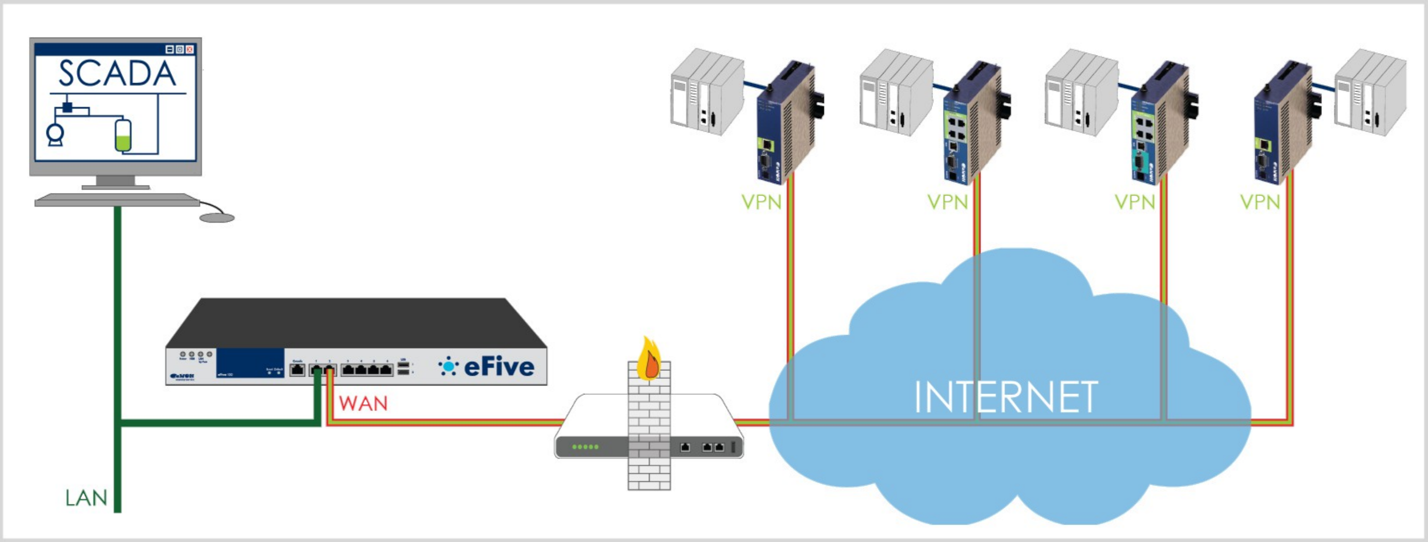
eWON Application User Guide

AUG 050 / Rev 1.6

eFive System and VPN Configuration



Contents

This application user guide explains step by step how to configure the eFive and the eWON in order to link them by a VPN network using the eWON as VPN-client and the eFive as VPN-Server.

What are the eFive 25 & 100 ?

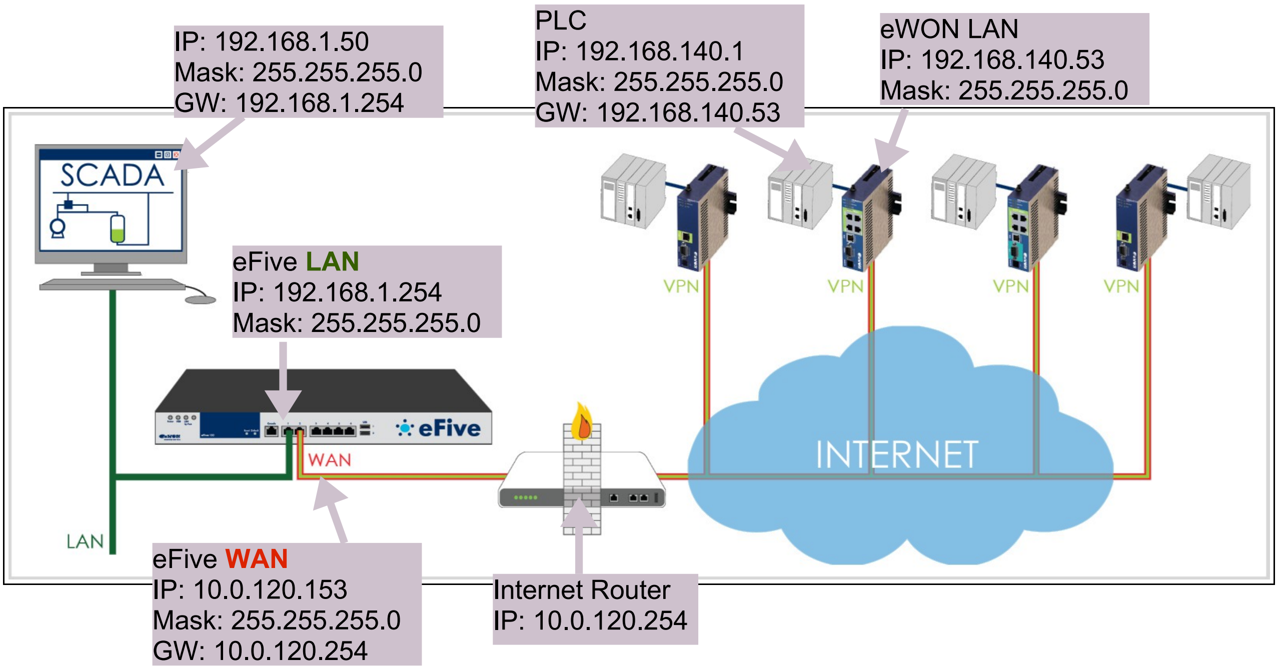
The eFive 25 and 100 are hardware platforms featuring a Virtual Private Network (VPN) gateway with OpenVPN. It has been designed to be a perfect match with the eWON range to build a VPN network. The eFive 25 and 100 act as OpenVPN Servers and the eWONs as OpenVPN Clients. The model eFive 25 is designed to support up to ***50 VPN Clients***; the eFive 100 supports up to ***200 VPN Clients***. Each model is covered by its own Installation Guide, namely IG-012-0-EN for the eFive 25 and IG-013-0-EN for the eFive 100. These guides are available on the eWON support site http://wiki.ewon.biz/efive.

This guide explains how to configure the eFive and the eWON to get the VPN network as shown on the diagram below.

How the VPN network is realized is explained in Step 1 to step 7 of this guide.
In the appendixes, you find additional information regarding

- ➔ Backup & restore
- ➔ Shutdown and Restart
- ➔ Firewall configuration

The objective is to connect for example a SCADA PC to the PLC devices behind the eWON. The SCADA PC makes part of the LAN network of the eFive and has the eFive as its default Gateway. When the VPN connection is established between the eWON and the eFive, the eFive routes the requests from the SCADA to the network behind the eWON.
An example of typical IP address configuration is given in the picture below. We will use these addresses during configuration steps inside this manual.

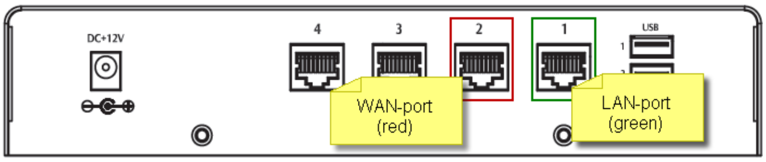


To reach the PLC behind the eWON, the SCADA PC will then just need to use the local IP address of the PLC (= 192.168.140.1).

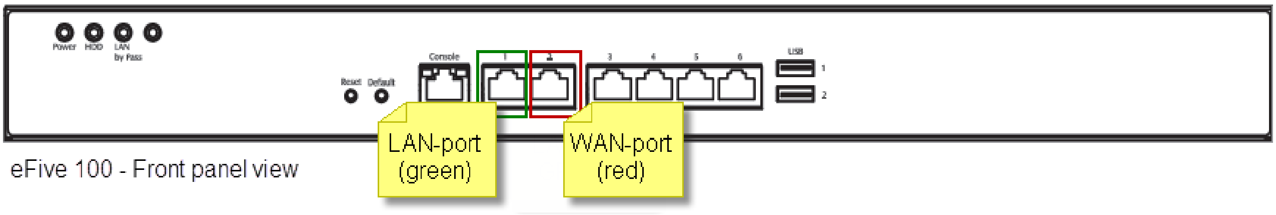
Step 1 - Connect to the eFive Web Page

The factory default IP address of the LAN port of the eFive is
IP: **10.0.0.153**
Mask: 255.255.555.0

Connect your PC to the LAN-port of your eFive (Port 1 as shown on the pictures here under). Make sure that your PC has an IP address that is compatible with the default LAN IP address of the eFive.



eFive 25 - backpanel view



eFive 100 - Front panel view

Open your browser and type the default address: **10.0.0.153** in the URL field (1)

Hit ***Enter***. The eFive redirects this address to https://10.0.0.153:8443/ .

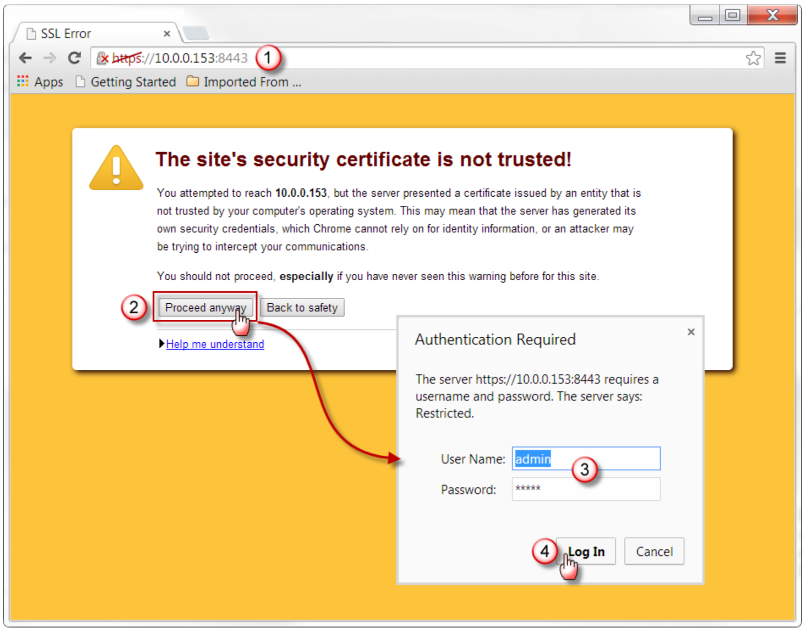
You can discard the security warning as shown (2).

A popup (3) allows you to enter the Login/Password of the eFive.

The default credentials are:

Default login: ***admin***
Default pwd: ***admin***

Click ***Log In*** (4)



The site's security certificate is not trusted!

You attempted to reach **10.0.0.153**, but the server presented a certificate issued by an entity that is not trusted by your computer's operating system. This may mean that the server has generated its own security credentials, which Chrome cannot rely on for identity information, or an attacker may be trying to intercept your communications.

You should not proceed, **especially** if you have never seen this warning before for this site.

Authentication Required

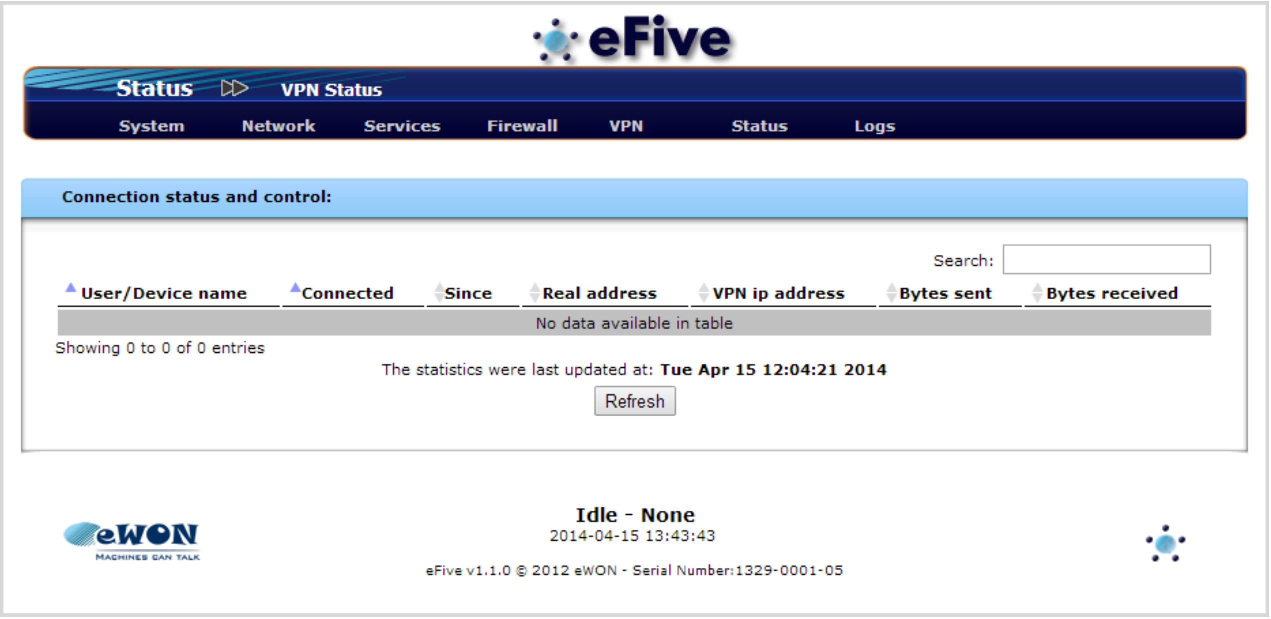
The server https://10.0.0.153:8443 requires a username and password. The server says: Restricted.

User Name: admin
Password: *****

Warning!

For security reasons, changing the default password ***admin*** is absolutely required.
Changing the password is explained in Step 5 - Password Change

The ***Home*** page of the eFive opens.



Connection status and control:

User/Device name	Connected	Since	Real address	VPN ip address	Bytes sent	Bytes received
No data available in table						

Showing 0 to 0 of 0 entries

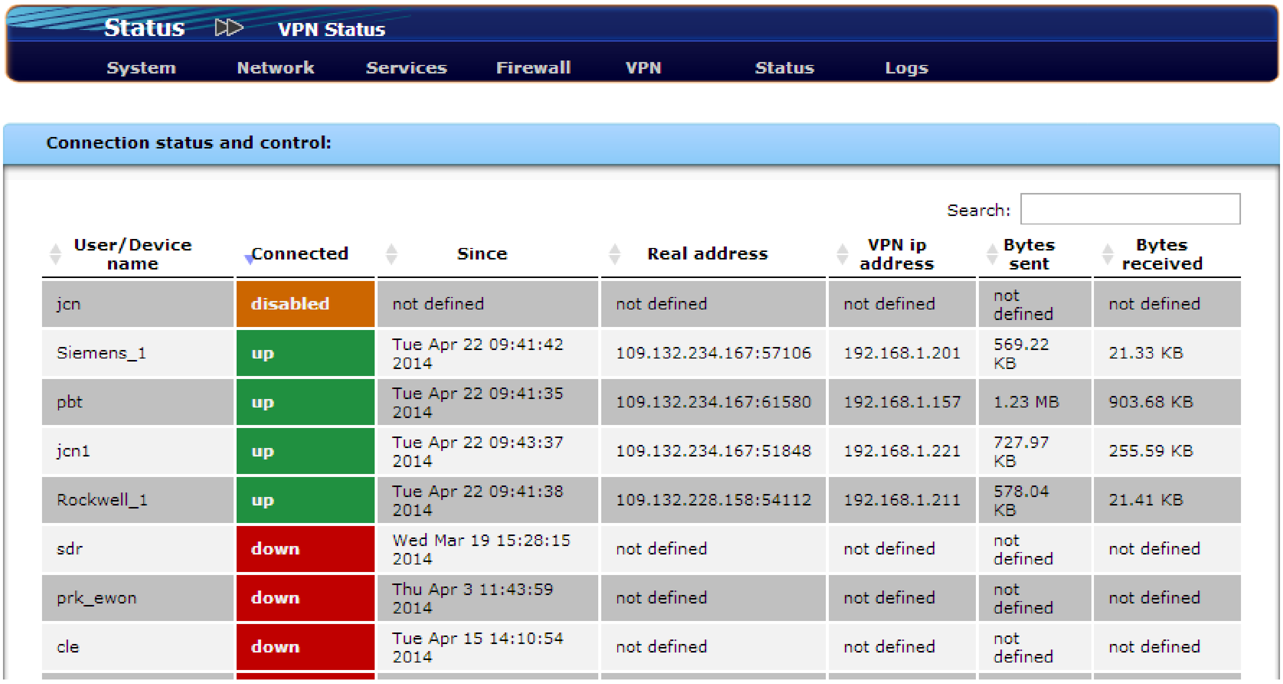
The statistics were last updated at: **Tue Apr 15 12:04:21 2014**

Idle - None
2014-04-15 13:43:43

eFive v1.1.0 © 2012 eWON - Serial Number:1329-0001-05

The ***Home*** page normally shows the list of ***Accounts*** (Users and Devices). As shown above, this list is empty when accessing an unconfigured (or reset) eFive for the first time.

Once ***Accounts*** will be created (see Creating User/Device Accounts (VPN Clients)), they will appear in this page with their respective status:



Connection status and control:

User/Device name	Connected	Since	Real address	VPN ip address	Bytes sent	Bytes received
jcn	disabled	not defined	not defined	not defined	not defined	not defined
Siemens_1	up	Tue Apr 22 09:41:42 2014	109.132.234.167:57106	192.168.1.201	569.22 KB	21.33 KB
pbt	up	Tue Apr 22 09:41:35 2014	109.132.234.167:61580	192.168.1.157	1.23 MB	903.68 KB
jcn1	up	Tue Apr 22 09:43:37 2014	109.132.234.167:51848	192.168.1.221	727.97 KB	255.59 KB
Rockwell_1	up	Tue Apr 22 09:41:38 2014	109.132.228.158:54112	192.168.1.211	578.04 KB	21.41 KB
sdr	down	Wed Mar 19 15:28:15 2014	not defined	not defined	not defined	not defined
prk_ewon	down	Thu Apr 3 11:43:59 2014	not defined	not defined	not defined	not defined
cle	down	Tue Apr 15 14:10:54 2014	not defined	not defined	not defined	not defined

As shown here, ***Accounts*** in the ***Home*** page can have three different connection status:

- ***Disabled*** – the account was disabled (access through ***VPN > Accounts***)
- ***Down*** – the account is not connected
- ***Up*** = the account is connected.

Step 2 - Network Interface Configuration

Network Color Definitions

eFive uses color-coding system of Red, Green, Blue and Orange to describe the roles or security levels which an interface/network segment will have in protecting your network.

Color coding is logical in that it represents a continuum of network access from restricted to permissive.

Red Represents your untrusted interface/segment. This is the interface connected to Internet where eFive will listen for VPN connections.

Green Is the trusted interface/segment of your internal network. All VPN connections will be bridged to this network.

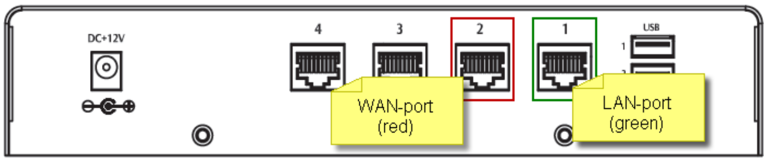
Blue This interface/segment can be used to create a separate network, like a separate WIFI network for example.
Note: There is no WIFI-card on the eFive device. But this interface could be used to connect a Wireless network and to allocate special firewall rules to it

Orange Is for a DMZ (Demilitarized Zone) – This interface/segment works with medium security level in order to allow access from outside (Red interface) and from inside (Green interface)

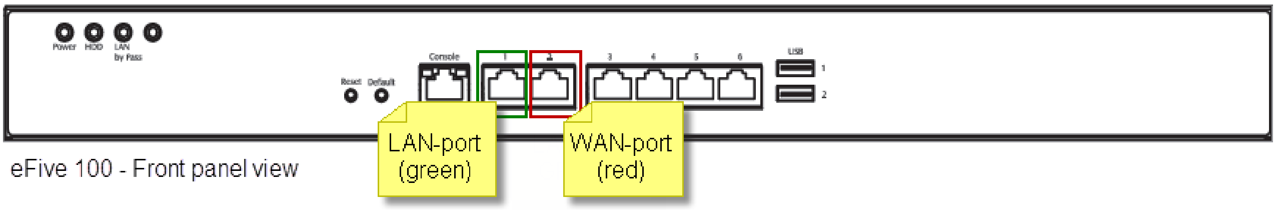
In this guide we will focus on the Green and Red networks.
This is the most common use of the eFive VPN server.

In a simple eFive VPN network, we just need:

- ➔ a LAN – Trusted internal network segment (Green interface)
- ➔ a WAN – Untrusted internet network segment (Red interface)



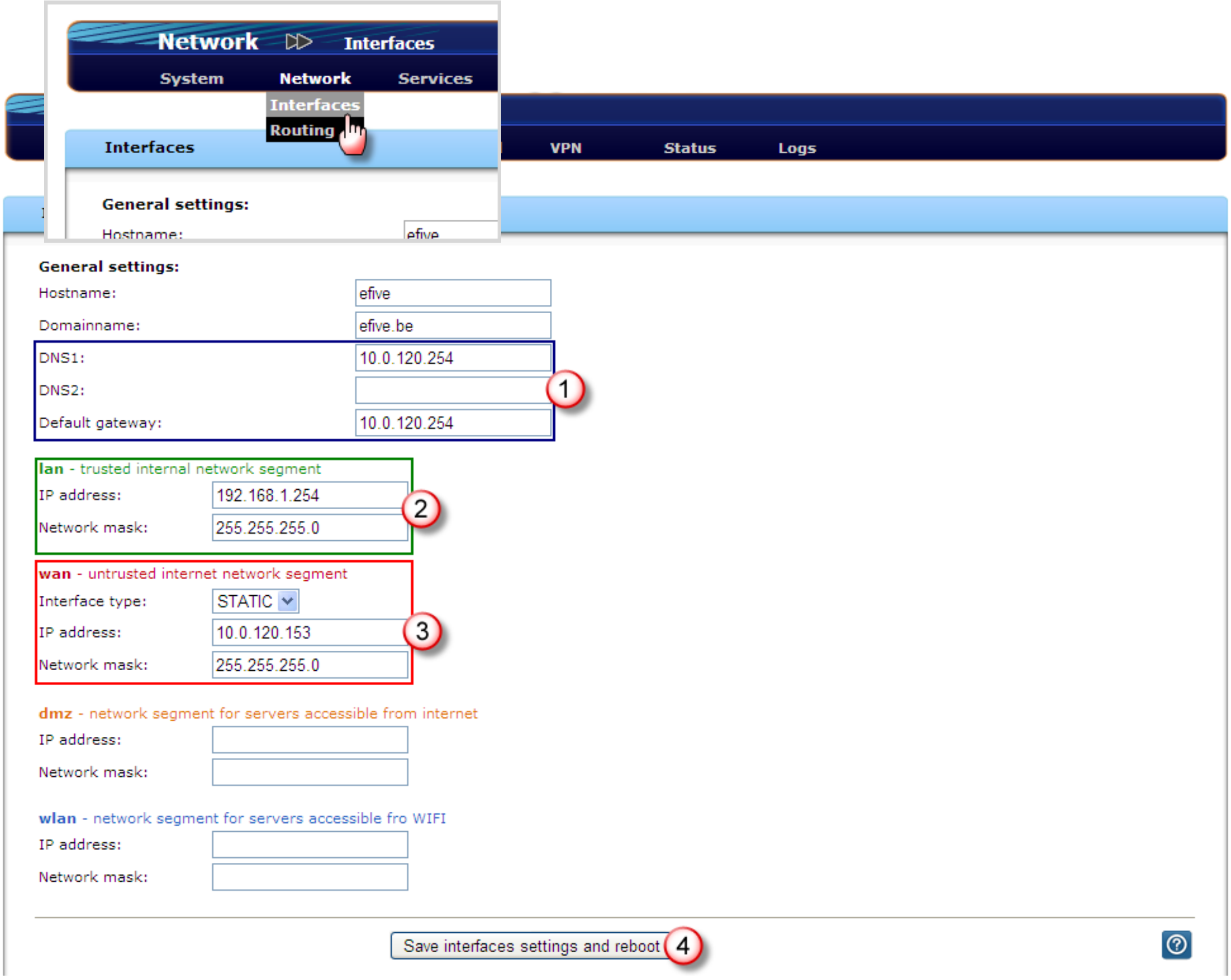
eFive 25 - backpanel view



eFive 100 - Front panel view

Configuration

- From the menu bar, click on ***Network***, ***Interfaces***. The following window appears:



General settings:

Hostname: efive

Domainname: efive.be

DNS1: 10.0.120.254

DNS2:

Default gateway: 10.0.120.254

lan - trusted internal network segment

IP address: 192.168.1.254

Network mask: 255.255.255.0

wan - untrusted internet network segment

Interface type: STATIC

IP address: 10.0.120.153

Network mask: 255.255.255.0

dmz - network segment for servers accessible from internet

IP address:

Network mask:

wlan - network segment for servers accessible fro WIFI

IP address:

Network mask:

- In the ***General Settings*** (1), enter the IP addresses for the ***DNS*** and ***Default Gateway*** in order to inform eFive how to reach the Internet.
  Inside the ***Host Name*** and ***Domain Name*** enter a specific host and domain name for the eFive if you have one. Otherwise leave them as they are.

- In the green network (2), configure the ***IP address*** and ***Network Mask*** for the LAN side of the eFive***.***

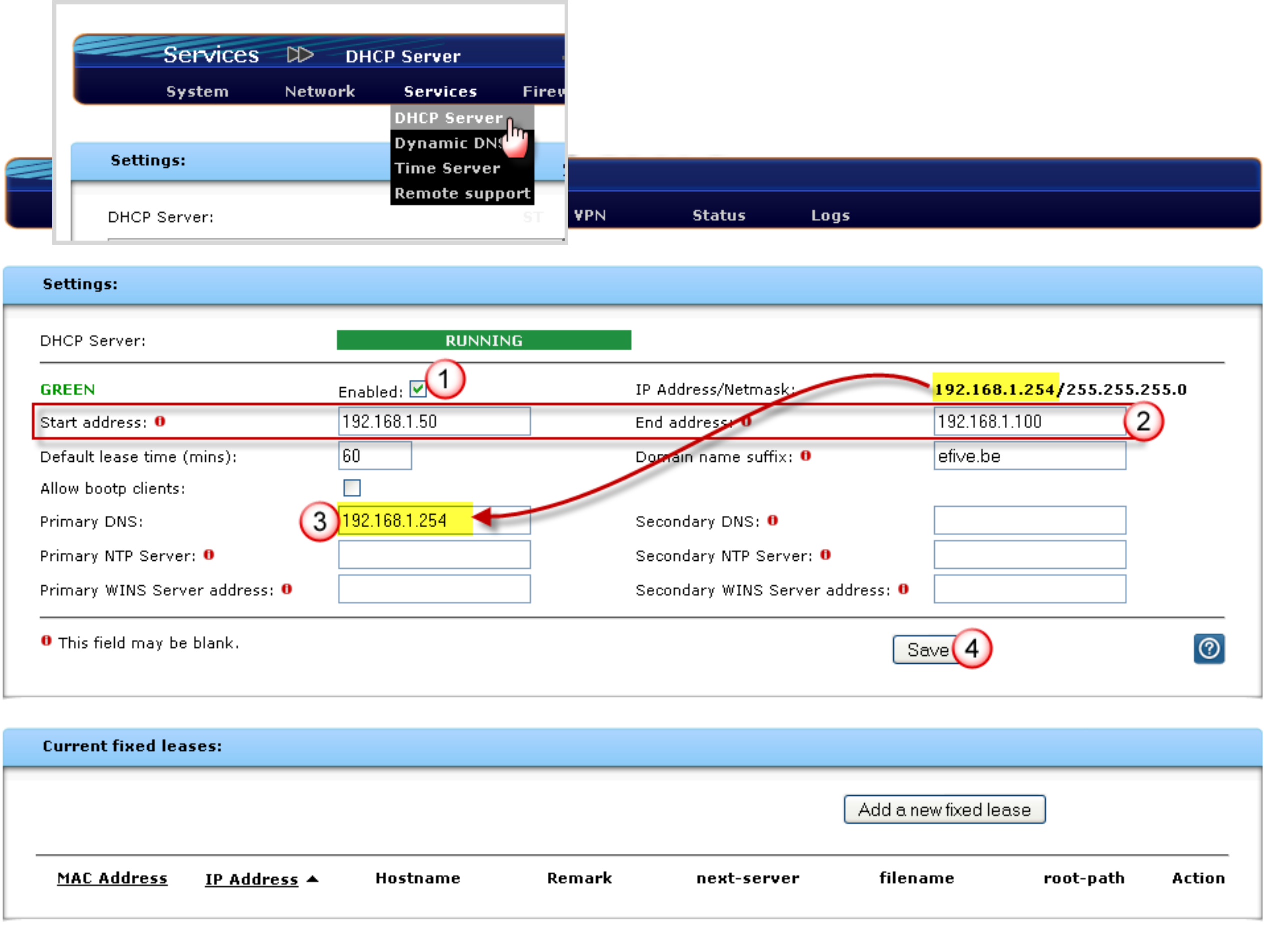
- In the red network (3), configure the ***IP address*** and ***Network Mask*** for the WAN side of the eFive***.***
  Note: DHCP could also be used for the network configuration. But as the Internet Router must forward the VPN packets to this interface, here it is better to use a fixed known IP address.

- As we will not use the orange (DMZ) and blue (Wlan) network, we will leave these fields blank do deactivate the interface.

- Click ***Save*** (4).
  The eFive will shutdown and reboot, a process that takes a couple of minutes. The unit emits typical tones at shutdown and restart. The reboot process ends with a beep.

DHCP Server

- If you want the eFive to allocate IP addresses automatically to computers that are connected to the eFive LAN side (like the SCADA PC for example) from the main menu, select ***Services, DHCP Server***



Settings:

DHCP Server: RUNNING

GREEN

Enabled:	☑	IP Address/Netmask:	192.168.1.254/255.255.255.0
Start address: !	192.168.1.50	End address: !	192.168.1.100
Default lease time (mins):	60	Domain name suffix: !	efive.be
Allow bootp clients:	□		
Primary DNS:	192.168.1.254	Secondary DNS: !	
Primary NTP Server: !		Secondary NTP Server: !	
Primary WINS Server address: !		Secondary WINS Server address: !	

! This field may be blank.

Save

Current fixed leases:

Add a new fixed lease

MAC Address	IP Address ▲	Hostname	Remark	next-server	filename	root-path	Action

- Check the ***Enabled*** check box (1) for the ***GREEN*** network.

- Configure a ***Start address*** and an ***End address*** for DHCP allocation on the green network (2). **Note**: *Specify here an IP range which is in the eFive LAN network. Make sure that the selected IP range does not overlap the IP range specified for the VPN Dynamic IP Pool server of the LAN network (under menu **VPN > Basic Settings,** see Step 4*).

- In the Primary DNS (3), enter the LAN IP address of the eFive you have configured. *This address can be copied from the IP Address/Network information field appearing in the top right corner as shown in the picture above.*

- You can leave the other fields blank.

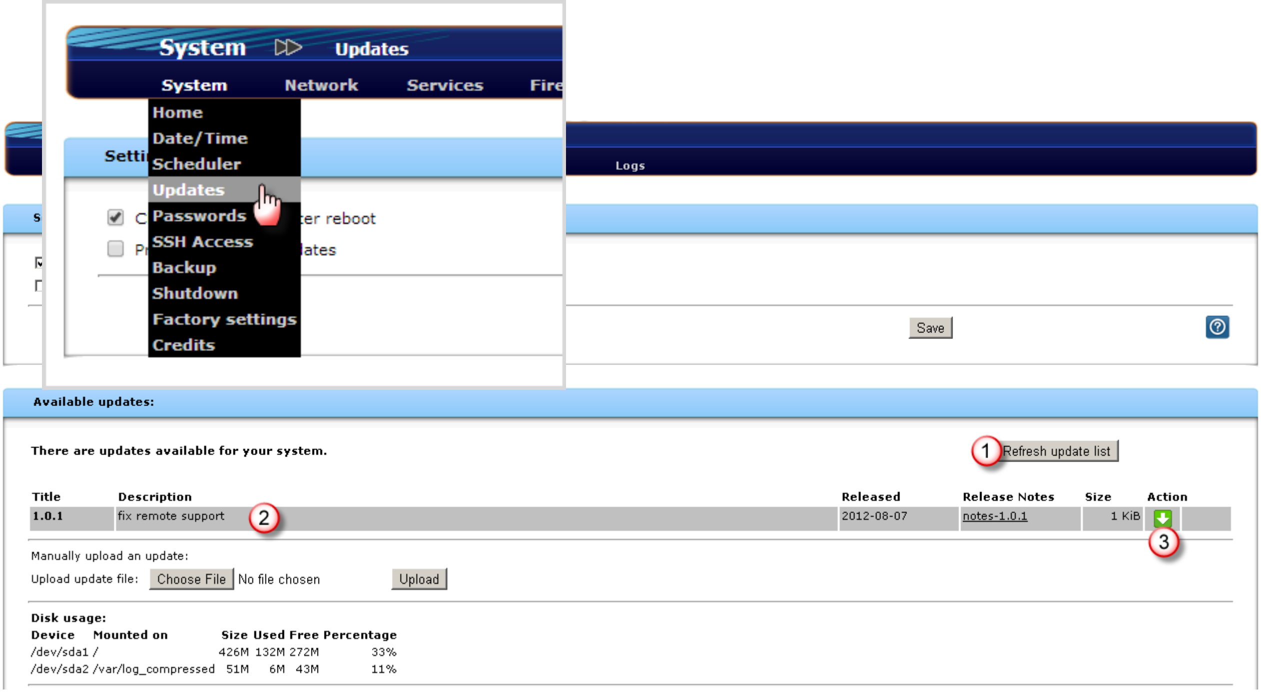
- Click ***Save*** (4).

Step 3 - Check for Updates

Before going further in the configuration, it is now recommended to check if updates are available for your eFive in order to benefit from the latest developments and fixes.

Note: this function works only if the DNS and Default Gateway have been configured as per Step 2 - Network Interface Configuration

- To check for updates, make sure the RED interface (Port #2) is connected to the network with Internet access.
- From the main menu, click on ***System*** > ***Updates***



Available updates:

There are updates available for your system.

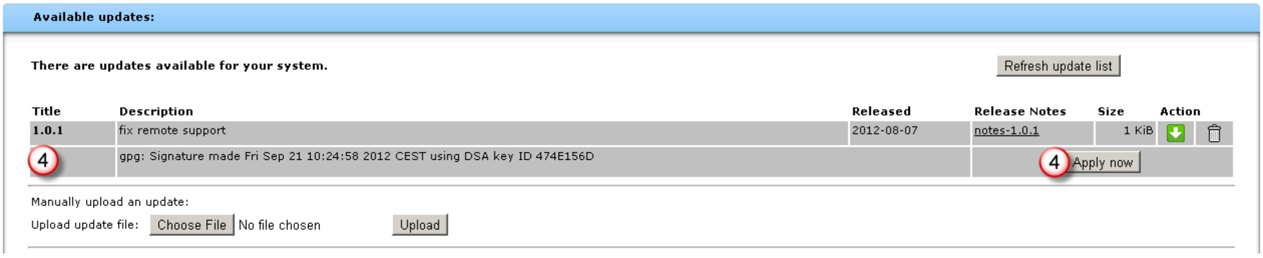
Refresh update list

Title	Description	Released	Release Notes	Size	Action
1.0.1	fix remote support	2012-08-07	notes-1.0.1	1 KiB	

Manually upload an update:

Upload update file: Choose File No file chosen Upload

```
Disk usage:
Device    Mounted on          Size Used Free Percentage
/dev/sda1 /                   426M 132M 272M        33%
/dev/sda2 /var/log_compressed  51M   6M  43M        11%
```



Available updates:

There are updates available for your system.

Refresh update list

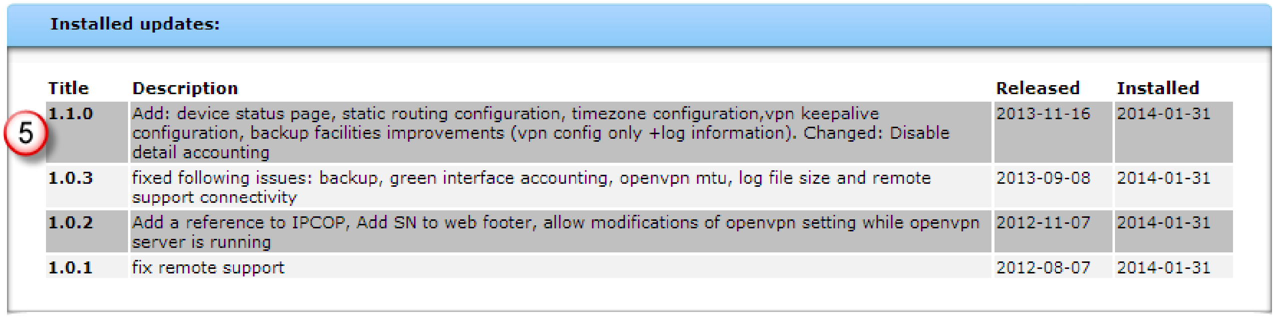
Title	Description	Released	Release Notes	Size	Action
1.0.1	fix remote support	2012-08-07	notes-1.0.1	1 KiB	
	gpg: Signature made Fri Sep 21 10:24:58 2012 CEST using DSA key ID 474E156D		Apply now		

Manually upload an update:

Upload update file: Choose File No file chosen Upload

- To refresh the list of available updates, click ***Refresh update list*** (1).
- This action is gathering the information and, if an update is found, it is displayed in the ***Available updates*** (2) zone.
- Click on the green arrow (3) to download the file on your eFive. This operation will not launch the update process; it will just copy the file on the disk of your eFive.
- To install the update on your eFive, click on ***Apply Now*** (4) button.

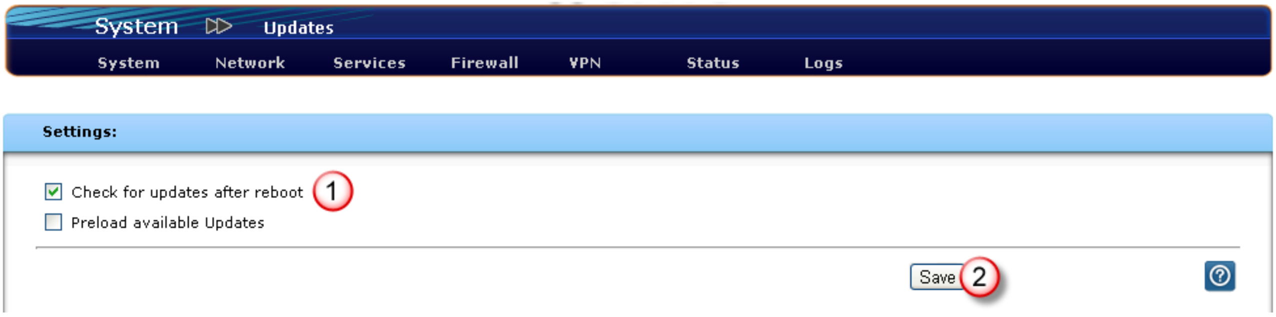
- After successful installation, the newly installed update is listed in the ***Installed updates*** zone (5) displayed on the bottom of the page.



Installed updates:

Title	Description	Released	Installed
1.1.0	Add: device status page, static routing configuration, timezone configuration,vpn keepalive configuration, backup facilities improvements (vpn config only +log information). Changed: Disable detail accounting	2013-11-16	2014-01-31
1.0.3	fixed following issues: backup, green interface accounting, openvpn mtu, log file size and remote support connectivity	2013-09-08	2014-01-31
1.0.2	Add a reference to IPCOP, Add SN to web footer, allow modifications of openvpn setting while openvpn server is running	2012-11-07	2014-01-31
1.0.1	fix remote support	2012-08-07	2014-01-31

Note: If the ***Check for updates after reboot*** (1) check box is checked, the eFive automatically looks for updates each time it is rebooted.



Settings:

☑ Check for updates after reboot

□ Preload available Updates

Don't forget to click ***Save*** (2) if you change one of these parameters.

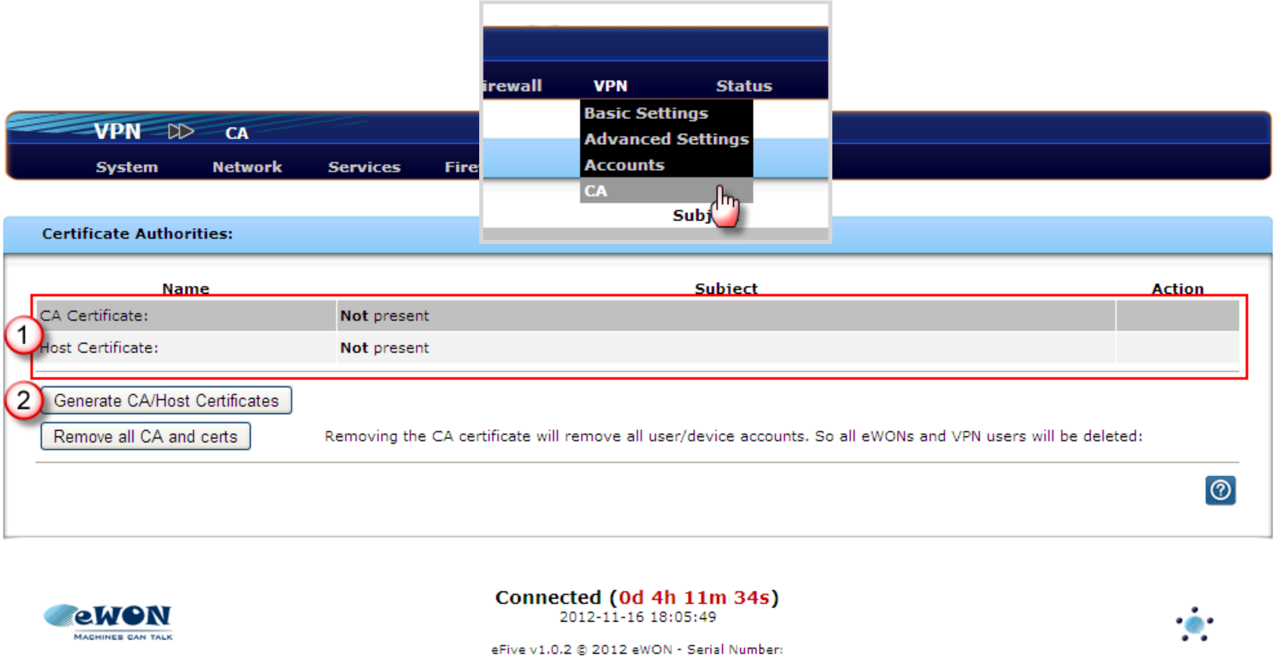
Step 4 - VPN Configuration

To be able to use your VPN server, you will need to go through the VPN configuration consisting in creating the ***Certificate Authorities*** (CA), define the VPN address and port, and create the VPN ***Accounts***.

Creating the Certificate Authorities (CA)

This is a key configuration item that needs to be done only once before starting to use the VPN server.

- To create the Certificate Authorities (CA), from the main menu select ***VPN, CA***



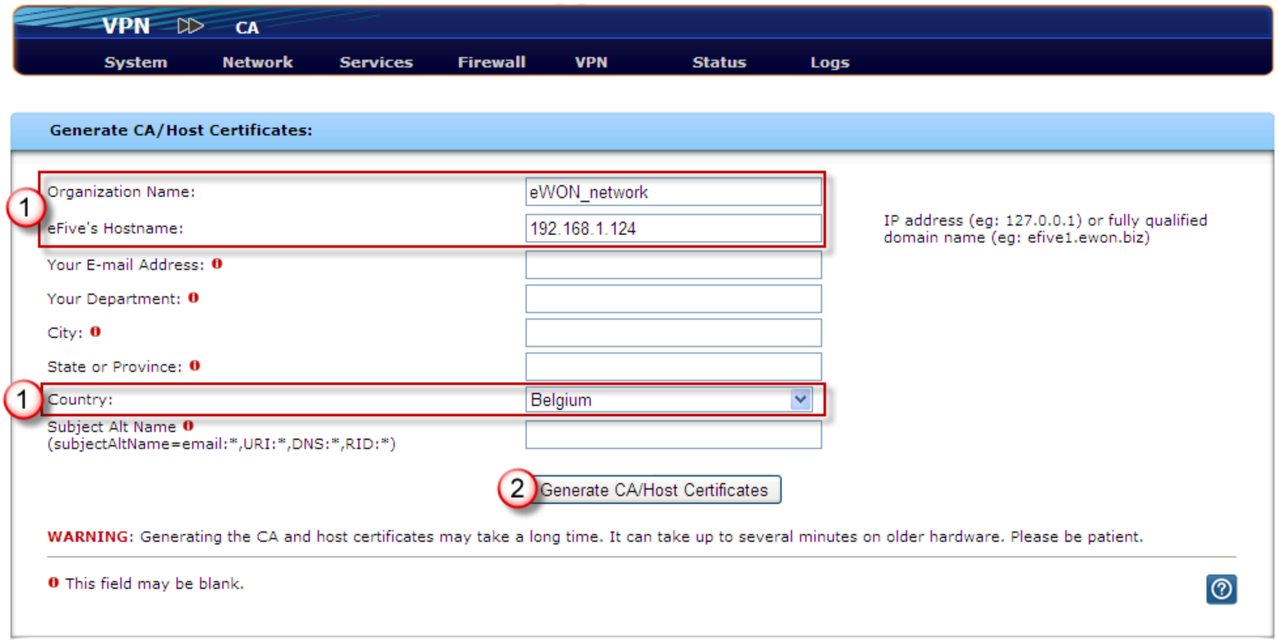
Certificate Authorities:

Name	Subject	Action
CA Certificate:	**Not** present	
Host Certificate:	**Not** present	

Removing the CA certificate will remove all user/device accounts. So all eWONs and VPN users will be deleted:

Connected (0d 4h 11m 34s)
2012-11-16 18:05:49
eFive v1.0.2 © 2012 eWON - Serial Number:

- By default the two rows (1) ***Root Certificate*** and ***Host Certificate*** mention "**Not** present".
- On the left side of the screen, click on the button (2) ***Generate CA/Host Certificates***



Generate CA/Host Certificates:

Organization Name:	eWON_network	
eFive's Hostname:	192.168.1.124	IP address (eg: 127.0.0.1) or fully qualified domain name (eg: efive1.ewon.biz)
Your E-mail Address: ❶		
Your Department: ❶		
City: ❶		
State or Province: ❶		
Country:	Belgium	
Subject Alt Name ❶ (subjectAltName=email:*,URI:*,DNS:*,RID:*)		

Generate CA/Host Certificates

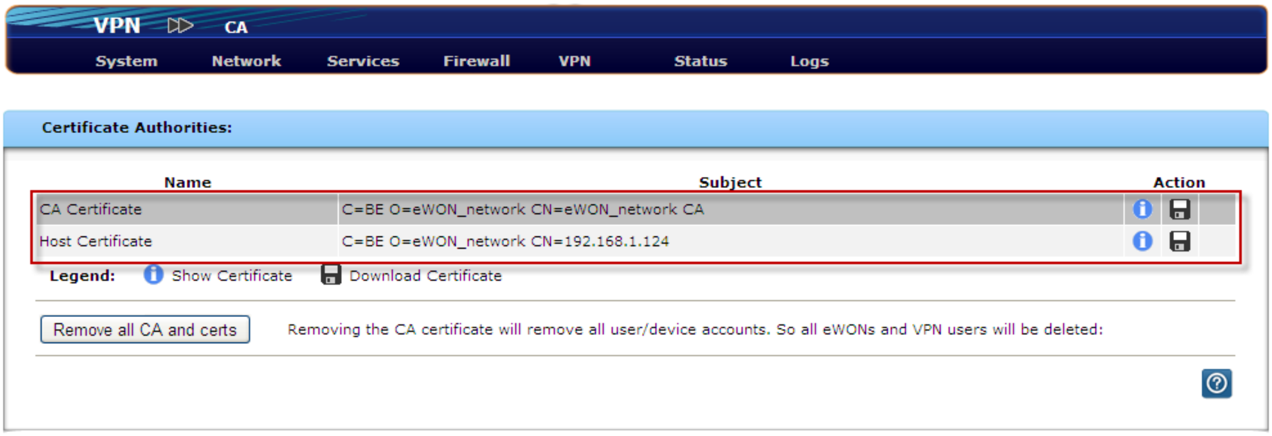
WARNING: Generating the CA and host certificates may take a long time. It can take up to several minutes on older hardware. Please be patient.

❶ This field may be blank.

- In the configuration interface, fill out at least the required fields (1) to create your Certificate Authorities (other fields are optional).

The field ***Organization Name*** accepts alphanumeric characters. There are no particular constraints as to the name you put in there. The field ***eFive Hostname*** on the contrary only accepts either an IP-address OR an URL type format. We suggest you to enter the public IP address of the Internet access which eFive will use (if this address is already known)

- When ready, click on the button ***CA/Host Certificates*** (2) to generate the certificates. When finished, the two certificates appear in the list of Certificate Authorities. **Note**: *This process can take up to several minutes.*



Certificate Authorities:

Name	Subject	Action
CA Certificate	C=BE O=eWON_network CN=eWON_network CA	ℹ 💾
Host Certificate	C=BE O=eWON_network CN=192.168.1.124	ℹ 💾

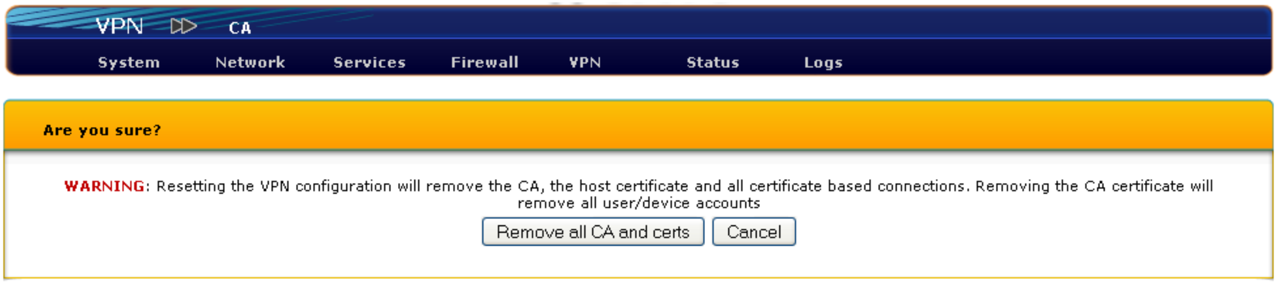
Legend: ℹ Show Certificate 💾 Download Certificate

Remove all CA and certs   Removing the CA certificate will remove all user/device accounts. So all eWONs and VPN users will be deleted:

- After completion of the process, the two certificates appear under ***Subject***.
- Click on the diskette icon in the ***Action*** column to save the ***CA Certificate*** file on your PC (on your desktop for example). You will need this file to configure your eWON later on.

Info! The VPN ***Accounts*** which we will create later in this step will be linked to this CA Certficate. Removing CA Authorities will result in removing ALL VPN ***Accounts*** (users and devices).

If you click on ***Remove all CA and certs*** by accident or not, you will be warned that this will delete all user/device accounts. This warning window leaves you the chance to cancel this action (see below).



Are you sure?

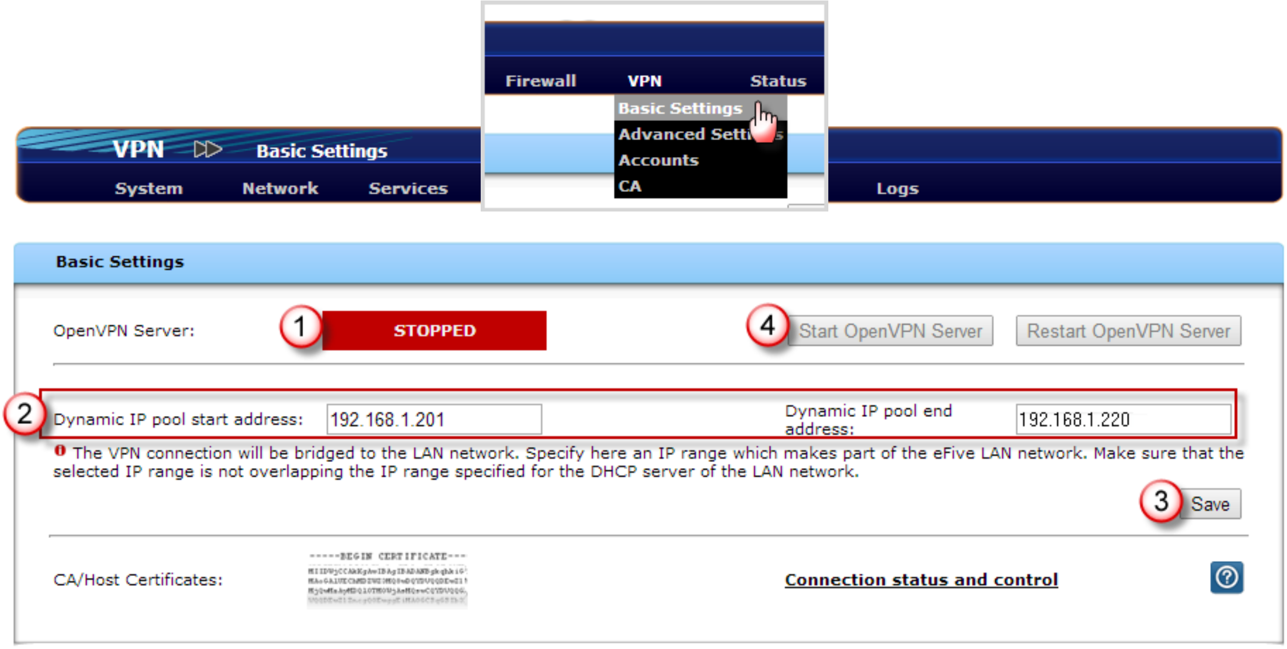
WARNING: Resetting the VPN configuration will remove the CA, the host certificate and all certificate based connections. Removing the CA certificate will remove all user/device accounts

Basic Settings

To go to the VPN Server parameters click on ***VPN, Basic Settings*** from the main menu.

Define the range of IP addresses for VPN connection

- At first configuration the VPN server status should be ***Stopped*** (1)
- Set first/last ***Dynamic IP pool address*** (2)
- **Note**: *Specify here an IP range which makes part of the eFive LAN network.*
  *Make sure that the selected IP range is not overlapping the IP range specified for the **DHCP server** (under menu **Services** > **DHCP Server**, see Step 2).*
  The VPN server <u>will not start</u> if the specified IP range is outside the LAN IP network.
- Click on ***Save*** (3)
  If required, before starting the VPN server, open the ***VPN > Advanced Settings*** page to configure the VPN Port and Protocol (see next §).
- Start the VPN Server by clicking on ***Start openVPN Server*** (4)



OpenVPN Server: STOPPED

Dynamic IP pool start address: 192.168.1.201 Dynamic IP pool end address: 192.168.1.220

The VPN connection will be bridged to the LAN network. Specify here an IP range which makes part of the eFive LAN network. Make sure that the selected IP range is not overlapping the IP range specified for the DHCP server of the LAN network.

CA/Host Certificates: -----BEGIN CERTIFICATE-----

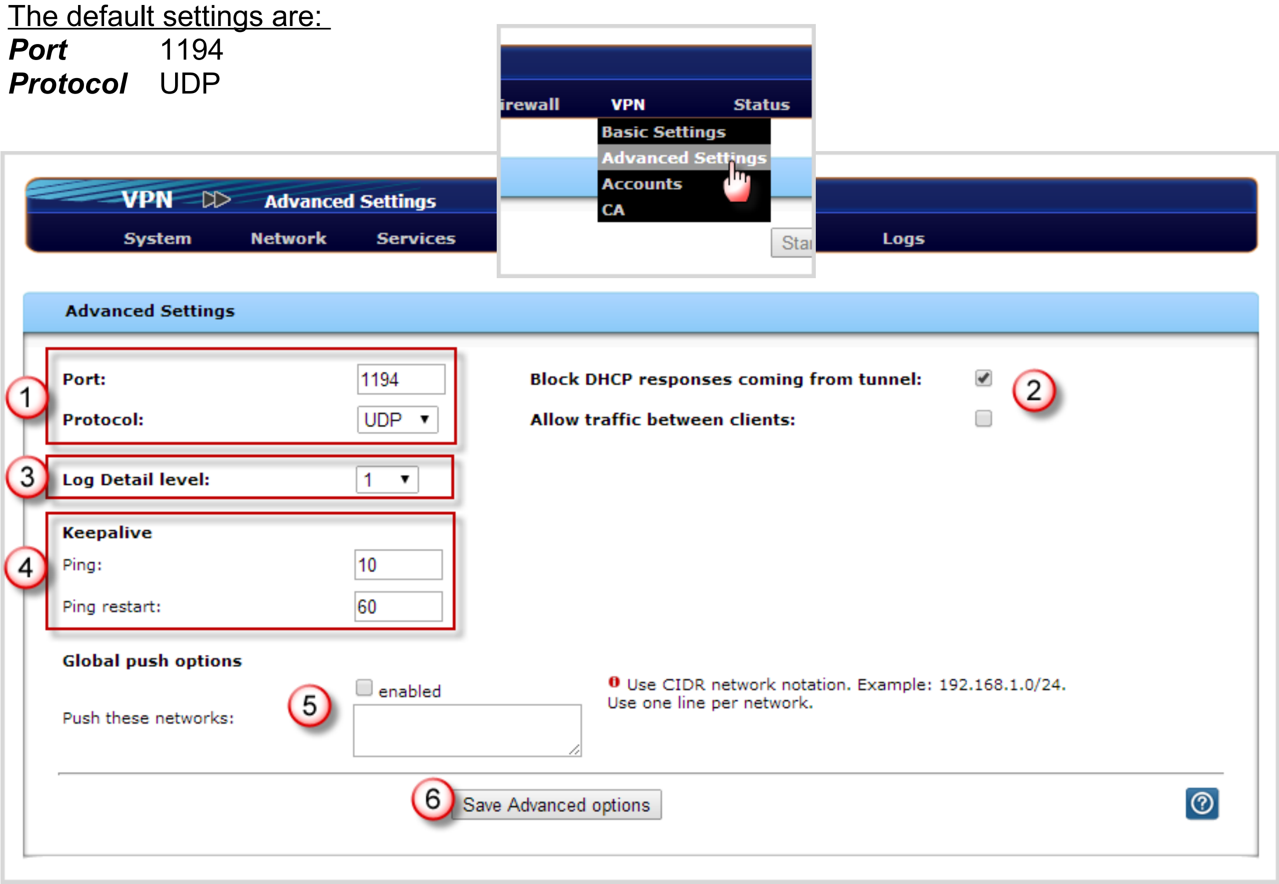
Advanced Settings

Optional VPN Protocol and Port Configuration

The ***VPN*** menu features the option ***Advanced Settings*** that is active only if the VPN-Server is stopped. The upper left zone (1) allows to specify the TCP type and port used for the VPN connection.

<u>The default settings are:</u>

Port	1194
Protocol	UDP



Advanced Settings

Port: 1194

Protocol: UDP

Log Detail level: 1

Keepalive

Ping: 10

Ping restart: 60

Global push options

Push these networks: □ enabled

Use CIDR network notation. Example: 192.168.1.0/24.
Use one line per network.

Block DHCP responses coming from tunnel: ☑

Allow traffic between clients: □

Save Advanced options

On the right you have two check boxes (2) allowing to define the global behavior for the VPN traffic.

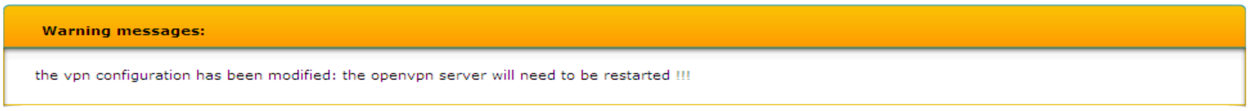
<u>Their default settings are:</u>
Block DHCP responses coming from tunnel - Checked
Allow traffic between clients - Unchecked

<u>Further parameters on this page include:</u>
Log detail level (3) - for diagnostic purposes - the default value is 1
Keepalive (4) – timeout values – the default values of 10 and 60 will fit most GPRS carriers
Global push options (5) is used only if special routing is required on all connected VPN clients. In this case you can define the networks that should be routed to the eFive VPN server.

Click ***Save Advanced options*** (6) to apply the modifications

Note: after having saved, the interface shows a warning message informing you that you need to restart the VPN server to keep the changes into account. To restart go to the ***VPN > Basic Settings*** page and click ***Restart OpenVPN Server****.* But keep in mind that you can restart the VPN server at a later time. So you can continue to do your configuration tasks including creating the user/device accounts and restart the VPN server only once your job is finished.

The restart process implies that all connected VPN clients (= user/device accounts) will be temporarily disconnected. Make sure you inform the people who may be affected.



Warning messages:

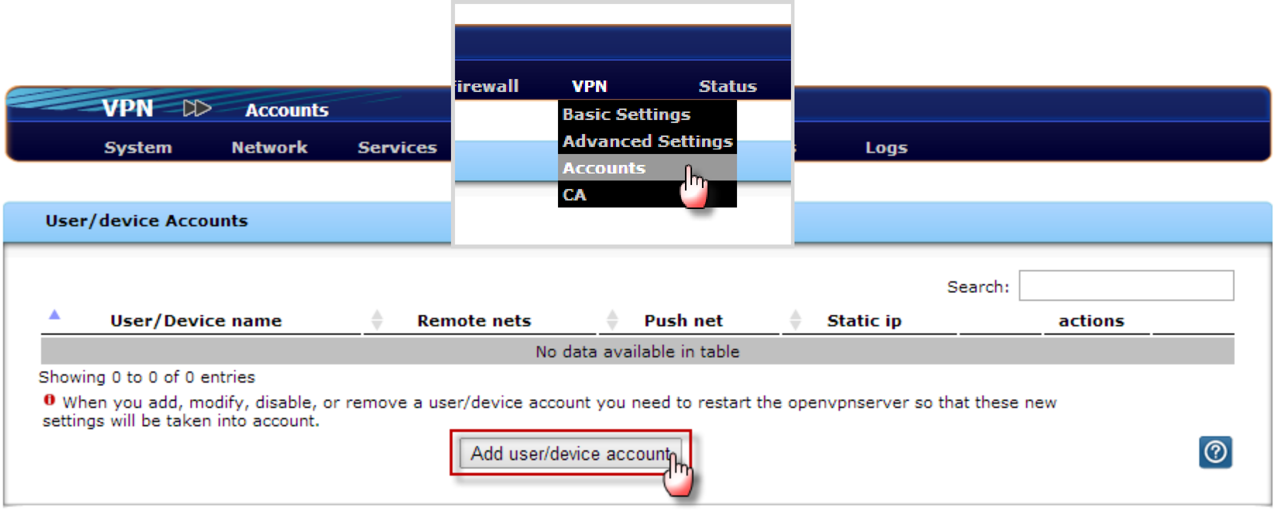
the vpn configuration has been modified: the openvpn server will need to be restarted !!!

Creating User/Device Accounts (VPN Clients)

For each user or eWON to connect, you need to create a VPN ***Account***.

To do this, from the main menu select ***VPN > Accounts***

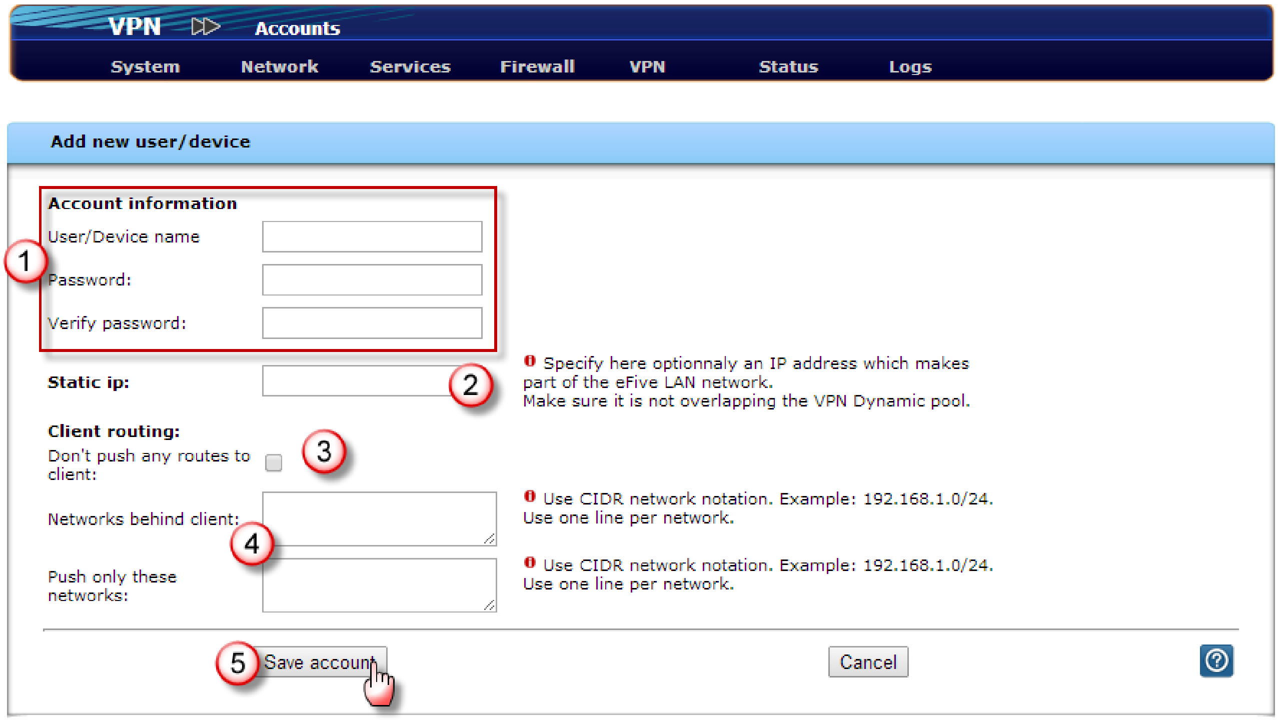
- In the ***Accounts*** windows click on the ***Add user/device account*** button



User/Device name	Remote nets	Push net	Static ip	actions
No data available in table				

Showing 0 to 0 of 0 entries

When you add, modify, disable, or remove a user/device account you need to restart the openvpnserver so that these new settings will be taken into account.



User/Device name

Password:

Verify password:

Static ip:

Specify here optionnaly an IP address which makes part of the eFive LAN network.
Make sure it is not overlapping the VPN Dynamic pool.

Client routing:

Don't push any routes to client: □

Networks behind client:

Use CIDR network notation. Example: 192.168.1.0/24.
Use one line per network.

Push only these networks:

Use CIDR network notation. Example: 192.168.1.0/24.
Use one line per network.

- Enter a ***Username*** and ***Password*** (1)

Further parameters on this page include:

- ***Static ip*** (2) - Only used if you want to work with a fixed IP address for the VPN client. If you leave this field blank, the IP address will be allocated using DHCP.
- ***Client routing*** (3) – Check this option if no routing should be sent (pushed) to the VPN client.
- ***Networks behind client*** (4) allows you to define the networks of the devices behind the eWON. The field should contain the eWON LAN network IP with subnet mask extension under CIDR notation.

  Examples of eWON LAN IP address in CIDR syntax:

  If the eWON LAN address is 192.168.140.53, mask 255.255.255.0
  then, the CIDR syntax of this network IP is 192.168.140.0/24

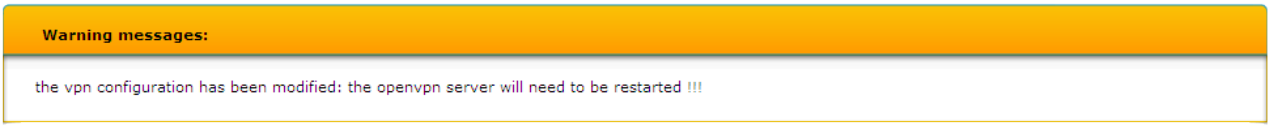
  If the eWON LAN address is 192.168.140.53, mask 255.255.0.0
  then, the CIDR syntax of this network IP is 192.168.0.0/18

  Referring to our network example shown at the beginning of this document, we should encode here 192.168.140.0/24.

- Click ***Save*** (5) to save the account.

Note: after having saved, the interface shows a warning message informing you that you need to restart the VPN server to keep the changes into account. To restart go to the ***VPN > Basic Settings*** page and click ***Restart OpenVPN Server***. But keep in mind that you can restart the VPN server at a later time.

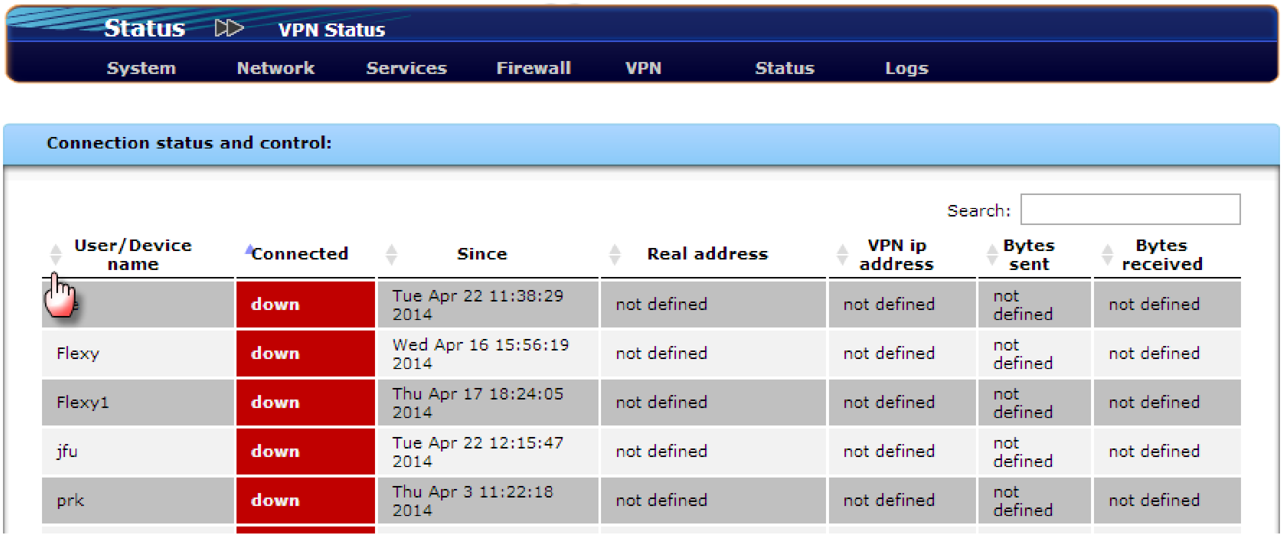
The restart process implies that all connected VPN clients (= user/device accounts) will be temporarily disconnected. Make sure you inform the people who may be affected.



Warning messages:

the vpn configuration has been modified: the openvpn server will need to be restarted !!!

The newly created accounts appear as ***Connected Down*** (red) in the list of the ***Home*** page.



Connection status and control:

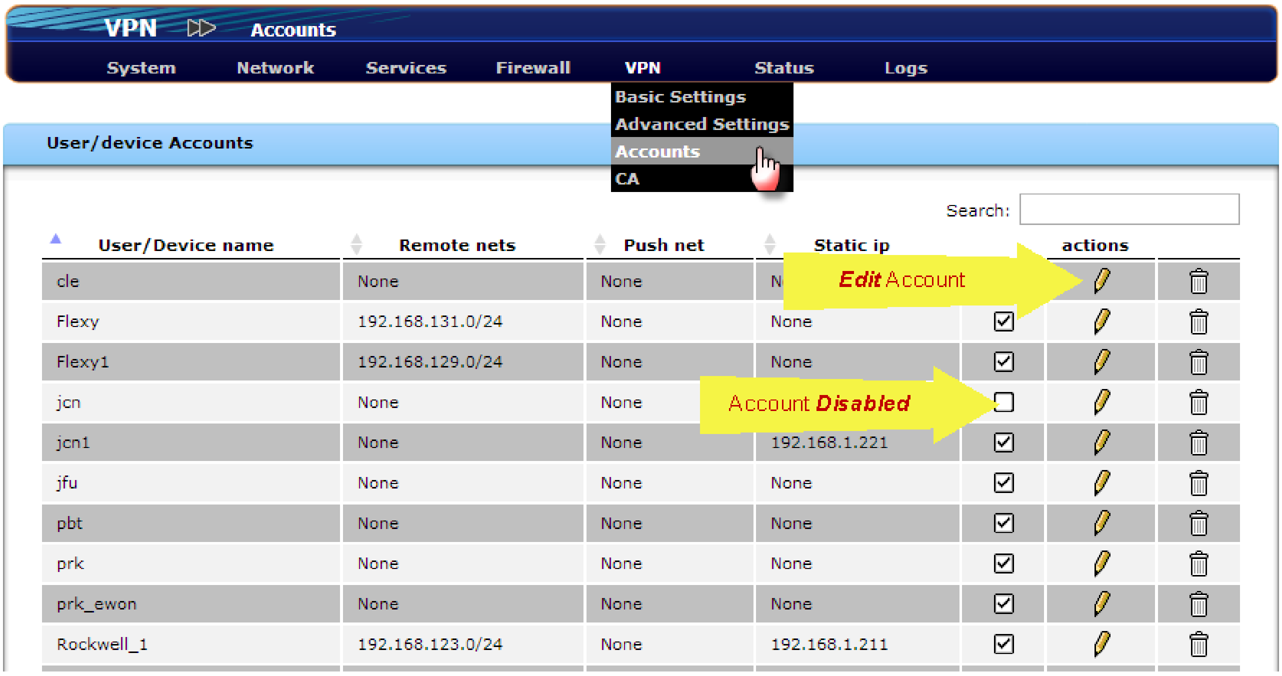
Search:

User/Device name	Connected	Since	Real address	VPN ip address	Bytes sent	Bytes received
	down	Tue Apr 22 11:38:29 2014	not defined	not defined	not defined	not defined
Flexy	down	Wed Apr 16 15:56:19 2014	not defined	not defined	not defined	not defined
Flexy1	down	Thu Apr 17 18:24:05 2014	not defined	not defined	not defined	not defined
jfu	down	Tue Apr 22 12:15:47 2014	not defined	not defined	not defined	not defined
prk	down	Thu Apr 3 11:22:18 2014	not defined	not defined	not defined	not defined

Entries in the list can be sorted by clicking the arrows in the column headers.

Edit or Temporarily Disable an Account

Go to the page ***VPN > Accounts*** if you want to ***Edit*** the ***Account*** parameters, or temporarily disable it.

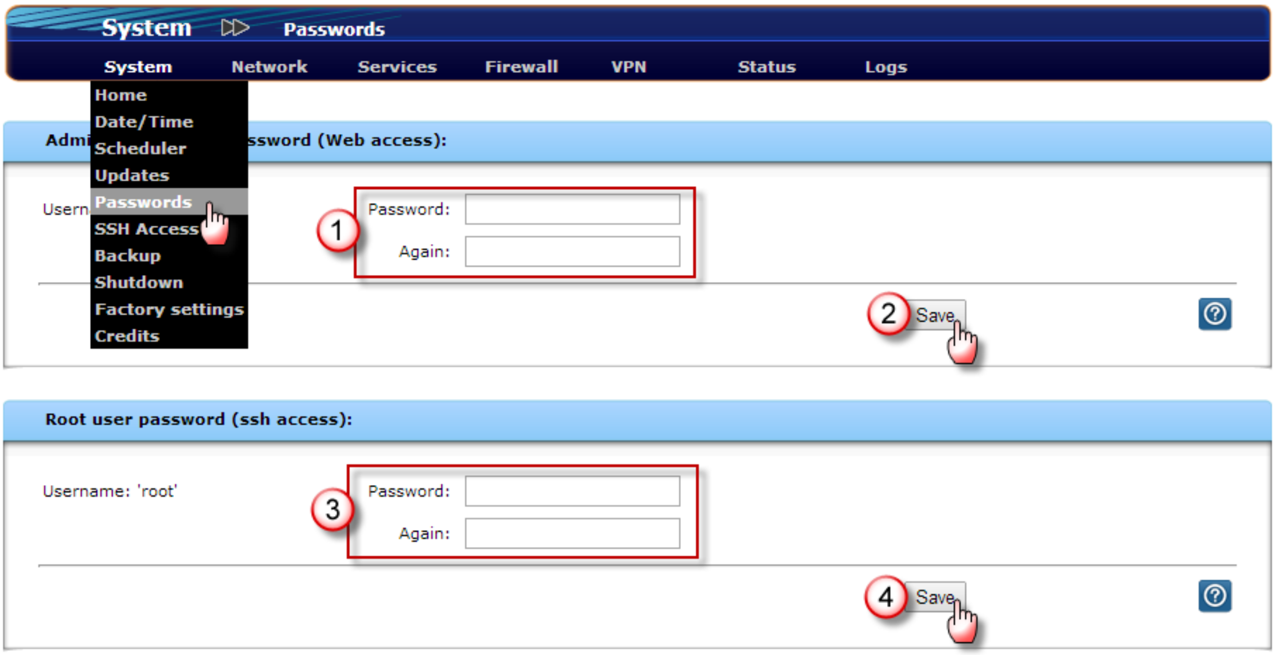


User/Device name	Remote nets	Push net	Static ip		actions	
cle	None	None	N		✎	🗑
Flexy	192.168.131.0/24	None	None	☑	✎	🗑
Flexy1	192.168.129.0/24	None	None	☑	✎	🗑
jcn	None	None		☐	✎	🗑
jcn1	None	None	192.168.1.221	☑	✎	🗑
jfu	None	None	None	☑	✎	🗑
pbt	None	None	None	☑	✎	🗑
prk	None	None	None	☑	✎	🗑
prk_ewon	None	None	None	☑	✎	🗑
Rockwell_1	192.168.123.0/24	None	192.168.1.211	☑	✎	🗑

Step 5 - Password Change

The VPN configuration of our eFive is now completed.
It is now necessary to change the admin user password of your eFive for security reasons.

To change the admin password, from the menu bar, click on ***System***, ***Passwords***.
Enter the new password twice (1) and click ***Save*** (2).



Perform the same for the ***Root*** user (3 & 4).

The root user will allow to connect to your eFive using SSH access (if activated). So for obvious security reason this password should also be changed.

Step 6 - Internet-Router Configuration

Public IP Address

You should use an Internet access with fixed IP address. This is recommended because a Dynamic DNS would involve a much longer reconnection time. This IP address will be used on all eWONs to reach the VPN server.

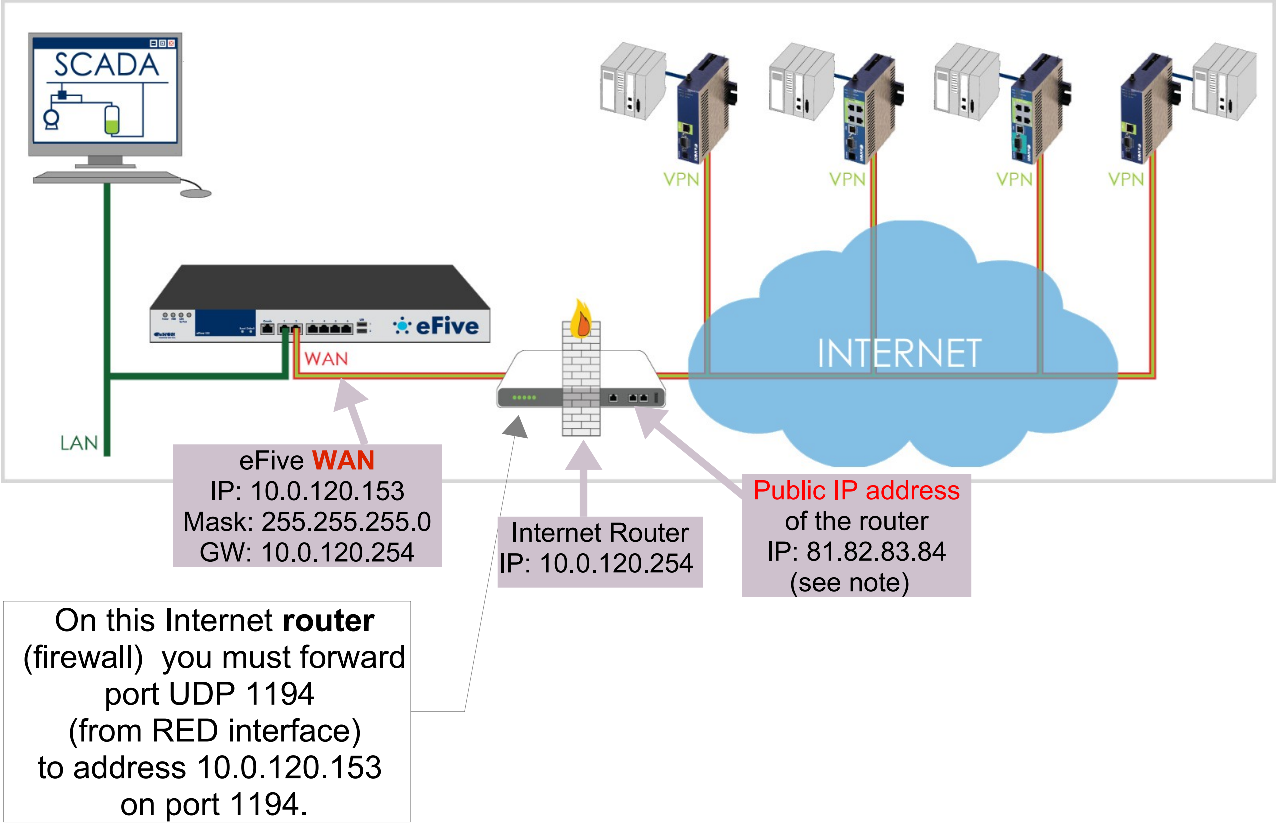
Protocol and Port Forwarding

Special configuration of your Internet router is required to allow the VPN connection between the eWONs and the eFive VPN server.

In fact, on the Internet router you'll need to forward the port used by the eFive for the VPN connection. (As configured in Step 4 - VPN Configuration)

By default the eFive will use protocol **UDP** and port **1194** for the VPN connection.

So on your Internet router you must forward an incoming UDP port (for example UDP 1194) to be redirected to the WAN IP address of the eFive on port 1194 (see example below).



eFive **WAN**
IP: 10.0.120.153
Mask: 255.255.255.0
GW: 10.0.120.254

Internet Router
IP: 10.0.120.254

Public IP address
of the router
IP: 81.82.83.84
(see note)

On this Internet **router**
(firewall) you must forward
port UDP 1194
(from RED interface)
to address 10.0.120.153
on port 1194.

Step 7 - eWON Configuration

What do you Need?

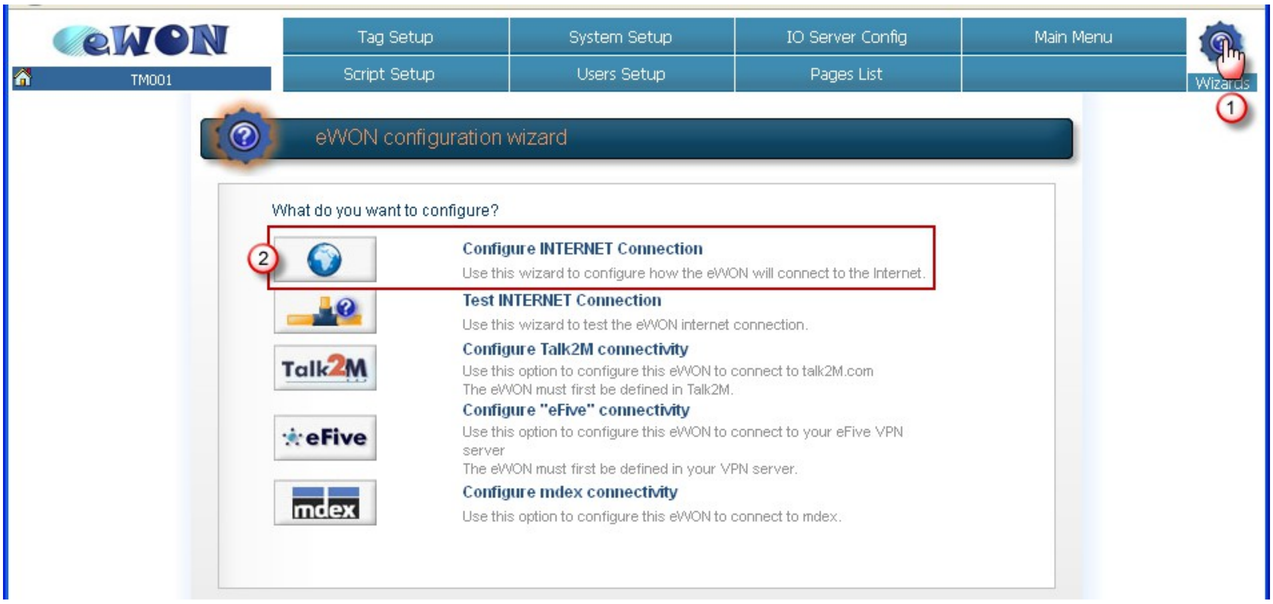
- ➔ The public IP address that will be used to reach the eFive
- ➔ The port and protocol used for the VPN connection with the eFive
- ➔ The VPN account username and password allocated to the eWON
- ➔ The Root CA Certificate of your eFive (e.g. saved on your desktop)
- ➔ An eWON hardware with VPN capabilities and Internet access (*) - this eWON should feature a firmware 6.4s6 or higher (upgrade first if necessary)

- ➔ (*) Only an ***outgoing*** Internet connection is necessary. No incoming port to open, the used VPN port has to be open only for outgoing connections.

Warning: If the eWON was already used for other VPN connections before (like Talk2M) then it should be first reset to its default config and rebooted. Some VPN settings are not compatible and will result in VPN connection issues.

Internet Configuration

Connect to the LAN port of the eWON and access its web interface
Open the eWON configuration wizard.



eWON configuration wizard

What do you want to configure?

Configure INTERNET Connection
Use this wizard to configure how the eWON will connect to the Internet.

Test INTERNET Connection
Use this wizard to test the eWON internet connection.

Configure Talk2M connectivity
Use this option to configure this eWON to connect to talk2M.com
The eWON must first be defined in Talk2M.

Configure "eFive" connectivity
Use this option to configure this eWON to connect to your eFive VPN server
The eWON must first be defined in your VPN server.

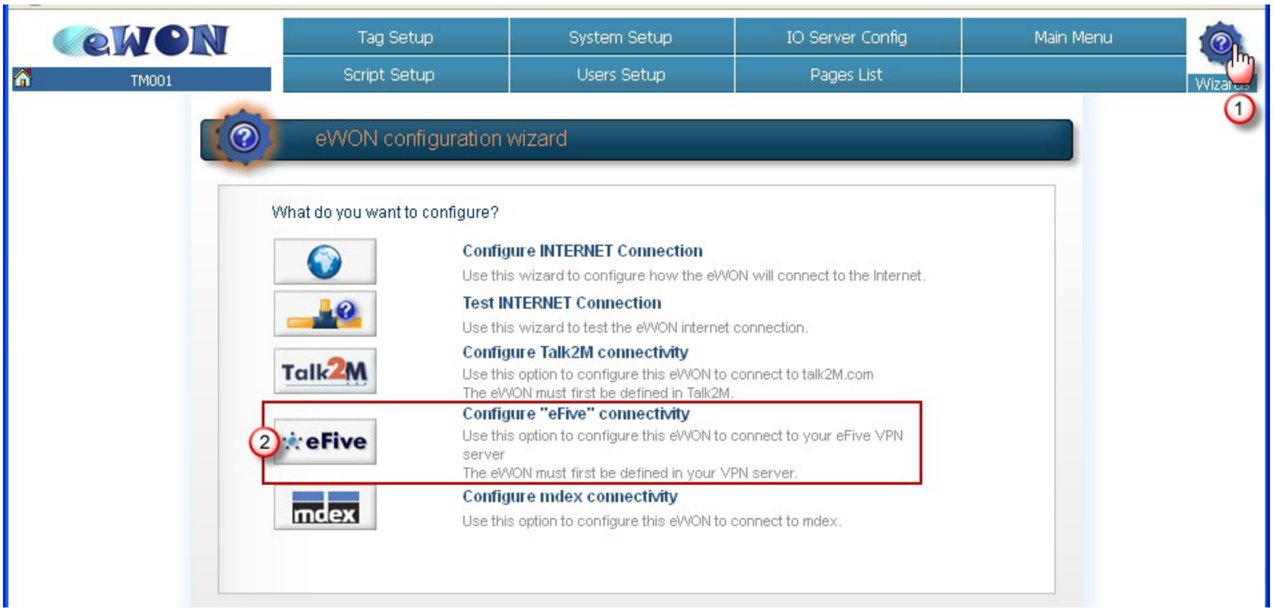
Configure mdex connectivity
Use this option to configure this eWON to connect to mdex.

- Select the ***Configure Internet Connection*** row.
  This will allow you to select between Internet WAN or GPRS as carrier type
- Go through the Internet wizard
- Check whether the connection test is successful

eFive Connectivity

Important remark: The creation of the VPN connection requires that both the eWON and the eFive have an accurate (actual) date/time. If there is a (too large) discrepancy between both, the CA Certificate will not be accepted.

Open the eWON configuration wizard page.
Click on the ***eFive connectivity*** button



What do you want to configure?

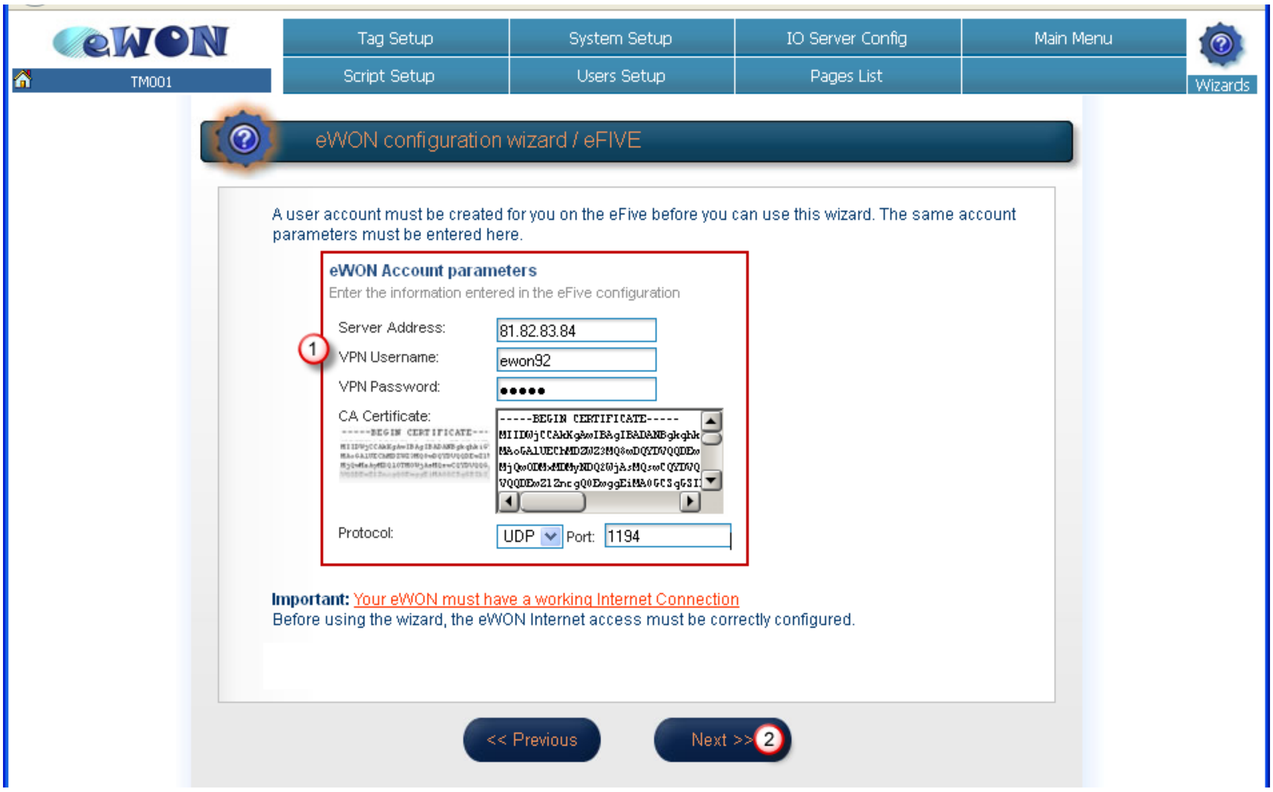
Configure INTERNET Connection
Use this wizard to configure how the eWON will connect to the Internet.

Test INTERNET Connection
Use this wizard to test the eWON internet connection.

Configure Talk2M connectivity
Use this option to configure this eWON to connect to talk2M.com
The eWON must first be defined in Talk2M.

Configure "eFive" connectivity
Use this option to configure this eWON to connect to your eFive VPN server
The eWON must first be defined in your VPN server.

Configure mdex connectivity
Use this option to configure this eWON to connect to mdex.



A user account must be created for you on the eFive before you can use this wizard. The same account parameters must be entered here.

eWON Account parameters
Enter the information entered in the eFive configuration

Server Address: 81.82.83.84
VPN Username: ewon92
VPN Password: •••••
CA Certificate:

```
-----BEGIN CERTIFICATE-----
MIIDOjCCAkKgAwIBAgIBADANBgkqhk
MAoGA1UECHMDZWZ2MQ8wDQYDVQQDEw
MjQwODMxMDMyNDQ2WjAxMQswCQYDVQ
VQQDEwZ12ncgQ0EwggEiMA0GCSqGSI
```

Protocol: UDP Port: 1194

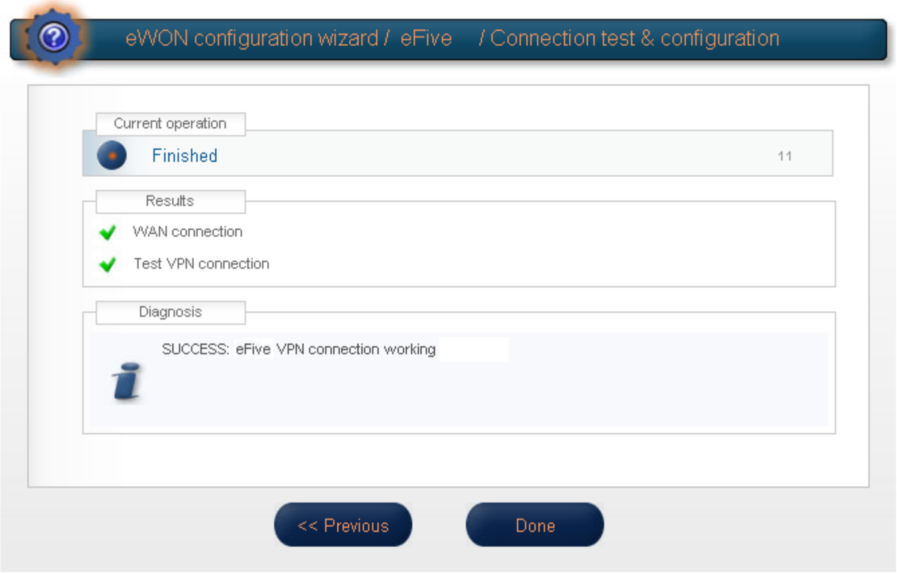
Important: Your eWON must have a working Internet Connection
Before using the wizard, the eWON Internet access must be correctly configured.

Set the parameters for the eFive connection.(1)

- The ***Server Address*** is the public IP address of the Internet router behind which the eFive is placed. This address can be a domain name like www.mycompany.com.
- The ***VPN Username*** & ***VPN Password*** are those of the ***Account*** created in the eFive for this eWON.
- Inside the ***CA Certificate*** field copy the CA Certificate of your eFive. To perform this, open the eFive CA Certificate with a text editor like Notepad and copy here the part starting with -----BEGIN CERTIFICATE----- and ending with -----END CERTIFICATE-----.
- In ***Protocol***, you configure UDP or TCP and specify the ***Port***. The selected port must be the same than the one configured in the eFive. The default values are UDP on port 1194.

Click ***Next***. (2)

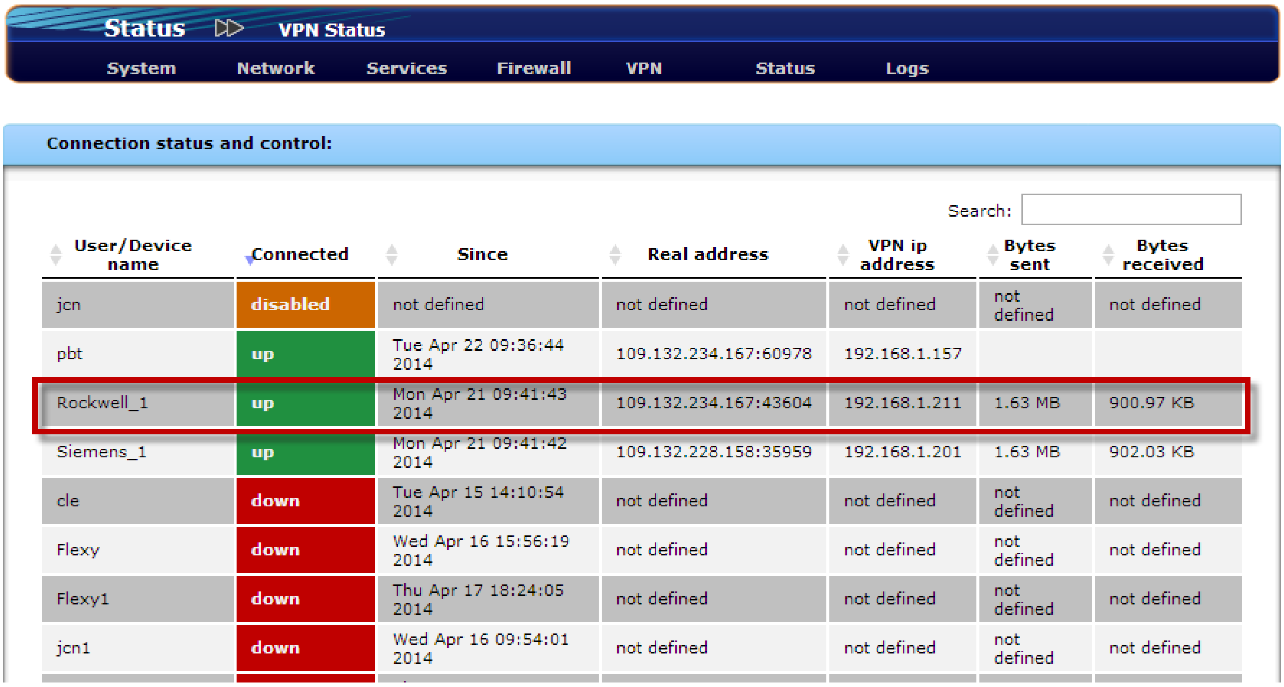
The configuration wizard goes through a VPN connection test that should end-up with a SUCCESS message.



SUCCESS: eFive VPN connection working

Click ***Done***.

The eWON is now configured and will appear as ***Connected Up*** (green) in the ***Home*** page of the eFive interface (see screen capture next page).



Connection status and control:

Search:

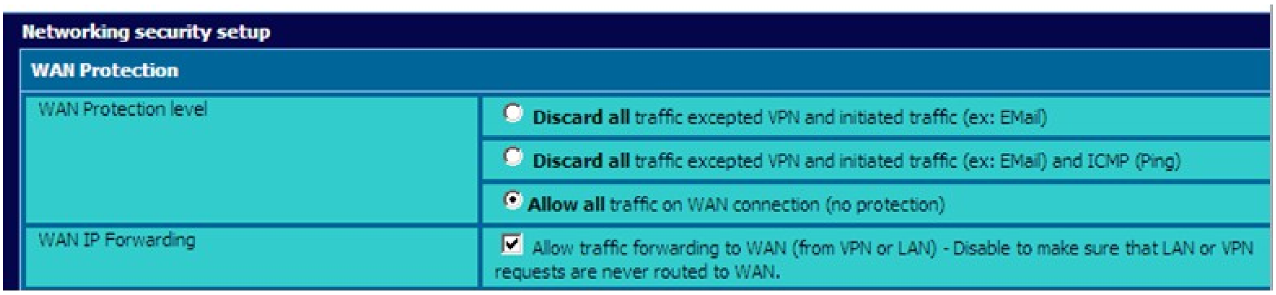
User/Device name	Connected	Since	Real address	VPN ip address	Bytes sent	Bytes received
jcn	disabled	not defined	not defined	not defined	not defined	not defined
pbt	up	Tue Apr 22 09:36:44 2014	109.132.234.167:60978	192.168.1.157		
Rockwell_1	up	Mon Apr 21 09:41:43 2014	109.132.234.167:43604	192.168.1.211	1.63 MB	900.97 KB
Siemens_1	up	Mon Apr 21 09:41:42 2014	109.132.228.158:35959	192.168.1.201	1.63 MB	902.03 KB
cle	down	Tue Apr 15 14:10:54 2014	not defined	not defined	not defined	not defined
Flexy	down	Wed Apr 16 15:56:19 2014	not defined	not defined	not defined	not defined
Flexy1	down	Thu Apr 17 18:24:05 2014	not defined	not defined	not defined	not defined
jcn1	down	Wed Apr 16 09:54:01 2014	not defined	not defined	not defined	not defined

As shown here, entries in the ***Home*** page can have three different connection status:

- ***Disabled*** – the account disabled in the Accounts page (***VPN > Accounts***)
- ***Down*** – the account is not connected
- ***Up*** = the account is connected.

WAN Security Settings

The default WAN protection level of the eWON is ***Allow All*** and ***Allow traffic forwarding to WAN*** as shown in ***System Setup, Communication, Networking Config, Security***



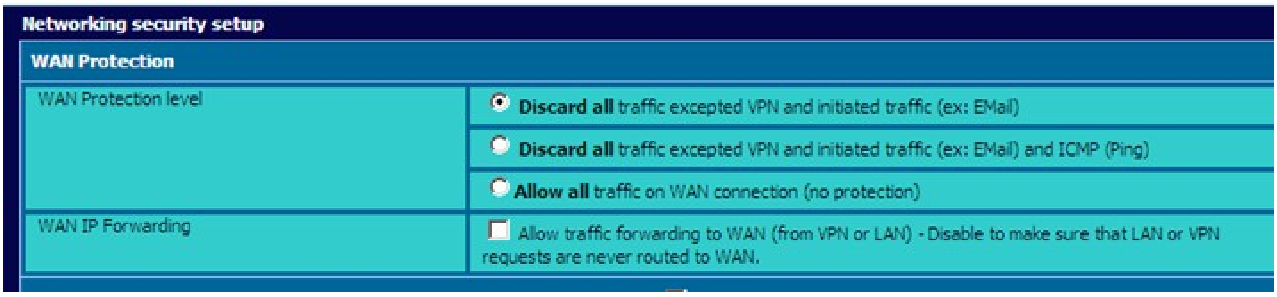
Networking security setup

WAN Protection

WAN Protection level	○ **Discard all** traffic excepted VPN and initiated traffic (ex: EMail)
	○ **Discard all** traffic excepted VPN and initiated traffic (ex: EMail) and ICMP (Ping)
	● **Allow all** traffic on WAN connection (no protection)
WAN IP Forwarding	☑ Allow traffic forwarding to WAN (from VPN or LAN) - Disable to make sure that LAN or VPN requests are never routed to WAN.

Though these settings are OK from a functional standpoint, they may induce a security weakness, mostly (but not only) when the eWON is accessed through a wireless modem. This weakness is even more critical if the default admin password of the eWON was not changed.

To avoid unwanted WAN access, it is recommended to change the default settings as follows:



Networking security setup

WAN Protection

WAN Protection level	● **Discard all** traffic excepted VPN and initiated traffic (ex: EMail)
	○ **Discard all** traffic excepted VPN and initiated traffic (ex: EMail) and ICMP (Ping)
	○ **Allow all** traffic on WAN connection (no protection)
WAN IP Forwarding	□ Allow traffic forwarding to WAN (from VPN or LAN) - Disable to make sure that LAN or VPN requests are never routed to WAN.

Set values to ***Discard All*** and uncheck ***Allow traffic forwarding to WAN*** (from VPN or LAN).

Appendix

1 - Firewall Configuration

By default, the eFive firewall settings are set to only allow VPN access from Red interface. It is possible to open other ports in the firewall settings. For obvious reasons, this should be done only by authorized qualified personnel.

- You can access to the Firewall parameters through the main menu option ***Firewall***.
- For further information on how to use the firewall settings use the online help button displayed on the eFive configuration page.

2 - Troubleshooting Routing Problems

In order to allow the eWON to establish the VPN connection to the eFive, following conditions must be fulfilled:

- The eWON WAN address range must be different from the eWON LAN address range.
- The VPN network will be bridged to the eFive LAN network. So to make the connection work, the eWON LAN address and the eWON WAN address must be in a different range than the eFive LAN address.

3 - Backup & Restore

If you want to take a backup of your eFive configuration proceed as follows:

- From the main menu select ***System, Backup***
- Select the media on which you want to store your backup
  - ➔ You can plug-in an USB storage media on the eFive frame
  - ➔ This device appears under the Select Media area
  - ➔ Click ***Mount*** to enable the media
- Enter a name in the ***Description*** field
- Click on ***Create a new backup set***
- The newly created backup appears in the list below ***backup sets***

Note: you can upload/restore/delete your backup from the ***Action*** column.

4 - Shutdown or Restart the eFive Hardware

In some circumstances a reboot or a shutdown of the hardware may be required.

Would you need a hardware shutdown and/or restart, please proceed as follows:

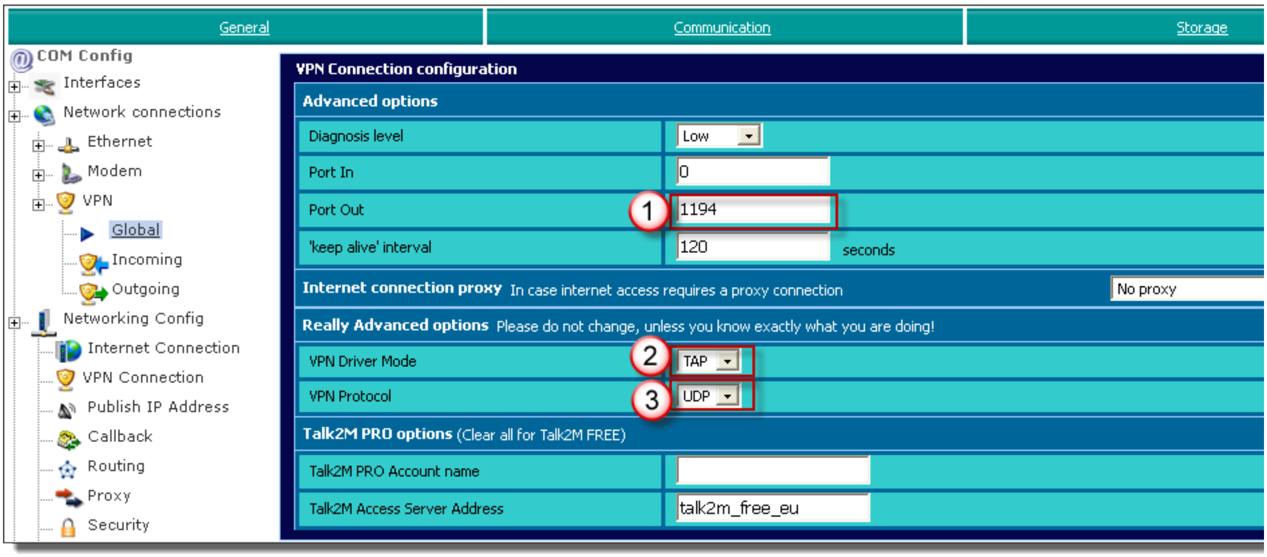
- From the main menu select ***System, Shutdown***
- Either click on the ***Reboot*** or on the ***Shutdown*** button, depending on the action you want to see executed.

Warning: Before unplugging the power supply of your eFive device, always make sure that you first performed a ***System shutdown*** as explained here above.

5 - Configuring an eFive Connection without Using the Wizard

To configure the eWON for an eFive connection without using the wizard proceed as follows:

- Launch the Internet connection wizard to configure the eWON to connect to the Internet.
- Open menu ***System Setup*** / ***Communication*** / ***VPN Global***



VPN Connection configuration

Advanced options

Diagnosis level	Low
Port In	0
Port Out	1194
'keep alive' interval	120 seconds

Internet connection proxy In case internet access requires a proxy connection: No proxy

Really Advanced options Please do not change, unless you know exactly what you are doing!

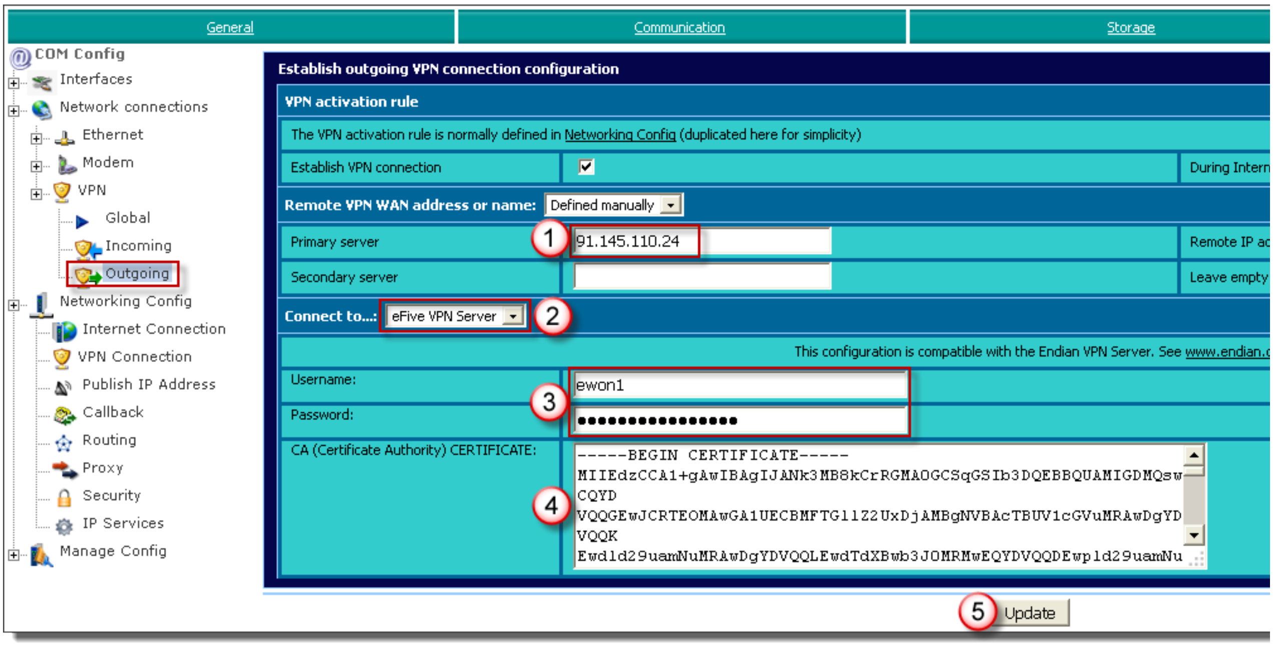
VPN Driver Mode	TAP
VPN Protocol	UDP

Talk2M PRO options (Clear all for Talk2M FREE)

Talk2M PRO Account name	
Talk2M Access Server Address	talk2m_free_eu

- Change the ***Port Out*** value if you use another port than the default UDP 1194
- Select ***VPN Drive Mode***: TAP
- Change the ***VPN Protocol*** if other than the default UDP

- Open menu ***System Setup*** / ***Communication*** / ***VPN Outgoing***



Establish outgoing VPN connection configuration

VPN activation rule

The VPN activation rule is normally defined in Networking Config (duplicated here for simplicity)

Establish VPN connection	☑	During Intern

Remote VPN WAN address or name: Defined manually

Primary server	91.145.110.24	Remote IP ac
Secondary server		Leave empty

Connect to...: eFive VPN Server

This configuration is compatible with the Endian VPN Server. See www.endian.c

Username:	ewon1
Password:	●●●●●●●●●●●●●●●●●

CA (Certificate Authority) CERTIFICATE:

```
-----BEGIN CERTIFICATE-----
MIIEdzCCA1+gAwIBAgIJANk3MB8kCrRGMA0GCSqGSIb3DQEBBQUAMIGDMQsw
CQYD
VQQGEwJCRTEOMAwGA1UECBMFTGllZ2UxDjAMBgNVBAcTBUV1cGVuMRAwDgYD
VQQK
Ewdld29uamNuMRAwDgYDVQQLEwdTdXBwb3J0MRMwEQYDVQQDEwpld29uamNu
```

- In the ***Primary server*** field,
  enter the public IP address on which the eFive can be reached
- For the ***Connect to***...:parameter select: ***eFive VPN server***
- Enter the ***Username*** and ***Password*** of the VPN account
- Inside the ***CA field*** copy the CA certificate of the eFive
  starting with -----BEGIN CERTIFICATE-----ending with -----END CERTIFICATE-----

- Click on ***Update***
  eWOn will automatically try to establish the VPN connection.
- You can check the VPN connection result using ***Diagnostic*** / ***Real Time Log***.
- Or check for received VPN IP address under ***Diagnostic*** / ***Status*** / ***Status***

Revision history

Revision Level	Date	Description
1.0	25/10/12	Initial version
1.1	11/11/12	Detailed IP addresses added on architecture pictures. Modifications on chapter Step 6 – Internet-Router Configuration
1.2	16/11/12	Update to new UI screens
1.3	08/03/13	Add/correct features + config without wizard
1.4	15/03/13	Correct wrong IP page 17 - Add manual WAN eWON security setting
1.5	22/04/14	Update to eFive firmware 1.1 - Consistency of screen captures and alignments - Step 4 sequence rearranged - Add account status - Add section ***Edit Accounts***.
1.6	09/05/14	eFive 25 supports up to 50 VPN Clients eFive 100 supports up to 200 VPN Clients

Document build number: *230*

<u>Note concerning the warranty and the rights of ownership:</u>

The information contained in this document is subject to modification without notice. The vendor and the authors of this manual are not liable for the errors it may contain, nor for their eventual consequences.

No liability or warranty, explicit or implicit, is made concerning quality, the accuracy and the correctness of the information contained in this document. In no case the manufacturer's responsibility could be called for direct, indirect, accidental or other damage occurring from any defect of the product or errors coming from this document.

The product names are mentioned in this manual for information purposes only. The trade marks and the product names or marks contained in this document are the property of their respective owners.

eWON sa, Member of ACT'L Group.