPN Clients unter **Profil** das von Ihnen gewünschte Verbindungsprofil aus und klicken auf **Verbinden**. Sind alle Einstellungen im Profil und auf dem VPN-Gateway korrekt, wird die Verbindung hergestellt. Der Client-Rechner hat damit Zugriff auf alle freigegebenen Ressourcen im LAN wie z.B. Mail-, Datei- oder Drucker-Server.

DE

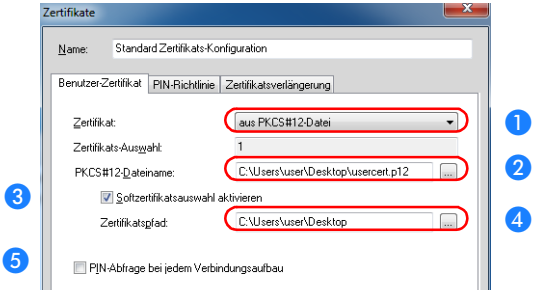
Um ein Profil nachträglich zu ändern, wählen Sie im LANCOM Advanced VPN Client den Menüpunkt **Konfiguration ▶ Profile**, markieren in der Liste der Profile den gewünschten Eintrag und klicken auf **Konfigurieren**.



5 LANCOM Advanced VPN Client auf Zertifikatsverbindungen einstellen

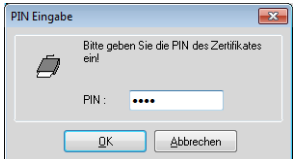
Bei der zertifikatsbasierten Einwahl mit dem LANCOM Advanced VPN Client in einen LANCOM VPN Router müssen die entsprechenden Profil-Einstellungen an die Verwendung von Zertifikaten angepasst werden.

1. Öffnen Sie über den Menüpunkt **Konfiguration ▶ Zertifikate ▶ Bearbeiten** die Einstellungen für eine vorhandene Zertifikats-Konfiguration oder legen Sie mit **Hinzufügen** eine neue Zertifikats-Konfiguration an.



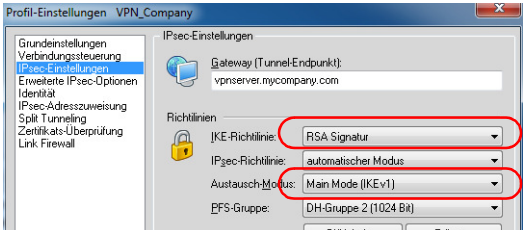
   - Wählen Sie als Zertifikattyp die 'PKCS#12-Datei aus (1) und geben Sie die gewünschte Zertifikatsdatei an (2).
   - Wenn Sie mit verschiedenen Zertifikaten arbeiten möchten, aktivieren Sie die Option 'Softzertifikatsauswahl' (3) und geben den Pfad zum Ordner an, in dem die Zertifikatsdateien abgelegt sind (4).

- Wählen Sie aus, ob die PIN (das Kennwort) für das Zertifikat bei jedem Verbindungsaufbau abgefragt werden soll (5). Alternativ können Sie die PIN über den Menüpunkt **Verbindung** ▶ **PIN eingeben** fest im LANCOM Advanced VPN Client speichern.



- Bei aktivierter Softzertifikatsauswahl können Sie beim Verbindungsaufbau im Hauptfenster des LANCOM Advanced VPN Clients jeweils das gewünschte Zertifikat aus der Liste auswählen, passend zum gewählten Profil.

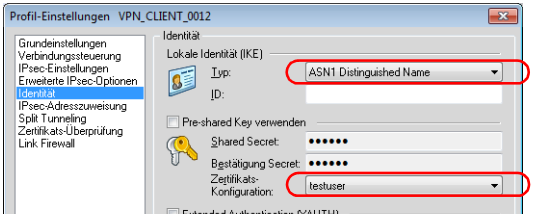
(2) Stellen Sie in den IPSec-Einstellungen des Profils die IKE-Richtlinie auf **RSA-Signatur** um und den Austausch-Modus auf **Main Mode**.



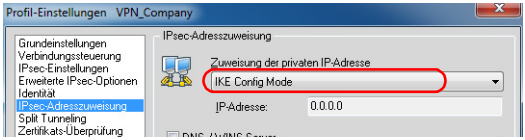
(3) Stellen Sie die Identität auf **ASN1 Distinguished Names** um. Die ID kann frei bleiben, da diese Information aus dem Zertifikat ausgelesen wird.

DE

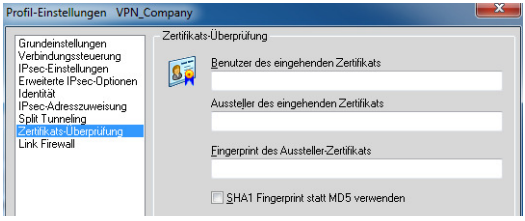
Deaktivieren Sie die Option **Pre-shared Key verwenden** und wählen Sie die zuvor definierte Zertifikats-Konfiguration für dieses Profil aus.



4 Verwenden Sie bei der IP-Adressen-Zuweisung den **IKE Config Mode**.



5 Bei der Zertifikatsüberprüfung können Sie optional die Zertifikate einschränken, die der LANCOM Advanced VPN Client akzeptiert. Dazu geben Sie den Benutzer und/oder den Aussteller des eingehenden Zertifikats und ggf. den zugehörigen „Fingerprint" an.



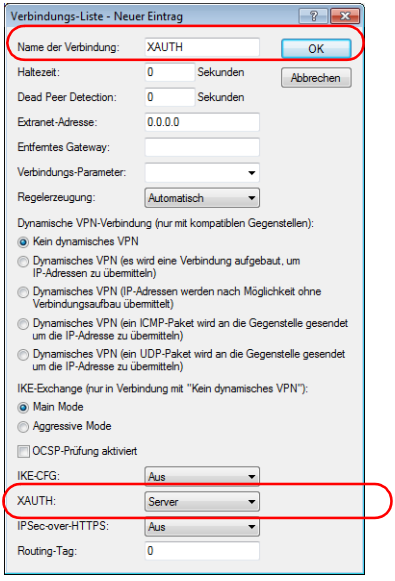
6 Extended Authentication Protocol (XAUTH)

Mit der Verwendung von XAUTH wird eine zusätzliche Authentifizierung mit XAUTH-Benutzernamen und XAUTH-Kennwort durchgeführt. Diese Authentifizierung kann im LCOS über eine interne Benutzertabelle (die PPP-Liste) geprüft werden.

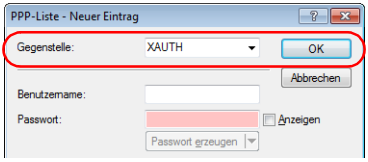
Um die Verwendung von XAUTH besonders sicher zu gestalten, sollten Sie nach Möglichkeit anstelle des Preshared-Key-Verfahrens (PSK) die Einwahl über RSA-SIG (Zertifikate) verwenden. Stellen Sie dabei sicher, dass das VPN-Gateway nur das Zertifikat der jeweils richtigen

Gegenstelle akzeptiert (und nicht alle von der gleichen CA ausgestellten Zertifikate).

Für die Authentifizierung von VPN-Gegenstellen über XAUTH wird der entsprechende Eintrag in der VPN-Verbindungsliste (LANconfig: VPN ▶ Allgemein ▶ Verbindungs-Liste) auf die Betriebsart als XAUTH-Server umgestellt.



Zusätzlich wird in der PPP-Liste ein Eintrag erstellt, in dem der Name der Gegenstelle dem Namen der VPN-Verbindung entspricht (LANconfig: Kommunikation ▶ Protokolle ▶ PPP-Liste). Weiterhin wird in diesem Eintrag das Kennwort hinterlegt sowie weitere Optionen wie die gerouteten Protokolle definiert.



Der Benutzername aus dem Eintrag in der PPP-Liste wird **nicht** für die Authentifizierung verwendet.

EN

Introduction

LANCOM Systems provides the LANCOM Advanced VPN Client, a program which features comprehensive security functions and is ideally designed to meet the requirements of the LANCOM VPN gateways. The following Quick Start Guide covers all of the necessary steps for the configuration of a VPN-secured RAS connection of a remote computer with LANCOM Advanced VPN Client via a LANCOM VPN gateway:

Instructions for the configuration of the LANCOM Advanced VPN Client in combination with other gateways can be taken from the integrated Help or from the relevant user manual.

In addition to the **Quick Start Guide** at hand, you will find more information about the VPN solution presented here in the complete documentation:

- The **User Manual for the LANCOM Advanced VPN Client** fully describes the extensive range of functions and parameters in the VPN client software.
- The **User Manual for your LANCOM device** contains all of the detailed information required for setting up your device. It also contains all of the important technical specifications.
- The **Reference Manual** supplements the User Manual and fully addresses issues concerning the LANCOM operating system LCOS that also apply to all other models.

The User and Reference Manual are supplied as Acrobat documents (PDF files) on the accompanying CD, depending on the model. The latest versions of documentation and software are always available from www.lancom.eu/download.

1 Installing, activating and upgrading the LANCOM Advanced VPN Client

To install the LANCOM Advanced VPN Client insert the program CD supplied with the device into your CD-ROM drive. The setup program should start automatically within seconds; if not, please manually execute the "autostart.exe" in the root directory of the CD. A Wizard starts that will guide you through the installation. Select 'Standard Installation'.

If a previous version of the client is already installed, it will be detected and updated automatically.

To complete the installation, you will need to restart the device.

Activation

Once the device has been restarted, the LANCOM Advanced VPN Client installation is complete. You can test the LANCOM Advanced VPN Client for 30 days before activation. Once the client has been started, the main window appears.

The product must be activated in order to make use of the complete set of features after the 30-day trial period has expired. There are three possible scenarios here:

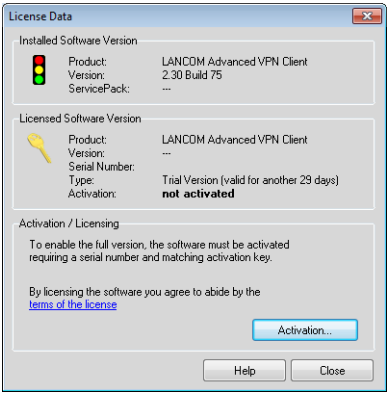
- This is the **first installation** with the purchase of a full license.

- A software and license **upgrade** from a previous version with the purchase of a new license.
- A software **update** for the sole purpose of bug fixing. You retain your previous license. In this case, the new client version is installed but the user only has access to the functionality of the previous version. The user benefits from bug-fixing improvements carried out since the last version.

In every case the following steps must be taken:

EN

1. Click on **Activation** in the main window. A dialog then appears which shows your current version number and the license used.



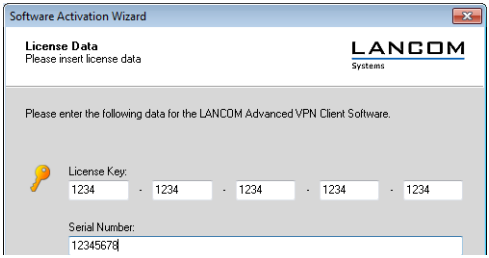
Alternatively, this dialog can be accessed via the menu item **Help ▶ License data and activation**.

2. Click on **Activation** again here. You can activate your product online or offline.

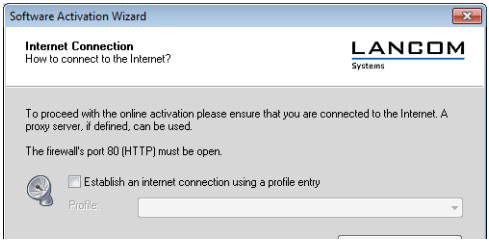
An Internet connection is required for "Offline Activation" as well.

Online Activation

1. If you select Online Activation, enter your license data in the following dialog. You received this information when you purchased your LANCOM Advanced VPN Client.



2. The client must now establish a connection to the LANCOM server.



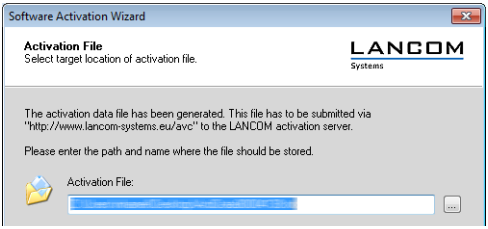
   If you are already using an older version of LANCOM Advanced VPN Client, then you can use your previous configured user profiles to connect to the Internet. As soon as the computer is connected to the Internet, it automatically connects to the activation server. No further action is necessary to carry out the activation and the process terminates automatically upon completion.

Offline Activation

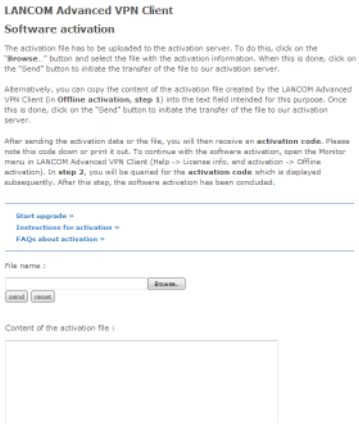
1. If you have selected Offline Activation, you will need to enter your license data and serial number when activating. These are then verified and

EN

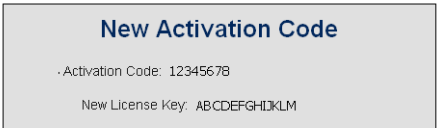
stored in a file on the hard drive. You may select the name of the file freely providing that it is a text file (.txt).



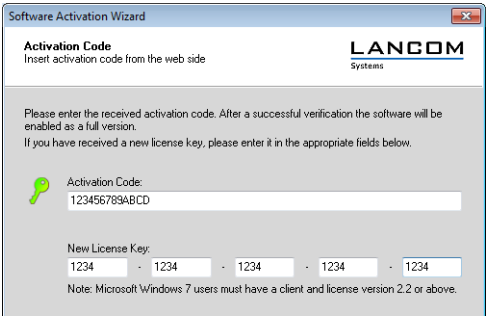
2 Your license data is included in this activation file. This file must be transferred to the activation server for activation. Start your browser and open the www.lancom.de/avc/activation website.



3 Click on **Search** and select the activation file that was just created. Then click **Send**. The activation server will now process the activation file. You will now be forwarded to a website where you will be able to view your activation code. Print this page or make a note of the code listed here.

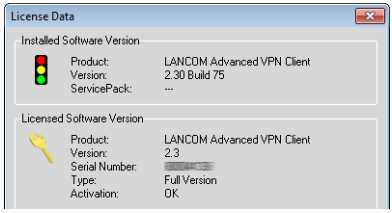


4 Switch back to LANCOM Advanced VPN Client and click on **Activation** in the main window. Enter the code that you printed or made a note of in the following dialog.



5 Once the activation code has been entered, the product activation is complete and you can use the LANCOM Advanced VPN Client as specified within the scope of your license.

Depending on the license you purchased, the license and version number will now appear.

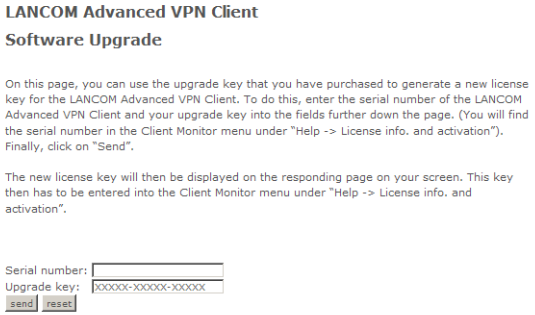


EN

EN

Upgrade

If you already have an earlier version of the LANCOM Advanced VPN Client and you have purchased an upgrade key for the current version, you can request a new license key from www.lancom.eu/avc/upgrade.



1. Enter the serial number of the LANCOM Advanced VPN Client and your upgrade key into the appropriate fields. You will find the serial number in the Client Monitor menu under **Help ▶ License info and activation**.
2. Finally, click on **Send**. The new license key will then be displayed on the responding page on your screen.
3. This key then has to be entered into the Client Monitor menu under **Help ▶ License info and activation**.

The activation procedure commences after entry of the new license key.

2 Set up VPN access on the router with 1-Click-VPN

VPN accesses for employees who dial into the network with the LANCOM Advanced VPN Client are very easy to set up with the Setup Wizard and exported to a file. This file can then be imported as a profile by the LANCOM Advanced VPN Client. All of the information about the LANCOM VPN Router's configuration is also included, and then supplemented with randomly generated values (e.g. for the preshared key).

1. Use LANconfig to start the 'Set up a RAS Account' wizard and select the 'VPN connection'.
2. Activate the options 'LANCOM Advanced VPN Client' and 'Speed up configuration with 1-Click-VPN'.

3. Enter a name for this access and select the address under which the router is accessible from the Internet.
4. In the final step you can select how the access data is to be entered:
   - ☐ Save profile as an import file for the LANCOM Advanced VPN Client
   - ☐ Send profile via e-mail
   - ☐ Print out profile

Sending a profile via e-mail could be a security risk should the e-mail be intercepted en route!

To send the profile via e-mail, the device configuration must be set up with an SMTP account with the necessary access data. Further, the configuration computer requires an e-mail program that is set up as the standard e-mail application and that can be used by other applications to send e-mails.

When setting up the VPN access, certain settings are made to optimize operations with the LANCOM Advanced VPN Client, including:

- Gateway: If defined in the LANCOM VPN Router, a DynDNS name is used here, or alternatively the IP address
- FQUN: Combination of the name of the connection, a sequential number and the internal domain in the LANCOM VPN Router.
- Domain: If defined in the LANCOM VPN Router, the internal domain is used here, or alternatively a a DynDNS name or IP address
- VPN IP networks: All IP networks defined in the device as type 'Intranet'.
- Preshared key: Randomly generated key 16 ASCII characters long.
- Automatic media detection as communication medium.
- VoIP prioritization: VoIP prioritization is activated as standard.
- Exchange mode: The exchange mode to be used is 'Aggressive Mode'.
- Seamless Roaming: Enabled by Default.
- IKE config mode: The IKE config mode is activated, the IP address information for the LANCOM Advanced VPN Client is automatically assigned by the LANCOM VPN Router.

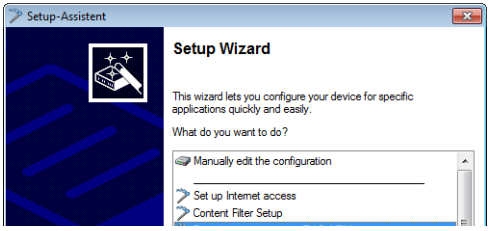
Set up VPN access manually on the router

Setting up VPN access for the LANCOM Advanced VPN Client with your LANCOM router is quick and convenient with the configuration software LANconfig under Windows:

EN

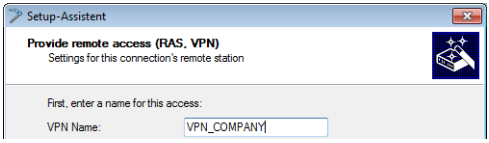
1. Start LANconfig, right-click on your device and select the **Setup Wizard** from the context menu.

2. In the Setup Wizard, select the entry **Provide remote access (RAS, VPN, IPSec over WLAN)**.

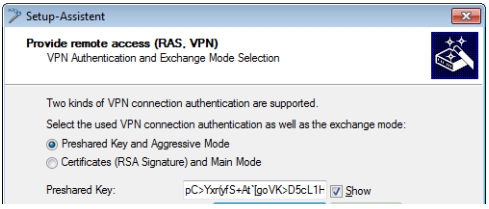


3. In the following windows, select **VPN connection over the Internet** and then **LANCOM Advanced LANCOM VPN Client**.

4. Enter a VPN name for the user who is dialing into the network, such as EXAMPLE.



5. Enter the **Pre-shared key** key for connection authentication in 'Aggressive Mode'. The pre-shared key is used to encrypt the connection between client and gateway.



Each user should be assigned their own pre-shared key. Observing this rule will further increase the security of your VPN connections.

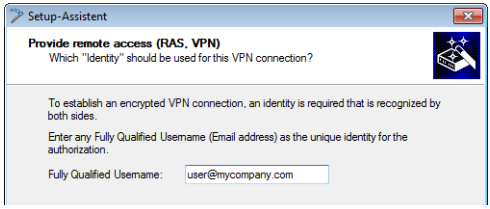
Alternatively, select the 'Certificates (RSA Signature)' option if the connection authentication should take place via the secure 'Main Mode' using digital certificates.

Please note that this will require digital certificates for the dial-up router and the VPN client.

EN

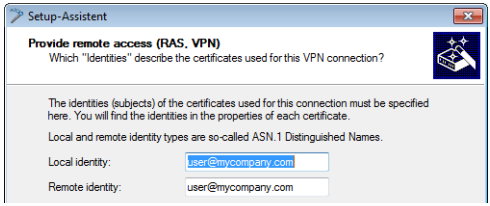
Only for Aggressive Mode/Preshared Key

6 Enter an e-mail address for the user as the **Fully Qualified Username**; this will be used to identify the client at the VPN gateway.



Only for Main Mode/RSA Signature

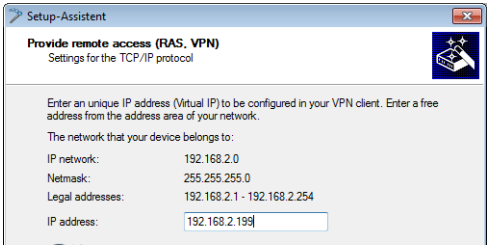
7 Enter the **local identity** and the **remote identity**, in order to allow connection establishment using certificates.



Local and remote identity types are "ASN.1.Distinguished Names" and can be inferred from the certificates.

8 To access the LAN, the VPN client requires a valid IP address from the LAN's address range. In the dialog that follows, enter the IP address that will be assigned to your client when it accesses the LAN.

Ensure that this IP address is freely available and that it cannot, for example, be assigned to another device in the LAN by a DHCP server.



9 The following window allows you to enter the areas of the local network that the client should have access to. In most cases the default setting **Allow all IP addresses to be available to the VPN client** can be used. If the client should have access that is limited to a particular subnet or a limited range of IP addresses, use the option **The following IP network**

should be available to the VPN client which allows you to define the IP network and netmask.

⑩ If you are working in a Microsoft Windows network, leave the option **Activate NetBIOS over IP routing** switched on. Confirm with **Next**. Conclude the configuration by clicking on **Finish**.

4

LANCOM Advanced VPN Client configuration

EN

The LANCOM Advanced VPN Client will run automatically each time Windows is started; to disable this function later in LANCOM Advanced VPN Client, access the menu **Window ▶ Autostart ▶ no Autostart**. As long as LANCOM Advanced VPN Client is active, a traffic light symbol will be displayed in the lower right-hand corner of the screen.

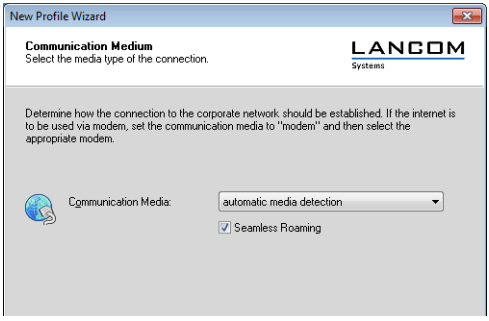
If no profile has been set up, the LANCOM Advanced VPN Client automatically starts a Wizard that will help you create the first profile. To set up additional profiles, you can run the Wizard manually under **Configuration ▶ Profile Settings ▶ New Entry**.

To generate a new profile, proceed as follows:

① Select the connection type **Link to Corporate Network using IPSec**. This ensures that the connection will be secured with encryption.

② Enter a name that adequately describes the profile that is being generated for the LANCOM Advanced VPN Client. One possibility is to use the name of the company whose network is being connected to, for example.

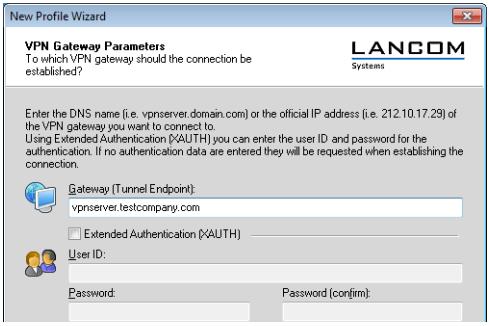
③ Select **Automatic media detection** as the communication medium. Optionally you may enable the **Seamless Roaming** option.



This description assumes that the computer with the LANCOM Advanced VPN Client already has an Internet connection. If the

Internet connection is not already set up, please select the corresponding type of connection now. The following dialogs let you enter the access information for your Internet account (user name, password, dial-up number etc.).

4 In the following window, enter either the IP address or the DNS name of the gateway (e.g. vpnserver.testcompany.com).



Note that this IP address must be the public address of the VPN gateway that you are connecting to. If you activate **Extended authentication (XAUTH)** you can enter the user ID and password for the authentication. If you leave the user ID and password fields empty, the user is asked to enter his credentials at each login. For a more secure XAUTH usage you should use certificate based login (RSA-SIG) whenever possible. Ensure that the VPN gateway will accept the certificates of the intended remote sites (and not all certificates issued by the same CA)

The section 'Extended Authentication Protocol (XAUTH)' > Page 17 provides more information about how to configure the Extended Authentication Protocol XAUTH in the VPN gateway.

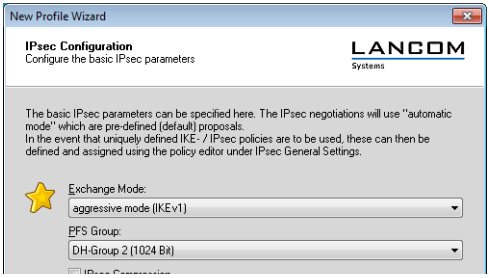
In section 'Set up LANCOM Advanced VPN Client for certificate connections' > Page 15 you will find more information about certificate based login to VPN gateways.

5 In the next window, the settings for connection establishment and encryption will be requested.

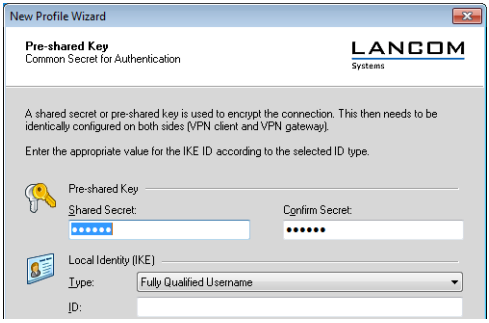
- Select the option **Aggressive Mode** as the Exchange Mode if you want to use pre-shared keys exclusively for authentication.
- Select the option **Main Mode** if you want to use digital certificates for connection authentication. In this case, after finishing the Profile

Wizard, you must manually set the profile to use certificates ('Set up LANCOM Advanced VPN Client for certificate connections' > Page 15).

The default settings for the PFS group (**DH group 2 (1024 Bit)**) can be retained.



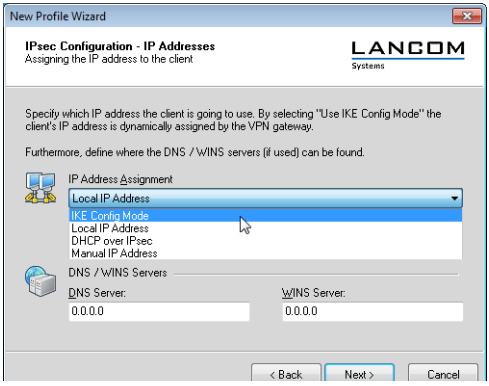
6 In the dialog that follows, enter the "pre-shared key" in the field **Shared Secret**. Select the "Local identity" type as **Fully Qualified Username**. In the field "ID" enter the e-mail address that the client will use for authentication at the VPN gateway.



Note that the "Pre-shared key" and the e-mail entries must agree exactly with those entered in the Setup Wizard for LANconfig when the RAS access was set up at the VPN gateway.

7 In the following window, the IP address intended for the client is requested. If you want to enter a fixed IP address for dial-up access you can choose between **Local IP Address** or **Manual IP Address**. Another possibility is to enter a pool of IP addresses in the LANCOM VPN gateway, one of which can be assigned dynamically to the VPN client (IKE Config Mode). If you select the option **Use IKE Config Mode** IP addresses and DNS servers are assigned via the IKE Config Mode protocol. Instead of

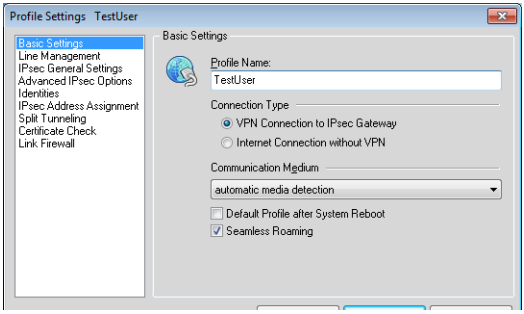
using the IKE Config Mode, you can use alternatively a DHCP Server connected to the gateway. By this way the client receives an IP address over the VPN tunnel after the DHCP negotiation.



8 The final window of the profile configuration is for entering the network addresses and netmasks that the client should have access to. Different portions of the network or subnets can be defined here. Conclude the configuration by clicking on **Finish**.

A connection can now be established to the company network that has been defined. To do this, access the main window of LANCOM Advanced VPN Client and use **Profile** to select the connection profile you require; click on **Connect**. If all of the settings in the profile and in the VPN gateway have been entered correctly, a connection will be successfully established. The client computer now has access to all of the available resources in the LAN such as mail, file, and printer servers.

A profile can be altered later in the LANCOM Advanced VPN Client by selecting the menu entry **Configuration ▶ Profile Settings**, marking the relevant profile and clicking on **Configure**.

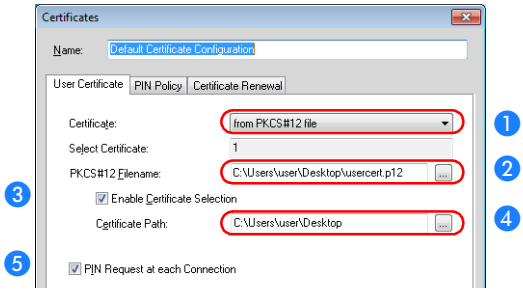


EN

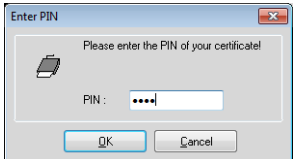
5 Set up LANCOM Advanced VPN Client for certificate connections

To use the LANCOM Advanced VPN Client to dial in to a LANCOM router, the appropriate profile settings must be adjusted to allow for the use of certificates.

1. Click on the menu item **Configuration** ▶ **Certificates** to open the settings for an existing certificate configuration or create a new certificate configuration with the **Add** button.

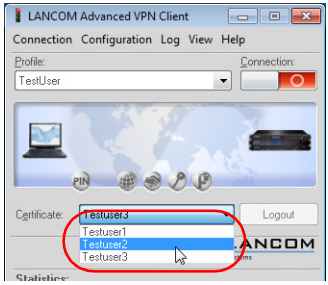


- Select the certificate type 'from PKCS#12 file' 1 and set the required certificate file 2.
- To work with different certificates, activate the option 'Soft Certificate Selection' 3 and enter the path for the folder where the certificate files are stored 4.
- Define whether or not the PIN (password) for the certificate should be entered before each connection establishment 5. Alternatively, you can save the PIN in the LANCOM Advanced VPN Client under the menu item **Connection** ▶ **Enter PIN** .

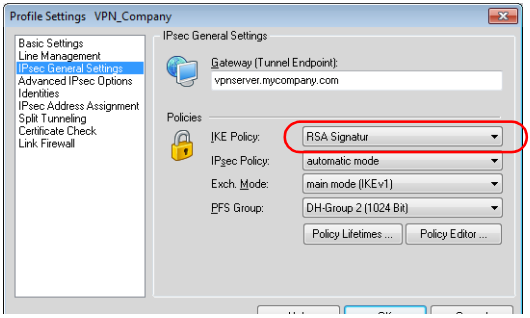


- If Soft Certificate Selection is activated, the certificate corresponding to the connection can be chosen from a list displayed in the main

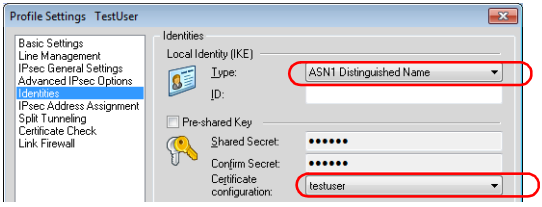
window of the LANCOM Advanced VPN Client, as befits the selected profile.



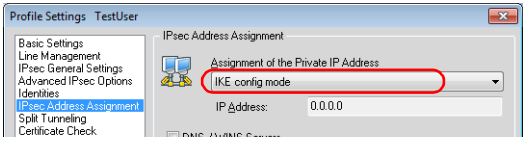
2. In the IPSec General Settings for the profile, change the IKE policy to 'RSA signature'.



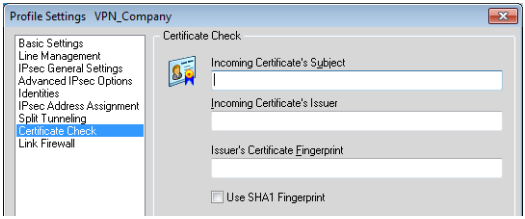
3. Switch the identity to 'ASN1 Distinguished Names'. The ID can remain blank since this information is taken from the certificate. Disable the **Pre-shared Key** option and select the previously defined certificate configuration.



4 For the IP address assignment use the 'IKE Config Mode'.



5 For the certificate check you can optionally place a limitation on the certificates accepted by the LANCOM Advanced VPN Client. To do this, you define the user and/or the issuer of the incoming certificate and, if applicable, the associated "fingerprint".



6 Extended Authentication Protocol (XAUTH)

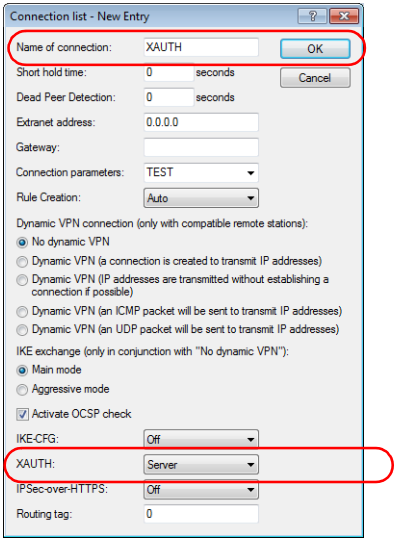
RADIUS servers are often used to authenticate users for remote sites dialing-in over WAN connections (such as via PPP). Over time, conventional WAN connections increasingly gave way to secure (encrypted) and more cost-effective VPN connections. However, the structure of VPN connections over IPSec with IKE does not permit unidirectional authentication of users by RADIUS or similar technologies.

The Extended Authentication Protocol (XAUTH) provides the ability to extend authentication with XAUTH user name and XAUTH password. The authentication is cheched in LCOS with the internal user table (PPP list).

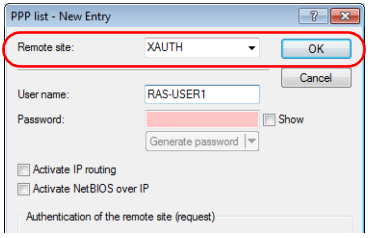
In order make XAUTH particularly secure, dial-in via RSA-SIG (certificates) was to be used instead of the preshared key method (PSK) whenever possible. Here it is important to ensure that the VPN gateway accepts only the certificate of the correct remote site (and not all certificates issued by the same CA).

The application of the XAUTH protocol is set up separately for each VPN remote site. Only the XAUTH operating mode is specified.

LANconfig: VPN ▶ General ▶ Connection list



Additionally a new entry in the PPP list has to be created, where the name of th repote site matches the name of the VPN connection (LANconfig: Communication ▶ Protocols ▶ PPP list). The user password and further options for routed protocols are stored in the this entry.



The user name from the PPP list entry is **not** used for authentication in this case.