Addendum LCOS 8.62 RU1

LCOS
[LANCOM OPERATING SYSTEM]

LANCOM
Systems

Inhalt

1 Addendum zur LCOS-Version 8.62 RU1

Dieses Dokument beschreibt die Änderungen und Ergänzungen in der LCOS-Version 8.62 gegenüber der vorherigen Version.

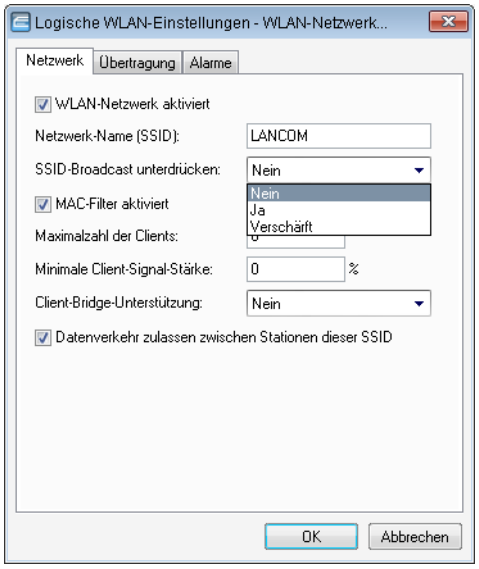
1.1 Wireless LAN – WLAN

1.1.1 Closed-Network-Funktion: SSID-Broadcast unterdrücken

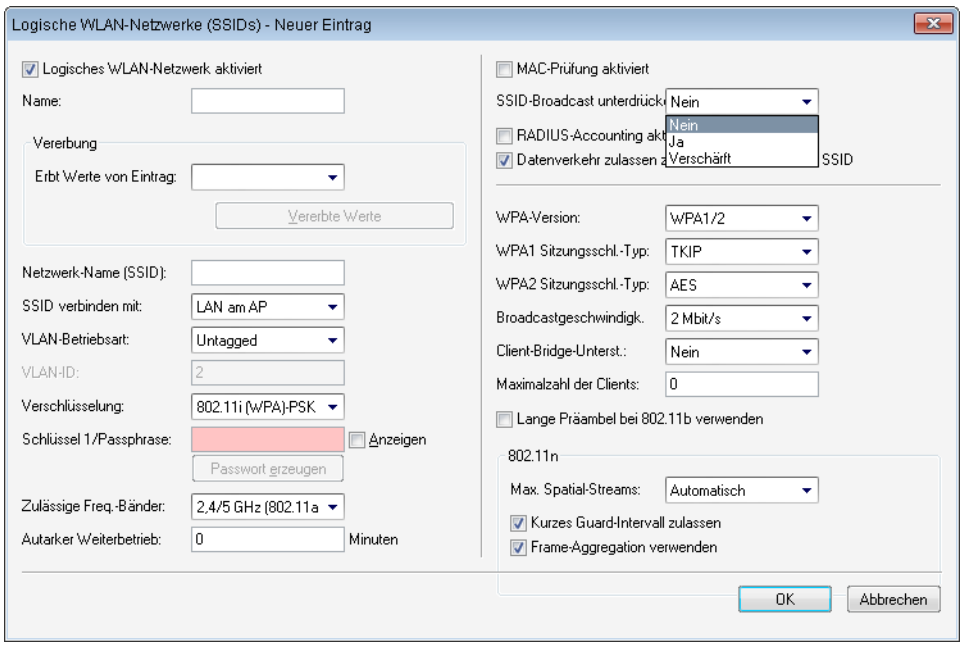
Nur mit der Kenntnis des Service Set Identifiers (SSID) kann sich ein WLAN-Client mit dem entsprechenden Funknetzwerk verbinden. In der Grundeinstellung erlauben viele drahtlose Netzwerke die Anmeldung mit der SSID "any" bzw. einer leeren SSID und ermöglichen so einem potenziellen Eindringling, das WLAN zu benutzen, ohne dessen SSID zu kennen. Die Closed-Network-Funktion verhindert, dass unbefugte WLAN-Clients sich am WLAN anmelden können. Der Access-Point verweigert dabei jeden Anmeldeversuch mit der SSID "any" bzw. einer leeren SSID. Jeder Benutzer muss die verwendete SSID genau kennen, um sich am WLAN anmelden zu können.

Das einfache Unterdrücken der SSID bietet keinen ausreichenden Zugriffsschutz, da der Access-Point diese bei der Anmeldung berechtigter WLAN-Clients im Klartext überträgt und sie somit für alle im WLAN-Netz befindlichen WLAN-Clients kurzfristig sichtbar ist.

LANconfig: Wireless-LAN > **Allgemein** > **Interfaces** > **Logische WLAN-Einstellungen** > **Netzwerk** .



LANconfig: WLAN-Controller > Profile > Logische WLAN-Netzwerke (SSIDs)



Die Option **SSID-Broadcast unterdrücken** ermöglicht folgende Einstellungen:

- **Nein**: Der Access-Point veröffentlicht die SSID der Funkzelle. Sendet ein Client einen Probe-Request mit leerer oder falscher SSID, antwortet das Gerät mit der SSID der Funkzelle (öffentlich sichtbares WLAN).
- **Ja**: Der Access-Point veröffentlicht die SSID der Funkzelle nicht. Sendet ein Client einen Probe-Request mit leerer SSID, antwortet das Gerät ebenfalls mit einer leeren SSID. Der Client kann sich nicht an der Funkzelle anmelden.
- **Verschärft**: Der Access-Point veröffentlicht die SSID der Funkzelle nicht. Sendet ein Client einen Probe-Request mit leerer oder falscher SSID, antwortet das Gerät überhaupt nicht. Der Client kann sich nicht an der Funkzelle anmelden. Diese Einstellung reduziert zusätzlich die Netzlast, wenn sich in der Funkzelle viele WLAN-Clients befinden.

Ergänzungen im Menüsystem

Closed-Network (nur bei Standalone-Access-Points)

Sie können Ihr Funk-LAN entweder in einem öffentlichen oder in einem privaten Modus betreiben. Ein Funk-LAN im öffentlichen Modus kann von Mobilstationen in der Umgebung ohne weiteres kontaktiert werden. Durch Aktivieren der Closed-Network-Funktion versetzen Sie Ihr Funk-LAN in einen privaten Modus. In dieser Betriebsart sind Mobilstationen ohne Kenntnis des Netzwerknamens (SSID) von der Teilnahme am Funk-LAN ausgeschlossen.

Schalten Sie den "Closed-Network-Modus" ein, wenn Sie verhindern möchten, dass sich WLAN-Clients mit der SSID "Any" oder einer leeren SSID in Ihrem Funknetzwerk anmelden.

Die Option **SSID-Broadcast unterdrücken** ermöglicht folgende Einstellungen:

- **Nein**: Der Access-Point veröffentlicht die SSID der Funkzelle. Sendet ein Client einen Probe-Request mit leerer oder falscher SSID, antwortet der Access-Point mit der SSID der Funkzelle (öffentliches WLAN).
- **Ja**: Der Access-Point veröffentlicht die SSID der Funkzelle nicht. Sendet ein Client einen Probe-Request mit leerer SSID, antwortet der Access-Point ebenfalls mit einer leeren SSID.
- **Verschärft**: Der Access-Point veröffentlicht die SSID der Funkzelle nicht. Sendet ein Client einen Probe-Request mit leerer oder falscher SSID, antwortet der Access-Point überhaupt nicht.

Das einfache Unterdrücken der SSID bietet keinen ausreichenden Zugriffsschutz, da der Access-Point diese bei der Anmeldung berechtigter WLAN-Clients im Klartext überträgt und sie somit für alle im WLAN-Netz befindlichen WLAN-Clients kurzfristig sichtbar ist.

SNMP-ID:

2.23.20.1.4

Pfad Telnet:

Pfad Telnet: Setup > **Schnittstellen** > **WLAN** > **Netzwerk**

Mögliche Werte:

Nein

Ja

Verschärft

Default:

Nein

SSID-Broadcast (nur bei WLAN-Controllern)

Sie können Ihr Funk-LAN entweder in einem öffentlichen oder in einem privaten Modus betreiben. Ein Funk-LAN im öffentlichen Modus kann von Mobilstationen in der Umgebung ohne weiteres kontaktiert werden. Durch Aktivieren der Closed-Network-Funktion versetzen Sie Ihr Funk-LAN in einen privaten Modus. In dieser Betriebsart sind Mobilstationen ohne Kenntnis des Netzwerknamens (SSID) von der Teilnahme am Funk-LAN ausgeschlossen.

Schalten Sie den "Closed-Network-Modus" im Access-Point ein, wenn Sie verhindern möchten, dass sich WLAN-Clients mit der SSID "Any" oder einer leeren SSID in Ihrem Funknetzwerk anmelden.

Die Option **SSID-Broadcast** ermöglicht folgende Einstellungen:

- **Ja**: Der Access-Point veröffentlicht die SSID der Funkzelle. Sendet ein Client einen Probe-Request mit leerer oder falscher SSID, antwortet der Access-Point mit der SSID der Funkzelle (öffentlich sichtbares WLAN).
- **Nein**: Der Access-Point veröffentlicht die SSID der Funkzelle nicht. Sendet ein Client einen Probe-Request mit leerer SSID, antwortet der Access-Point ebenfalls mit einer leeren SSID.
- **Verschärft**: Der Access-Point veröffentlicht die SSID der Funkzelle nicht. Sendet ein Client einen Probe-Request mit leerer oder falscher SSID, antwortet der Access-Point überhaupt nicht.

Das einfache Unterdrücken der SSID bietet keinen ausreichenden Zugriffsschutz, da der Access-Point diese bei der Anmeldung berechtigter WLAN-Clients im Klartext überträgt und sie somit für alle im WLAN-Netz befindlichen WLAN-Clients kurzfristig sichtbar ist.

Die Funktion "Closed-Network" finden Sie im Access-Point unter **Setup** > **Schnittstellen** > **WLAN** > **Netzwerk** . Beachten Sie: Wenn Sie im WLAN-Controller bei **SSID-Broadcast** die Option "Nein" auswählen (Gerät veröffentlicht die SSID nicht), setzt der Access-Point bei **Closed-Network** die Einstellung auf "Ja" und umgekehrt. Nur die Logik bei der Einstellung "Verschärft" ist in beiden Geräten identisch.

SNMP-ID:

2.37.1.1.19

Pfad Telnet:

Pfad Telnet: Setup > **WLAN-Management** > **AP-Konfiguration** > **Netzwerkprofile**

Mögliche Werte:

Nein

Ja

Verschärft

Default:

Ja

1.1.2 Neuer Parameter für die Signalstärke von WLAN-CLients

Die LCOS-Version 8.62 wertet nun optional die Signalstärken beim Einbuchen von WLAN-Clients aus.

Ergänzungen im Menüsystem

Minimal-Stations-Staerke

Mit diesem Eintrag bestimmen Sie den Schwellwert in Prozent für die minimale Signalstärke für Clients beim Einbuchen. Unterschreitet ein Client diesen Wert, sendet der Access-Point keine Probe-Responses mehr an diesen Client und verwirft die entsprechenden Anfragen.

Ein Client mit schlechter Signalstärke findet den Access-Point somit nicht und kann sich nicht darauf einbuchen. Das sorgt beim Client für eine optimierte Liste an verfügbaren Access-Points, da keine Access-Points aufgeführt werden, mit denen der Client an der aktuellen Position nur eine schwache Verbindung aufbauen könnte.

SNMP-ID:

2.23.20.1.16

Pfad Telnet:

Pfad Telnet: Setup > Schnittstellen > WLAN > Netzwerk

Mögliche Werte:

0-100

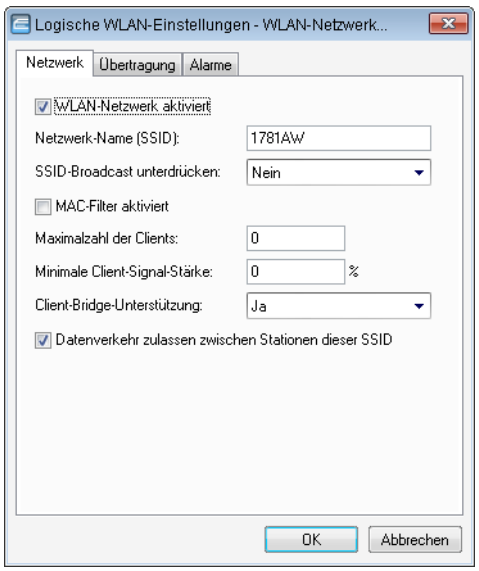
Default:

0

1.1.3 Ergänzungen in LANconfig

Netzwerkeinstellungen

LANconfig: Wireless-LAN > Allgemein > Logische WLAN-Einstellungen > Netzwerk



- **WLAN-Netzwerk aktiviert**

  Mit diesem Schalter aktivieren bzw. deaktivieren Sie das entsprechende logische WLAN.

- **Netzwerk-Name** (SSID)

  Bestimmen Sie für jedes benötigte logische Funknetzwerk eine eindeutige SSID (den Netzwerknamen). Nur solche Netzwerkkarten, die über die gleiche SSID verfügen, können sich in diesem Funknetzwerk anmelden.

- **SSID-Broadcast unterdrücken**

  Sie können Ihr Funk-LAN entweder in einem öffentlichen oder in einem privaten Modus betreiben. Ein Funk-LAN im öffentlichen Modus kann von Mobilstationen in der Umgebung ohne weiteres kontaktiert werden. Durch Aktivieren der Closed-Network-Funktion versetzen Sie Ihr Funk-LAN in einen privaten Modus. In dieser Betriebsart sind Mobilstationen ohne Kenntnis des Netzwerknamens (SSID) von der Teilnahme am Funk-LAN ausgeschlossen.

  Schalten Sie den "Closed-Network-Modus" ein, wenn Sie verhindern möchten, dass sich WLAN-Clients mit der SSID "Any" oder einer leeren SSID in Ihrem Funknetzwerk anmelden.

  Die Option **SSID-Broadcast unterdrücken** ermöglicht folgende Einstellungen:

  - **Nein**: Der Access-Point veröffentlicht die SSID der Funkzelle. Sendet ein Client einen Probe-Request mit leerer oder falscher SSID, antwortet der Access-Point mit der SSID der Funkzelle (öffentliches WLAN).
  - **Ja**: Der Access-Point veröffentlicht die SSID der Funkzelle nicht. Sendet ein Client einen Probe-Request mit leerer SSID, antwortet der Access-Point ebenfalls mit einer leeren SSID.
  - **Verschärft**: Der Access-Point veröffentlicht die SSID der Funkzelle nicht. Sendet ein Client einen Probe-Request mit leerer oder falscher SSID, antwortet der Access-Point überhaupt nicht.

  Das einfache Unterdrücken der SSID bietet keinen ausreichenden Zugriffsschutz, da der Access-Point diese bei der Anmeldung berechtigter WLAN-Clients im Klartext überträgt und sie somit für alle im WLAN-Netz befindlichen WLAN-Clients kurzfristig sichtbar ist.

- **MAC-Filter aktiviert**

  In der MAC-Filterliste (**Wireless-LAN** > **Stationen** > **Stationen**) sind die MAC-Adressen der Clients hinterlegt, die sich bei einem Access-Point einbuchen dürfen. Mit dem Schalter **MAC-Filter aktiviert** können Sie die Verwendung der MAC-Filterliste gezielt für einzelne logische Netzwerke ausschalten.

  Die Verwendung der MAC-Filterliste ist auf jeden Fall erforderlich für logische Netzwerke, in denen sich die Clients mit einer individuellen Passphrase über LEPS anmelden. Die bei LEPS verwendete Passphrase wird ebenfalls in der MAC-Filterliste eingetragen. Für die Anmeldung mit einer individuellen Passphrase beachtet der Access-Point daher immer die MAC-Filterliste, auch wenn Sie diese Option hier deaktivieren.

- **Maximale Client-Anzahl**

  Legen Sie hier die maximale Anzahl der Clients fest, die sich bei diesem Access-Point einbuchen dürfen. Weitere Clients, die sich über diese Anzahl hinaus anmelden wollen, lehnt der Access-Point ab.

- **Minimale Client-Signal-Stärke**

  Mit diesem Eintrag bestimmen Sie den Schwellwert in Prozent für die minimale Signalstärke für Clients beim Einbuchen. Unterschreitet ein Client diesen Wert, sendet der Access-Point keine Probe-Responses mehr an diesen Client und verwirft die entsprechenden Anfragen.

  Ein Client mit schlechter Signalstärke findet den Access-Point somit nicht und kann sich nicht darauf einbuchen. Das sorgt beim Client für eine optimierte Liste an verfügbaren Access-Points, da keine Access-Points aufgeführt werden, mit denen der Client an der aktuellen Position nur eine schwache Verbindung aufbauen könnte.

- **Client-Bridge-Unterstützung**

  Aktivieren Sie diese Option für einen Access-Point, wenn Sie im WLAN-Client-Modus für eine Client-Station die Client-Bridge-Unterstützung aktiviert haben.

  Sie können den Client-Bridge-Modus ausschließlich zwischen zwei LANCOM-Geräten verwenden.

- **Datenverkehr zulassen zwischen Stationen dieser SSID**

Aktivieren Sie diese Option, wenn alle Stationen, die an dieser SSID angemeldet sind, untereinander kommunizieren dürfen.

1.2 Public-Spot

1.2.1 Erweiterungen beim Public-Spot

In der LCOS-Version 8.62 können Sie nun bei der Registrierung neuer Public-Spot-Benutzer festlegen, ob sie diesem Benutzer erlauben möchten, sich mehrfach mit einem Benutzer-Account anmelden zu können (Mehrfach-Login).

Die Erweiterung betrifft sowohl den Assistenten "Public-Spot-Benutzer einrichten" als auch die Einrichtung neuer Public-Spot-Benutzer über das Web-API.

Statt des Voucher-Drucks können Sie sich bei der Registrierung neuer Public-Spot-Benutzer über den Assistenten nun auch eine CSV-Datei ausgeben lassen.

Verwaltung von Public-Spot-Nutzern über das Web-API

Über die Eingabe einer speziellen URL in der Adresszeile haben Sie die Möglichkeit, Public-Spot-Benutzer direkt statt über den Setup-Assistenten anzuzeigen, neu anzulegen oder zu löschen.

Hinzufügen eines Public-Spot-Benutzers

Über die folgende URL registrieren Sie einen neuen Public-Spot-Benutzer:

```
http://<Geräte-URL>/cmdpbspotuser/
   ?action=addpbspotuser&parameter1=value1&parameter2=value2&...
```

Ihnen stehen folgende Parameter zur Verfügung:

`comment`

Kommentar zum registrierten Benutzer

Sind für einen Public-Spot-Benutzer mehrere Kommentare möglich, geben Sie die Kommentare und die entsprechenden Kommentarfeld-Namen wie folgt an:

```
&comment=<Inhalt1>:<Feldname1>;<Inhalt2>:<Feldname1>;
   ...;<Inhalt5>:<Feldname5>
```

Existiert ausschließlich ein Kommentarfeld pro Benutzer, genügt die Angabe des Kommentars:

```
&comment=<Kommentar>
```

Deutsche Umlaute werden nicht unterstützt.

Die maximale Zeichenanzahl des Kommentar-Parameters beträgt 191 Zeichen.

`print`

Automatischer Ausdruck des Vouchers.

Fehlt dieser Parameter, zeigt der Assistent anschließend eine entsprechende Schaltfläche, über die Sie den Voucher ausdrucken können.

`printcomment`

Kommentar auf den Voucher drucken.

Fehlt dieser Parameter, erscheint der Kommentar nicht auf dem Voucher (Default-Einstellung).

`nbguests`

Anzahl der anzulegenden Public-Spot-Benutzer.

Fehlt dieser Parameter, legt der Assistent ausschließlich einen Benutzer an (Default-Einstellung).

`defaults`

Default-Werte verwenden

Der Assistent ersetzt fehlende oder falsche Parameter durch Default-Werte.

`expiretype`

Kombinierte Angabe von Ablauf-Typ und Verfalls-Dauer des Vouchers.

Geben Sie diesen Parameter wie folgt an:

```
&expiretype=<Wert1>+validper=<Wert2>
```

Die Parameter-Werte haben folgende Bedeutung:

- `Wert1`: Ablauf-Typ (absolut, relativ, absolute und relativ, none)
- `Wert2`: Verfallsdauer des Vouchers

Fehlt dieser Parameter oder geben Sie falsche Werte ein, setzt der Assistent die Default-Werte ein.

`ssid`

Netzwerk-Name

Fehlt dieser Parameter, verwendet der Assistent den Standard-Netzwerk-Namen (Default-Einstellung).

`unit`

Zugangsdauer

Geben Sie diesen Parameter wie folgt an:

```
&unit=<Wert1>+runtime=<Wert2>
```

Die Parameter-Werte haben folgende Bedeutung:

- `Wert1`: Einheit der Laufzeit. Mögliche Werte sind: Minute, Stunde, Tag
- `Wert2`: Laufzeit

`timebudget`

Zeit-Budget

Fehlt dieser Parameter, verwendet der Assistent den Default-Wert.

`volumebudget`

Volumen-Budget

Fehlt dieser Parameter, verwendet der Assistent den Default-Wert.

`multilogin`

Mehrfach-Login

Wenn Sie diesen Parameter angeben, kann sich der Benutzer mehrfach mit seinem Benutzer-Account anmelden. Fehlt dieser Parameter, ist der Mehrfach-Login defaultmäßig deaktiviert.

Sind für fehlende Parameter in der Public-Spot-Verwaltung keine Default-Werte angegeben, öffnet Ihnen der Assistent einen entsprechenden Dialog. Tragen Sie in diesen die fehlenden Werte ein.

Public-Spot-Benutzer-Verwaltung

Die Setup-Wizards unterstützen Sie auch bei der einfachen Verwaltung von Public-Spot-Benutzern.

Neue Public-Spot-Benutzer mit einem Klick hinzufügen

Registrieren Sie neue Public-Spot-Benutzer über WEBconfig mit dem Setup-Wizard **Public-Spot-Benutzer einrichten.**. Der Wizard ist mit Standard-Werten voreingestellt, so dass Sie mit einem Klick auf **Speichern & Drucken** einen neuen Benutzer einrichten. Bei einem Klick auf **Speichern & CSV-Export** stellt Ihnen der Assistent die Voucherdaten als CSV-Datei zum Download zur Verfügung.

Die folgenden Einstellungen sind nach Bedarf konfigurierbar:

- **Startzeitpunkt des Zugangs:** Legt fest, ab wann der Voucher gültig ist. Mögliche Werte sind:
  - **erster Login (Default)**: Zugang gilt ab Erstanmeldung des Benutzers
  - **sofort:** Zugang gilt ab Anlegen des Benutzers
- **Gültigkeitsdauer des Vouchers:** Geben Sie die Dauer an, nach der der Voucher ungültig wird.

  Es ist unmöglich eine Gültigkeitsdauer einzutragen, wenn der Zugang ab sofort gültig ist.
- **Dauer des Zugangs:** Wählen Sie die Dauer aus, für die dieser Zugang ab Registrierung oder Erstanmeldung gültig ist.
- **SSID (Netzwerkname):** Wählen Sie aus, für welches WLAN-Netz der Zugang gilt. Der Standard-Netzwerkname ist bereits markiert. Die hier aufgelisteten SSIDs verwalten Sie in der SSID-Tabelle.

  Drücken Sie die "Strg"-Taste, um mehrere Einträge auszuwählen.
- **Anzahl Voucher:** Geben Sie an, wie viele Vouchers Sie gleichzeitig erstellen möchten (Default: 1).
- **Zeit-Budget (Minuten):** Geben Sie an, nach welcher Online-Zeit der Public-Spot-Zugang schließt.

  Je nach gewählter Ablauf-Methode bestimmt entweder dieses Zeit-Budget (inkrementell) oder die eingestellte Voucher-Zugangsdauer (absolut) die Frist für den Zugang.
- **Volumen-Budget (MByte):** Geben Sie an, nach welcher übertragenen Datenmenge der Zugang schließt.
- **Kommentar (optional):** Fügen Sie einen Kommentar ein.
- **Drucke Kommentar auf Voucher:** Aktivieren Sie diese Option, damit der Kommentar auf dem Voucher erscheint.
- **Drucken:** Aktivieren Sie diese Option, damit Sie beim Speichern gleichzeitig die registrierten Vouchers ausdrucken (Default: an).

  Wenn Sie diese Option deaktiviert haben, zeigt Ihnen der Assistent nach der Registrierung eine Übersicht der neuen Public-Spot-Benutzer. Sie erhalten dann noch einmal die Gelegenheit, die Vouchers auszudrucken.
- **Mehrfach-Logins:** Aktivieren Sie diese Option, damit sich ein Benutzer mehrfach mit seinem Benutzer-Account am Public-Spot anmelden kann (Default: aus).

Konfigurieren Sie die Default-Werte für die Einrichtung neuer Public-Spot-Zugänge in folgenden Menüs:

- LANconfig: **Public-Spot** > **Public-Spot Assistent**
- WEBconfig: **LCOS-Menübaum** > **Setup** > **Public-Spot-Modul** > **Neuer-Benutzer-Assistent**

1.3 Voice over IP - VoIP

1.3.1 Default-Wert für die WAN-Anmeldung eines SIP-Benutzers

Der Default-Wert für die WAN-Anmeldung eines SIP-Benutzers hat sich geändert von 'Ja' zu 'Nein'.

Ergänzungen im Menüsystem

Zugriff von WAN

Bestimmen Sie hier, ob und wie sich SIP-Clients über eine WAN-Verbindung mit dem entsprechenden Benutzerdaten anmelden können.

SNMP-ID:

2.33.3.1.1.8

Pfad Telnet:

Setup > **Voice-Call-Manager** > **User** > **SIP-User** > **User**

Mögliche Werte:

ja

nein

VPN

Default:

Nein

1.4 Virtual Private Networks - VPN

1.4.1 Default-Proposals für IKE und IPSec

Die Proposals für IKE und IPSec unterstützen nun in den Default-Einstellungen eine Schlüssellänge von 256 Bit.

Ein Firmware-Upgrade aktiviert diese Änderung zunächst nicht, um bestehende Installationen nicht zu gefährden. Um die Änderungen zu übernehmen, müssen Sie einen Reset des Gerätes oder einen Reset der Tabellen durchführen. Bei Neugeräten, die LCOS 8.62 oder neuer enthalten, sind die neuen Defaults bereits aktiv.

1.4.2 myVPN

Mit der LANCOM myVPN App können Sie sehr komfortabel einen VPN-Zugang zu Ihrem Firmennetzwerk auf Ihrem iPhone, iPad oder iPod (allgemein: iOS-Gerät) einrichten. LANCOM myVPN bietet die folgenden Funktionen:

- Hochsichere, mobile VPN-Verbindungen
- Übernimmt die komplexe VPN-Konfiguration des in iOS-Geräten integrierten VPN-Clients und des LANCOM Routers
- PIN-Verfahren zur Authentisierung beim VPN-Tunnelaufbau
- Zugriffskontrolle durch einstellbare Firewall-Regeln auf den LANCOM VPN-Gateways
- LANCOM myVPN-Benutzermanagement und automatische Erkennung myVPN-aktivierter LANCOM Gateways
- Für iOS-Geräte ab Version 4.1 geeignet

Nach der Installation von LANCOM myVPN bezieht die App ein VPN-Profil von Ihrem LANCOM VPN-Gerät und konfiguriert automatisch alle erforderlichen Einstellungen im iOS-Gerät. Anschließend können Sie über die betriebssystem-internen Funktionen des iOS mit wenigen Schritten einen VPN-Verbindung zum Firmennetzwerk aufbauen.

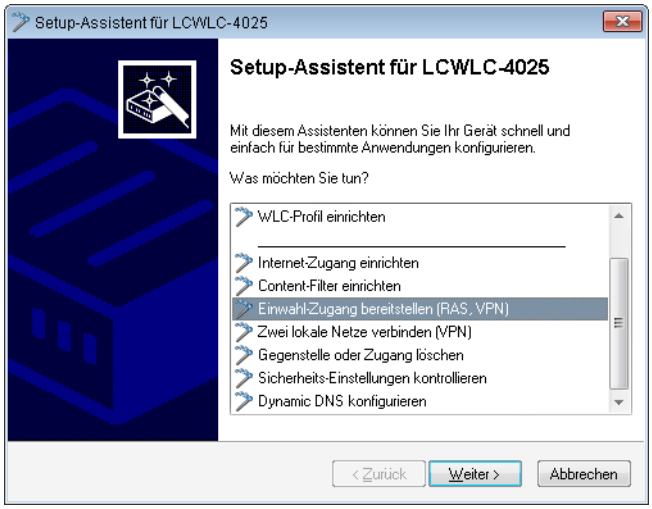
VPN-Profil für die LANCOM myVPN App mit dem Setup-Assistenten von LANconfig einrichten

So konfigurieren Sie mit dem Setup-Assistenten einen Zugang für einen VPN-Client auf einem iOS-Gerät:

1. Rufen Sie LANconfig z. B. aus der Windows-Startleiste auf mit **Start** > **Programme** > **LANCOM** > **LANconfig** .

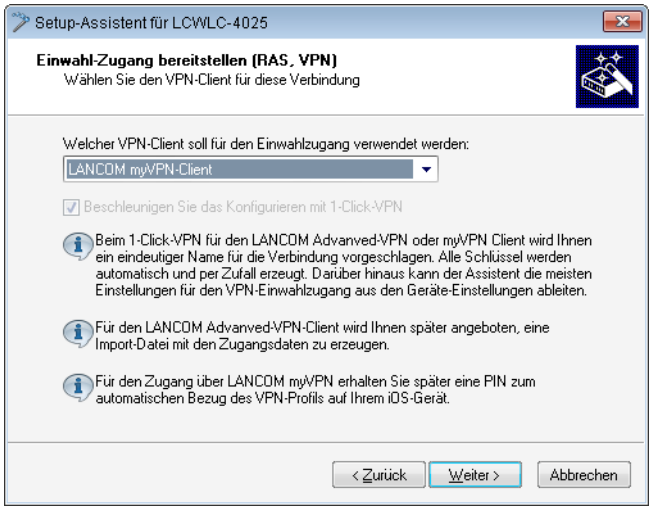
LANconfig sucht nun automatisch im lokalen Netz nach Geräten.

2. Markieren Sie das gewünschte Gerät im Auswahlfenster von LANconfig und wählen Sie die Schaltfläche **Setup Assistent** oder aus der Menüleiste den Punkt **Extras** > **Setup Assistent** .
3. Wählen Sie den Punkt **Einwahl-Zugang bereitstellen (RAS, VPN)** und klicken Sie auf **Weiter**.

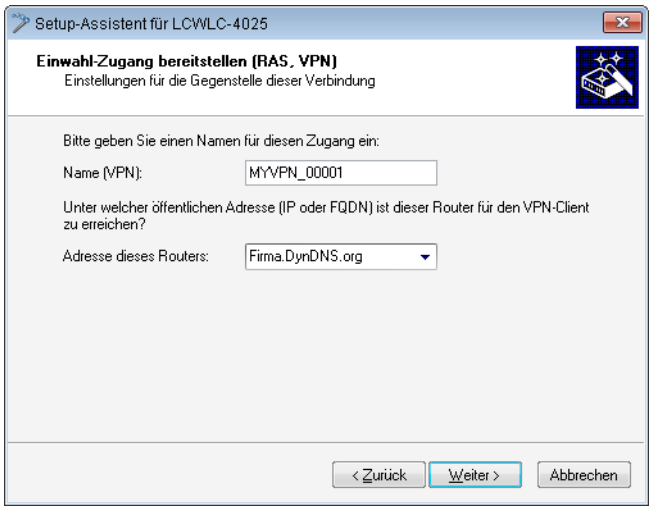


Sie können das nächste Informations-Fenster mit **Weiter** überspringen.

4. Wählen Sie aus der Auswahlliste die Option **LANCOM myVPN-Client** und klicken Sie auf **Weiter**.

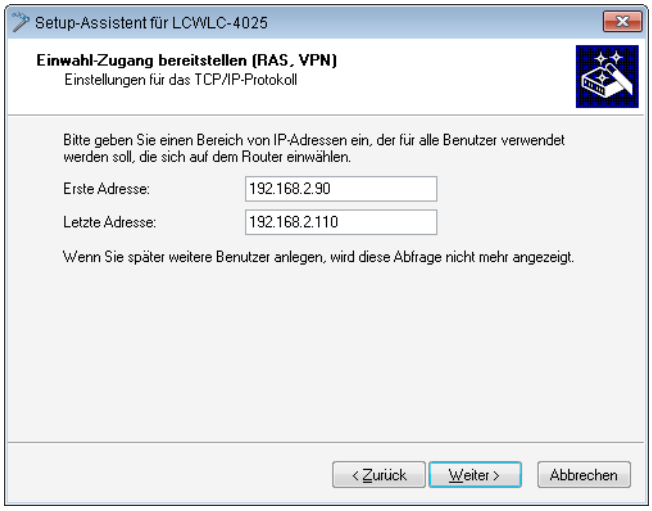


5. Vergeben Sie einen Namen für diesen Zugang und bestimmen Sie die Adresse, über die der Router für den VPN-Client auf dem iOS-Gerät zu erreichen ist. Klicken Sie anschließend auf **Weiter**.



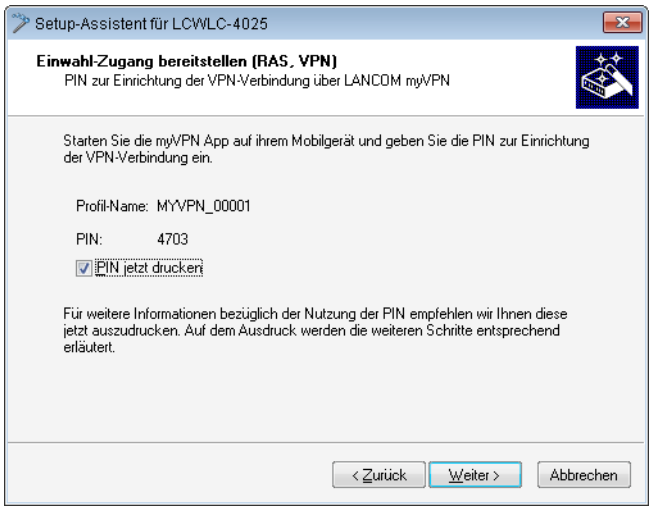
Der Setup-Assistent schlägt Ihnen einen Namen vor, den Sie übernehmen können.

6. Wenn in dem VPN-Gerät bisher noch kein Pool für die Zuweisung von IP-Adressen für die einwählenden VPN-Clients konfiguriert wurde, fordert Sie der Assistent im folgenden Dialog auf, einmalig einen Bereich von IP-Adressen als Pool anzugeben. Bei der Einwahl weist das VPN-Gerät dem iOS-Gerät dann automatisch eine freie IP-Aresse aus diesem Pool zu.



Wenn in dem VPN-Gerät zuvor schon ein Pool für die Zuweisung von IP-Adressen für die einwählenden VPN-Clients konfiguriert wurde, so nutzt das VPN-Gerät automatisch die Adressen aus diesem Adress-Pool, der Assistent überspringt den hier abgebildeten Dialog.

7. Der Setup-Assistent zeigt Ihnen den Profil-Namen sowie die automatisch generierte PIN für den VPN-Client an. Wenn Sie die PIN zum Abschluss ausdrucken möchten, markieren Sie die Option **PIN jetzt drucken**. Klicken Sie auf **Weiter**.



8. Mit einem Klick auf **Fertig stellen** speichert der Setup-Assistent alle Einstellungen auf dem entsprechenden VPN-Gerät. Ggf. startet er anschließend den Ausdruck der myVPN-PIN.
   Das myVPN-Modul ist auf dem gewählten VPN-Gerät nun aktiviert. Sie können nun die myVPN-App auf Ihrem iOS-Gerät starten und mit Eingabe der PIN das VPN-Profil beziehen.

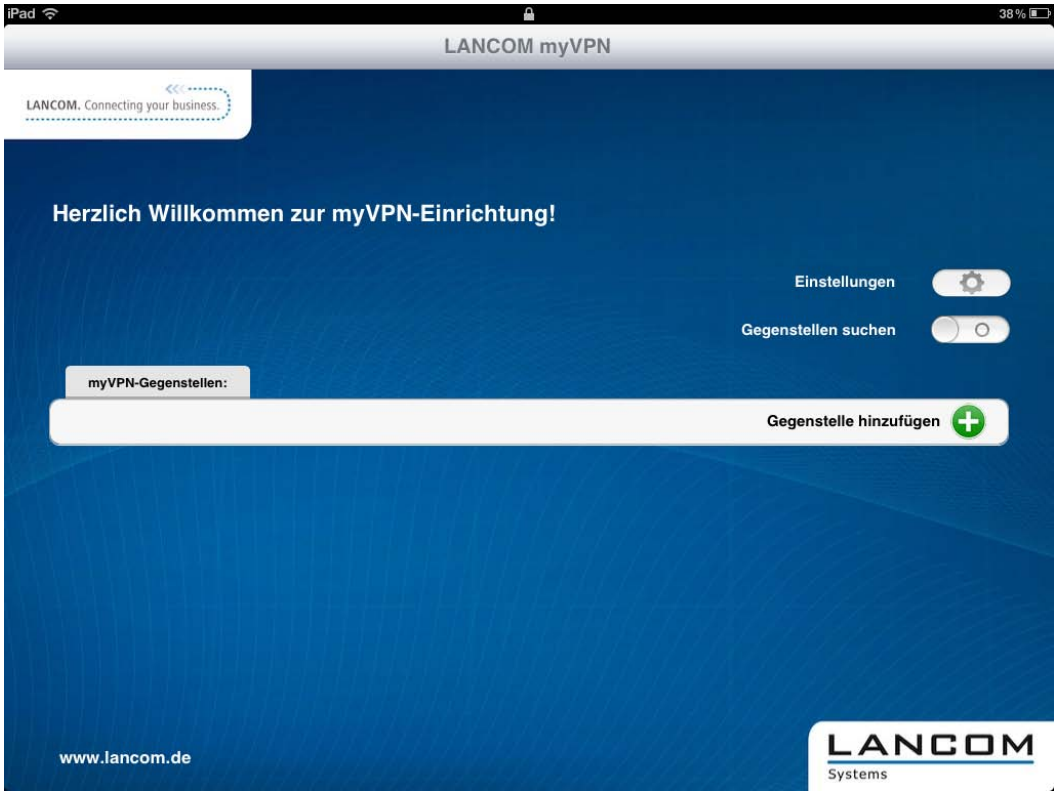
VPN-Profil mit der LANCOM myVPN App beziehen

So beziehen Sie auf Ihrem iOS-Gerät mit Hilfe der LANCOM myVPN App ein VPN-Profil von einem LANCOM VPN-Gerät:

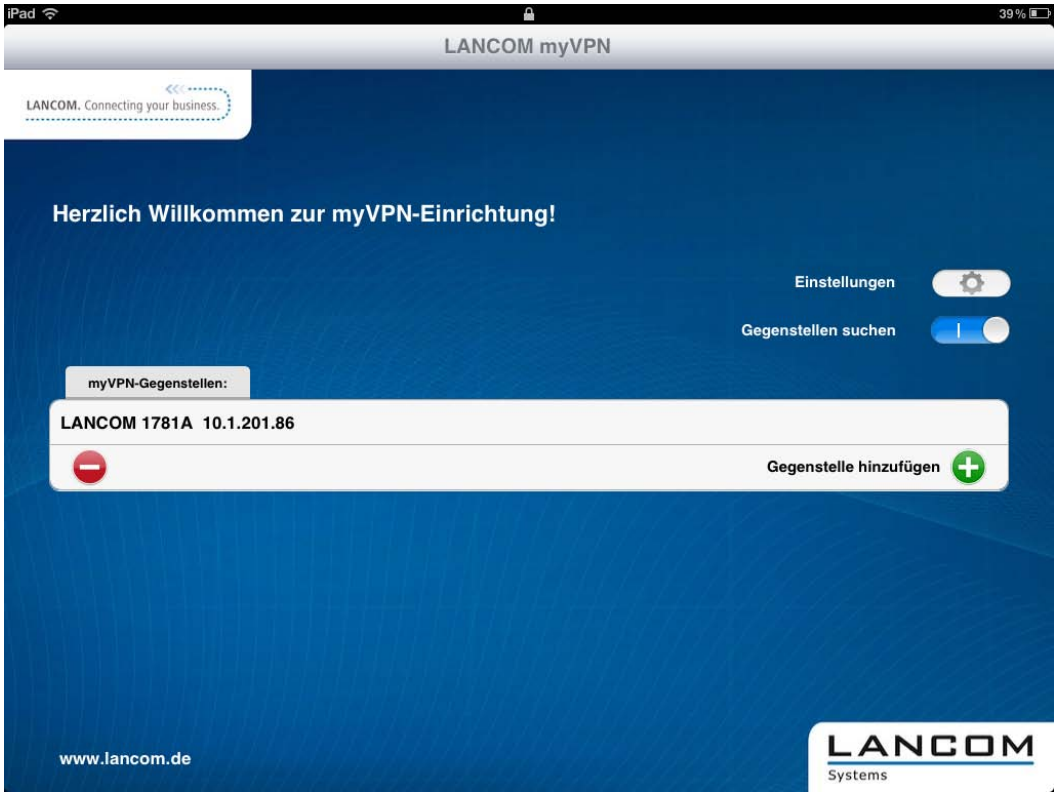
Die LANCOM myVPN App hat ausschließlich die Aufgabe, die korrekten Einstellungen für den im iOS-Gerät vorhandenen VPN-Client schnell und komfortabel einzurichten. Das Aufbau der VPN-Verbindung zum Firmennetzwerk selbst erfolgt direkt über den VPN-Client im iOS-Gerät.

1. Laden Sie die LANCOM myVPN App aus dem Apple-App-Store.

2. Öffnen Sie die App auf Ihrem iPhone oder iPad.

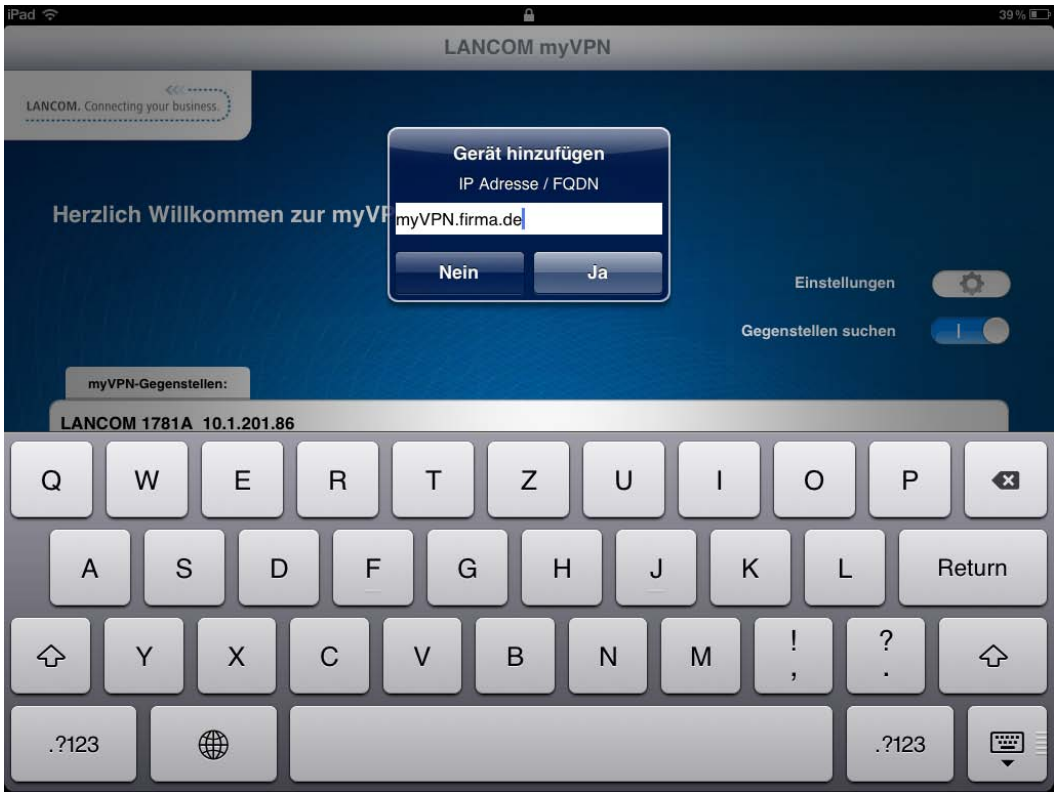


3. Optional: Aktivieren Sie die Option **Gegenstellen suchen**, um VPN-Geräte mit aktiviertem LANCOM myVPN Modul zu finden, welche das iOS-Gerät über WLAN erreichen kann.

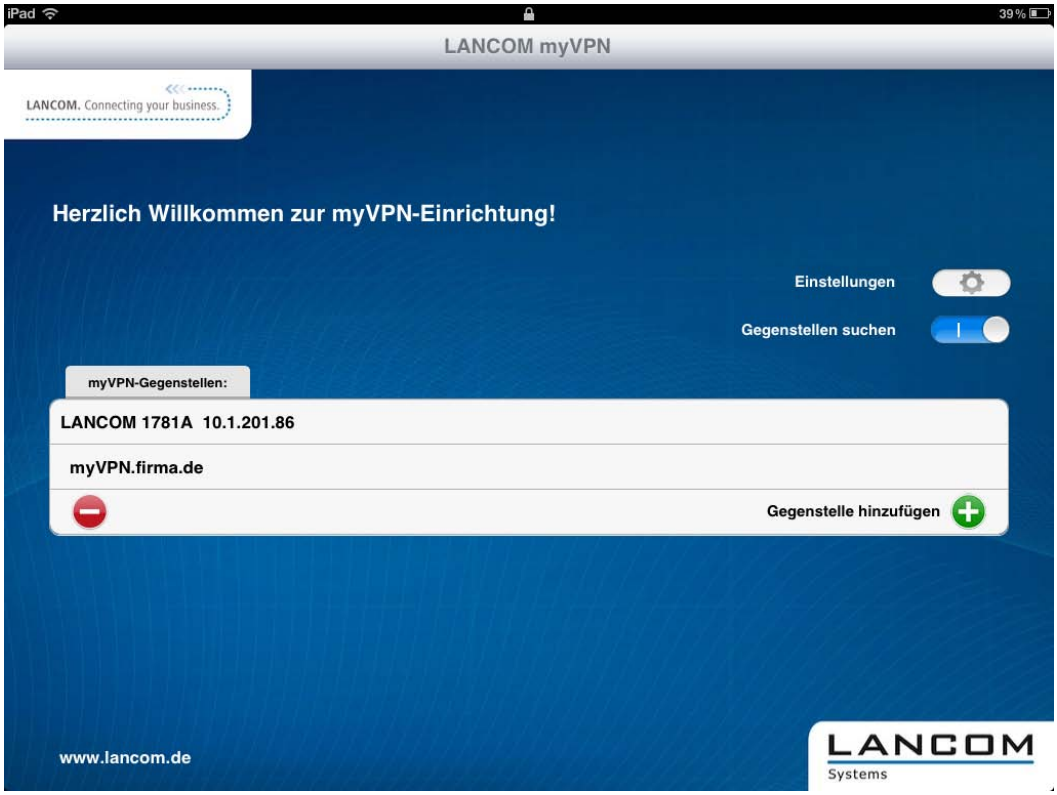


Das iOS-Gerät listet nun alle über WLAN erreichbaren VPN-Geräte mit aktiviertem LANCOM myVPN Modul auf. Ein Eintrag in dieser Liste bedeutet dabei nicht, dass Ihr iOS-Gerät von diesem VPN-Gerät auch ein LANCOM myVPN-Profil beziehen kann.

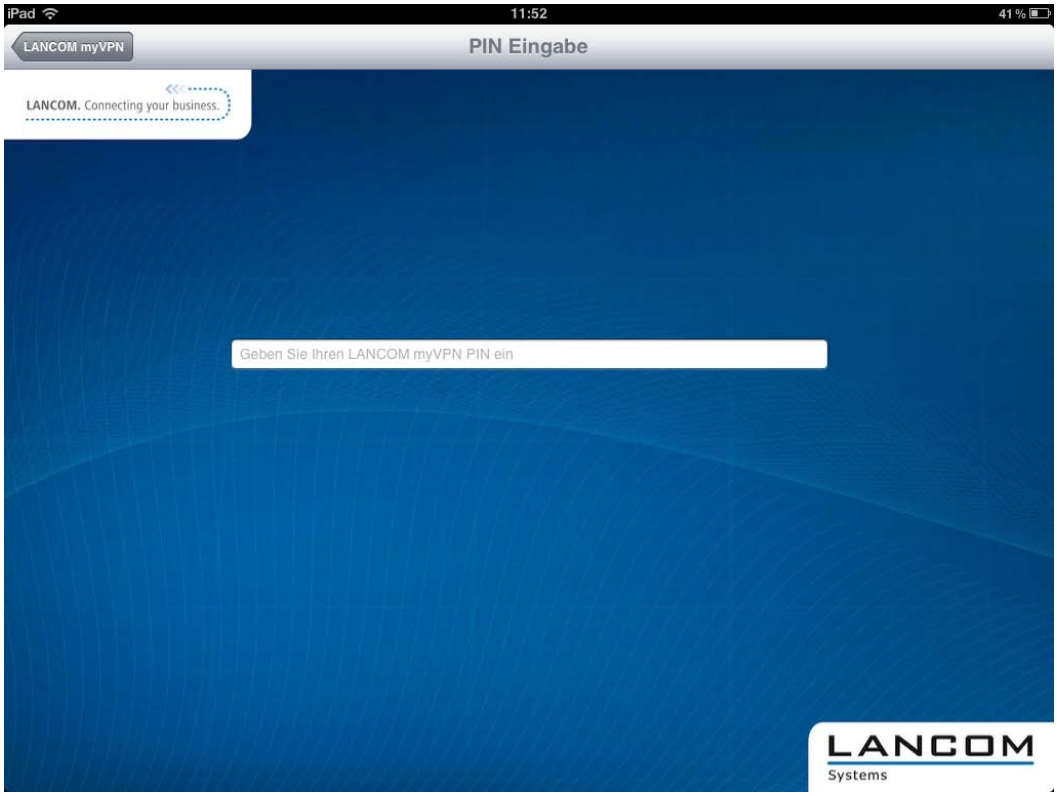
4. Optional: Wählen Sie die Option **Gerät manuell hinzufügen**, um die IP-Adresse oder den Namen von VPN-Geräten einzugeben, welche das iOS-Gerät über eine Internet-Verbindung (3G oder WLAN) erreichen kann. Geben Sie im folgenden Dialog die IP-Adresse oder den Namen des VPN-Gerätes ein und bestätigen Sie mit **Ja**.



5. Die App zeigt nun alle VPN-Geräte, welche Profile für die LANCOM myVPN App anbieten.



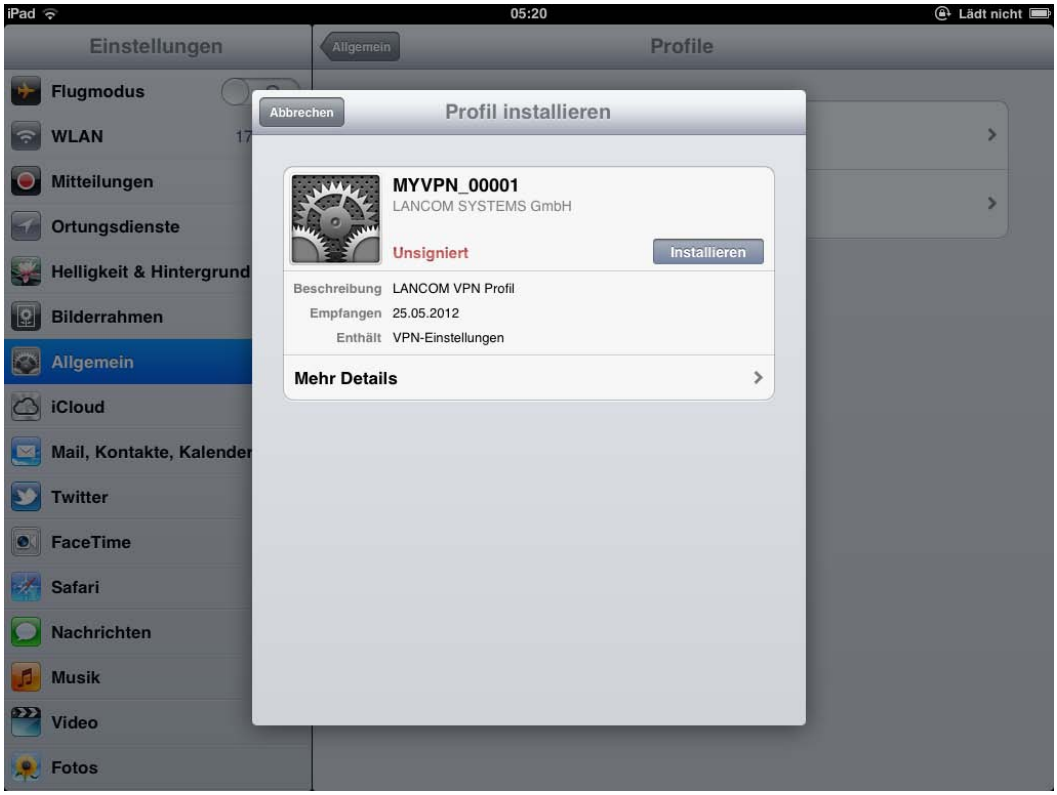
6. Wählen Sie durch Antippen das gewünschte VPN-Gerät aus der Liste aus und geben Sie im folgenden Dialog die PIN für den Bezug des VPN-Profils ein.



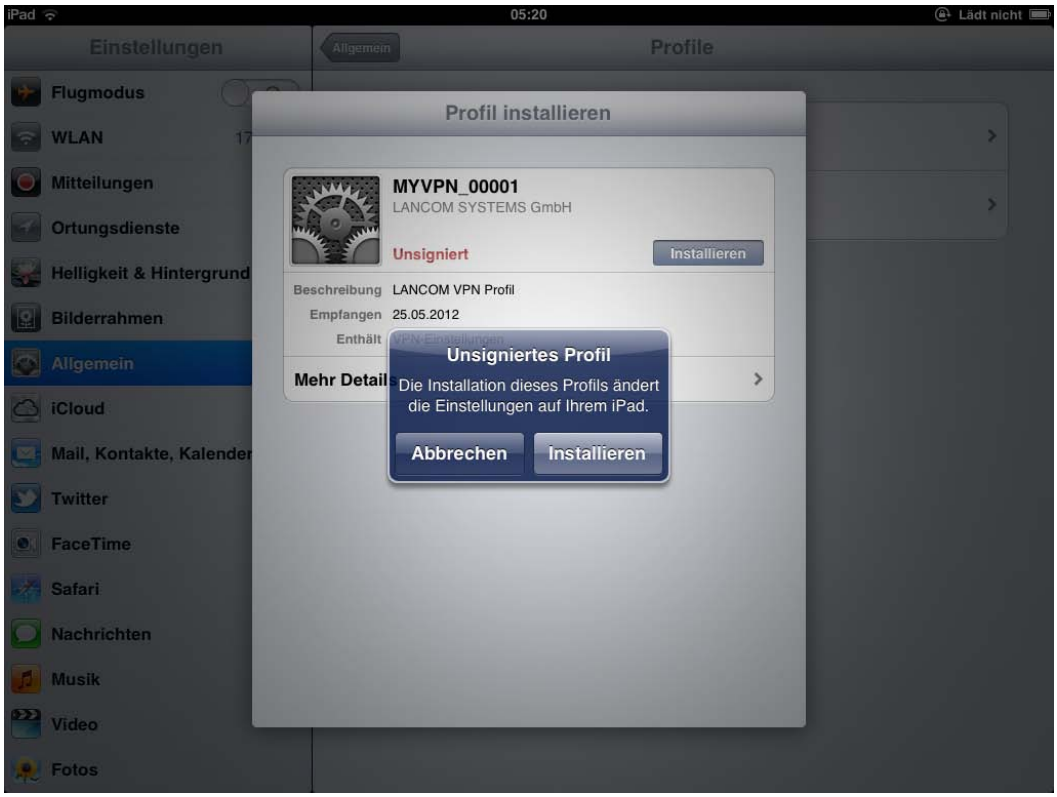
Wenn Sie die PIN 5 Mal falsch eingeben, wird das myVPN-Modul auf dem LANCOM VPN-Gerät komplett für eine bestimmte Zeit gesperrt. VPN-Verbindungen von iOS-Geräten mit zuvor erfolgreich eingerichteten VPN-Zugängen sind in diesem Zustand weiter möglich. Allerdings können iOS-Geräte von diesem VPN-Gerät für die Dauer der Sperrung keine neuen myVPN-Profile beziehen. Ein Administrator kann die Sperrung im myVPN-Modul wieder aufheben.

7. Bestätigen Sie im nächsten Dialog den Hinweis auf ein evtl. nicht signiertes Zertifikat mit der Schaltfläche **Ja**.

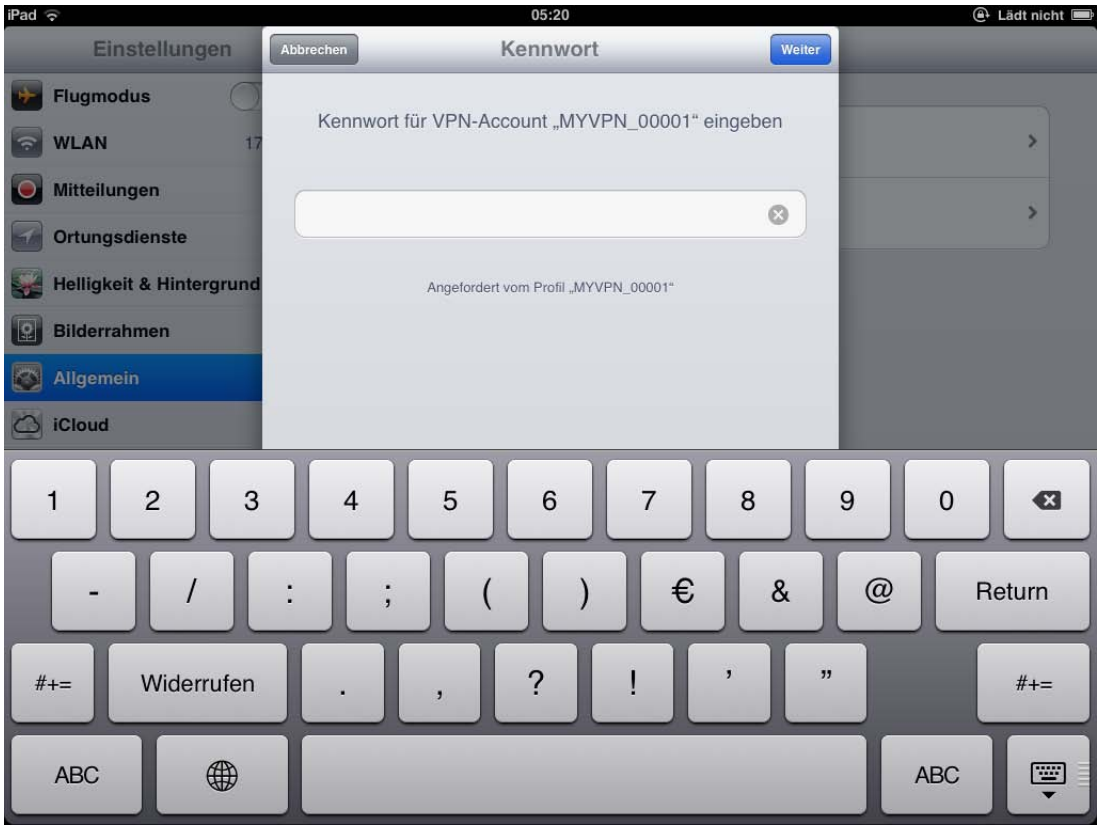
8. Bestätigen Sie im nächsten Dialog die Aufforderung zur Installation des Profils mit der Schaltfläche **Installieren**.



Bestätigen Sie auch die notwendigen Änderungen der Einstellungen auf Ihrem iOS-Gerät.

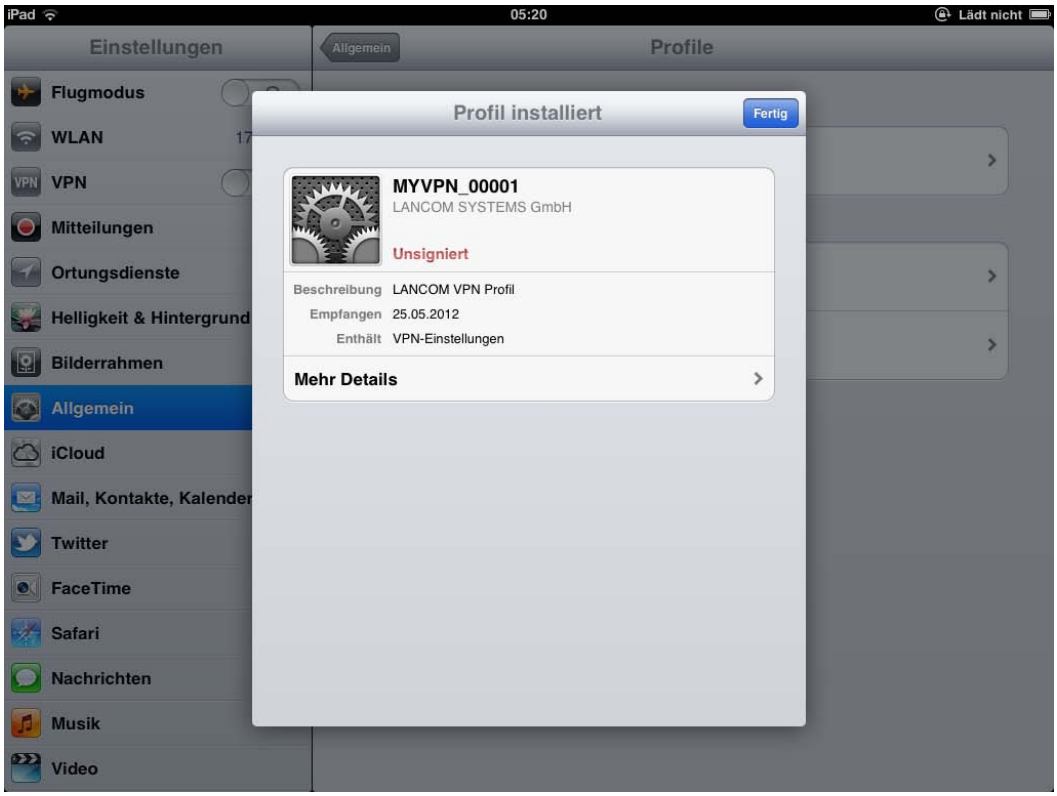


9. Die Installations-Routine fordert Sie im nächsten Schritt zur Eingabe des Kennworts für den VPN-Zugang auf. Das VPN-Kennwort entspricht standardmäßig der PIN für das myVPN-Profil. Wenn Sie das Kennwort für den VPN-Zugang hier eingeben, kann das iOS-Gerät anschließend ohne weitere Kennworteingabe eine VPN-Verbindung zu Ihrem Firmennetzwerk aufbauen. Lassen Sie das Feld für das VPN-Kennwort frei, damit das iOS-Gerät Sie bei jedem Verbindungsaufbau erneut zur Eingabe des VPN-Kennworts auffordert. Bestätigen Sie Ihre Auswahl mit der Schaltfläche **Weiter**.

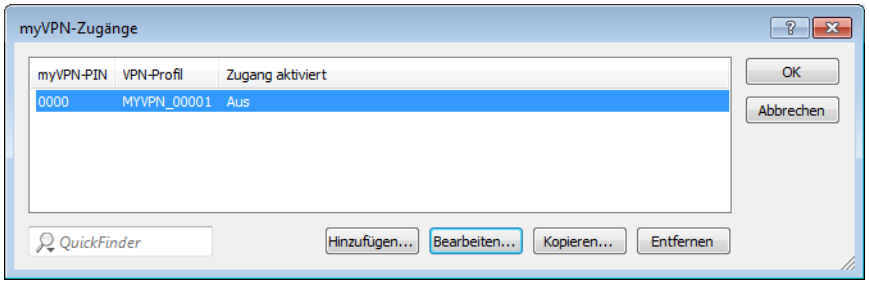


Wir empfehlen aus Sicherheitsgründen, das Kennwort für den VPN-Zugang **nicht** auf dem Gerät zu speichern, sondern sie bei jedem Verbindungsaufbau einzugeben.

10. Das VPN-Profil ist nun vollständig auf Ihrem iOS-Gerät installiert und bereit für den Aufbau einer VPN-Verbindung in Ihr Firmennetzwerk. Bestätigen Sie Ihre den Abschluss der Installation mit der Schaltfläche **Fertig**.



Sobald das myVPN-Profil von einem iOS-Gerät bezogen wurde, deaktiviert die Installationsroutine dieses myVPN-Profil auf dem LANCOM VPN-Gerät. Sie können diesen Zustand z.B. über LANconfig im Konfigurationsbereich **VPN** > **myVPN** in der Liste **myVPN-Zugänge** überprüfen:



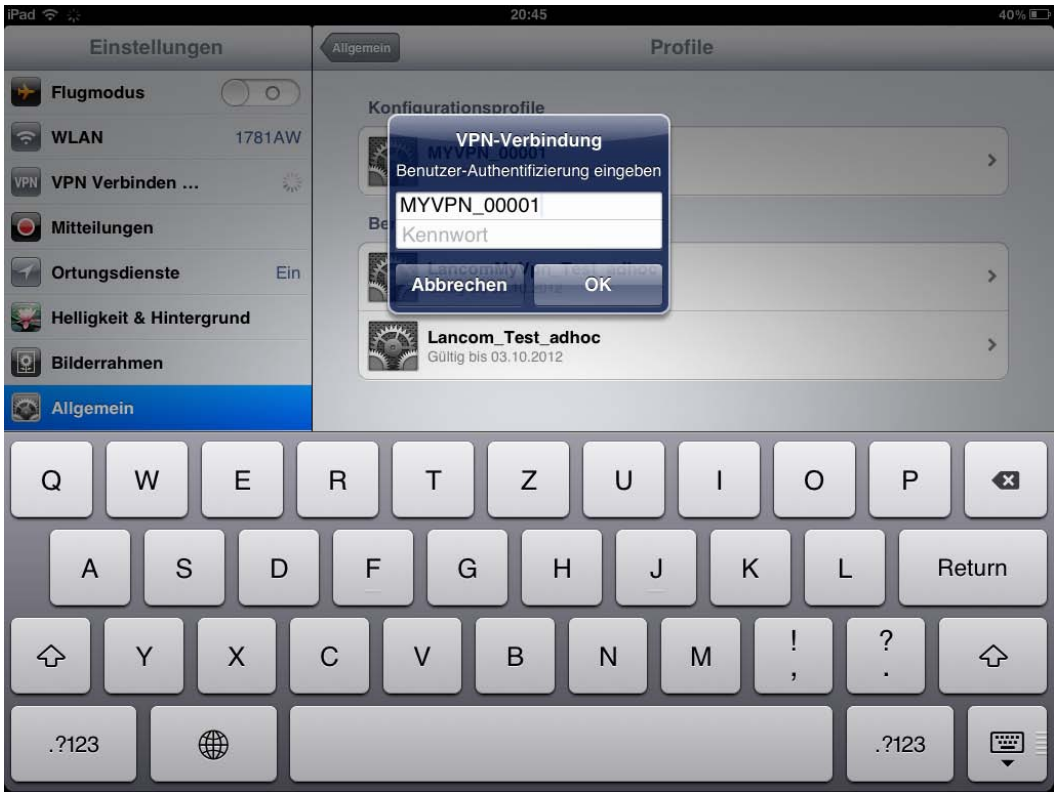
Das Deaktivieren des myVPN-Profils verhindert ausschließlich, dass ein weiteres iOS-Gerät das gleiche myVPN-Profil noch einmal installiert und somit die gleichen Einstellungen für den VPN-Zugang verwendet. Das Deaktivieren des myVPN-Profils hat hingegen keine Auswirkung auf den VPN-Zugang selbst.

VPN-Verbindung auf dem iOS-Gerät herstellen und beenden

Nachdem Sie das VPN-Profil mit der LANCOM myVPN App auf Ihrem iOS-Gerät installiert haben, stellen Sie wie folgt die VPN-Verbindung zu Ihrem Firmennetzwerk her oder beenden diese:

1. Aktivieren Sie den VPN-Tunnel im Konfigurationsbereich **Einstellungen** über die Option **VPN**.

2. Im folgenden Dialog ist der Benutzername aus dem myVPN-Profil bereits eingetragen. Geben Sie das Kennwort für die VPN-Verbindung ein und bestätigen Sie mit **OK**.



Standardmäßig entspricht das Kennwort für die VPN-Verbindung der PIN für das myVPN-Profil.

Das Kennwort ist bereits eingetragen, wenn Sie das Kennwort für die VPN-Verbindung bei der Installation des myVPN-Profils eingegeben haben. In diesem Fall erscheint dieses Fenster nicht, die Verbindung wird direkt hergestellt.

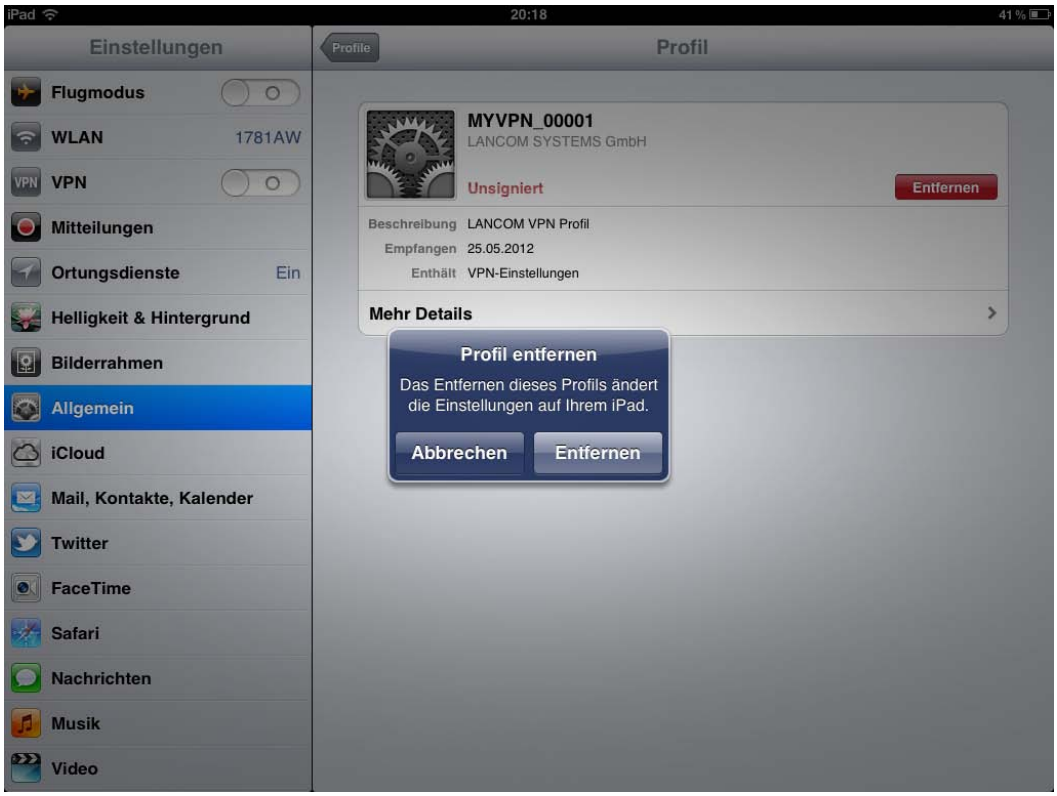
3. Beenden Sie die VPN-Verbindung auf Ihrem iOS-Gerät im Konfigurationsbereich **Einstellungen** über die Option **VPN**.

VPN-Profil auf dem iOS-Gerät löschen

So löschen Sie das VPN-Profil wieder von Ihrem iOS-Gerät:

1. Wechseln Sie mit **Einstellungen** > **Allgemein** > **Profile** in die Liste der verfügbaren Profile Ihres iOS-Gerätes.

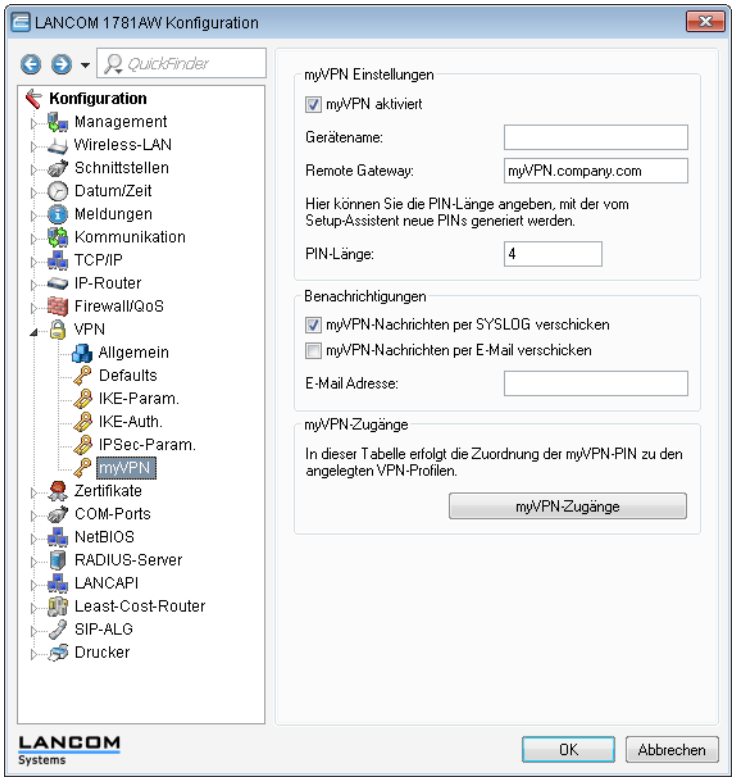
2. Wählen Sie das gewünschte Profil aus, klicken Sie auf **Entfernen** und bestätigen Sie im nächsten Dialog die Aktion noch einmal mit **Entfernen**.



Ergänzungen in LANconfig

Konfiguration der LANCOM myVPN App

Unter **VPN** > **myVPN** können Sie die Einstellungen für die LANCOM myVPN App manuell festlegen.



Markieren Sie **myVPN aktiviert**, um der LANCOM myVPN App zu ermöglichen, ein VPN-Profil zu laden.

Geben Sie hier den **Gerätenamen** an, wenn ein vertrauenswürdiges SSL-Zertifikat auf diesem Gerät eingerichtet ist und bei dem Bezug des Profils auf dem iOS-Gerät keine Warnmeldung bezüglich eines nicht vertrauenswürdigen Zertifikats auftauchen soll.

Bestimmen Sie im Feld **Remote-Gateway** die WAN-Adresse oder den über öffentliche DNS-Server auflösbaren Namen dieses Routers. Geben Sie dieses Remote-Gateway in der LANCOM myVPN App an, sofern die App das Gateway nicht über die automatische Suche findet.

Bestimmen Sie die **PIN-Länge**, mit der der Setup-Assistent neue PINs generiert (Default = 4).

Aktivieren Sie die Option **myVPN-Nachrichten per SYSLOG verschicken**, um Nachrichten der LANCOM myVPN App an SYSLOG zu versenden.

Aktivieren Sie die Option **myVPN-Nachrichten per Email verschicken**, um Nachrichten der LANCOM myVPN App an eine bestimmte E-Mail-Adresse zu versenden.

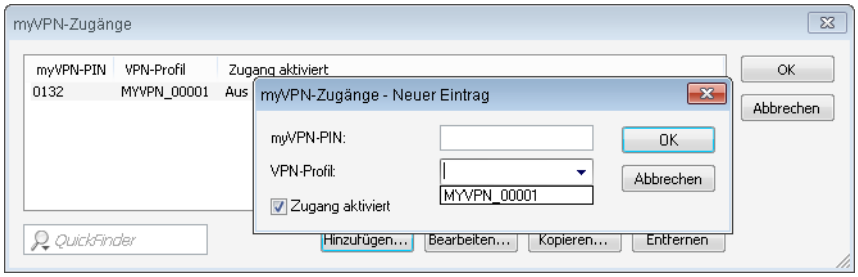
Diese Nachrichten umfassen:

- Erfolgreicher Profilbezug
- Auftreten einer Loginsperre für die LANCOM myVPN App aufgrund zu vieler Fehlversuche
- Aufhebung der Loginsperre (wobei nicht berücksichtigt wird, ob sie durch den Ablauf der vorgegebenen Zeitspanne oder manuell erfolgt ist)

Bestimmen Sie die **E-Mail-Adresse**, an welche die LANCOM myVPN App Nachrichten versenden soll.

Der Versand von E-Mails muss auf dem VPN-Gerät dazu konfiguriert sein.

Über **myVPN-Zugänge** erfolgt die Zuordnung der myVPN-PIN zu den angelegten VPN-Profilen.



Bestimmen Sie hier das **VPN-Profil**, dessen Daten die LANCOM myVPN App beim Profilbezug laden soll.

Vergeben Sie hier die myVPN-PIN zum Profilbezug der LANCOM myVPN App.

Sicherheitshinweis: Um das myVPN-Feature abzusichern, deaktiviert das Gerät bei der wiederholten Falscheingabe einer spezifischen PIN temporär den Profilbezug und versendet ggf. eine entsprechende Benachrichtigung sowohl per SYSLOG als auch per E-Mail. Nach den ersten fünf Fehlversuchen sperrt das Gerät den Profilbezug für 15 Minuten. Fünf weitere Fehlversuche sperren den Profilbezug für einen Tag. Bei weiteren Fehlversuchen alternieren die Zeitspannen. Eine manuelle Entsperrung setzt den entsprechenden Zähler wieder zurück. Hierbei ist auch zu beachten, dass das Gerät einen versuchten Profilbezug bei einem deaktiviertem Zugang (z. B. durch vorherigen erfolgreichen Profilbezug) ebenfalls als Fehlversuch wertet.

Aktivieren Sie das Profil, indem Sie die Option **Zugang aktiviert** markieren.

Nach einem erfolgreichen Profilbezug deaktiviert das Gerät das entsprechende Profil automatisch, um den wiederholten Download von einem anderen Gerät zu vermeiden.

Sobald Sie diese Einstellungen im Gerät speichern, ist das myVPN-Modul auf dem gewählten VPN-Gerät aktiviert. Sie können nun die LANCOM myVPN App auf Ihrem iOS-Gerät starten und mit Eingabe der PIN das VPN-Profil beziehen.

Ergänzungen im Menüsystem

myVPN

Die Funktion "myVPN" dient dazu, auf Endgeräten mit IOS-Betriebsystem VPN-Profile automatisch zu beziehen und die Konfiguration des internen VPN-Clients zu übernehmen. Auf Seiten des Routers konfigurieren Sie dazu das VPN-Profil und die myVPN-Parameter. Mit der LANCOM myVPN App und einer passenden PIN können Sie Ihr Endgerät in wenigen Schritten für eine VPN-Einwahl konfigurieren.

Weitere Informationen zur myVPN-App finden Sie auf der *LANCOM-Homepage*.

SNMP-ID:

2.19.28

Pfad Telnet:

Pfad Telnet: Setup > Vpn > myVPN

Aktiv

Mit diesem Schalter können sie myVPN für dieses Gerät aktivieren.

SNMP-ID:

2.19.28.1

Pfad Telnet:

Pfad Telnet: Setup > **Vpn** > **myVPN**

Mögliche Werte:

Ja

Nein

Default:

Nein

PIN-Laenge

Hier können Sie die PIN-Länge angeben, mit der der Setup-Assistent neue PINs generiert.

SNMP-ID:

2.19.28.2

Pfad Telnet:

Pfad Telnet: Setup > **Vpn** > **myVPN**

Mögliche Werte:

Maximale Länge: 12

Minimale Länge: 4

Default:

4

Geraetename

Geben Sie hier den Gerätenamen an, wenn ein vertrauenswürdiges SSL-Zertifikat auf diesem Gerät eingerichtet ist und bei dem Bezug des Profils auf dem iOS-Gerät keine Warnmeldung bezüglich eines nicht vertrauenswürdigen Zertifikats auftauchen soll.

SNMP-ID:

2.19.28.3

Pfad Telnet:

Pfad Telnet: Setup > **Vpn** > **myVPN**

Mögliche Werte:

max. 31 Zeichen aus

0-9

a-z

A-Z

#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

leer

Mapping

In dieser Tabelle erfolgt die Zuordnung der myVPN-PIN zu den angelegten VPN-Profilen.

SNMP-ID:

2.19.28.4

Pfad Telnet:

Pfad Telnet: Setup > **Vpn** > **myVPN**

PIN

Hinterlegen Sie hier die PIN zum Profilbezug der myVPN-App.

Der myVPN-Setup-Assisstent benutzt diese PIN auch in der PPP-Liste für den eigentlichen VPN-Login. Sollten Sie also die PIN hier ändern, müssen Sie sie auch mit LANconfig unter **Kommunikation** > **Protokolle** > **PPP-Liste** ändern, sofern Sie keine unterschiedliche PIN wünschen.

Sicherheitshinweis: Um das myVPN-Feature abzusichern, deaktiviert das Gerät bei der wiederholten Falscheingabe einer spezifischen PIN temporär den Profilbezug und versendet ggf. eine entsprechende Benachrichtigung sowohl per SYSLOG als auch per E-Mail. Nach den ersten drei Fehlversuchen sperrt das Gerät den Profilbezug für 15 Minuten. Drei weitere Fehlversuche sperren den Profilbezug für 24 Stunden. Bei weiteren Fehlversuchen alternieren die Zeitspannen. Eine manuelle Entsperrung setzt den entsprechenden Zähler wieder zurück. Hierbei ist auch zu beachten, dass das Gerät einen versuchten Profilbezug bei einem deaktiviertem Zugang (z. B. durch vorherigen erfolgreichen Profilbezug) ebenfalls als Fehlversuch wertet.

SNMP-ID:

2.19.28.4.1

Pfad Telnet:

Pfad Telnet: Setup > **Vpn** > **myVPN** > **Mapping**

Mögliche Werte:

max. 12 Ziffern aus 1234567890

Default:

leer

VPN-Profil

Bestimmen Sie hier das VPN-Profil, dessen Daten die myVPN-App beim Profilbezug laden soll.

SNMP-ID:

2.19.28.4.2

Pfad Telnet:

Pfad Telnet: Setup > **Vpn** > **myVPN** > **Mapping**

Mögliche Werte:

16 Zeichen aus

0-9

a-z

A-Z

@{|}~!$%&'()+-,/:;<=>?[\]^_.

Default:

leer

Aktiv

Mit diesem Schalter können sie den Profilbezug mit Hilfe der myVPN-App aktivieren. Nach einem erfolgreichen Profilbezug deaktiviert das Gerät das entsprechende Profil automatisch, um den wiederholten Download von einem anderen Gerät zu vermeiden.

SNMP-ID:

2.19.28.4.3

Pfad Telnet:

Pfad Telnet: Setup > **Vpn** > **myVPN** > **Mapping**

Mögliche Werte:

Nein

Ja

Default:

Nein

Loginsperre-aufheben

Mit dem Befehl `do Loginsperre-aufheben` können Sie eine durch Fehlversuche hervorgerufene Loginsperre aufheben. Ggf. erzeugt die Aufhebung eine Nachricht über SYSLOG oder E-Mail.

SNMP-ID:

2.19.28.5

Pfad Telnet:

Pfad Telnet: Setup > **Vpn** > **myVPN**

E-Mail-Benachrichtigung

Aktivieren Sie diese Option, um Nachrichten der myVPN-App an eine bestimmte E-Mail-Adresse zu versenden. Diese Nachrichten umfassen:

- Erfolgreicher Profilbezug
- Auftreten einer Loginsperre für myVPN aufgrund zu vieler Fehlversuche
- Aufhebung der Loginsperre (wobei nicht berücksichtigt wird, ob sie durch den Ablauf der vorgegebenen Zeitspanne oder manuell erfolgt ist)

SNMP-ID:

2.19.28.6

Pfad Telnet:

Pfad Telnet: Setup > **Vpn** > **myVPN**

Mögliche Werte:

Nein

Ja

Default:

Nein

E-Mail-Adresse

Bestimmen Sie hier die E-Mail-Adresse, an die die myVPN-App Nachrichten versenden soll.

SNMP-ID:

2.19.28.7

Pfad Telnet:

Pfad Telnet: Setup > **Vpn** > **myVPN**

Mögliche Werte:

max. 63 Zeichen aus

0-9

a-z

A-Z

@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

leer

Syslog

Aktivieren Sie diese Option, um Nachrichten der myVPN-App an SYSLOG zu versenden. Diese Nachrichten umfassen:

- Erfolgreicher Profilbezug
- Auftreten einer Loginsperre für myVPN aufgrund zu vieler Fehlversuche
- Aufhebung der Loginsperre (wobei nicht berücksichtigt wird, ob sie durch den Ablauf der vorgegebenen Zeitspanne oder manuell erfolgt ist)

SNMP-ID:

2.19.28.8

Pfad Telnet:

Pfad Telnet: Setup > **Vpn** > **myVPN**

Mögliche Werte:

Nein

Ja

Default:

Nein

Remote-Gateway

Bestimmen Sie hier die WAN-Adresse oder den über öffentliche DNS-Server auflösbaren Namen dieses Routers. Geben Sie das Remote-Gateway zusätzlich in der myVPN-App an, sofern die App das Gateway nicht über die automatische Suche findet.

SNMP-ID:

2.19.28.9

Pfad Telnet:

Pfad Telnet: Setup > **Vpn** > **myVPN**

Mögliche Werte:

max. 63 Zeichen aus

0-9

a-z

A-Z

#@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

leer