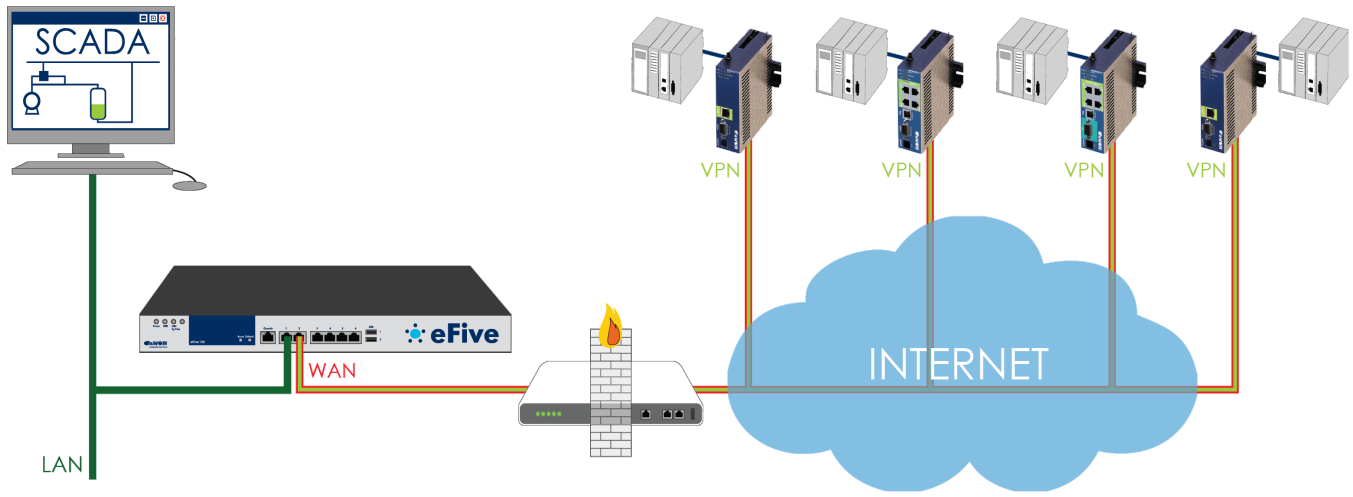
eWON Application User Guide

AUG 050 / Rev 1.4

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 ?

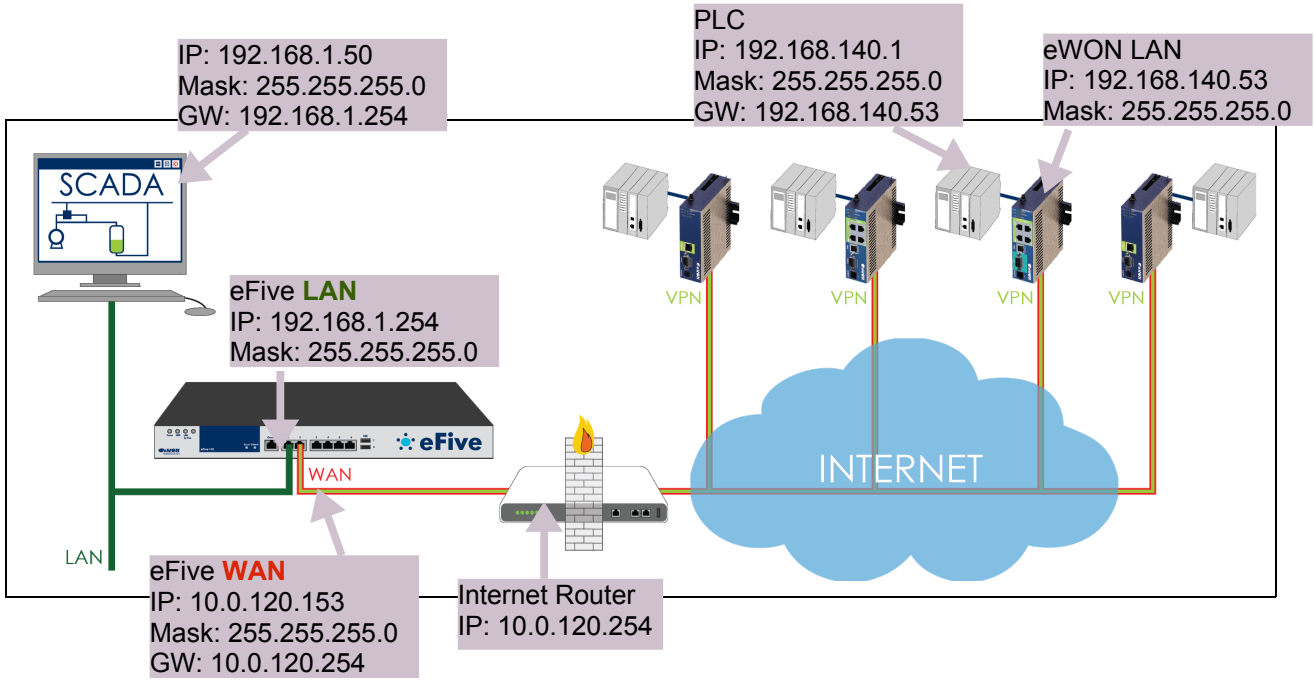
The eFive 25 and 100 are hardware platforms featuring a Virtual Private Network (VPN) gateway with OpenVPN. It has been designed to be a perfect match with the eWON range to build a VPN network. The eFive 25 and 100 act as OpenVPN Servers and the eWONs as OpenVPN Clients. The model eFive 25 is designed to support up to 25 eWONs; the eFive 100 supports up to 100 eWONs. 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 picture.

Step 1 to step 7 of this guide explains how to realize the VPN network.
In the appendixes, you find additional information regarding

- ➔ Backup & restore
- ➔ Restart & shut down
- ➔ 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.

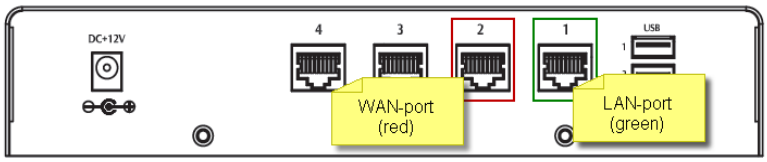


To reach the PLC behind the eWON, the SCADA PC will then just need to use the local IP address of the PLC (= 192.168.140.1).

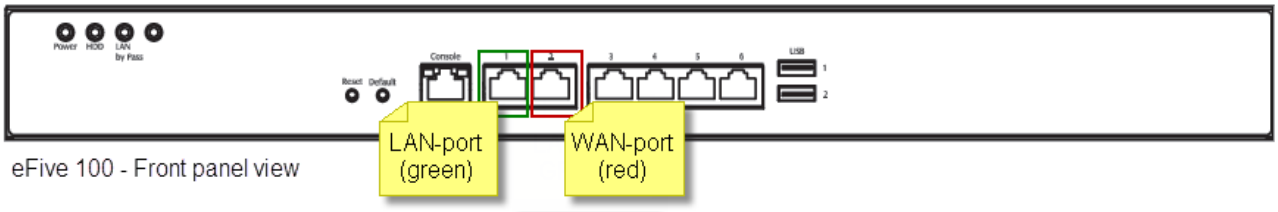
Step 1 – Connect to the eFive web page

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



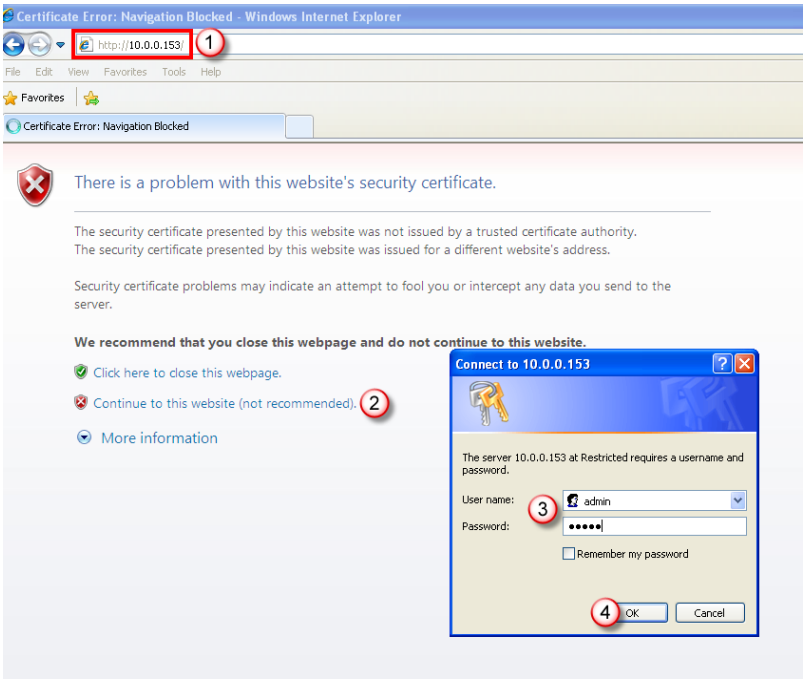
eFive 100 - Front panel view

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.

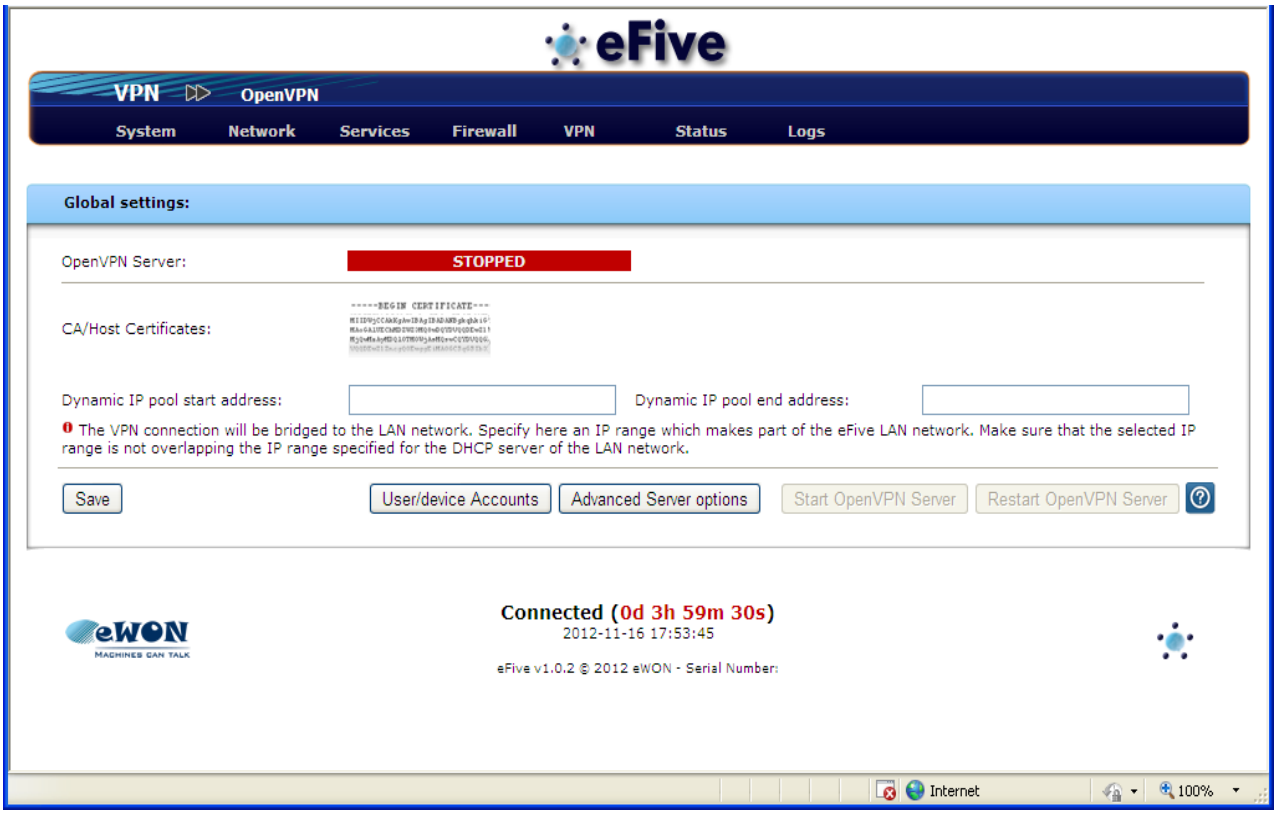


The default credentials are:

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

Click ***OK*** *(4)*

The home page of the eFive opens.



The home page contains info about the VPN server status and will display the connected VPN devices.
At first connection, no connected clients are listed in the lower part. Once the VPN clientswill be created, they will appear in this page with their respective status.

Warning!

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

Step 2 - Network interface configuration

What you should know about 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.

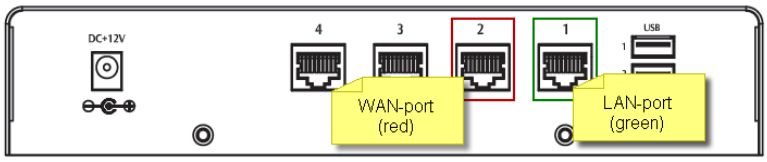
Color coding is logical in that it represents a continuum of network access from restricted to permissive.

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 attribute 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)

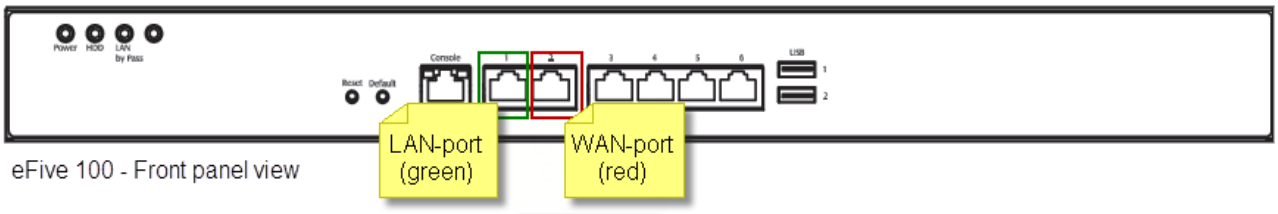
In this guide we will focus on the Green and Red networks.
This is the most common use of the eFive VPN server.

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)



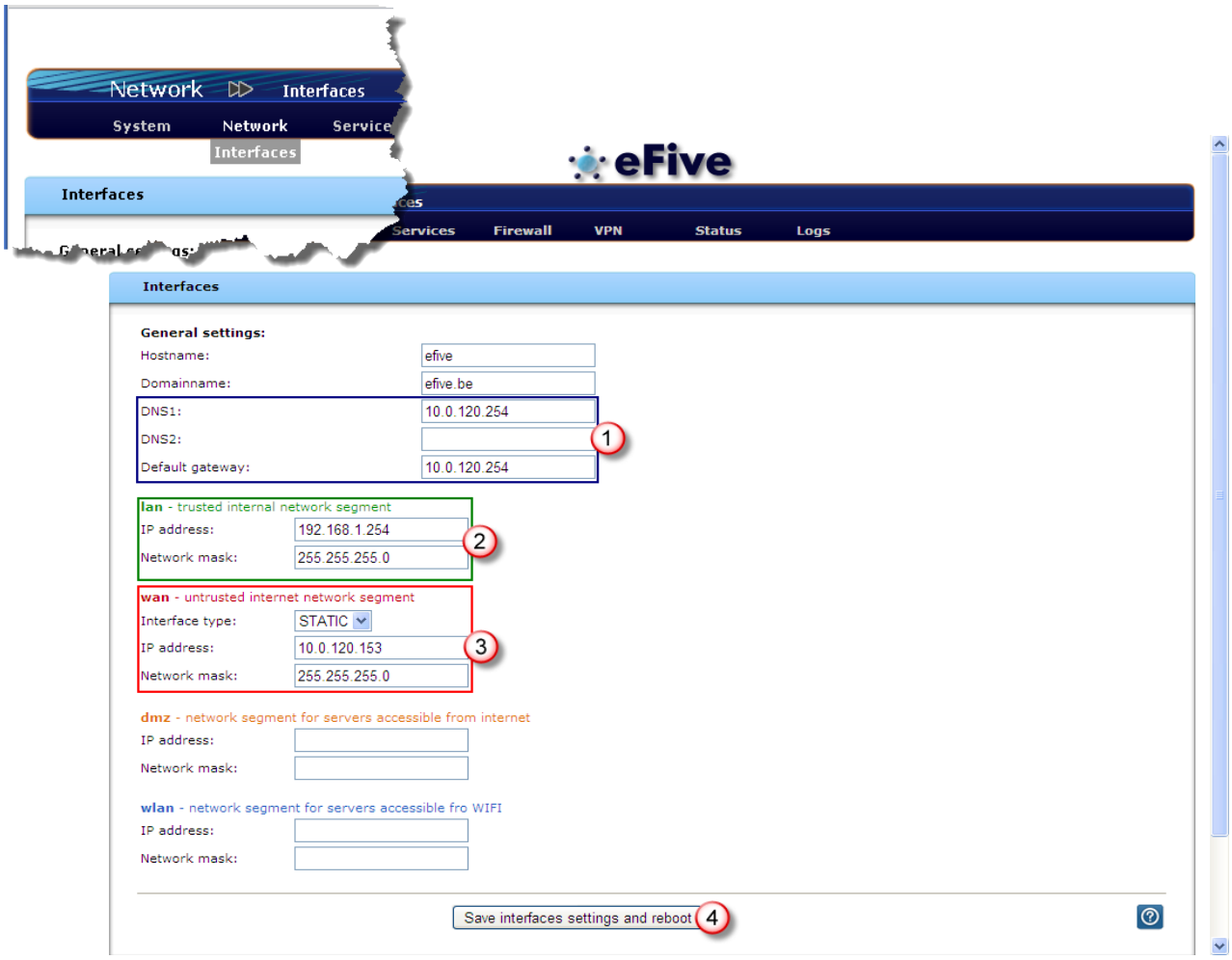
eFive 25 - backpanel view



eFive 100 - Front panel view

Configuration

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



- 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 it.

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

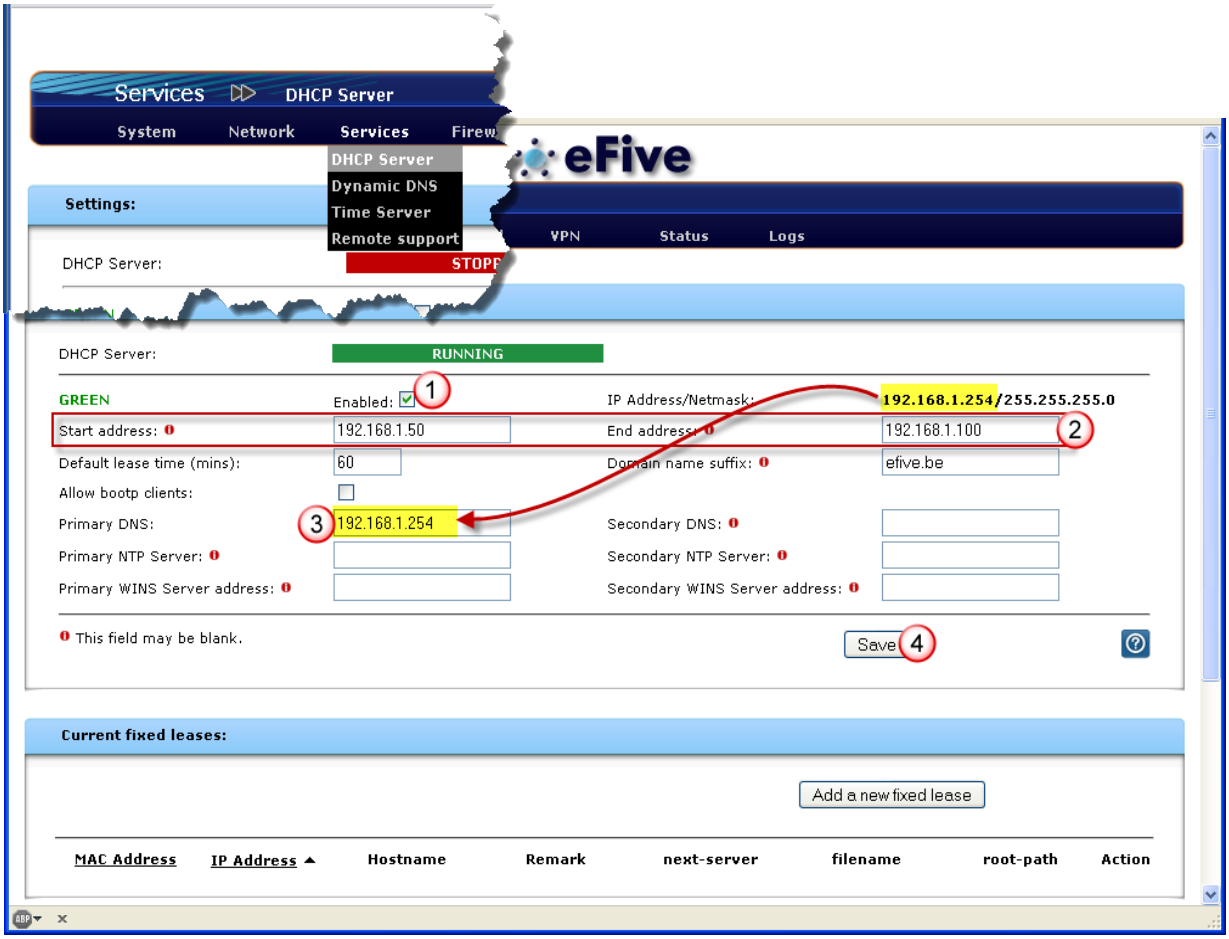
- In the red network (3), configure the ***IP address*** and ***Network Mask*** for the WAN side of the eFive***.***
  Note: DHCP could also be used for the network configuration. But as the Internet Router must forward the VPN packets to this interface, better use here a fixed known IP address.

- 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***



- 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** > **OpenVPN,** see Step 4).*
- In the Primary DNS (3), enter the LAN IP address of the eFive you have configured.

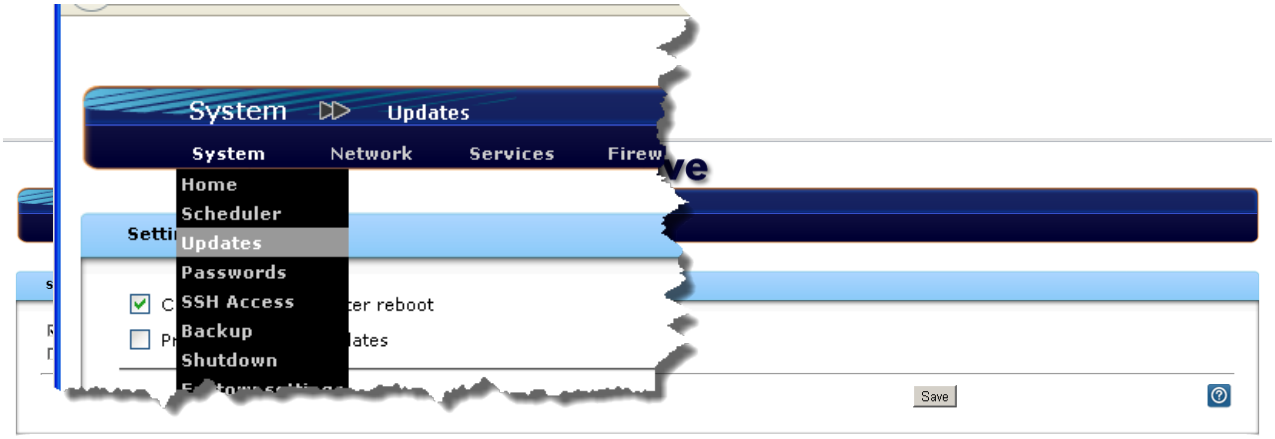
  This address can be copied from the IP Address/Network information field appearing in the top right corner as shown in the picture above.
- You can leave the other fields blank.
- Click ***Save*** (4).

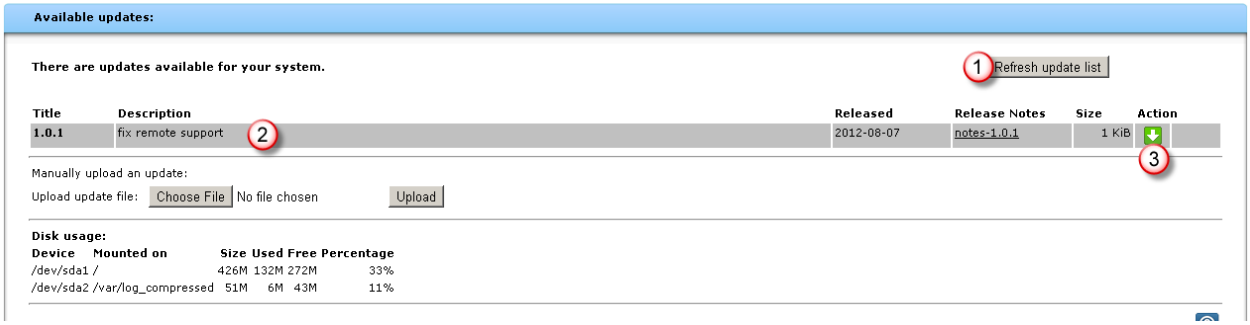
Step 3 - Check for updates

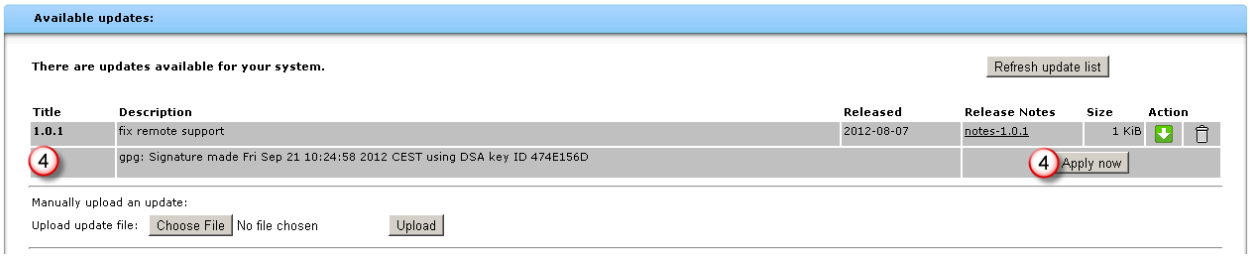
Before going further in the configuration, it is now recommended to check if updates are available for your eFive in order to benefit from the latest developments and fixes.

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***

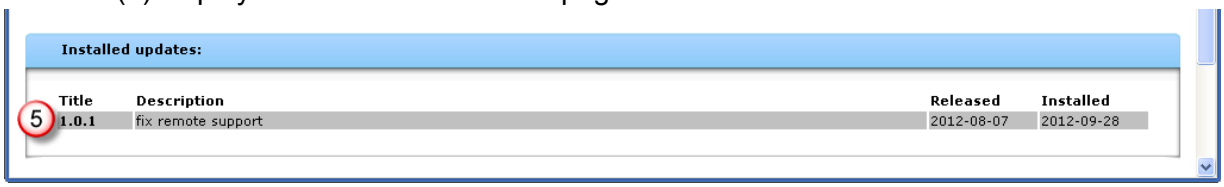






- To refresh the list of available updates, click ***Refresh update list*** (1).
- This action is gathering the information and, if an update is found, it is displayed in the ***Available updates*** (2) zone.
- Click on the green arrow (3) to download the file on your eFive. This operation will not launch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



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

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) and at least one VPN-account.

Creating Certificate Authorities (CA)

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

- To create the Certificate authorities, from the main menu select ***VPN, CA***

- By default the two rows (1) ***Root Certificate*** and ***Host Certificate*** mention "**Not** present".
- On the right side of the screen, click on the button (2) ***Generate CA/Host Certificates***
- In the configuration interface, fill out at least the required fields (1) to create your Certificate Authorities (other fields are optional only). Read more on this next page.

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)

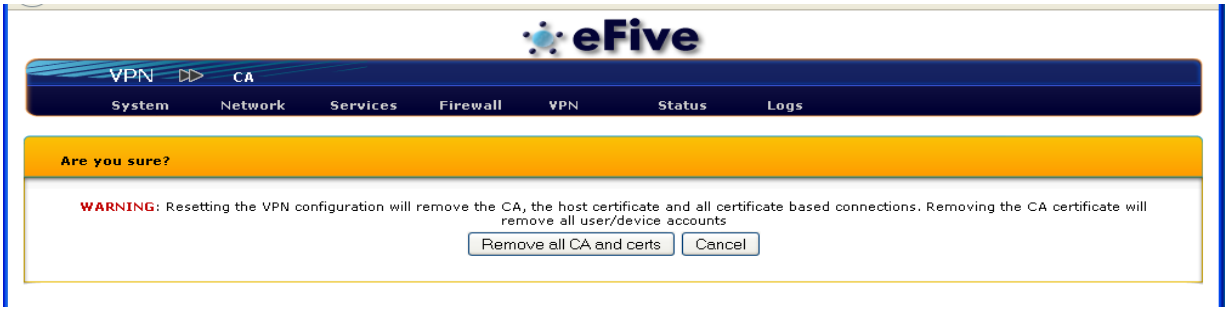
- When ready, click on the button ***CA/Host Certificates*** (2) to generate the certificates. When finished, the two certificates appear in the list of Certificate Authorities. **Note**: *This process can take up to several minutes.*

- After completion of the process, the two certificate 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.

Warning! Removing CA Authorities also results in removing ALL VPN accounts.

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



Configuring the VPN-server

To go to the VPN-server parameters click on ***VPN, OpenVPN*** from main menu.

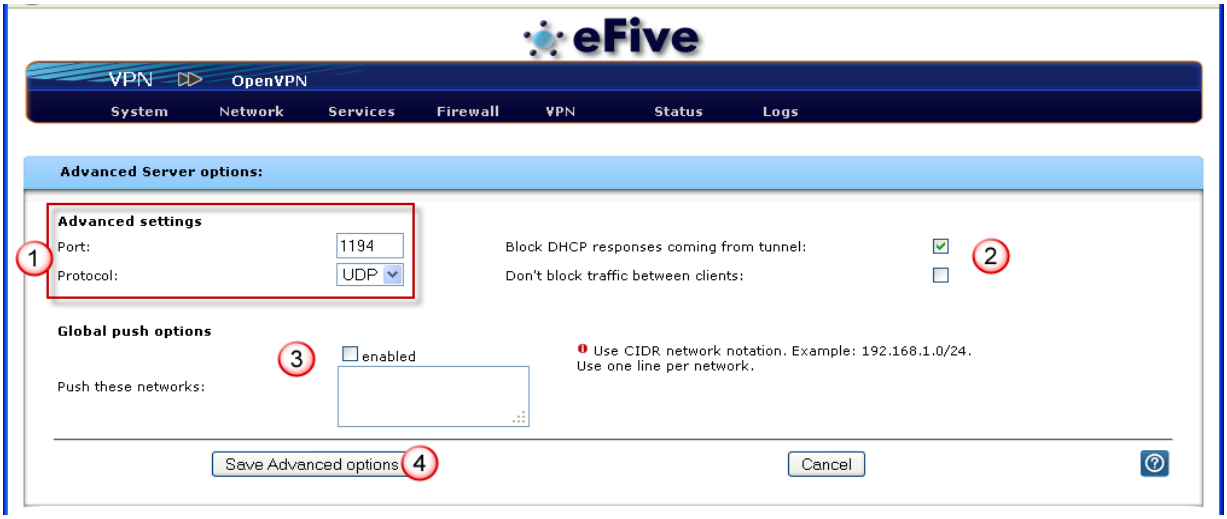
A. Define the range of IP addresses for VPN connection

- 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 will not start if the specified IP range is outside the LAN IP network.*
- Click on ***Save*** (3)
- Start the VPN-server by clicking on ***Start open VPN Server*** (4)

B. Optional VPN protocol and port configuration

The ***OpenVPN*** window features a button ***Advanced server options*** that is active only if the VPN-Server is stopped.
The Advanced Server option window allows to specify the TCP type and port used for the VPN connection (1).
Default settings are:

Port: **1194**
Protocol: **UDP**



The other fields of this page allow to define global behavior for the VPN network.
Default settings are:

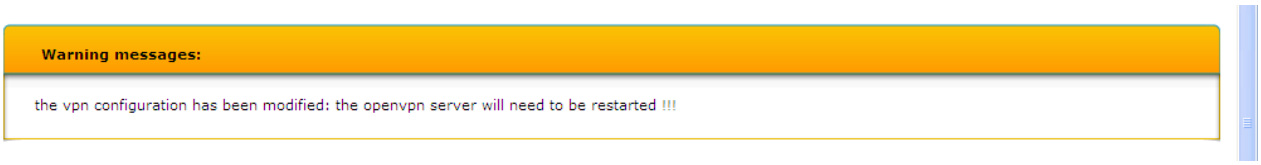
- To block DHCP responses coming from tunnel
- Not to allow VPN clients to communicate with each other.

If you want to change this behavior, check the corresponding check boxes:
Block DHCP responses coming from tunnel (2)
Don't block traffic between clients(2)

If special routing is required on all connected VPN clients, then you can define inside the ***Global push options*** the networks which should be routed to the eFive device (3).

Click ***Save Advanced options*** button (4) to apply the modifications

Note: after having saved, the interface shows a warning message informing the user that the restarting the VPN server is needed to keep the changes into account.

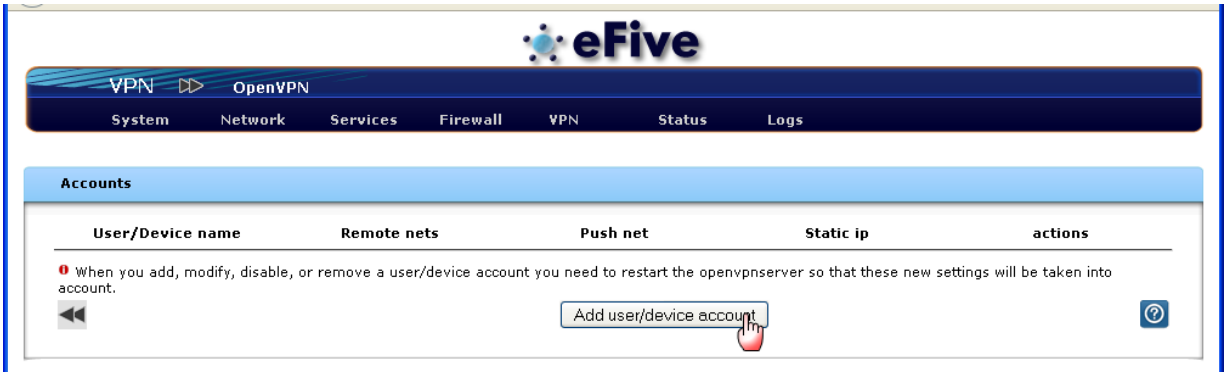


Creating a VPN account

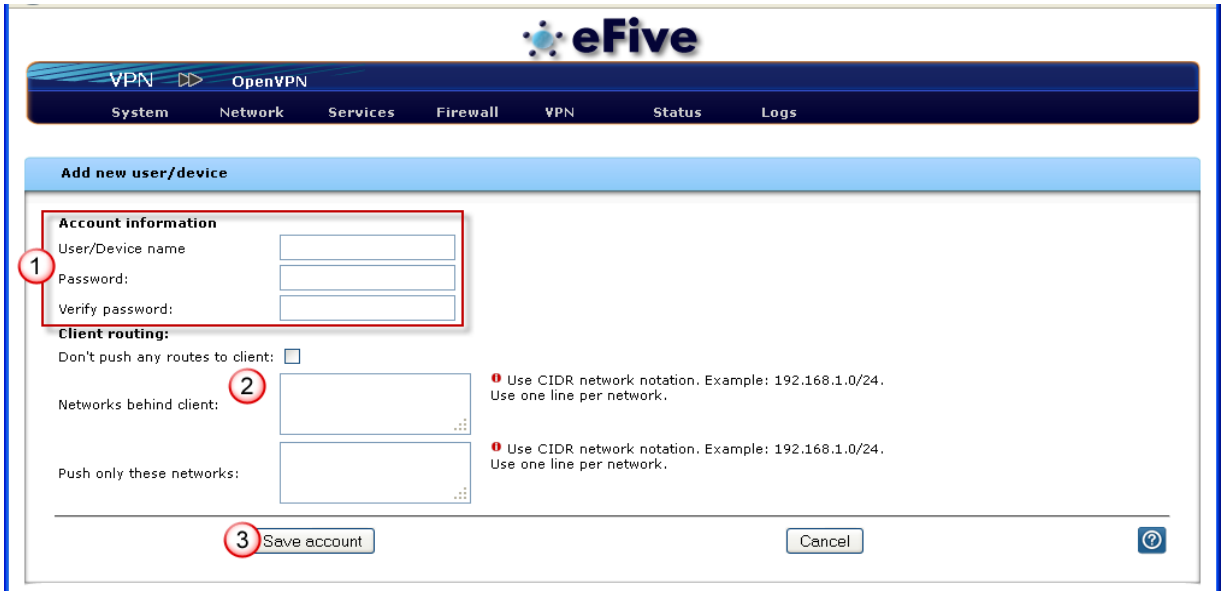
For each eWON to connect, you need to create a VPN account.

To do this, from the main menu select ***VPN, OpenVPN***

- In the ***Global Settings*** window click on the ***User/Device Accounts*** button (2)



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



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

If you need to access devices behind the eWON, you need to configure in addition (2):

- the ***Networks behind client*** field should contain the IP address of the eWON with subnet mask extension under CIDR notation.

  Examples of eWON LAN IP address in CIDR syntax:

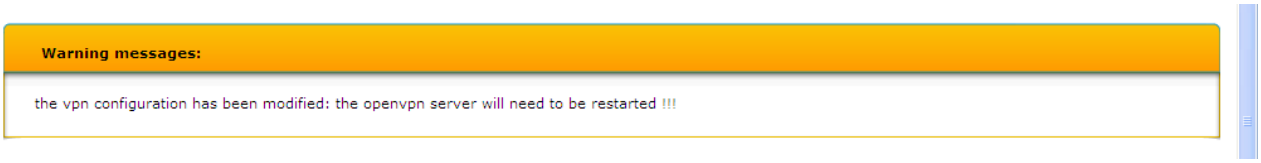
  If the eWON LAN address is 192.168.140.53, mask 255.255.255.0
  then, the CIDR syntax of this address is 192.168.140.0/24

  If the eWON LAN address is 192.168.140.53, mask 255.255.0.0
  then, the CIDR syntax of this address 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*** to save the account.

Note: after having saved, the interface shows a warning message informing the user that the restarting the VPN server is needed to keep the changes into account. Keep in mind that you can also restart the VPN server at a later time. So you can first add all needed accounts and then only restart the VPN server once. At the moment of a planned maintenance for example.



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 and click ***Save***.

Perform the same for the ***Root*** user.
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.

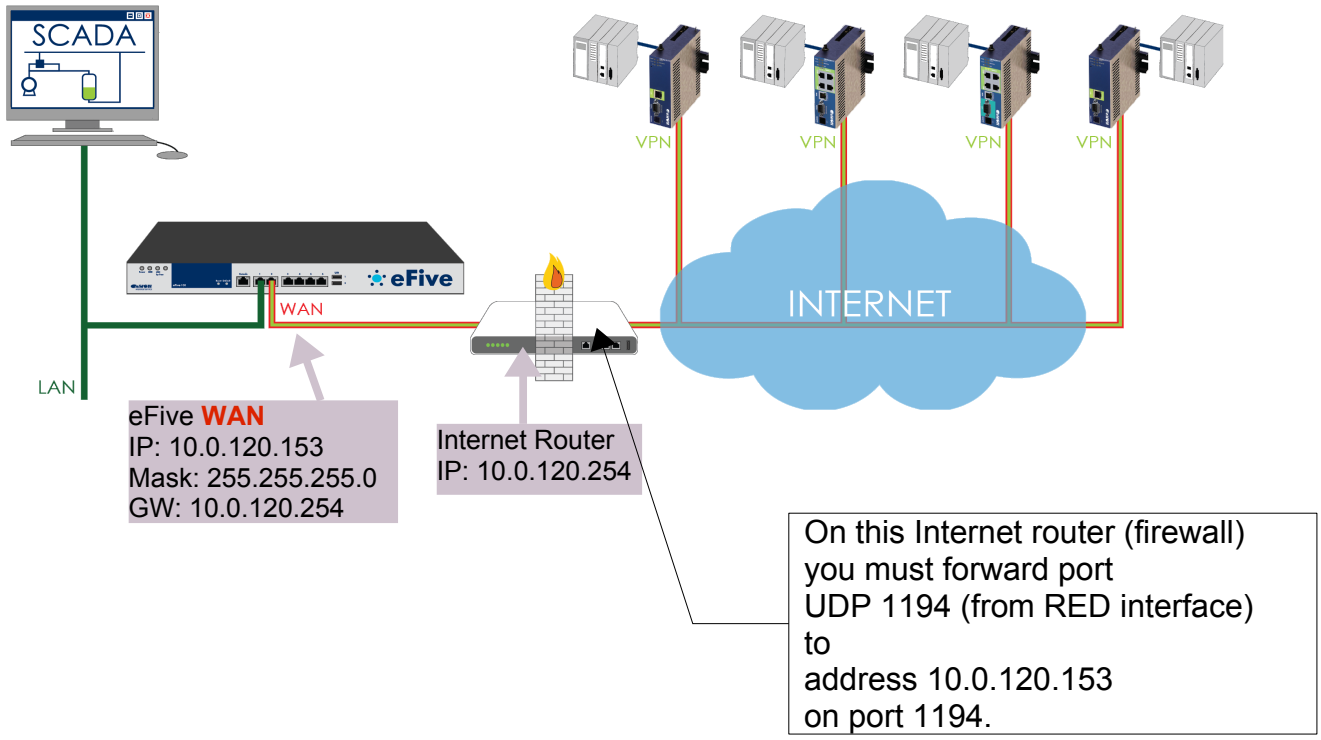
Step 6 – Internet-Router Configuration

Special configuration is required on your Internet router 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, Configuring the VPN-server point B.)

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

So on your Internet router you must forward incoming port UDP 1194 to be redirected to the WAN IP address of the eFive on port 1194.



Step 7 - eWON Configuration

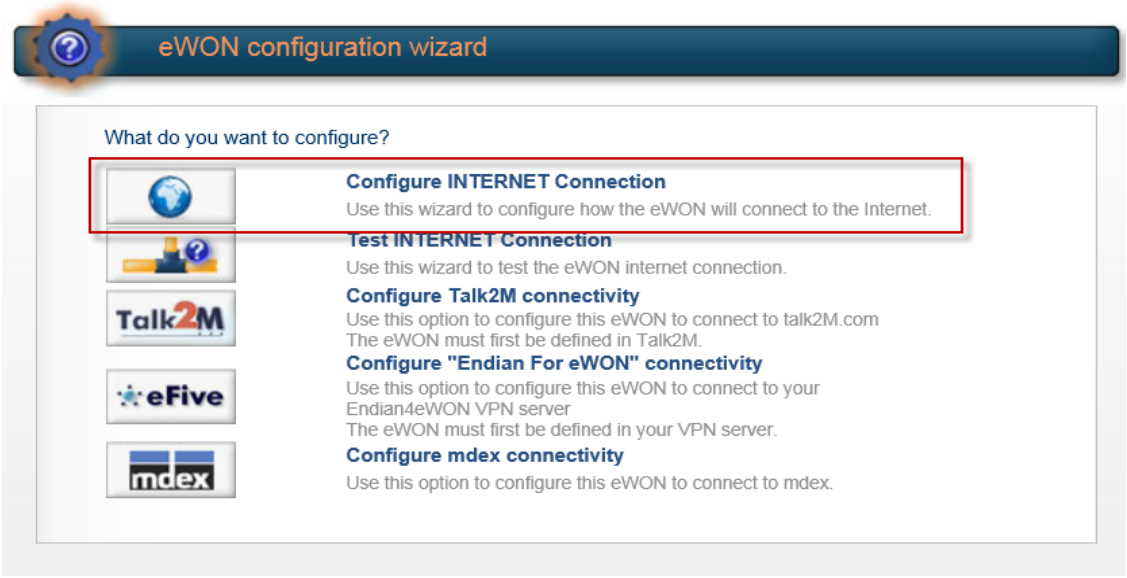
What will you need?

- ➔ The public address that must be used to reach the eFive. (public IP of Internet router)
- ➔ 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 (any form of web access) - this eWON should feature a firmware 6.4s6 or higher (upgrade first if necessary)

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.



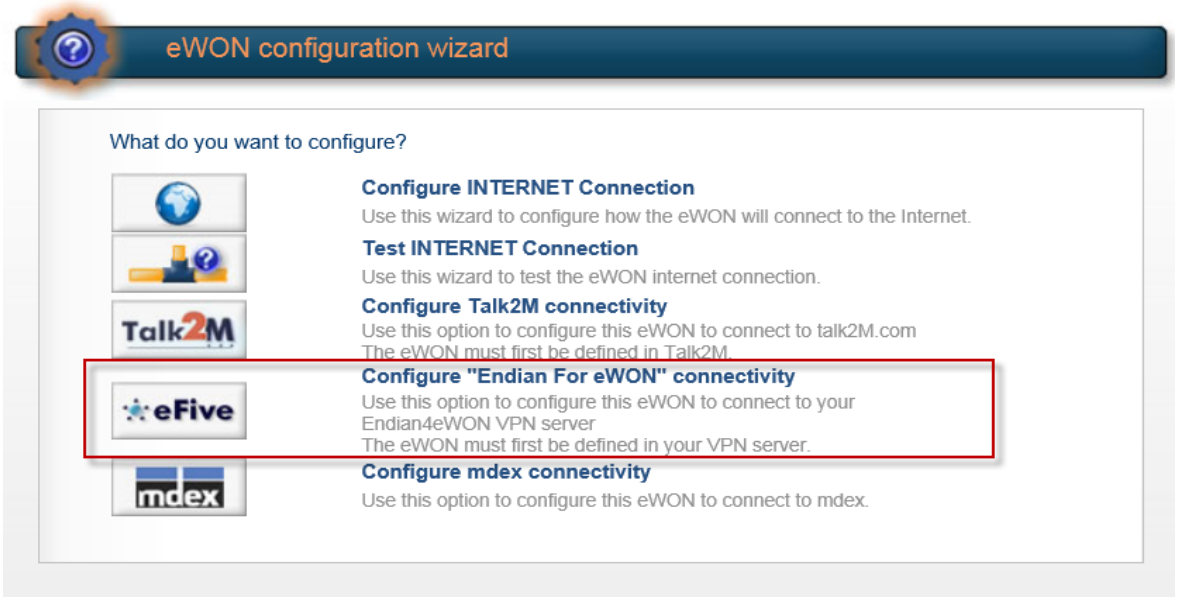
- Select the ***Configure Internet Connection*** row.
- Go through the Internet wizard.
- Check whether the connection test is successful

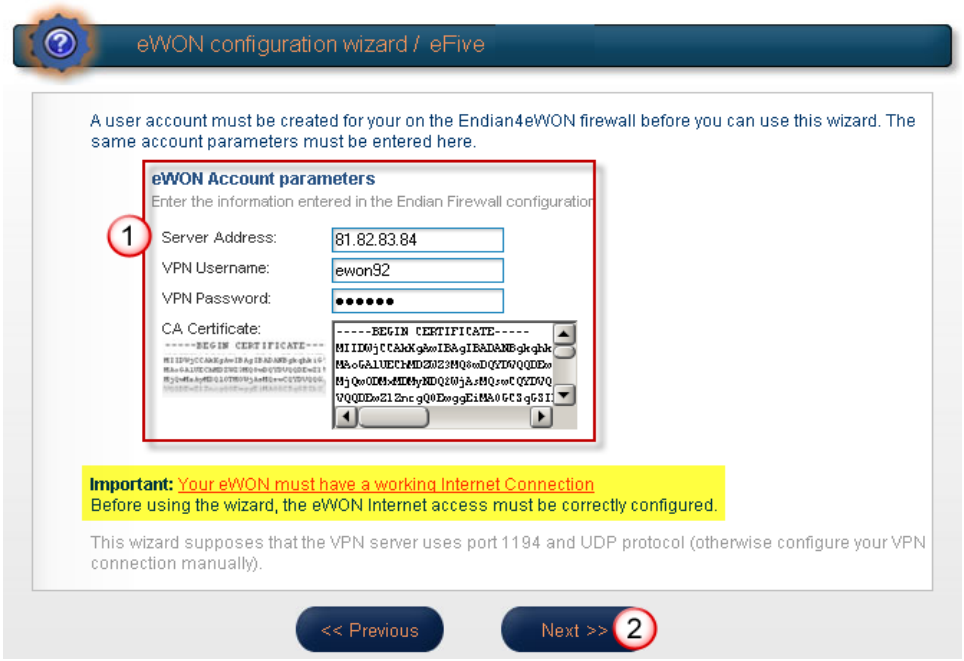
eFive connectivity

Important remarks:

1) This wizard works only on the UDP 1194 port. If you use another UDP port or a TCP port, then refer to the appendix “configuring an eFive connection without using the wizard”.
2) The creation of the VPN connection requires that both the eWON and the eFive have their respective clocks at the same date/time. If there a (too large) discrepancy between both, the certificate will not be accepted.

Return to the eWON configuration wizard page.
Click on the ***eFive connectivity*** button (formerly ***Endian for eWON connectivity***)



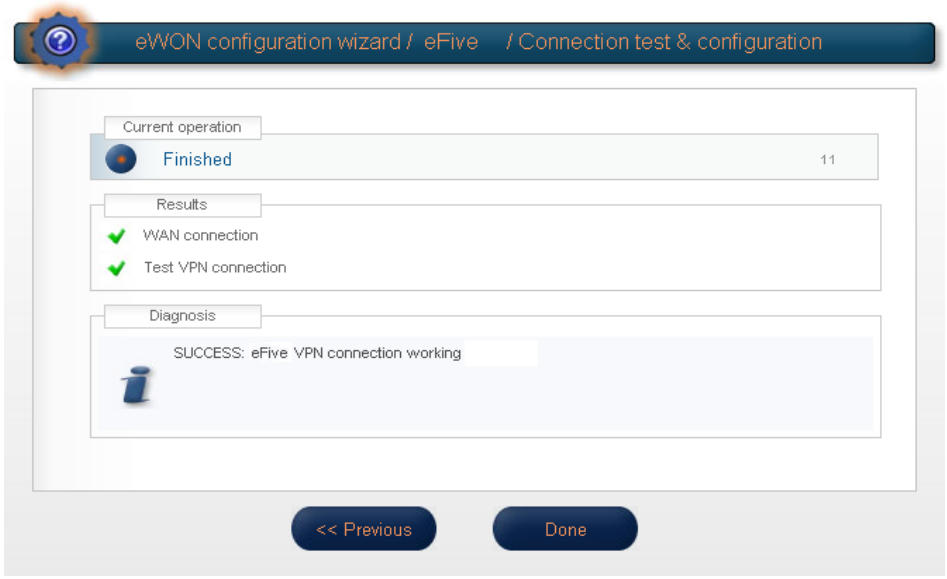


Set the parameters for the eFive connection.(1)

- The ***Server Address*** is the public address of the Internet router behind which the eFive is placed.
- 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 from -----BEGIN CERTIFICATE----- and ending with -----END CERTIFICATE-----.

Cick ***Next***. (2)

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

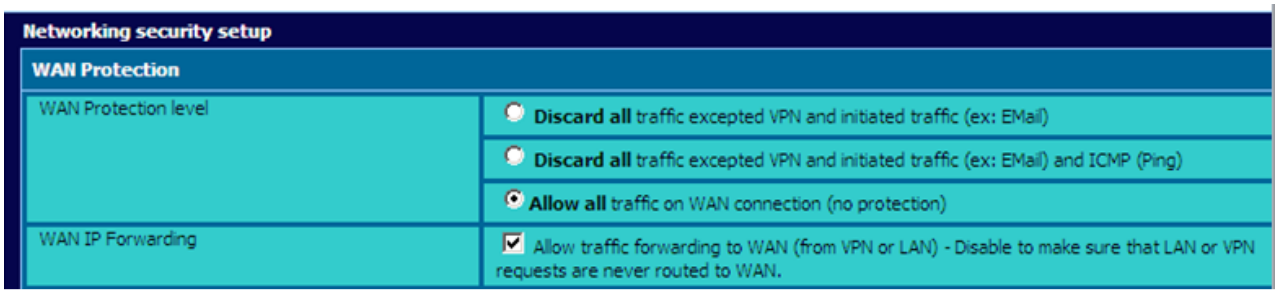


Click ***Done***.

On the eFive side, the newly created eWON now appears in the list ***Connection status and control*** displayed on the home page or accessed through the main menu ***VPN, OpenVPN.***

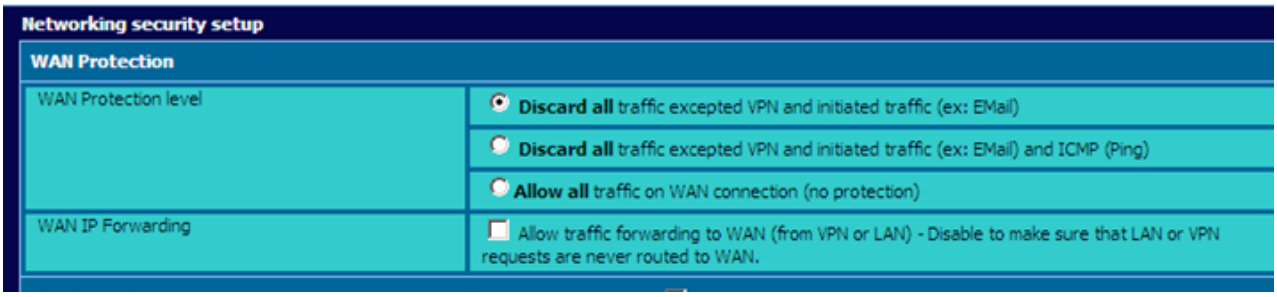
WAN security setting

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



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 [adm] of the eWON was not changed.

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



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 roles 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***
- You can plug-in an USB storage media on the eFive frame
- This device appears under the Select Media area
- Select the media on which you want to store your backup
- 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 - Restarting or shutdown 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:

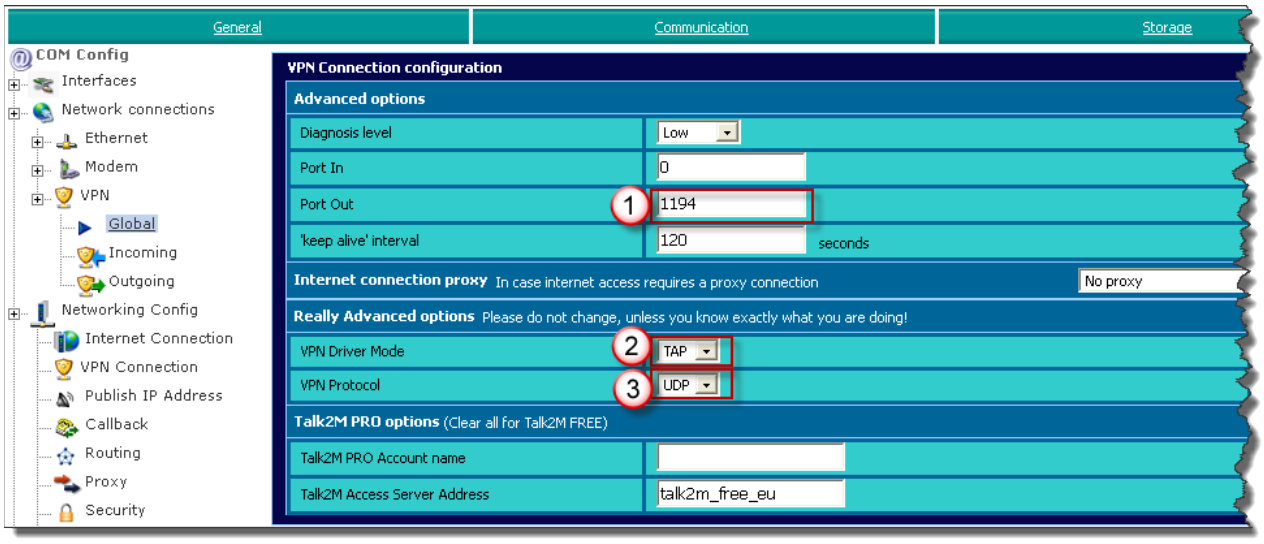
- From the main menu select ***System, Shutdown***
- Either click on the ***Reboot*** or on the ***Shutdown*** button, depending on the action you want to see executed.

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

5 – Configuring an eFive connection without using the wizard

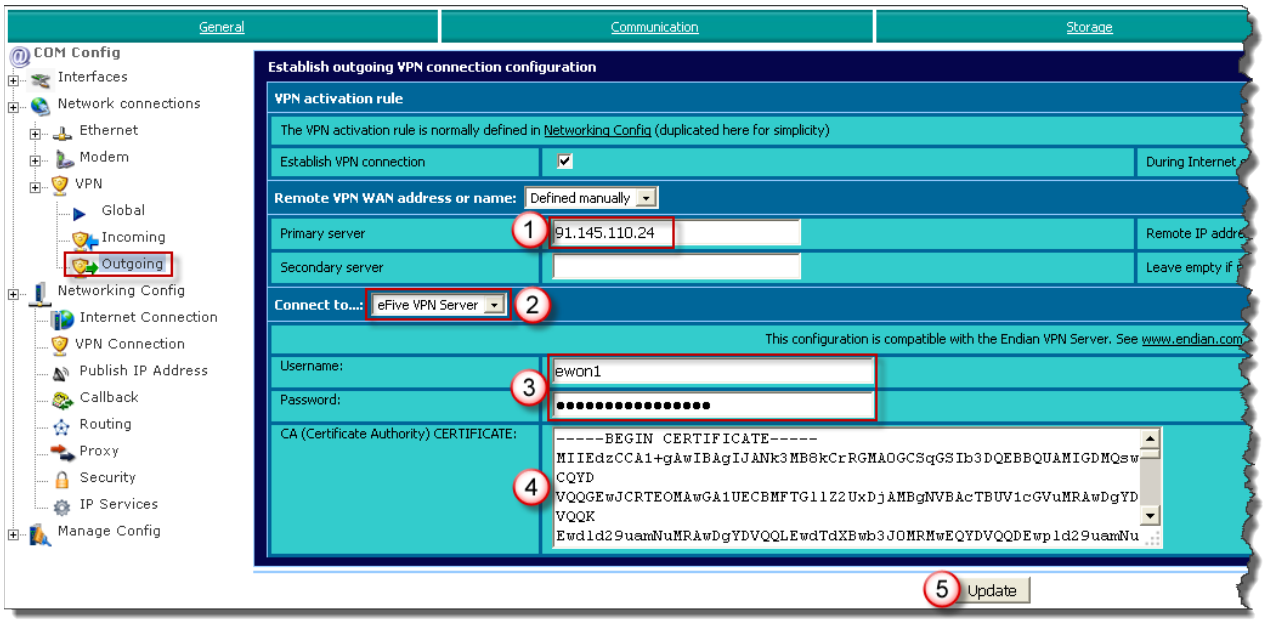
To configure the eWON for an eFive connection without using the wizard proceed as follows:

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



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

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



- 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-----

- 4) 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	10/25/12	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

i

Document build number: *148*
