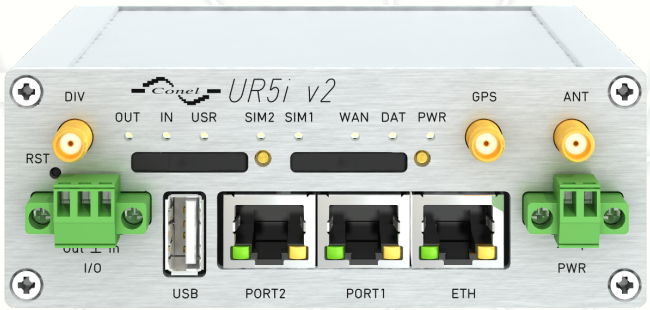
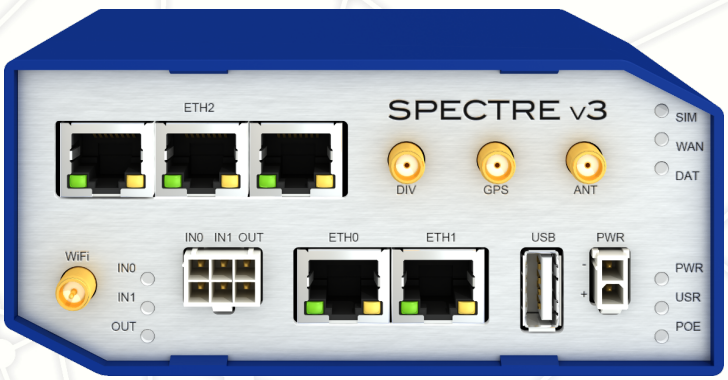
B+B SmartWorx®

ENABLING CONNECTED INTELLIGENCE

SmartCluster

APPLICATION NOTE





Trademarks, Licences and Brands

Conel, the Conel Logo, SmartCluster and MiniCluster are trademarks of Conel s.r.o..

Other trademarks, brands and company names may appear in this manual; if so, they shall remain the exclusive property of their respective owners. The absence of an explicit labelling of registered trademarks does not allow the conclusion that this brand was not subject to third party rights.

® & © 2014 Conel s.r.o.
Sokolská 71
562 04 Ústí nad Orlicí
Czech Republic

http://www.conel.cz//

Version of this manual: 26th October 2015.

This manual describes: SmartCluster 2.0.2 and its named variants.

The content of this manual can change due to technical innovations. Any such changes will be made without separate notification.

Editorial staff:

M. Kraft – Software-Dokumentation – http://www.software-dokumentation.net/
J. Hilgner – LUCOM GmbH – http://www.lucom.eu/

Contents

List of Figures

List of Tables

Part I

Introduction

1. Preface

1.1 SmartCluster — Conel´s VPN service portal

Complementary to mobile network and LAN-to-LAN routers, SmartCluster is an optimised VPN service portal that enables the adjustable connection of entire networks, machines, sites, control centres and sales representatives. By means of VPN the routers directly connected to the SmartCluster. An additional VPN interface allows smartphones to access each device that is connect to the router.

Identically constructed machines and sites with identical IP addresses can be interconnected a number of times via 1:1 NAT. A certificate-based encryption safeguards Road warriors' access authorisation and communication between sites. Tedious manual setting of routers and PCs to enable remote maintenance is not required: SmartCluster creates the required VPN settings automatically and offers them for download.

1.2 SmartCluster — Different variants

You may acquire SmartCluster different variants, adjusted to your needs. It's up to you to decide how many connections you require.

	Single access	**Virtual Machine**	**Mini-cluster**	**Industrial PC (IPC)**	**Customer Data Center**	**Data Center Internet Server**
Client Access	yes	yes	yes	yes	yes	yes
Administrative Access	no	yes	yes	yes	yes	yes
Server Hardware from	Conel	Customer	Conel	Conel	Customer	Provider
Internet access by	Conel	Customer	Customer	Customer	Customer	Provider
Installation by	Conel	Customer or Conel	Conel	Conel	Customer or Conel	Conel

1.3 MiniCluster — Conel´s security appliance

Complementary to Conel´s industrial mobile network and LAN-to-LAN routers, MiniCluster is a further development of Conel´s SmartCluster VPN service portal. Being installed on a small, electricity saving hardware MiniCluster is immediately operational and functioning. Not only does it connect single machines, sites, control centres and sales representatives but also entire networks.

The routers directly connect to the MiniCluster via VPN with a limited number of 100 connections at most. Noteworthy is the fact that identically built machines and sites with identical IP addresses can be interconnected a number of times via 1:1 NAT. A certificate-based encryption preserves the access authorisation of the Road warriors and communication between sites.

An outside attack or internet eavesdropping is not possible. Tedious manual and thus error-prone setting of routers and PCs to enable remote maintenance is not required as MiniCluster automatically

creates the required VPN settings and offers them for download on the MiniCluster portal. MiniCluster is operated by the company owned data centre. Without any tedious settings – just plug and play!

1.4 About this manual

In this manual you will find all the information required to set up and manage a SmartCluster. As MiniCluster uses an almost identical user interface you can use this manual for setting up a MiniCluster as well. All differences between the two products are described in “IV, 1 Differences to SmartCluster” on Page 65.

Set up your SmartCluster only **once** initially! Failing to do so will delete all previously created participants.

1.4.1 Objectives

This manual has several objectives. Firstly we will prepare you to do an initial set up of the SmartCluster and carry out an initial configuration to get the SmartCluster going.

Secondly, based on the figure below, we will demonstrate the small number of steps in the workflow you must go through to enable a Road warrior (left side) to get remote access via a VPN tunnel to FACILITY 1 (right side) and its controls. We will explain all settings and configuration necessary.

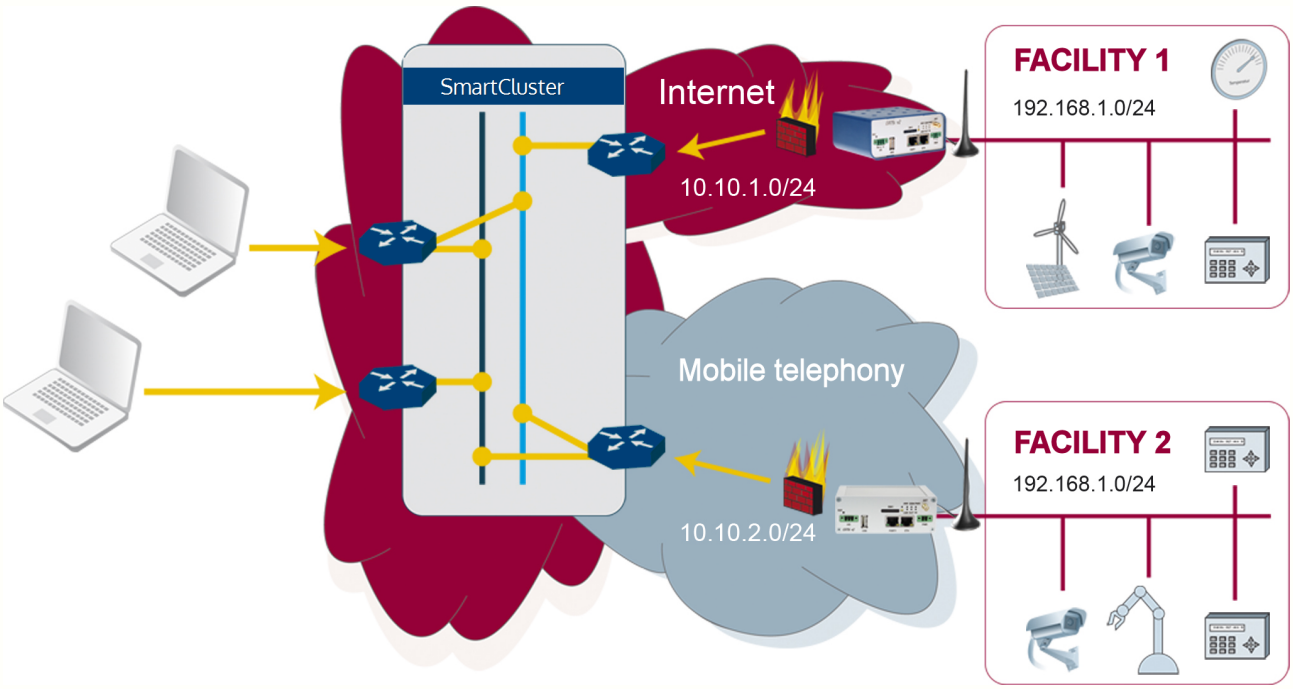


Figure 1.1: Example of a SmartCluster network scheme

- Necessary procedures as a *SmartCluster administrator*
  1. Create a Group, see “II, 4.3 Creating a Group” on Page 27
  2. Create a Network, see “II, 4.4 Creating and managing a Network” on Page 29
  3. Create a Road Warrior, see “II, 4.5 Creating a Road warrior” on Page 31
  4. Send access data, see “II, 4.6 Submitting access data” on Page 33
- Necessary procedures as a *Group administrator*
  1. Define ways of communication, see “III, 3.7 Specifying communication routes” on Page 54
  2. Download configuration files for the router, see “III, 3.4 Download files” on Page 46
  3. Configure the router, see “III, 3.5 Configure the router” on Page 47

Our third objective is to give you an understanding of how to manage a SmartCluster with the help of use cases.

The remaining parts and sections provide additional information and explain the use of the graphical user interface.

1.4.2 User concept

SmartCluster works with two different types of users. Because of their different tasks each user type is explained its own part in the manual.

In the interests of simplifying this document terms such as “he” are used to cover both male and female users.

1.4.3 *SmartCluster administrator*

The *SmartCluster administrator* (on Page 12) main tasks are creating and deleting participants (i.e. Groups, Networks and Road warriors). He can manage the (server) settings for the initial set up and query the status of the SmartCluster.

The *SmartCluster administrator* may as a matter of principle use his log in to carry out the tasks of a *Group administrator*.

1.4.4 *Group administrator*

We understand the term “Groups” as communication groups, clients or projects.

The *Group administrator* (on Page 41) is responsible for the configuration of the participants in his group. He can edit the groups and road warrior settings, disconnect participants and display the log files of his group. He is not able to delete participants.

Practically speaking it is a good idea to have one *Group administrator* for each group.

1.4.5 Accentuations

Function	Accentuation	Example
Username	Slanted	*SmartCluster administrator*
File name	Typewriter	`openvpngui.exe`
Dialogue name	Italics	*Authentication required*
Field name	Italics	*User name*
Menu/Menu item	Italics	*Road Warrior*
Option	Italics	*Grant Group Access*
Program code	Typewriter	`NTP_ENABLED=1`
Command	Typewriter	`# /.../scripts/backup.sh`
Button	Small Caps	*Reboot*
Icon	Sans Serif	Edit

1.4.6 Figures

All screen shots of the Web interface were taken from a current Firefox browser. Dialogues and/or adjustment of contents may differ if you use a different browser.

Display windows have been reduced down to the necessary information.

1.4.7 Data in figures

Do not use any data as used in a screen shot. Use only data (IP addresses, host names, user names, passwords, etc.) which are relevant for your environment. Using data taken from the examples may result in an unusable system.

1.4.8 Links

Links without roman numbering refer to a chapter in the recent part, e.g.: “1 Preface” on Page 2.

Links with roman numbering refer to part and chapter, e.g.: “III, 3.7 Specifying communication routes” on Page 54.

Links without any numbering are glossary terms, which are linked to the Glossary and Acronyms section, e.g.: Road warriors.

2. Security advices

Although every effort has been made to ensure accuracy, Conel cannot guarantee the correctness or completeness of the information within this manual. Conel does not assume any responsibility for (and expressly disclaims any such responsibility) either for any unintentional technical inaccuracies or for any losses, damages, consequential damages or lost profits that may be caused directly or indirectly by our software and its accompanying documentation.

All hard- and software products of Conel s.r.o. are subject to constant further development in relation to functionality, usage and presentation. Therefore their descriptions have no binding or contract-like character.

The information listed and explained in this manual applies only for the currently valid version.

This manual contains all the information necessary for the normal use of the product described within. It is written for technically qualified personnel.

All products are developed, manufactured and reviewed in accordance with the relevant standards (VDE provisions, VDE regulations and IEC recommendations).

These notes are intended on the one hand for your own personal safety and on the other to prevent damage to the described products or to other connected equipment.

2.1 Normal use, equipment configuration and installation

This device may only be used for the purposes described in this manual and only in combination with third party devices and components recommended or approved by Conel s.r.o..

ATTENTION

All the functions described in this manual can only be guaranteed to their full extent when using the latest version of the product.

Please also note that

- The proper and safe operation of the product requires proper transport, storage, positioning and assembly as well as careful operation.
- The automation system must be disconnected from any power source before it is assembled, disassembled or the structure is changed.
- The systems must be installed by qualified personnel. The corresponding specifications of DIN and VDE must be taken into account.

2.2 Notes on the installation of the product

- Safety and accident prevention regulations valid for the specific application must be observed.
- For 24V power supply ensure a reliable electrical isolation of the low voltage. Use only power supplies manufactured in compliance with IEC 364-4-41 or HD 384.04.41 (VDE 0100 Part 410).

2.3 Prevention of property damage and personal injury

- The voltage values must not be less than or greater than the voltage values listed in the technical data since it may lead to malfunctions or damage to the devices.
- Wherever errors in the automation system can cause great damage or even personal injury, additional external precautions must be taken or facilities provided to ensure or enforce a defined operating state in case of error (e.g. through independent threshold switches, mechanical latching, etc.).

2.4 Additional notes

During initial operation change the default password for the *SmartCluster administrator*! Failing to do so leaves the SmartCluster unprotected. Unauthorised access to SmartCluster is possible.

Do **not** change any server/VPN settings retrospectively! The settings between router and SmartCluster will differ. No further connections will be possible.

Create only **one** root certificate! Creating a second root certificate deletes all existing certificates. All previously created VPN tunnels become invalid. No further connections will be possible.

Do not enter any special characters into the fields *Name* and *Alias-Name*.
Do not use any names twice as this will overwrite any existing entry of the same name.

Change the default password for the user *root* on the router! Failing to do leaves the router unprotected. Unauthorised access to the router is possible.

3. Concept

The issue of remote service is becoming increasingly important. One the one hand customers and users expect global services around the clock. On the other many markets are already saturated and competition has increased due to copyists.

Against this background the topic "Services" has become an important tool for companies to clearly differentiate themselves from the competition and generate growth.

Using remote service enables technicians to access remote machines and plants from the central location. One of the important objectives is to pro-actively prevent outage of machines and plants by transmitting status reports to the 24/7 service desk at the central location for an immediate response via remote access.

Various routine jobs, such as updates and maintenance, can be conducted from the central location. Taken in sum remote services reduce the amount of on-site work for technicians thus reducing maintenance costs significantly.

3.1 SmartCluster

Usually you can initiate an outgoing VPN connection from your mobile device, allowing you remote access to a computer behind the VPN server and to interact with this computer. From your computer you cannot initiate a VPN connection to your mobile device as telephone service providers allocate IP addresses from a private address range to the mobile device.

SmartCluster has the ability to connect networks with private IP addresses via mobile telephony. Depending on the configuration you will be able to work with the local IP addresses of the remote devices. The access to the private IP networks is carried out via a mobile telephony router.

3.2 1:1 NAT

1:1 NAT is a very common network communication type in the industry. Within its scope one internal address is mapped to exactly one external address. The implementation of 1:1 NAT is interpreted differently.

The 1:1 NAT variant of Conel maps the real IP address (as configured in the device) to a VPN IP address. This VPN IP address is then used for the remote access.

The 1:1 NAT variant of Conel only works in a combination of SmartCluster and Conel VPN mobile telephony routers respectively LAN routers.

Example

The content of Fig. 3.1 on Page 9 serves as the basis for all examples used in this manual.

FACILITY 1 (network address 192.168.1.0/255.255.255.0) resides behind a Conel VPN router. As a road warrior you want to access FACILITY 1 using a smartphone or a computer. Therefore you connect the Road warrior to the SmartCluster via a VPN tunnel.

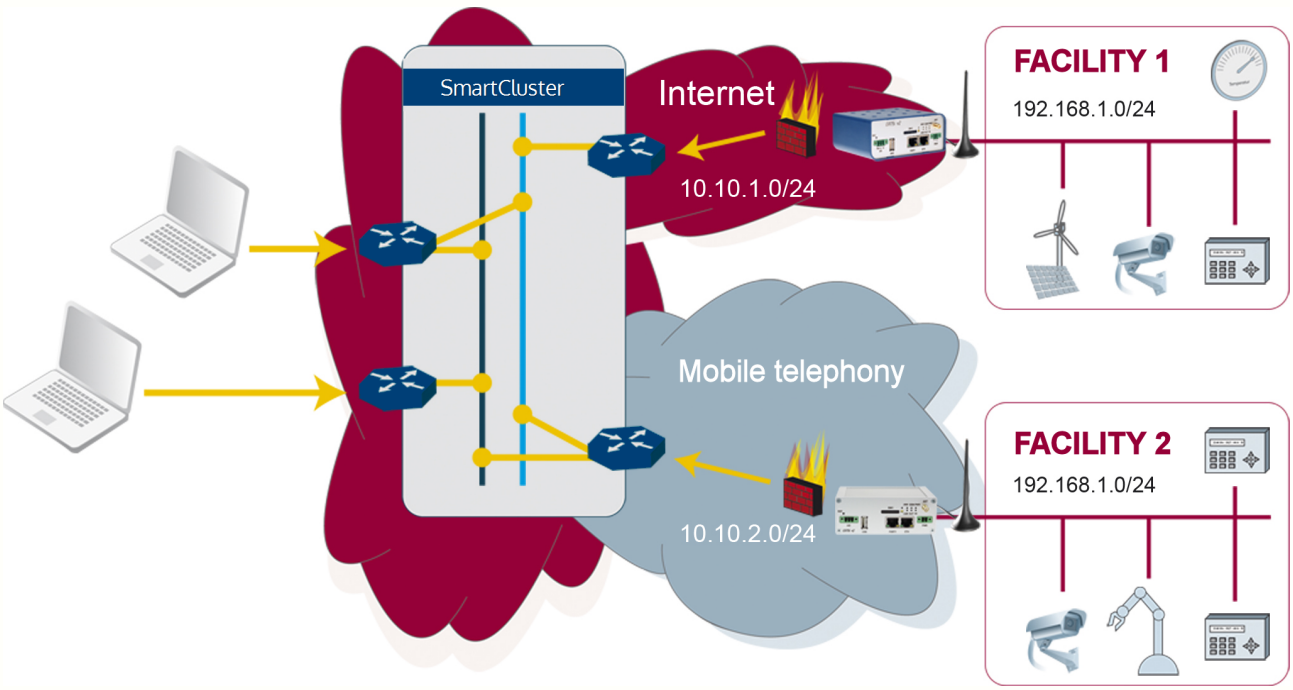


Figure 3.1: Example of a SmartCluster network scheme

Let's assume that FACILITY 1's camera in our example SmartCluster network scheme has the real IP address 192.168.1.11. The VPN access to this camera will be realised via the 1:1 mapped VPN IP address 10.10.1.11.

The first three octets (= 192.168.1) of the real IP address are substituted by the first three octets of the VPN IP address (= 10.10.1). Or in other words the first three octets of the VPN IP address are mapped over the first three octets of the real IP address.

The last octet of the IP address (= .11) is not affected by the mapping and is still used to access the camera.

Table Example provides some examples to illustrate the use of VPN IP addresses to access the real IP addresses in FACILITY 1's LAN.

Table 3.1: 1:1 NAT of VPN and real IP addresses in FACTORY 1

VPN address	LAN address
10.10.1.1	192.168.1.1
10.10.1.2	192.168.1.2
10.10.1.3	192.168.1.3

In our network scheme FACILITY 2 is locates behind another Conel router. This facility's LAN is configured with the same IP addresses as FACILITY 1 (192.168.1.0/255.255.255.0).

Let's assume that FACILITY 2's camera also can be accessed via the real IP address 192.168.1.11.

As the VPN IP address of FACILITY 2 (= 10.10.2.0) is different to the VPN IP address of FACILITY 1 (= 10.10.1.0), so you can access the FACILITY 2's camera using the VPN IP address 10.10.2.11.

Table Example provides some examples to illustrate the use of VPN IP addresses to access the real IP addresses in FACILITY 2's LAN.

Table 3.2: 1:1 NAT of VPN and real IP addresses in FACTORY 2

VPN address	LAN address
10.10.2.1	192.168.1.1
10.10.2.2	192.168.1.2
10.10.2.3	192.168.1.3

There is no danger of address conflicts for the remote access to the cameras. Access is carried out via the unique VPN IP address in the SmartCluster VPN combination and not double assigned real IP address 192.168.1.11.

You may remotely access systems without a VPN tunnel via real IP addresses, see "V, 11 Special case: Remote service for Siemens controls" on Page 73.

Part II

SmartCluster administrator

1. Tasks

As *SmartCluster administrator* you are allowed to create and delete network participants (Groups, Networks and Road warriors).

Generally your authorisation allows you to also carry out *Group administrator* tasks.

After the initial set up we will show in “4 Workflows” on Page 26 which steps are necessary for a *SmartCluster administrator* to grant a Road warrior remote access to system.

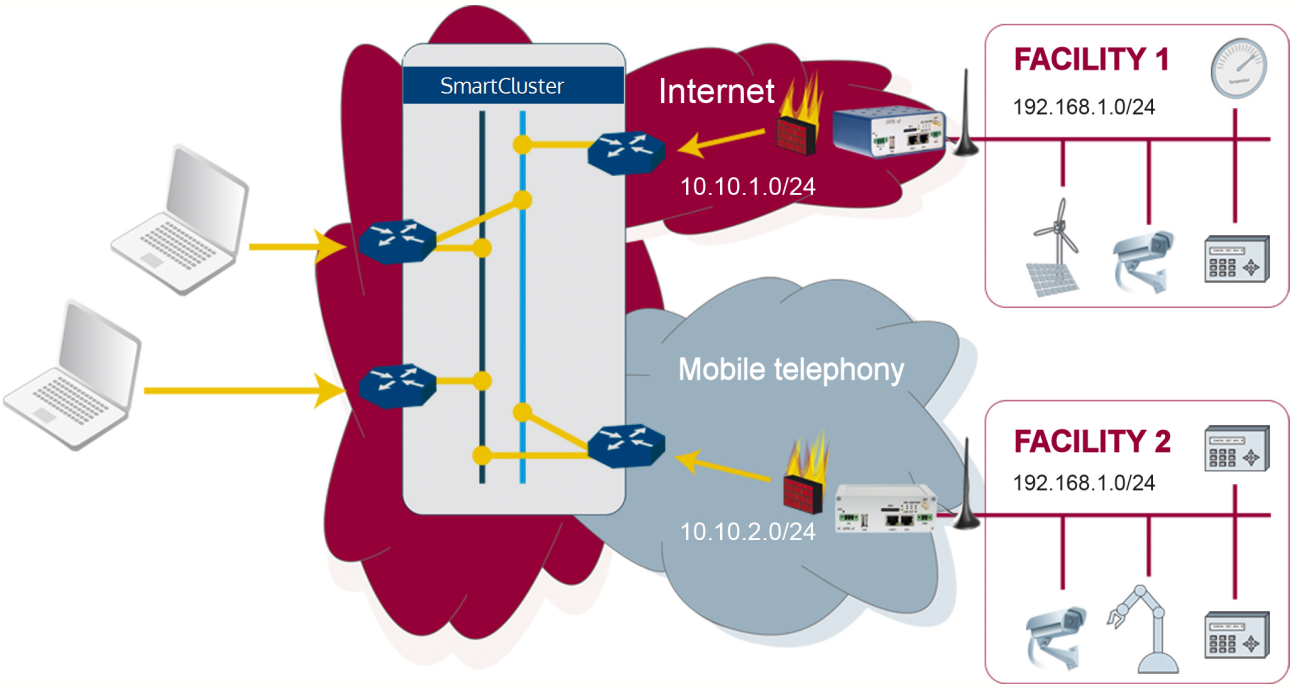


Figure 1.1: Example of a SmartCluster network scheme

- Necessary procedures as a *SmartCluster administrator*
  1. Create a Group, see “II, 4.3 Creating a Group” on Page 27
  2. Create a Network, see “II, 4.4 Creating and managing a Network” on Page 29
  3. Create a Road Warrior, see “II, 4.5 Creating a Road warrior” on Page 31
  4. Send access data, see “II, 4.6 Submitting access data” on Page 33
- Necessary procedures as a *Group administrator*
  1. Define communication routes, see “III, 3.7 Specifying communication routes” on Page 54
  2. Download configuration files for the router, see “III, 3.4 Download files” on Page 46
  3. Configure the router, see “III, 3.5 Configure the router” on Page 47

2. Graphical user interface

2.1 Start page

In this chapter we will explain the graphical user interface and its components for the *SmartCluster administrator*.

Figure 2.1: The *SmartCluster administrator* start page

On the left side of the start page you will find the Navigation menu.

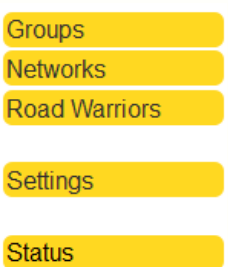


Figure 2.2: Navigation menu

In the lower left corner of all pages there is a green button to initiate the reboot of the server.

At the bottom of the start page you will find the contact data as well as the version number of your SmartCluster.

On some masks you can call up the online help by clicking on the *?* button.

2.1.1 *Groups* menu

"4.3 Creating a Group" on Page 27 describes ow to create a Group.

2.1.2 *Networks* menu

"4.4 Creating and managing a Network" on Page 29 describes how to create and manage a Network.

2.1.3 *Road warriors* menu

"4.5 Creating a Road warrior" on Page 31 describes how to create a Road warrior.

2.1.4 *Settings* menu

The *Settings* menu is described in "3.3 Menu settings" on Page 20. You must adjust the necessary settings only once.

You must configure the VPN server and E-Mail (server settings and mail template). You will create a root certificate (X.509 certificate) and define the global settings for Networks (routers) and Road warriors.

2.1.5 *Status* menu

Use the *Status* menu to find out more about the status of the server.

Table 2.1: SmartCluster status

Server	
IP Address / Netmask	SmartCluster IP address and network mask
RAM total / used	Main memory total / used
RAM free	Main memory free
Client IP	Web browser IP address
VPN	
Tunnel	Number of tunnels via OpenVPN and PPtP
	Tunnel online
	Total number of tunnel
Network	
Traffic data	Quantity of traffic data for current hour / day /month
	incoming and outgoing / total quantity
Network load	Network load, incoming and outgoing

2.2 General functions

2.2.1 Lists

Some symbols in tables will appear only after you have created the particular participant (e.g. a group). Before the initial set up most of the symbols are not yet present.

2.2.2 Symbols in lists

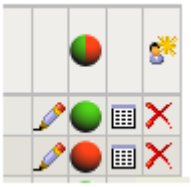


Figure 2.3: Symbols in lists

All overview lists are controlled via the symbols on the right side of the list. Symbols in the header/footer apply for all entries. Symbols in a row apply to this particular row.

Some symbols in tables will appear only after you have created the particular participant (e.g. a group). Before the initial set up most of the symbols are not yet present.

Table 2.2: Symbols and their functions

Symbol	Function
	All connections, show only online or only offline connections
	Online connections only
	Offline connections only
	Add a new entry
	Edit entry
	Display log file for entry, if available
	Delete entry
	Display CA certificate

2.2.3 Filter list entries

You can filter (larger) lists according to specific criteria.

You can use one criterion per filter only!

Groups

In the *Groups* overview list you can filter by the fields *Group Name* and *User Name*.

Enter a value in one of the two input fields. Press the ↵ button or click on the name of the field. The overview lists all entries according to the filter criterion.

Networks and Road warriors

In the *Networks* and *Road warriors* overview lists you can filter by the field *Name*.

Enter the name as a filter criterion. Press the ↵ button or click on the name of the field. The overview lists all entries according to the filter criterion.

To search for a group choose the desired group name from the *Group* drop-down list. The overview is adjusted automatically.

To remove a filter, delete the entry in the field or choose the entry "– – –" in the drop-down list. The complete overview will be displayed.

2.2.4 Sort list entries

To sort a list according to column values, click on the column header. The current list sorting type will be reversed, e.g. from ascending to descending.

> You can only sort one column at a time!

2.2.5 Names and alias names

Each network participant has a name (not subsequently modifiable) and an alias name (later modifiable). If you do not enter an alias name the SmartCluster adopts the entry in the *Name* field.

- The *SmartCluster administrator* chooses and enters the names.
- The *Group administrator* cannot edit the names (insufficient rights).
- The *Group administrator* may modify the alias names.

By using aliases you can achieve a certain degree of pre-sorting of list items via dexterous naming (descriptive names, uniform spelling).

You can tell at first glance the type of network participant and the corresponding group the participant belongs to.

Naming suggestions

- Groups: Group01, Group02. etc. or name of company
- Networks: group01-router01, group01-router02, group02-router01, etc.
- Road warriors: group01-user01, group02-user01, group02-user02, etc.

3. Initial set up

During the initial set up you must configure certain settings once (mandatory). The settings for Networks and Road warriors will be adopted from this base configuration.

A subsequent change to these settings affects all network participants already created. All configured VPN connections become invalid and cannot be used any longer.

3.1 Requirements

The following requirements must be met before initial set up:

- The SmartCluster IP address must be reachable.
- You are using the latest version of a web browser.
- User name: `admin`
- Password: `admin`

3.2 Log in

For the initial set up you must log in as a *SmartCluster administrator*.

Enter the SmartCluster IP address into the browser's navigation toolbar. The required protocol is https.

Example: `https://<IPAddress>/vpnadmin`

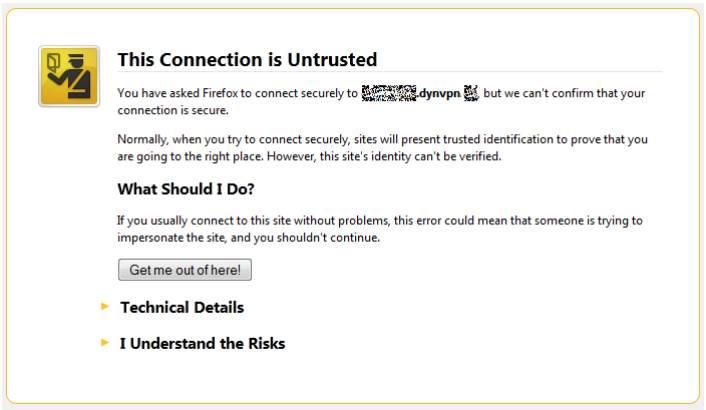


Figure 3.1: Dialogue box *This Connection is Untrusted*

During initial set up the browser may issue the warning *This Connection is Untrusted*. You must add an exception to the browser's security settings. This must be carried out once per domain and web browser.

Click the *I Understand the Risks* button. The dialogue box will then be expanded.

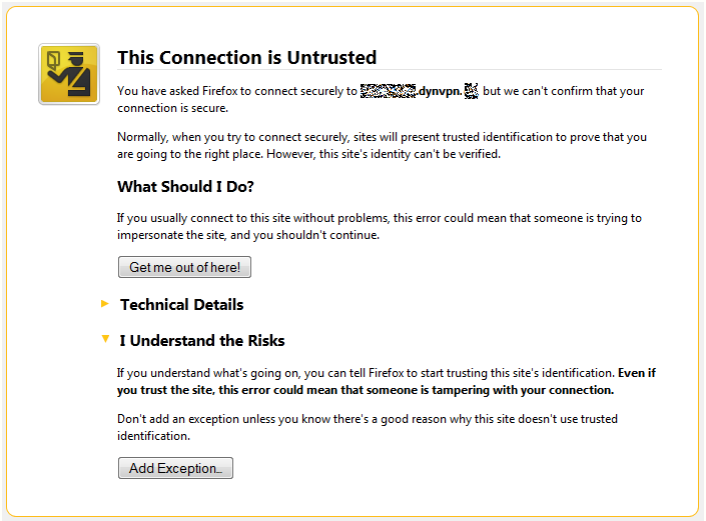


Figure 3.2: Dialogue box *This Connection is Untrusted – Add Exception...*

Click on the *Add Exception. . .* button.

The dialogue box *Add Security Exception* will be displayed.

Figure 3.3: Dialogue box *Add Security Exception*

Click on the *Confirm Security Exception* button.

The dialogue box *Authentification required* will be diplayed.

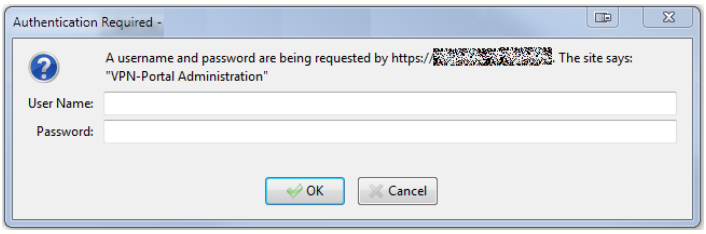


Figure 3.4: Dialogue box *Authentification required*

Enter the user name `root` into the *User Name:* field and the password `admin` into the *Password:* field.

Do not forget to change user name and password, see “II, 3.4 *Settings – Server*” on Page 20.

Click on the *OK* button.

Figure 3.5: The *SmartCluster administrator* start page

The SmartCluster start page will be displayed.

Now choose the *Settings* menu to make the necessary settings.

3.3 Menu settings

3.4 *Settings – Server*

In the navigation click on the *Settings* menu item. The *Server*, *CA*, *E-Mail* and *Options* sub-menu items will be displayed.

First click on the *Server* sub-menu item.

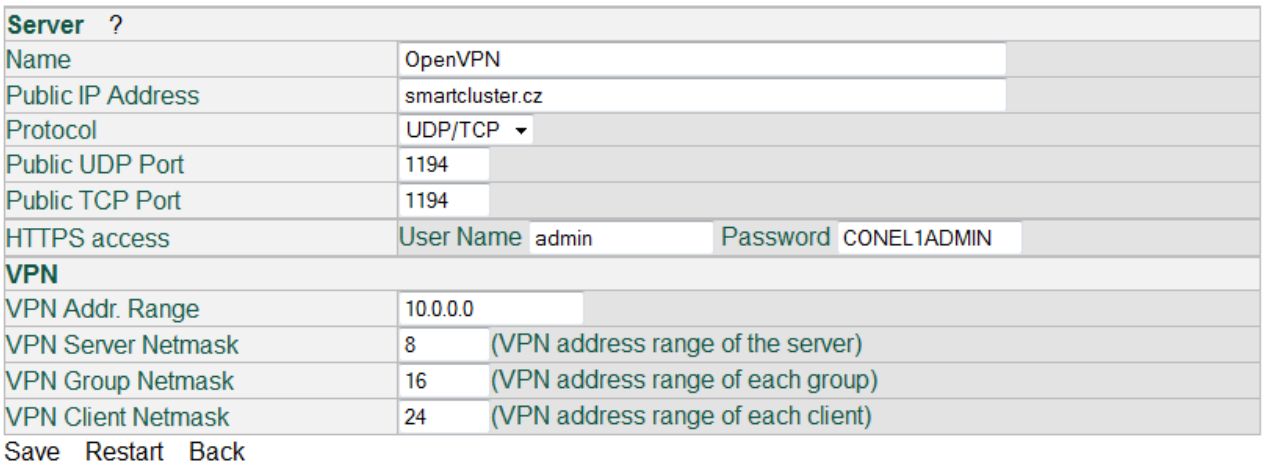


Figure 3.6: Server input mask

The input mask shows the following fields, see Table 3.1 on P. 21.

Enter an IP address in the *Public IP Adress* field. Otherwise your SmartCluster is not accessible via OpenVPN.

Modify the values accordingly. Use descriptive names as these are adopted by the router.

Port numbers for UDP and TCP must be larger than 1024.

To save the settings click on the *Save* button.

To restart the OpenVPN service click on the *Restart* button. Save any changes beforehand.

To initiate a reboot click on the *Reboot* button.

To discard any changes and go back to the previous page click on the *Back* button.

Table 3.1: Settings – Server

Server	
Name	Your server's name (any string)
Public IP Address	IP address (format: IPv4) or host name with the domain under which the server is accessible from the Internet. **Mandatory**
Protocol	Protocol for VPN tunnel communication: UDP, TCP or UDP/TCP – Default: UDP/TCP
Public UDP Port	UDP port number – Default: 1194
	The VPN server accepts UDP connections via this port.
	Recommendation: Accept value
Public TCP Port	TCP port number – Default: 1194
	The VPN server accepts TCP connections via this port.
	Recommendation: Accept value
HTTPS access	User name / Password
	Administrative access to the SmartCluster's graphical user interface via a Web browser

Change the user name and password now!

VPN	
VPN Addr. Range	IP address range for the complete VPN – Default: 10.0.0.0
	Network masks define the local sub-net. Change the values for the network masks only if this is necessary for operational reasons, see "VI, 13 How many device can I use?" on Page 75.
VPN Server Netmask	Network mask for the server's IP address range – Default: 8
VPN Group Netmask	Network mask for the groups' IP address range – Default: 16
	Only network participants who belong to the same group can communicate with each other, see "II, 4.3 Creating a Group" on Page 27.
VPN Client Netmask	Network mask for the clients' IP address range – Default: 24
	Recommendation: accept the default values for the network masks. Additional information in "V FAQ" on Page 70.

Do not change any server or VPN settings once you have initiated the reboot of the SmartCluster. Subsequent changes will lead to an unusable SmartCluster. You may change the user name and password. Please be sure to contact Conel if you have any questions regarding configuration, ideally beforehand.

3.5 *Settings – CA*

In the next step create a new, unique root certificate (CA = Certificate Authority). The root certificate contains keys and additional information used for authentication and decryption of confidential data are disseminated via the Internet and/or other networks. The root certificate is used during the set up of the VPN tunnel to the SmartCluster.

> Create the root certificate once before setting up the first access.

In the navigation click on the *Settings* menu item and then on the *CA* sub-menu item.

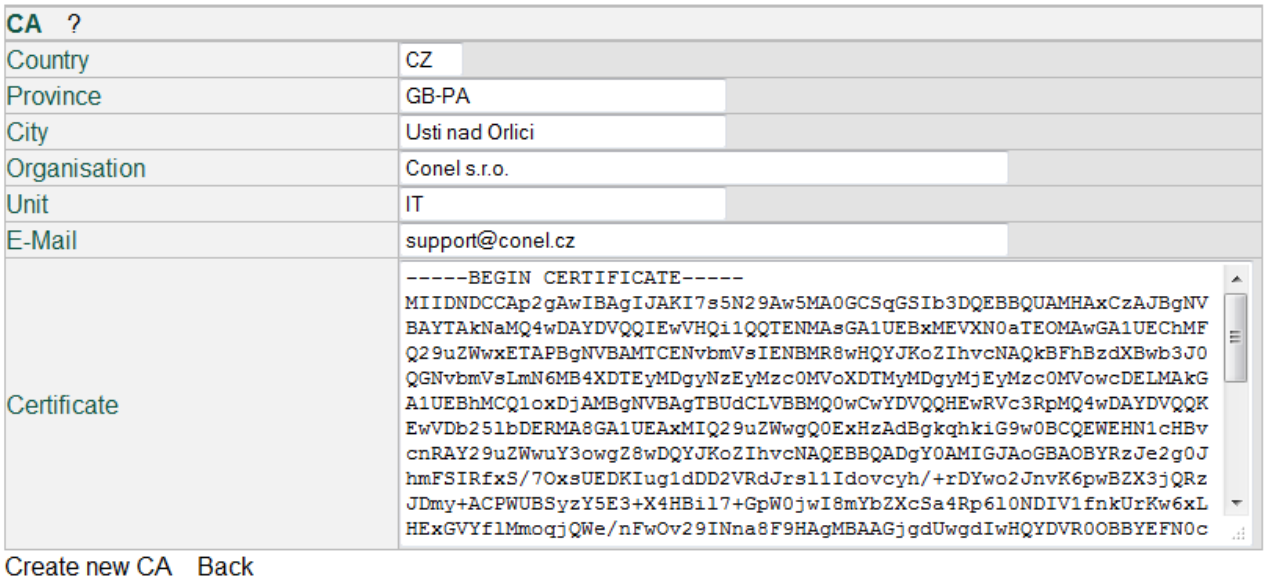


Figure 3.7: CA input mask

The input mask shows the following fields which have to be completed once during the initial set up:

Table 3.3: Settings – CA

Name	CA
Country	Two-digit country code (ISO-3166) – Default: DE (for Germany)
Province	Abbreviation for the federal state
City	Location information of the company which is owner of the certificate, normally the SmartCluster operator.
Organisation	Name of the company who is owner of the certificate.
Unit	Unit responsible for the root certificate
E-Mail	The company's E-Mail address
Certificate	Certificate

To create the new root certificate click on the *Create new CA* button.

Create only **one** root certificate! Creating a second root certificate deletes all existing certificates. All previously created VPN tunnels become invalid. No further connections will be possible.

To discard any changes and go back to the previous page click on the *Back* button.

3.6 *Settings – E-Mail* (Optional)

Use the *E-Mail* sub-menu item to define the SMTP settings for sending out E-Mails. The settings are similar to the settings of your E-Mail programme. E-Mails will be generated by the SmartCluster once you have created a new Group.

Recommendation: Configure the SMTP settings for sending out E-Mails now.

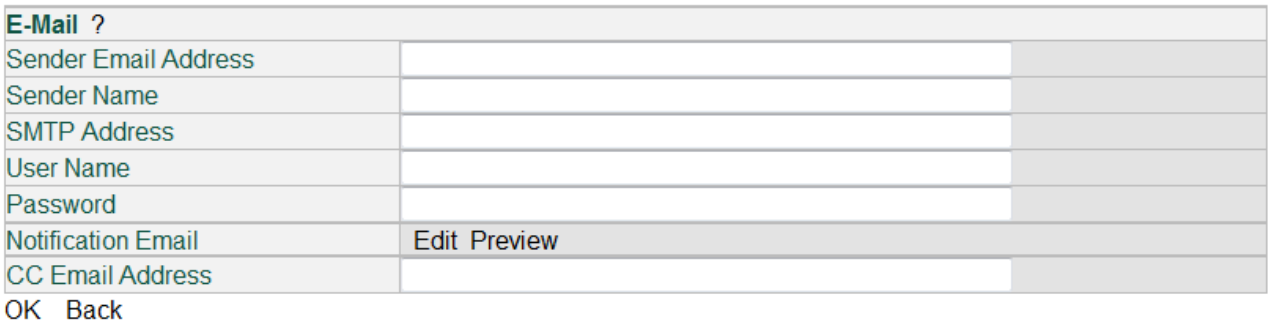


Figure 3.8: E-Mail input mask

The input mask shows the following fields:

Table 3.4: Settings – Email

SMTP	
Sender Email Address	Sender's E-Mail address
Sender Name	Sender's name, normally the *SmartCluster administrator*
SMTP Address	SMTP address of mail server
User Name	Mail server user's name
Password	Password
Notification Email	*Edit* button / *Preview* button
CC Email Address	E-Mail address for copy

The E-Mail contains the access data and a short description for the user on how to proceed.

Editing the E-Mail template

To edit the template text click on the *Edit* button. All text appearing in #, e.g. #PUBLICADDR#, are variables which are filled with values from the other masks, here the public IP Address of the server from *Server* input mask.

You can send E-Mails to the *Group administrator* once you have created a group and added the necessary contact information.

To preview the E-Mail click on the *Preview* button.

3.7 *Settings – Options* (Optional)

Use the *Options* sub-menu item to define additional parameters for the router which are not directly related to the SmartCluster.

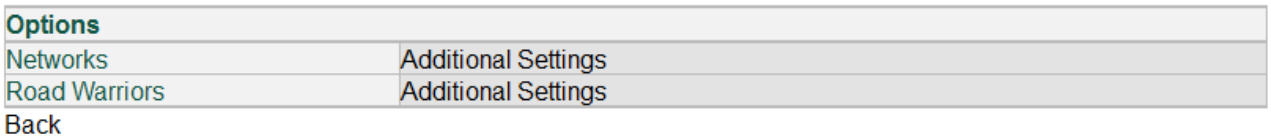


Figure 3.9: Options input mask

To define new parameters for the router click on the *Additional Settings* button. These parameters define global settings for all routers in the VPN network. Recurring general basic settings can be automated in the router. These settings overwrite the router's default settings.

All settings defined here are valid for all new Networks (routers), created in the future.

Example for best practice settings

```
PPP_PING=1
PPP_PING_IPADDR=172.27.0.1
PPP_PING_SINTVL=300
PPP_PING_INTVL=5
PPP_MONITORING=0
NTP_ENABLED=1
NTP_PRIMARY_SERVER=pool.ntp.org
```

These values, based on experience, help to stabilise mobile telephone and VPN connections.

Change/edit the parameters. To save the settings, click on the *OK* button.

If the version of your SmartCluster is 2.0.0 or lower, use `172.16.0.1` as the value for `PPP_PING_IPADDR` (ping address).

To discard any changes and go back to the previous page click on the *Back* button.

To add additional settings for Road warriors, click on the *Additional Settings* button. These OpenVPN settings define global settings for all Road warriors..

3.8 Finishing the initial set up

Finish the initial set up by initiating a reboot of the server.

Change to “4 Workflows” on Page 26 now to set up network participants.

4. Workflows

In this chapter we describe recurring workflows for the *SmartCluster administrator*. We will show which steps are necessary for a *SmartCluster administrator* to grant a Road warrior remote access to FACILITY 1.

As a *SmartCluster administrator* you create

1. Groups
2. Networks and
3. Road warriors

in this order. The *Group administrator* is denied the right to create network participants.

To set up the SmartCluster successfully you need:

- the SmartCluster IP address and
- user name and password for the SmartCluster

4.1 Requirements

The following requirements must be met before initial set up:

- The SmartCluster IP address of must be reachable.
- You are using the latest version of a web browser.

4.2 Log in

Enter the SmartCluster IP address into the browser's navigation toolbar. The required protocol is https.

Example: `https://<IPAddress>/vpnadmin`

The *Authentification required* dialogue box will be displayed.

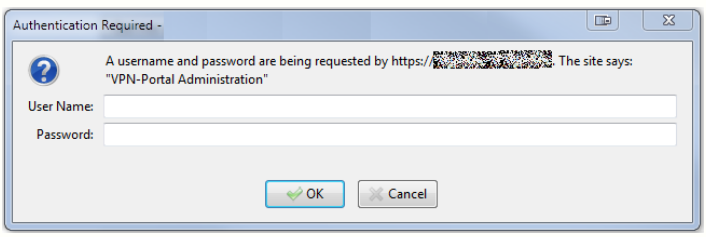


Figure 4.1: Dialogue box *Authentification required*

Enter the user name into the *User Name:* field and the password into the *Password:* field. The default user name and password were changed during the initial set up, see "3.6 Server input mask" on Page 20.

Click on the *OK* button. Your SmartCluster start page will be displayed, see Fig. "3.5 The *SmartCluster administrator* start page" on Page 19.

4.3 Creating a Group

As the first step of the workflow you will create a Group using the *Groups* menu item. We understand the term “Groups” as communication groups, clients or projects. The creation of groups is based on our global example, see Fig. “3.1 Example of a SmartCluster network scheme” on Page 9.

Only network participants (users and/or devices) within a group can communicate with each other. The default settings of the VPN client netmask (see “3.4 *Settings – Server*” on Page 20) allows you to create up to 254 network participants for one group.

Access to the service portal is created for each group. The *Group administrator* is able to see all network participants and manage his group.

A group generally consists of a project or a client who is able to access its devices only.

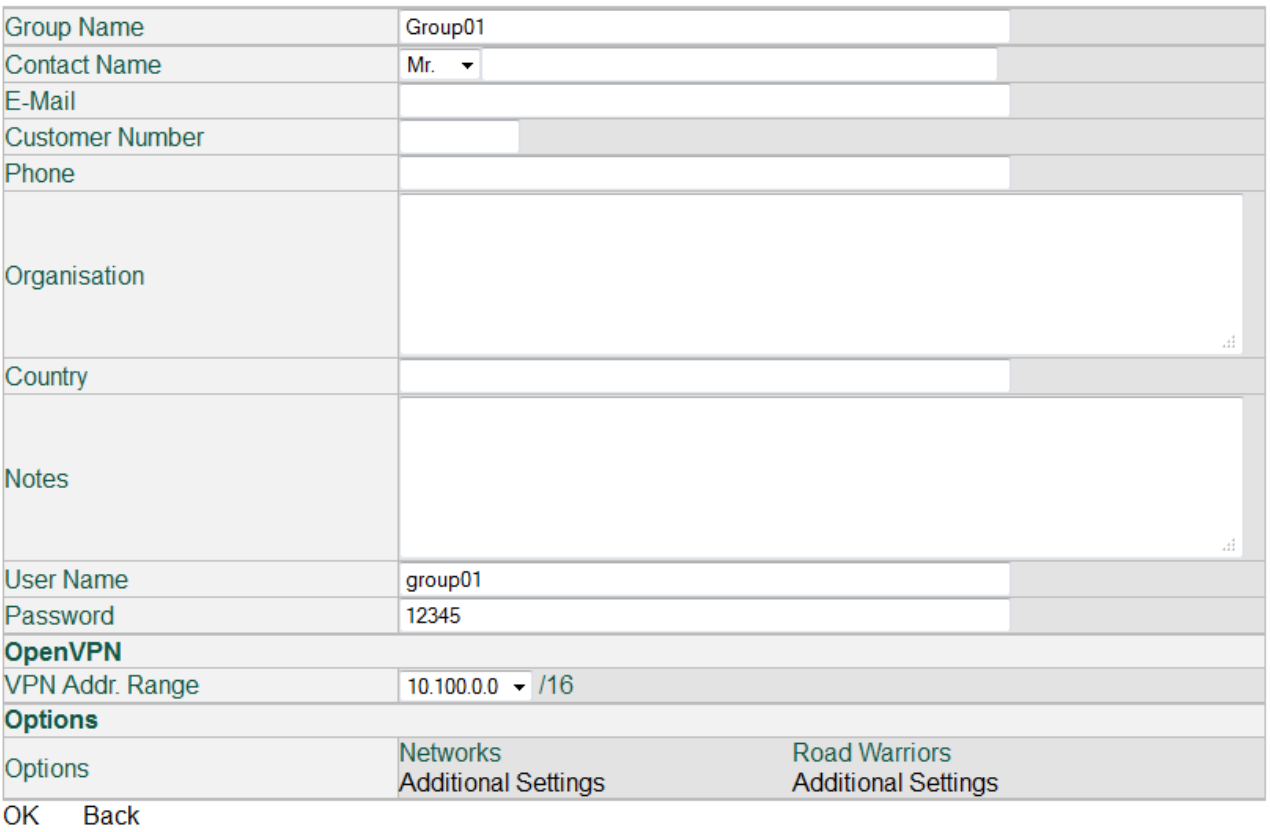


Figure 4.2: Dialogue box *Create Group*

Click on the *Groups* menu item in the navigation. The overview list for Groups will be displayed. This overview list is empty before initial set up.

To create a new Group click on the New symbol on the right side of the first line.

Do not enter any special characters into the fields *Group Name* and *User Name*.
Do not use any names twice as this will overwrite any existing entry of the same name.

The input mask shows the following fields:

Table 4.1: Input mask – Group

General		
Group Name	Name of group, e.g.: *Group01* If possible choose a descriptive name, see "II, 2.2.5 Names and alias names" on Page 16. Once saved do not change a group name because otherwise this will create an new group with the changed name.	**Mandatory**
Created on	Date of creation Shown after creation of group.	
Contact Name	Mr./Mrs.	
E-Mail	E-Mail address of *Group administrator* *E-Mail* button, details see below	
Customer Number	Customer number	
Phone	Phone number	
Organisation	Name of company	
Country	Country	
Notes	Notes	
User Name	User name	**Mandatory**
Password	Password You can also use the randomly generated password.	**Mandatory**
OpenVPN		
VPN Addr. Range	IP address range of the VPN tunnel According to the value in the network mask (default: 16 in *Settings* → *Server*) 256 different IP addresses will be displayed. You must save (Click on the *OK* button) the Group once before setting up the IP address range.	
Options		
Options	You can configure additional setting for the Network (router parameters) and for the Road warriors (OpenVPN parameters) here. All settings apply to this Group only. These parameters are added to the global server configuration.	

Change/edit the other parameters if necessary. To save the settings click on the *OK* button.

Now the *E-Mail* button is displayed. Click on this button to send an E-Mail with access data and further instructions to the *Group administrator*. (E-Mail template text: see "II, 3.6 *Settings – E-Mail* (Optional)" on Page 23).

To discard any changes and go back to the previous page click on the *Back* button.

4.4 Creating and managing a Network

In the second step of our workflow you will create a new Network (router).

Click on the *Network* menu item in the navigation.

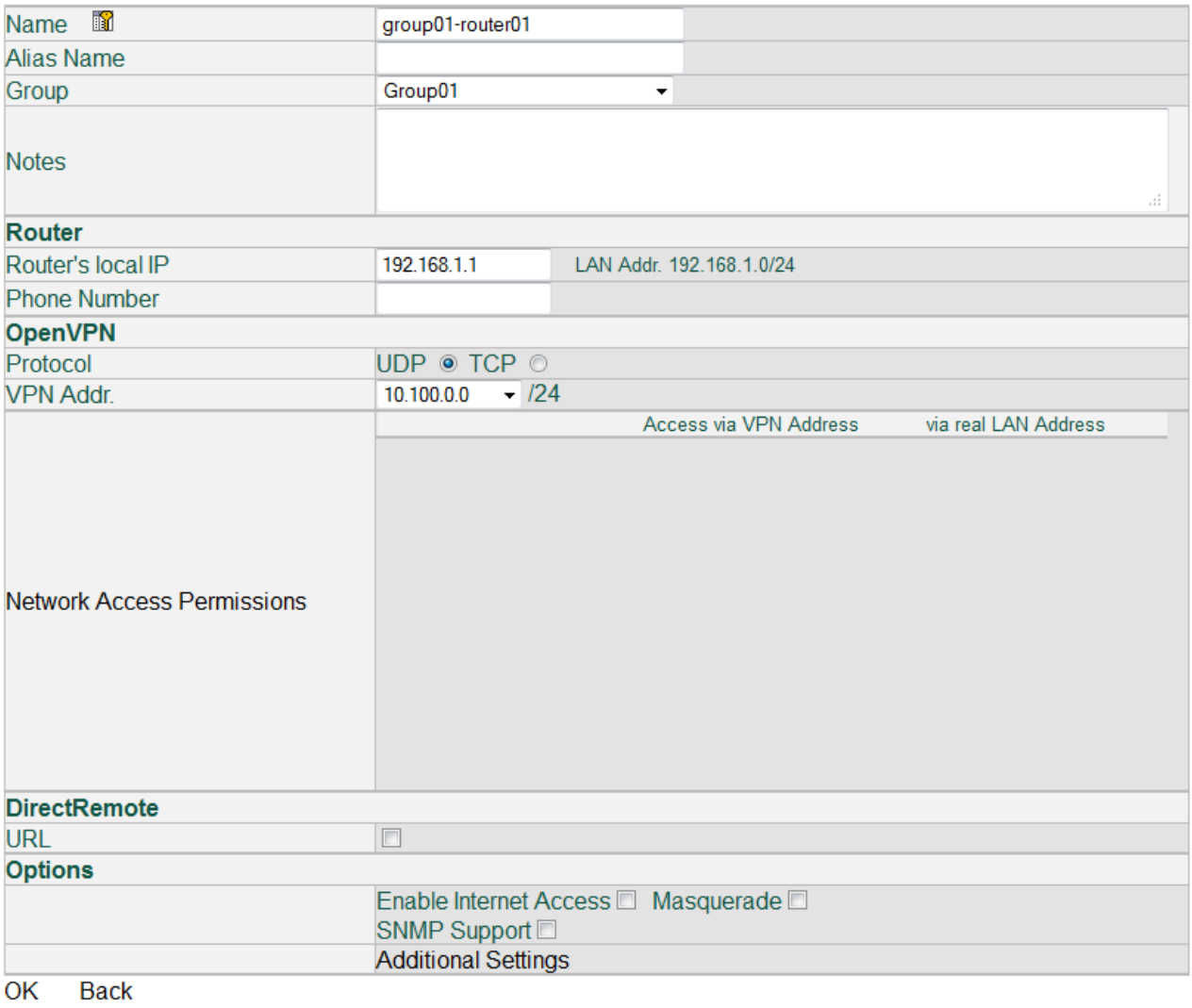


Figure 4.3: Dialogue box *Create Network*

The overview list for Networks will be displayed. This overview list is empty before initial set.

To create a new Network click on the New symbol on the right side of the first line.

Next choose the communication group you want to create a network for from the drop-down list. Click on the *OK* button.

The name of the network is not modifiable subsequently as its used for the creation of the root certificate. Use an alias name.

> Do not enter any special characters into the fields *Name* and *Alias-Name*.
> Do not use any names twice as this will overwrite any existing entry of the same name.

The input mask shows the following fields:

Table 4.2: Input mask – Network

General		
Name	Name of the Network, e.g.: *group01-router01*	**Mandatory**
	If possible choose a descriptive name, see "II, 2.2.5 Names and alias names" on Page 16.	
	Once saved do not change a network name because otherwise this will create a new network with the changed name.	
Alias Name	Subsequently modifiable name of the network (optional)	
	The alias name will be displayed in the overview list in the *Name* column	
Group	Shows previously chosen name of group.	
Created on	Date of creation – Shown after creation of the Network.	
Notes	Notes	
Router		
Router's local IP	Local IP address of router – LAN Addr. 192.168.1.0/24	
	The address range is defined by the value of <LAN Addr.>.	
	Change the local IP address only if the router has been configured accordingly.	
Phone Number	SIM card number (optional)	
OpenVPN		
Protocol	UDP or TCP	Recommendation: UDP
VPN Addr.	VPN IP address of router (suggestion)	**Mandatory**
	According to the network mask setting (default: 24 in *Settings* → *Server*) 254 different IP addresses will be displayed.	
Network Access Permissions		
	Access permissions to other network participants (local or VPN IP addresses). Permit all necessary access.	
DirectRemote		
URL	Option stays deactivated. This option is explained in "III, 5 Configuration options" on Page 57.	
Options		
Enable Internet Access	All options stay deactivated.	
Masquerade	(see also IP masquerade)	
SNMP Support	See "III, 5 Configuration options" on Page 57.	
Additional Settings	See "3.7 *Settings – Options* (Optional)" on Page 24.	
	All settings apply to this network only. These parameters (router and/or VPN configuration) are added to the global server configuration/group configuration.	

To save the settings click on the *OK* button.

A new link to the configuration file for this Network will be displayed in the input mask. The exact position of the link depends on the browser you use. Click on the link and save the file `.cfg` on your local computer.

4.5 Creating a Road warrior

In the third step of our workflow you will create a Road warrior, i.e., access for smartphones, Windows- or Linux computers, in other words (mobile) end devices.

Click on the *Road Warriors* menu item in the navigation.

The overview list for over Road warriors will be displayed. This overview list is empty before initial set up.

To create a new Road warriors click on the New symbol on the right side of the first line.

Next choose the group you want to create a Road warrior for from the drop-down list. Click on the *OK* button.

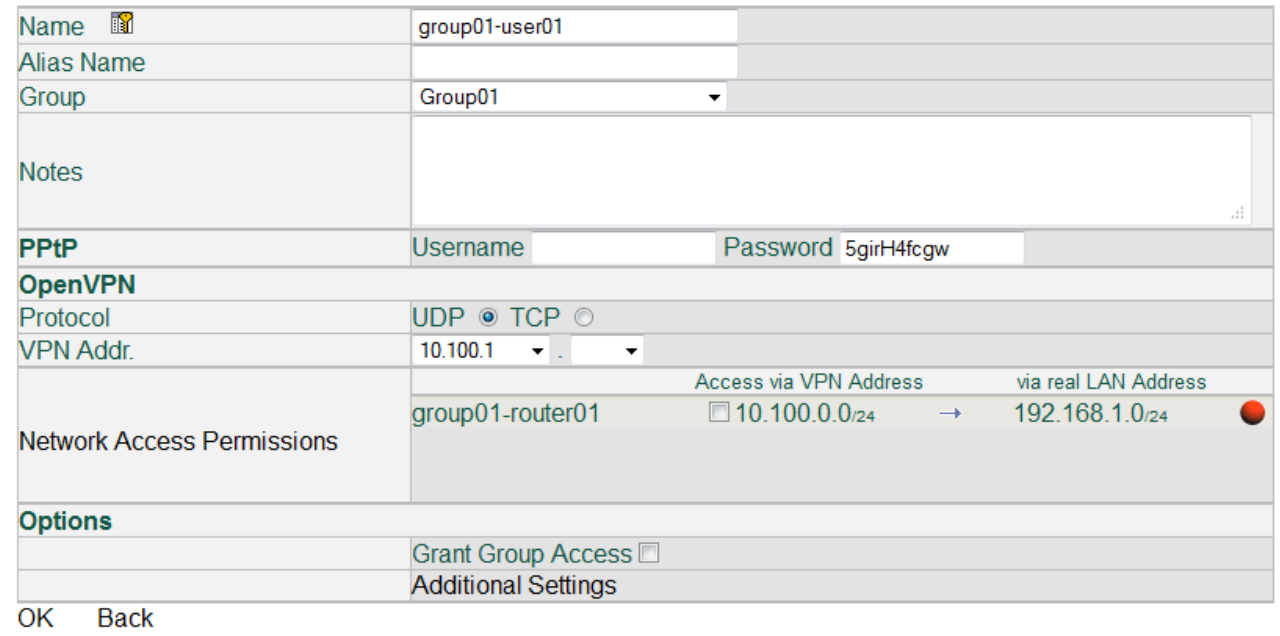


Figure 4.4: Dialogue box *Create Road warrior*

Do not enter any special characters into the fields *Name* and *Alias-Name*.
Do not use any names twice as this will overwrite any existing entry of the same name.

The input mask shows the following fields:

Table 4.3: Input mask – Road Warrior

General	
Name	Name of Road warrior, e.g.: *group01-user01* **Mandatory** If possible choose a descriptive name, see “II, 2.2.5 Names and alias names” on Page 16.
Alias Name	Subsequently modifiable name of the road warrior (optional) The alias name is displayed in the overview in the *Name* column
Group	Shows the previously chosen name of the Group.
Created on	Date of creation Shown after creation of Network.
Notes	Notes
PPtP	Settings for access via mobile phone (obsolete)
OpenVPN	
Protocol	UDP or TCP
VPN Addr.	VPN address of router Choose the first three octets from the first drop-down list, the fourth octet from the second.
Network Access Permissions	
	Access permission to other network participants (local or VPN IP address) Define the communication routes here.
Options	
Grant Group Access	Activate this option to allow communication with all other network participants of this group instead of permitting access to each single member of the group.
Additional Settings	All settings apply to this Road warrior only. These parameters (VPN configuration) are added to configuration file. Normally no additional settings are required.

To save the settings click on the *OK* button.

A new link to the configuration files for this Road warrior will be displayed in the input mask. The exact position of the link depends on the browser you use. Click on the link and save the files `<name>.zip`, `<name>.ovpn` und `openvpngui.exe` on your local computer.

4.6 Submitting access data

In the final step of our workflow you send the access data and some further instructions to the *Group administrator*.

In the navigation click on the *Groups* menu item and then on the *E-Mail* button.

The text of the E-Mail will be displayed. Click on the *Send E-Mail button to <Recipient's E-Mail Address>*. The E-Mail with the access data is sent to the *Group administrator*.

Your tasks for the initial set up up as a *SmartCluster administrator* are thus completed. Change to "III, 3.1 Receive access data" on Page 45, to manage the initial configuration of the network participants as a *Group administrator*.

5. Uses cases

In this chapter we describe use cases which are regularly carried out by a *SmartCluster administrator*.

5.1 Define communication routes

Click on the Edit symbol behind an entry to edit the settings for this network participant. 

> Use the *Network Access Permissions* settings to specify individually which other network participants can be communicated with.

In the case of the Road warrior you can use the *Grant Group Access* option to create the default setting to allow him to access all other network participants. Manual activation of access to every single network participant is thus superfluous.

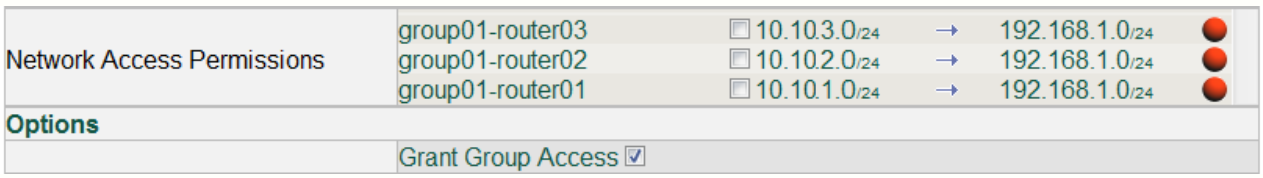


Figure 5.1: Specify communication routes

To save the settings click on the *OK* button.

To discard any changes and go back to the previous page click on the *Back* button.

5.2 Create multiple routers simultaneously

You may create several routers in one step.

Click on the *Networks* menu item in the navigation and on the New symbol in the overview list for Networks. 

Enter the name of the first router, e.g. `group01-router01` and click on the *OK* button. The *Create group* input mask stays displayed.

Now change the entry in the *Name* field for the second router, e.g. `group01-router02`. To save the settings click on the *OK* button.

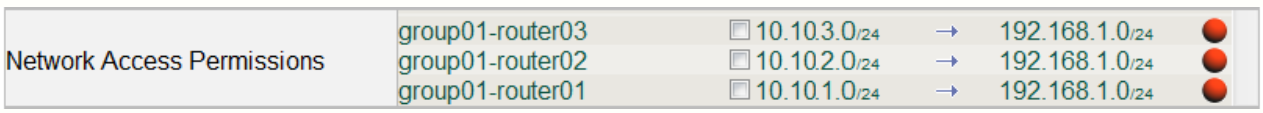


Figure 5.2: Network Access Permissions section

The second router is assigned the next free VPN IP address. The alias name is adjusted automatically. The router created previously will be display in the *Network Access Permissions* section.

Repeat the steps for all routers you want to create now. The number of routers displayed in the *Network Access Permissions* section will increase accordingly.

The routers are created but may still need individual configuration.

To discard any changes and go back to the previous page click on the *Back* button.

5.3 Delete network participants

To delete a network participant click on the Delete symbol in the overview.

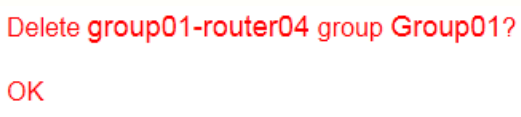


Figure 5.3: Dialogue box Confirmation – Delete

Answer the confirmation dialogue box by clicking on the *OK* button.

To cancel the action click on any entry in the navigation menu.

Deleting a network participant is done in a hierarchical way. If you delete a group all of its Networks and Road warriors will be deleted too.

> Deleting a Group or a Network does not automatically delete or deactivate the VPN configuration on the Conel mobile telephony and LAN routers. The router continues to try to establish a VPN connection to the SmartCluster but this is no longer possible. This could unintentionally result in high connection costs.

Inform the router administrator at once to change the following settings:

- Deactivate the OpenVPN tunnel on the router.
- In addition to this the value of IP address under the *Check connection to mobile network* option must be changed e.g to `8.8.8.8` and the *Ping Interval* value to `300`. (*Configuration* menu → *Mobile WAN* menu item)

5.4 Road warrior as main administrator

Generally a SmartCluster provider will use a Road warrior as main administrator for e.g. debugging.

This Road warrior may access all network participants in all groups but remains invisible for the other network participants.

Characteristics

- Create this Road warrior without any group membership, i.e., choose the entry “– – –” in the *Group* drop-down list.

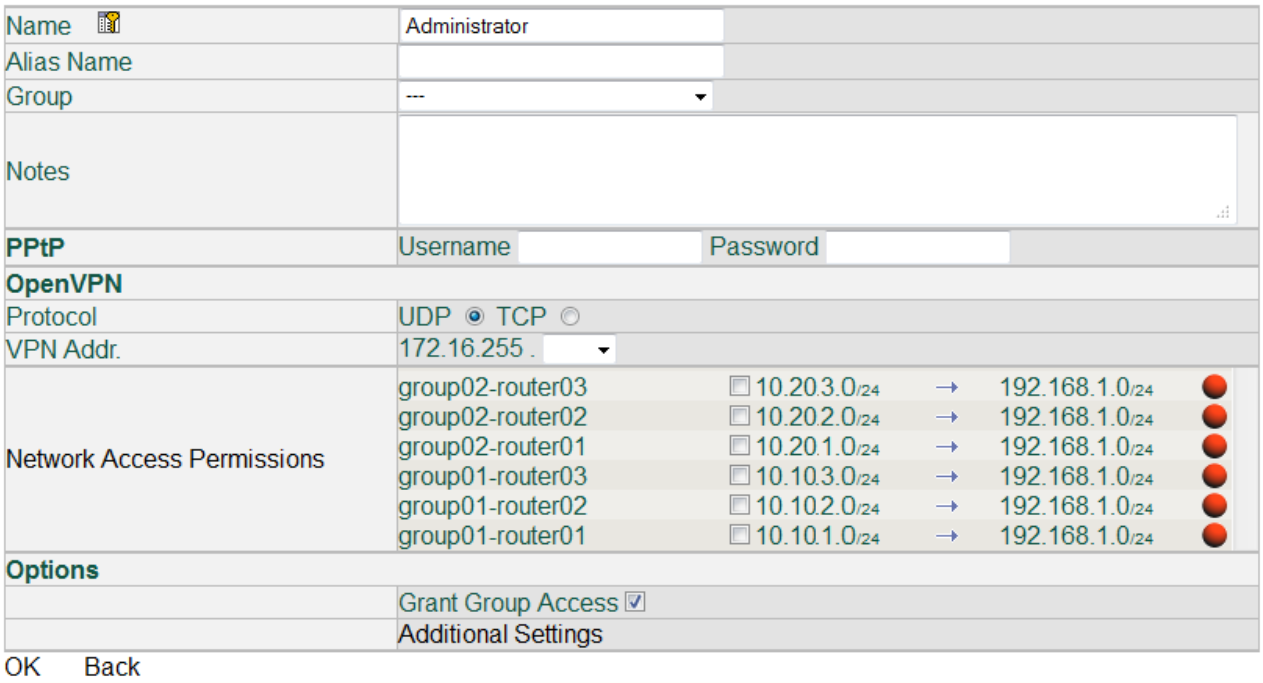


Figure 5.4: Road warrior as main administrator

Network Access Permissions

- Grant access to all other network participants: activate the *Grant Group Access* option.

5.5 Server PC for all network participants in the SmartCluster

A server PC in a SmartCluster may be used as data storage for devices such as sensors.

This server PC is a special case of Road warrior because it stays invisible but can be reached by all other network participants in a VPN network due to its fixed IP address.

- First create a Road warrior without a group membership, i.e., choose the entry “– – –” in the *Group* drop-down list.
- The fixed IP address must be reachable within the VPN network.
  So secondly choose a VPN IP address from the drop-down list, e.g.: `172.27.255.5`.

Network Access Permissions

- Activate the *Grant Group Access* option.

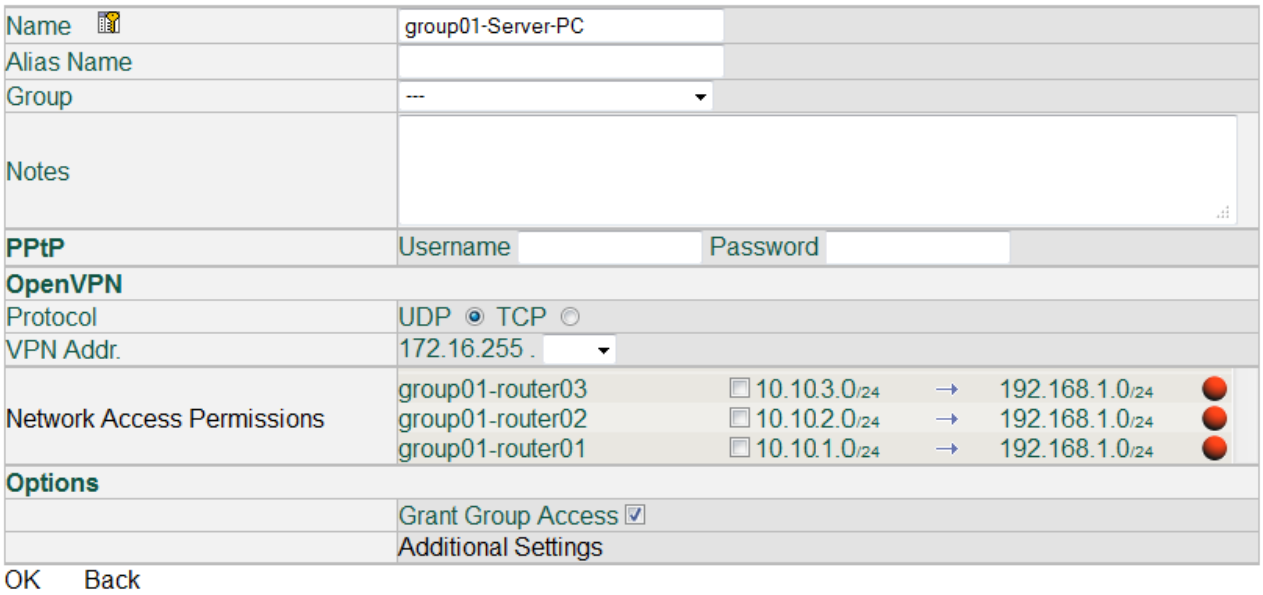


Figure 5.5: Server PC for network participant in a SmartCluster

5.6 Backup and restore

5.6.1 Backup

SmartCluster installed by Conel

All SmartClusters installed by Conel create a backup of the following items every night:

- All Groups, Networks and Road warriors created and their settings
- Database entries
- Certificates
- Configuration file
- Server settings

This requires no more settings from your side.

SmartCluster not installed by Conel

All SmartClusters not installed by Conel and also all MiniClusters do not create a backup automatically. You may initiate the creation of a backup manually.

Before you begin to create a backup you must first install a communication programme able to understand the *Secure Shell* protocol, e.g.: `Putty` or `SSH`.

Start the communication programme and connect to your SmartCluster. Log in to the command line of the SmartCluster using your user name and password.

> Contact Conel for the required password. The user name is: `root`

Starting Backup

To create a backup start the `backup.sh` script.

```
# /usr/share/phpopenvpnadmin/scripts/backup.sh
```

You will see the following output (example/shortened) in the SSH console:

```
mkdir: cannot create directory ‘/home/dcadmin/backup.old’: File exists
tar: Removing leading ‘/’ from member names
/etc/openvpn/rsa/keys/
/etc/openvpn/rsa/keys/06.pem
...
tar: Removing leading ‘/’ from member names
/usr/share/phpopenvpnadmin/scripts/__GROUP__0__CLIENT__Group01_User01_CONNECT
/usr/share/phpopenvpnadmin/scripts/__GROUP__0__CLIENT__RoadWarrior_DISCONNECT
...
/usr/share/phpopenvpnadmin/scripts/disconnect.sh
tar: Removing leading ‘/’ from member names
/usr/share/phpopenvpnadmin/ccd/__GROUP__2__CLIENT__Group01_User01
dots
/usr/share/phpopenvpnadmin/ccd/__GROUP__0__CLIENT__RoadWarrior
tar: Removing leading ‘/’ from member names
/usr/share/phpopenvpnadmin/cfg/__GROUP__0__CLIENT__Group01_User01.zip
...
/usr/share/phpopenvpnadmin/cfg/__GROUP__0__CLIENT__RoadWarrior.zip
tar: Removing leading ‘/’ from member names
/usr/share/phpopenvpnadmin/cron/crontab
/usr/share/phpopenvpnadmin/cron/.htaccess
tar: Removing leading ‘/’ from member names
/home/dcadmin/backup/cron.tar
/home/dcadmin/backup/openvpn.sql
/home/dcadmin/backup/chap-secrets
/home/dcadmin/backup/scripts.tar
/home/dcadmin/backup/cfg.tar
```

The backup archive is created in the directory `/home/dcadmin/backup.old/` and with a name according to the naming scheme `backup-<DATUM>.tar.gz`.

Example: `dc-backup-20130613.tar.gz` for the backup from 13th June 2013.

Starting the backup script several times a day will result in one archive only, as the previously created archive is overwritten, i.e., just one backup archive per day.

5.6.2 Restore

Before you begin to restore a backup on SmartCluster or MiniCluster you must first install a communication programme able to understand the *Secure Shell* protocol, e.g.: `Putty` or `SSH`.

Start the communication programme and connect to your SmartCluster. Log in to the command line of the SmartCluster using your user name and password.

> Contact Conel for the required password. The user name is: `root`

Starting Restore

To restore a backup start the `restore.sh` script. The script expects as parameter the path to the archive and the name of the archive you wish to restore (fully qualified path).

The following command consists of one line.

```
# /usr/share/phpopenvpnadmin/scripts/restore.sh ⤸
/home/dcadmin/backup.old/dc-backup-20130613.tar.gz
```

You will see the following output (example/shortened) in the SSH console:

```
Stopping web server: apache2
apache2:
    Could not reliably determine the server's fully qualified domain name,
using 127.0.1.1 for ServerName
... waiting .
Stopping virtual private network daemon: server-tcp server-udp.
home/dcadmin/backup/cron.tar
home/dcadmin/backup/openvpn.sql
...Stopping web server: apache2
apache2:
    Could not reliably determine the server's fully qualified domain name,
using 127.0.1.1 for ServerName
... waiting .
Stopping virtual private network daemon: server-tcp server-udp.
home/dcadmin/backup/cron.tar
home/dcadmin/backup/openvpn.sql
home/dcadmin/backup/cfg.tar
```

Restoring a backup requires a reboot of the SmartCluster. In the web interface click on the *Reboot* button in the lower left corner of the screen.

Alternatively you may initiate reboot of the SmartCluster via the command line. Enter the command `reboot`. The SmartCluster will reboot now.

```
# reboot
```

Part III

Group administrator

1. Tasks

A *Group administrator* manages his group and the network participants of this group. He cannot create or delete additional network participants.

We understand the term “Groups” as communication groups, clients or projects.

In principle a *SmartCluster administrator* may also manage network participants using the rights granted to him.

In this part we presume that the *SmartCluster administrator* has worked his way through all the steps listed in grey, see below. All necessary network participants (Groups, networks and Road warriors) have to be created before you start your work as *Group administrator*.

After the initial configuration we will show in “4 Workflows” on Page 55 all steps necessary to grant a Road warrior remote access to the system, see Fig. “3.1 Example of a SmartCluster network scheme” on Page 9.

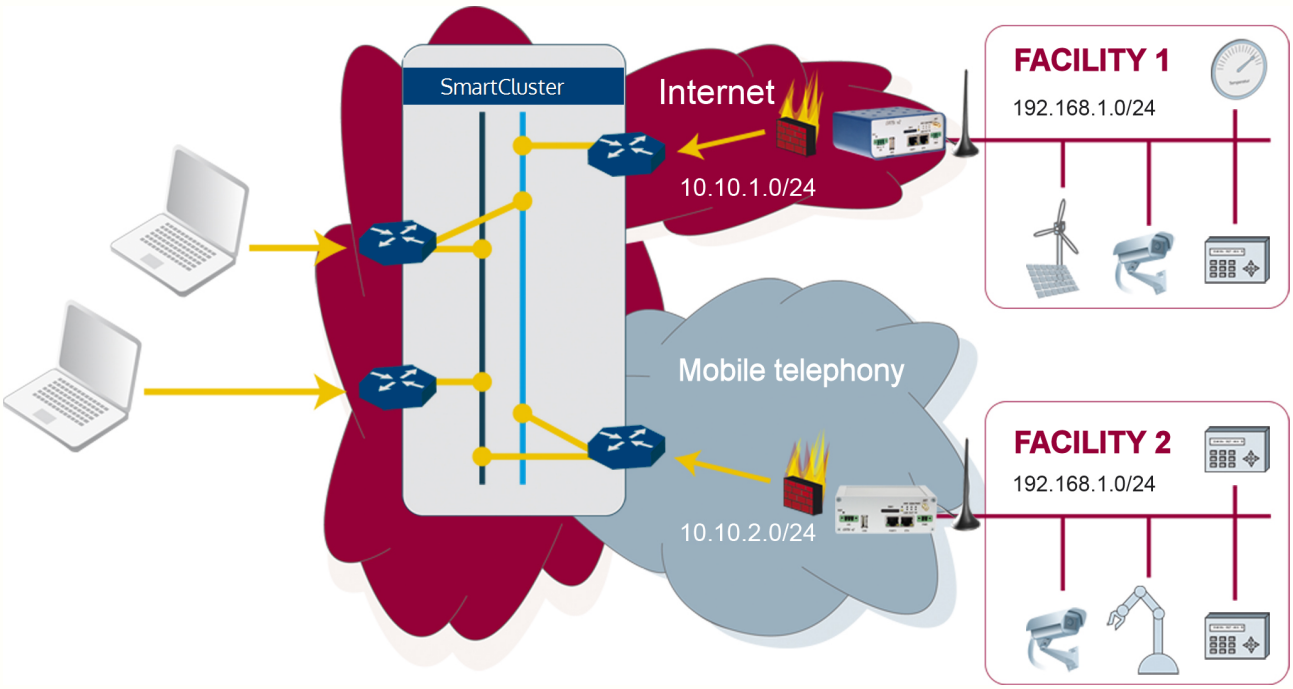


Figure 1.1: Example for a SmartCluster network scheme

- Necessary procedures as a *SmartCluster administrator*
  1. Create a Group, see “II, 4.3 Creating a Group” on Page 27
  2. Create a Network, see “II, 4.4 Creating and managing a Network” on Page 29
  3. Create a Road Warrior, see “II, 4.5 Creating a Road warrior” on Page 31
  4. Send access data, see “II, 4.6 Submitting access data” on Page 33
- Necessary procedures as a *Group administrator*
  1. Define communication routes, see “III, 3.7 Specifying communication routes” on Page 54
  2. Download configuration files for the router, see “III, 3.4 Download files” on Page 46
  3. Configure a router, see “III, 3.5 Configure the router” on Page 47

2. Graphical user interface

2.1 Start page

In this chapter we will explain the graphical user interface and its components for the *Group administrator*.

Figure 2.1: The *Group administrator* start page

At the bottom of the start page you will find contact data and the version number of your SmartCluster or MiniCluster.

On some masks you can call up the online help by clicking on the *?* button.

2.2 General functions

2.2.1 Lists

Some symbols in tables will appear only after you have created the particular participant (e.g. a group). Before the initial set up most of the symbols are not yet present.

2.2.2 Symbols in lists

Figure 2.2: Symbols in lists

You control all overview lists via the symbols on the right side of the list. Symbols in the header/footer apply for all entries. Symbols in a row apply to this particular row.

Table 2.1: Symbols and their functions

Symbol	Function
	All connections, show only online or only offline connections
	Online connections only
	Offline connections only
	Add a new entry
	Edit entry
	Display log files for entry, if available

2.2.3 Filter list entries

You can filter (larger) lists according to specific criteria.

> You can use one criterion per filter only!

Groups

In the *Groups* overview list you can filter by the fields *Group Name* and *User Name*.

Enter a value in one of the two input fields. Press the  button or click on the name of the field. The overview lists all entries according to the filter criterion.

Networks and Road warriors

In the *Networks* and *Road warriors* overview lists you can filter by the field *Name*.

Enter the name as a filter criterion. Press the  button or click on the name of the field. The overview lists all entries according to the filter criterion.

To search for a group choose the desired group name from the *Group* drop-down list. The overview is adjusted automatically.

To remove a filter, delete the entry in the field or choose the entry “– – –” in the drop-down list. The complete overview will be displayed.

2.2.4 Sort list entries

To sort a list according to column values, click on the column header. The current list sorting type will be reversed, e.g. from ascending to descending.

> You can only sort one column at a time!

2.2.5 Names and alias names

Each network participant has a name (not subsequently modifiable) and an alias name (later modifiable). If you do not enter an alias name the SmartCluster adopts the entry in the *Name* field.

- The *SmartCluster administrator* chooses and enters the names.
- The *Group administrator* cannot edit the names (insufficient rights).
- The *Group administrator* may modify the alias names.

By using aliases you can achieve a certain degree of pre-sorting of list items via dexterous naming (descriptive names, uniform spelling).

You can tell at first glance the type of network participant and the corresponding group the participant belongs to.

Naming suggestions

- Groups: Group01, Group02. etc. or name of company
- Networks: group01-router01, group01-router02, group02-router01, etc.
- Road warriors: group01-user01, group02-user01, group02-user02, etc.

3. Initial configuration

During the initial configuration you must to set up a network connection to the router. Use an Ethernet cable and connect the router to a laptop set up as a DHCP client.

The initial configuration must be performed only once. In “4 Workflows” on Page 55 you will find a description of regularly recurring activities of a *Group administrator*.

3.1 Receive access data

After the initial set up the *SmartCluster administrator* sends an E-Mail containing the access data (URL, user name and password) for the SmartCluster to the *Group administrator*. If you did not receive this E-Mail contact the *SmartCluster administrator*.

3.2 Log in page

Figure 3.1: The *Group administrator* log in page

Enter the SmartCluster IP address into the browser’s navigation toolbar. The required protocol is https.

Example: `https://<IPAddress>/vpn` – The log in page will be displayed.

If the browser issues the warning *This Connection is Untrusted*, proceed as described in "II, 3.2 Log in" on Page 17.

Enter user name and password, see E-Mail with access data or data received from *SmartCluster administrator*. Click on the *Log in* button.

3.3 Start page

The overview list of all network participants created for this group by the *SmartCluster administrator* will be displayed as start page.

Figure 3.2: The *Group administrator* Group01 start page

3.4 Download files

You need to download the following files:

1. The SmartCluster configuration file (`.cfg`) for the router;
2. The OpenVPN configuration file (`.ovpn` – Recommended procedure for Road warriors and smartphones) or alternatively
3. The OpenVPN configuration archive (`.zip` – Recommended procedure for Linux users) and, if necessary
4. The OpenVPN client for Windows (`openvpngui.exe`).

SmartCluster configuration file

Click on the Edit symbol behind the entry for a router. 

The *Group* mask will be displayed. Download the SmartCluster configuration file (`.cfg`). You need this file to configure the router.

Click on the *Back* button.

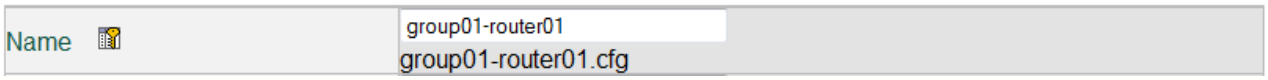


Figure 3.3: SmartCluster configuration file

OpenVPN files

Now click on the Edit symbol behind the entry for a Road warrior in the overview.

The *Road warrior* mask will be displayed. Download either the OpenVPN configuration file (`.ovpn`) or the OpenVPN configuration archive (`.zip`) and, if you use Windows as operating system, the file `openvpngui.exe`.

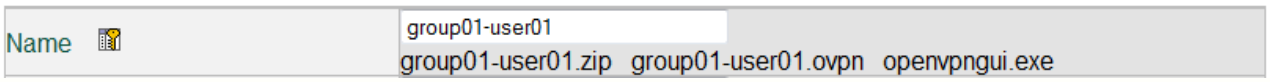


Figure 3.4: OpenVPN files

For the difference between configuration file and configuration archive, see “V, 2 OpenVPN – Configuration archive or configuration file?” on Page 70.

> For Windows computers and smartphones we recommend downloading and using the configuration file (`.ovpn`) as it is easier to handle.
> For Linux users we recommend downloading the configuration archive (`.zip`).

3.5 Configure the router

The configuration of a router requires the following steps:

1. Log in on the router.
2. Load the SmartCluster configuration file on the router.
3. Reboot the router.

3.5.1 Log in

Enter the router’s IP address into the browser’s navigation toolbar. The required protocol is http or https.

Example: `http://192.168.1.1`

The *Authentication required* dialogue box is displayed.

In the *User Name:* field enter `root` as user name, in the *Password:* field again `root` as password. Click on the *OK* button.

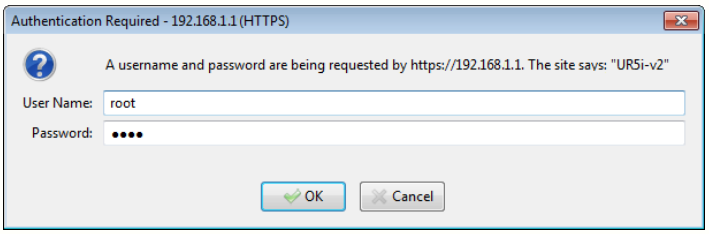


Figure 3.5: Dialogue box *Authentication required*

Change the password for the user *root* (on the router) now!

In the navigation column click on the *Change Password* menu item in the *Administration* section, see Fig.3.6, red entry.

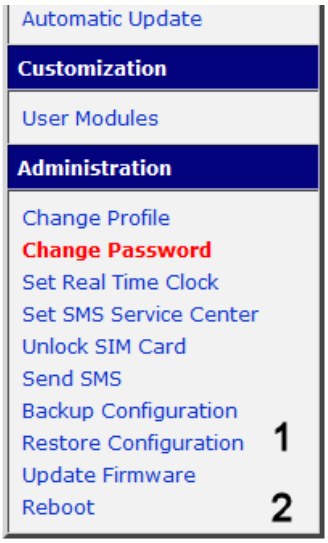


Figure 3.6: Navigation column (lower part)

Enter the new password both in the *New Password* field and in the *Confirm Password* field. Save the changes by clicking on the *Apply* button.

The *Change Password* message indicates that the password was changed successfully. Click on the *Back* button.

Log in as user *root* with the **new** password.

3.5.2 Load the SmartCluster configuration file on the router

Click on the *Restore Configuration* menu item (Mark **1**) in the *Administration* section in the navigation column, see fig. 3.6.

Click on the *Browse* button and select the configuration file (`.cfg`) for this router (see above). Click on the *Open* button.

The name of the file selected will be displayed. Click on the *Apply* button to load the new configuration into the router.

Once the configuration is restore, a corresponding message will be displayed.

A reboot of the rooter is necessary to start the new configuration. You can initiate a reboot by clicking on the *Reboot* button in the message or by proceeding as described below.

3.5.3 Reboot the router

A reboot of the router is necessary to make the router use the new configuration. To do so, go to the *Reboot* menu item (mark **2**) in the *Administration* section, see Fig. "3.6 Navigation column (lower part)" on Page 48. Click on the *Reboot* button.

The reboot of the router takes some seconds. Following this the router start page will be reloaded. Alternatively click on the *Reload now* button.

The re-establishing of the mobile and VPN connections also takes some seconds.

After approximately one minute you can click on the *Status* menu item in the *Network* section of the navigation. The overview list for all different connection types will be shown, see Fig. "3.5.3 Reboot the router" on Page 49.

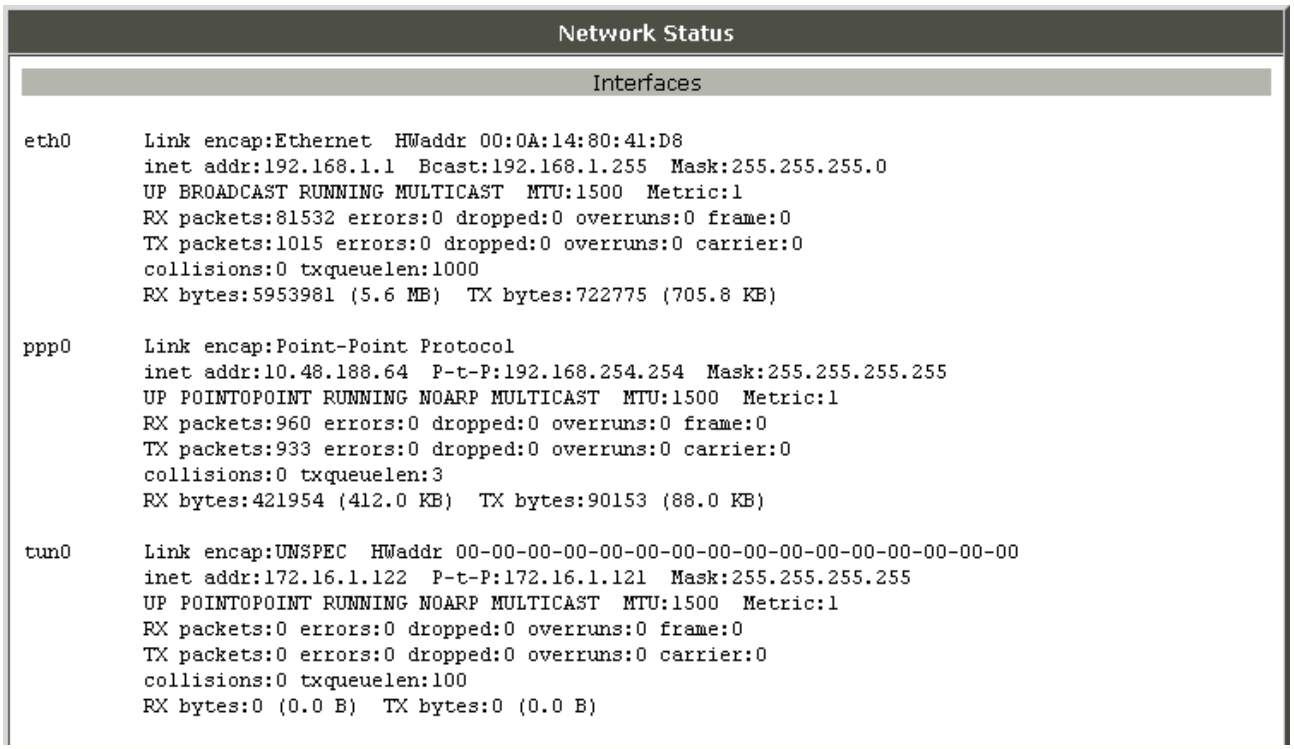


Figure 3.7: The router's network status

eth0: Status of Ethernet connections

ppp0/usb0: Status of mobile telephony connections

tun0: Status of OpenVPN tunnel
This entry will be displayed only after the OpenVPN tunnel to the SmartCluster has been successfully established.

Successful establishment of an OpenVPN tunnel can be checked in three places:

1. On the router: display of network status (router start page).
2. On the SmartCluster as *SmartCluster administrator*: overview list of network participants.
3. On the SmartCluster as *Group administrator*: overview list of network participants.

In the overview lists of the SmartCluster the display of the connection symbol for the router changes from red to green.

3.6 Installing an OpenVPN client

Before setting up the OpenVPN connection on the computer install a OpenVPN client convenient for the operating system.

3.6.1 OpenVPN – Linux

We will show the configuration of an OpenVPN client under Linux based on Ubuntu distribution. Other Linux distributions behave similarly.

Install the OpenVPN extension `network-manager-ovpn` and `network-manager-openvpn-gnome` for the Gnome Network Manager.

Extract the OpenVPN configuration archive (`.zip`) into a directory, e.g.: `tmp/`.

In the *Network Manager* menu click on the *VPN Connections* menu item and choose the *Configure VPN* submenu item. The dialogue box *Network connections* will be displayed. Click on the *Import* button.

In the *Choose file for import* dialogue box choose and mark the file `.ovpn` from the archive extracted. Click on the *Open* button.

In the dialogue box *Edit <Name of Connection>* the fields show the prepared data. Click on the *Save...* button.

In the dialogue box *Network connections* a new entry will appear in the *VPN* section. Click on the *Close* button to end the dialogue.

This completes installation and configuration of OpenVPN on a Linux computer.

3.6.2 OpenVPN – Windows

The installation of the OpenVPN client requires administrator rights. Start the installation of the file `openvpngui.exe`. A *setup wizard* will guide you through the installation process.

Notes

1. Remove previously installed versions of the OpenVPN client, because installing the new version over an existing one may cause unforeseen difficulties in setting up the VPN tunnel.
2. The installation of the OpenVPN client under Windows 7 requires administrator rights. Open the context menu of `openvpngui.exe` by clicking the right mouse button. Choose the *Execute as Administrator* menu item.
3. Accept all defaults during the installation.
4. After the installation of the clients copy the SmartCluster OpenVPN configuration file `.ovpn` into the `config` subdirectory in the directory you installed the OpenVPN client to.

Installing the OpenVPN client on a Windows PC

Open the folder where you stored the file `openvpngui.exe` and start the OpenVPN Setup Wizard which will guide you through the installation process.

Figure 3.8: OpenVPN Setup – Step 1

Click on the *Next* button.

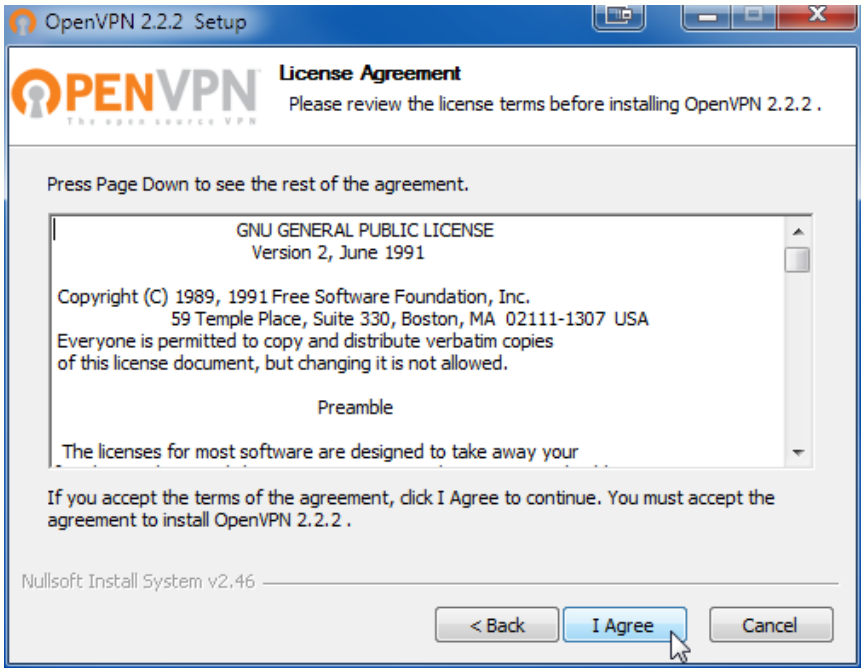


Figure 3.9: OpenVPN Setup – Step 2

Accept the license agreement by clicking on the *I Agree* button.

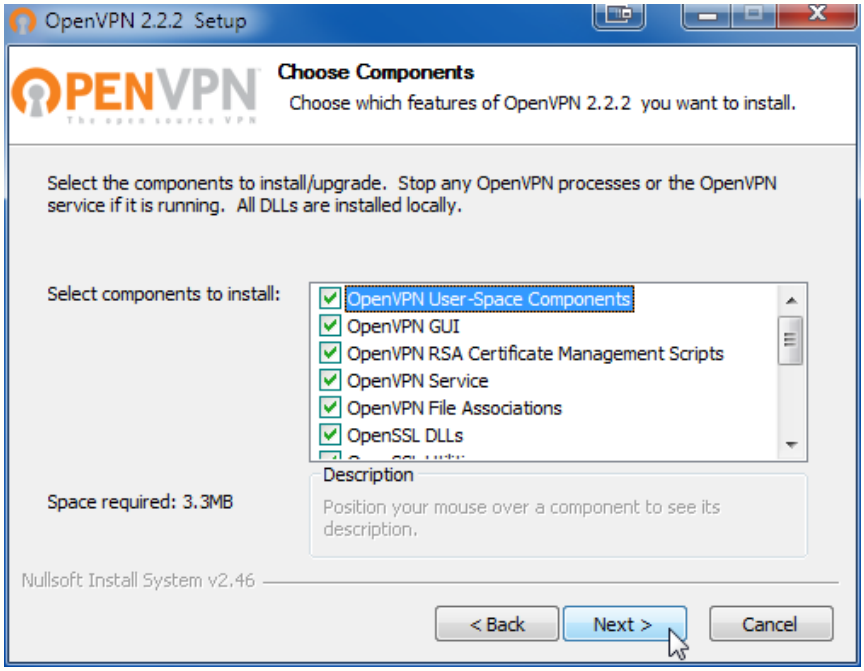


Figure 3.10: OpenVPN Setup – Step 3

Choose the components to install. It is best to take accept the suggested components.

Click on the *Next* button.

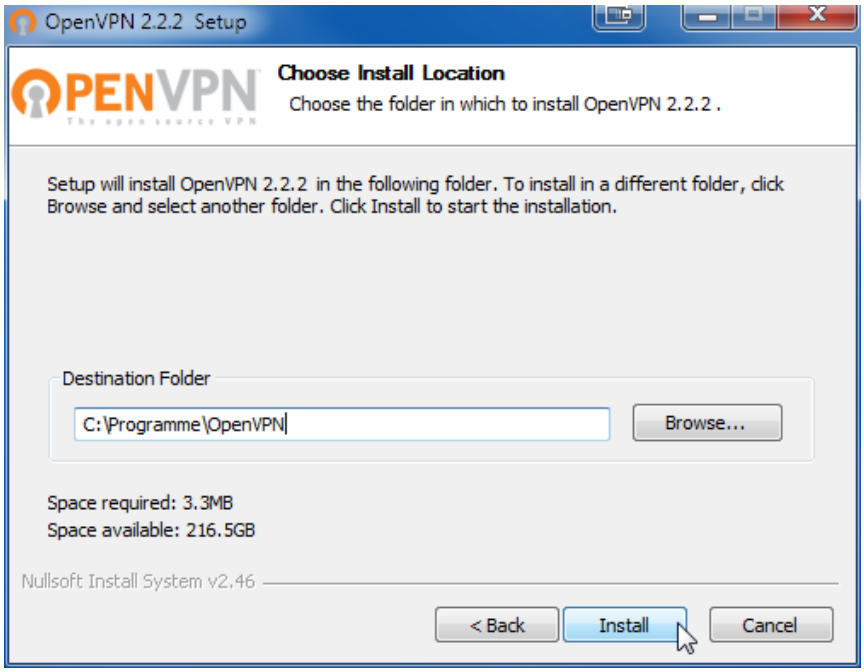


Figure 3.11: OpenVPN Setup – Step 4

Accept the suggested target directory or enter a new directory by clicking on the *Browse* button.

Click on the *Install* button to start the installation.

After the installation of the client copy the SmartCluster OpenVPN configuration file `.ovpn` into the `config` subdirectory in the directory you installed the OpenVPN client to.

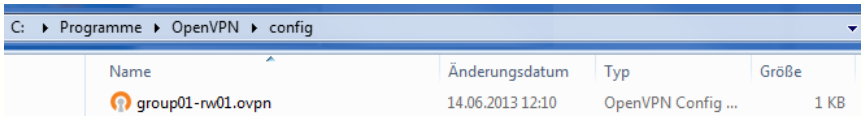


Figure 3.12: OpenVPN – Save configuration file `.ovpn`

This completes installation and configuration of OpenVPN on a Windows computer.

3.7 Specifying communication routes

The overview list for the network participants created by the *SmartCluster administrator* will be displayed on the start page.

Name ?	group	VPN Addr.	LAN Addr.			
group01-router01	Group01	10.10.1.0/24	192.168.1.0/24			
group01-router02	Group01	10.10.2.0/24	192.168.1.0/24			
group01-router03	Group01	10.10.3.0/24	192.168.1.0/24			
group01-user01	Group01					

Figure 3.13: Overview list of network participants

Click on the Edit symbol behind an entry to edit the settings for this network participant.

Use the *Network Access Permissions* settings to specify individually which other network participants can be communicated with.

In the case of the Road warrior you can use the *Grant Group Access* option to create the default setting to allow him to access all other network participants. Manual activation of access to every single network participant is thus superfluous.

Network Access Permissions	group01-router03	10.10.3.0/24	→	192.168.1.0/24
	group01-router02	10.10.2.0/24	→	192.168.1.0/24
	group01-router01	10.10.1.0/24	→	192.168.1.0/24
Options				
	Grant Group Access ☑			

Figure 3.14: Specify communication routes

To save the settings click on the *OK* button.

To discard any changes and go back to the previous page click on the *Back* button.

For a detailed description of the configuration options, see “5 Configuration options” on Page 57.

3.8 Ending the initial configuration

This completes the initial configuration by the *Group administrator*. Proceed to “4.4 Using VPN connections” on Page 56.

4. Workflows

In this chapter we describe recurring workflows for the *Group administrator*.

4.1 Log in

Enter the SmartCluster IP address into the browser's navigation toolbar of the browser. The required protocol is https.

Example: `https://<IPAddress>/vpn`

- User name from the access data E-Mail or from *SmartCluster administrator*
- Password

If the browser issues the warning *This Connection is Untrusted*, proceed as described in "II, 3.2 Log in" on Page 17.

Enter the user name and password (see E-Mail with access data or data received from the *SmartCluster administrator*. Click on the *Log in* button.

The start page of your SmartCluster will be displayed, see Fig. "2.1 The *Group administrator* start page" on Page 42.

4.2 Managing Networks

Click on the Edit symbol behind a network entry in the overview list of the network participants. 

The *Network* input mask will be displayed. To change/add the data, see "II, 4.4 Creating and managing a Network" on Page 29.

To save the settings click on the *OK* button.

Click on the *Back* button to display the overview page.

To discard any changes and go back to the previous page click on the *Back* button.

4.3 Managing Road warriors

Click on the Edit symbol behind a Road warrior entry in overview over the network participants. 

The *Road warrior* input mask will be displayed. To change/add the data, see "II, 4.5 Creating a Road warrior" on Page 31.

To save the settings click on the *OK* button.Click on the *Back* button to display the overview page.

To discard any changes and go back to the previous page click on the *Back* button.

4.4 Using VPN connections

4.4.1 Windows

Using Windows start the OpenVPN client as administrator.

Click the right mouse button on the entry `openvpn-gui.exe` to open the context menu of the OpenVPN client. Choose the *Connect* menu item. The VPN tunnel will be established. You can now connect to the remote network participant.

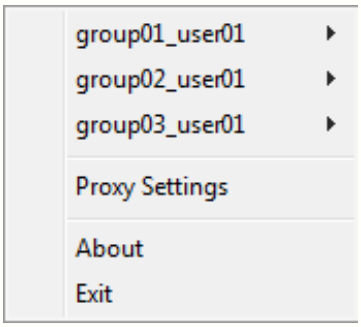


Figure 4.1: OpenVPN – Context menu

Should you use different VPN tunnels, choose the desired network participant in the context menu first then click on the *Connect* menu item. The VPN tunnel will be established. You can now connect to the remote network participant.

Red monitors	=	The system is not connected to the SmartCluster yet.
Yellow monitors	=	The OpenVPN client is trying to establish a connection.
Green monitors	=	The connection to the SmartCluster has been established.

Table 4.1: OpenVPN – Status

4.4.2 Linux

We will show the use of an OpenVPN tunnel under Linux based on Ubuntu distribution. Other Linux distributions behave similarly.

In the Network Manager click on the *VPN Connections* menu item. Choose the desired tunnel. The VPN connection is established.

A successful connection of a VPN tunnel is symbolised in the Network Manager by a little lock.

5. Configuration options

In this chapter we describe the optional configuration parameters for Networks (routers) and Road warriors which were not addressed up to now.

5.1 Network (router) options

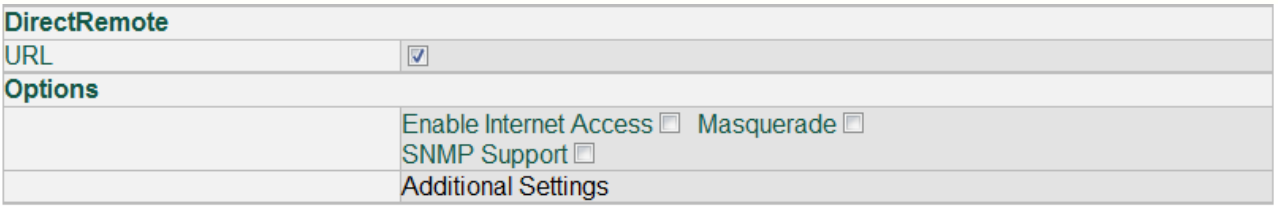


Figure 5.1: Optional configuration parameters

5.1.1 Direct Remote

Via DirectRemote you may grant direct access to the web interface of the router or a web server in the router's LAN via a VPN tunnel without the need to start a VPN client.

The URL can be used manifold as long at it is not deactivated. You can send the URL to an authorised user, who cannot access the web server otherwise via E-Mail.

Activate URL

Activated the *URL* option and click on the *OK* button. The URL for the direct access to the web server behind the router will be displayed.

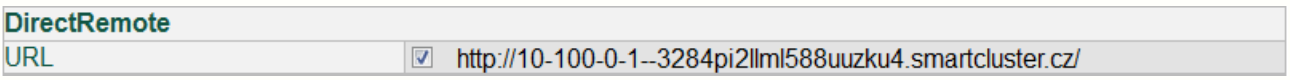


Figure 5.2: Direct Remote URL

Deactivate URL

Deactivate the *URL* option and click on the *OK* button. The URL will no longer displayed. New connection using the deactivated URL are no longer possible.

Create a new URL

Creating a new URL automatically creates a new password. The old password becomes invalid.

URL structure

The URL consists of the following parts:

- Internet protocol: `http://` or `https://`
- VPN IP address using **-** instead of **.** for separating the octets: `10-10-1-1`
- 2 dividers: `-{}-`
  The port number is expected between the dividers. Default is `-{}-` corresponding to Port 80.
- Randomly generated password with 20 digits: `<password>`
- VPN domain: `.dyndns.de`

The last octet **1** in the IP address corresponds to the Conel-Router. To connect to a web service on another device behind the router change the IP address as per 1:1 NAT.

5.1.2 Enable Internet Access

By default devices connecting to the router may communicate via VPN only. To allow data communication to the Internet via the router, activate the *Enable Internet Access* option. To save the settings click on the *OK* button.Click on the *Back* button to display the overview page.

Afterwards transfer the new configuration onto the router and restart the router, see “3.5.2 Load the SmartCluster configuration file on the router” on Page 48 and “3.5.3 Reboot the router” on Page 49.

5.1.3 Masquerade

IP masquerade becomes necessary for network devices which should be accessed via the VPN router but cannot be configured for a default gateway (no possibility or default gateway already configured for another LAN).

Activate the *Masquerade* option to access this device via SmartCluster and VPN router despite this.

Afterwards transfer the new configuration onto the router and restart the router, see “3.5.2 Load the SmartCluster configuration file on the router” on Page 48 and “3.5.3 Reboot the router” on Page 49.

5.1.4 SNMP Support

Activate the *SNMP Support* option if the router itself, not the devices connected, should be monitored via SNMP.

Afterwards transfer the new configuration onto the router and restart the router, see “3.5.2 Load the SmartCluster configuration file on the router” on Page 48 and “3.5.3 Reboot the router” on Page 49.

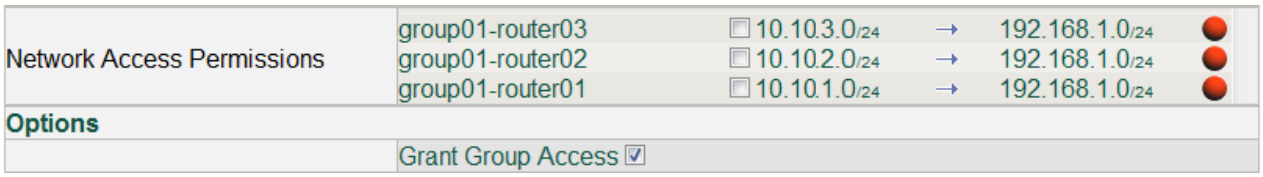


Figure 5.3: Network Access Permissions or Grant Group Access

5.2 Road warrior options

5.2.1 Grant Group Access (Road warrior)

The *Grant Group Accees* option is like setting permissions collectively for all network participants instead of granting access rights on an individual basis.

Activating the option grants the Road warrior access to all network participants of its group currently created or in future. Access is granted to VPN IP addresses not to real IP addresses.

6. Use cases

6.1 Setting up access for smartphones

To access the SmartCluster via smartphone we recommend downloading and using the configuration file (`.ovpn`) for setting up OpenVPN on a smartphone as this file is created especially for this Road warrior.

For more information about the settings for the access via VPN on smartphones with different operating systems, see “V, 3 Which settings for my smartphone?” on Page 71.

6.2 Terminating connections

To terminate an active connection (Network or Road warrior) click as *Group administrator* on the green bullet behind the desired connection.

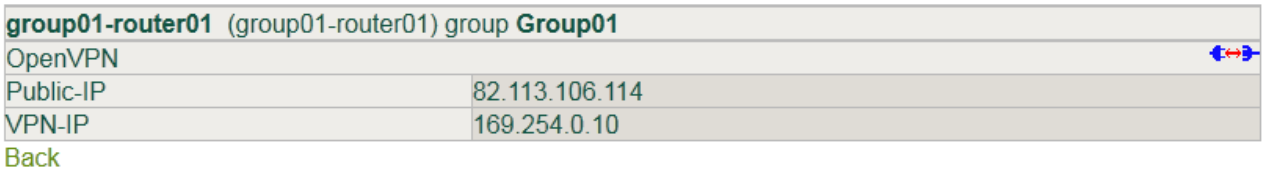


Figure 6.1: Terminate active connection (Network)

Click on the Disconnect symbol. The connection terminates and is marked with a red bullet.

The connection is re-established as the router or the VPN client on the device recognises the interruption.

6.3 Editing configurations

Changing the router configuration in the SmartCluster requires making the changes known to the router. In the majority of cases a reboot is required also, see “V, 12 Reconfiguration of router necessary?” on Page 73.

In the SmartCluster switch as *Group administrator* to the network participants overview created by the *SmartCluster administrator*.

Click on the Edit symbol behind the router entry.

The *Group* mask will be displayed. Download the SmartCluster configuration file (`.cfg`).

To change the configuration on the router log in as user *root* on the router.

Click on the *Restore Configuration* menu item (Mark**1**) in the *Administration* section of the navigation column, see Fig. “6.2 Navigation column of router (lower part)” on Page 61.

Click on the *Browse* button and choose the configuration file (`.cfg`) for this router (previously saved, see above). Click on the *Open* button.

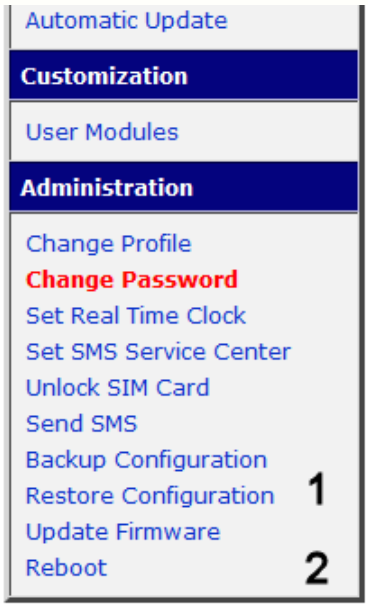


Figure 6.2: Navigation column of router (lower part)

The name of the file chosen will be displayed. Click on the *Apply* button to load the new configuration.

Once the restore has been finished the router displays a message.

A reboot of the router is necessary to make the router use the new configuration. To do so, go to the *Reboot* menu item (mark **2**) in the *Administration* section, see Fig. "3.6 Navigation column (lower part)" on Page 48. Click on the *Reboot* button.

The reboot of the router takes some seconds. Following this the router start page will be reloaded. Alternatively click on the *Reload now* button.

The re-establishing of the mobile and VPN connections also takes some seconds.

After approximately one minute you can click on the *Status* menu item in the *Network* section of the navigation. The overview list for all different connection types will be shown, see Fig. "3.5.3 Reboot the router" on Page 49.

After the reboot of the router all VPN connections need to be re-established manually where this does not happen automatically.

6.4 Road warrior as *Group administrator*

This Road warrior may access all network participants in its group but remains invisible for the other network participants.

Characteristics

- Create this Road warrior with group membership, i.e., choose the entry of the desired group in the *Group* drop-down list.

Network Access Permissions

- Grant access to all network participants of its group: activate the *Grant Group Access* option.

6.5 Server PC for all network participants of a group

A server PC in a SmartCluster may be used as data storage for devices such as sensors.

This server PC is a special case of Road warrior because it can be reached by all other network participants of its group due to its fixed IP address.

- First choose a Road warrior with a Group.
- The fixed IP address must be reachable within the VPN network.
  So secondly in the first drop-down list choose the first three octets of the VPN IP address, e.g.: `10.1.0`.
- In the second drop-down list choose the fourth octet, e.g.: `1`.

Network Access Permissions

- Activate the *Grant Group Access* option.
- For each network participant grant access to the server PC's VPN IP address.

6.6 Road warrior has access to two routers

This Road warrior has access to two LANs with an identical configuration via VPN IP addresses, i.e. both LANs use the same local IP addresses.

- Two LANs with identical configuration
- But different SmartCluster VPN IP addresses

Network Access Permissions

Grant access to

- Router 1
- Router 2

6.7 Router to router connection

Both networks can be connected. Control 1 may access Control 2 via Router 1 and Router 2. Generally this is not possible due to the same local IP addresses.

- Two LANs with identical configuration
- But different SmartCluster VPN IP addresses

Network Access Permissions

- For Router 1 grant access to Router 2
- For Router 2 grant access to Router 1

Click on the Edit symbol in the line for the first router (Router 1) in the overview list for the Networks.

In the *Network Access Permissions* section grant the access to Router 2. To save the settings click on the *OK* button.

Click on the Edit symbol in the line for the second router (Router 2).

In the *Network Access Permissions* section grant the access to Router 1. To save the settings click on the *OK* button.

Part IV

Excursion MiniCluster

1. Differences to SmartCluster

This chapter explains the differences between MiniCluster and SmartCluster.

1.1 Number of access points

The number of access points for MiniCluster is restricted to 100 Networks (routers) and 100 Road warriors (computer/smartphones).

1.2 Logging in

To log in as MiniCluster administrator enter the MiniCluster's IP address into the browser's navigation toolbar. The required protocol is https.

Example: `https://192.168.1.200/vpnadmin`

- User name: `admin`
- Password: `admin`

1.3 Backup and restore

1.3.1 Backup

MiniCluster does not create backups automatically as SmartCluster, if installed by Conel, does. You can initiate the creation of backups manually, see "II, 5.6.1 Backup" on Page 37.

1.3.2 Restore

To restore a backup proceed as described in "II, 5.6.2 Restore" on Page 39.

1.4 Shutdown server

As a *Minicluster administrator* you will find an additional red button for initiating the shutdown of the MiniCluster server at the foot of each page.

Shutting down of the MiniCluster instead of just switching off is necessary because MiniClusters are based on an embedded PC running Linux as operating system.

1.5 Additional fields

The MiniCluster is normally operated in the data center of the operator and not in the cloud. You configure all necessary network settings in the additional fields as *Minicluster administrator*.

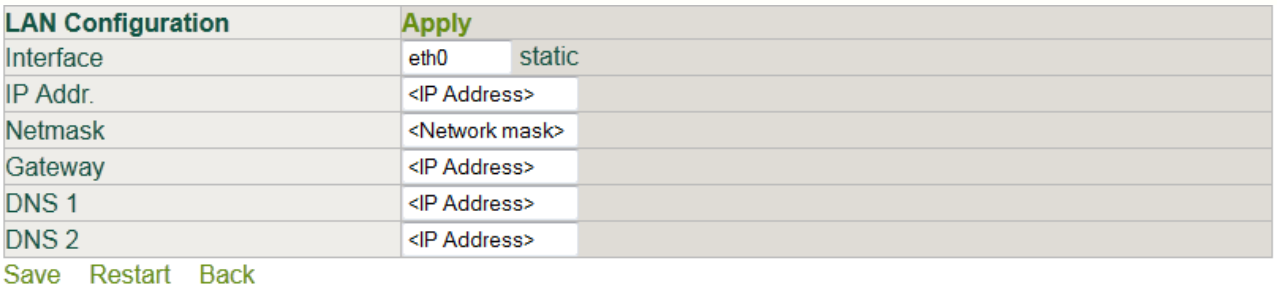


Figure 1.1: Server input mask – Additional fields for Minicluster

On the *Settings* input mask → *Server* (see "II, 3.4 *Settings – Server*" on Page 20) additional fields are shown.

Table 1.1: Settings – Server: Additional fields

LAN Configuration	*Apply* button / LAN and interface configuration for VPN server
Interface	Network interface – Default: eth0 *static*
IP Addr.	Server IP address
Netmask	Server network mask – Default: 255.255.255.0
Gateway	Gateway IP address
DNS 1	DNS server IP address
DNS 2	Additional DNS server IP address (optional)

Save settings

To save the settings click on the *Save* button.

Apply settings immediately

To save and apply changes in the network settings click on the *Save* and *Apply* buttons.

Restart OpenVPN

To restart the OpenVPN service click on the *Restart* button. Save any changes beforehand.

Restart Minicluster

To initiate a reboot click on the *Reboot* button.

Discard changes

To discard any changes and go back to the previous page click on the *Back* button.

2. Workflows

2.1 Connection via serial interface

If you cannot access your MiniCluster via the Ethernet network interface, e.g. because of failed configuration, you can use its serial interface to restore a working configuration.

You need:

- Either a serial cable (RS-232) and a serial interface on your computer
- Or an adapter cable USB-to-serial and an USB interface on your computer
- And a terminal software, suitable for the operating system of your computer

2.1.1 Procedure

Once you connect the USB cable to the USB interface Windows will automatically install the appropriate device drivers and display a dialogue box stating which port number has been used, e.g. COM5.

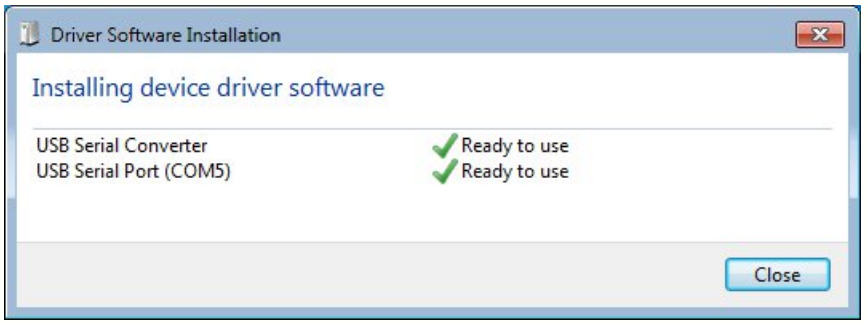
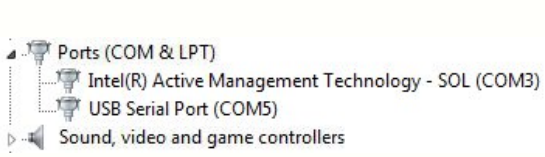
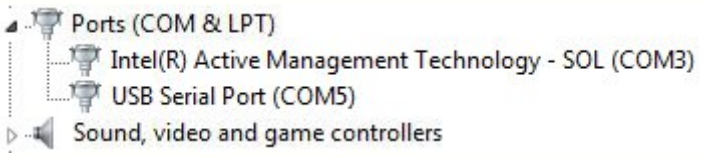


Figure 2.1: Device installation

Alternatively use the Windows Device manager to find out which COM port is used.



COM1: Default COM port



COM5: COM Port of USB adapter

Figure 2.2: Device manager

Connect the MiniCluster and your computer with the one of the cables mentioned. Start the terminal software and configure these settings:

Interface: <COMx>	Speed: 9600 baud	Data bits: 8	Parity: None	Stop bits: 1

That's all! No more settings needed.

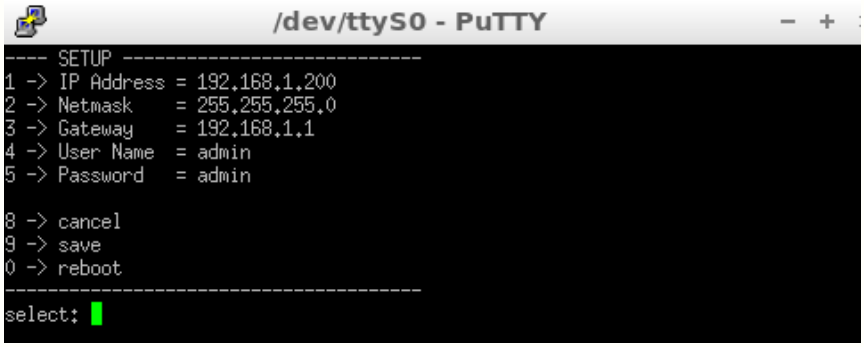


Figure 2.3: Terminal software – Start screen (Linux version)

2.1.2 Operation

To change a value choose the number in front of the value. Confirm the input by pressing the ↵ key.

Table 2.2: Terminal software operation

#	Text	Function	#	Text	Function
1	IP Address	Change IP address	5	Password	Change password
2	Netmask	Change netmask	8	cancel	Cancel
3	Gateway	Change gateway	9	save	Save settings
4	User Name	Change user name	0	reboot	Reboot MiniCluster

Part V

FAQ

1. Why is my VPN connection not stable?

We recommend using UDP as the default protocol for VPN. For some applications and especially the Conel LAN router TCP has proven to be better as default protocol for more stable VPN tunnels and less data overheads. Unfortunately no global recommendation can be given.

Change the protocol if necessary to TCP, see “II, 3.4 *Settings – Server*” on Page 20.

2. OpenVPN – Configuration archive or configuration file?

For configuration of a Road warrior device (computer) you can either use the OpenVPN configuration file `.ovpn` or the OpenVPN configuration archive `.zip` since both have the same content.

> We recommend using of the OpenVPN configuration file `.ovpn`.

The advantage of the OpenVPN configuration file is that all necessary data (including certificate and keys) are stored in a single file. This file can be processed by most of the VPN clients offered by different operating systems or device classes with any problem.

> Take care not to overwrite the OpenVPN configuration file (`.ovpn`) with the file with the same name from the configuration archive. The file from the configuration archive contains less data because the rest in distributed in the archive’s other files.

Mobile Road warriors simply log in on the SmartCluster from their smartphone and download the especially created OpenVPN configuration file (`.ovpn`). After that everything will run automatically up to the connection to the SmartCluster. Generally the device will store the settings for the VPN connection for later use.

> We recommend that Linux users use the configuration archive (`.zip`) and the configuration files contained therein.

3. Which settings for my smartphone?

Conel cannot give any guarantees for the following descriptions. Please refer to the manual of your smartphone for the setup of VPN.

3.1 Android

Import the Road warrior's OpenVPN configuration file (`.ovpn`) into your Android smartphone's the VPN manager. The VPN manager detects and configures the necessary settings automatically.

You may now access every IP address in the SmartCluster for which access was granted.

3.2 BlackBerry

Set up your BlackBerry smartphone as follows:

Settings

- Create a VPN profile
  - Expand Policy > Wi-Fi configuration on the BlackBerry solution management menu in the BlackBerry Administration Service.
  - Click on Create VPN profile.
  - Type a name for the VPN profile into the Name field.
  - Click on Save.
- Configure a VPN profile
  - Expand Policy > Wi-Fi configuration on the BlackBerry solution management menu in the BlackBerry Administration Service.
  - Click on Manage VPN profiles.
  - Click on the name of the VPN profile.
  - Click on Edit profile.
  - Change the values for the configuration settings on the VPN profile settings tab.
  - Click on Save All.

3.3 iPhone/iOS

Import the Road Warrior's OpenVPN configuration file (`.ovpn`) into the iPhone's VPN manager. The VPN manager detects and configures the necessary settings automatically.

You may now access every IP address in the SmartCluster for which access was granted.

3.4 Windows Phone 7/8

Contact your mobile phone manufacturer’s support service.

4. What does “*It works*” in my browser mean?

This messages indicates that the SmartCluster has been started successfully. The address (URL) used in the web browser is, however, not quite valid. Check whether

- You used the right protocol (`https`).
- You enter the address completely. The address for
  - the *SmartCluster administrator* start page is: `https://<IP-Adresse>/vpnadmin/`
  - the *Group administrator* start page is: `https://<IP-Adresse>/vpn/`

5. Why should I change the default passwords?

You should change the default passwords so that only authorised users have access to the management pages. Default passwords are easy to crack or commonly known. Server security can easily be compromised.

6. How many access points can I use?

Generally the number of VPN access points in unlimited. However, experience shows that it makes sense to create a new instance of SmartCluster after approx. 1.000 access points for Networks and Road warriors.

7. Why do I have to shut down the MiniCluster?

Shutting down the MiniCluster instead of just switching off is necessary because MiniClusters are based on an embedded PC with Linux as operating system.

8. Can I transfer a configuration?

Yes, you can transfer a configuration from one SmartCluster to another SmartCluster. Proceed as described in “II, 5.6.2 Restore” on Page 39.

9. Can I set up a replacement VPN service portal?

Yes, you can. Restoring a different instance of the MiniCluster creates a VPN service portal with the same values and settings as the first portal. The second MiniCluster can thus serve as a replacement VPN service portal.

10. How do I establish VPN connections?

Proceed as described in “III, 4.4 Using VPN connections” on Page 56.

11. Special case: Remote service for Siemens controls

The LAN IP addresses in the remote LAN differ. Access via the Conel-Router is possible without VPN.

The Road warrior needs access (*Network Access Permissions*) to the real IP addresses of the SPSses.

- Router 1: IP address 192.168.1.0/24 SPS: IP address 192.168.1.11
- Router 2: IP address 192.168.2.0/24 SPS: IP address 192.168.2.11

Activate the *Network Access Permissions* option to the real IP addresses.

Using this procedure results in a far higher administrative burden since all necessary information about the subnets and their distribution must be collected at one point.

12. When is a reconfiguration of the router necessary?

Some of the options listed below can be changed by a *SmartCluster administrator* but not by a *Group administrator*.

The actions required after making changes to the settings in the masks are listed in the tables following.

Networks

Table 12.1: Networks

Field changed or Option changed	New configuration?	Reconfigure router?	Reboot router?
Alias-Name	yes	–	–
Notes	–	–	–
Local IP (1st, 2nd or 3rd digit)	yes	yes	yes
Protocol	yes	yes	yes

Table 12.1: Networks

Field changed or Option changed	New configuration?	Reconfigure router?	Reboot router?
VPN Addr.	yes	yes	yes
Network Access Permissions	–	–	yes
URL	–	–	–
Enable Internet Access	yes	yes	yes
Masquerade	yes	yes	yes
SNMP Support	yes	yes	yes
Additional Settings	yes	yes	yes

If the *Reconfigure router?* column contains a *yes* load the new configuration file into the router and reboot, see “III, 3.5.3 Reboot the router” on Page 49.

A reboot of the SmartCluster connection is **not** necessary if you only change the settings for *Network Access Permissions* or *Direct Remote*.

Road warriors

Table 12.2: Road warriors

Field changed or Option changed	New configuration?	Reconfigure router?	Restart VPN tunnel?
Alias-Name	yes	–	–
Notes	–	–	–
Protocol	yes	yes	yes
VPN Addr.	yes	yes	yes
Network Access Permissions	–	–	yes
Grant Group Access	–	–	yes
Additional Settings	yes	yes	yes

If the *Restart VPN tunnel?* column contains a *yes* restart the VPN tunnel, see “III, 6.2 Terminating connections” on Page 60.

13. How many device can I use?

In a SmartCluster with the IP address range 10.0.0.0 and a netmask with the value 8 you can address a total of 16.581.375 (= 255 * 255 * 255) different devices.

The maximum number of groups possible is calculated as follows:

$$2^{((32-Value\,of\,VPN\,Server\,Netmask)-(32-Value\,of\,VPN\,Group\,Netmask))}$$

The maximum number of possible clients in one group is calculated as follows:

$$2^{((32-Value\,of\,VPN\,Group\,Netmask)-(32-Value\,of\,VPN\,Client\,Netmask))}$$

The address range of a client is calculated as follows:

$$2^{(32-Value\,of\,VPN\,Client\,Netmask)} - 2$$

Calculations with default settings

VPN server netmask = 8 / VPN group netmask = 16

$2^{((32-8)-(32-16))} = 2^{(24-16)} = 2^8 =$ 256 groups possible in SmartCluster

VPN group netmask = 16 / VPN client netmask = 24

$2^{((32-16)-(32-24))} = 2^{(16-8)} = 2^8 =$ 256 clients possible in one group

VPN client netmask = 24

$2^{(32-24)} - 2 = 2^8 - 2 =$ 254 IP addresses possible behind a router

Table 13.1: Best practise VPN group netmasks

VPN Group Netmask	Number of Groups	VPN Participants
16	256	256
17	512	128
18	1024	64

As a service provider offering SmartCluster you can vary the value for the VPN group netmask, e.g increase to 18, to increase the number of Groups: to 1.024. The number of Networks (routers) in one group will simultaneously be decreased to 64. To change the values of the netmask open the *Server* mask as a *SmartCluster administrator* using the navigation *Settings* → *Server*. Change the settings in the *VPN Server Netmask*, *VPN Group Netmask* or *VPN Client Netmask* fields as desired. To save the settings click on the *OK* button.

Part VI

Appendix

License / Copyright

Before using this software read the following text carefully.

If you do not agree with the following do not use the software and remove it from your storages.

Liability

We try to make our software as error-free as possible. It is, however, a general rule that no software is ever error-free and the number of errors increases with the complexity of the programme.

We cannot therefore assume any guarantee that our software will perform error-free in any environment, on any computer, and in combination with all other applications.

No liability is accepted for damages which may result directly or indirectly from the use of this software.

Our liability is, in all cases, limited to the purchase price of the software or the device.

Test this software with uncritical data. We accept no responsibility and liability for defects or damage to the data.

You may send us error reports but we can not guarantee that all errors will be fixed.

FAQ, BUG report and updates

Check http://www.conel.cz/ for the most current information about updates for your device.

- Firmware versions (download)
- Functional extensions
- Bug fixes
- FAQ
- Updates
- Documentation

Conel, the Conel logo, SmartCluster and MiniCluster are trademarks of Conel s.r.o..

Other trademarks, brands and company names may appear in this manual; if so, they shall remain the exclusive property of their respective owners. The absence of an explicit labelling of registered trademarks does not allow the conclusion that this brand was not subject to the rights of third party.

Place of jurisdiction: Hradec Králové/Czech Republic

Conel s.r.o. general terms and conditions are solely applicable.

Glossary and Acronyms

Most of the information in this glossary can be found at Wikipedia http://en.wikipedia.org/.

1:1 NAT 1:1 NAT is a special form of NAT. An internal IP address is mapped to an external IP address.
Example: In your network there is an service with the internal IP address 192.168.1.10. Via 1:1 NAT this IP address is mapped to the external IP address 203.0.113.10, provided by your Internet Service Provider.

communications protocol Within computer science, a communications protocol is a system of digital rules for message exchange within or between computers.
Communicating systems use well-defined formats for exchanging messages. Each message has an exact meaning intended to provoke a particular response of the receiver. Thus, a protocol must define the syntax, semantics, and synchronization of communication; the specified behaviour is typically independent of how it is to be implemented. A protocol can therefore be implemented as hardware, software, or both. Communications protocols have to be agreed upon by the parties involved. To reach agreement a protocol may be developed into a technical standard. A programming language describes the same for computations, so there is a close analogy between protocols and programming languages: protocols are to communications as programming languages are to computations.

DHCP The Dynamic Host Configuration Protocol (DHCP) is a network protocol used to configure devices that are connected to a network so they can communicate on that network using the Internet Protocol (IP). The protocol is implemented in a client-server model, in which DHCP clients request configuration data, such as an IP address, a default route, and one or more DNS server addresses from a DHCP server.

DHCP client Requests network configuration from DHCP server.

DHCP server Answers configuration request by DHCP clients and sends network configuration details.

DNS The Domain Name System (DNS) is a hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network. It associates various information with domain names assigned to each of the participating entities. Most prominently, it translates easily memorized domain names to the numerical IP addresses needed for the purpose of locating computer services and devices worldwide. By providing a worldwide, distributed keyword-based redirection service, the Domain Name System is an essential component of the functionality of the Internet.

Group From the SmartCluster point of view a Group is an access to a virtual private network (VPN), used by network participants for communication. Network participants may be networks (routers) or Road warriors.

host name A host name is a label that is assigned to a device connected to a computer network and that is used to identify the device in various forms of electronic communication such as the World Wide Web, e-mail or Usenet. Host names may be simple names consisting of a single word or phrase, or they may have appended a domain name, which is a name in a Domain Name System (DNS), separated from the host specific label by a period (dot). In the latter form, the hostname is also called a domain name. If the domain name is completely specified including a top-level domain of the Internet, then the hostname is said to be a fully qualified domain name (FQDN).

http The Hypertext Transfer Protocol (HTTP) is an application protocol for distributed, collaborative, hypermedia information systems. HTTP

is the foundation of data communication for the World Wide Web.
Hypertext is structured text that uses logical links (hyperlinks) between nodes containing text. HTTP is the protocol to exchange or transfer hypertext.

https The Hypertext Transfer Protocol Secure (HTTPS) is a communications protocol for secure communication over a computer network, with especially wide deployment on the Internet. Technically, it is not a protocol in and of itself; rather, it is the result of simply layering the Hypertext Transfer Protocol (HTTP) on top of the SSL/TLS protocol, thus adding the security capabilities of SSL/TLS to standard HTTP communications.

IP address An Internet Protocol address (IP address) is a numerical label assigned to each device (e.g., computer, printer) participating in a computer network that uses the Internet Protocol for communication. An IP address serves two principal functions: host or network interface identification and location addressing. Its role has been characterized as follows: *A name indicates what we seek. An address indicates where it is. A route indicates how to get there*
The designers of the Internet Protocol defined an IP address as a 32-bit number and this system, known as Internet Protocol Version 4 (IPv4), is still in use today. However, due to the enormous growth of the Internet and the predicted depletion of available addresses, a new version of IP (IPv6), using 128 bits for the address, was developed in 1995.

IP masquerade Kind of NAT.

IP masquerading see NAT.

IPC Industrial PCs are used primarily for process control and/or data acquisition. In some cases, an industrial PC is simply used as a front-end to another control computer in a distributed processing environment. Software can be custom written for a particular application or an off-the-shelf package such as Wonder Ware, Labtech Notebook or LabView can be used to provide a base level of programming.

IPv4 The Internet Protocol version 4 (IPv4) is the fourth version in the development of the Internet Protocol (IP) and the first version of the protocol to be widely deployed. It is one of the core protocols of standards-based internetworking methods of the Internet, and routes most traffic in the Internet. However, a successor protocol, IPv6, has been defined and is in various stages of production deployment. IPv4 is described in IETF publication RFC 791 (September 1981), replacing an earlier definition (RFC 760, January 1980).

IPv6 The Internet Protocol version 6 (IPv6) is the latest revision of the Internet Protocol (IP), the communications protocol that provides an identification and location system for computers on networks and routes traffic across the Internet. IPv6 was developed by the Internet Engineering Task Force (IETF) to deal with the long-anticipated problem of IPv4 address exhaustion.
IPv6 is intended to replace IPv4, which still carries the vast majority of Internet traffic as of 2013. As of late November 2012, IPv6 traffic share was reported to be approaching 1%.
IPv6 addresses are represented as eight groups of four hexadecimal digits separated by colons, for example 2001:0db8:85a3:0042:1000:8a2e:0370:7334, but methods of abbreviation of this full notation exist.

LAN A local area network (LAN) is a computer network that interconnects computers in a limited area such as a home, school, computer laboratory, or office building using network media. The defining characteristics of LANs, in contrast to wide area networks (WANs), include their usually higher data-transfer rates, smaller geographic area, and lack of a need for leased telecommunication lines.

MAN A metropolitan area network (MAN) is a computer network in which two or more computers or communicating devices or networks which are geographically separated but in same metropolitan city and are connected to each other are said to be connected on MAN. The limits of Metropolitan cities are determined by

local municipal corporations and we cannot define them. Hence, the bigger the Metropolitan city the bigger the MAN, smaller a metro city smaller the MAN.

NAT In computer networking, Network Address Translation (NAT) is the process of modifying IP address information in IPv4 headers while in transit across a traffic routing device.
The simplest type of NAT provides a one-to-one translation of IP addresses. RFC 2663 refers to this type of NAT as basic NAT, which is often also called a one-to-one NAT. In this type of NAT only the IP addresses, IP header checksum and any higher level checksums that include the IP address are changed. The rest of the packet is left untouched (at least for basic TCP/UDP functionality; some higher level protocols may need further translation). Basic NATs can be used to interconnect two IP networks that have incompatible addressing.

netmask A subnetwork, or subnet, is a logically visible subdivision of an IP network. The practice of dividing a network into two or more networks is called subnetting.
All computers that belong to a subnet are addressed with a common, identical, most-significant bit-group in their IP address. This results in the logical division of an IP address into two fields, a network or routing prefix and the rest field or host identifier. The rest field is an identifier for a specific host or network interface.
The routing prefix is expressed in CIDR notation. It is written as the first address of a network, followed by a slash character (/), and ending with the bit-length of the prefix. For example, 192.168.1.0/24 is the prefix of the Internet Protocol Version 4 network starting at the given address, having 24 bits allocated for the network prefix, and the remaining 8 bits reserved for host addressing. The IPv6 address specification 2001:db8::/32 is a large address block with 296 addresses, having a 32-bit routing prefix. In IPv4 the routing prefix is also specified in the form of the subnet mask, which is expressed in quad-dotted decimal representation like an address. For example, 255.255.255.0 is the network mask for the 192.168.1.0/24 prefix. Traffic between sub networks is exchanged or routed with special gateways called routers which constitute the logical or physical boundaries between the subnets.

Network A computer network is a telecommunications network that allows computers to exchange data. The physical connection between networked computing devices is established using either cable media or wireless media. The best-known computer network is the Internet.
Network devices that originate, route and terminate the data are called network nodes. Nodes can include hosts such as servers and personal computers, as well as networking hardware. Two devices are said to be networked when a process in one device is able to exchange information with a process in another device.
Computer networks support applications such as access to the World Wide Web, shared use of application and storage servers, printers, and fax machines, and use of email and instant messaging applications. The remainder of this article discusses local area network technologies and classifies them according to the following characteristics: the physical media used to transmit signals, the communications protocols used to organize network traffic, along with the network's size, its topology and its organizational intent.

PAT Port and Address Translation (PAT) or Network Address Port Translation (NAPT) see NAT.

port In computer networking, a port is an application-specific or process-specific software construct serving as a communications endpoint in a computer's host operating system. A port is associated with an IP address of the host, as well as the type of protocol used for communication. The purpose of ports is to uniquely identify different applications or processes running on a single computer and thereby enable them to share a single physical connection to a packet-switched network like the Internet.

remote service Remote service is the remote access to IT systems for maintenance and servicing purposes.

Road warrior The term Road warrior is generally attributed to people who are mostly travelling (away from their office or desk) but need to make heavy use of their laptop and/or phone.[1] These people often require access to network/computing resources that are available only at their office, and require a virtual private network (or similar connection) to connect back to their office.

root certificate In cryptography and computer security, a root certificate is either an unsigned public key certificate or a self-signed certificate that identifies the Root Certificate Authority (CA). A root certificate is part of a public key infrastructure scheme. The most common commercial variety is based on the ITU-T X.509 standard, which normally includes a digital signature from a certificate authority (CA).
Digital certificates are verified using a chain of trust. The trust anchor for the digital certificate is the Root Certificate Authority (CA). See also X.509.

router A router is a device that forwards data packets between computer networks, creating an overlay internetwork. A router is connected to two or more data lines from different networks. When a data packet comes in one of the lines, the router reads the address information in the packet to determine its ultimate destination. Then, using information in its routing table or routing policy, it directs the packet to the next network on its journey. Routers perform the *traffic directing* functions on the Internet. A data packet is typically forwarded from one router to another through the networks that constitute the internetwork until it reaches its destination node.

smartphone A smartphone, or smart phone, is a mobile phone built on a mobile operating system, with more advanced computing capability and connectivity than a feature phone. The first smartphones combined the functions of a personal digital assistant (PDA) with a mobile phone. Later models added the functionality of portable media players, low-end compact digital cameras, pocket video cameras, and GPS navigation units to form one multi-use device. Many modern smartphones also include high-resolution touch screens and web browsers that display standard web pages as well as mobile-optimized sites. High-speed data access is provided by Wi-Fi and mobile broadband. In recent years, the rapid development of mobile app markets and of mobile commerce have been drivers of smartphone adoption.

SNMP The Simple Network Management Protocol (SNMP) is an *Internet-standard protocol for managing devices on IP networks*. Devices that typically support SNMP include routers, switches, servers, workstations, printers, modem racks, and more. It is used mostly in network management systems to monitor network-attached devices for conditions that warrant administrative attention. SNMP is a component of the Internet Protocol Suite as defined by the Internet Engineering Task Force (IETF). It consists of a set of standards for network management, including an application layer protocol, a database schema, and a set of data objects.

TCP The Transmission Control Protocol (TCP) is one of the core protocols of the Internet protocol suite (IP), and is so common that the entire suite is often called TCP/IP. TCP provides reliable, ordered, error-checked delivery of a stream of octets between programs running on computers connected to a local area network, intranet or the public Internet. It resides at the transport layer.
Web browsers use TCP when they connect to servers on the World Wide Web, and it is used to deliver email and transfer files from one location to another.

UDP The User Datagram Protocol (UDP) is one of the core members of the Internet protocol suite (the set of network protocols used for the Internet). With UDP, computer applications can send messages, in this case referred to as datagrams, to other hosts on an Internet Protocol (IP) network without prior communications to set up special transmission channels or data paths. The protocol was designed by David P. Reed in 1980 and formally defined in RFC 768.

URL A uniform resource locator, abbreviated URL, also known as web address, is a specific

character string that constitutes a reference to a resource. In most web browsers, the URL of a web page is displayed on top inside an address bar. An example of a typical URL would be http://en.example.org/wiki/Main_Page. A URL is technically a type of uniform resource identifier (URI), but in many technical documents and verbal discussions, URL is often used as a synonym for URI, and this is not considered a problem.

virtual machine A virtual machine (VM) is a software implemented abstraction of the underlying hardware, which is presented to the application layer of the system. Virtual machines may be based on specifications of a hypothetical computer or emulate the computer architecture and functions of a real world computer.

VM see: virtual machine.

VPN A virtual private network (VPN) extends a private network across a public network, such as the Internet. It enables a computer to send and receive data across shared or public networks as if it were directly connected to the private network, while benefiting from the functionality, security and management policies of the private network. This is done by establishing a virtual point-to-point connection through the use of dedicated connections, encryption, or a combination of the two.

A VPN connection across the Internet is similar to a wide area network (WAN) link between the sites. From a user perspective, the extended network resources are accessed in the same way as resources available from the private network.

VPN server see VPN.

VPN tunnel see VPN.

WAN A wide area network (WAN) is a network that covers a broad area (i.e., any telecommunications network that links across metropolitan, regional, or national boundaries) using private or public network transports. Business and government entities utilize WANs to relay data among employees, clients, buyers, and suppliers from various geographical locations. In essence, this mode of telecommunication allows a business to effectively carry out its daily function regardless of location. The Internet can be considered a WAN as well, and is used by businesses, governments, organizations, and individuals for almost any purpose imaginable.

X.509 In cryptography, X.509 is an ITU-T standard for a public key infrastructure (PKI) and Privilege Management Infrastructure (PMI). X.509 specifies, amongst other things, standard formats for public key certificates, certificate revocation lists, attribute certificates, and a certification path validation algorithm.

Index

F

G

H

I

L

M

N

O

P

R

S

T

U

V

W

X