
# Addendum LCOS 8.62 RU1

LCOS
[LANCOM OPERATING SYSTEM]

LANCOM
Systems

# Contents

# 1 Addendum to LCOS version 8.62

The document describes the new functions and changes to LCOS version 8.62 over the previous version.

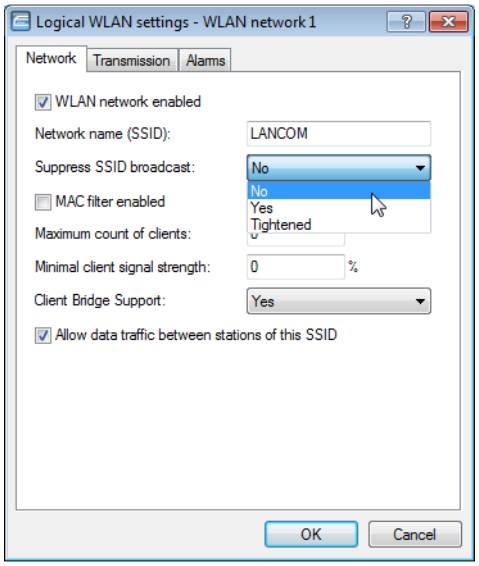
## 1.1 Wireless LAN – WLAN

### 1.1.1 Closed-network function: Suppress SSID broadcast

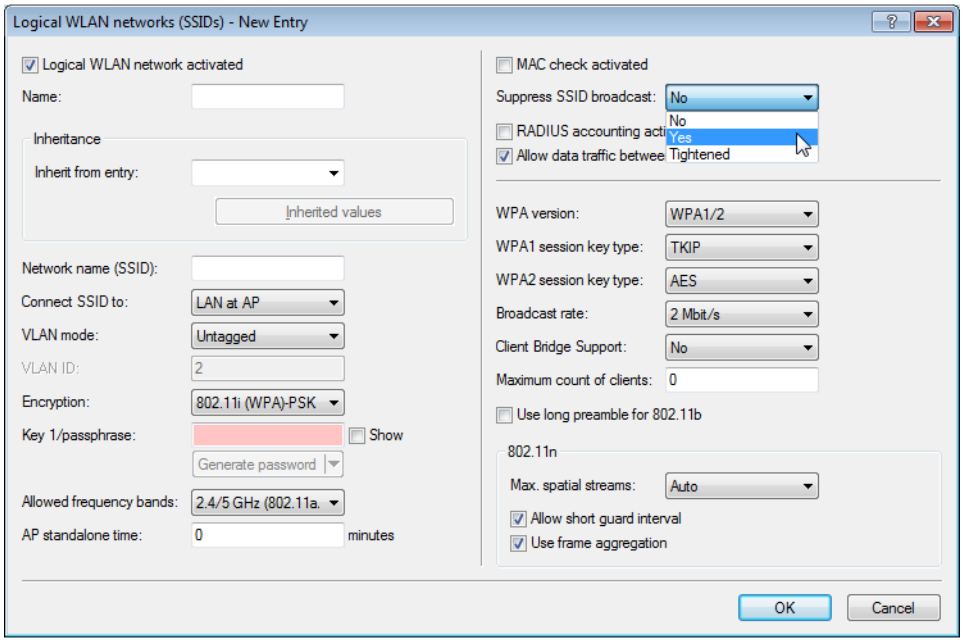
A WLAN client can only connect to a wireless network if it is informed of the corresponding SSID. The factory settings for many wireless networks allow the use of a blank SSID or the SSID "any", and continuing to use this means that potential intruders do not need to know the wireless LAN's SSID. The closed network function prevents unauthorized WLAN clients from logging into the WLAN. The access point rejects any attempt to log on with a blank SSID or the SSID "any". Any user wanting to logon to the WLAN must know the correct SSID.

Simply suppressing the SSID broadcast does not provide adequate protection: When legitimate WLAN clients associate with the access point, this transmits the SSID in plain text so that it is briefly visible to all clients in the WLAN network.

**LANconfig:Wireless LAN** > **General** > **Interfaces** > **Logical WLAN settings** > **Network**.



**LANconfig:WLAN Controller > Profiles > Logical WLAN networks (SSIDs)**




The option **Suppress SSID broadcast** provides the following settings:

- **No**: The access point broadcasts the radio cell's SSID. When a client sends a probe request with a blank or incorrect SSID, the device responds with the SSID of the radio cell (publicly visible WLAN).
- **Yes**: The access point does not broadcast the radio cell's SSID. When a client sends a probe request with an empty SSID, the device similarly responds with an empty SSID. The client cannot log on to the radio cell.
- **Tightened**: The access point does not broadcast the radio cell's SSID. When a client sends a probe request with a blank or incorrect SSID, the device does not respond. The client cannot log on to the radio cell. This setting also reduces the network load if there is a large number of WLAN clients in the radio cell.

## Additions to the menu system

### Closed network (for standalone access points only)

You can operate your wireless LAN either in public or private mode. A wireless LAN in public mode can be contacted by any mobile station in the area. Your wireless LAN is put into private mode by activating the closed network function. In this operation mode, mobile stations that do not know the network name (SSID) are excluded from taking part in the wireless LAN.

With the closed-network mode activated, WLAN clients that use an empty SSID or the SSID "ANY" are prevented from associating with your network.

The option **Suppress SSID broadcast** provides the following settings:

- **No**: The access point broadcasts the radio cell's SSID. When a client sends a probe request with an empty or incorrect SSID, the access point responds with the SSID of the radio cell (public WLAN).
- **Yes**: The access point does not broadcast the radio cell's SSID. When a client sends a probe request with an empty SSID, the access point similarly responds with an empty SSID.
- **Tightened**: The access point does not broadcast the radio cell's SSID. When a client sends a probe request with an empty or incorrect SSID, the access point does not respond.

Simply suppressing the SSID broadcast does not provide adequate protection: When legitimate WLAN clients associate with the access point, this transmits the SSID in plain text so that it is briefly visible to all clients in the WLAN network.

**SNMP ID:**

2.23.20.1.4

**Telnet path:**

**Telnet path:Setup** > **Interfaces** > **WLAN** > **Network**

**Possible values:**

No

Yes

Tightened

**Default:**

No

**SSID broadcast (for WLAN controllers only)**

You can operate your wireless LAN either in public or private mode. A wireless LAN in public mode can be contacted by any mobile station in the area. Your wireless LAN is put into private mode by activating the closed network function. In this operation mode, mobile stations that do not know the network name (SSID) are excluded from taking part in the wireless LAN.

With the closed-network mode activated on the access point, WLAN clients that use an empty SSID or the SSID "ANY" are prevented from associating with your network.

The option **SSID broadcast** provides the following settings:

- **Yes**: The access point broadcasts the radio cell's SSID. When a client sends a probe request with an empty or incorrect SSID, the access point responds with the SSID of the radio cell (publicly visible WLAN).
- **No**: The access point does not broadcast the radio cell's SSID. When a client sends a probe request with an empty SSID, the access point similarly responds with an empty SSID.
- **Tightened**: The access point does not broadcast the radio cell's SSID. When a client sends a probe request with an empty or incorrect SSID, the access point does not respond.

Simply suppressing the SSID broadcast does not provide adequate protection: When legitimate WLAN clients associate with the access point, this transmits the SSID in plain text so that it is briefly visible to all clients in the WLAN network.

The "closed network" function for the access point is to be found under **Setup** > **Interfaces** > **WLAN** > **Network**. Please note: If the WLAN controller has the option **SSID broadcast** set to "No" (device does not broadcast the SSID), the access point sets its **closed network** option to "Yes", and vice versa. Only with the setting "Tightened" do both devices retain identical settings.

**SNMP ID:**

2.37.1.1.19

**Telnet path:**

**Telnet path:Setup** > **WLAN-Management** > **AP-Configuration** > **Networkprofiles**

**Possible values:**

No

Yes

Tightened

**Default:**

Yes

## 1.1.2 New parameter for WLAN client signal strength

LCOS version 8.62 now optionally evaluates the signal strengths of wireless LAN clients when they logon.

### Additions to the menu system

#### 2.23.20.1.16 Min-Client-Strength

This values defines the minimum signal strength of WLAN clients which the access point will accept, even if a matching SSID or a wildcard SSID is provided. The access point will silently discard all probe requests below this threshold.

You can use this option to prevent large numbers of potential WLAN clients, e.g. mobile handsets, to decrease the WLAN performance with probe requests looking for available WLAN networks.

The strength threshold is specified in percent, which can be translated into an SNR: a threshold of 100 percent means a minimum SNR of 64 dBm, 50 percent means 32 dBm and so on.

**Path Telnet:** /Setup/Interfaces/WLAN/Network

**Possible values:**

- 0% to 100%

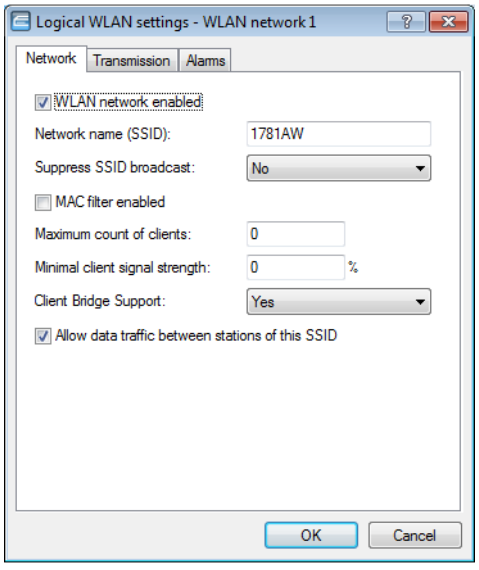
**Default:** 0

**Special values:** '0' deactivates the minimum signal strenght, the access point will answer all requests.

## 1.1.3 Additions to LANconfig

### Network settings

**LANconfig:Wireless LAN** > **General** > **Logical WLAN settings** > **Network**




- **WLAN network enabled**

  This switch enables or disenables the corresponding logical WLAN.

- **Network name** (SSID)

  Specify a unique SSID (the network name) for each of the required logical wireless LANs. Only network cards that have the same SSID can register with this wireless network.

- **Suppress SSID broadcast**

  You can operate your wireless LAN either in public or private mode. A wireless LAN in public mode can be contacted by any mobile station in the area. Your wireless LAN is put into private mode by activating the closed network function. In this operation mode, mobile stations that do not know the network name (SSID) are excluded from taking part in the wireless LAN.

  With the closed-network mode activated, WLAN clients that use an empty SSID or the SSID "ANY" are prevented from associating with your network.

  The option **Suppress SSID broadcast** provides the following settings:

  - **No**: The access point broadcasts the radio cell's SSID. When a client sends a probe request with an empty or incorrect SSID, the access point responds with the SSID of the radio cell (public WLAN).
  - **Yes**: The access point does not broadcast the radio cell's SSID. When a client sends a probe request with an empty SSID, the access point similarly responds with an empty SSID.
  - **Tightened**: The access point does not broadcast the radio cell's SSID. When a client sends a probe request with an empty or incorrect SSID, the access point does not respond.

  Simply suppressing the SSID broadcast does not provide adequate protection: When legitimate WLAN clients associate with the access point, this transmits the SSID in plain text so that it is briefly visible to all clients in the WLAN network.

- **MAC filter enabled**

  The MAC addresses of the clients that are allowed to associate with an access point are stored in the MAC filter list (**Wireless LAN** > **Stations** > **Stations**). The **MAC filter enabled** switch allows you to switch off the use of the MAC filter list for individual logical networks.

  Use of the MAC filter list is required for logical networks in which the clients register via LEPS with an individual passphrase. The passphrase used by LEPS is also entered into the MAC filter list. The access point always consults the MAC filter list for registrations with an individual passphrase, even if this option is deactivated here.

- **Maximum number of clients**

  Here you set the maximum number of clients that may associate with this access point. Additional clients wanting to associate will be rejected by the access point.

- **Minimum client signal strength**

  This value sets the threshold value in percent for the minimum signal strength for clients when logging on. If the client's signal strength is below this value, the access point stops sending probe responses and discards the client's requests.

  A client with poor signal strength will not detect the access point and cannot associate with it. This ensures that the client has an optimized list of available access points, as those offering only a weak connection at the client's current position are not listed.

- **Client-bridge support**

  Enable this option for an access point if you have enabled the client-bridge support for a client station in WLAN client mode.

  The client-bridge mode operates between two LANCOM devices only.

- **Allow traffic between stations of this SSID**

  Check this option if all stations logged on to this SSID are to be able to communicate with one another.

# 1.2 Public-Spot

## 1.2.1 Enhancements to the Public Spot

When registering a new Public Spot user with LCOS version 8.62, you can now specify whether the user is able to log on multiple times with a single user account (multiple login).

This enhancement is available with the "Create Public Spot account" wizard and when setting-up new Public-Spot users with the web API.

You can now also output a CSV file instead of printing out vouchers when registering new Public-Spot users with the wizard.

### Managing Public Spot users via the web API

As an alternative to using the Setup Wizard, entering a special URL in the address bar gives you the option of displaying, creating or deleting Public-Spot users directly.

#### Adding a Public Spot user

To register a new Public Spot user, simply enter the following URL:

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

The following parameters are available:

**`comment`**

Comment on the registered user

If it is possible to enter multiple comments for a Public Spot user, you can enter the comments and their corresponding comment-field names as follows:

```
&comment=<Content1>:<Fieldname1>;<Content2>:<Fieldname1>;
   ...;<Content5>:<Fieldnamee5>
```

If there is just one comment field per user, then the comment is entered as follows:

```
&comment=<Comment>
```

Special characters such as German umlauts are not supported.

The maximum number of characters for the comment parameter is 191 characters.

**`print`**

Automatic print-out of the voucher.

If this parameter is omitted, the wizard displays a button that you can use to print the voucher.

**`printcomment`**

Print the comment on the voucher.

If this parameter is omitted, no comment will appear on the voucher (default setting).

**`nbguests`**

The number of Public Spot users to be created.

If this parameter is omitted, the wizard creates one user only (default setting).

**`defaults`**

Use default values

The wizard replaces missing or incorrect parameters with default values.

**`expiretype`**

Combined output of expiry type and validity period of the voucher.

Specify this parameter as follows:

```
&expiretype=<Value1>+validper=<Value2>
```

The parameter values have the following meaning:

- `Value1`: Expiry type (absolute, relative, absolute and relative, none)
- `Value2`: Expiration period of the voucher

If these parameters are omitted or set with incorrect values the wizard will apply the default values.

**`ssid`**

Network name

If this parameter is omitted, the wizard uses the default network name (default setting).

**`unit`**

Access time

Specify this parameter as follows:

```
&unit=<Value1>+runtime=<Value2>
```

The parameter values have the following meaning:

- `Value1`: Unit used to measure runtime. Possible values are: Minute, hour, day
- `Value2`: Runtime

**`timebudget`**

Time budget

If this parameter is omitted, the wizard uses the default value.

**`volumebudget`**

Volume budget

If this parameter is omitted, the wizard uses the default value.

**`multilogin`**

Multiple login

If you specify this parameter, the user can login multiple times with his/her user account. If omitted, then multi-login is disabled by default.

If the Public Spot administration contains no default values to replace missing parameters, the wizard opens a dialog. Enter the missing values here.

## Public Spot user administration

The Setup Wizards provide you with an easy method of managing Public Spot users.

#### Adding new Public Spot users with a single click

In WEBconfig, you can register new Public Spot users with the setup wizard **Create Public Spot Account**. This wizard is preset with default values, so you can set up a new user with a single click on **Save & Print**. By clicking on **Save & CSV export** the wizard provides you with the voucher data as a CSV file for download.

The following settings can be configured if required:

- **Starting time for account:** Sets the time when the voucher becomes valid. Possible values are:
  - **First login (default):** The time starts running when the user logs in for the first time
  - **Immediately:** The time starts running when the user is created
- **Validity period:** Enter the overall time period within which the voucher can remain valid.

  If the access is to be valid immediately, it is not possible to enter a validity period.
- **Duration:** Set how long access is to be available after registration or the first login.
- **SSID (network name):** Select the wireless LAN network for which the access applies. The default network name is already highlighted. This SSIDs listed here are managed in the SSID table.

  Press the "Ctrl" key to select multiple entries.
- **Number of vouchers:** Specify how many vouchers you want to create at a time (default: 1).
- **Time budget (minutes):** Specify the amount of time after which access to the Public Spot is closed.

  Depending on the chosen expiry method, access time is limited either to the time budget (incremental) or to the set voucher validity period (absolute).
- **Volume budget (MByte):** Specify the available data volume after which access is closed.
- **Comment (optional):** Add a comment.
- **Prints comment on voucher:** Check this option if the comment is to appear on the voucher.
- **Print:** Check this option to print the vouchers as soon as they are registered (default: on)

  If this option is disabled, the wizard displays a summary of the new Public Spot users after they have been registered. You then have the opportunity to print the vouchers again.
- **Multiple logins:** Enabling this option allows a user to login multiple times at the Public Spot with his/her user account (default: off).

You can configure the default values that are to be used when creating new Public Spot accounts in the following menus:

- LANconfig: **Public Spot** > **Public Spot Wizard**
- WEBconfig: **LCOS Menu Tree** > **Setup** > **Public-Spot module** > **Add user wizard**

# 1.3 Voice over IP - VoIP

## 1.3.1 Default setting for WAN registration of a SIP user

The default setting for the WAN registration of a SIP user has changed from 'yes' to 'no'.

### Additions to the menu system

#### Access from WAN

This item determines whether and how SIP clients can register via a WAN connection.

**SNMP ID:**

2.33.3.1.1.8

**Telnet path:**

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

**Possible values:**

Yes

No

VPN

**Default:**

No

# 1.4 Virtual Private Networks - VPN

## 1.4.1 Default proposals for IKE and IPSec

The proposals for IKE and IPSec all now support a key length of 256 bits in the default settings.

A firmware upgrade initially does not enable this change, to avoid any problems for existing installations. To accept the changes, you must perform a reset of the device or reset the tables. For new devices with LCOS 8.62 or later, the new defaults are already active.

## 1.4.2 myVPN

The LANCOM myVPN app offers you a very easy way to set up a VPN connection to your company network from your iPhone, iPad or iPod (or from any iOS device in general). The LANCOM myVPN app offers the following functions:

- Highly secure, mobile VPN connections made easy
- Facilitates the complex VPN configuration of the integrated VPN client of iOS devices and the LANCOM router
- PIN operation for the authentication during the VPN tunnel establishment
- Access control via adjustable firewall rules on LANCOM VPN gateways
- LANCOM myVPN user management and automatic detection of myVPN-activated LANCOM gateways
- For version 4.1 iOS devices and later

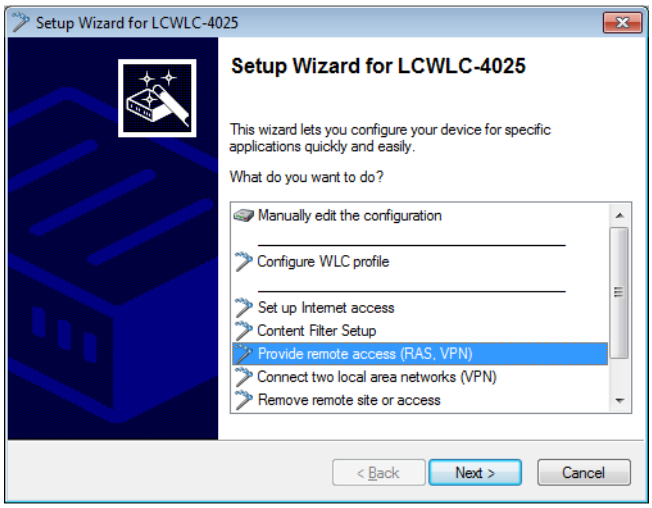
After its installation, the LANCOM myVPN app retrieves a VPN profile from your LANCOM VPN device and automatically configures all of the necessary settings on the iOS device. You can then use the internal features of iOS to establish a VPN connection to your company network in just a few steps.

### Using the Setup Wizard in LANconfig to set up a VPN profile for the LANCOM myVPN app

This is how to use the Setup Wizard to provide an access account for a VPN client on an iOS device:

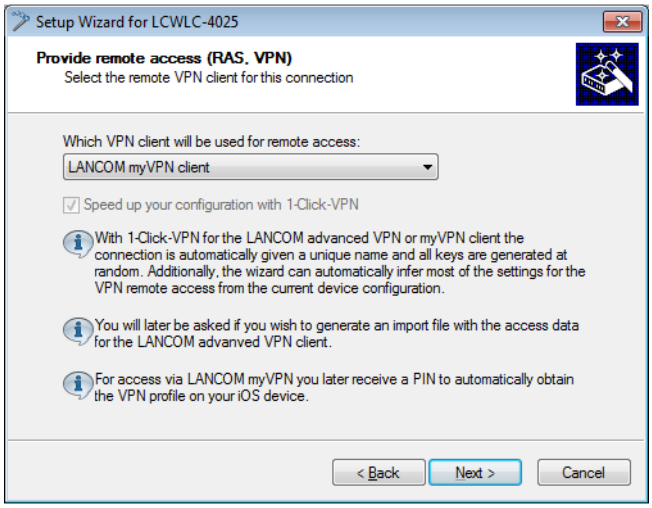
1. Start LANconfig, for example from the Windows start menu with **Start** > **Programs** > **LANCOM** > **LANconfig**. LANconfig now automatically searches the local network for devices.
2. Choose the required device from the selection window in LANconfig and select the **Setup Wizard** button or use the menu under **Tools** > **Setup Wizard**.

3. Select the item **Provide remote access (RAS, VPN)** and then click on **Next**.

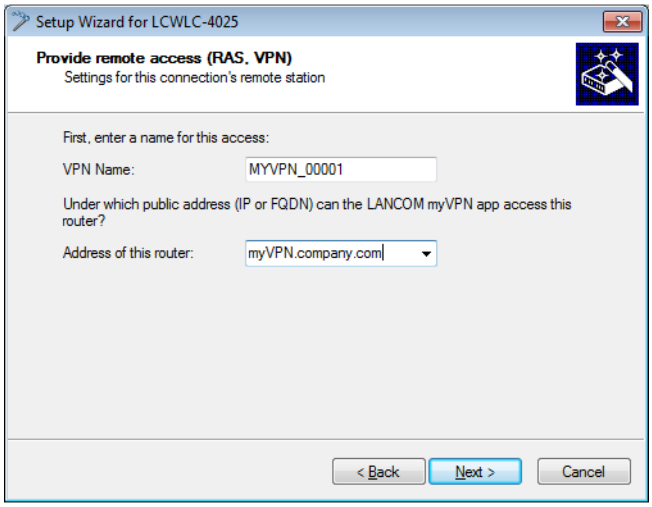



You can skip the following information dialog with **Next**.

4. From the drop-down list select the option **LANCOM myVPN client** and click on **Next**.

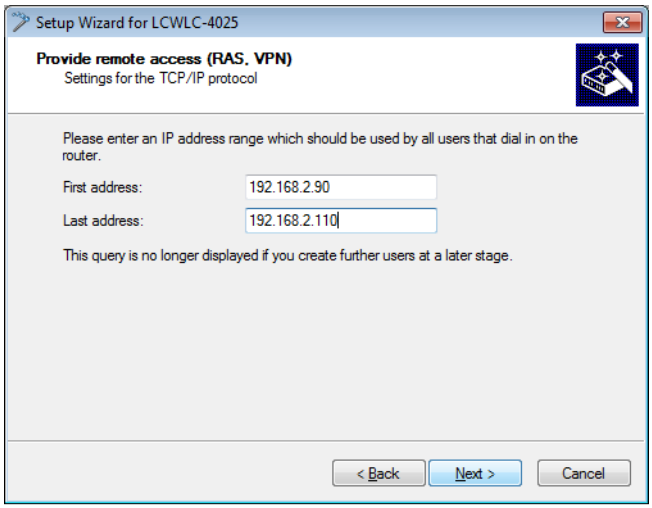


5. Enter a name for this access account and select the address at which the VPN client on the iOS device can reach the router from the Internet. To continue, click on **Next**.



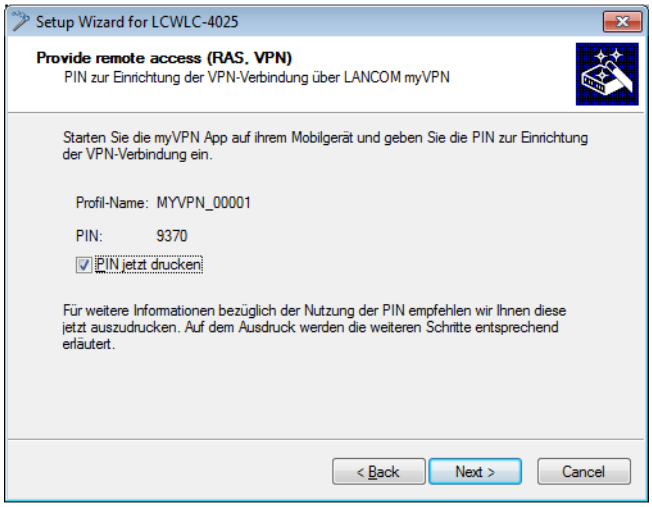

The Setup Wizard will suggest a name that you can accept if you wish.

6. If the VPN device doesn't have a pool of IP addresses configured already, the following dialog will prompt you to specify a unique range of IP addresses as a pool. During dial-in the VPN device will assign a free IP address from this pool to the iOS device.




If the VPN device already has configured a pool of IP addresses for VPN clients, it will automatically use this address pool and skip the dialog shown above.

7. The Setup Wizard displays the profile name and the PIN that was auto-generated for the VPN client. If you want to print out the PIN now, select the option **Print PIN now**. Click on **Next**.




8. By clicking on **Finish** the Setup Wizard stores all the settings on the corresponding VPN device. If applicable, it then starts with the printout of the myVPN PIN.
   The myVPN module is now enabled on the selected VPN device. On your iOS device, you can now start the myVPN app and enter the PIN to retrieve the VPN profile.

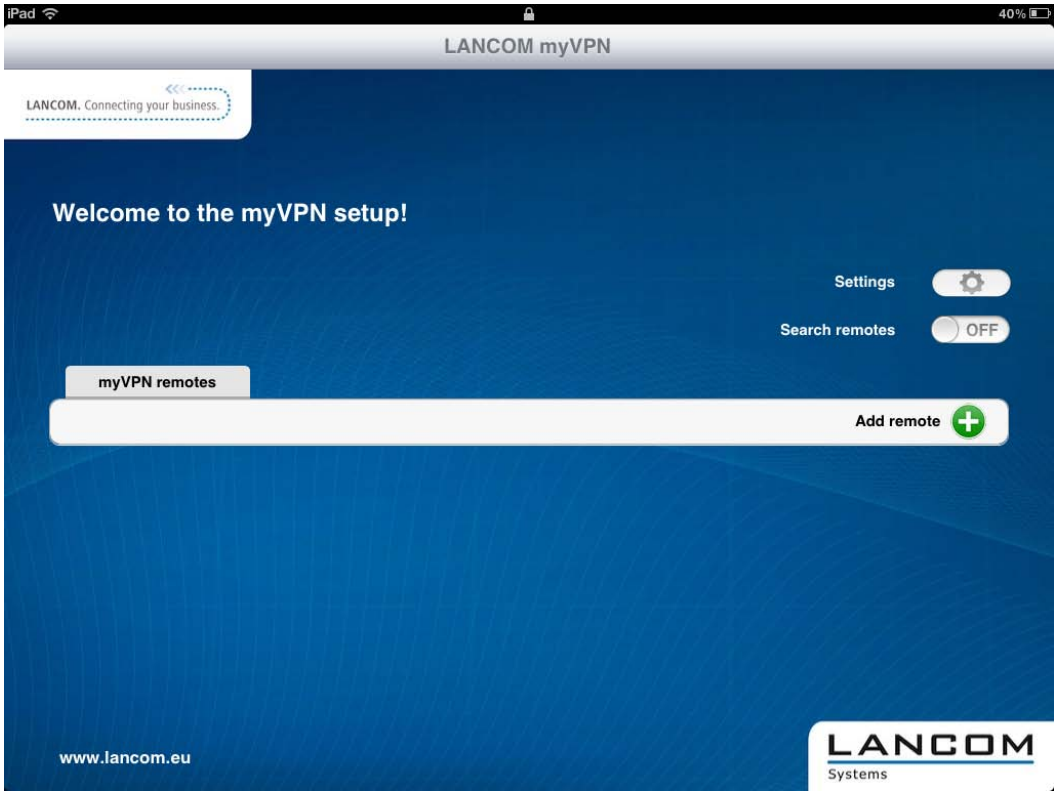
## Retrieve the VPN profile with the LANCOM myVPN app

This is how you can use the LANCOM myVPN app on your iOS device to retrieve a VPN profile from a LANCOM VPN device:

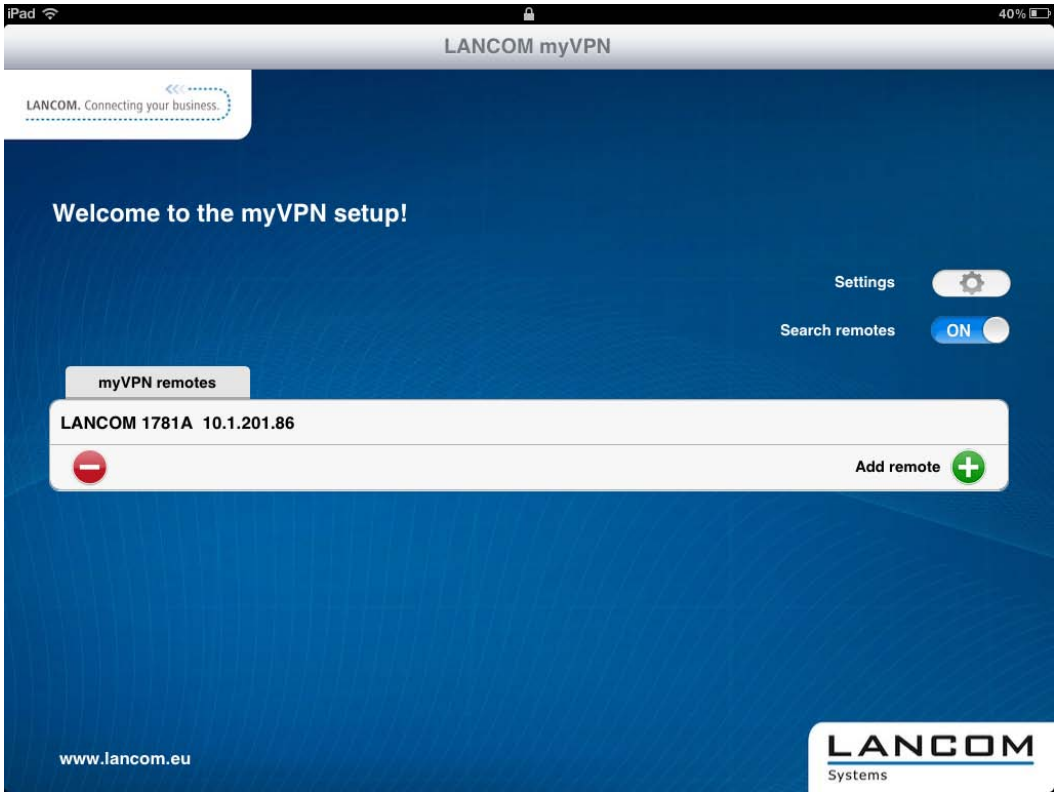
The purpose of the LANCOM myVPN app is to set up the VPN client on iOS devices with the correct parameters and in a quick and easy way. The establishment of the VPN connection to the company network itself is handled directly by the VPN client in the iOS device.

1. Download the LANCOM myVPN app from the Apple App Store.

2. Open the app on your iPhone or iPad.

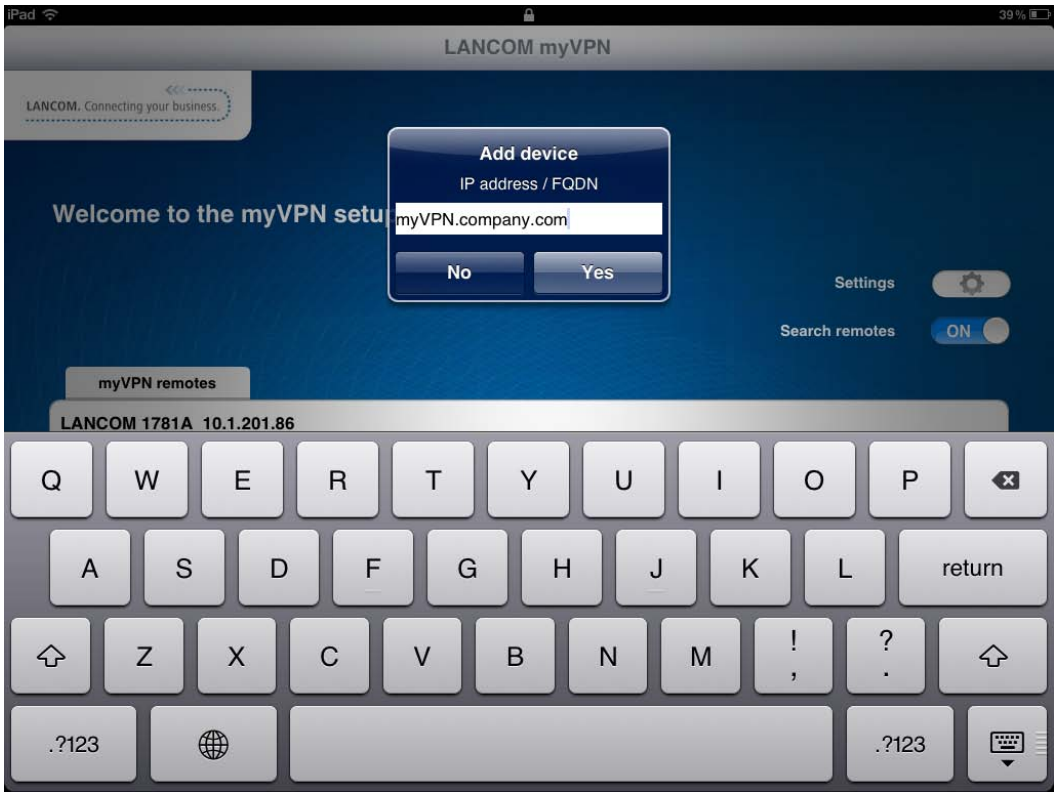



3. Optional: Enable the option **Search remotes** to find VPN devices with an activated LANCOM myVPN module and which is available to iOS devices via WLAN.

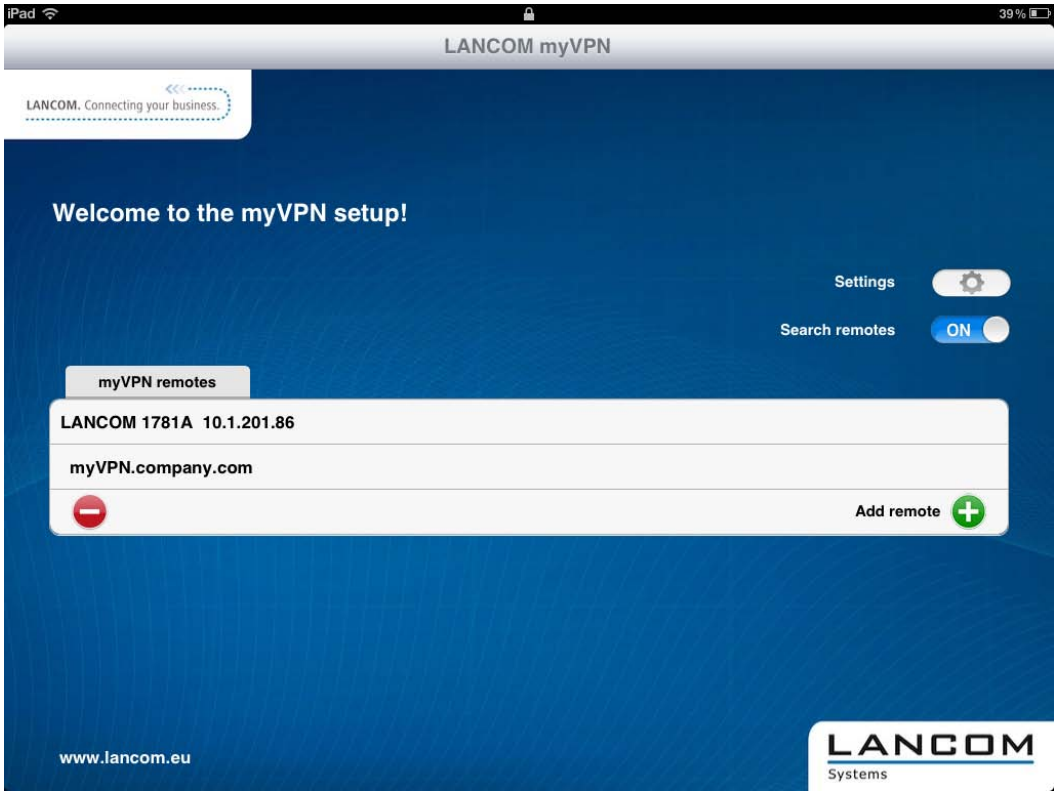


The iOS device now lists all VPN devices which are accessible via WLAN and which have an active LANCOM myVPN module. However, the inclusion of an entry in this list does not necessarily mean that your iOS device can retrieve a LANCOM myVPN profile from this VPN device.

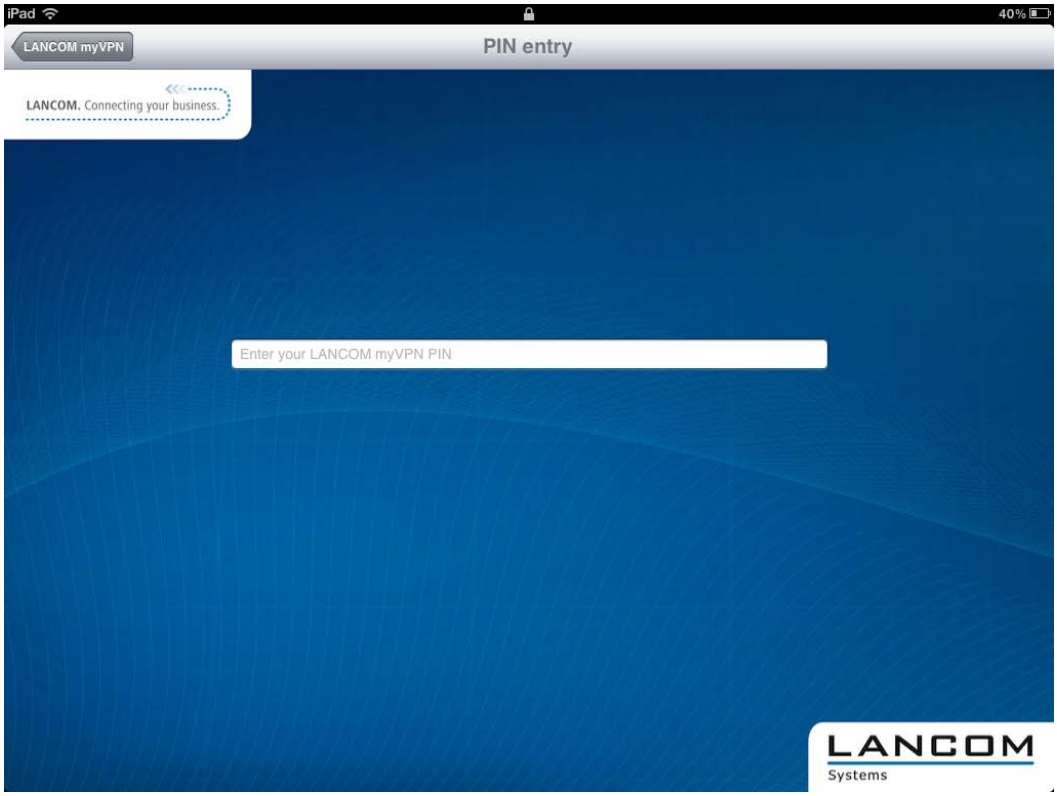
4. Optional: Select the option **Add device manually** to enter the IP address or name of VPN devices that the iOS device can access via an Internet connection (3G or WLAN). In the dialog that follows, enter the IP address or the name of the VPN device and confirm with **Yes**.



5. The app now displays all VPN devices that offer profiles for the LANCOM myVPN app.



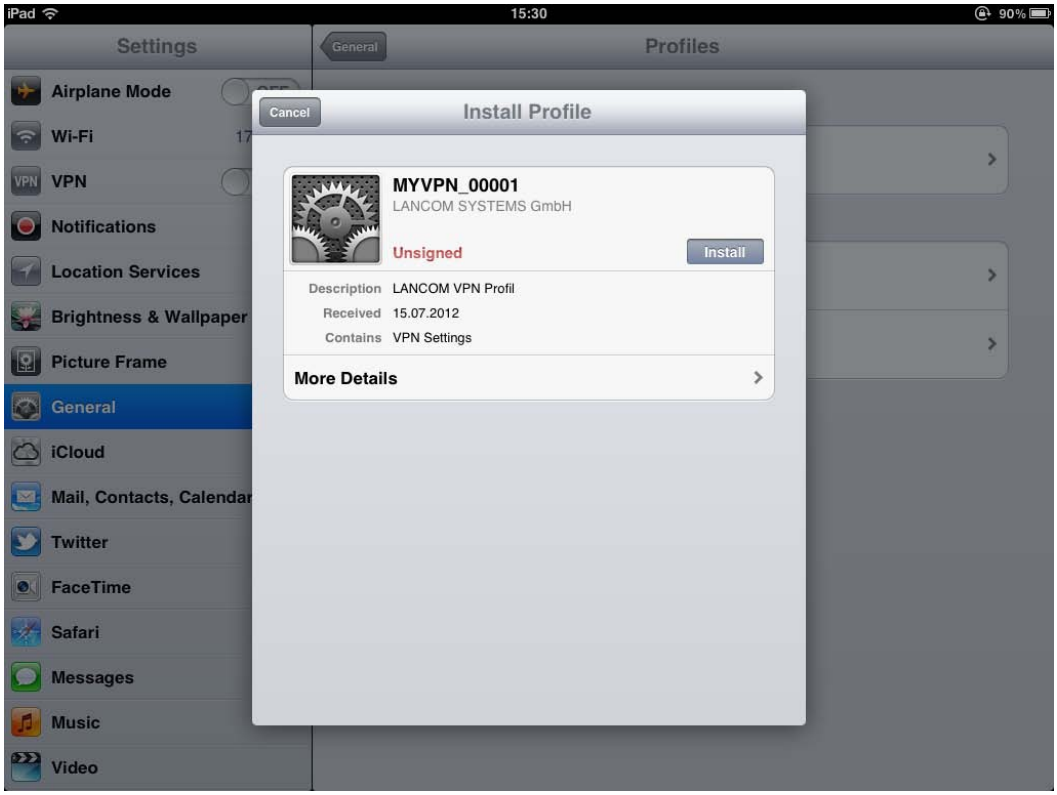

6. Tap on the entry in the list to select the desired VPN device and then enter the PIN required for retrieving the VPN profile.



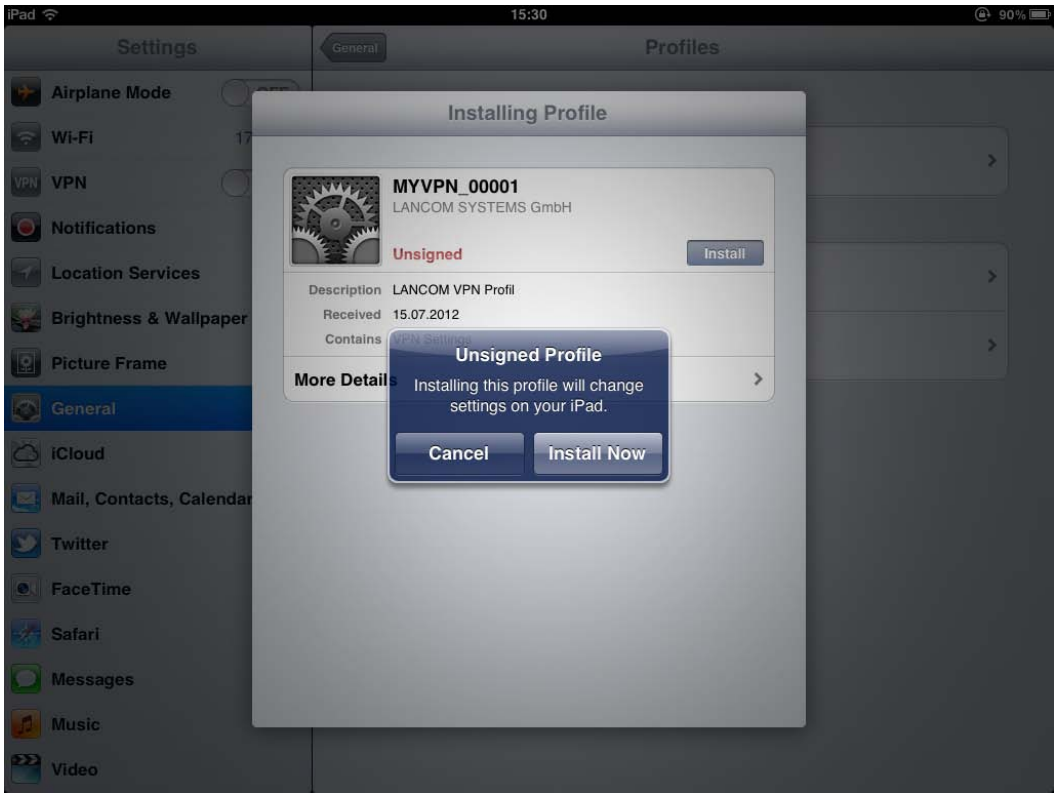
If you enter your PIN incorrectly 5 times, the myVPN module on the LANCOM VPN device will be completely locked for a definite period. In this state, VPN connections remain possible for iOS devices that previously set up their VPN access accounts successfully. However, iOS devices cannot retrieve myVPN profiles from this VPN device so long as the lock is in place. An administrator can re-enable the myVPN module.

7. In the case that the following dialog contains a notice about a non-signed certificate, simply confirm with the **Yes** button.

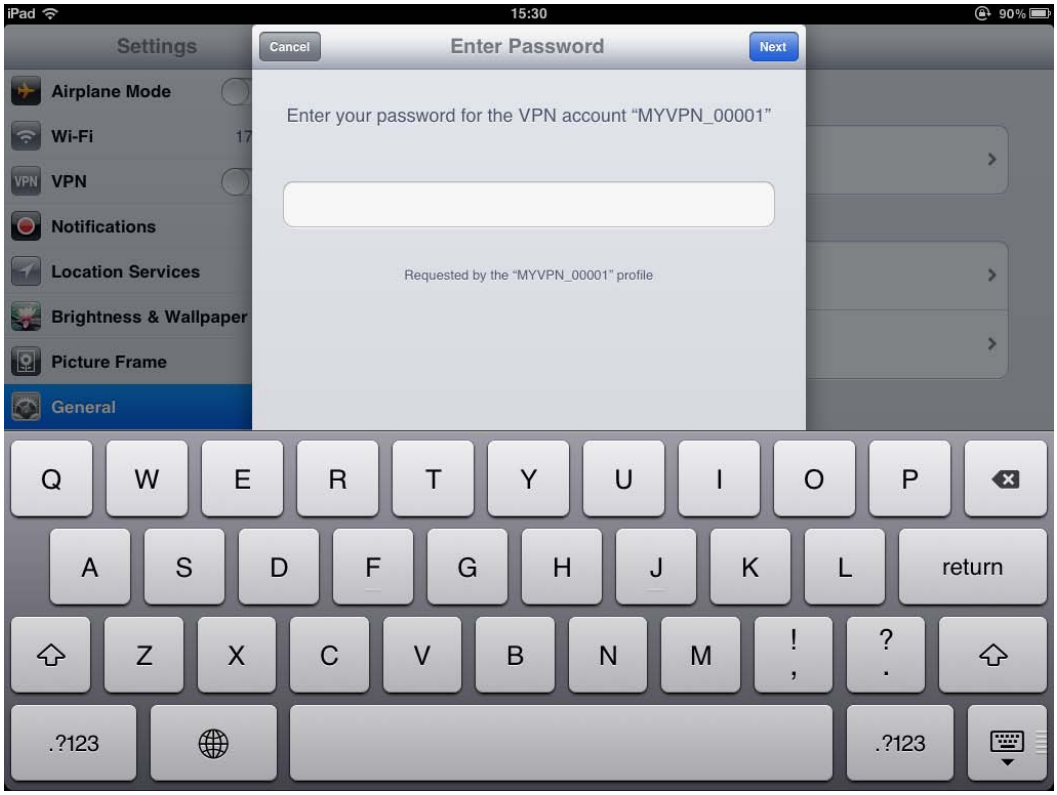
8. In the next dialog, confirm the request to install the profile with the **Install** button.




Confirm the necessary changes to the settings on your iOS device.

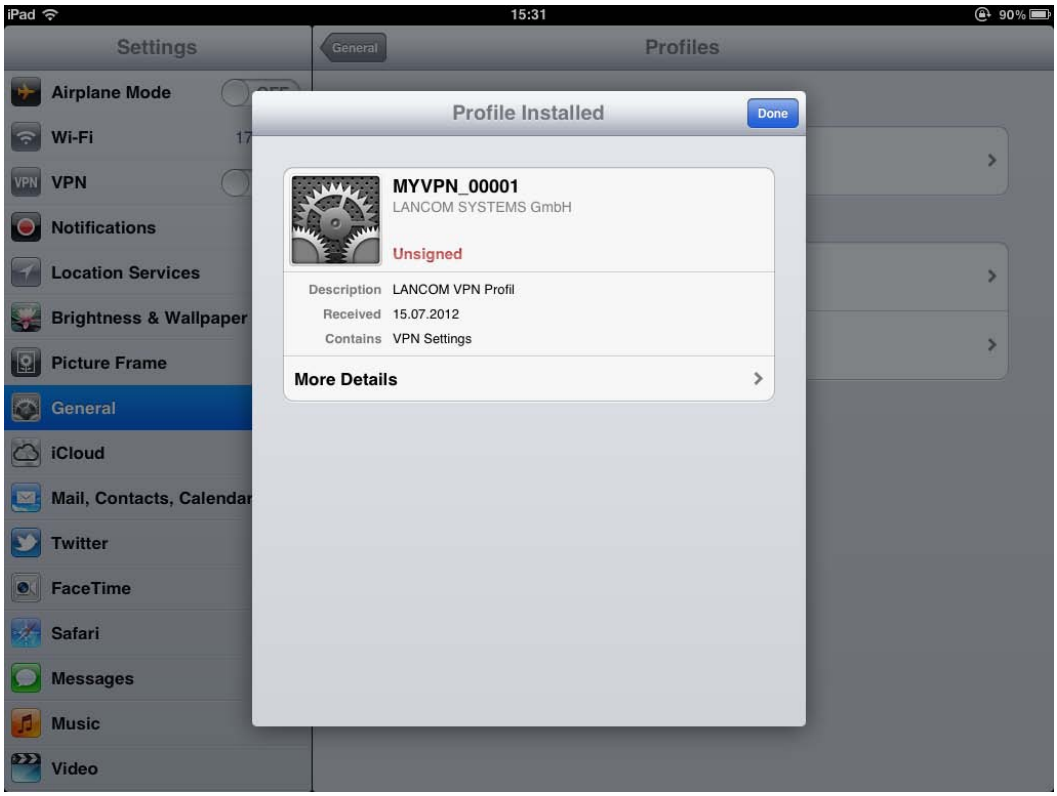


9. The next step of the installation routine is to enter the password for the VPN access account. By default the VPN password is the PIN for the myVPN profile. If you enter the password for the VPN access account here, the iOS device can then establish VPN connections to your company network without requesting a password again. If you leave the box for the VPN password empty, you will be requested for the VPN password every time you connect using the iOS device. Confirm your selection with the **Next** button.

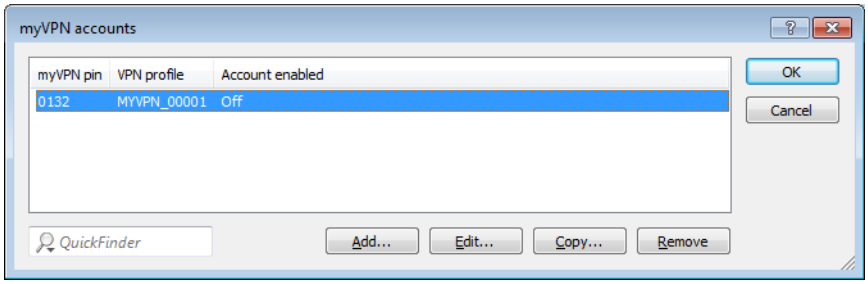



For security reasons we recommend that you do **not** save the VPN-access password on the device. It is a better policy to enter it each time you make the connection.

**10.** The VPN profile is now fully installed on your iOS device and is ready for establishing a VPN connection to your company network. Confirm that the installation has been concluded by clicking on the **Done** button.




Once retrieved from an iOS device, the myVPN profile is disabled on the LANCOM VPN device. You can check your status with LANconfig by navigating to the configuration area **VPN** > **myVPN** and viewing the **myVPN accounts** list:



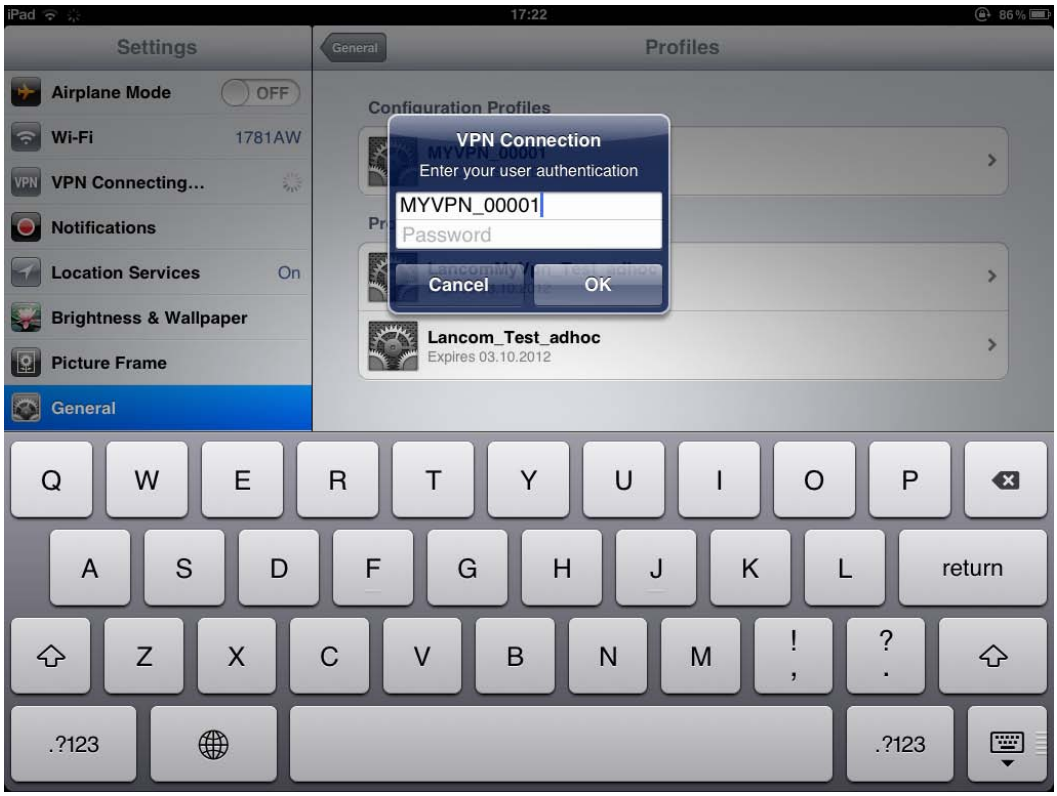

By disabling the myVPN profile, other IOS device are prevented from installing the same myVPN profile and thus using the same VPN access credentials. However, disabling the myVPN profile has no effect on the VPN connection itself.

## Establishing and closing the VPN connection on the iOS device

After you have installed the VPN profile on your iOS device with the LANCOM myVPN app, you establish and close the VPN connection to your company network as follows:

**1.** Activate the VPN tunnel in the configuration area **Settings** under the option **VPN**.

2. The following dialog already displays the user name from the myVPN profile. Enter the password for the VPN connection and confirm with **OK**.




By default, the password for the VPN connection is the PIN for the myVPN profile.

The password is already displayed if you entered the password for the VPN connection while installing the myVPN profile. In this case the connection is established directly without showing this window.

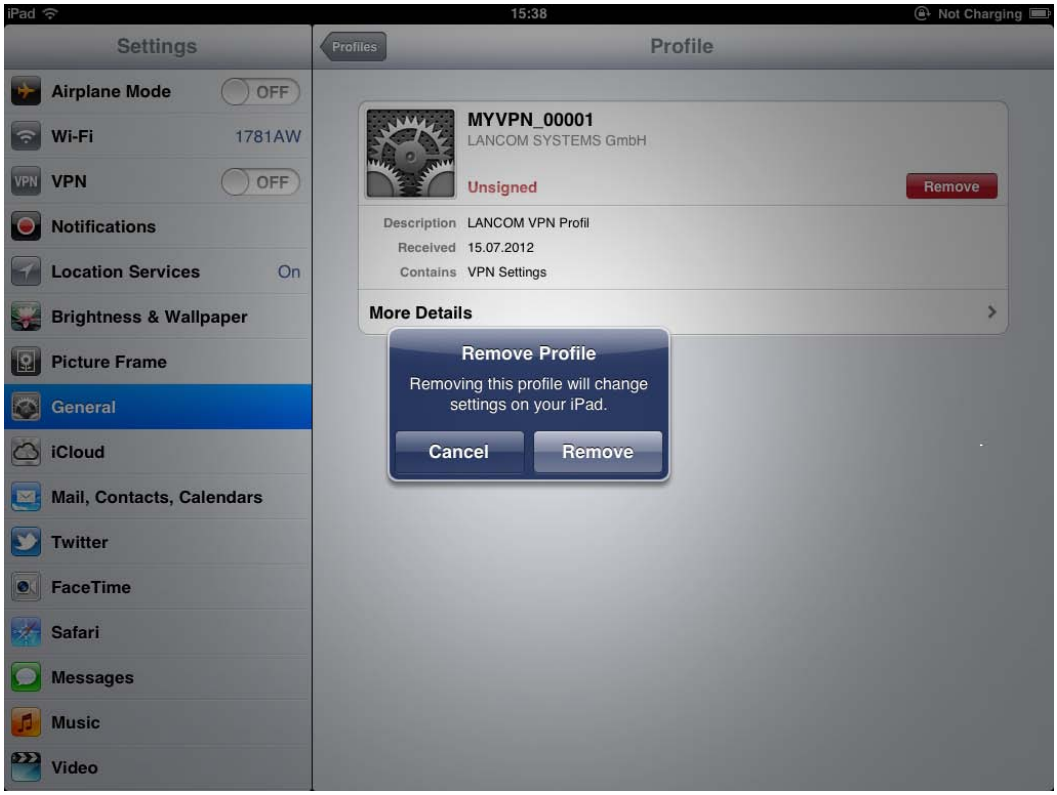
3. Close the VPN connection on your iOS device in the configuration area **Settings** under the option **VPN**.

## Deleting a VPN profile from the iOS device

To delete the VPN profile you can use the LANCOM myVPN app:

1. Navigate to **Settings** > **General** > **Profiles** to the list of available profiles on your iOS device.

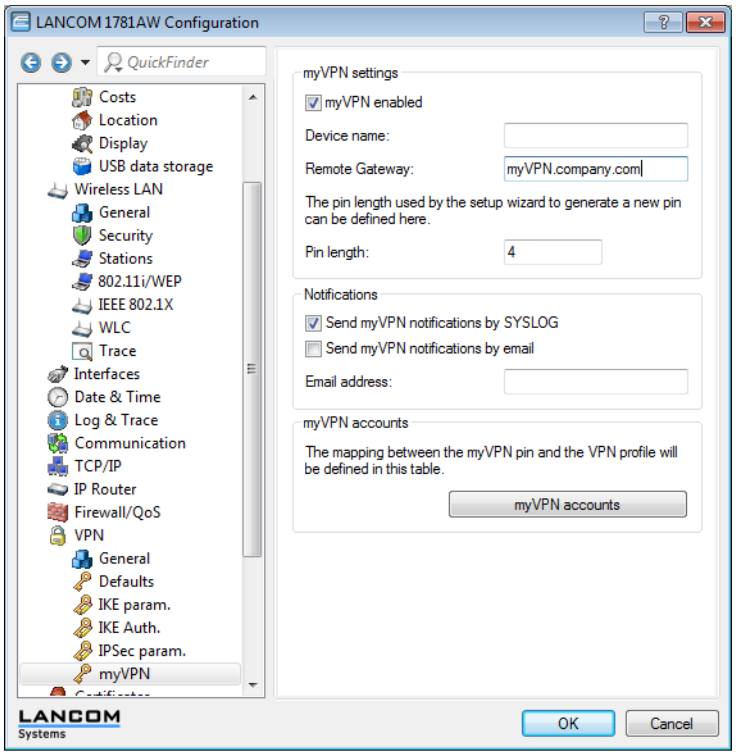
2. Select the profile, click on **Remove** and confirm the action again in the next dialog with **Remove**.



## Additions to LANconfig

### Configuring the LANCOM myVPN app

Under **VPN** > **myVPN** you can manually adjust the settings for the LANCOM myVPN app.




Check the **myVPN enabled** box to allow the LANCOM myVPN app to load a VPN profile.

Specify the **Device name** here if a trusted SSL certificate is installed on this device. This ensures that the IOS device does not issue a warning about an untrusted certificate when the profile is retrieved.

Use the field **Remote gateway** to enter the WAN address of the router or its name as resolved by public DNS servers. If the myVPN app cannot find the remote gateway by means of automatic search, you should enter this gateway into the myVPN app.

The item **PIN length** sets the length of new PINs generated by the setup wizard (default = 4).

Activate the option **Send myVPN notifications by SYSLOG** to send messages about the myVPN app to SYSLOG.

Activate the option **Send myVPN notifications by e-mail** to send messages about the myVPN app to a specified e-mail address.

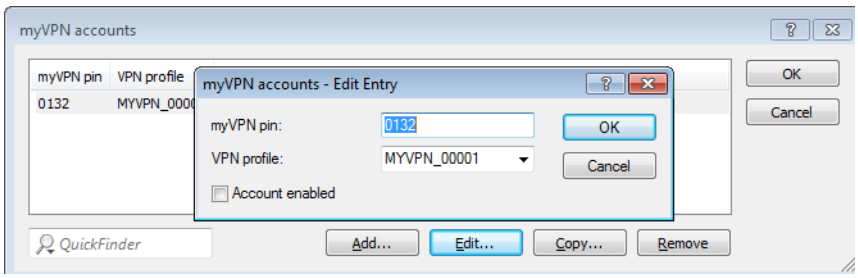
These messages include:

- Successful profile retrieval
- Disabled login for LANCOM myVPN due to too many failed attempts
- Re-enabling of the login (irrespective of whether this is done manually or if the specified time period has expired)

Specify the **E-mail address** to which messages about the myVPN app are to be sent.

The transmission of e-mails must be enabled in the VPN device.

The item **myVPN accounts** is used to assign the myVPN PIN to the VPN profiles.




Here you determine which **VPN profile** is to supply data to the myVPN app upon retrieval of the profile.

You set the myVPN PIN that is to be entered when the LANCOM myVPN app is to retrieve the profile.

**Security notice:** As a security feature of myVPN, the repeated incorrect entry of a PIN causes the device to temporarily disable profile retrieval, and a notification is sent by SYSLOG and by e-mail. After five failed attempts, the device disables profile retrieval for 15 minutes. Five more failed attempts, profile retrieval is disabled for a day. In case of further failed attempts, the time periods vary. Manually releasing this lock resets the corresponding counter. Please also be aware that an attempt to retrieve the profile while access is disabled (e. g. when the profile has previously been retrieved successfully) is also considered by the device to be a failed attempt.

You activate the profile by checking the **Account enabled** box.

After the profile has been retrieved successfully, the device automatically disables the corresponding profile to avoid the repeated download by another device.

Once you save these settings to the device, the myVPN module is active on the selected VPN device. On your iOS device, you can now start the LANCOM myVPN app and enter the PIN to retrieve the VPN profile.

## Additions to the menu system

### myVPN

The "myVPN" function is used by devices with the iOS operating system. These are able to automatically retrieve VPN profiles and the internal iOS VPN client is configured to suit. At the router's end, you must configure the VPN profile and the parameters for myVPN. With the aid of the LANCOM myVPN app and a suitable PIN, you can configure your device for VPN dial-in in just a few easy steps.

More information on the myVPN app is available on the *LANCOM homepage*.

**SNMP ID:**

2.19.28

**Telnet path:**

**Telnet path:Setup** > **Vpn** > **myVPN**

### Operating

Use this switch to activate myVPN for this device.

**SNMP ID:**

2.19.28.1

**Telnet path:**

**Telnet path:Setup** > **Vpn** > **myVPN**

**Possible values:**

Yes

No

**Default:**

No

**PIN length**

This item sets the length of new PINs generated by the setup wizard.

**SNMP ID:**

2.19.28.2

**Telnet path:**

**Telnet path:Setup** > **Vpn** > **myVPN**

**Possible values:**

Maximum length: 12

Minimum length: 4

**Default:**

4

**Device hostname**

Enter the device name here if a trustworthy SSL certificate is installed on this device. This ensures that the IOS device does not issue a warning about an untrusted certificate when the profile is retrieved.

**SNMP ID:**

2.19.28.3

**Telnet path:**

**Telnet path:Setup** > **Vpn** > **myVPN**

**Possible values:**

Max. 31 characters from

0-9

a-z

A-Z

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

**Default:**

Blank

**Mapping**

This table assigns the myVPN PIN to the VPN profiles.

**SNMP ID:**

2.19.28.4

**Telnet path:**

**Telnet path:Setup** > **Vpn** > **myVPN**

**PIN**

Define here the PIN to be entered into the myVPN app in order to retrieve the profile.

The myVPN setup wizard also uses this PIN in the PPP list for the actual VPN login. If you change your PIN here, you must also change it in LANconfig under **Communication** > **Protocols** > **PPP list** if you wish to avoid having a different PIN.

**Security notice:** As a security feature of myVPN, the repeated incorrect entry of a PIN causes the device to temporarily disable profile retrieval, and a notification is sent by SYSLOG and by e-mail. After three failed attempts, the device disables profile retrieval for 15 minutes. A further three failed attempts cause the profile retrieval to be disabled for 24 hours. In case of further failed attempts, the time periods vary. Manually releasing this lock resets the corresponding counter. Please also be aware that an attempt to retrieve the profile while access is disabled (e. g. when the profile has previously been retrieved successfully) is also considered by the device to be a failed attempt.

**SNMP ID:**

2.19.28.4.1

**Telnet path:**

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

**Possible values:**

Max. 12 digits from 1234567890

**Default:**

Blank

### VPN profile

Here you can determine which VPN profile is to supply data to the myVPN app upon retrieval of the profile.

**SNMP ID:**

2.19.28.4.2

**Telnet path:**

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

**Possible values:**

16 characters from

0-9

a-z

A-Z

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

**Default:**

Blank

### Operating

This switch activates the profile retrieval by means of the myVPN app. After the profile has been retrieved successfully, the device automatically disables the corresponding profile to avoid the repeated download by another device.

**SNMP ID:**

2.19.28.4.3

**Telnet path:**

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

**Possible values:**

No

Yes

**Default:**

No

### Re-enable login

The command `do re-enable-login` releases the lock that was caused by failed attempts. If required, this generates a message about the re-enabling via SYSLOG or e-mail.

**SNMP ID:**

2.19.28.5

**Telnet path:**

**Telnet path:Setup** > **Vpn** > **myVPN**

### E-mail notification

Activate this option to send messages about the myVPN app to a specific e-mail address. These messages include:

- Successful profile retrieval
- Disabled login for myVPN due to too many failed attempts
- Re-enabling of the login (irrespective of whether this is done manually or if the specified time period has expired)

**SNMP ID:**

2.19.28.6

**Telnet path:**

**Telnet path:Setup** > **Vpn** > **myVPN**

**Possible values:**

No

Yes

**Default:**

No

### E-mail address

Specify the e-mail address to which messages about the myVPN app are to be sent.

**SNMP ID:**

2.19.28.7

**Telnet path:**

**Telnet path:Setup** > **Vpn** > **myVPN**

**Possible values:**

Max. 63 characters from

0-9

a-z

A-Z

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

**Default:**

Blank

### Syslog

Activate this option to send messages about the myVPN app to SYSLOG. These messages include:

- Successful profile retrieval
- Disabled login for myVPN due to too many failed attempts
- Re-enabling of the login (irrespective of whether this is done manually or if the specified time period has expired)

**SNMP ID:**

2.19.28.8

**Telnet path:**

**Telnet path:Setup** > **Vpn** > **myVPN**

**Possible values:**

No

Yes

**Default:**

No

### Remote gateway

Here you enter the WAN address of the router or its name as resolved by public DNS servers. If the myVPN app cannot find the remote gateway by means of automatic search, you should enter the gateway into the app as well.

**SNMP ID:**

2.19.28.9

**Telnet path:**

**Telnet path:Setup** > **Vpn** > **myVPN**

**Possible values:**

Max. 63 characters from

0-9

a-z

A-Z

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

**Default:**

Blank

# Index

## M



## W