APPLICATION NOTE 003

WeConnect

Industrial Remote Access – Made Easy

Table of Contents

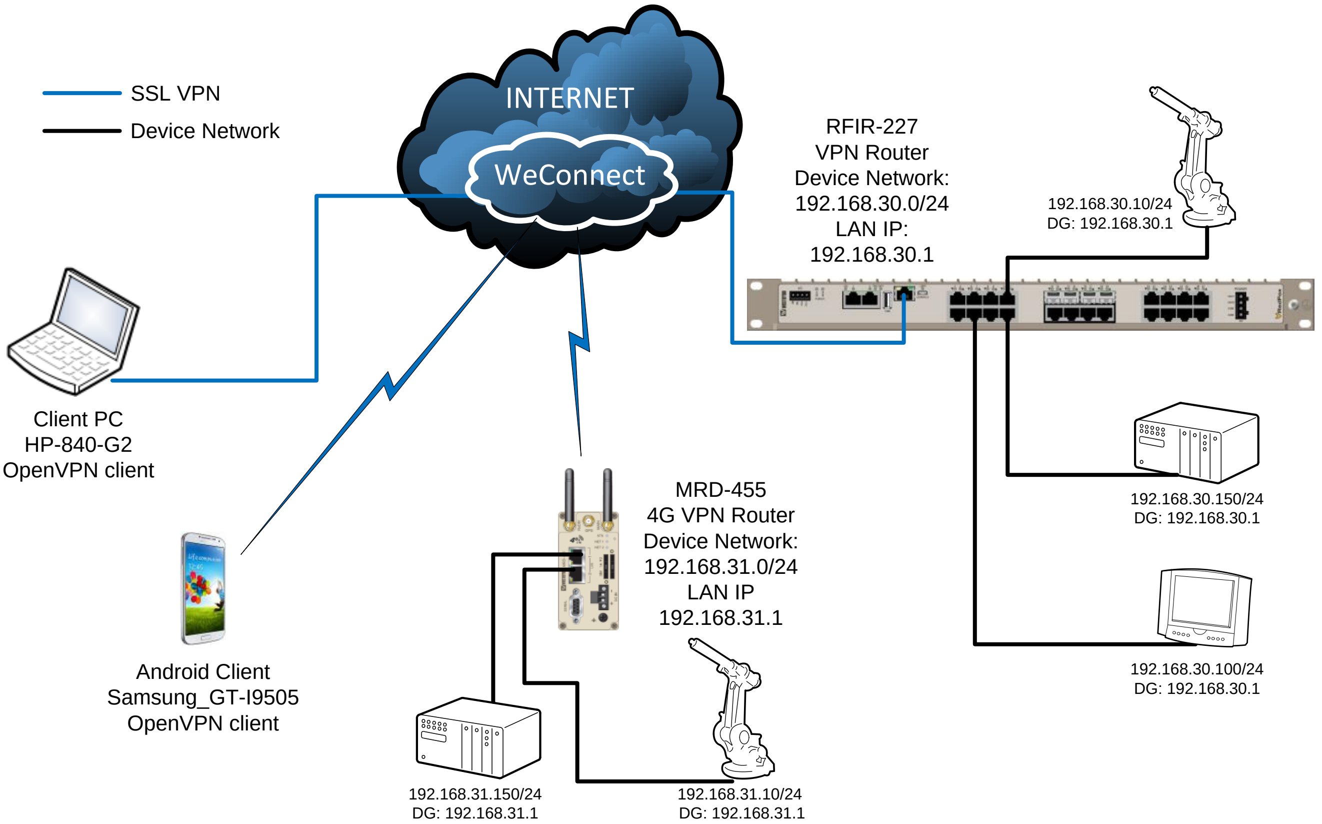
Application Note Network Layout

This Application Note shows how to use the Westermo WeConnect service to access remote sites without having public IP-addresses or any other connectivity servers.

Background

WeConnect controls exactly which units are allowed to access any resources within a customer network.
It securely interconnect Clients (PCs, Smartphones or Tablets using VPN software) and Nodes (WeOS or MRD VPN routers with connected Device Networks).
Nodes and Clients are placed in WeConnect Secure Networks, the Secure Networks control how Clients and Nodes are allowed to connect to each other.
Both Clients and Nodes use secure SSL VPNs to safely access WeConnect over the unsecure Internet.
No public IP-addresses are needed on either Clients or Nodes, only an access to Internet is required. This dramatically decreases the risk of unwanted Internet traffic hitting the remote networks.
All WeOS products (with VPN functionality) as well as Westermo MRD 3G/4G and ADSL units can be used with WeConnect.

All configuration in this Application Note is made using WeOS version 4.17.0 and MRD software version 1.7.1.10.B00680.
SSL software OpenVPN client version 2.3.4 for MS Windows 7 64-bit Professional.
Android version 5.0.1, Apple iOS 9 and OpenVPN Connect app version 1.1.16.

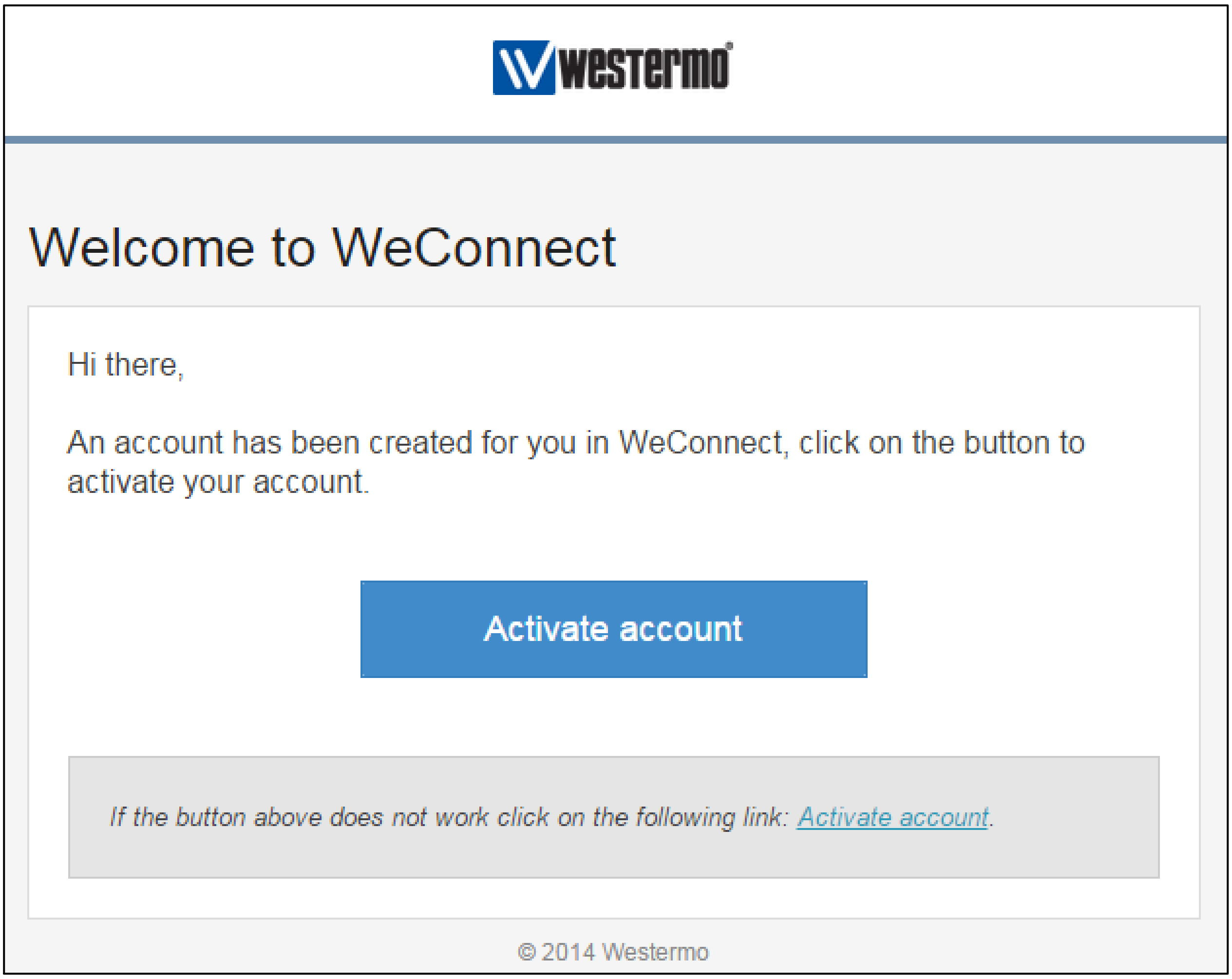


The WeConnect Portal

Setup an Account

When a WeConnect account has been ordered an e-mail with an activation link will be sent out.

1. In the e-mail received click the *Activate account* link to get started.



Welcome to WeConnect

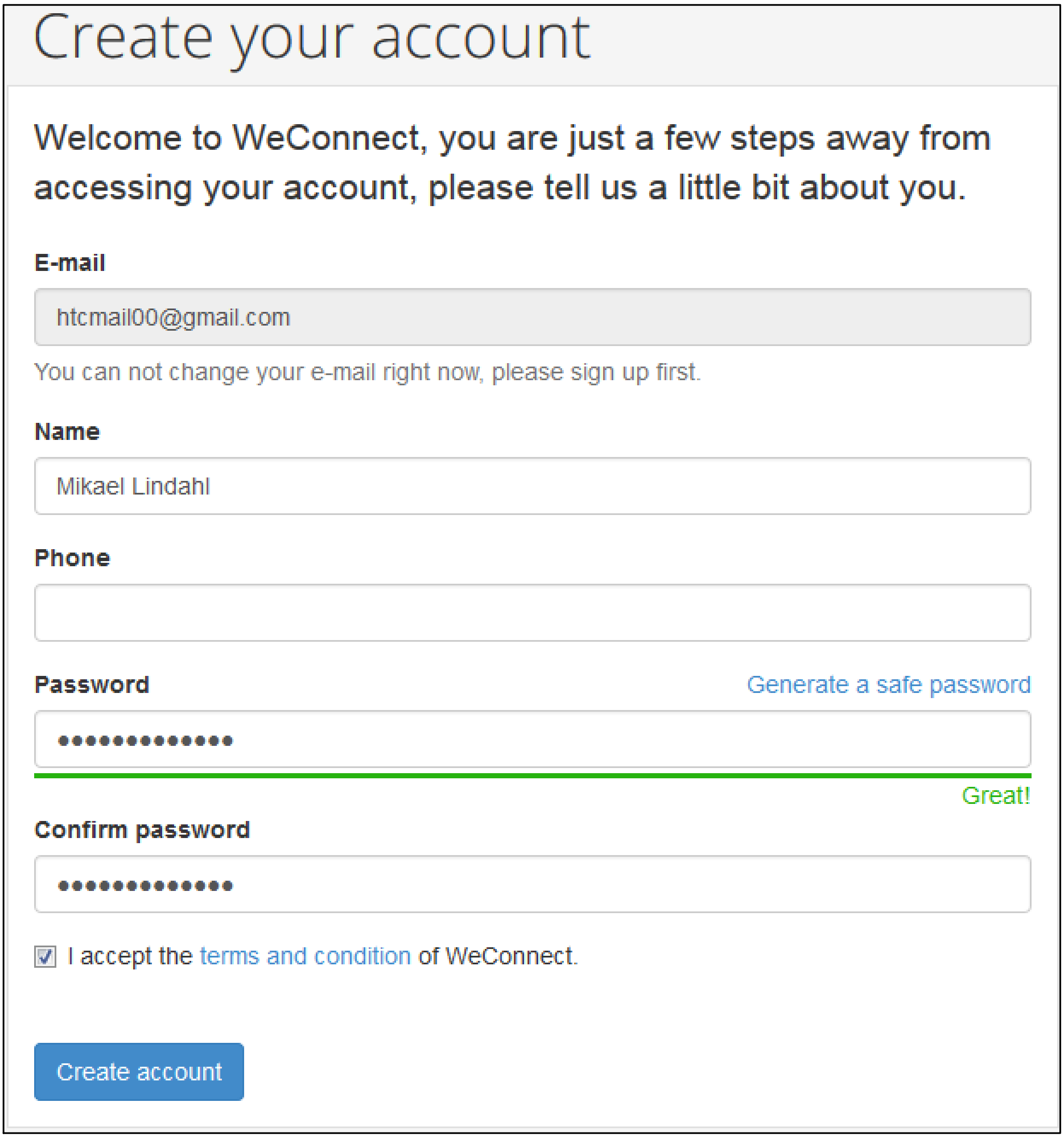
Hi there,

An account has been created for you in WeConnect, click on the button to activate your account.

If the button above does not work click on the following link: Activate account.

© 2014 Westermo

2. Fill in the account form, set a secure password and read through the terms and conditions. Activate the account by clicking Create account.



Create your account

Welcome to WeConnect, you are just a few steps away from accessing your account, please tell us a little bit about you.

E-mail

htcmail00@gmail.com

You can not change your e-mail right now, please sign up first.

Name

Mikael Lindahl

Phone

Password

●●●●●●●●●●●●●

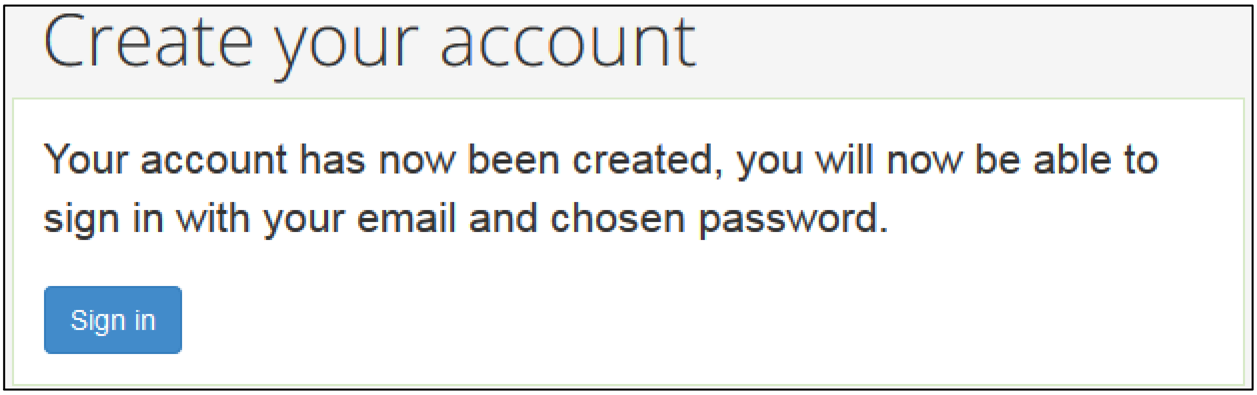
Great!

Confirm password

●●●●●●●●●●●●●

☑ I accept the terms and condition of WeConnect.

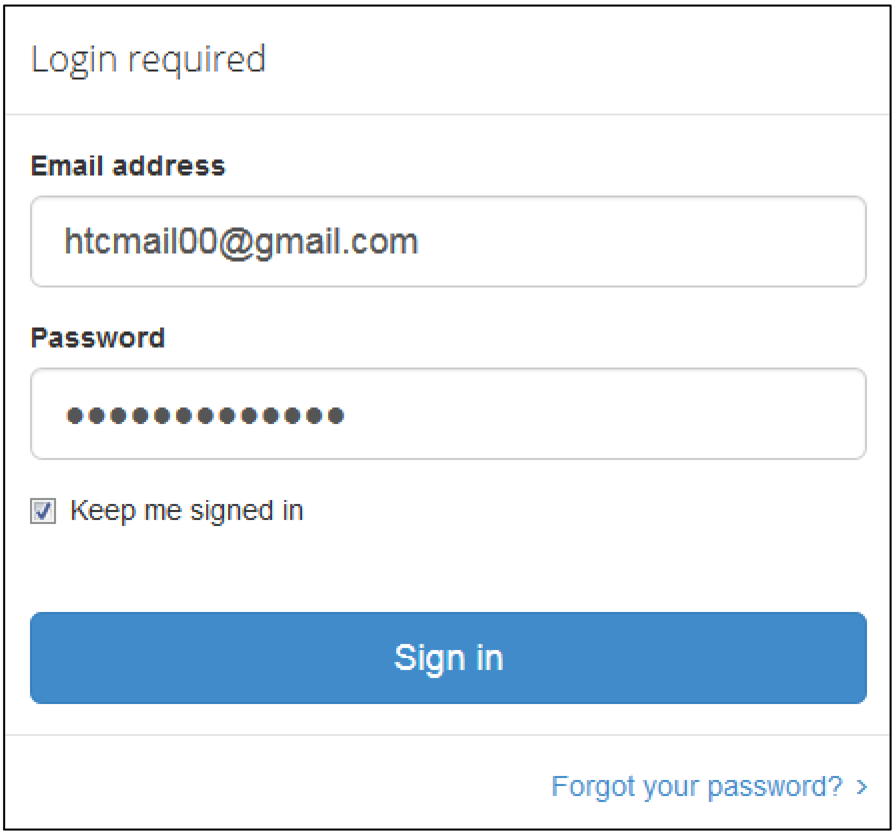
3. Click sign in to get started.



Create your account

Your account has now been created, you will now be able to sign in with your email and chosen password.

4. Sign in using the e-mail address and password created for the account.



Login required

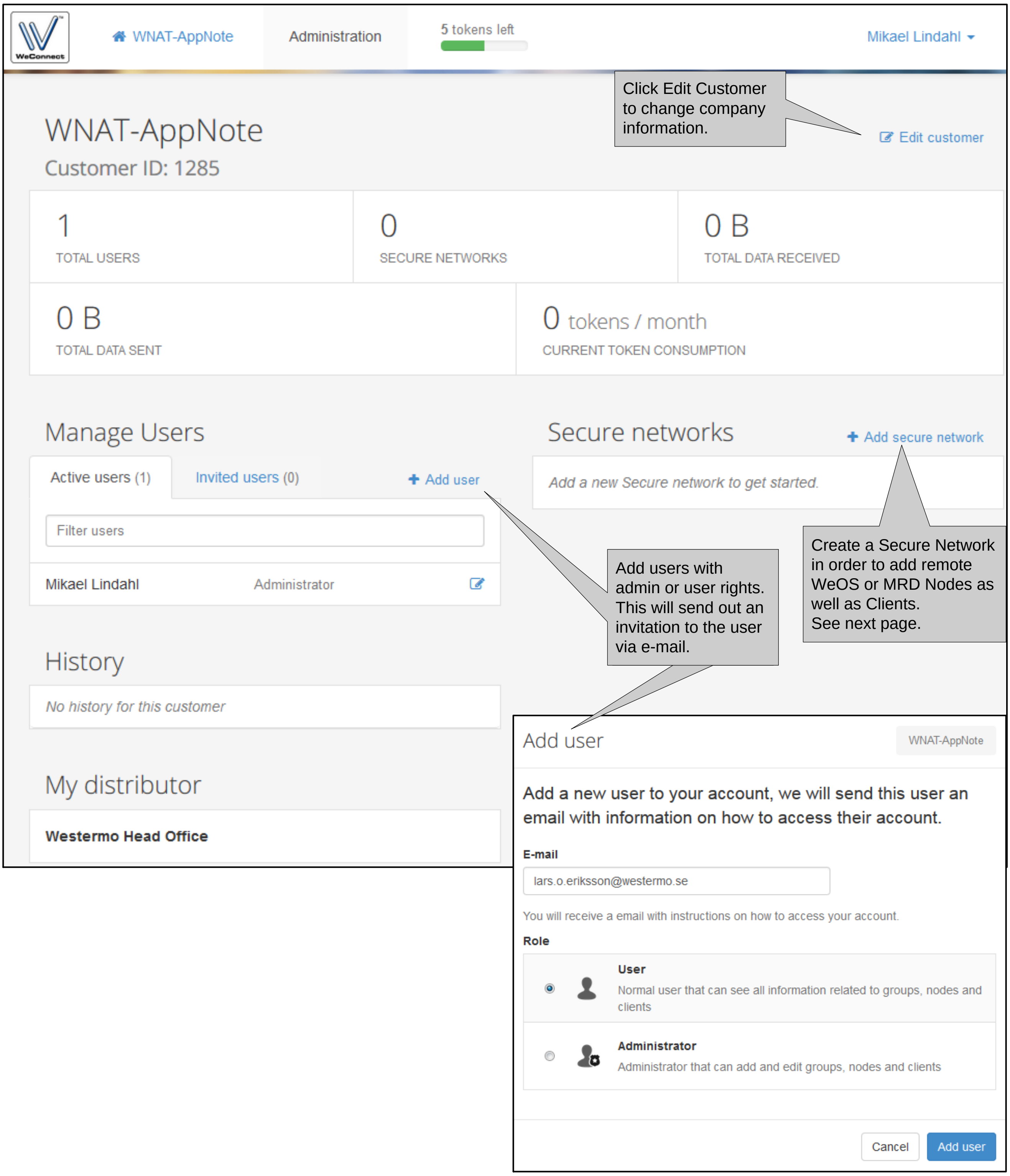
Email address: htcmail00@gmail.com

Password: ●●●●●●●●●●●●●

☑ Keep me signed in

Account Administration

The WeConnect portal is located at https://weconnect.westermo.com.
When logging in for the first time the user will always be forwarded to the Administration screen as no Secure Network has yet been defined.
After a Secure Network is configured the user will then be directed directly to the status screen of that network after log in.



Click Edit Customer to change company information.

WNAT-AppNote
Customer ID: 1285

1 TOTAL USERS	0 SECURE NETWORKS	0 B TOTAL DATA RECEIVED
0 B TOTAL DATA SENT	0 tokens / month CURRENT TOKEN CONSUMPTION	

Manage Users

Active users (1) | Invited users (0)

Filter users

Mikael Lindahl	Administrator

Secure networks

Add a new Secure network to get started.

Create a Secure Network in order to add remote WeOS or MRD Nodes as well as Clients.
See next page.

Add users with admin or user rights. This will send out an invitation to the user via e-mail.

History

No history for this customer

My distributor

Westermo Head Office

Add user — WNAT-AppNote

Add a new user to your account, we will send this user an email with information on how to access their account.

E-mail
lars.o.eriksson@westermo.se

You will receive a email with instructions on how to access your account.

Role

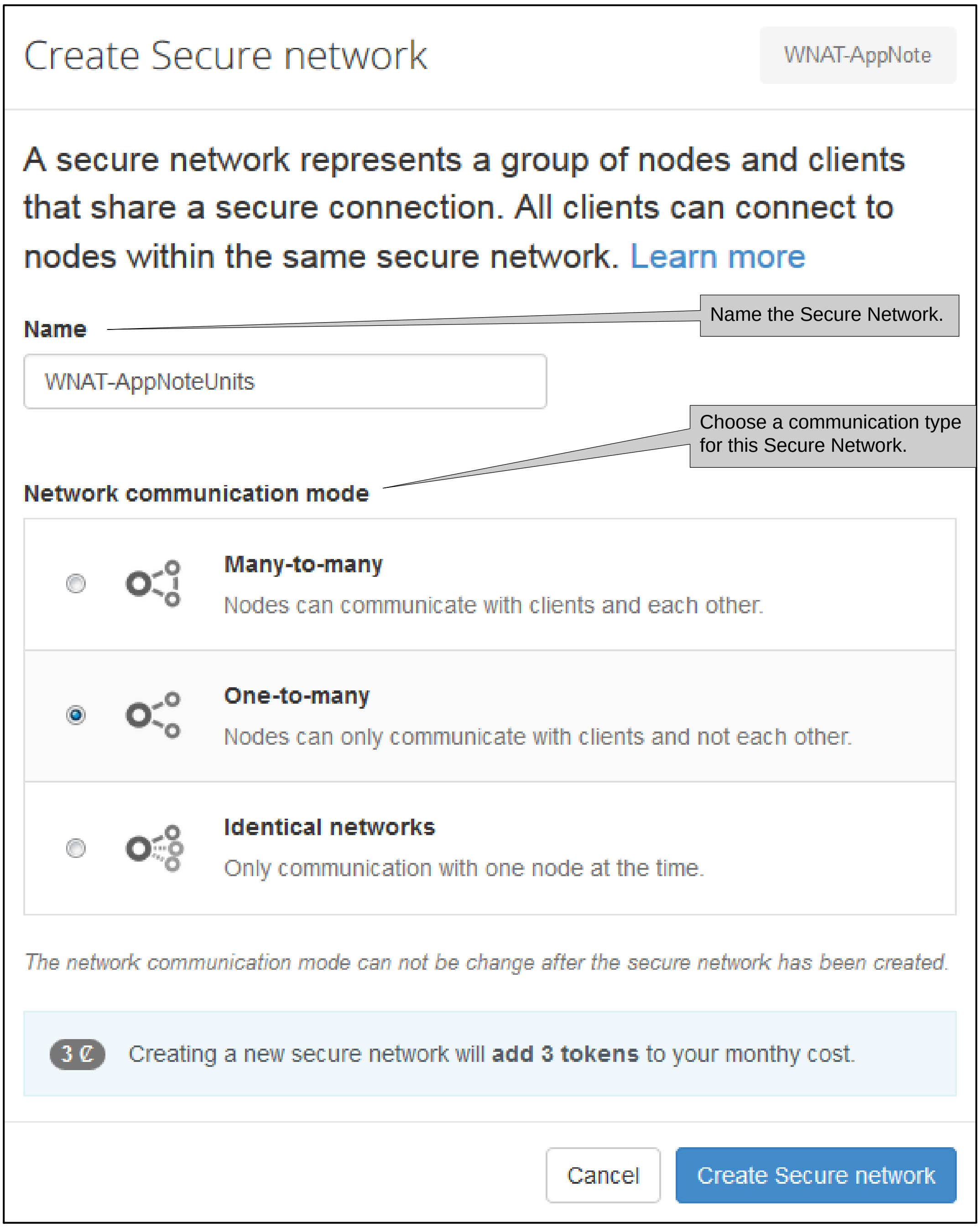
● **User**
Normal user that can see all information related to groups, nodes and clients

○ **Administrator**
Administrator that can add and edit groups, nodes and clients

WeConnect Secure Network Creation

Create a WeConnect Secure Network for the units, Nodes and Clients, that are allowed to communicate with each other.

Many-to-many means that the remote sites can communicate with Clients and directly between each other.
In the *One-to-many* scenario the remote sites can not communicate with each other, only with Clients.
With *Identical networks* all Device Networks are able to have the same LAN subnet. Which Device Network to connect to is controlled from the WeConnect Portal.
This Application Note will first show a setup based on a *One-to-many* application (*Many-to-many* is basically the same as *One-to-many*) and then an Identical Networks setup.



Create Secure network

WNAT-AppNote

A secure network represents a group of nodes and clients that share a secure connection. All clients can connect to nodes within the same secure network. Learn more

Name: WNAT-AppNoteUnits

Name the Secure Network.

Network communication mode

Choose a communication type for this Secure Network.

○ **Many-to-many**
Nodes can communicate with clients and each other.

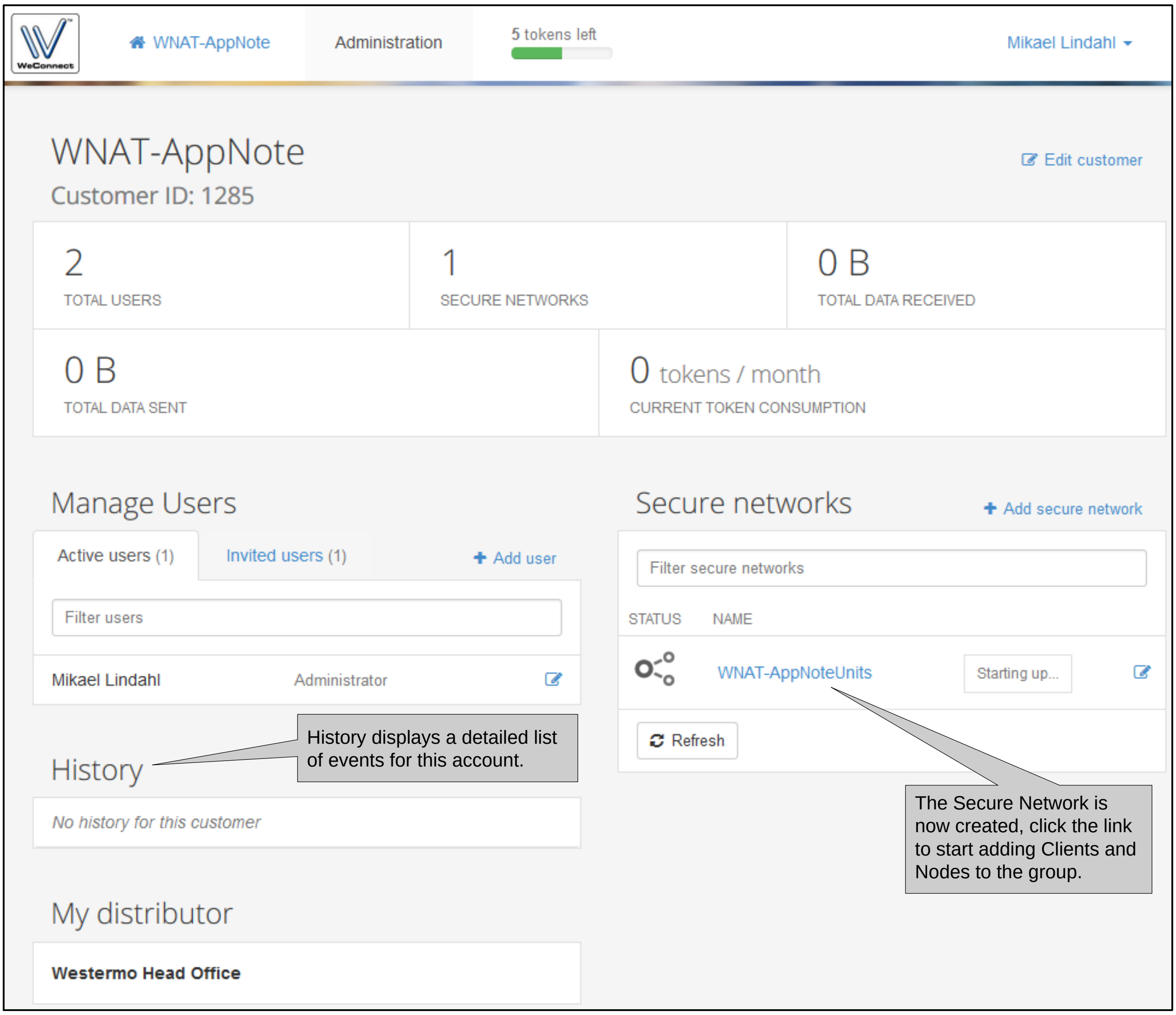
● **One-to-many**
Nodes can only communicate with clients and not each other.

○ **Identical networks**
Only communication with one node at the time.

The network communication mode can not be change after the secure network has been created.

3 Ȼ Creating a new secure network will **add 3 tokens** to your monthy cost.

The Secure Network will now appear in the Administration view of the WeConnect portal.



WNAT-AppNote

Customer ID: 1285

2 TOTAL USERS	1 SECURE NETWORKS	0 B TOTAL DATA RECEIVED
0 B TOTAL DATA SENT	0 tokens / month CURRENT TOKEN CONSUMPTION	

Manage Users

Active users (1) Invited users (1)

Filter users

Mikael Lindahl Administrator

History

History displays a detailed list of events for this account.

No history for this customer

My distributor

Westermo Head Office

Secure networks

Filter secure networks

STATUS	NAME	
	WNAT-AppNoteUnits	Starting up...

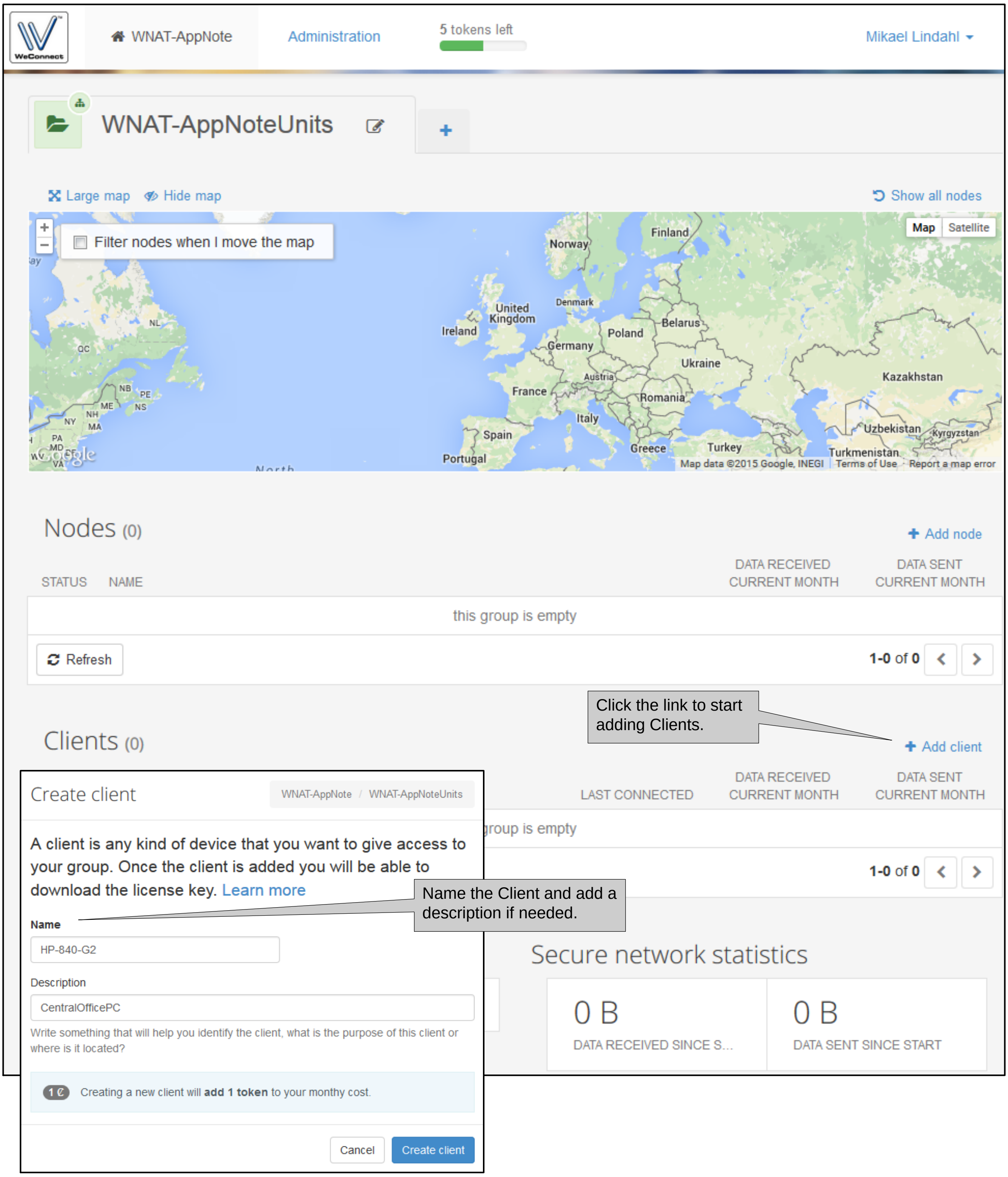
The Secure Network is now created, click the link to start adding Clients and Nodes to the group.

Adding Clients

Clients are PCs, Smartphones or Tablets running an SSL VPN software that setup a secure connection to WeConnect.

Add a WeConnect PC Client

Add a Client by clicking *Add client* in the WeConnect portal.



this group is empty

group is empty

Click the link to start adding Clients.

A client is any kind of device that you want to give access to your group. Once the client is added you will be able to download the license key. Learn more

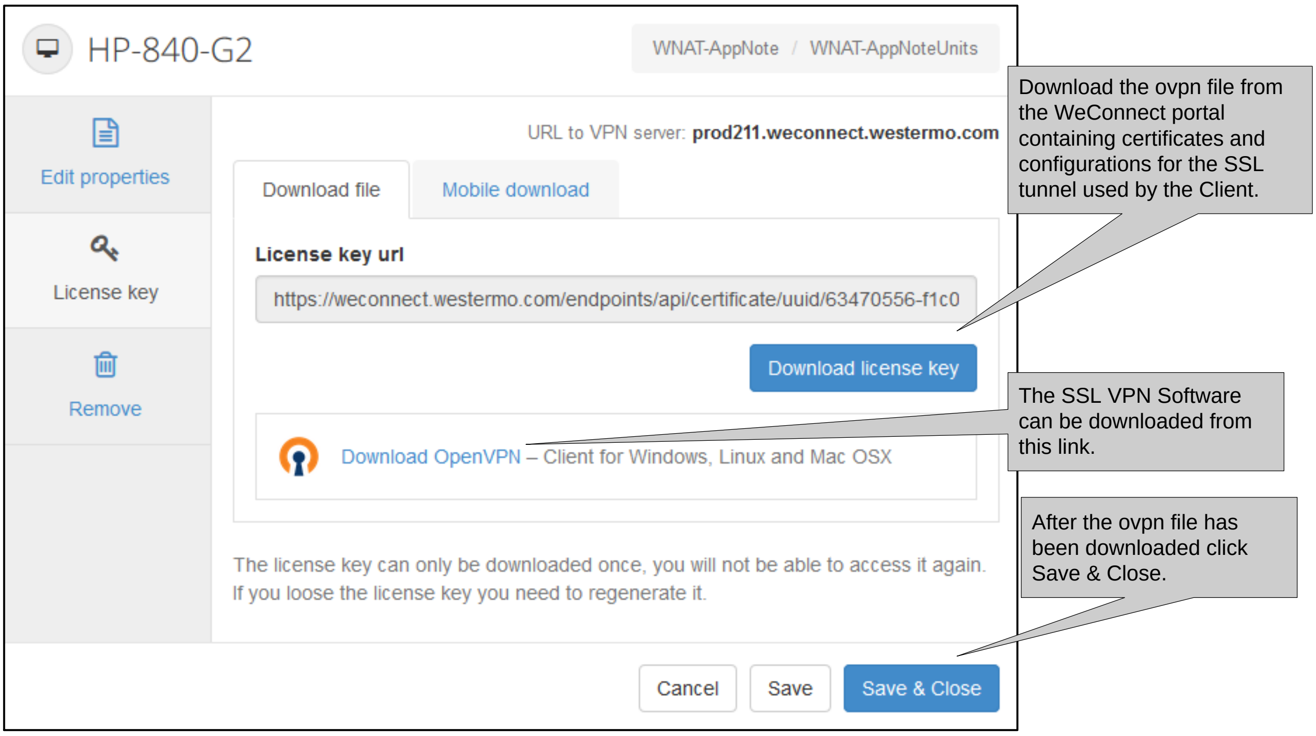
Name the Client and add a description if needed.

Name: HP-840-G2

Description: CentralOfficePC

Write something that will help you identify the client, what is the purpose of this client or where is it located?

1 Creating a new client will **add 1 token** to your monthy cost.



URL to VPN server: **prod211.weconnect.westermo.com**

License key url

https://weconnect.westermo.com/endpoints/api/certificate/uuid/63470556-f1c0

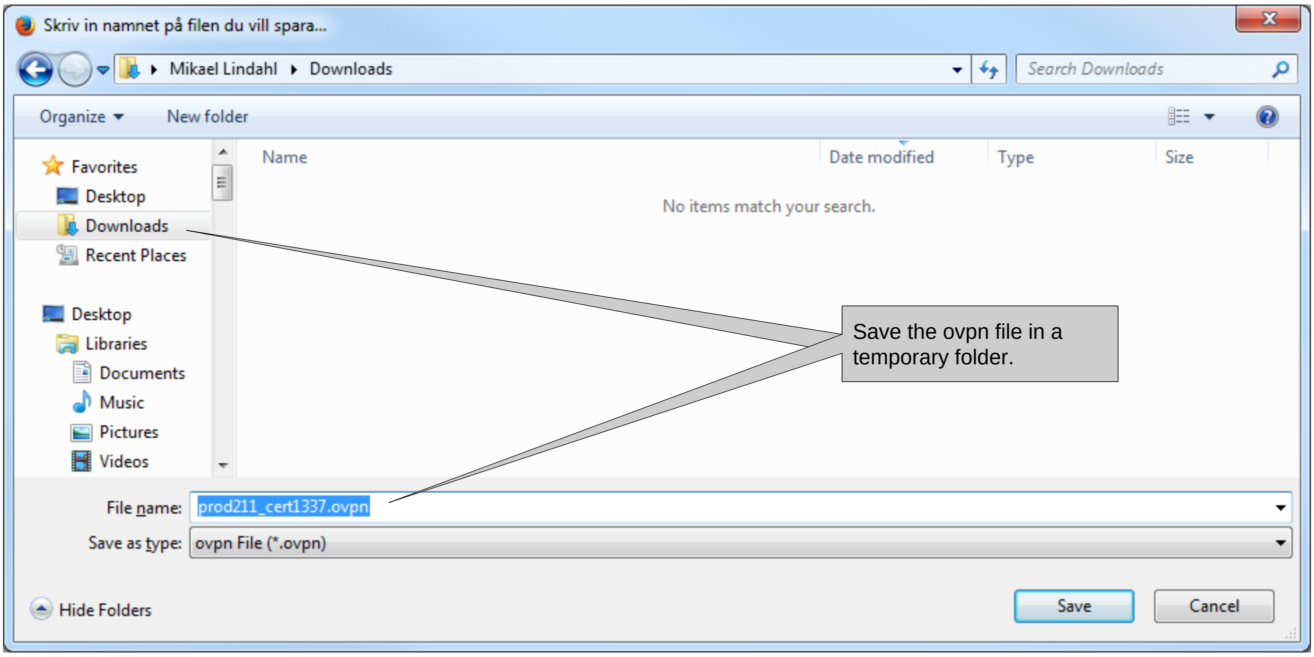
Download OpenVPN – Client for Windows, Linux and Mac OSX

The license key can only be downloaded once, you will not be able to access it again. If you loose the license key you need to regenerate it.

Download the ovpn file from the WeConnect portal containing certificates and configurations for the SSL tunnel used by the Client.

The SSL VPN Software can be downloaded from this link.

After the ovpn file has been downloaded click Save & Close.



No items match your search.

File name: prod211_cert1337.ovpn

Save as type: ovpn File (*.ovpn)

Save the ovpn file in a temporary folder.

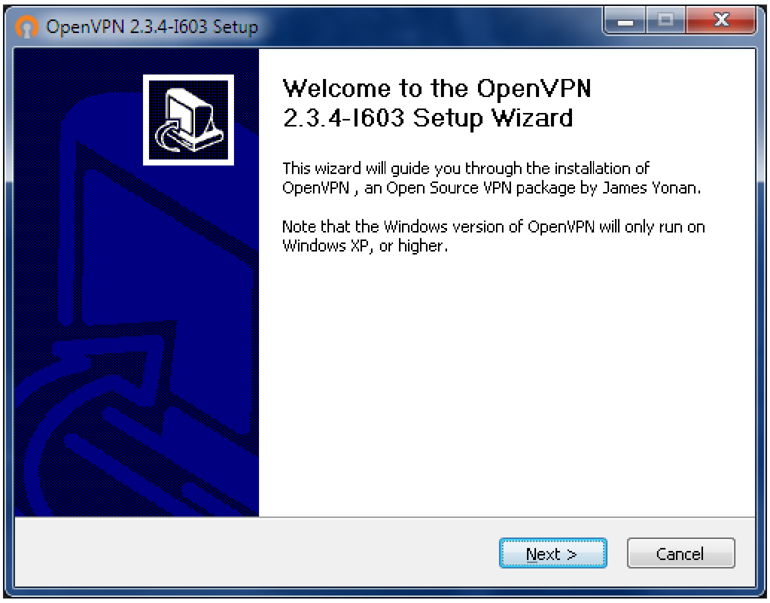
Now the Client is added to the WeConnect portal and the configuration and certificates file for a SSL VPN software client is downloaded.

Configure an SSL VPN Software Client

There are many SSL VPN softwares on the market but this Application Note will show how to connect using the OpenVPN software client.

1. Start by downloading the latest client software from the WeConnect Portal (see the previous page) or directly from the OpenVPN homepage:
https://openvpn.net/index.php/open-source/downloads.html

2. Choose the right client version for the PC operating system it shall be run on and install it.

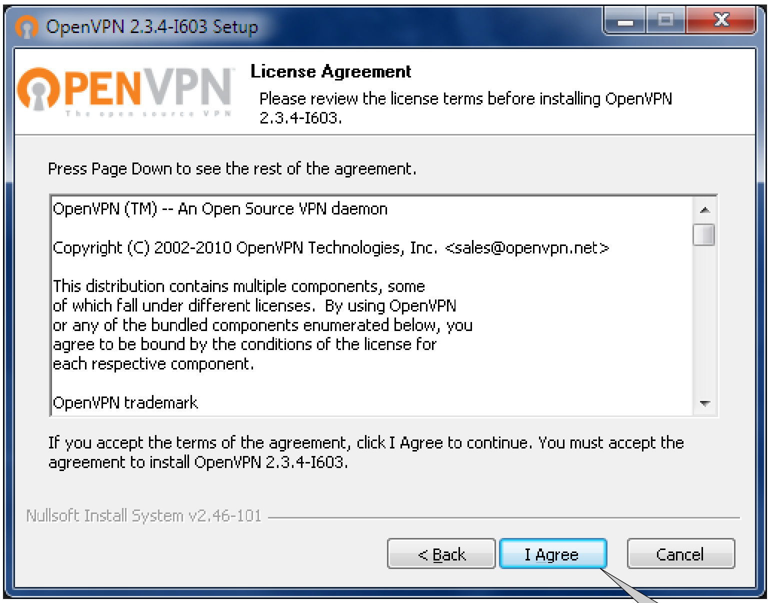


OpenVPN 2.3.4-I603 Setup

Welcome to the OpenVPN 2.3.4-I603 Setup Wizard

This wizard will guide you through the installation of OpenVPN , an Open Source VPN package by James Yonan.

Note that the Windows version of OpenVPN will only run on Windows XP, or higher.



OpenVPN 2.3.4-I603 Setup

License Agreement

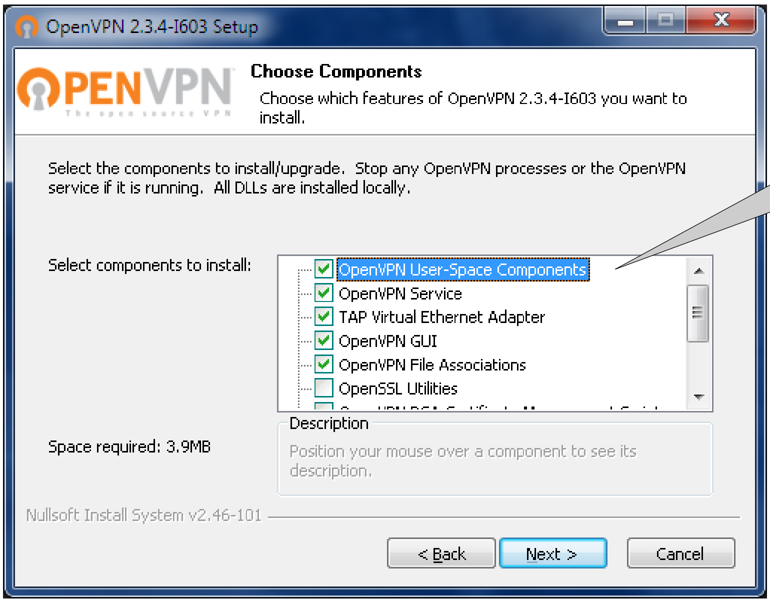
Please review the license terms before installing OpenVPN 2.3.4-I603.

Press Page Down to see the rest of the agreement.

```
OpenVPN (TM) -- An Open Source VPN daemon

Copyright (C) 2002-2010 OpenVPN Technologies, Inc. <sales@openvpn.net>

This distribution contains multiple components, some
of which fall under different licenses.  By using OpenVPN
or any of the bundled components enumerated below, you
agree to be bound by the conditions of the license for
each respective component.

OpenVPN trademark
```

If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install OpenVPN 2.3.4-I603.

Agree to the License Agreement to continue installing the software.



OpenVPN 2.3.4-I603 Setup

Choose Components

Choose which features of OpenVPN 2.3.4-I603 you want to install.

Select the components to install/upgrade. Stop any OpenVPN processes or the OpenVPN service if it is running. All DLLs are installed locally.

Select components to install:

- ☑ OpenVPN User-Space Components
- ☑ OpenVPN Service
- ☑ TAP Virtual Ethernet Adapter
- ☑ OpenVPN GUI
- ☑ OpenVPN File Associations
- □ OpenSSL Utilities

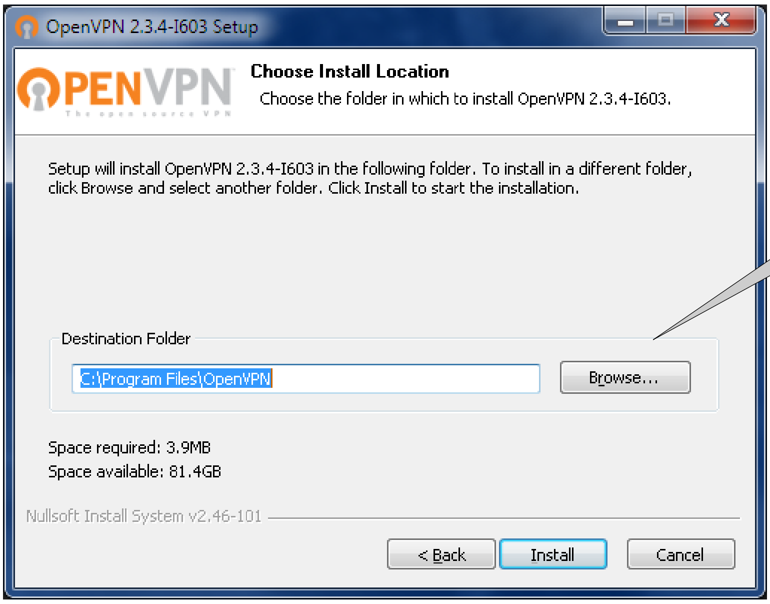
Space required: 3.9MB

Description

Position your mouse over a component to see its description.

Nullsoft Install System v2.46-101

The default settings should be sufficient for most systems otherwise adapt the installed components in this list.



OpenVPN 2.3.4-I603 Setup

Choose Install Location

Choose the folder in which to install OpenVPN 2.3.4-I603.

Setup will install OpenVPN 2.3.4-I603 in the following folder. To install in a different folder, click Browse and select another folder. Click Install to start the installation.

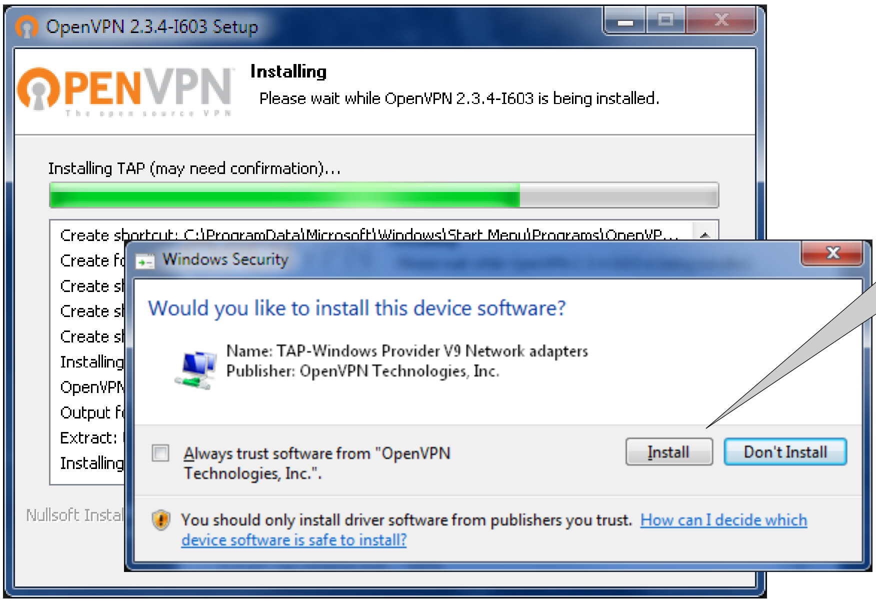
Destination Folder: C:\Program Files\OpenVPN

Space required: 3.9MB

Space available: 81.4GB

Nullsoft Install System v2.46-101

Change installation folder if needed otherwise use the default settings.



OpenVPN 2.3.4-I603 Setup

Installing

Please wait while OpenVPN 2.3.4-I603 is being installed.

Installing TAP (may need confirmation)...

```
Create shortcut: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\OpenVP...
Create fo
Create sl
Create sl
Create sl
Installing
OpenVPN
Output fo
Extract:
Installing
```

Nullsoft Instal

Windows Security

Would you like to install this device software?

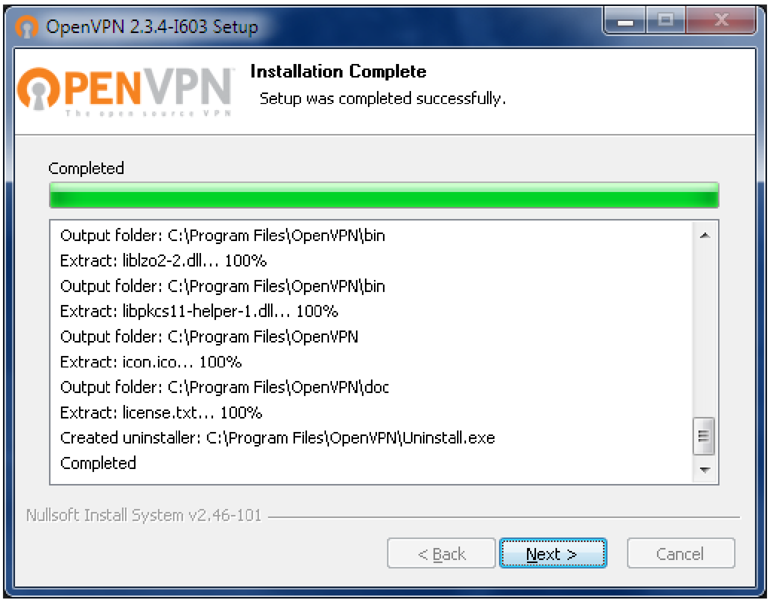
Name: TAP-Windows Provider V9 Network adapters

Publisher: OpenVPN Technologies, Inc.

□ Always trust software from "OpenVPN Technologies, Inc.".

You should only install driver software from publishers you trust. How can I decide which device software is safe to install?

During the istallation MS Windows wants confirmation that it is ok to install the TAP interface which is needed for the SSL tunnel. Click Install to proceed.

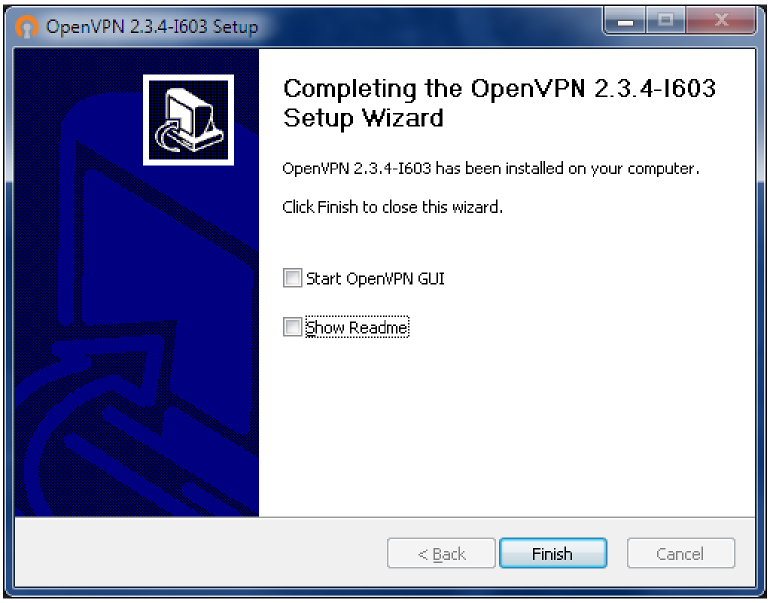


Installation Complete

Setup was completed successfully.

Completed

```
Output folder: C:\Program Files\OpenVPN\bin
Extract: liblzo2-2.dll... 100%
Output folder: C:\Program Files\OpenVPN\bin
Extract: libpkcs11-helper-1.dll... 100%
Output folder: C:\Program Files\OpenVPN
Extract: icon.ico... 100%
Output folder: C:\Program Files\OpenVPN\doc
Extract: license.txt... 100%
Created uninstaller: C:\Program Files\OpenVPN\Uninstall.exe
Completed
```



Completing the OpenVPN 2.3.4-I603 Setup Wizard

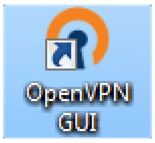
OpenVPN 2.3.4-I603 has been installed on your computer.

Click Finish to close this wizard.

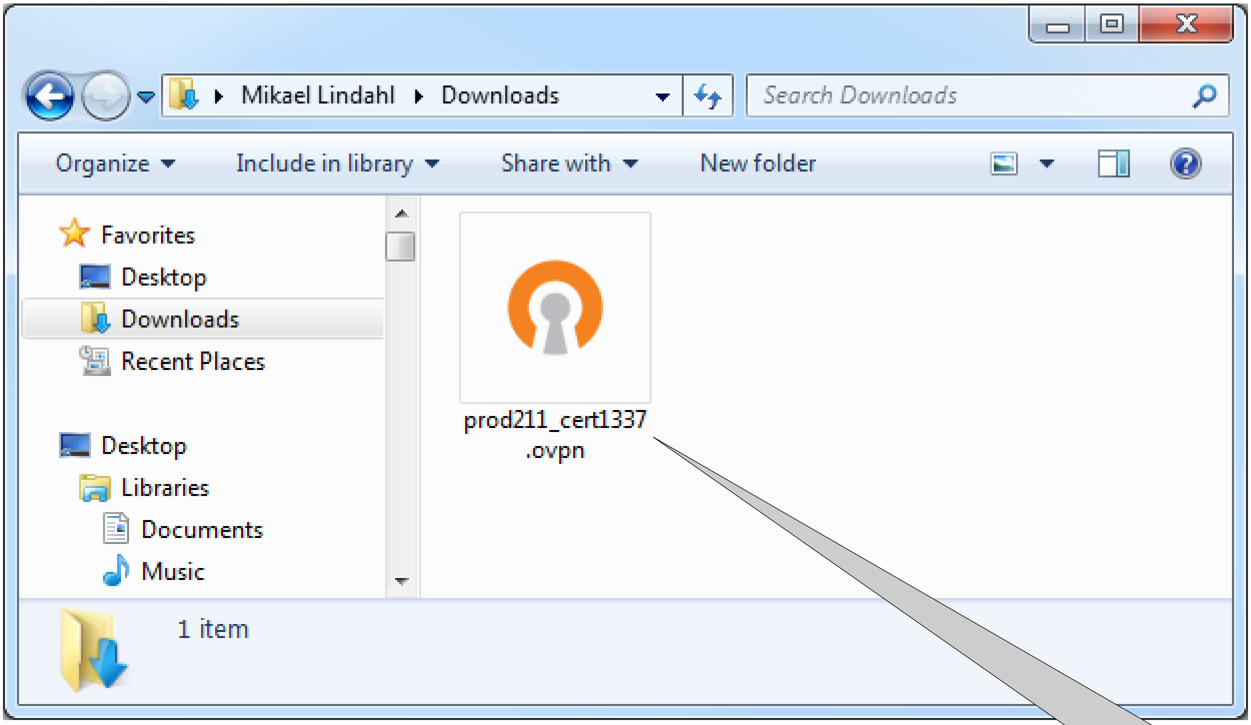
□ Start OpenVPN GUI

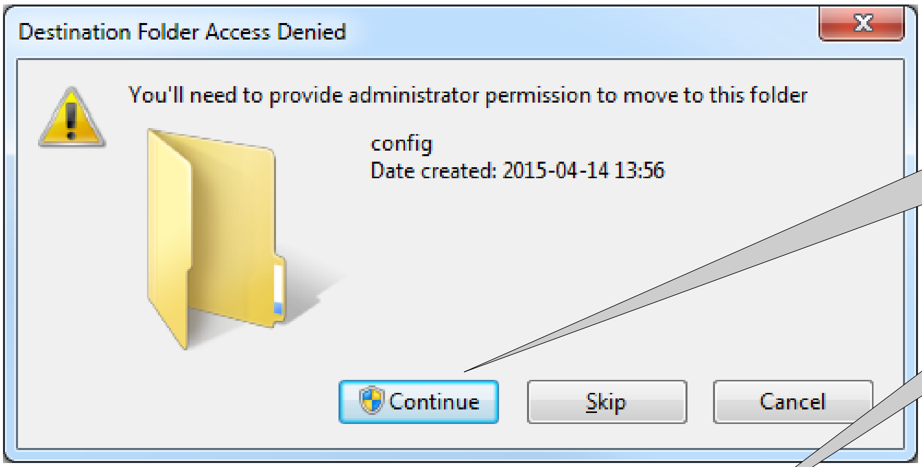
□ Show Readme

When the installation process has finished an OpenVPN GUI icon will appear on the desktop.



3. Install the opvn file in the OpenVPN software client.

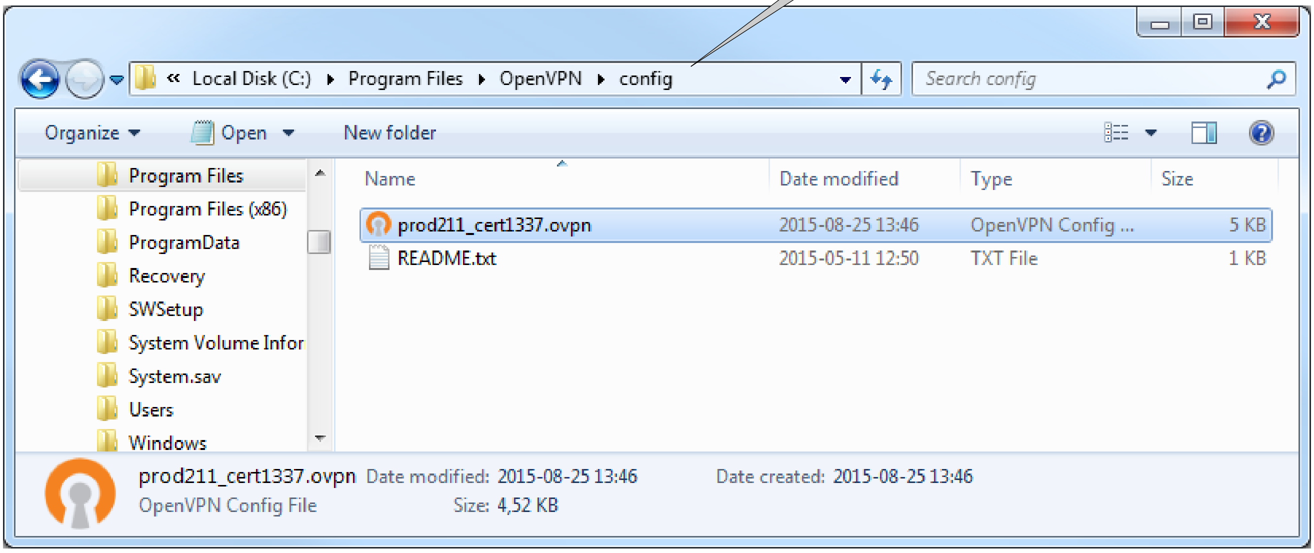



Destination Folder Access Denied

You'll need to provide administrator permission to move to this folder

config
Date created: 2015-04-14 13:56

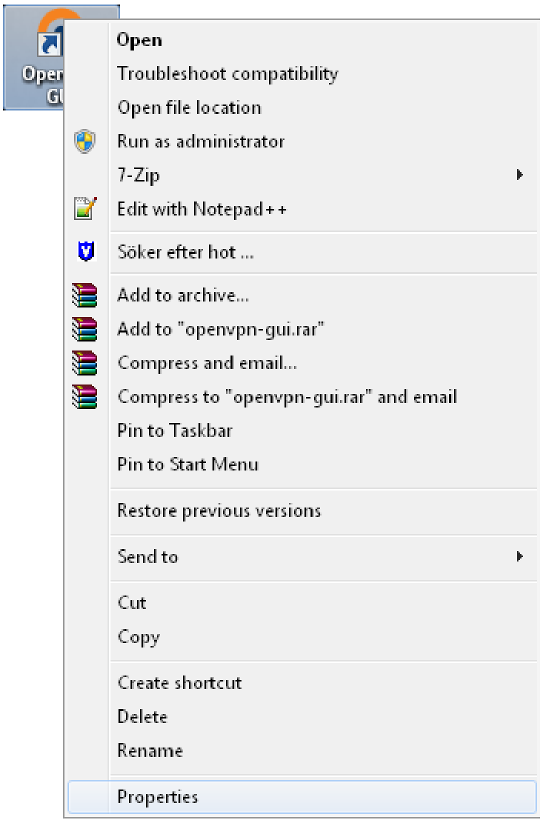
Move the ovpn file to the config folder within the OpenVPN folder. The same location path that was choosen during the installation process, see item 2 of this section. This is an administrator rights folder so click Continue to move the file. The default path for Win 7 64-bit is shown below.

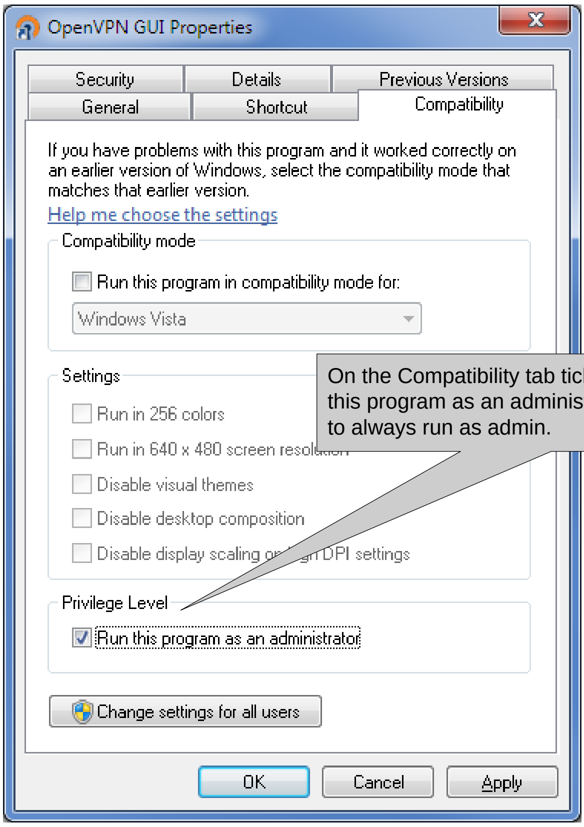


Name	Date modified	Type	Size
prod211_cert1337.ovpn	2015-08-25 13:46	OpenVPN Config ...	5 KB
README.txt	2015-05-11 12:50	TXT File	1 KB

prod211_cert1337.ovpn Date modified: 2015-08-25 13:46 Date created: 2015-08-25 13:46
OpenVPN Config File Size: 4,52 KB

4. The SSL client software must be run as administrator otherwise MS Windows will not allow WeConnect to push out the routes leading to the connected Device Networks. Therefore set administrator rights by right-clicking the OpenVPN GUI icon on the desktop and choose Properties.





If you have problems with this program and it worked correctly on an earlier version of Windows, select the compatibility mode that matches that earlier version.

Help me choose the settings

Compatibility mode

□ Run this program in compatibility mode for:

Windows Vista

Settings

□ Run in 256 colors

□ Run in 640 x 480 screen resolution

□ Disable visual themes

□ Disable desktop composition

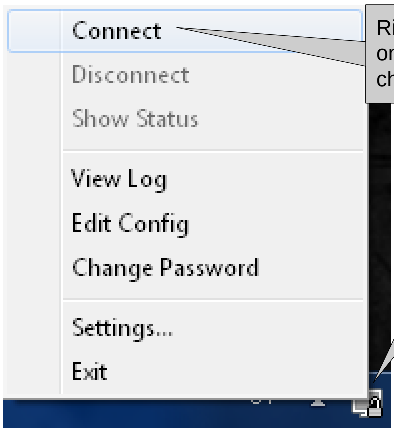
□ Disable display scaling on high DPI settings

Privilege Level

☑ Run this program as an administrator

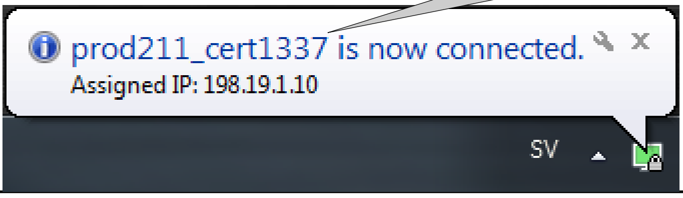
On the Compatibility tab tick the Run this program as an administrator box to always run as admin.

5. Start the tunnel by double-click the OpenVPN GUI icon on the desktop.

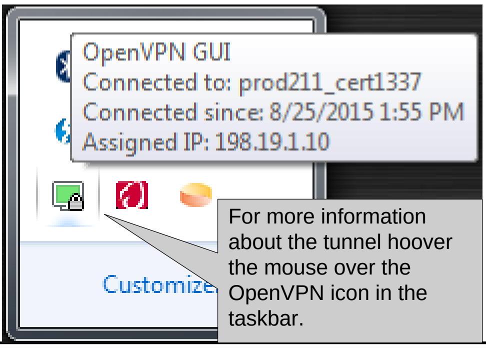


Right-click on the icon that appears on the MS Windows taskbar and choose Connect to start the tunnel.

This notification will appear to confirm that the SSL tunnel is properly connected to WeConnect.



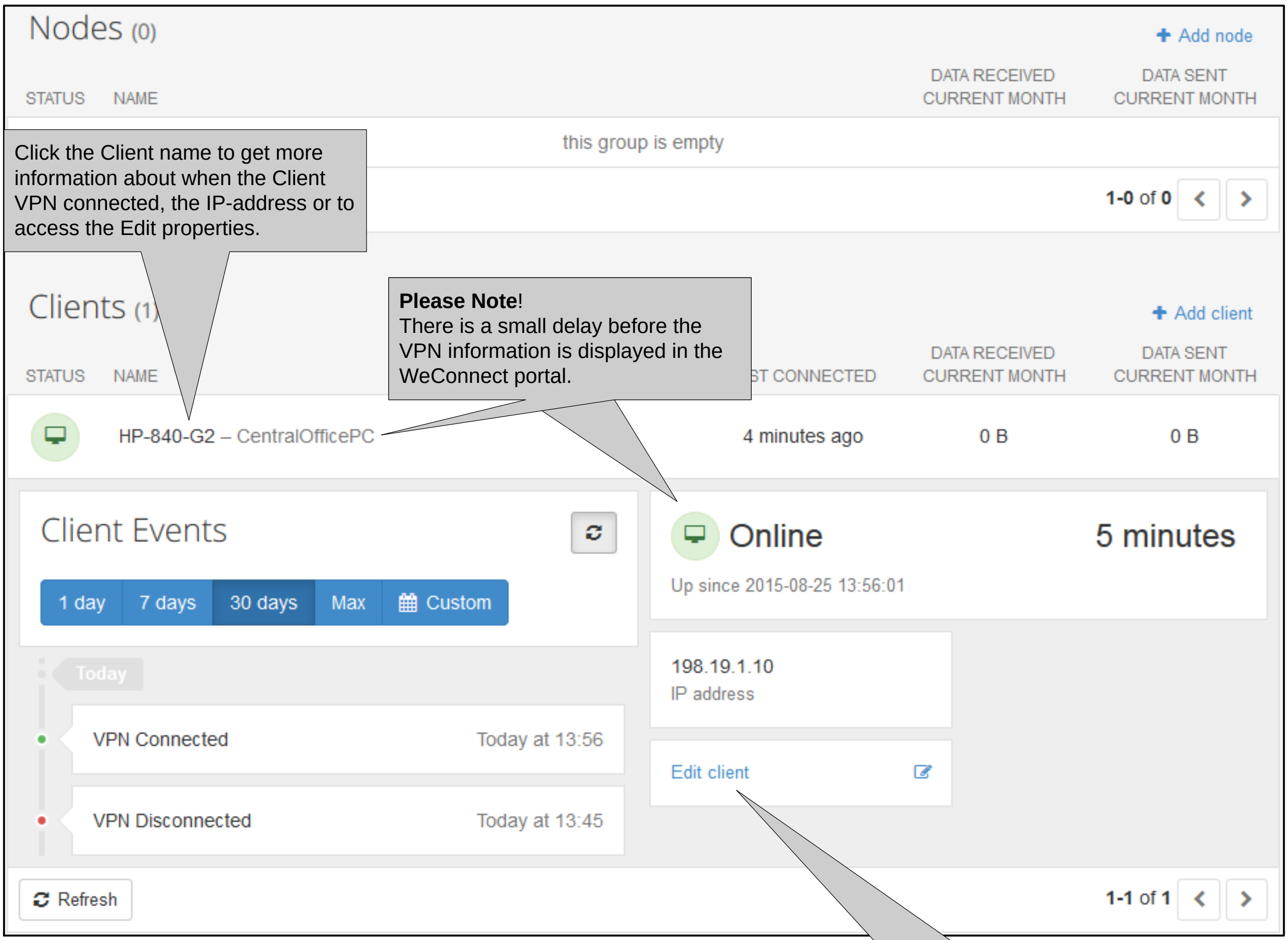
prod211_cert1337 is now connected.
Assigned IP: 198.19.1.10



OpenVPN GUI
Connected to: prod211_cert1337
Connected since: 8/25/2015 1:55 PM
Assigned IP: 198.19.1.10

For more information about the tunnel hoover the mouse over the OpenVPN icon in the taskbar.

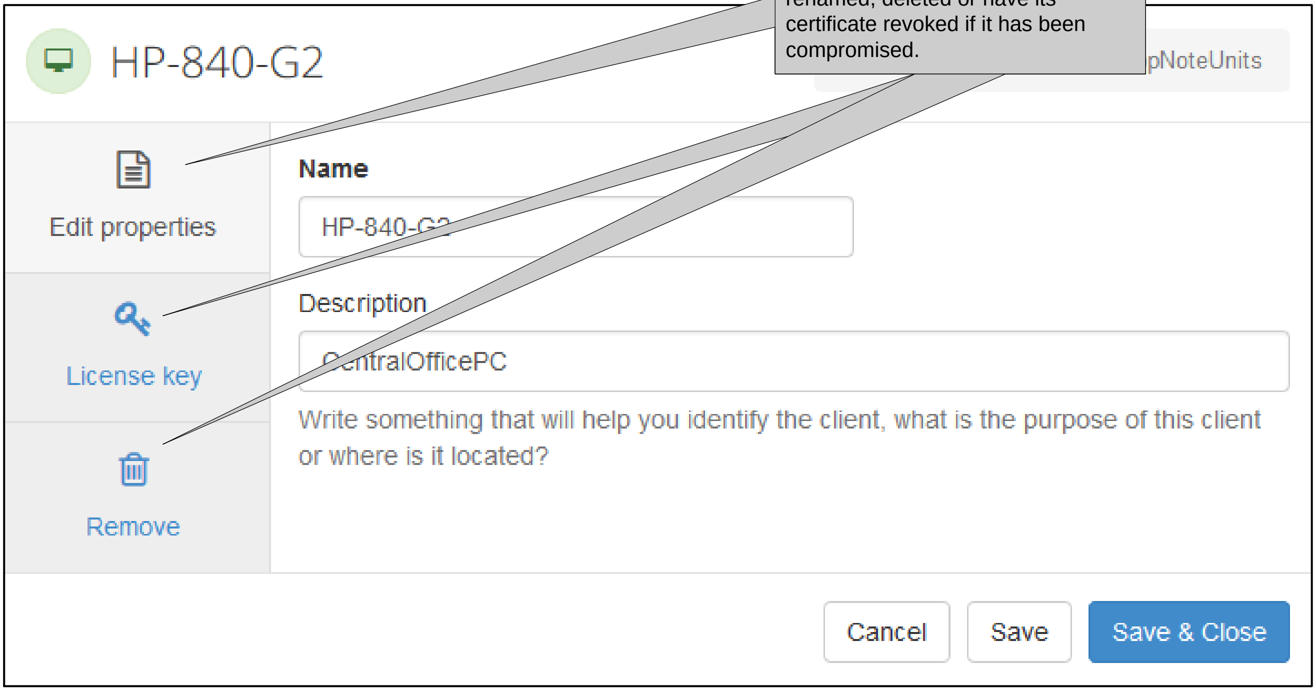
6. The PC Client is now connected to WeConnect through a secure SSL tunnel.
This is visible in the WeConnect portal for the Secure Network the Client belongs to.



Click the Client name to get more information about when the Client VPN connected, the IP-address or to access the Edit properties.

Please Note!
There is a small delay before the VPN information is displayed in the WeConnect portal.

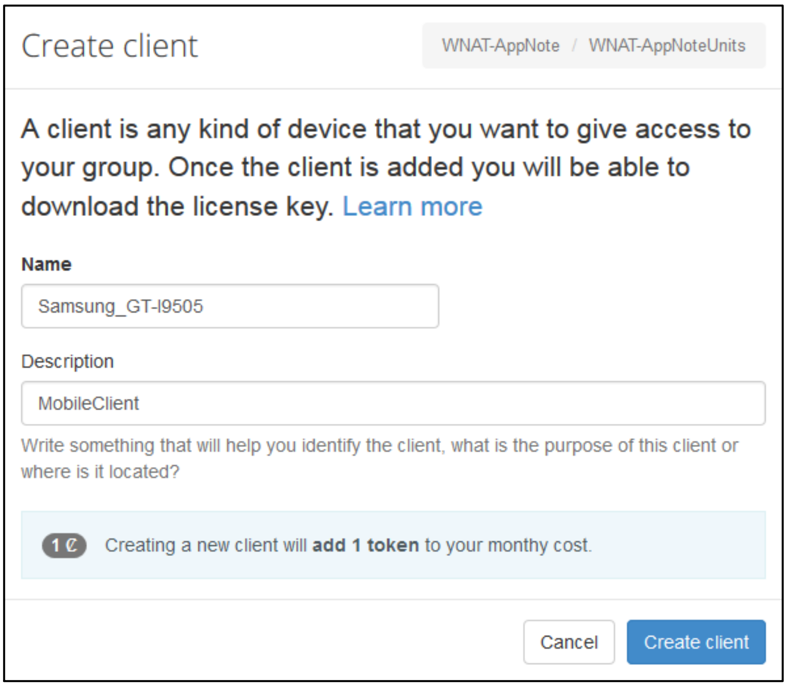
In the Edit properties a Client can be renamed, deleted or have its certificate revoked if it has been compromised.



Add a WeConnect Smartphone or Tablet Client

The Smartphone or Tablet client will have to use the *OpenVPN Connect* app available for both Android and Apple devices.

Start by creating a new Client as shown in the section *Add a WeConnect PC Client*.



Create client

A client is any kind of device that you want to give access to your group. Once the client is added you will be able to download the license key. Learn more

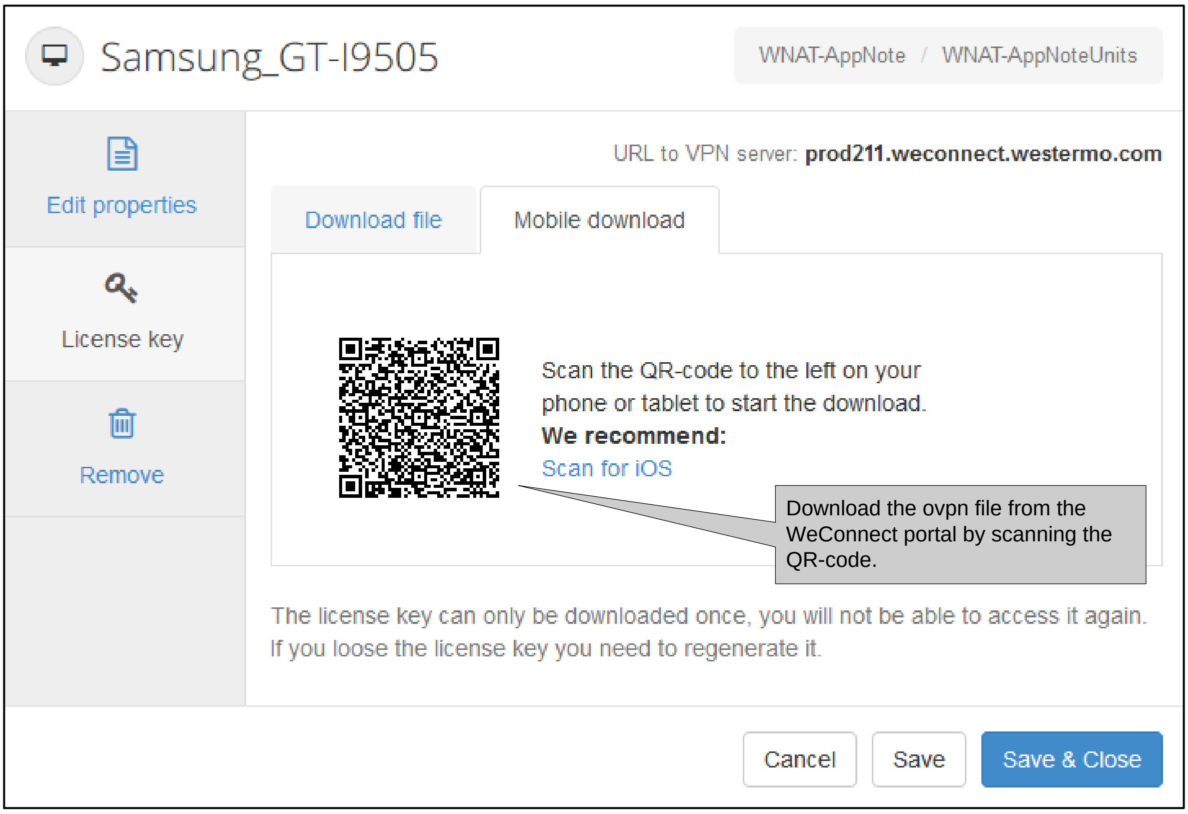
Name: Samsung_GT-I9505

Description: MobileClient

Write something that will help you identify the client, what is the purpose of this client or where is it located?

1 ₡ Creating a new client will **add 1 token** to your monthy cost.

Instead of using the Download File tab use the Mobile Download tab.



Samsung_GT-I9505

URL to VPN server: **prod211.weconnect.westermo.com**

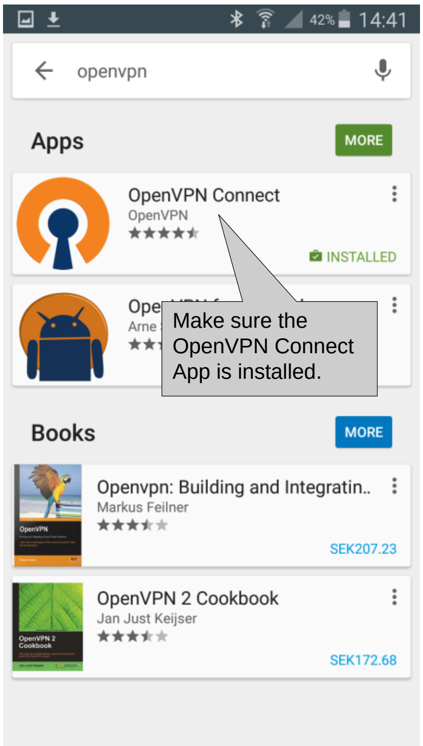
Scan the QR-code to the left on your phone or tablet to start the download.
We recommend:
Scan for iOS

Download the ovpn file from the WeConnect portal by scanning the QR-code.

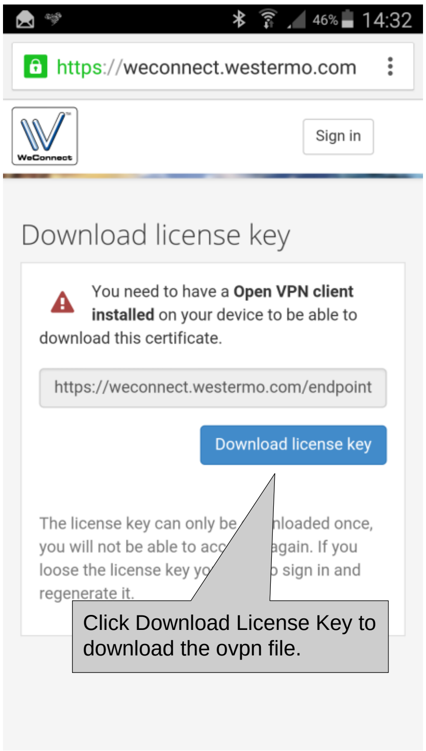
The license key can only be downloaded once, you will not be able to access it again. If you loose the license key you need to regenerate it.

Install the ovpn file received from WeConnect inorder to establish a secured connection to the Device Networks.

Android



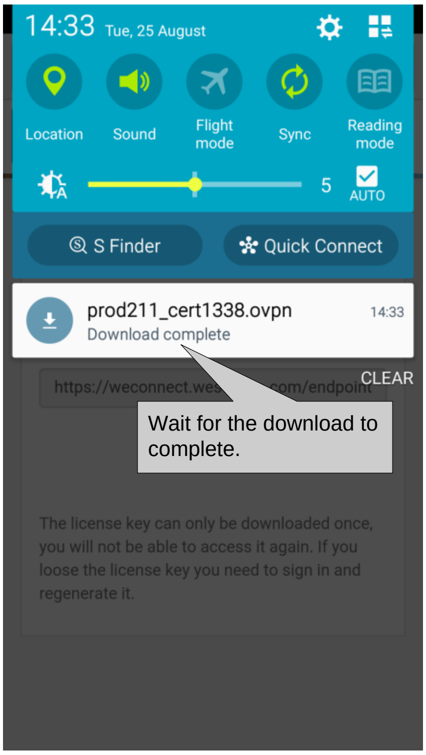
Make sure the OpenVPN Connect App is installed.


https://weconnect.westermo.com
Sign in
Download license key
https://weconnect.westermo.com/endpoint
Download license key

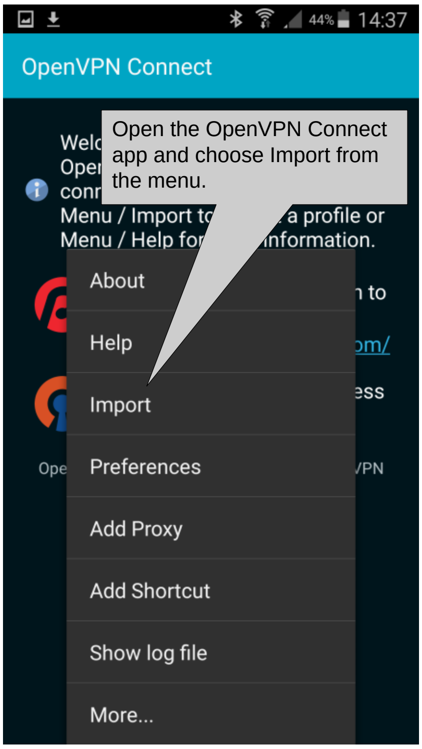
You need to have a **Open VPN client installed** on your device to be able to download this certificate.

The license key can only be downloaded once, you will not be able to access it again. If you loose the license key you need to sign in and regenerate it.

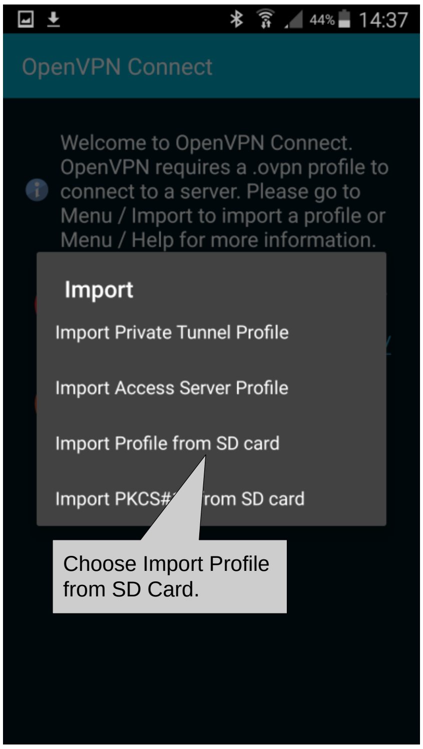
Click Download License Key to download the ovpn file.



Wait for the download to complete.

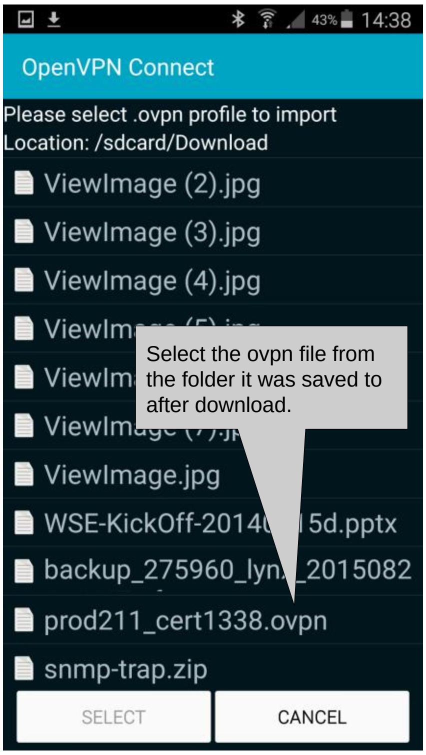


Open the OpenVPN Connect app and choose Import from the menu.


OpenVPN Connect
Import
Import Private Tunnel Profile
Import Access Server Profile
Import Profile from SD card
Import PKCS#12 from SD card

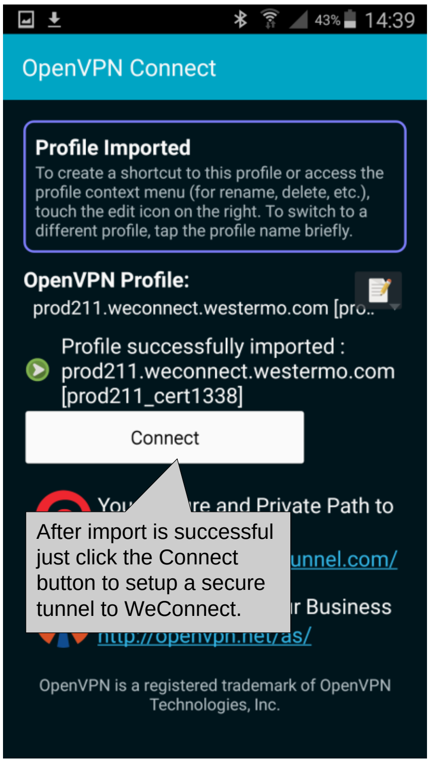
Welcome to OpenVPN Connect. OpenVPN requires a .ovpn profile to connect to a server. Please go to Menu / Import to import a profile or Menu / Help for more information.

Choose Import Profile from SD Card.



Please select .ovpn profile to import
Location: /sdcard/Download

Select the ovpn file from the folder it was saved to after download.



OpenVPN Connect

Profile Imported

To create a shortcut to this profile or access the profile context menu (for rename, delete, etc.), touch the edit icon on the right. To switch to a different profile, tap the profile name briefly.

OpenVPN Profile:

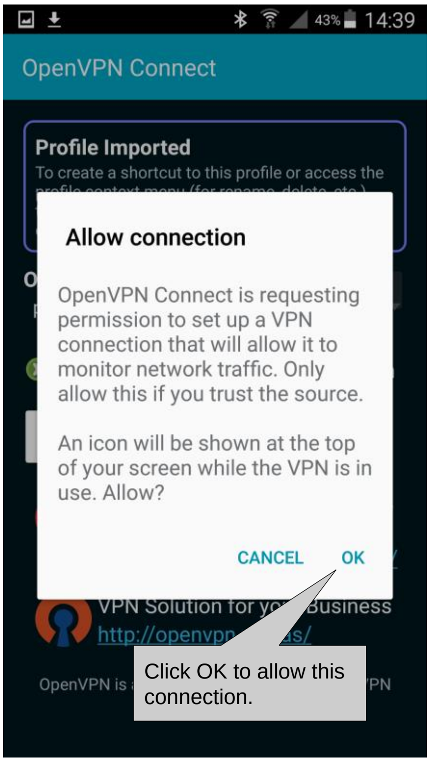
prod211.weconnect.westermo.com [pro..

Profile successfully imported : prod211.weconnect.westermo.com [prod211_cert1338]

Connect

OpenVPN is a registered trademark of OpenVPN Technologies, Inc.

After import is successful just click the Connect button to setup a secure tunnel to WeConnect.



OpenVPN Connect

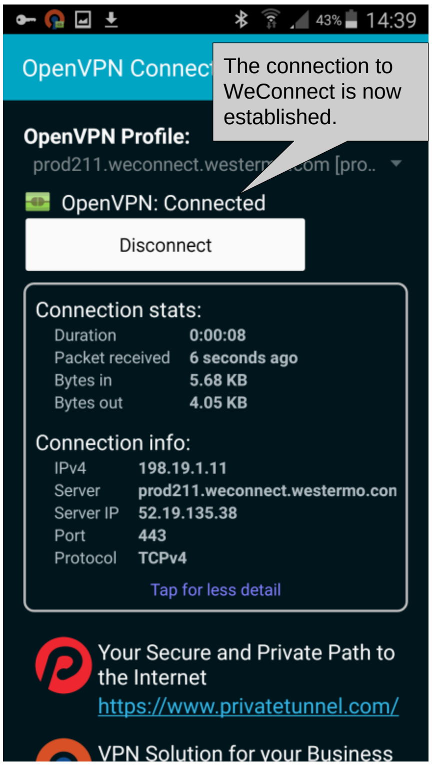
Allow connection

OpenVPN Connect is requesting permission to set up a VPN connection that will allow it to monitor network traffic. Only allow this if you trust the source.

An icon will be shown at the top of your screen while the VPN is in use. Allow?

CANCEL OK

Click OK to allow this connection.



OpenVPN Connect

OpenVPN Profile:

prod211.weconnect.westermo.com [pro..

OpenVPN: Connected

Disconnect

Connection stats:

Duration	0:00:08
Packet received	6 seconds ago
Bytes in	5.68 KB
Bytes out	4.05 KB

Connection info:

IPv4	198.19.1.11
Server	prod211.weconnect.westermo.con
Server IP	52.19.135.38
Port	443
Protocol	TCPv4

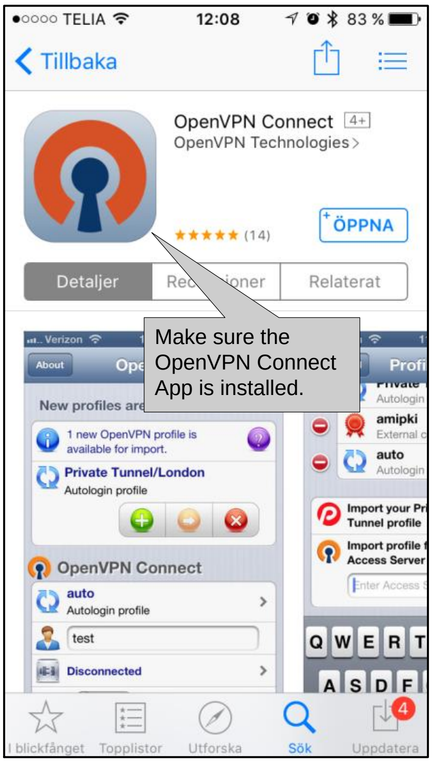
Tap for less detail

Your Secure and Private Path to the Internet https://www.privatetunnel.com/

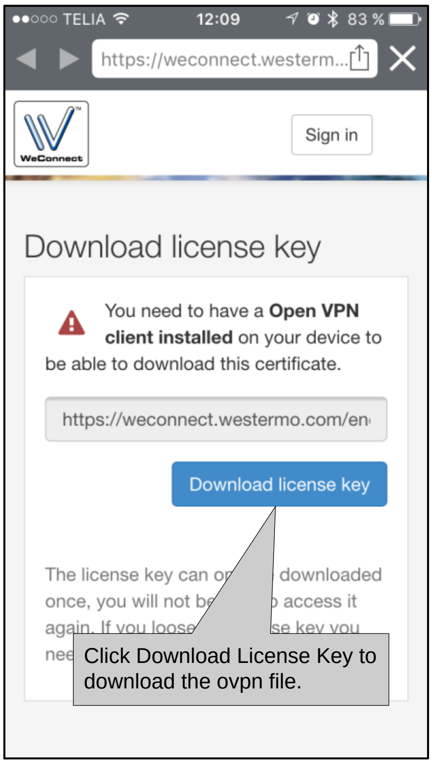
VPN Solution for your Business

The connection to WeConnect is now established.

iOS



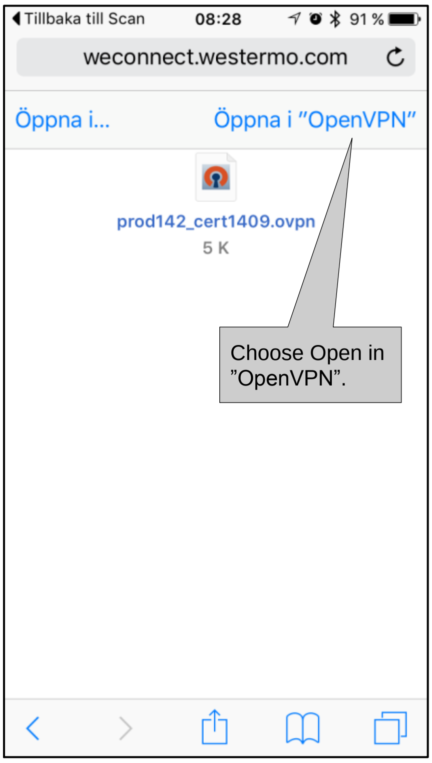
Make sure the OpenVPN Connect App is installed.



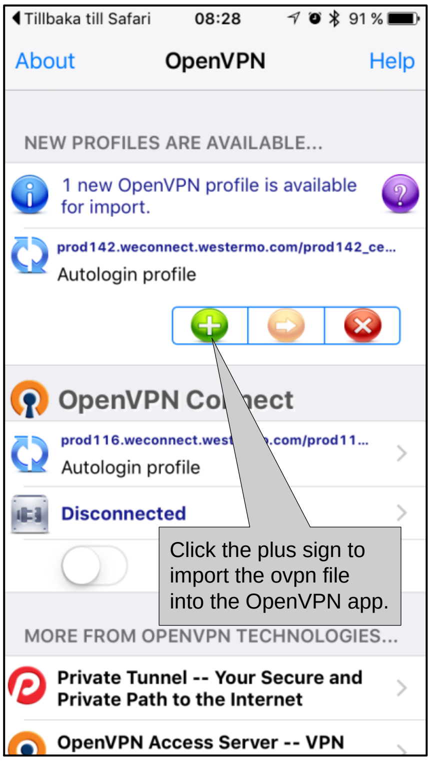
You need to have a **Open VPN client installed** on your device to be able to download this certificate.

The license key can only be downloaded once, you will not be able to access it again. If you loose the license key you need

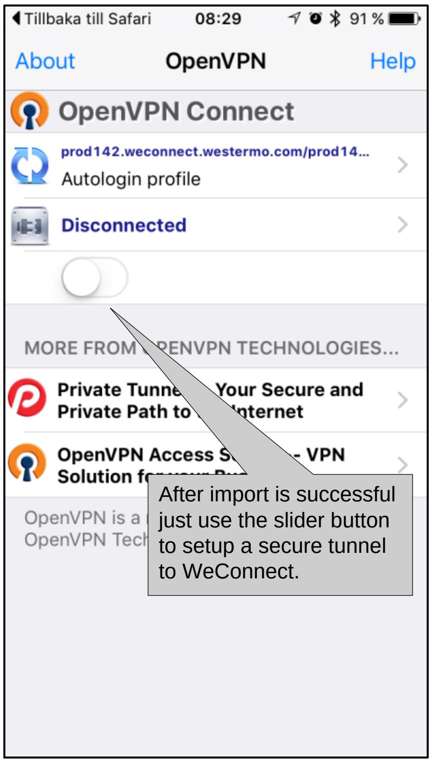
Click Download License Key to download the ovpn file.



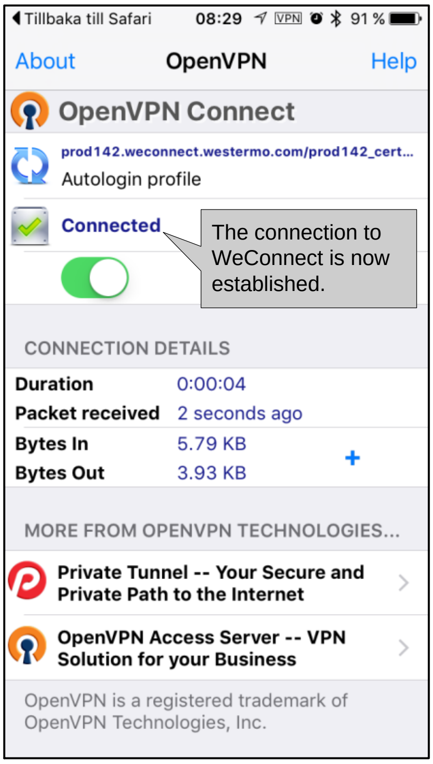
Choose Open in ”OpenVPN”.


Tillbaka till Safari 08:28 91 %
About
OpenVPN
Help
NEW PROFILES ARE AVAILABLE...
1 new OpenVPN profile is available for import.
prod142.weconnect.westermo.com/prod142_ce...
Autologin profile
OpenVPN Connect
prod116.weconnect.westermo.com/prod11...
Autologin profile
Disconnected
MORE FROM OPENVPN TECHNOLOGIES...
Private Tunnel -- Your Secure and Private Path to the Internet
OpenVPN Access Server -- VPN

Click the plus sign to import the ovpn file into the OpenVPN app.


Tillbaka till Safari 08:29 91 %
About
OpenVPN
Help
OpenVPN Connect
prod142.weconnect.westermo.com/prod14...
Autologin profile
Disconnected
MORE FROM OPENVPN TECHNOLOGIES...
Private Tunnel -- Your Secure and Private Path to the Internet
OpenVPN Access Server -- VPN Solution for your Business
OpenVPN is a registered trademark of OpenVPN Technologies, Inc.

After import is successful just use the slider button to setup a secure tunnel to WeConnect.


Tillbaka till Safari 08:29 VPN 91 %
About
OpenVPN
Help
OpenVPN Connect
prod142.weconnect.westermo.com/prod142_cert...
Autologin profile
Connected
CONNECTION DETAILS
MORE FROM OPENVPN TECHNOLOGIES...
Private Tunnel -- Your Secure and Private Path to the Internet
OpenVPN Access Server -- VPN Solution for your Business
OpenVPN is a registered trademark of OpenVPN Technologies, Inc.

Duration	0:00:04
Packet received	2 seconds ago
Bytes In	5.79 KB
Bytes Out	3.93 KB

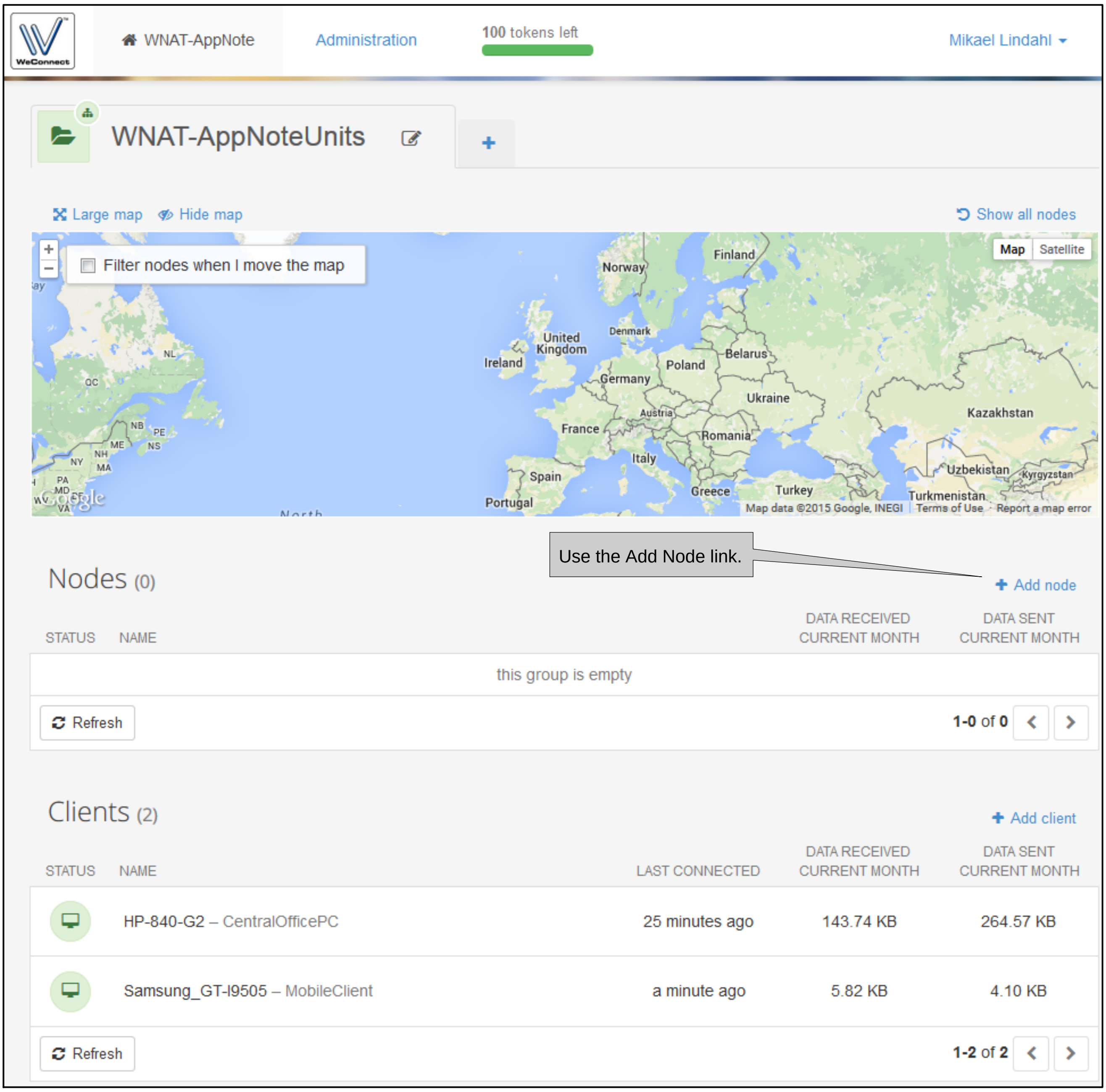
The connection to WeConnect is now established.

Adding Nodes

Nodes are network equipment that connects entire networks to WeConnect using SSL VPNs. This Application Note will show what the connection setup looks like for both WeOS and MRD units.

Add a WeConnect Node

Add a Node by clicking *Add node* in the WeConnect portal.



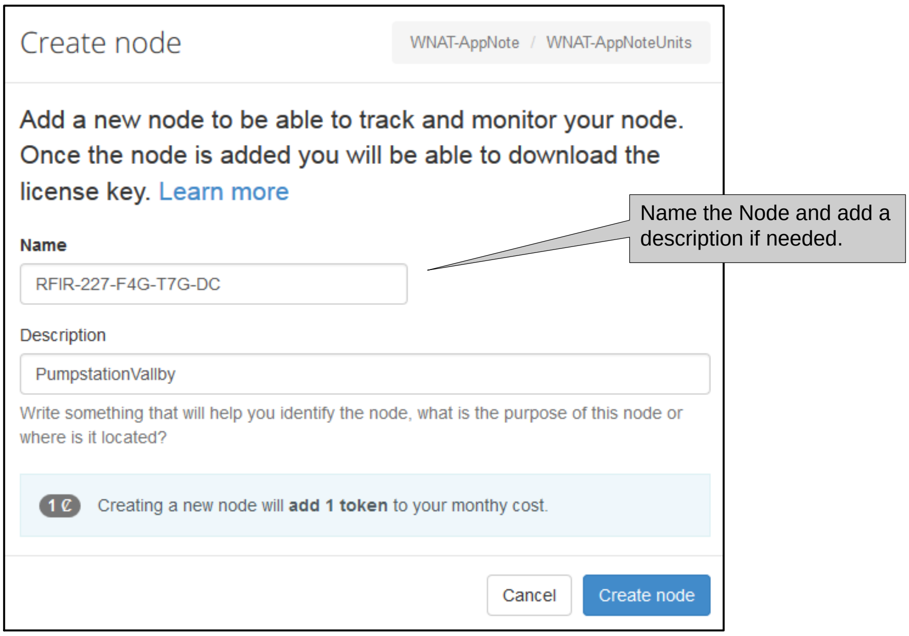
Use the Add Node link.

Nodes (0)

STATUS	NAME	DATA RECEIVED CURRENT MONTH	DATA SENT CURRENT MONTH
this group is empty			

Clients (2)

STATUS	NAME	LAST CONNECTED	DATA RECEIVED CURRENT MONTH	DATA SENT CURRENT MONTH
	HP-840-G2 – CentralOfficePC	25 minutes ago	143.74 KB	264.57 KB
	Samsung_GT-I9505 – MobileClient	a minute ago	5.82 KB	4.10 KB



Create node

WNAT-AppNote / WNAT-AppNoteUnits

Add a new node to be able to track and monitor your node. Once the node is added you will be able to download the license key. Learn more

Name: RFIR-227-F4G-T7G-DC

Description: PumpstationVallby

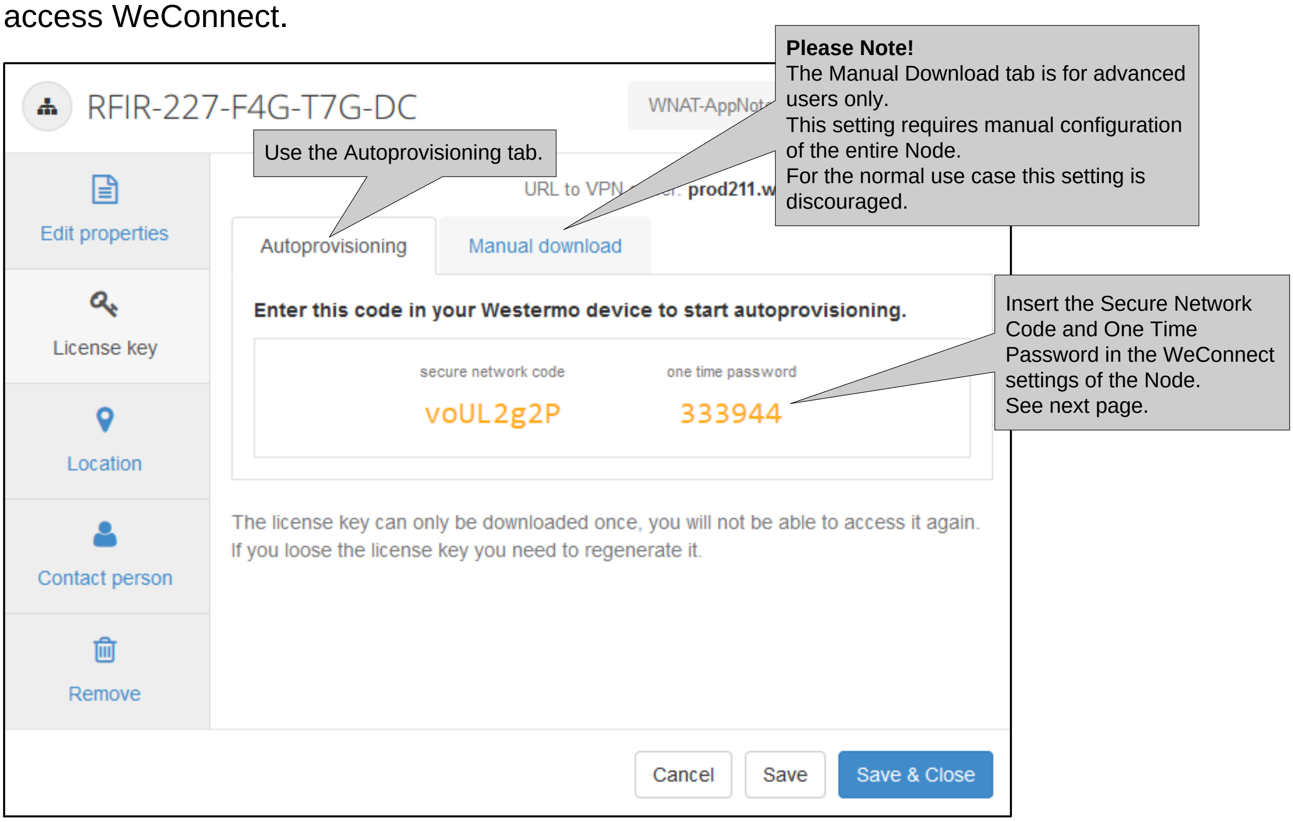
Write something that will help you identify the node, what is the purpose of this node or where is it located?

1 Ȼ Creating a new node will **add 1 token** to your monthy cost.

Name the Node and add a description if needed.

Autoprovisioning

Autoprovisioning is the prefered way of adding Nodes to WeConnect it makes sure that the configuration is done correctly.
Manual configuration is also supported but should in general setups not be used.
When using Autoprovisioning the Node will automatically download and install the required certificates and make the configuration changes necessary for the Node to be able to access WeConnect.



RFIR-227-F4G-T7G-DC

URL to VPN ...r: **prod211.w**

Enter this code in your Westermo device to start autoprovisioning.

secure network code: voUL2g2P

one time password: 333944

The license key can only be downloaded once, you will not be able to access it again. If you loose the license key you need to regenerate it.

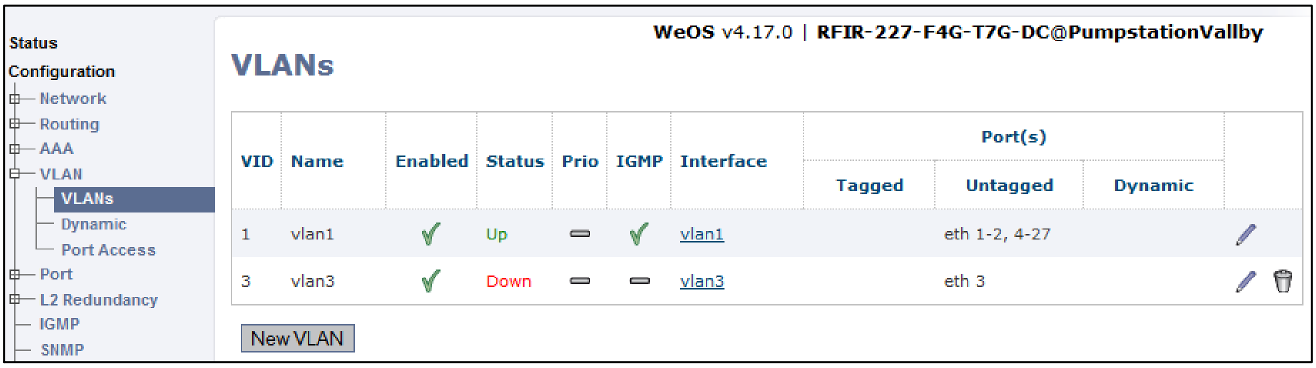
Please Note!
The Manual Download tab is for advanced users only.
This setting requires manual configuration of the entire Node.
For the normal use case this setting is discouraged.

Use the Autoprovisioning tab.

Insert the Secure Network Code and One Time Password in the WeConnect settings of the Node.
See next page.

Prepare WeOS Units for Autoprovisioning

1. Start by creating the VLANs needed, one for the WAN side (VLAN 3) and one for the LAN side (VLAN 1 already created by default).
Configuration -> VLAN -> VLANs.

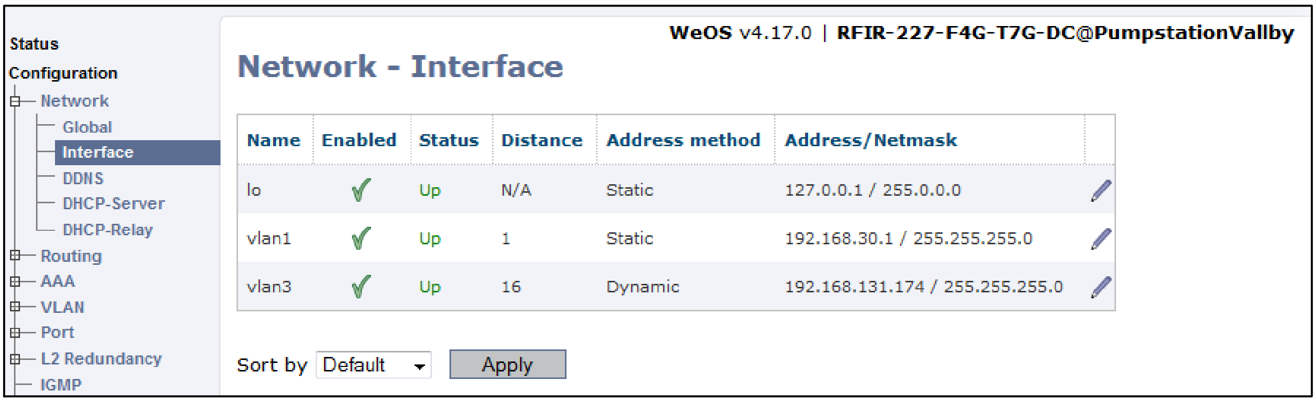


WeOS v4.17.0 | **RFIR-227-F4G-T7G-DC@PumpstationVallby**

VLANs

VID	Name	Enabled	Status	Prio	IGMP	Interface	Port(s)			
							Tagged	Untagged	Dynamic	
1	vlan1	✓	Up	−	✓	vlan1		eth 1-2, 4-27		✎
3	vlan3	✓	Down	−	−	vlan3		eth 3		✎ 🗑

2. Then setup IP-addresses to turn the VLANs into layer 3 interfaces.
Configuration -> Network -> Interface.
Please Note! Do not use the 198.18.0.0/16 or 198.19.0.0/16 networks as LAN addresses as these are used by WeConnect.



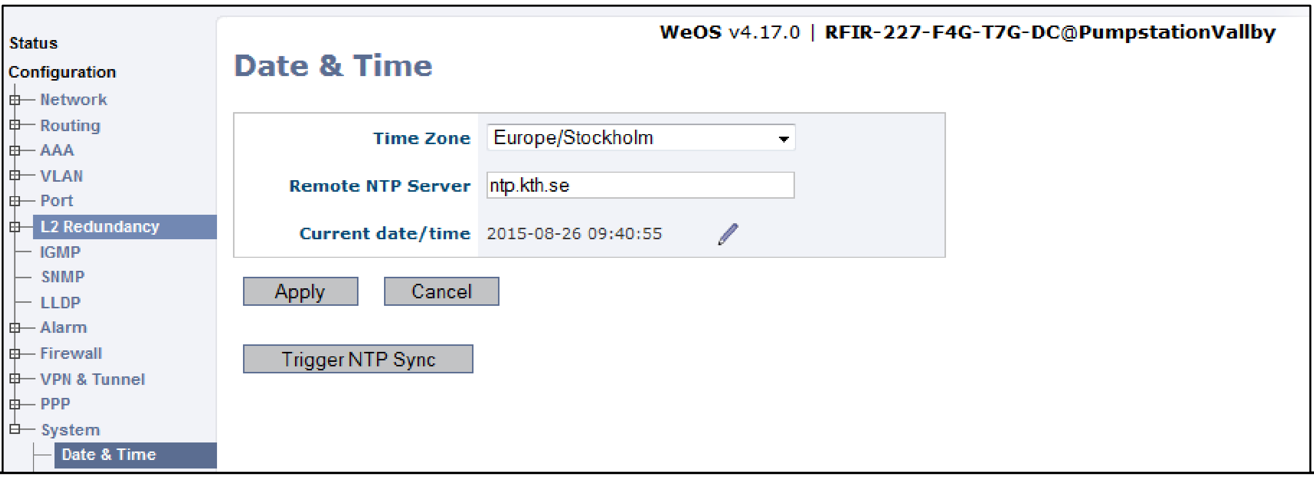
WeOS v4.17.0 | **RFIR-227-F4G-T7G-DC@PumpstationVallby**

Network - Interface

Name	Enabled	Status	Distance	Address method	Address/Netmask	
lo	✓	Up	N/A	Static	127.0.0.1 / 255.0.0.0	✎
vlan1	✓	Up	1	Static	192.168.30.1 / 255.255.255.0	✎
vlan3	✓	Up	16	Dynamic	192.168.131.174 / 255.255.255.0	✎

Sort by Default

3. Set the correct time for the Node, this is necessary for the certificates to function properly. NTP synchronization is preferred.
Configuration -> System -> Date & Time.

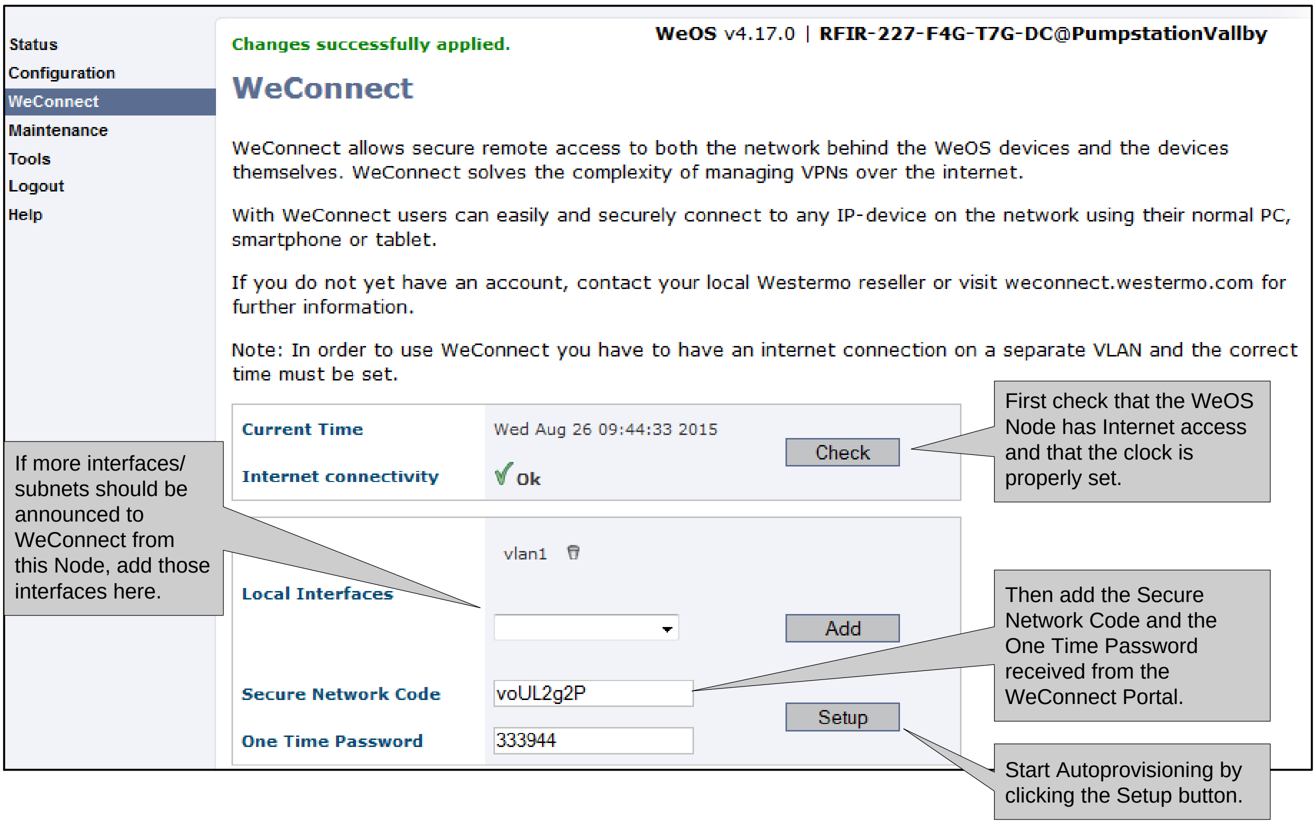


WeOS v4.17.0 | **RFIR-227-F4G-T7G-DC@PumpstationVallby**

Date & Time

Time Zone	Europe/Stockholm
Remote NTP Server	ntp.kth.se
Current date/time	2015-08-26 09:40:55 ✎

4. Activate the Autoprovisioning function by going to the WeConnect instance in the WeOS menu.



Changes successfully applied.

WeOS v4.17.0 | RFIR-227-F4G-T7G-DC@PumpstationVallby

WeConnect

WeConnect allows secure remote access to both the network behind the WeOS devices and the devices themselves. WeConnect solves the complexity of managing VPNs over the internet.

With WeConnect users can easily and securely connect to any IP-device on the network using their normal PC, smartphone or tablet.

If you do not yet have an account, contact your local Westermo reseller or visit weconnect.westermo.com for further information.

Note: In order to use WeConnect you have to have an internet connection on a separate VLAN and the correct time must be set.

Current Time	Wed Aug 26 09:44:33 2015
Internet connectivity	✓ Ok
Local Interfaces	vlan1
Secure Network Code	voUL2g2P
One Time Password	333944

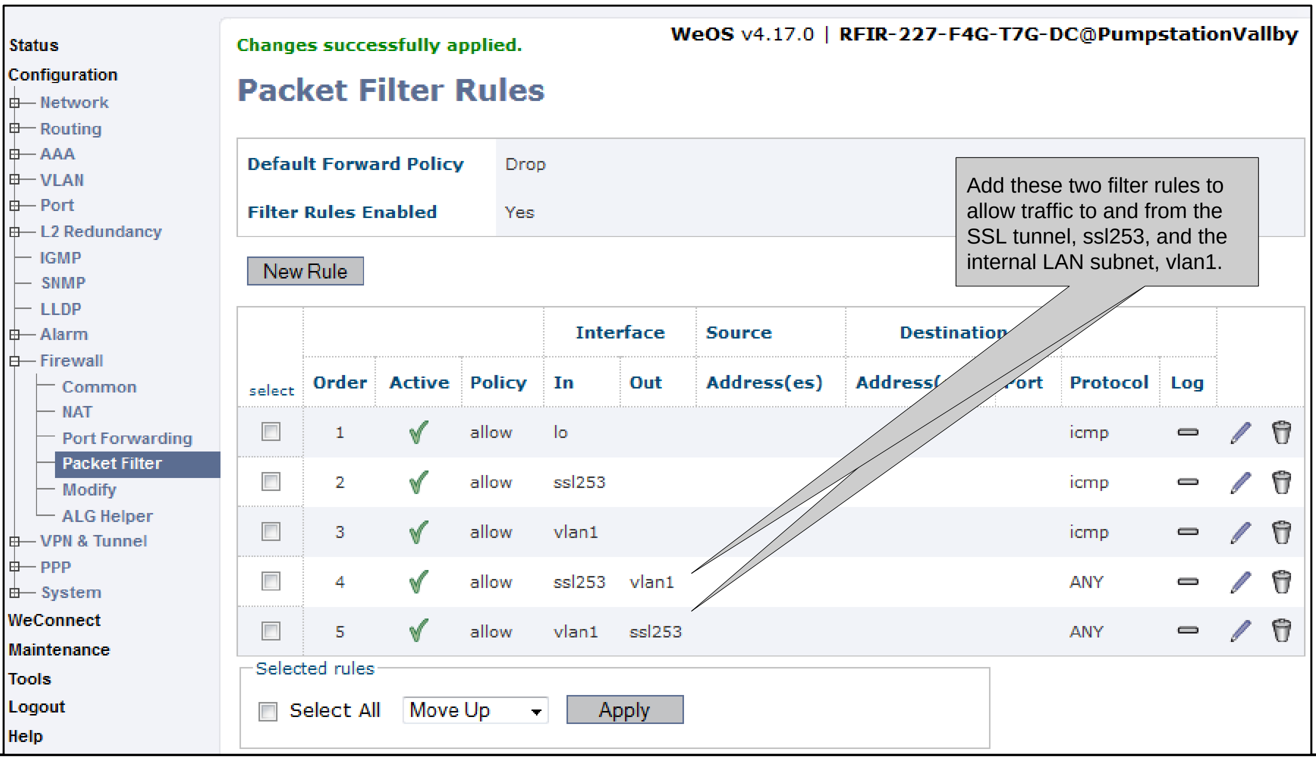
First check that the WeOS Node has Internet access and that the clock is properly set.

If more interfaces/ subnets should be announced to WeConnect from this Node, add those interfaces here.

Then add the Secure Network Code and the One Time Password received from the WeConnect Portal.

Start Autoprovisioning by clicking the Setup button.

5. **Please Note!**
Remember to enable the firewall to protect the WAN Interface of the Node.
When the firewall is enabled the traffic to and from the SSL tunnel must be allowed.
Configuration -> Firewall -> Packet Filter.



Changes successfully applied.

WeOS v4.17.0 | RFIR-227-F4G-T7G-DC@PumpstationVallby

Packet Filter Rules

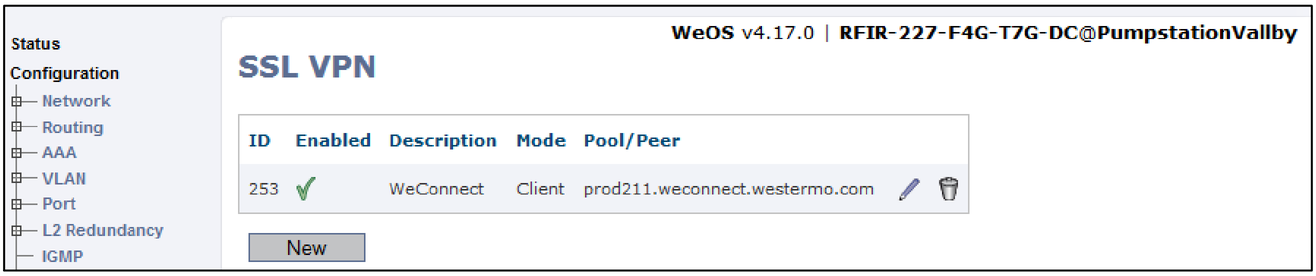
Default Forward Policy	Drop
Filter Rules Enabled	Yes

				Interface		Source	Destination			
select	Order	Active	Policy	In	Out	Address(es)	Address(es)	Port	Protocol	Log
□	1	✓	allow	lo					icmp	−
□	2	✓	allow	ssl253					icmp	−
□	3	✓	allow	vlan1					icmp	−
□	4	✓	allow	ssl253	vlan1				ANY	−
□	5	✓	allow	vlan1	ssl253				ANY	−

Selected rules
□ Select All   Move Up ▾   Apply

Add these two filter rules to allow traffic to and from the SSL tunnel, ssl253, and the internal LAN subnet, vlan1.

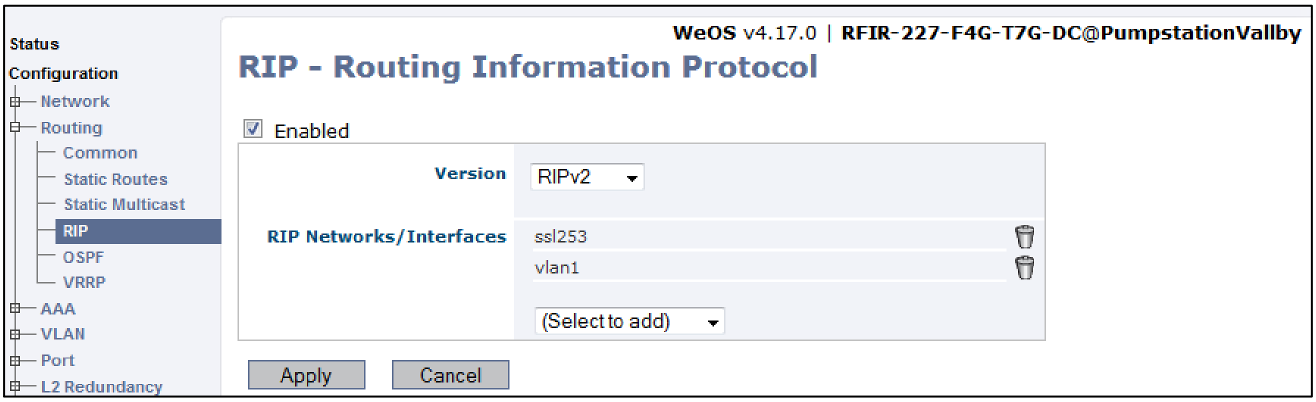
6. Done!
The Node will now automatically download and install the certificates needed and configuration settings for the SSL VPN tunnel from the WeConnect Provisioning Server. It will also configure the appropriate routing using RIPv2 to announce the Device Network(s) to WeConnect.



WeOS v4.17.0 | RFIR-227-F4G-T7G-DC@PumpstationVallby

SSL VPN

ID	Enabled	Description	Mode	Pool/Peer
253	✓	WeConnect	Client	prod211.weconnect.westermo.com



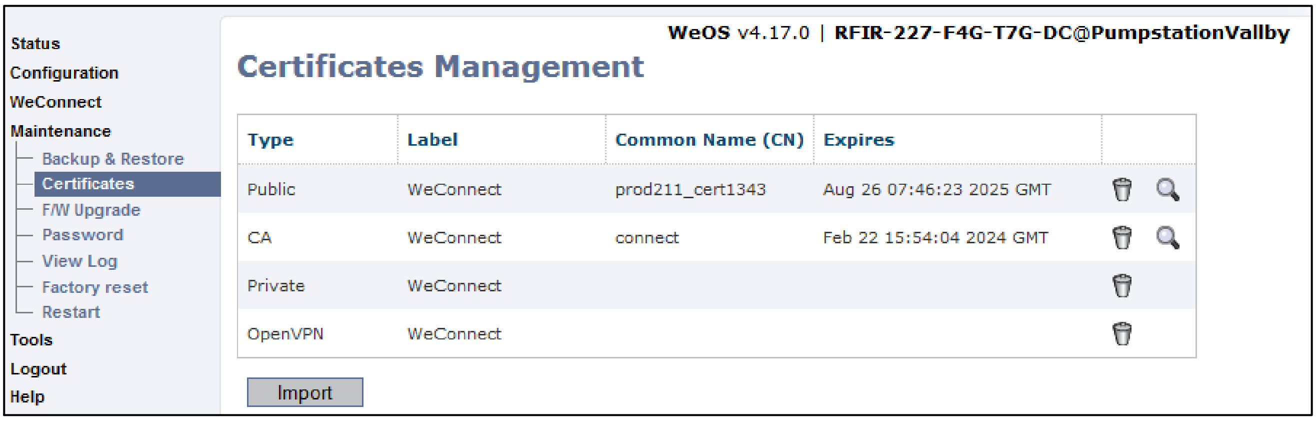
WeOS v4.17.0 | RFIR-227-F4G-T7G-DC@PumpstationVallby

RIP - Routing Information Protocol

☑ Enabled

Version: RIPv2

RIP Networks/Interfaces: ssl253, vlan1, (Select to add)



WeOS v4.17.0 | RFIR-227-F4G-T7G-DC@PumpstationVallby

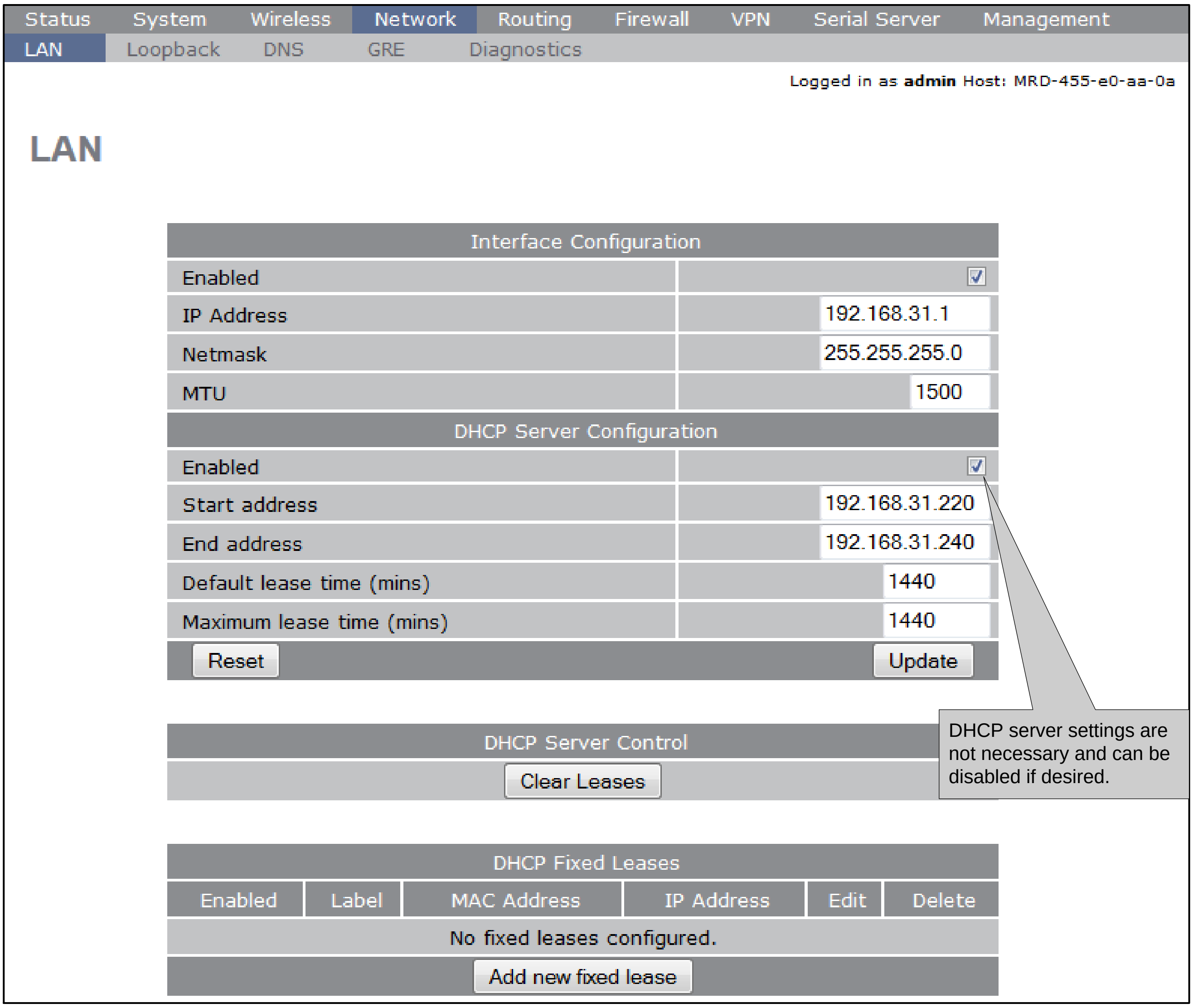
Certificates Management

Type	Label	Common Name (CN)	Expires
Public	WeConnect	prod211_cert1343	Aug 26 07:46:23 2025 GMT
CA	WeConnect	connect	Feb 22 15:54:04 2024 GMT
Private	WeConnect		
OpenVPN	WeConnect		

Prepare MRD Units for Autoprovisioning

1. Setup an Internet connection for the MRD according to the *Getting started* section of the MRD user guide which can be found on the Westermo WEB page www.westermo.com.

2. Configure the Device Network of the MRD.
Network -> LAN.
Please Note! Do not use the 198.18.0.0/16 or 198.19.0.0/16 networks as LAN addresses as these are used by WeConnect.



Logged in as **admin** Host: MRD-455-e0-aa-0a

LAN

Interface Configuration	
Enabled	☑
IP Address	192.168.31.1
Netmask	255.255.255.0
MTU	1500

DHCP Server Configuration	
Enabled	☑
Start address	192.168.31.220
End address	192.168.31.240
Default lease time (mins)	1440
Maximum lease time (mins)	1440

DHCP Server Control

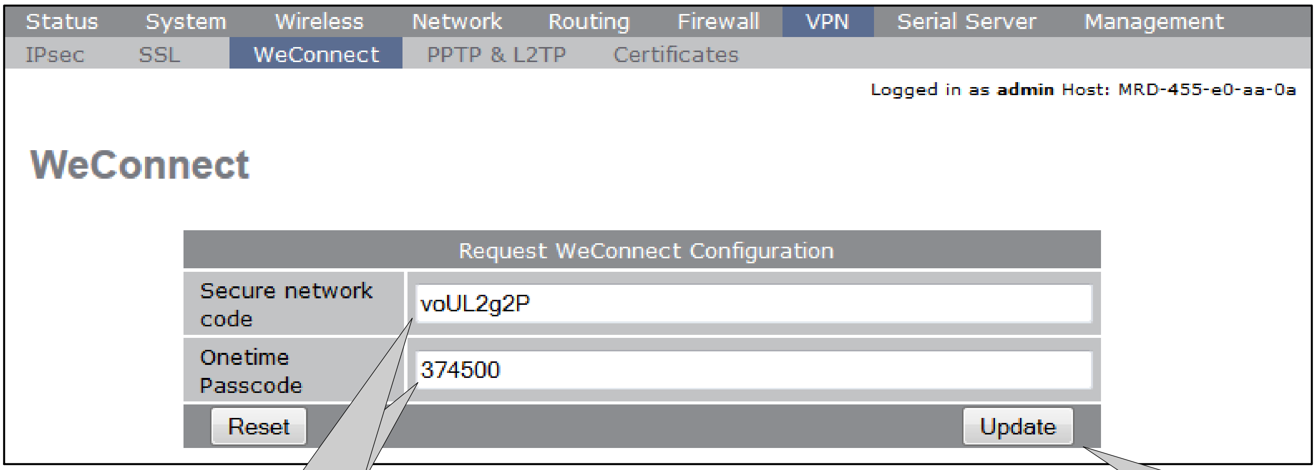
DHCP Fixed Leases

Enabled	Label	MAC Address	IP Address	Edit	Delete
No fixed leases configured.					

DHCP server settings are not necessary and can be disabled if desired.

3. Add another Node to the WeConnect portal according to section *Add a WeConnect Node* of this Application Note.

4. Activate the Autoprovisioning function by going to the new WeConnect instance in the VPN menu. *VPN -> WeConnect.*



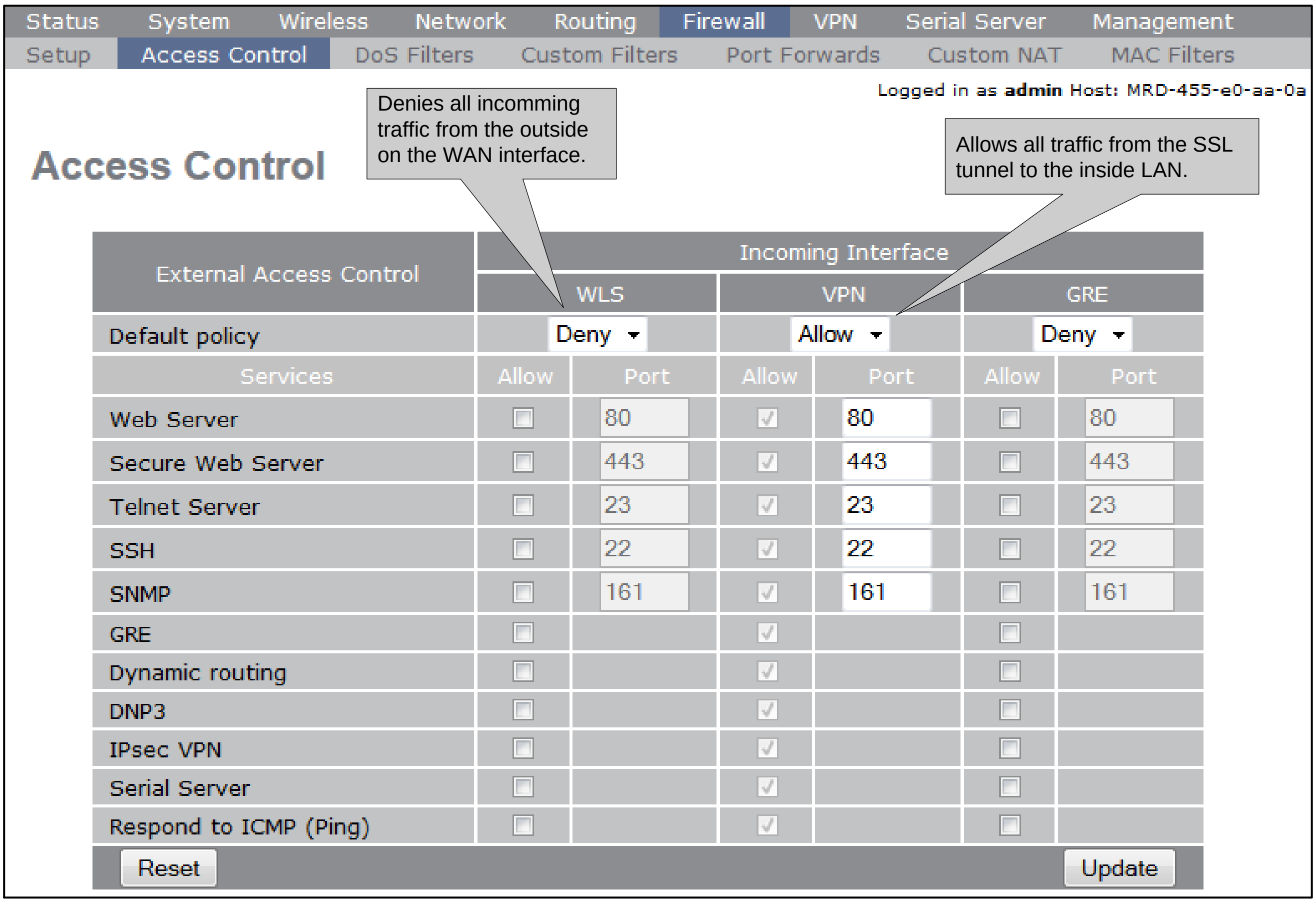
WeConnect

Request WeConnect Configuration	
Secure network code	voUL2g2P
Onetime Passcode	374500

Add the Secure Network Code and the One Time Password received from the WeConnect Portal.

Start Autoprovisioning by clicking the Update button.

5. The Firewall of the MRD units is enabled by default to protect the WAN interface and to allow traffic from the tunnel to the inside LAN.



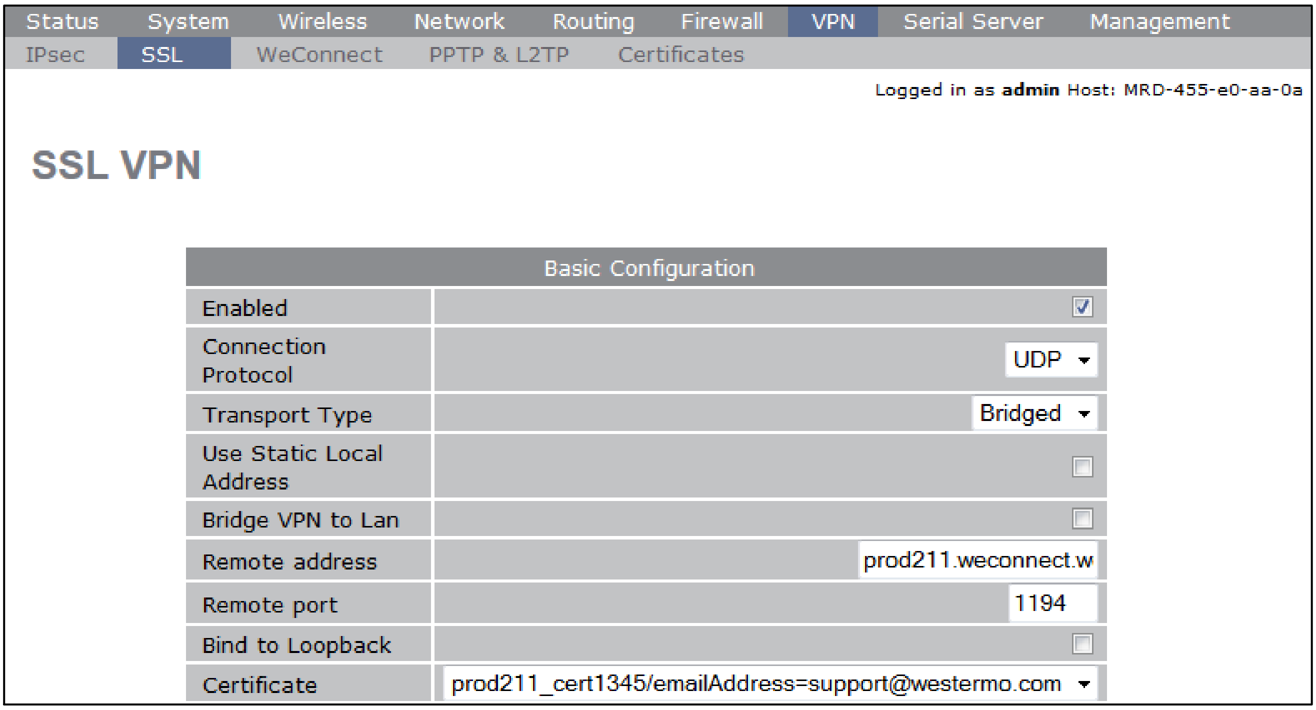
Access Control

Denies all incomming traffic from the outside on the WAN interface.

Allows all traffic from the SSL tunnel to the inside LAN.

External Access Control	Incoming Interface					
	WLS		VPN		GRE	
Default policy	Deny		Allow		Deny	
Services	Allow	Port	Allow	Port	Allow	Port
Web Server	□	80	☑	80	□	80
Secure Web Server	□	443	☑	443	□	443
Telnet Server	□	23	☑	23	□	23
SSH	□	22	☑	22	□	22
SNMP	□	161	☑	161	□	161
GRE	□		☑		□	
Dynamic routing	□		☑		□	
DNP3	□		☑		□	
IPsec VPN	□		☑		□	
Serial Server	□		☑		□	
Respond to ICMP (Ping)	□		☑		□	

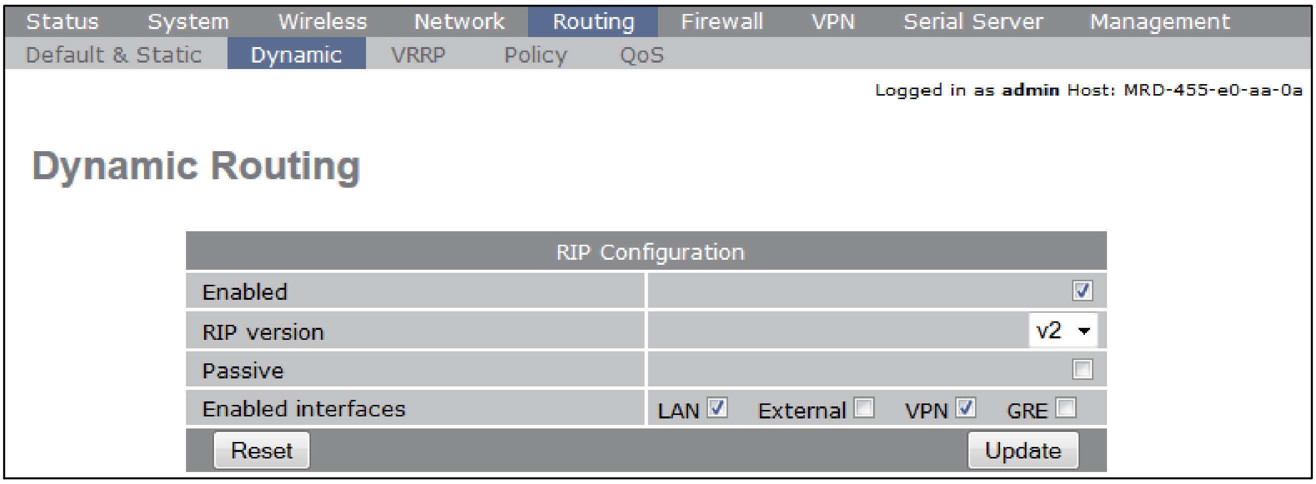
6. Done!
The Node will now download and install the certificates needed and configuration settings for the SSL VPN tunnel from the WeConnect Provisioning Server. As well as the appropriate routing using RIPv2 to announce the Device Network to WeConnect.



Logged in as **admin** Host: MRD-455-e0-aa-0a

SSL VPN

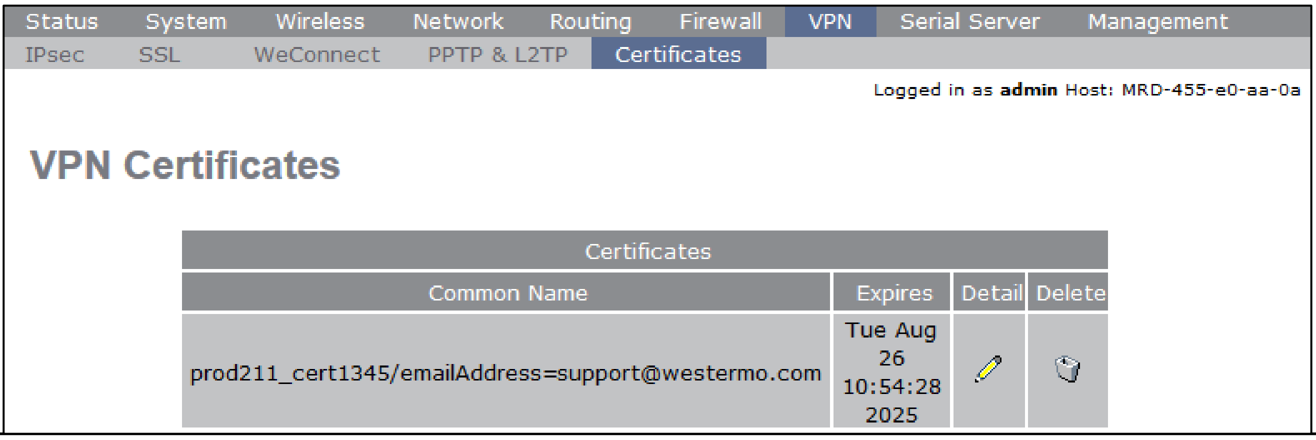
Basic Configuration	
Enabled	☑
Connection Protocol	UDP ▾
Transport Type	Bridged ▾
Use Static Local Address	□
Bridge VPN to Lan	□
Remote address	prod211.weconnect.w
Remote port	1194
Bind to Loopback	□
Certificate	prod211_cert1345/emailAddress=support@westermo.com ▾



Logged in as **admin** Host: MRD-455-e0-aa-0a

Dynamic Routing

RIP Configuration	
Enabled	☑
RIP version	v2 ▾
Passive	□
Enabled interfaces	LAN ☑ External □ VPN ☑ GRE □



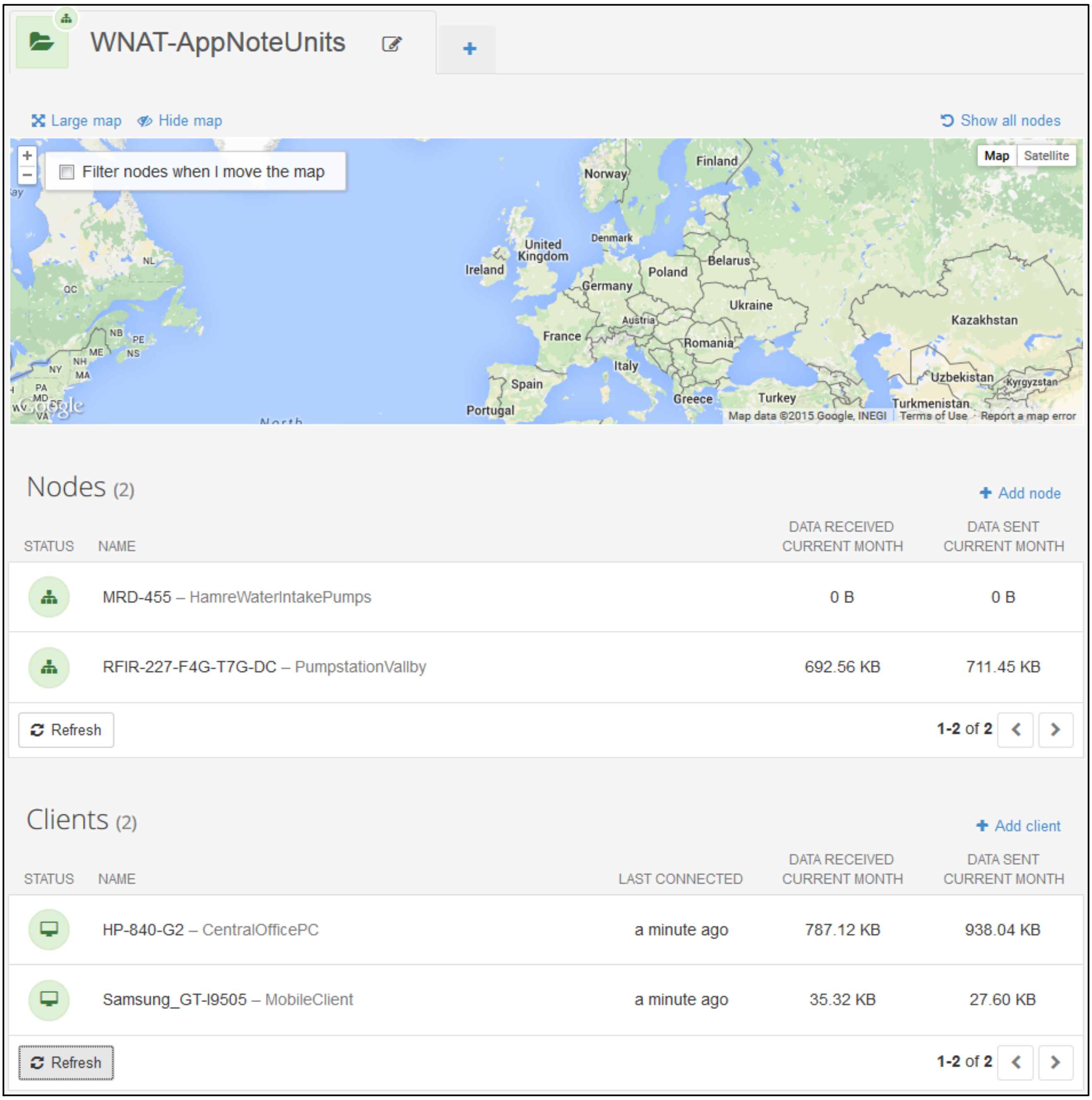
Logged in as **admin** Host: MRD-455-e0-aa-0a

VPN Certificates

Certificates

Common Name	Expires	Detail	Delete
prod211_cert1345/emailAddress=support@westermo.com	Tue Aug 26 10:54:28 2025	✎	🗑

Now all Nodes and Clients are added to WeConnect and are visible in the portal. Connectivity is established to all remote sites through WeConnect without any public IP-addresses on the connected equipment.



Nodes (2)

+ Add node

STATUS	NAME	DATA RECEIVED CURRENT MONTH	DATA SENT CURRENT MONTH
	MRD-455 – HamreWaterIntakePumps	0 B	0 B
	RFIR-227-F4G-T7G-DC – PumpstationVallby	692.56 KB	711.45 KB

Refresh   1-2 of 2

Clients (2)

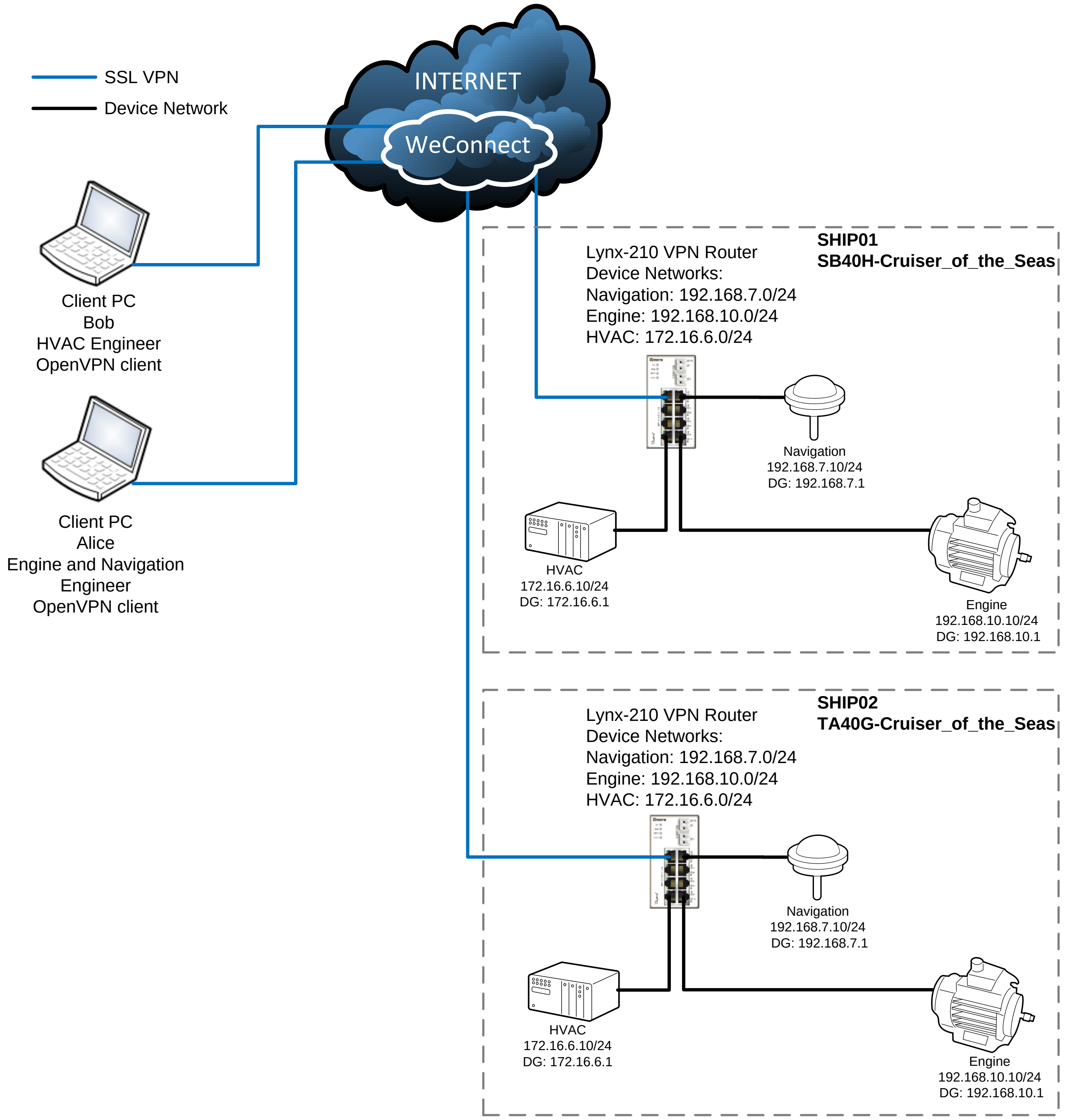
+ Add client

STATUS	NAME	LAST CONNECTED	DATA RECEIVED CURRENT MONTH	DATA SENT CURRENT MONTH
	HP-840-G2 – CentralOfficePC	a minute ago	787.12 KB	938.04 KB
	Samsung_GT-I9505 – MobileClient	a minute ago	35.32 KB	27.60 KB

Refresh   1-2 of 2

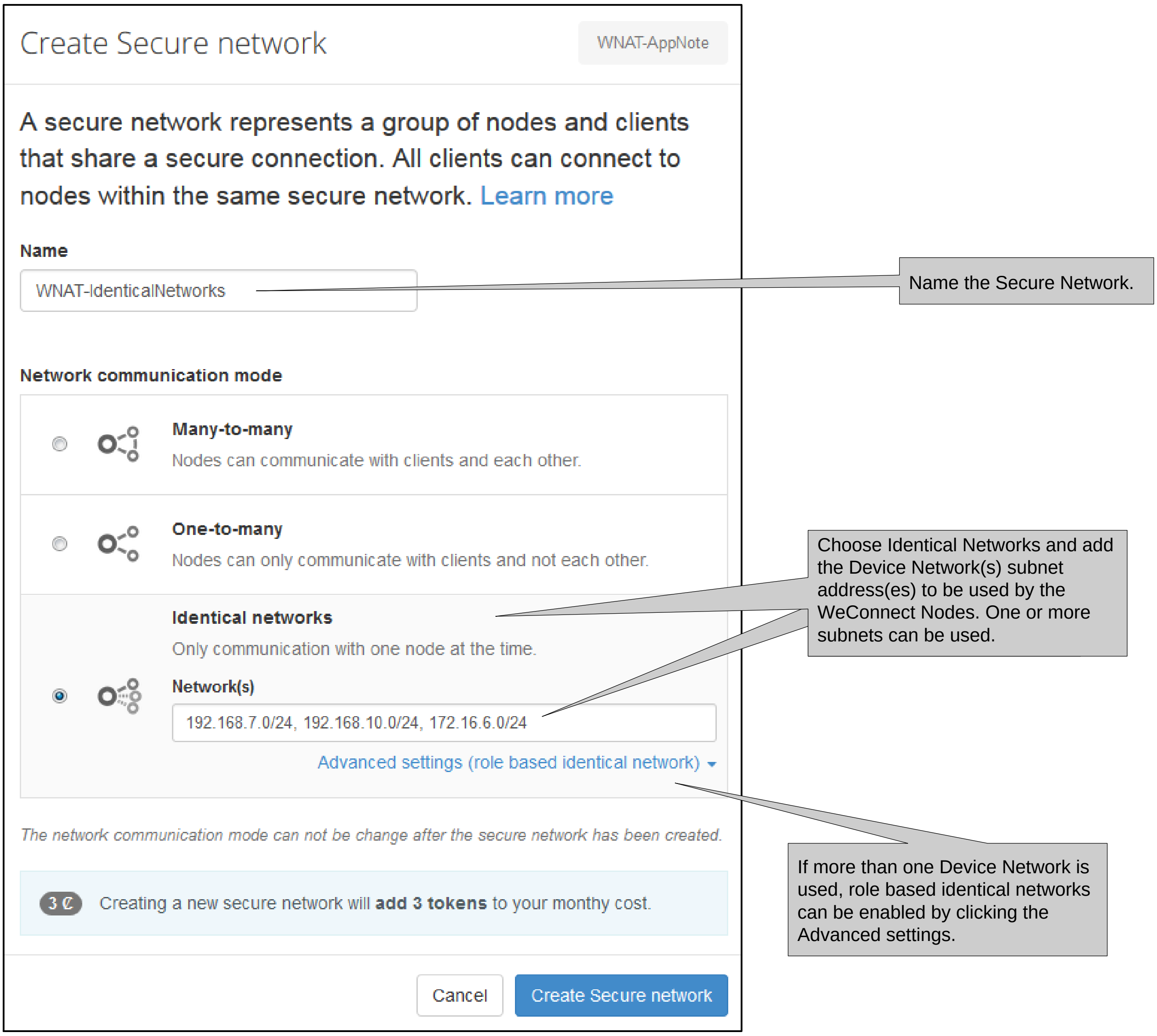
Identical Networks Setup

Identical Networks allows all remote sites to use the same LAN subnet address for its Device Network(s).
This is needed when shipping equipment or systems that are configured identically with the same Device Network(s) on all delivered systems.
There is an advanced setting for Identical Networks where roles can be defined.
Because in some systems not all clients are allowed to communicate with all equipment in the network and this is controlled by different roles and which Device Networks these roles are able to access.
This is examplified with a passenger cruise ship application as shown below.



Setting it Up

1. Start by adding a new Secure Network in the WeConnect Portal as in sections *Account Administration* and *WeConnect Secure Network Creation*.



Create Secure network

A secure network represents a group of nodes and clients that share a secure connection. All clients can connect to nodes within the same secure network. Learn more

Name: WNAT-IdenticalNetworks

Network communication mode

○ **Many-to-many**
Nodes can communicate with clients and each other.

○ **One-to-many**
Nodes can only communicate with clients and not each other.

● **Identical networks**
Only communication with one node at the time.
Network(s): 192.168.7.0/24, 192.168.10.0/24, 172.16.6.0/24

The network communication mode can not be change after the secure network has been created.

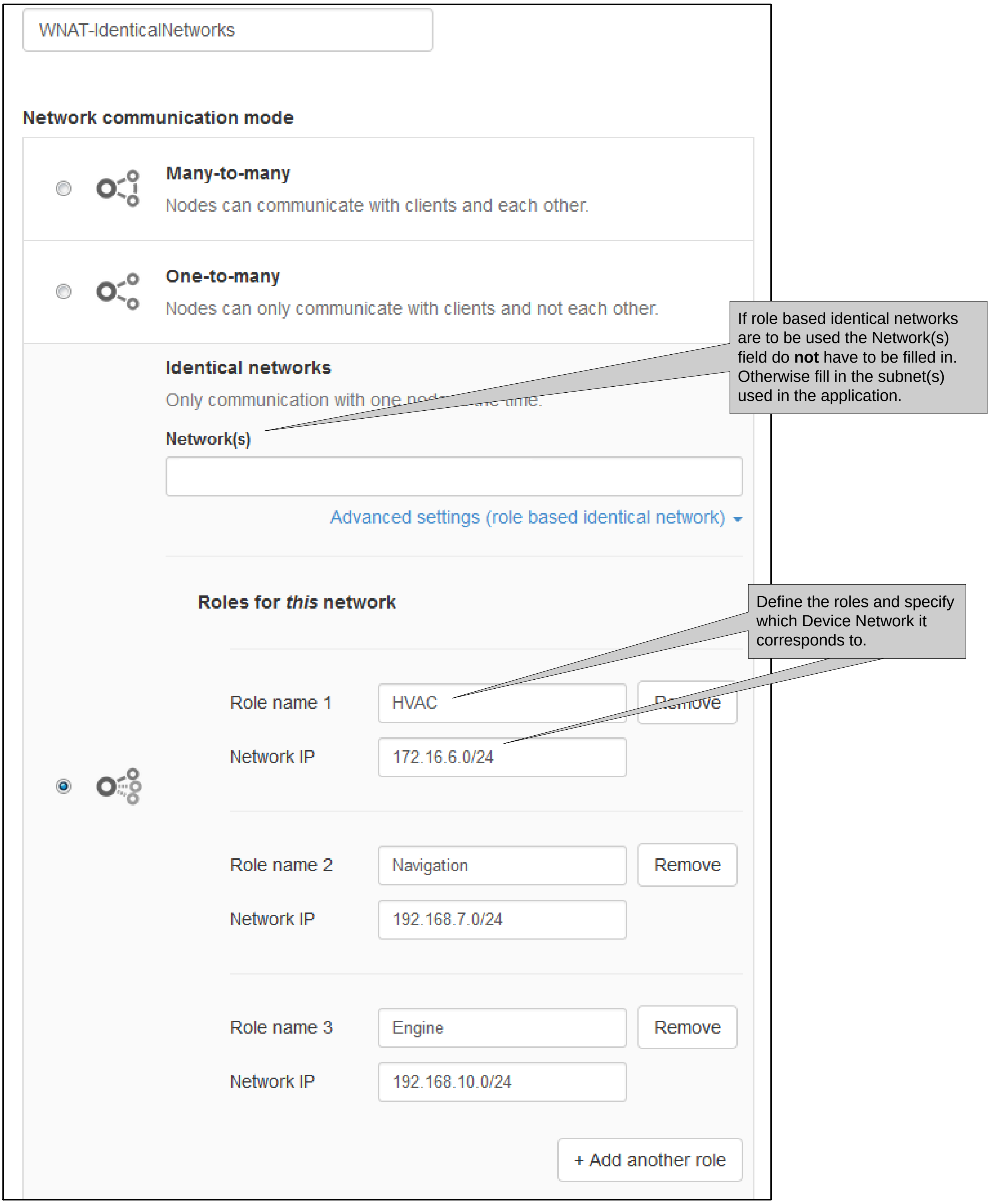
3 ₵ Creating a new secure network will **add 3 tokens** to your monthy cost.

Name the Secure Network.

Choose Identical Networks and add the Device Network(s) subnet address(es) to be used by the WeConnect Nodes. One or more subnets can be used.

If more than one Device Network is used, role based identical networks can be enabled by clicking the Advanced settings.

2. If no role definition is needed proceed to item 3.
Otherwise define the roles needed for the application.
In the cruise ship example three different subnets are defined HVAC, Navigation and Engine.



WNAT-IdenticalNetworks

Network communication mode

○ **Many-to-many**
Nodes can communicate with clients and each other.

○ **One-to-many**
Nodes can only communicate with clients and not each other.

● **Identical networks**
Only communication with one node at the time.

Network(s):

Advanced settings (role based identical network)

Roles for *this* network

Role name 1: HVAC
Network IP: 172.16.6.0/24

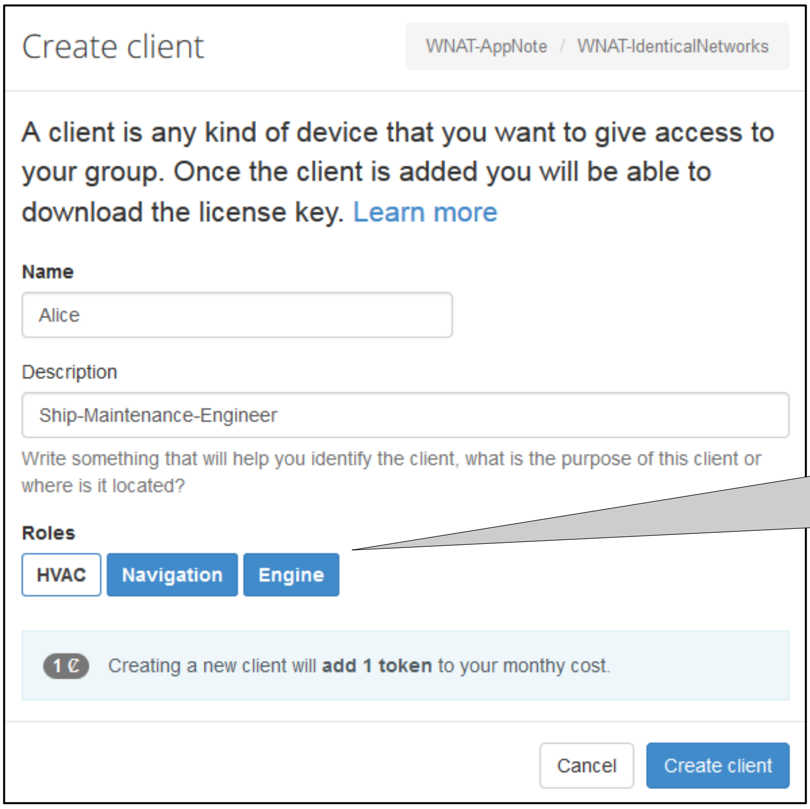
Role name 2: Navigation
Network IP: 192.168.7.0/24

Role name 3: Engine
Network IP: 192.168.10.0/24

If role based identical networks are to be used the Network(s) field do **not** have to be filled in. Otherwise fill in the subnet(s) used in the application.

Define the roles and specify which Device Network it corresponds to.

3. Add clients as in the *Adding Clients* section.
If role based identical networks are configured this is where the roles are defined for each client.



Create client

WNAT-AppNote / WNAT-IdenticalNetworks

A client is any kind of device that you want to give access to your group. Once the client is added you will be able to download the license key. Learn more

Name: Alice

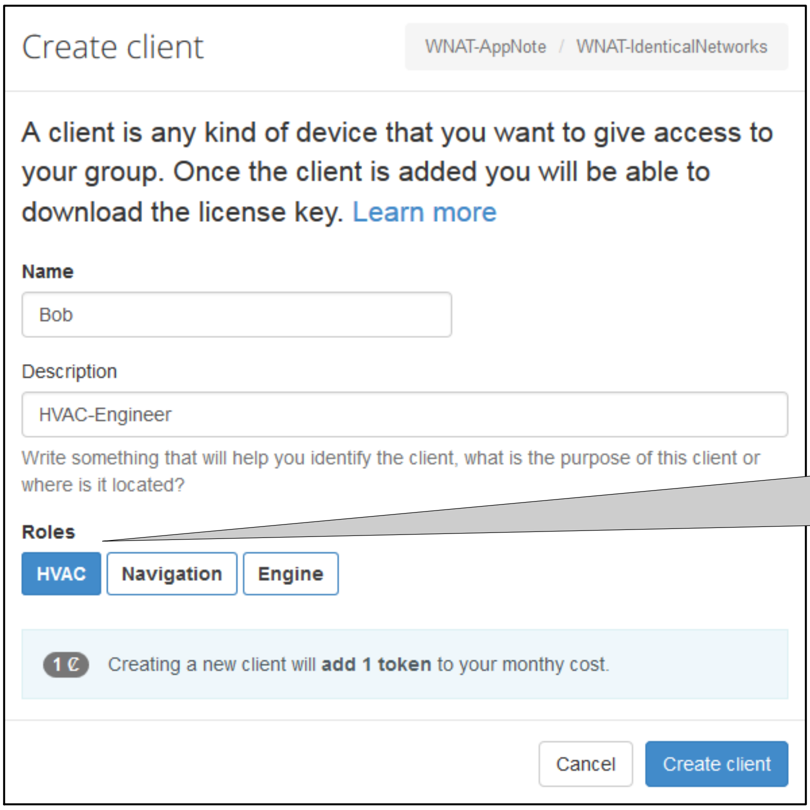
Description: Ship-Maintenance-Engineer

Write something that will help you identify the client, what is the purpose of this client or where is it located?

Roles: HVAC, Navigation (selected), Engine (selected)

1 ₵ Creating a new client will **add 1 token** to your monthy cost.

Mark the roles that the client shall have. This will dictate exactly which Device Network the client are allowed to access.
In the cruise ship example Alice is an Engine and Navigation engineer so she is only allowed to access the Navigation and Engine networks.



Create client

WNAT-AppNote / WNAT-IdenticalNetworks

A client is any kind of device that you want to give access to your group. Once the client is added you will be able to download the license key. Learn more

Name: Bob

Description: HVAC-Engineer

Write something that will help you identify the client, what is the purpose of this client or where is it located?

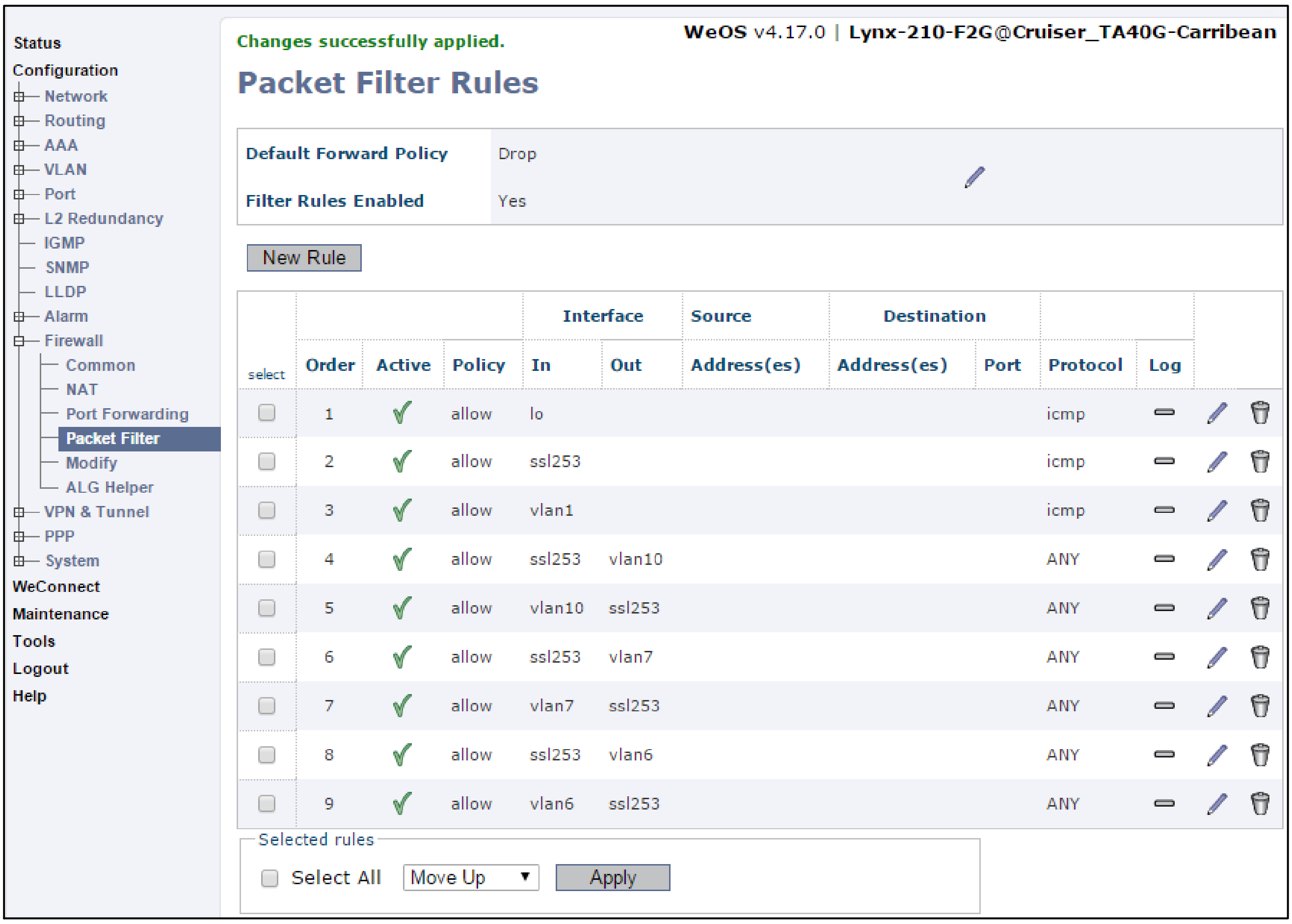
Roles: HVAC (selected), Navigation, Engine

1 ₵ Creating a new client will **add 1 token** to your monthy cost.

Mark the roles that the client shall have. This will dictate exactly which Device Network the client are allowed to access.
In the cruise ship example Bob is an HVAC engineer so he is only allowed to access the HVAC network.

4. Then add the Nodes as in the *Adding Nodes* section.

5. Finally adapt the firewall for the Device Networks used.



Changes successfully applied.

WeOS v4.17.0 | **Lynx-210-F2G@Cruiser_TA40G-Carribean**

Packet Filter Rules

Default Forward Policy	Drop
Filter Rules Enabled	Yes

				Interface		Source	Destination					
select	Order	Active	Policy	In	Out	Address(es)	Address(es)	Port	Protocol	Log		
□	1	✓	allow	lo					icmp	—	✎	🗑
□	2	✓	allow	ssl253					icmp	—	✎	🗑
□	3	✓	allow	vlan1					icmp	—	✎	🗑
□	4	✓	allow	ssl253	vlan10				ANY	—	✎	🗑
□	5	✓	allow	vlan10	ssl253				ANY	—	✎	🗑
□	6	✓	allow	ssl253	vlan7				ANY	—	✎	🗑
□	7	✓	allow	vlan7	ssl253				ANY	—	✎	🗑
□	8	✓	allow	ssl253	vlan6				ANY	—	✎	🗑
□	9	✓	allow	vlan6	ssl253				ANY	—	✎	🗑

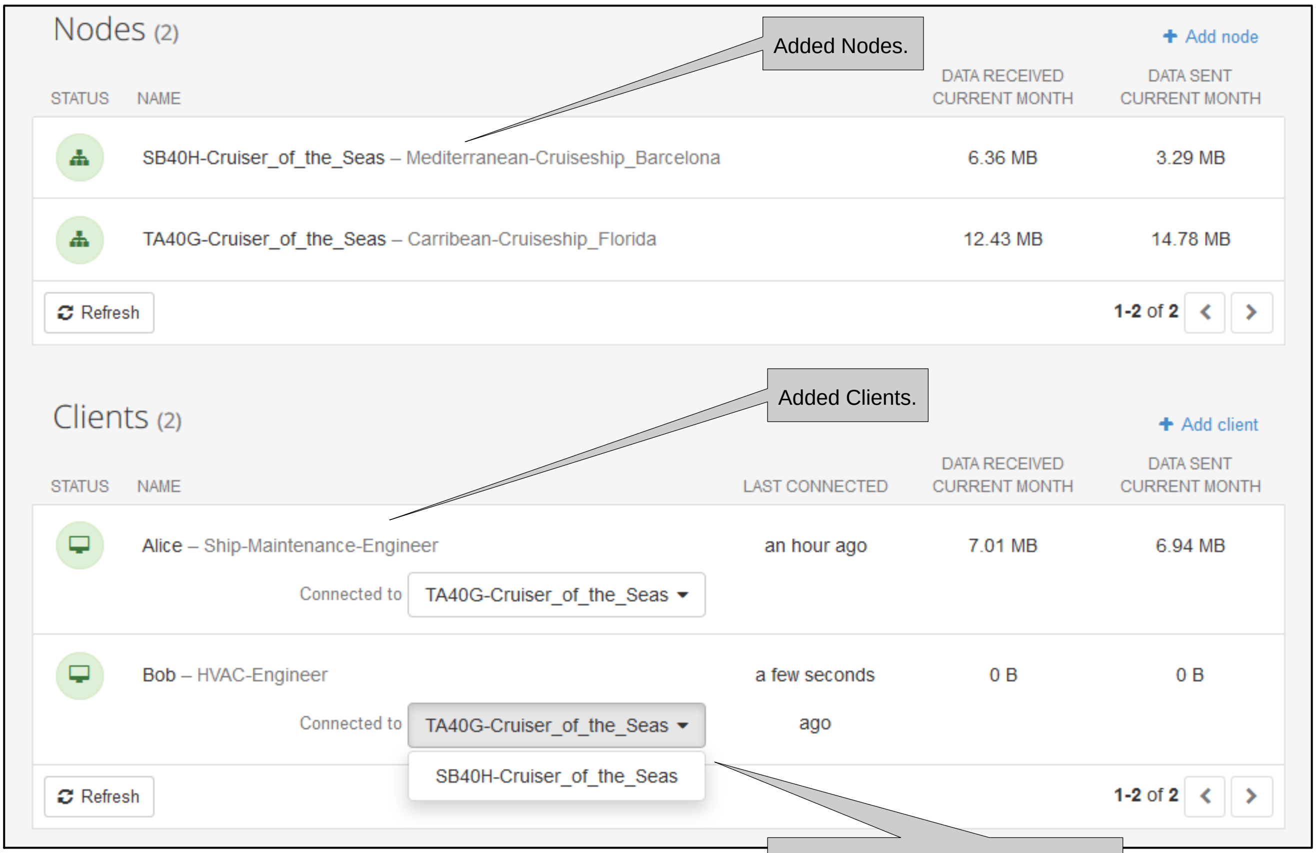
Selected rules

□ Select All Move Up ▼ Apply

Connecting to Device Networks

6. Connecting to the Nodes requires additional input as all Device Networks have the same subnet addresses so the client must distinguish, in the WeConnect Portal, which Node to connect to.

Please Note! If role based identical networks are configured the clients are still only allowed to access those Device Networks that are defined by their role(s) for each Node, eventhough they share the same VPN tunnel.



Nodes (2)

✚ Add node

STATUS	NAME	DATA RECEIVED CURRENT MONTH	DATA SENT CURRENT MONTH
●	SB40H-Cruiser_of_the_Seas – Mediterranean-Cruiseship_Barcelona	6.36 MB	3.29 MB
●	TA40G-Cruiser_of_the_Seas – Carribean-Cruiseship_Florida	12.43 MB	14.78 MB

Refresh 1-2 of 2

Clients (2)

✚ Add client

STATUS	NAME	LAST CONNECTED	DATA RECEIVED CURRENT MONTH	DATA SENT CURRENT MONTH
●	Alice – Ship-Maintenance-Engineer Connected to TA40G-Cruiser_of_the_Seas ▾	an hour ago	7.01 MB	6.94 MB
●	Bob – HVAC-Engineer Connected to TA40G-Cruiser_of_the_Seas ▾ SB40H-Cruiser_of_the_Seas	a few seconds ago	0 B	0 B

Refresh 1-2 of 2

Added Nodes.

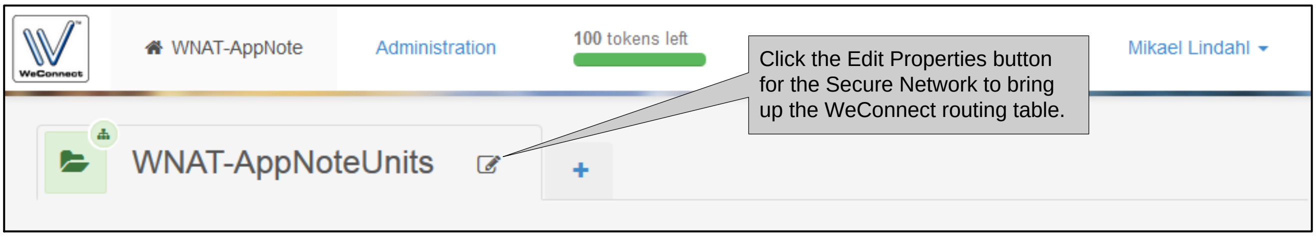
Added Clients.

Choose which Node to connect to from the list.

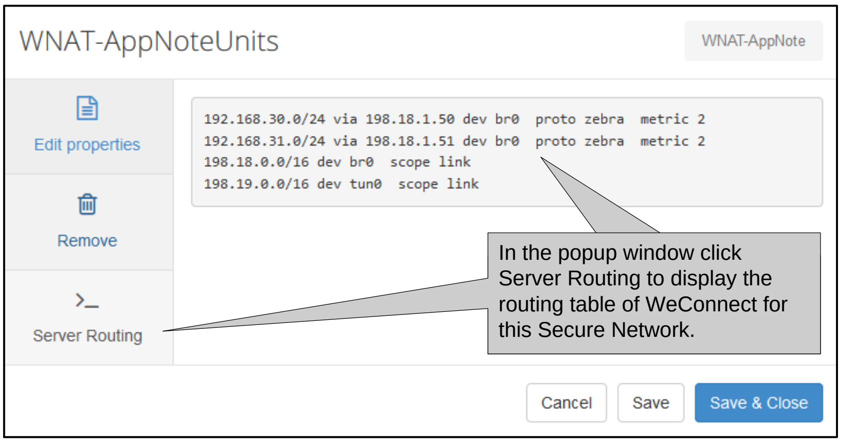
Trouble Shooting

WeConnect Portal

All connections can easily be monitored in the WeConnect portal.

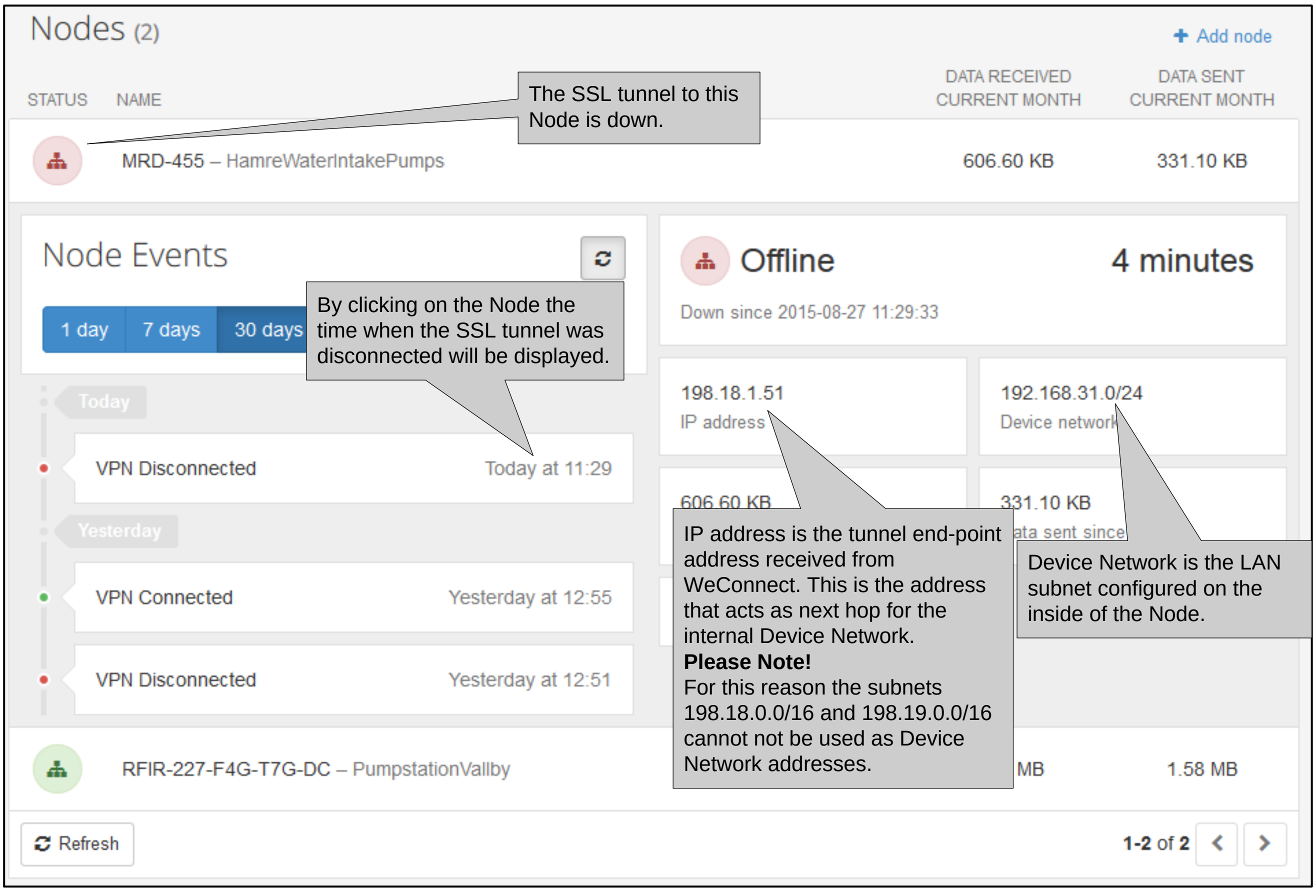


Click the Edit Properties button for the Secure Network to bring up the WeConnect routing table.



```
192.168.30.0/24 via 198.18.1.50 dev br0  proto zebra  metric 2
192.168.31.0/24 via 198.18.1.51 dev br0  proto zebra  metric 2
198.18.0.0/16 dev br0  scope link
198.19.0.0/16 dev tun0  scope link
```

In the popup window click Server Routing to display the routing table of WeConnect for this Secure Network.



STATUS	NAME	DATA RECEIVED CURRENT MONTH	DATA SENT CURRENT MONTH
	MRD-455 – HamreWaterIntakePumps	606.60 KB	331.10 KB
	RFIR-227-F4G-T7G-DC – PumpstationVallby	MB	1.58 MB

VPN Disconnected Today at 11:29

VPN Connected Yesterday at 12:55

VPN Disconnected Yesterday at 12:51

Down since 2015-08-27 11:29:33

198.18.1.51 IP address

192.168.31.0/24 Device network

606.60 KB

331.10 KB ata sent since

The SSL tunnel to this Node is down.

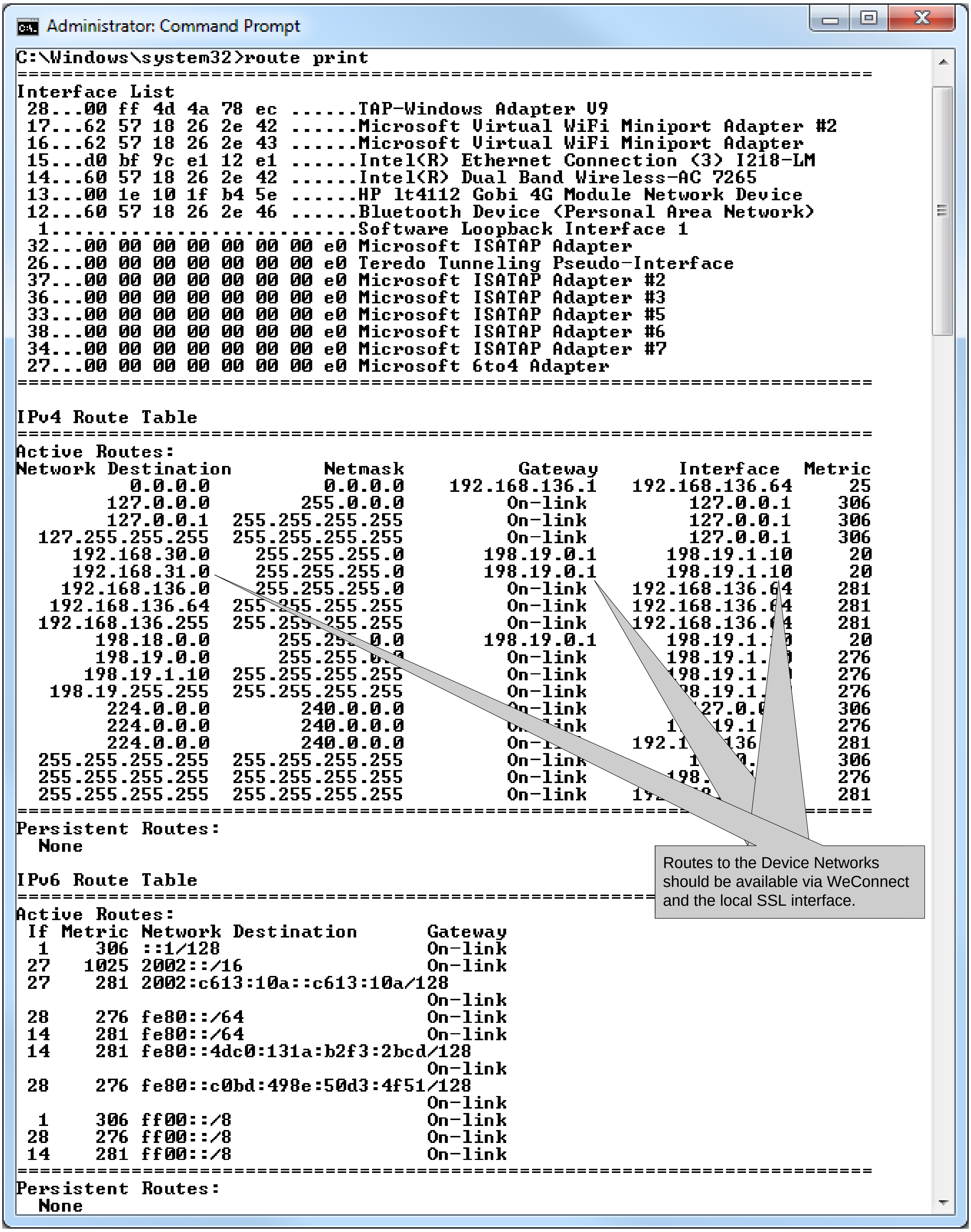
By clicking on the Node the time when the SSL tunnel was disconnected will be displayed.

IP address is the tunnel end-point address received from WeConnect. This is the address that acts as next hop for the internal Device Network.
Please Note!
For this reason the subnets 198.18.0.0/16 and 198.19.0.0/16 cannot not be used as Device Network addresses.

Device Network is the LAN subnet configured on the inside of the Node.

WeConnect Clients

Verify connectivity with Device Networks by issuing the *route print* command from the MS Windows Command Prompt.



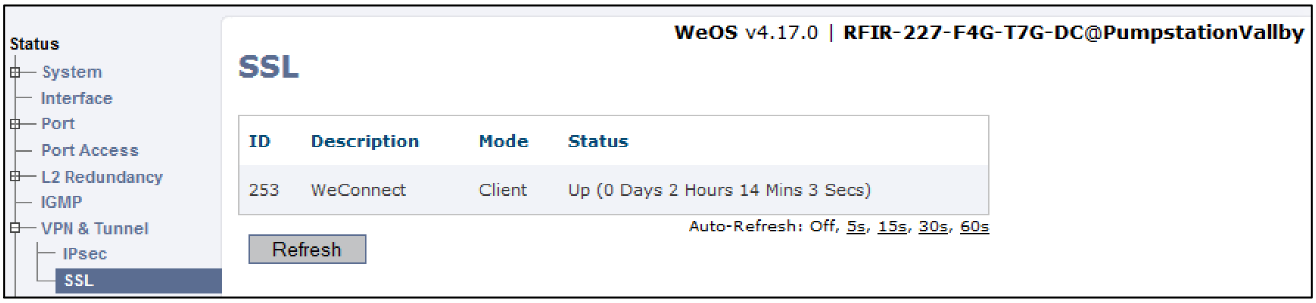
```
C:\Windows\system32>route print
===========================================================================
Interface List
 28...00 ff 4d 4a 78 ec ......TAP-Windows Adapter V9
 17...62 57 18 26 2e 42 ......Microsoft Virtual WiFi Miniport Adapter #2
 16...62 57 18 26 2e 43 ......Microsoft Virtual WiFi Miniport Adapter
 15...d0 bf 9c e1 12 e1 ......Intel(R) Ethernet Connection (3) I218-LM
 14...60 57 18 26 2e 42 ......Intel(R) Dual Band Wireless-AC 7265
 13...00 1e 10 1f b4 5e ......HP lt4112 Gobi 4G Module Network Device
 12...60 57 18 26 2e 46 ......Bluetooth Device (Personal Area Network)
  1...........................Software Loopback Interface 1
 32...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter
 26...00 00 00 00 00 00 00 e0 Teredo Tunneling Pseudo-Interface
 37...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #2
 36...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #3
 33...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #5
 38...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #6
 34...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #7
 27...00 00 00 00 00 00 00 e0 Microsoft 6to4 Adapter
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0    192.168.136.1   192.168.136.64     25
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    306
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    306
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    306
     192.168.30.0    255.255.255.0       198.19.0.1      198.19.1.10     20
     192.168.31.0    255.255.255.0       198.19.0.1      198.19.1.10     20
    192.168.136.0    255.255.255.0         On-link    192.168.136.64    281
   192.168.136.64  255.255.255.255         On-link    192.168.136.64    281
  192.168.136.255  255.255.255.255         On-link    192.168.136.64    281
       198.18.0.0      255.255.0.0       198.19.0.1      198.19.1.10     20
       198.19.0.0      255.255.0.0         On-link       198.19.1.10    276
      198.19.1.10  255.255.255.255         On-link       198.19.1.10    276
   198.19.255.255  255.255.255.255         On-link       198.19.1.10    276
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    306
        224.0.0.0        240.0.0.0         On-link       198.19.1.10    276
        224.0.0.0        240.0.0.0         On-link    192.168.136.64    281
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    306
  255.255.255.255  255.255.255.255         On-link       198.19.1.10    276
  255.255.255.255  255.255.255.255         On-link    192.168.136.64    281
===========================================================================
Persistent Routes:
  None

IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
  1    306 ::1/128                  On-link
 27   1025 2002::/16                On-link
 27    281 2002:c613:10a::c613:10a/128
                                    On-link
 28    276 fe80::/64                On-link
 14    281 fe80::/64                On-link
 14    281 fe80::4dc0:131a:b2f3:2bcd/128
                                    On-link
 28    276 fe80::c0bd:498e:50d3:4f51/128
                                    On-link
  1    306 ff00::/8                 On-link
 28    276 ff00::/8                 On-link
 14    281 ff00::/8                 On-link
===========================================================================
Persistent Routes:
  None
```

Routes to the Device Networks should be available via WeConnect and the local SSL interface.

WeConnect Nodes

WeOS Status Information

Verify functionality by checking the status of the SSL tunnel.
Status -> VPN & Tunnel -> SSL.

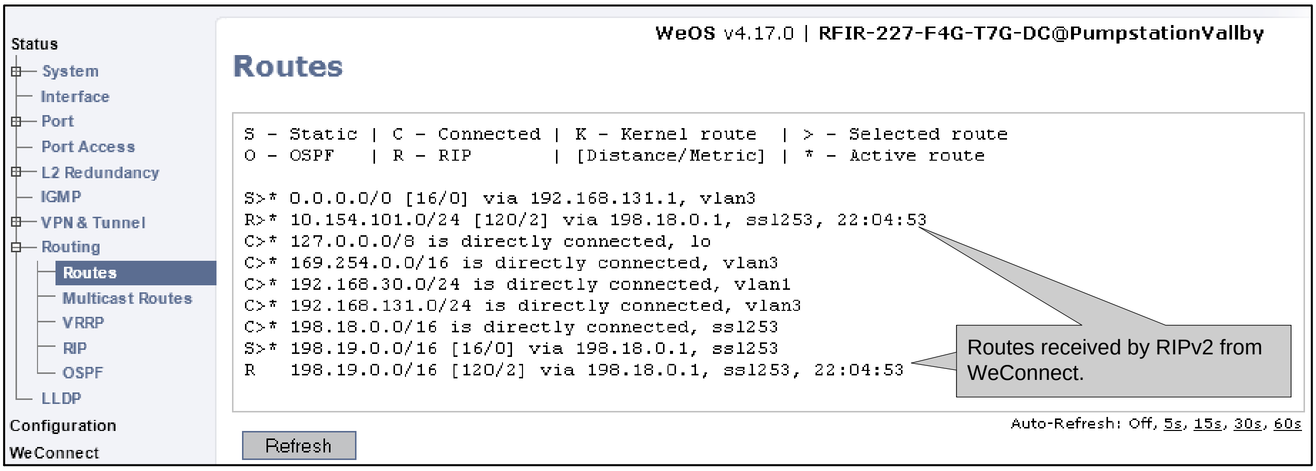


WeOS v4.17.0 | RFIR-227-F4G-T7G-DC@PumpstationVallby

SSL

ID	Description	Mode	Status
253	WeConnect	Client	Up (0 Days 2 Hours 14 Mins 3 Secs)

Verify that the proper routes are received from WeConnect.
Status -> Routing -> Routes



WeOS v4.17.0 | RFIR-227-F4G-T7G-DC@PumpstationVallby

Routes

```
S - Static | C - Connected | K - Kernel route   | > - Selected route
O - OSPF   | R - RIP       | [Distance/Metric] | * - Active route

S>* 0.0.0.0/0 [16/0] via 192.168.131.1, vlan3
R>* 10.154.101.0/24 [120/2] via 198.18.0.1, ssl253, 22:04:53
C>* 127.0.0.0/8 is directly connected, lo
C>* 169.254.0.0/16 is directly connected, vlan3
C>* 192.168.30.0/24 is directly connected, vlan1
C>* 192.168.131.0/24 is directly connected, vlan3
C>* 198.18.0.0/16 is directly connected, ssl253
S>* 198.19.0.0/16 [16/0] via 198.18.0.1, ssl253
R   198.19.0.0/16 [120/2] via 198.18.0.1, ssl253, 22:04:53
```

Routes received by RIPv2 from WeConnect.

Problems connecting to the WeConnect provisioning server.

If the auto provisioning server can not be reached this message will be displayed in the WeOS log:
WeConnect download failed with error code: 2

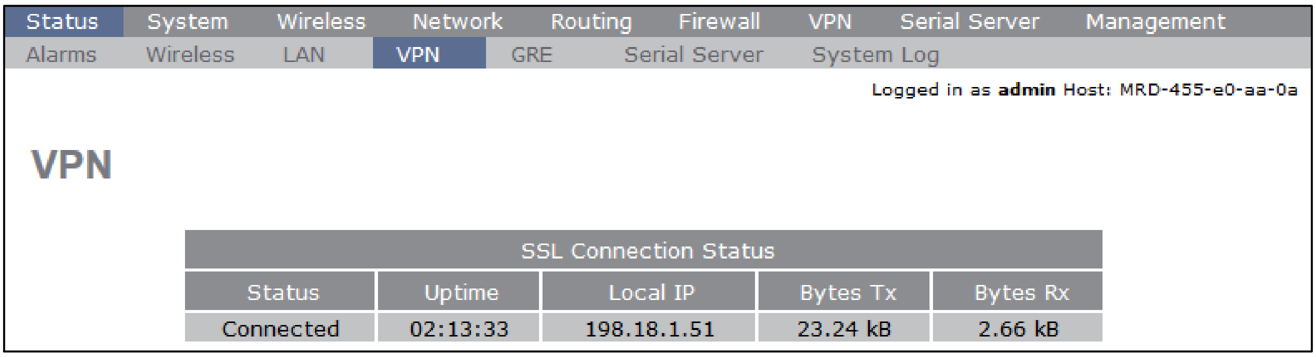
If this occurs make sure that:
-The hostname of the auto provisioning server can be properly resolved.

Problems establishing the VPN tunnel to WeConnect

If the VPN tunnel to WeConnect can not be established make sure that:
-The hostname of the VPN peer (WeConnect) can be properly resolved.
-UDP port 1194 is allowed out to the Internet from where the Node is located.

MRD Status Information

Verify functionality by checking the status of the SSL tunnel.
Status -> VPN.



Logged in as **admin** Host: MRD-455-e0-aa-0a

VPN

SSL Connection Status				
Status	Uptime	Local IP	Bytes Tx	Bytes Rx
Connected	02:13:33	198.18.1.51	23.24 kB	2.66 kB

The System Log will show problems with the tunnel establishment.
A correct tunnel negotiation is shown below.
Status -> System Log.

```
Aug 26 15:12:05 openvpn[30231]: UDPv4 link local (bound): [undef]:1194
Aug 26 15:12:05 openvpn[30231]: UDPv4 link remote: 52.19.135.38:1194
Aug 26 15:12:08 openvpn[30231]: [server] Peer Connection Initiated with 52.19.135.38:1194
Aug 26 15:12:11 openvpn[30231]: TUN/TAP device tap0 opened
Aug 26 15:12:11 openvpn[30231]: /sbin/ifconfig tap0 198.18.1.51 netmask 255.255.0.0 mtu 1500
                                broadcast 198.18.255.255
Aug 26 15:12:11 openvpn[30231]: /etc/ip-up tap0 1500 1589 198.18.1.51 255.255.0.0 init
Aug 26 15:12:11 openvpn[30231]: Initialization Sequence Completed
```

Revision history for version 1.0

Revision	Rev by	Revision note	Date
00	ML	First version	151007
01			
02			
03			
04			
05			
06			
07			

HEAD OFFICE

Sweden
Westermo
SE-640 40 Stora Sundby
Tel: +46 (0)16 42 80 00
Fax: +46 (0)16 42 80 01
info@westermo.se
www.westermo.com

Sales Units
Westermo Data Communications

China
sales.cn@westermo.com
www.cn.westermo.com

France
infos@westermo.fr
www.westermo.fr

Germany
info@westermo.de
www.westermo.de

North America
info@westermo.com
www.westermo.com

Singapore
sales@westermo.com.sg
www.westermo.com

Sweden
info.sverige@westermo.se
www.westermo.se

United Kingdom
sales@westermo.co.uk
www.westermo.co.uk

Other Offices

For complete contact information, please visit our website at www.westermo.com/contact or scan the QR code with your mobile phone.