Clavister Software Series
Getting Started Guide

Clavister AB
Sjögatan 6J
SE-89160 Örnsköldsvik
SWEDEN

Phone: +46-660-299200
Fax: +46-660-12250

www.clavister.com

Published 2010-03-15

Clavister Software Series
Getting Started Guide

Published 2010-03-15

Copyright Notice

Disclaimer

The information in this document is subject to change without notice. Clavister makes no representations or warranties with respect to the contents hereof and specifically disclaims any implied warranties of merchantability or fitness for a particular purpose. Clavister reserves the right to revise this publication and to make changes from time to time in the content hereof without any obligation to notify any person or parties of such revision or changes.

Limitations of Liability

UNDER NO CIRCUMSTANCES SHALL CLAVISTER OR ITS SUPPLIERS BE LIABLE FOR DAMAGES OF ANY CHARACTER (E.G. DAMAGES FOR LOSS OF PROFIT, SOFTWARE RESTORATION, WORK STOPPAGE, LOSS OF SAVED DATA OR ANY OTHER COMMERCIAL DAMAGES OR LOSSES) RESULTING FROM THE APPLICATION OR IMPROPER USE OF THE CLAVISTER PRODUCT OR FAILURE OF THE PRODUCT, EVEN IF CLAVISTER IS INFORMED OF THE POSSIBILITY OF SUCH DAMAGES. FURTHERMORE, CLAVISTER WILL NOT BE LIABLE FOR THIRD-PARTY CLAIMS AGAINST CUSTOMER FOR LOSSES OR DAMAGES. CLAVISTER WILL IN NO EVENT BE LIABLE FOR ANY DAMAGES IN EXCESS OF THE AMOUNT CLAVISTER RECEIVED FROM THE END-USER FOR THE PRODUCT.

Table of Contents

Preface

Target Audience

The target audience for this guide is the user who wants to run the CorePlus network operating system on non-Clavister hardware. The guide takes the user from the installation of CorePlus through to start up of the software, including network connections and initial CorePlus configuration.

Text Structure

The text is divided into chapters and subsections. Numbered subsections are shown in the table of contents at the beginning of the document.

Text links

Where a "See section" link is provided in the main text, this can be clicked on to take the reader directly to that reference. For example, see *Appendix A, Troubleshooting Setup*.

Web links

Web links included in the document are clickable. For example, *http://www.clavister.com*.

Notes to the main text

Special sections of text which the reader should pay special attention to are indicated by icons on the the left hand side of the page followed by a short paragraph in italicized text. There are the following types of such sections:

Note
This indicates some piece of information that is an addition to the preceding text. It may concern something that is being emphasised or something that is not obvious or explicitly stated in the preceding text.

Tip
This indicates a piece of non-critical information that is useful to know in certain situations but is not essential reading.

Caution
This indicates where the reader should be careful with their actions as an undesirable situation may result if care is not exercised.

Important
This is an essential point that the reader should read and understand.

Warning
This is essential reading for the user as they should be aware that a serious situation may result if certain actions are taken or not taken.

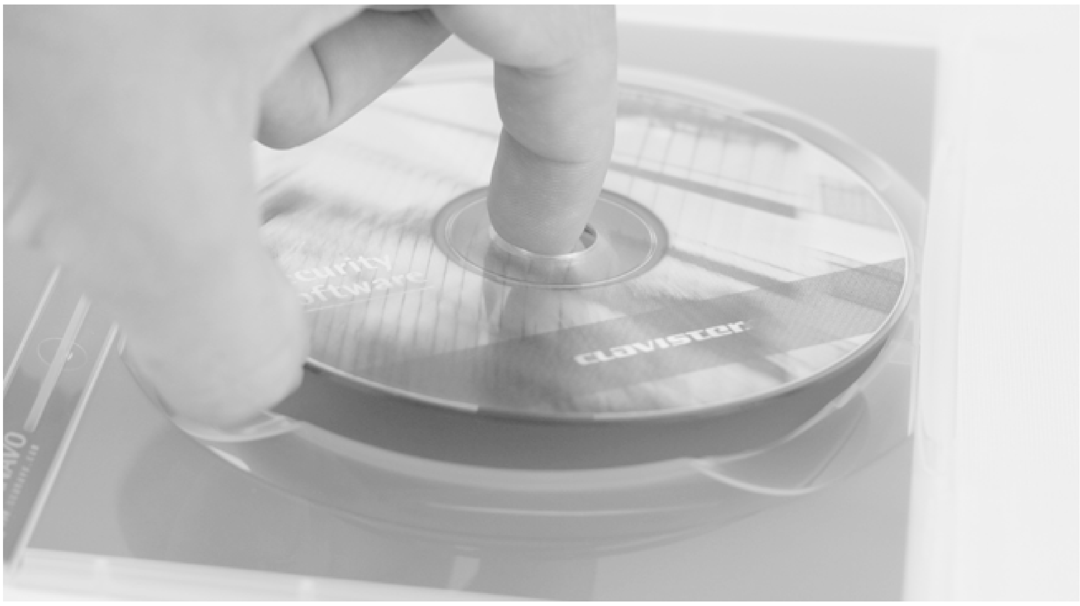
Trademarks

Certain names in this publication are the trademarks of their respective owners.

CorePlus is the trademark of Clavister AB.

Windows, *Windows XP*, *Windows Vista* and *Windows 7* are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Chapter 1: CorePlus Installation



Purpose of this Guide

When setting up CorePlus with non-Clavister hardware, the product must first be installed. This guide explains the installation and initial configuration of CorePlus on non-Clavister hardware.

CorePlus is an Operating System

CorePlus is Clavister's proprietary security network operating system that can run on Clavister hardware, third party hardware or in a VMware virtual environment. In all these cases, the differences in CorePlus management are minor and relate to such details as which interface becomes the default management Ethernet port.

It is important to understand that CorePlus does not run as an application under an operating system such as Microsoft Windows. (The one exception to this is when it runs under a hypervisor such as VMware but that is covered by a separate manual.)

Warning: CorePlus will overwrite existing disk data

CorePlus will overwrite any data on the physical disk allocated to it.

Minimum Hardware Requirements

The following are the minimum requirements for non-Clavister hardware that will run CorePlus:

- Processor architecture is x86. Usually this consists of a standard PC.
- 128 Mbytes RAM. CorePlus can run in 64 Mbytes of RAM but certain functions such as the UTM subsystems won't be able to execute. 128 is therefore the recommended minimum.
- A minimum disk size of 128 Mbytes. The entire physical disk will be used by CorePlus so this minimum does **not** refer to a logical partition.
- The Ethernet interface NIC cards used must be from the Clavister *Hardware Compatibility List* (HCL). The latest list can be found at *http://www.clavister.com*.

BIOS Compatability

The question of hardware BIOS compatibility can only be answered by trial and error. In almost all instances the BIOS will be compatible with CorePlus. Very infrequently, a BIOS can be encountered which is not compatible and the symptom will be that CorePlus will not boot after power up.

Installation Steps

The following steps should be followed for CorePlus installation:

1. Boot from the CorePlus CD-ROM

CorePlus is supplied on a CD-ROM. Place this in a CD drive and boot the computer from the CD.

In some cases, it may be appropriate to download the the ISO image of the CD over the Internet from a link provided by your sales representative. The filesystem contained within this file (and not the file itself) should be burned onto a CD-R disk to create the bootable CD.

2. Select a disk drive

The computer's screen will now display a list of the available disk drives. Select the physical disk drive on which to install CorePlus. **Note that any existing data will be lost after installation.**

3. Wait for the transfer to complete

After selecting the drive, the installation program will now transfer the CorePlus core to the drive. Wait for this to complete.

4. Reboot the hardware

When the transfer is complete, reboot the computer. The hardware will now boot up under CorePlus control. The computer's screen and keyboard will become the CorePlus *console* which is normally connected via the RS-232 port on Clavister hardware. The screen will display CorePlus messages showing the startup sequence.

5. Connect a management workstation

The hardware is now functioning as a Clavister Security Gateway. The next step is to connect a separate management workstation to perform CorePlus configuration. This is described next in *Chapter 2, Management Connection*

Chapter 2: Management Connection

The Default Management Interface

After first time startup, CorePlus scans the available Ethernet interfaces and makes management access available on the first interface found and assigns the internal IP address *192.168.1.1* to it.

Identifying the Default Interface

If the hardware has more than one Ethernet NICs installed and it is uncertain which one CorePlus has selected as the management interface, there are two ways of identifying the correct NIC:

- Try connecting to each interface in turn with a web browser (see the next section for details on this) to see if there is a response.
- Connect to the RS-232 console port of the hardware, press the enter key and at the CorePlus CLI prompt enter the *ifstat* command. This will list all interfaces with their IP address and show if there is an Ethernet link present (in other words, a cable has been plugged in). By plugging a cable into each interface in turn and then issuing the *ifstat* command, a match of the *192.168.1.1* IP address with the indication of Ethernet connection will identify the correct interface.

Configuration Methods

Initially, CorePlus will start with a set of factory defaults and configuration is needed to adapt the installation for a particular environment. Initial configuration can be done in one of the following ways:

- **Through a web browser.**

  A standard web browser running on any standalone computer can be used to access the CorePlus *web interface* user interface (also called the *WebUI*). The web interface provides an intuitive graphical interface for performing administration tasks. When the web interface is accessed for the first time, a *setup wizard* runs automatically to guide a new user through key setup steps. The wizard can be closed if the administrator wishes to instead go directly to the web interface to perform setup.

  Using the wizard is described next in *Chapter 3, Web Interface and Wizard Setup*.

  The wizard can greatly simply overall setup of CorePlus and is recommended for initial configuration of CorePlus.

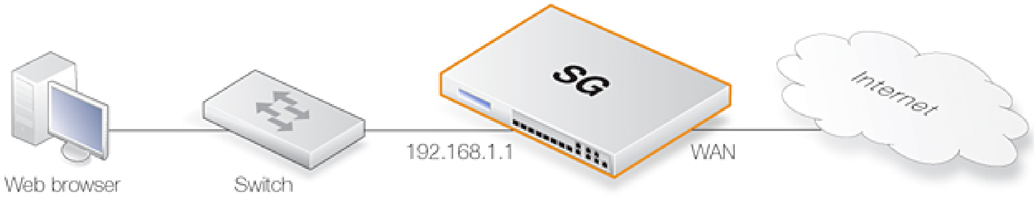
- **Through a terminal console using CLI commands.**

  The setup process can be performed using CLI commands instead of through a graphical user interface. This is described in *Chapter 5, CLI Setup* and that chapter mirrors the layout of *Chapter 3, Web Interface and Wizard Setup*. The CLI allows precise step by step control of the setup process and should be performed by administrators that fully understand both the CLI and the setup process.

  CLI setup could alternatively be performed directly through the computer's screen and keyboard which act as the CorePlus console normally connected via the RS-232 port on Clavister hardware.

Network Connection Setup

For setup using the Web Interface or the remote CLI, we must first connect a workstation to the Clavister Security Gateway. Workstation connection is illustrated below.



The management interface should be connected to the same network as the management workstation (or a network accessible from the workstation via one or more routers). Typically the connection is made via a switch or hub in the network using a regular straight-through Ethernet cable. For connection to the public Internet, another interface should be connected to your ISP and this is referred to below and in the setup wizard as the *WAN* interface.

Using Crossover Cables

Connection to the management interface by the workstation can be done directly without a switch or hub. This is done by using a crossover cable.

Workstation Interface Setup

Traffic will be able to flow between the designated workstation interface and the Clavister Security Gateway interface because they are on the same IP network. This means the workstation interface must be first assigned the following static IP addresses:

- **IP address:** *192.168.1.30*
- **Subnet mask:** *255.255.255.0*
- **Default gateway:** *192.168.1.1*

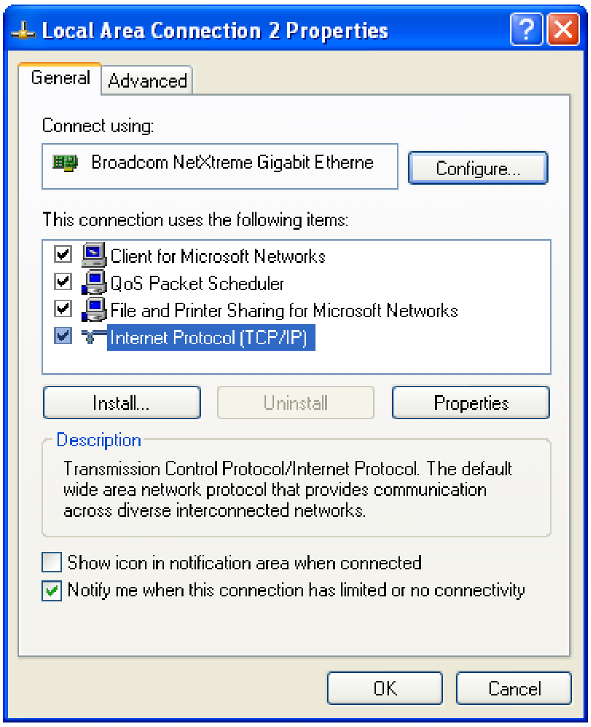
Tip

The assigned IP address ***192.168.1.30*** *could be another address from the 192.168.1.0/24 network as long as it is different from* ***192.168.1.1*** *which is the address used by CorePlus.*

To enter these settings on a PC running Windows XP, the following steps are needed:

- Click the **Start** button.
- Right click on **My Network Places** and select **Properties**.

- Right click the chosen Ethernet interface and select **Properties**.
- Select **Internet Protocol (TCP/IP)** and click **Properties**.



Local Area Connection 2 Properties

General | Advanced

Connect using:

Broadcom NetXtreme Gigabit Etherne

Configure...

This connection uses the following items:

☑ Client for Microsoft Networks
☑ QoS Packet Scheduler
☑ File and Printer Sharing for Microsoft Networks
☑ Internet Protocol (TCP/IP)

Install... | Uninstall | Properties

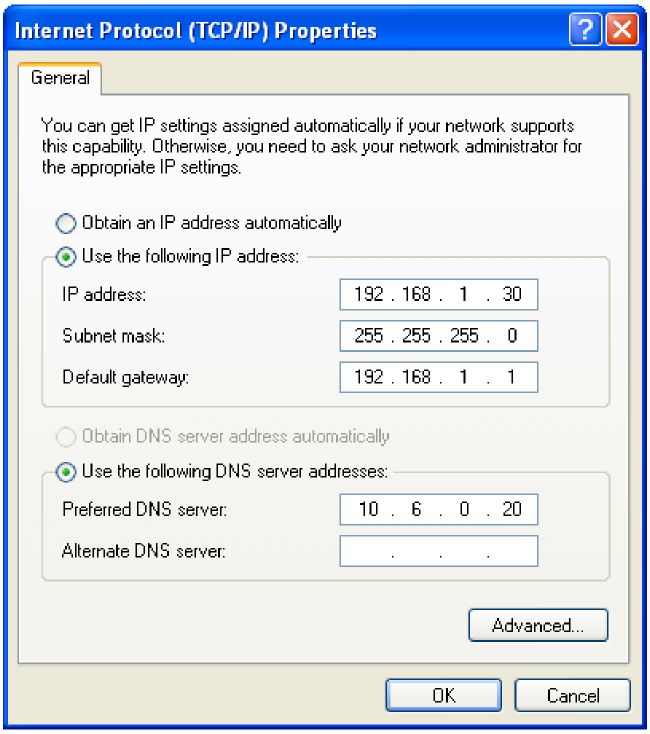
Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

☐ Show icon in notification area when connected
☑ Notify me when this connection has limited or no connectivity

OK | Cancel

- Enter the IP addresses given above and click **OK**.



Internet Protocol (TCP/IP) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:

IP address:	192 . 168 . 1 . 30
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	192 . 168 . 1 . 1

○ Obtain DNS server address automatically
● Use the following DNS server addresses:

Preferred DNS server:	10 . 6 . 0 . 20
Alternate DNS server:	. . .

Advanced...

OK | Cancel

IP Setup on Other Platforms

The following appendicies describe management workstation IP setup for other platforms:

- ***Appendix B, Vista IP Setup***.
- ***Appendix C, Windows 7 IP Setup***.
- ***Appendix D, Apple Mac IP Setup***.

Chapter 3: Web Interface and Wizard Setup

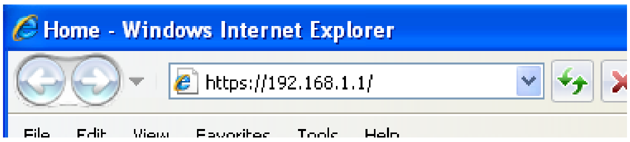
This chapter describes the setup when accessing CorePlus for the first time through a web browser. The user interface accessed in this way is called the *web interface* (also known as the *WebUI*).

Note

Many of the screenshots in this chapter have had whitespace removed from the original image to improve the readability. However, all of the informational content in the images has been preserved.

Connect By Surfing to *https://192.168.1.1*

Using a web browser (Internet Explorer or Firefox is recommended) enter the address *https://192.168.1.1* into the navigation window as shown below.



Home - Windows Internet Explorer

https://192.168.1.1/

Check for a proxy server and turn off popup blocking.

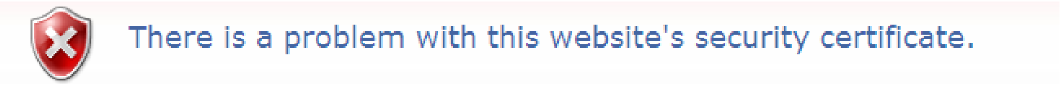
Make sure the web browser doesn't have a proxy server configured.

Any popup blocking in the browser should also be temporarily turned off to allow the setup wizard to run.

If there is no response from CorePlus and the reason is not clear, refer to the help checklist in *Appendix A, Troubleshooting Setup*.

The CorePlus Self-signed Certificate

When responding to an *https://* request, CorePlus sends a self-signed certificate which will not be initially recognised so it will be necessary to tell the browser to accept the certificate for this and future sessions. Different browsers handle this in slightly different ways. In Microsoft Internet Explorer the following error message will be displayed in the browser window.



There is a problem with this website's security certificate.

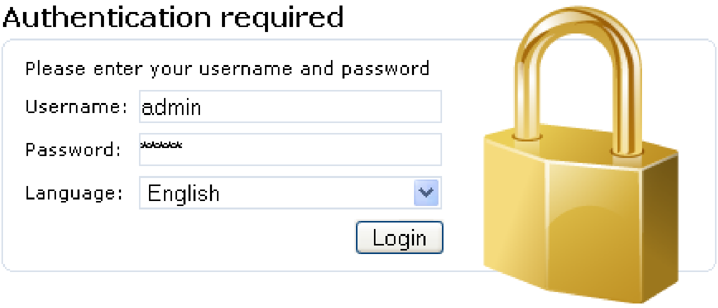
To continue, tell IE to accept the certificate by clicking the following link which appears near the bottom of the browser window.

Continue to this website (not recommended).

In FireFox this procedure is called *Add a security exception*.

The Login Dialog

CorePlus will next respond like a web server with the initial login dialog page as shown below.



Authentication required

Please enter your username and password

Username: admin

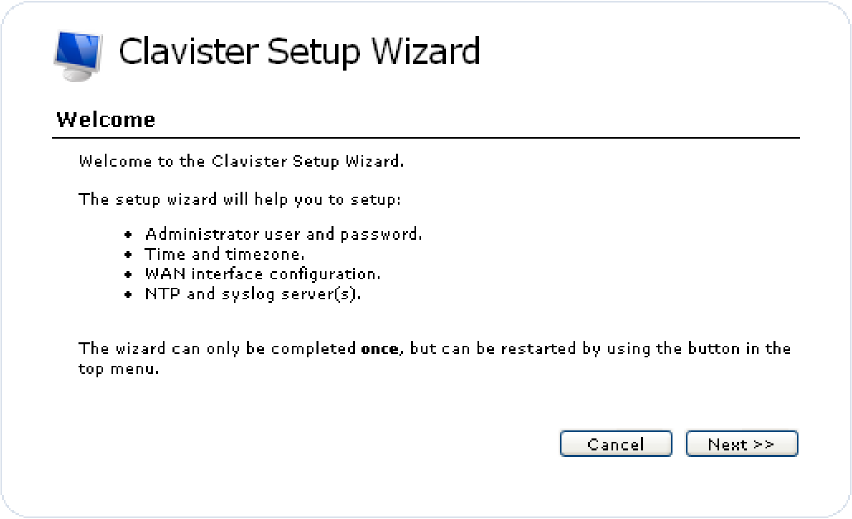
Password: *****

Language: English

The available web interface language options are selectable at the bottom of this dialog. This defaults to the language set for the browser if CorePlus supports that language.

Logging In and the Setup Wizard

Now login with the username *admin* and the password *admin*. The web interface will appear and the CorePlus setup wizard should begin automatically. The first wizard dialog is the wizard welcome screen which should appear as shown below.



Clavister Setup Wizard

Welcome

Welcome to the Clavister Setup Wizard.

The setup wizard will help you to setup:

- Administrator user and password.
- Time and timezone.
- WAN interface configuration.
- NTP and syslog server(s).

The wizard can only be completed **once**, but can be restarted by using the button in the top menu.

Cancelling the Wizard

The setup wizard can be cancelled at any point before the final *Activate* screen and run again by choosing the *Setup Wizard* option from the web interface toolbar. Once any configuration changes have been made and activated, either through the wizard, web interface or CLI, then the wizard cannot be run since the wizard requires that CorePlus has the factory defaults.

The Wizard Assumes Internet Access will be Configured

The wizard assumes that Internet access will be configured. If this is not the case, for example if the Clavister Security Gateway is being used in *Transparent Mode* between two internal networks, then the configuration setup is best done with individual web interface steps or through the CLI instead of through the wizard.

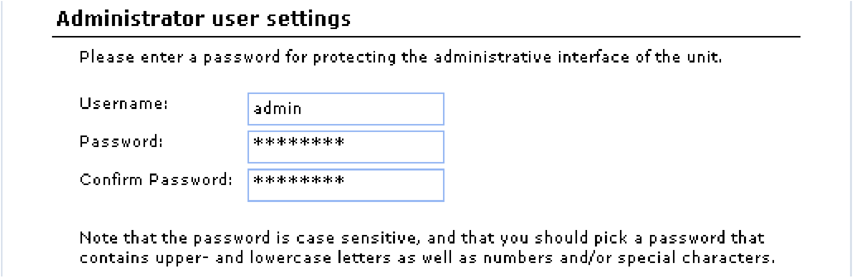
Advantages of the Wizard

The wizard makes setup easier because it automates what would otherwise be a more complex set of individual setup steps. It also reminds you to perform important tasks such as setting the date and time and configuring a log server.

The steps that the wizard goes through after the welcome screen are listed next.

Wizard step 1: Enter a new username and password

You will be prompted to enter a new administration username and password as shown below. It is recommended that this is always done and the new username/password is remembered (if these are forgotten, restoring to factory defaults will restore the original *admin*/*admin* combination). The password should be composed in a way which makes it difficult to guess.



Administrator user settings

Please enter a password for protecting the administrative interface of the unit.

Username: admin

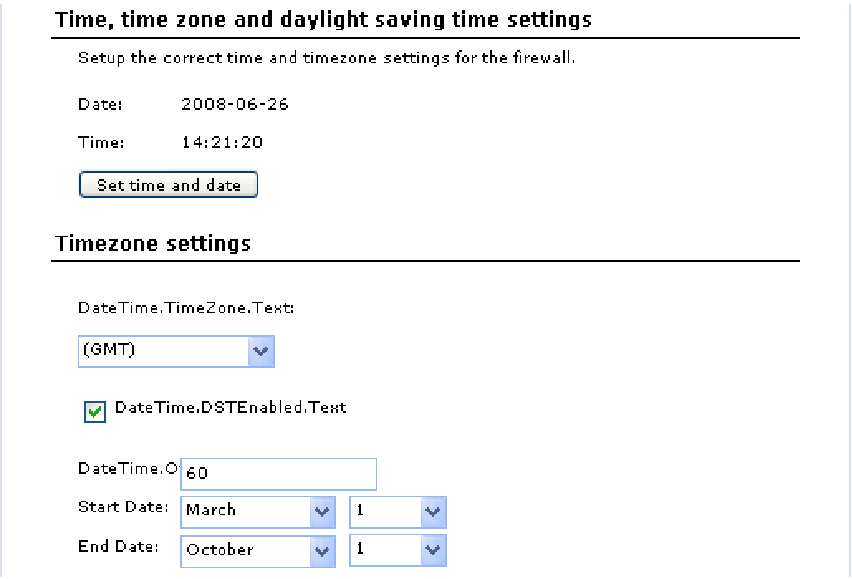
Password: ********

Confirm Password: ********

Note that the password is case sensitive, and that you should pick a password that contains upper- and lowercase letters as well as numbers and/or special characters.

Wizard step 2: Set the date and time

Many CorePlus functions rely on an accurate date and time, so it is important that this is set correctly in the fields shown below.



Time, time zone and daylight saving time settings

Setup the correct time and timezone settings for the firewall.

Date: 2008-06-26

Time: 14:21:20

Timezone settings

DateTime.TimeZone.Text:

(GMT)

☑ DateTime.DSTEnabled.Text

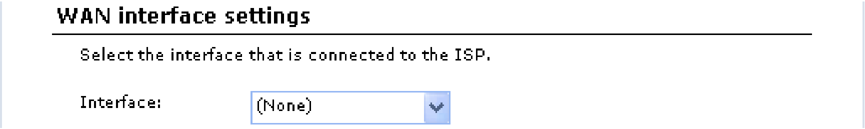
DateTime.O 60

Start Date: March 1

End Date: October 1

Wizard step 3: Select the *WAN* interface

Next, you will be asked for the *WAN* interface that will be used to connect to your ISP for Internet access.



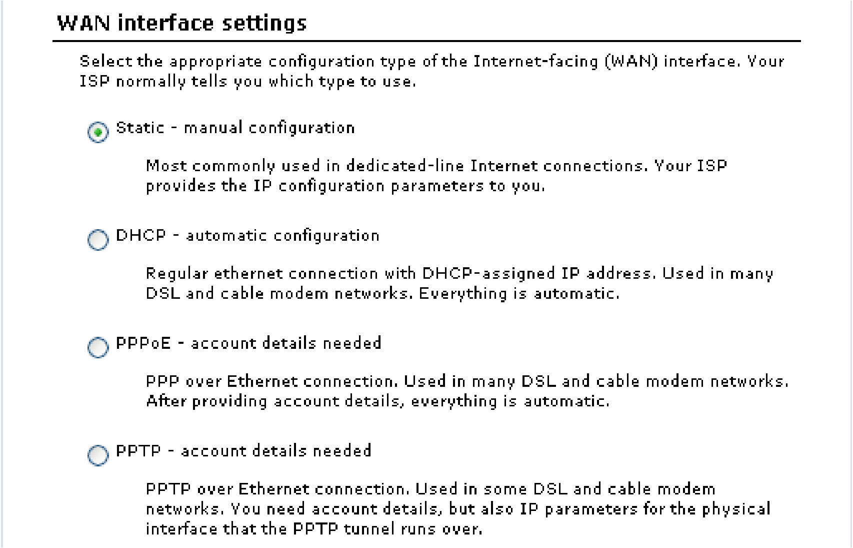
WAN interface settings

Select the interface that is connected to the ISP.

Interface: (None)

Wizard step 4: Select the *WAN* interface settings

This step selects how the WAN connection to the Internet will function. It can be one of *Manual configuration*, *DHCP*, *PPPoE* or *PPTP* as shown below.



WAN interface settings

Select the appropriate configuration type of the Internet-facing (WAN) interface. Your ISP normally tells you which type to use.

● Static - manual configuration

Most commonly used in dedicated-line Internet connections. Your ISP provides the IP configuration parameters to you.

○ DHCP - automatic configuration

Regular ethernet connection with DHCP-assigned IP address. Used in many DSL and cable modem networks. Everything is automatic.

○ PPPoE - account details needed

PPP over Ethernet connection. Used in many DSL and cable modem networks. After providing account details, everything is automatic.

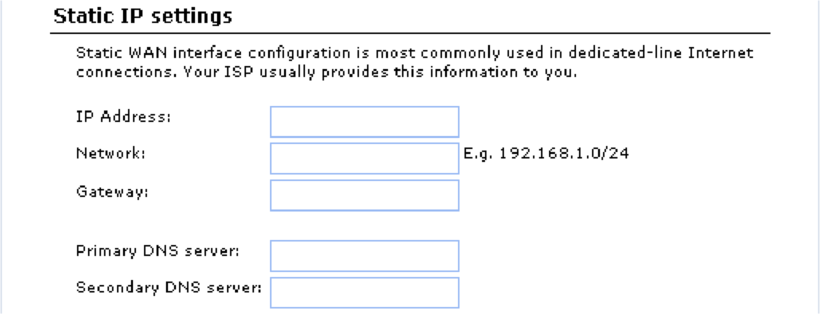
○ PPTP - account details needed

PPTP over Ethernet connection. Used in some DSL and cable modem networks. You need account details, but also IP parameters for the physical interface that the PPTP tunnel runs over.

These four different connection options are discussed next in the following subsections **4A** to **4D**.

- **4A. Static - manual configuration**

  Information supplied by the ISP should be entered in the next wizard screen. All fields need to be entered except for the *Secondary DNS server* field.



Static IP settings

Static WAN interface configuration is most commonly used in dedicated-line Internet connections. Your ISP usually provides this information to you.

IP Address:

Network: E.g. 192.168.1.0/24

Gateway:

Primary DNS server:

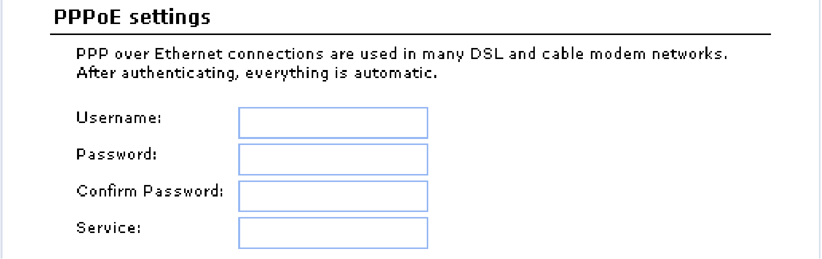
Secondary DNS server:

- **4B. DHCP - automatic configuration**

  All required IP addresses will automatically be retrieved from the ISP's DHCP server with this option. No further configuration is required for this so it does not have its own wizard screen.

- **4C. PPPoE settings**

  The username and password supplied by your ISP for PPPoE connection should be entered. The *Service* field should be left blank unless the ISP supplies a value for it.



PPPoE settings

PPP over Ethernet connections are used in many DSL and cable modem networks. After authenticating, everything is automatic.

Username:

Password:

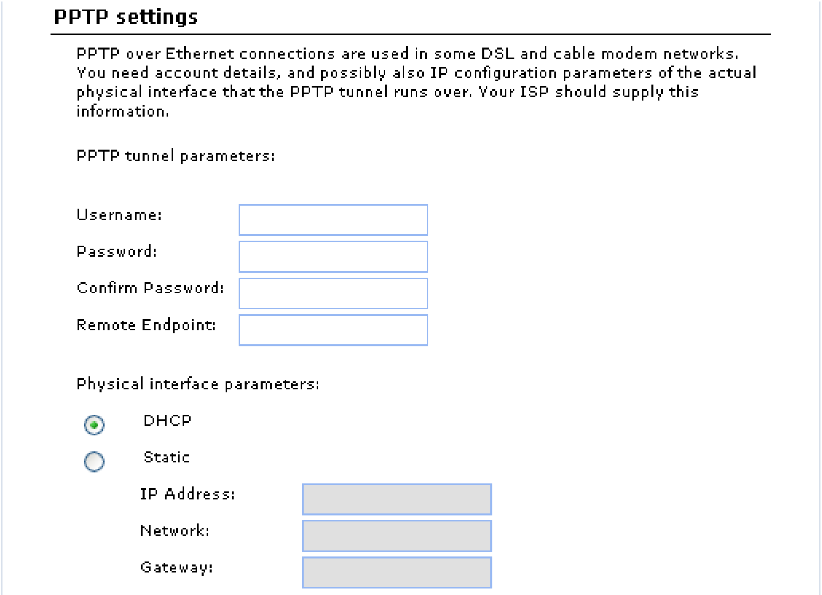
Confirm Password:

Service:

DNS servers are set automatically after connection with PPPoE.

- **4D. PPTP settings**

  The username and password supplied by your ISP for PPTP connection should be entered. If DHCP is to be used with the ISP then this should be selected, otherwise *Static* should be selected followed by entering the static IP address supplied by the ISP.



PPTP settings

PPTP over Ethernet connections are used in some DSL and cable modem networks. You need account details, and possibly also IP configuration parameters of the actual physical interface that the PPTP tunnel runs over. Your ISP should supply this information.

PPTP tunnel parameters:

Username:

Password:

Confirm Password:

Remote Endpoint:

Physical interface parameters:

● DHCP

○ Static

IP Address:

Network:

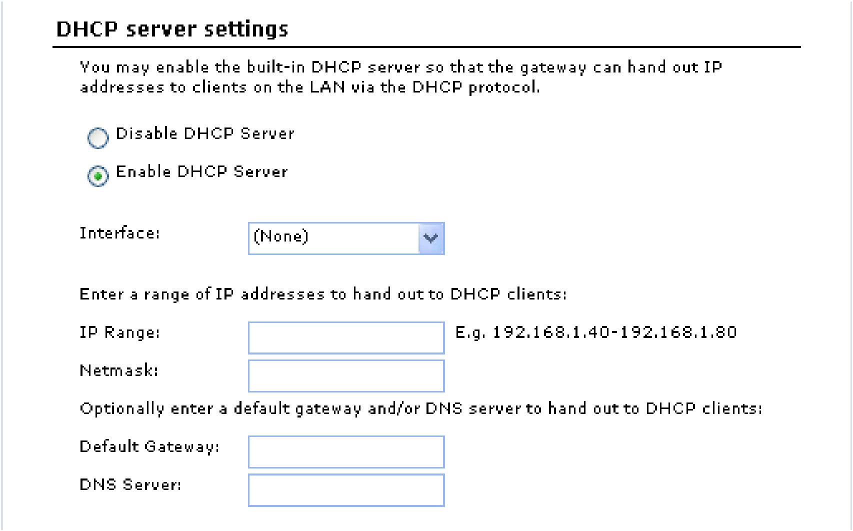
Gateway:

DNS servers are set automatically after connection with PPTP.

Wizard step 5: DHCP server settings

If the Clavister Security Gateway is to function as a DHCP server, it can be enabled here in the wizard on a particular interface or configured later.

The range of IP addresses that can be handed out must be specified in the form *nn.nn.nn.nn - nn.nn.nn.nn*. For instance, the internal IP address range *192.168.1.50 - 192.168.1.150* might be specified.



DHCP server settings

You may enable the built-in DHCP server so that the gateway can hand out IP addresses to clients on the LAN via the DHCP protocol.

○ Disable DHCP Server

● Enable DHCP Server

Interface: (None)

Enter a range of IP addresses to hand out to DHCP clients:

IP Range: E.g. 192.168.1.40-192.168.1.80

Netmask:

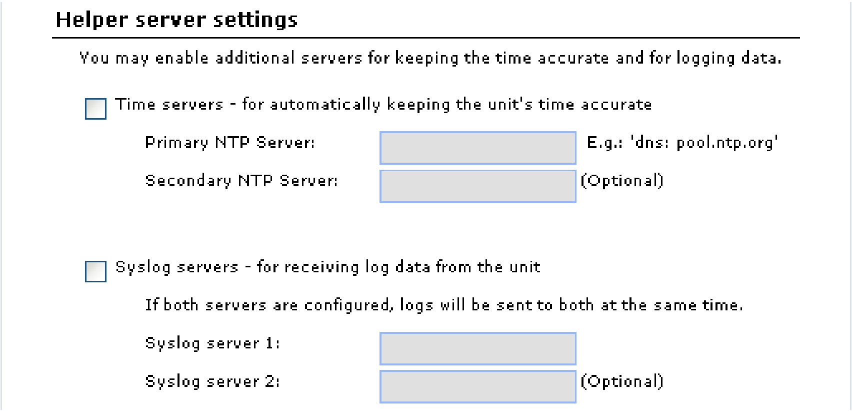
Optionally enter a default gateway and/or DNS server to hand out to DHCP clients:

Default Gateway:

DNS Server:

Wizard step 6: Helper server settings

Optional NTP and Syslog servers can be enabled here in the wizard or configured later. *Network Time Protocol* servers keep the system date and time accurate. Syslog servers can be used to receive and store log messages sent by CorePlus.



Helper server settings

You may enable additional servers for keeping the time accurate and for logging data.

□ Time servers - for automatically keeping the unit's time accurate

Primary NTP Server: E.g.: 'dns: pool.ntp.org'

Secondary NTP Server: (Optional)

□ Syslog servers - for receiving log data from the unit

If both servers are configured, logs will be sent to both at the same time.

Syslog server 1:

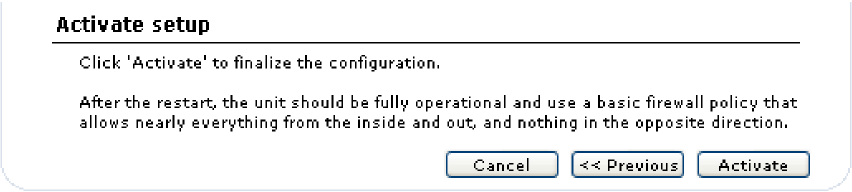
Syslog server 2: (Optional)

For the default gateway, it is recommended to specify the IP address *192.168.1.1* and the DNS server specified should be the DNS supplied by your ISP.

When specifying a hostname as a server instead of an IP address, the hostname should be prefixed with the string *dns:*. For example, the hostname *host1.company.com* should be entered as *dns:host1.company.com*.

Wizard step 7: Activate setup

The final step is to activate the setup by pressing the *Activate* button. After this step the web interface returns to its normal appearance and the administrator can continue to configure the system.



Activate setup

Click 'Activate' to finalize the configuration.

After the restart, the unit should be fully operational and use a basic firewall policy that allows nearly everything from the inside and out, and nothing in the opposite direction.

Running the Wizard Again

Once the wizard has been successfully finished and activated, it cannot be run again. The exception to this is if the Clavister Security Gateway has its factory defaults restored in which case the unit will behave as though it were being started for the first time.

Uploading a License

If the wizard has been run or not, the web interface can now be used to upload a valid license to the Clavister Security Gateway. Without a license, CorePlus will run in *demonstration mode* which means that it will cease to function after two hours of operation (restarting the system will re-enable CorePlus for another two hours). The steps for license upload are:

- Using a web browser, surf to the Clavister *Customer Web* (this can be found at *https://clientweb.clavister.com*) and register for the first time. You will require your Clavister *registration key* to do this. For software-only licenses the key is supplied following purchase. If you are already registered as a customer then you will need to login to the Customer Web.

- The Customer Web system will ask for a *MAC address* to associate with the Clavister license.

This is the hardware Ethernet address associated with any of the Ethernet interfaces on the hardware.

A MAC address can be read from the output of the *ifstat* CLI command (this can be entered via the serial console).

First use the console command:

```
Device:/> ifstat
```

This gives the list of interface names. To get the MAC address of any one of these, use the command:

```
Device:/> ifstat <interface_name>
```

The MAC address has the field name *HW address* in the output.

- Now download a valid *.lic* license file from the Customer Web to the hard disk of the workstation.

- In the web interface menu bar, select **Maintenance > Upgrade** and use the **Browse** button to select the license file, then upload it. As soon as the license is uploaded, demonstration mode will end and CorePlus will be restricted only by the limitations of the license.

Chapter 4: Manual Web Interface Setup

This section describes initial CorePlus configuration performed directly through the web interface, without using the setup wizard. Configuration is done as a series of individual steps, giving the administrator more direct control over the process. Even if the wizard is used, this section can also be read as a good introduction to using the Web Interface for configuring key aspects of CorePlus.

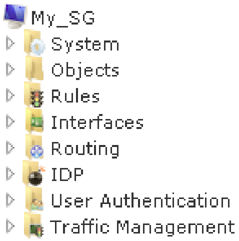
Ethernet Interfaces

The physical connection of external networks to the Clavister Security Gateway is through the various *Ethernet interfaces* which are provided by the hardware platform. On first-time startup, CorePlus scans for these interfaces and determines which are available and allocates their names. The first interface detected in the scan always becomes the initial default management interface and this cannot be changed beforehand.

All CorePlus interfaces are logically equal for CorePlus and although their physical capabilities may be different, any interface can perform any logical function. With the Clavister Software Series, the first interface is called *If1* and is always the management interface. We will assume that the hardware used has 3 Ethernet interfaces so the other two will automatically be given the names *If2* and *If3* by CorePlus. For this section, we will assume that the *If2* interface will be used for connection to the public Internet and the *If3* interface will be used for connection to a protected, local network.

The Navigation Tree

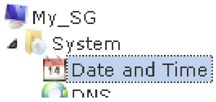
The web interface presents the various components of CorePlus in a tree structure in the left-hand pane of the browser window.



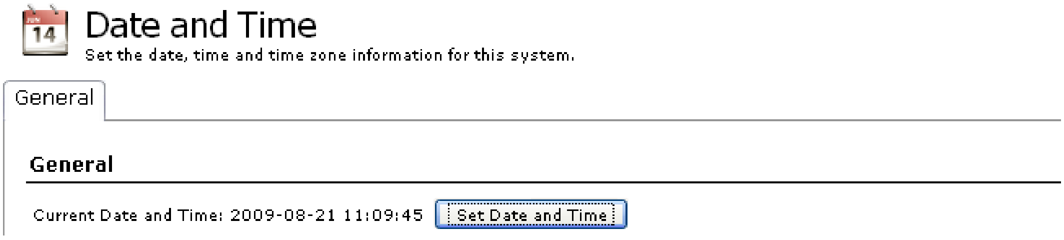
By clicking on the navigation tree we can expand its nodes to examine and change the properties of the various *settings*, *objects* and *rules* that make up a CorePlus configuration. A simple example of changing a configuration is discussed next.

Setting the Date and Time

Many CorePlus functions rely on an accurate date and time, so it is important that this is set correctly. To do this, open the *System* node in the navigation tree.



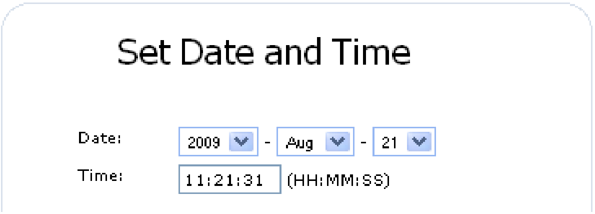
If we now click on the *Date and Time* node in the tree, the properties of the current date and time settings will appear in the central panel of the web interface.



Set the date, time and time zone information for this system.

Current Date and Time: 2009-08-21 11:09:45

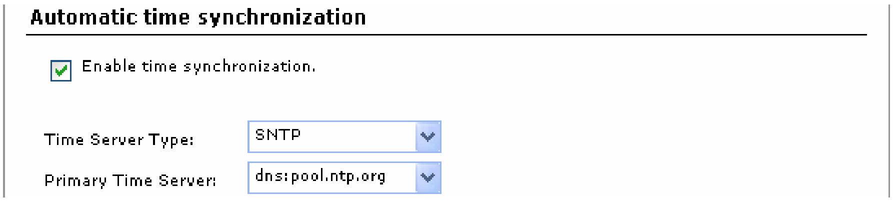
By pressing the **Set Date and Time** button, a dialog appears that allows the exact time to be set.



Date: 2009 - Aug - 21

Time: 11:21:31 (HH:MM:SS)

A **Network Time Protocol** (NTP) servers can optionally be configured to maintain the accuracy of the system date and time and this will require public Internet access. Enabling this option is strongly recommended since it ensures the accuracy of the date and time. A typical NTP setup is shown below.



☑ Enable time synchronization.

Time Server Type: SNTP

Primary Time Server: dns:pool.ntp.org

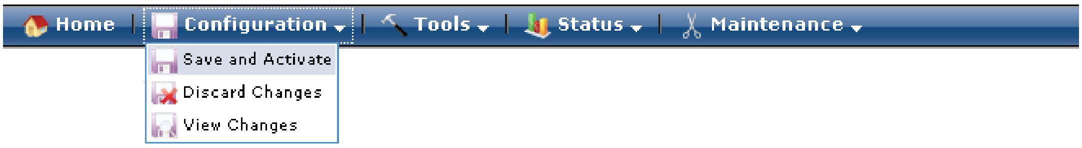
Note: The time server URL requires the "dns:" prefix

*When specifying a URL in CorePlus for the time server, the URL must have the prefix "**dns:**".*

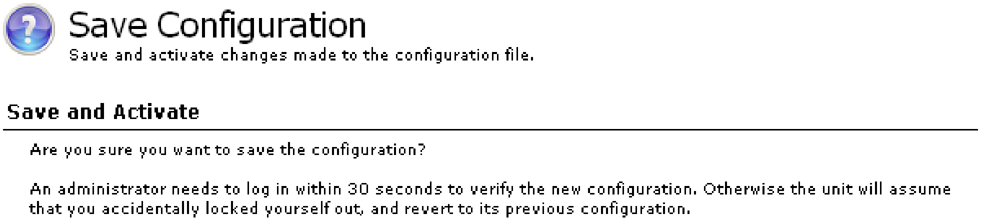
Once the values are set correctly, we can press the **OK** button to save the values while we move on to more steps in CorePlus configuration. Although changed values like this are saved by CorePlus, they do not become active until the entire saved configuration becomes the current and active configuration. We will look at how to do this next.

Activating Configuration Changes

To activate any CorePlus configuration changes made so far, we need to select the **Save and Activate** option from the **Configuration** menu (this process is also sometimes referred to as *deploying* a configuration).



A dialog is then presented to confirm that the new configuration is to become the running configuration.



Save Configuration

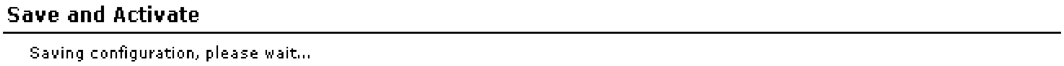
Save and activate changes made to the configuration file.

Save and Activate

Are you sure you want to save the configuration?

An administrator needs to log in within 30 seconds to verify the new configuration. Otherwise the unit will assume that you accidentally locked yourself out, and revert to its previous configuration.

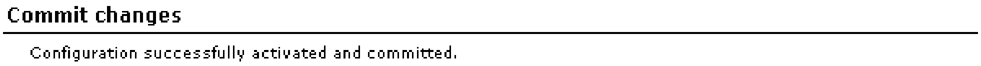
After clicking **OK**, CorePlus *reconfiguration* will take place and, after a short delay, the web interface will try and connect again to the security gateway.



Save and Activate

Saving configuration, please wait...

If no reconnection is detected by CorePlus within 30 seconds (this length of time is a setting that can be changed) then CorePlus will revert back to the original configuration. This is to ensure that the new configuration does not accidentally lock out the administrator. After reconfiguration and successful reconnection, a success message is displayed indicating successful reconfiguration.



Commit changes

Configuration successfully activated and committed.

Reconfiguration is a process that the CorePlus administrator may initiate often. Normally, reconfiguration takes a brief amount of time and causes only a slight delay in traffic throughput. Active user connections through the Clavister Security Gateway should rarely be lost.

Tip: How frequently to commit changes

It is up to the administrator to decide how many changes to make before activating a new configuration. Sometimes, activating configuration changes in small batches can be appropriate in order to check that a small set of changes work as planned. It is, however, not advisable to leave changes uncommited for long periods of time, such as overnight, since any system outage will result in these edits being lost.

Automatic Logout

If there is no activity through the web interface for a period of time (the default is 15 minutes), CorePlus will automatically log the user out. If they log back in through the same web browser session then they will return to the point they were at before the logout occurred and no saved (but not yet activated) changes are lost.

Setting Up Internet Access

Next, we shall look at how to set up public Internet access. The setup wizard described in the previous chapter, provides the following four options:

A. Static - manual configuration.

B. DHCP - automatic configuration.

C. PPPoE setup

D. PPTP setup

The individual manual steps to configure these connection alternatives with the web interface are discussed next.

A. Static - manual configuration

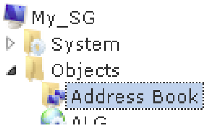
Manual configuration means that there will be a direct connection to the ISP and all the relevant IP addresses for the connecting interface are fixed values provided by the ISP which are entered into CorePlus manually.

> ***Note: The interface DHCP option should be disabled***
>
> *For static configuration of the Internet connection, the DHCP option must be disabled (the default) in the properties of the interface that will connect to the ISP.*

The initial step is to set up a number of IP address objects in the CorePlus *Address Book*. Let us assume for this section that the physical interface used for Internet connection is *If2* the static IP address for this interface is to be *10.5.4.35*, the ISP's gateway IP address is *10.5.4.1*, and the network to which they both belong is *10.5.4.0/24*.

> ***Note: Private IP addresses are used for example only***
>
> *Each installation's IP addresses will be different from these IP addresses but they are used here only to illustrate how setup is done. Also, these addresses are private IP addresses and in reality an ISP would use public IP addresses instead.*

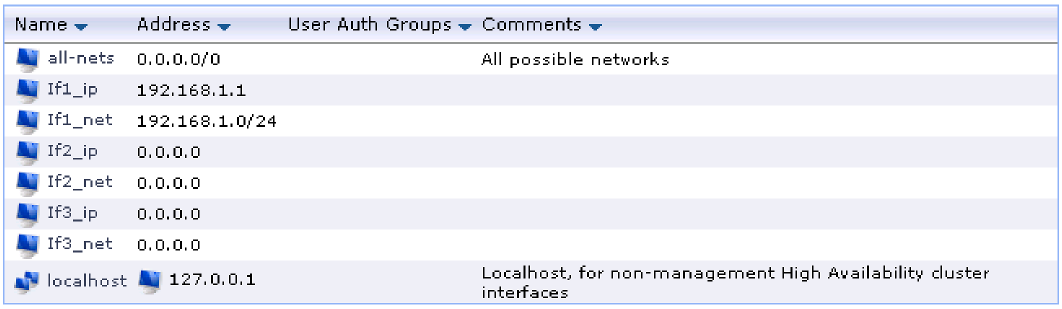
Let's now add the gateway *IP4 Address* object which we will call *wan_gw* and assign it the IP address *10.5.4.1*. The ISP's gateway is the first router hop towards the public Internet from the Clavister Security Gateway. Go to **System > Objects > Address Book** in the web interface navigation tree.



The current contents of the address book will be listed and will contain a number of predefined objects created by CorePlus after it scans the interfaces for the first time. The screenshot below shows the initial address book for the Software Series.

Note: The all-nets address

*The IP address object **all-nets** is a wildcard address that should never be changed and can be used in many types of CorePlus rules to refer to any IP address or network range.*



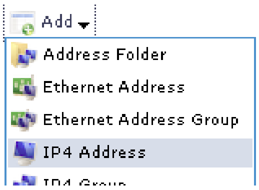
Name	Address	User Auth Groups	Comments
all-nets	0.0.0.0/0		All possible networks
If1_ip	192.168.1.1		
If1_net	192.168.1.0/24		
If2_ip	0.0.0.0		
If2_net	0.0.0.0		
If3_ip	0.0.0.0		
If3_net	0.0.0.0		
localhost	127.0.0.1		Localhost, for non-management High Availability cluster interfaces

By default on initial startup, two IP address objects are create automatically for each interface detected by CorePlus. One IP address object is named by combining the physical interface name with the suffix *_ip* and this is used for the IP address assigned to that interface. The other address object is named by combining the interface name with the suffix *_net* and this is the network to which the interface belongs.

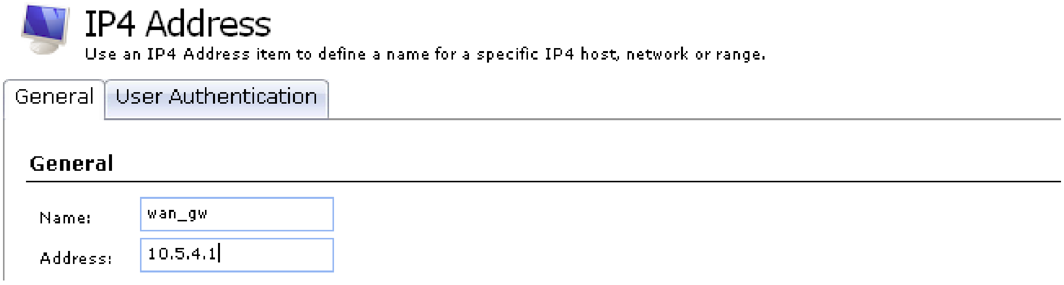
Tip: Creating address book folders

New folders can be created when needed and provide a convenient way to group together related IP address objects. The folder name can be chosen to indicate the folder's contents.

Now click the **Add** button at the top left of the list and choose the *IP4 Address* option to add a new address to the folder.



Enter the details of the object into the properties fields for the IP4 Address. Below, we have entered the IP address *10.5.4.1* for the address object called *wan_gw*. This is the IP of the ISP's router which acts as the gateway to the Internet.



IP4 Address

Use an IP4 Address item to define a name for a specific IP4 host, network or range.

General

Name: wan_gw

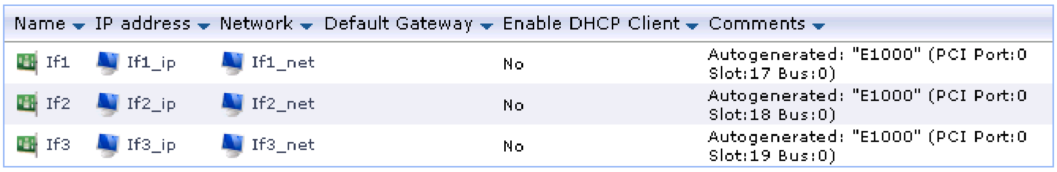
Address: 10.5.4.1

Click the **OK** button to save the values entered.

Then set up *If2_ip* to be *10.5.4.35*. This is the IP address of the *If2* interface which will connect to the ISP's gateway.

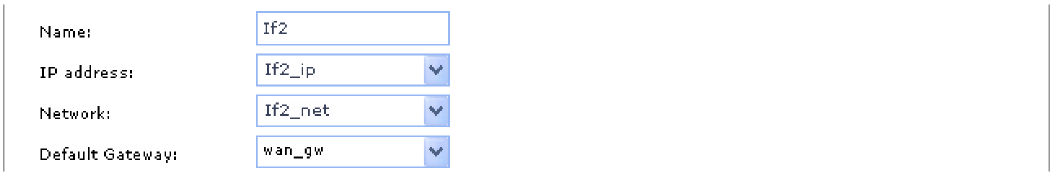
Lastly, set the IP4 Address object *If2_net* to be *10.5.4.0/24*. Both *If2_ip* and *wan_gw* must belong to this network in order for the interface to communicate with the ISP.

Together, these 3 IP address objects will be used to configure the interface connected to the Internet which in this example is *If2*. Select **Interfaces > Ethernet** in the navigation tree to display a list of the physical interfaces.



Name	IP address	Network	Default Gateway	Enable DHCP Client	Comments
If1	If1_ip	If1_net		No	Autogenerated: "E1000" (PCI Port:0 Slot:17 Bus:0)
If2	If2_ip	If2_net		No	Autogenerated: "E1000" (PCI Port:0 Slot:18 Bus:0)
If3	If3_ip	If3_net		No	Autogenerated: "E1000" (PCI Port:0 Slot:19 Bus:0)

Click on the interface in the list which is to be connected to the Internet. The properties for this interface will now appear and the relevant settings can be entered or changed.



Name:	If2
IP address:	If2_ip
Network:	If2_net
Default Gateway:	wan_gw

Press **OK** to save the changes. Although changes are remembered by CorePlus, the changed configuration is not yet activated and won't be activated until CorePlus is told to activate the changed configuration.

Remember that DHCP should **not** be enabled when using static IP addresses and also that the IP address of the *Default Gateway* (which is the ISP's router) **must** be specified. As explained in more detail later, specifying the *Default Gateway* also has the additional effect of automatically adding a route for the gateway in the CorePlus routing table.

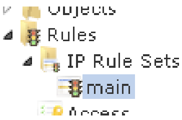
At this point, the connection to the Internet is configured but no traffic can flow to or from the Internet since all traffic needs a minimum of the following two CorePlus configuration objects to exist before it can flow through the Clavister Security Gateway:

- An *IP rule* defined in a CorePlus *IP rule set* that explicitly allows traffic to flow from a given source network and source interface to a given destination network and destination interface.
- A *route* defined in a CorePlus routing table which specifies on which interface CorePlus can find the traffic's destination IP address.

  If multiple matching routes are found, CorePlus uses the route that has the smallest (in other words, the narrowest) IP range.

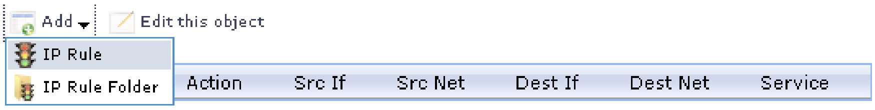
We must therefore first define an IP rule that will allow traffic from a designated source interface and source network. In this case let us assume we want to allow web surfers on the internal network *If3_net* connected to the interface *If3* to be able to access the public Internet.

To do this, we first go to **Rules > IP Rule Sets > main** in the navigation tree.

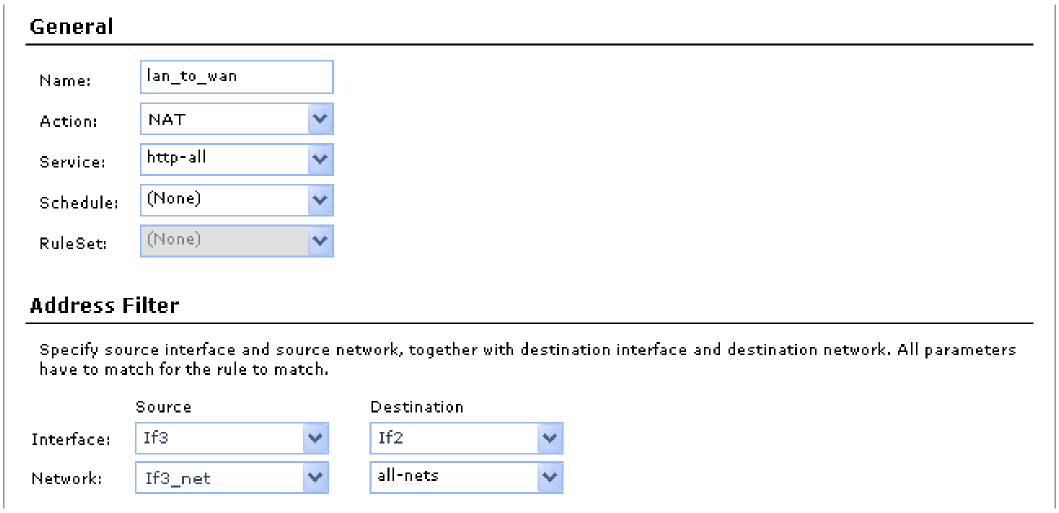


The empty *main* IP rule set will now appear. Press the **Add** button at the top left and select **IP**

Rule from the menu.



The properties for the new IP rule will appear. In this example, we will call the rule *lan_to_wan*. The rule *Action* is set to *NAT* (this is explained further below) and the *Service* is set to *http-all* which is suitable for most web surfing (it allows both HTTP and HTTPS connections). The interface and network for the source and destinations are defined in the *Address Filter* section of the rule.



General

Name: lan_to_wan

Action: NAT

Service: http-all

Schedule: (None)

RuleSet: (None)

Address Filter

Specify source interface and source network, together with destination interface and destination network. All parameters have to match for the rule to match.

	Source	Destination
Interface:	If3	If2
Network:	If3_net	all-nets

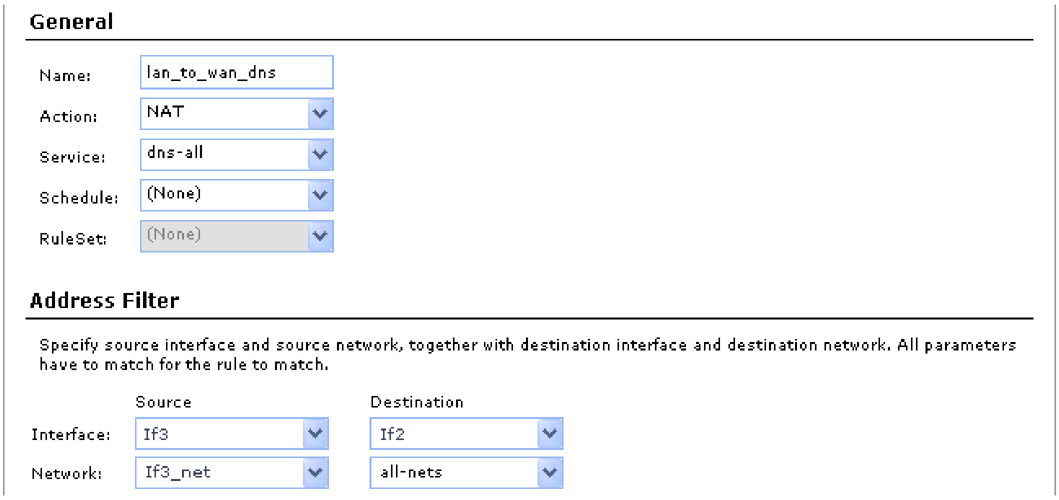
The destination network in the IP rule is specified as the predefined IP4 Address object *all-nets*. This is used since we don't know to which IP address the web surfing will be done and this allows surfing to any IP address. IP rules are processed in a top down fashion, with the first matching rule being obeyed. An *all-nets* rule like this should be placed towards the bottom of the rule set since other rules with narrower destination addreses should trigger before it does.

Only one rule is needed since any traffic controlled by a *NAT* rule will be controlled by the CorePlus *state engine*. This means that the rule will allow *connections* that originate from the source network/destination and also implicitly allow any returning traffic that results from those connections.

In the above, we selected the service called *http_all* which is already defined in CorePlus. It is advisable to make the service in an IP rule as restrictive as possible to provide the best security possible. Custom service objects can be created and new service objects can be created which are combinations of existing services.

We could have specified the rule *Action* to be *Allow*, but only if all the hosts on the protected local network have public IP addresses. By using *NAT*, CorePlus will use the destination interface's IP address as the source IP. This means that external hosts will send their responses back to the interface IP and CorePlus will automatically direct the traffic back to the originating local host. Only the outgoing interface therefore needs to have a public IP address and the internal network topology is hidden.

To allow web surfing, DNS lookup also needs to be allowed in order to resolve URLs into IP addresses. The service *http_all* does not include the *DNS* protocol so we need a similar IP rule that allows this. This could be done with one IP rule that uses a custom service which combines the *HTTP* and *DNS* protocols but the recommended method is to create an entirely new IP rule that mirrors the above rule but specifies the service as *dns-all*. This method provides the most clarity when the configuration is examined for any problems. The screenshot below shows a new rule called *lan_to_wan_dns* being created to allow DNS.



General

Name:	lan_to_wan_dns
Action:	NAT
Service:	dns-all
Schedule:	(None)
RuleSet:	(None)

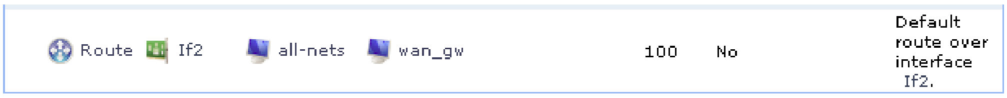
Address Filter

Specify source interface and source network, together with destination interface and destination network. All parameters have to match for the rule to match.

	Source	Destination
Interface:	If3	If2
Network:	If3_net	all-nets

This IP rule also specifies that the action for DNS requests is *NAT* so all DNS request traffic is sent out by CorePlus with the outgoing interface's IP address as the source IP.

For the Internet connection to work, we also need a *route*defined so that CorePlus knows on which interface the web surfing traffic should leave the Clavister Security Gateway. This route will define the interface where the network *all-nets* will be found. If we open the default *main* routing table by going to **Routing > Routing Tables > Main** in the navigation tree, the route needed should appear as below.



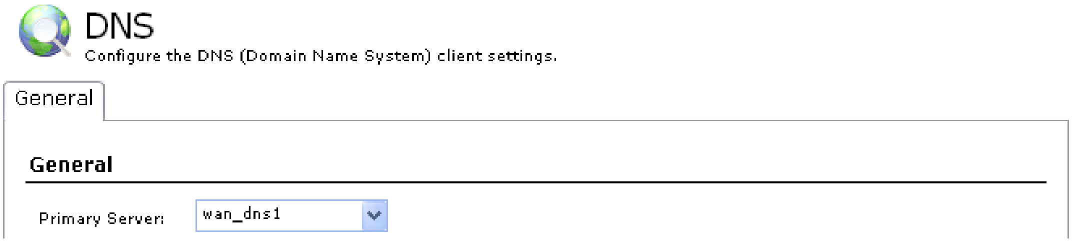
Route	If2	all-nets	wan_gw	100	No	Default route over interface If2.

This required *all-nets* route is, in fact, added automatically after specifing the *Default Gateway* for a particular Ethernet interface which we did earlier after setting up the required IP4 Address objects.

Note: Disabling automatic route generation

*Automatic route generation is enabled and disabled with the setting "**Automatically add a default route for this interface using the given default gateway**" which can be found in the properties of the interface.*

As part of the setup, it is also recommended that at least one DNS server is also defined in CorePlus. This DSN server or servers (a maximum of three can be configured) will be used when CorePlus itself needs to resolve URLs which is the case when a URL is specified in a configuration instead of an IP address. Let's assume an IP address object called *wan_dns1* has already been defined in the address book which is the IP address for the first DNS server. By choosing **System > DNS** in the navigation tree, the DNS server dialog will open and this object from the address book can be assigned as the first server.



DNS

Configure the DNS (Domain Name System) client settings.

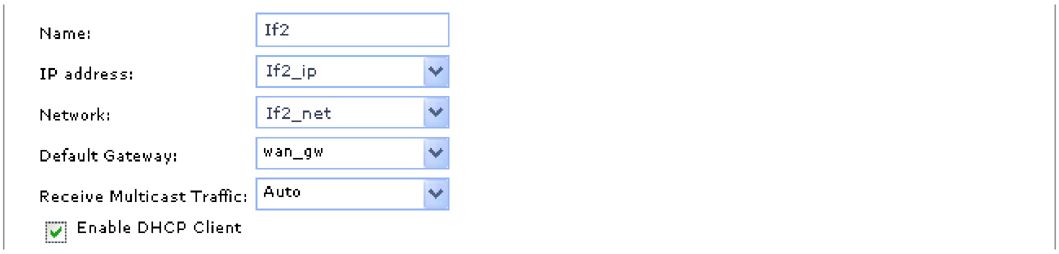
General

Primary Server: wan_dns1

B. DHCP - automatic configuration

All the required IP addresses for Internet connection can, alternatively, be automatically retrieved from an ISP's DHCP server by enabling the **DHCP Client** option for the interface connected to the ISP. We enable this option by first selecting **Ethernet > Interfaces** in the navigation tree to display a list of all the interfaces.

Click the *If2* interface in the list to display its properties.



Name: If2

IP address: If2_ip

Network: If2_net

Default Gateway: wan_gw

Receive Multicast Traffic: Auto

☑ Enable DHCP Client

In the above screenshot, DHCP is enabled for this interface and this is the required setting if IP addresses are to be retrieved automatically. Usually, a DHCP *Host Name* does not need to be specified but can sometimes be used by an ISP to uniquely identify this Clavister Security Gateway as a particular DHCP client to the ISP's DHCP server.

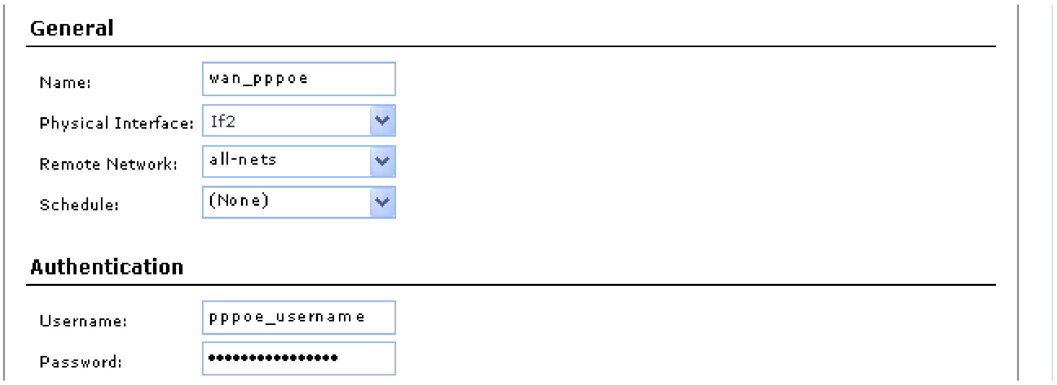
On connection to the ISP, all required IP addresses are retrieved automatically from the ISP via DHCP and CorePlus automatically sets the relevant address objects in the address book with this information.

For CorePlus to know on which interface to find the public Internet, a *route* has to be added to the *main* CorePlus routing table which specifies that the network *all-nets* can be found on the interface connected to the ISP and this route must also have the correct *Default Gateway* IP address specified. This *all-nets* route is added automatically by CorePlus during the DHCP address retrieval process.

After all IP addresses are set via DHCP and an *all-nets* route is added, the connection to the Internet is configured but no traffic can flow to or from the Internet since there is no IP rule defined that allows it. As was done in the previous option (**A**) above, we must therefore define an IP rule that will allow traffic from a designated source interface and source network. (in this example, the network *If3_net* and interface *If3*) to flow to the destination network *all-nets* and the destination interface *If2*.

C. PPPoE setup

For PPPoE connection, we must create a PPPoE tunnel interface associated with the physical Ethernet interface. Assume that the physical interface is *If2* and the PPPoE tunnel object created is called *wan_pppoe*. Go to **Interfaces > PPPoE** in the navigation tree and select **Add > PPPoE Tunnel**. These values can now be entered into the PPPoE Tunnel properties dialog.



General

Name: wan_pppoe

Physical Interface: If2

Remote Network: all-nets

Schedule: (None)

Authentication

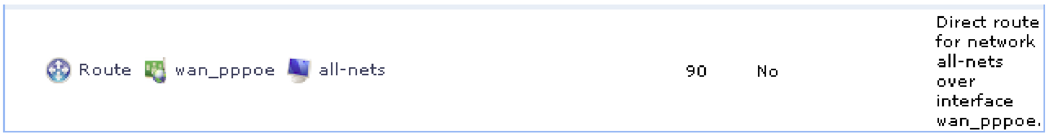
Username: pppoe_username

Password: ••••••••••••••••

Your ISP will supply the correct values for *pppoe_username* and *pppoe_password* in the dialog above.

The PPPoE tunnel interface can now be treated exactly like a physical interface by the policies defined in CorePlus rule sets.

There also has to be a route associated with the PPPoE tunnel to allow traffic to flow through it, and this is automatically created in the *main* routing table when the tunnel is defined. If we go to **Routing** > **Routing Tables** > **Main** in the navigation tree we can see this route.



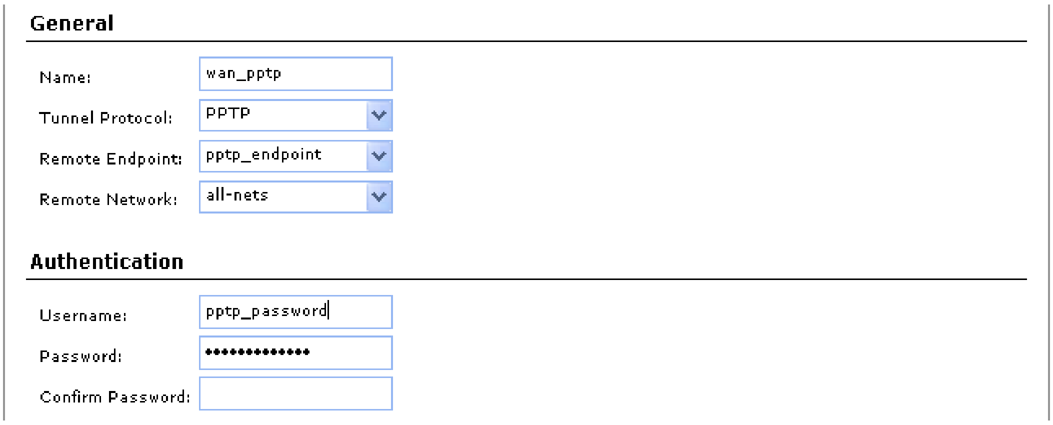
Route	wan_pppoe	all-nets	90	No	Direct route for network all-nets over interface wan_pppoe.

If the PPPoE tunnel object is deleted, this route is also automatically deleted.

At this point, no traffic can flow through the tunnel since there is no IP rule defined that allows it. As was done in option **A** above, we must define an IP rule that will allow traffic from a designated source interface and source network (in this example, the network *If3_net* and interface *If3*) to flow to the destination network *all-nets* and the destination interface which is the PPPoE tunnel we have defined.

D. PPTP setup

For PPTP connections, a PPTP client tunnel interface object needs to be created. Let us assume that the PPTP tunnel will be called *wan_pptp* with a a remote endpoint *10.5.4.1* which has been defined as the IP4 Address object *pptp_endpoint*. Go to **Interfaces** > **PPTP/L2TP Clients** in the navigation tree and select **Add** > **PPTP/L2TP Client**. The values can now be entered into the properties dialog and the *PPTP* option should be selected.



General

Name: wan_pptp

Tunnel Protocol: PPTP

Remote Endpoint: pptp_endpoint

Remote Network: all-nets

Authentication

Username: pptp_password

Password: ••••••••••••••

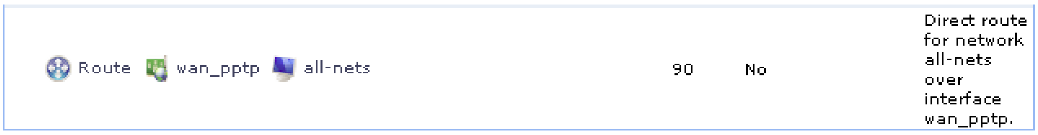
Confirm Password:

Your ISP will supply the correct values for *pptp_username*, *pptp_password* and the remote endpoint. An interface is not specified when defining the tunnel because this is determined by CorePlus looking up the *Remote Endpoint* IP address in its routing tables.

The PPTP client tunnel interface can now be treated exactly like a physical interface by the policies defined in CorePlus rule sets.

There also has to be an associated route with the PPTP tunnel to allow traffic to flow through it, and this is automatically created in the *main* routing table when the tunnel is defined. The destination network for this route is the *Remote Network* specified for the tunnel and for the public Internet this should be *all-nets*.

If we go to **Routing** > **Routing Tables** > **Main** in the navigation tree we can see this route.



Route	wan_pptp	all-nets	90	No	Direct route for network all-nets over interface wan_pptp.

If the PPTP tunnel object is deleted, this route is also automatically deleted.

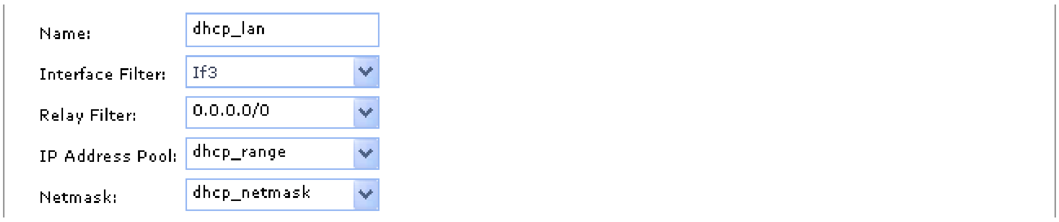
At this point, no traffic can flow through the tunnel since there is no IP rule defined that allows it. As was done in option **A** above, we must define an IP rule that will allow traffic from a designated source network and source interface (in this example, the network *If3_net* and interface *If3*) to flow to the destination network *all-nets* and the destination interface which is the PPTP tunnel that we have defined.

DHCP Server Setup

If the Clavister Security Gateway is to act as a DHCP server then this can be set up in the following way:

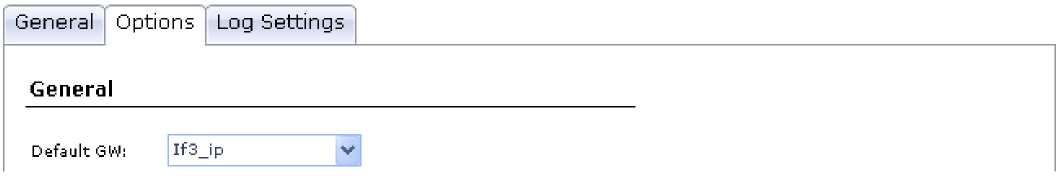
First create an IP4 Address object which defines the address range to be handed out. Here, we will assume this is called *dhcp_range*. We will also assume that an IP4 Address object *dhcp_netmask* has been created which specifies the netmask.

We now create a DHCP server object called *dhcp_lan* which will only be available only on the *If3* interface. To do this, go to **System** > **DHCP** > **DHCP Servers** and select **Add** > **DHCP Server**. We can now specify the server properties.



Name: dhcp_lan
Interface Filter: If3
Relay Filter: 0.0.0.0/0
IP Address Pool: dhcp_range
Netmask: dhcp_netmask

In addition it is important to specify the *Default gateway* for the server. This will be handed out to DHCP clients on the internal networks so that they know where to find the public Internet. The default gateway is always the IP address of the interface on which the DHCP server is configured. In this case, *If3_ip*



General

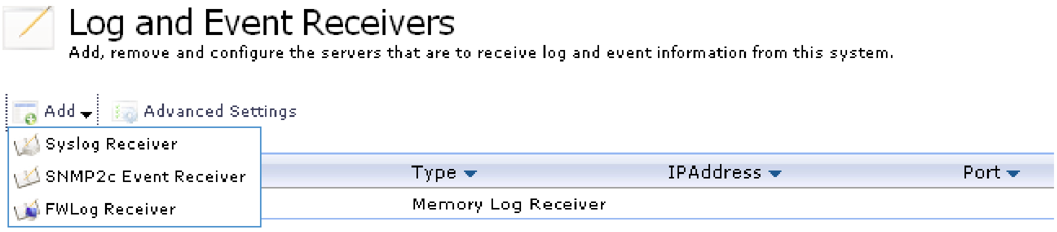
Default GW: If3_ip

Also in the **Options** tab, we should specify the DNS address which is handed out with DHCP leases. This could be set, for example, to be the IP address object *dns1_address*.

Syslog Server Setup

Although logging may be enabled, no log messages are captured unless at least one log server is set up to receive them and this is configured in CorePlus. *Syslog* is one of the most common server types.

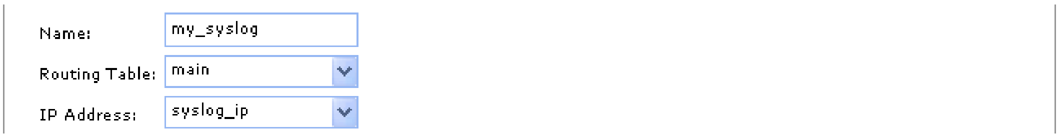
First we create an IP4 Address object called, for example, *syslog_ip* which is set to the IP address of the server. We then configure the sending of log messages to a Syslog server from CorePlus by selecting **System** > **Log and Event Receivers** from the navigation tree and then choosing **Add** > **Syslog Receiver**.


Log and Event Receivers

Add, remove and configure the servers that are to receive log and event information from this system.

Type	IPAddress	Port
Memory Log Receiver		

The syslog server properties dialog will now appear. We give the server a name, for example *my_syslog*, and specify its IP address as the *syslog_ip* object.


Name: my_syslog

Routing Table: main

IP Address: syslog_ip

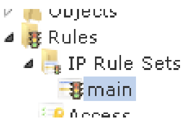
Tip: Address book object naming

*The CorePlus address book is organized alphabetically so when choosing names for IP address objects it is best to have the descriptive part of the name first. In this case, use **syslog_ip** as the name and not **ip_syslog**.*

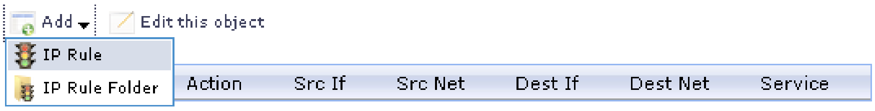
Allowing ICMP *Ping* Requests

As a further example of setting up IP rules, it can be very useful to allow ICMP *Ping* requests to flow through the Clavister Security Gateway. As discussed earlier, the CorePlus will drop any traffic unless an IP rule explicitly allows it. Let us suppose that we wish to allow the pinging of external hosts with the ICMP protocol by computers on the internal *If3_net* network.

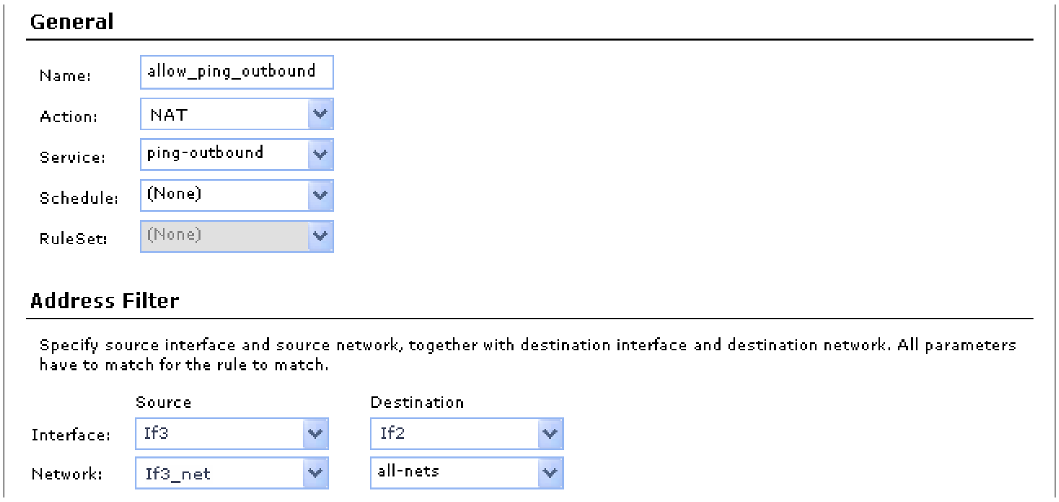
There can be several rule sets defined in CorePlus but there is only one rule set defined by default and this is called *main*. To add a rule to it, first select **Rules** > **IP Rule Sets** > **main** from the navigation tree.



The *main* rule set list contents are now displayed. Press the **Add** button and select **IP Rule**.



The properties for a new IP rule will appear and we can add a rule, in this case called *allow_ping_outbound*.



General

Name:	allow_ping_outbound
Action:	NAT
Service:	ping-outbound
Schedule:	(None)
RuleSet:	(None)

Address Filter

Specify source interface and source network, together with destination interface and destination network. All parameters have to match for the rule to match.

	Source	Destination
Interface:	If3	If2
Network:	If3_net	all-nets

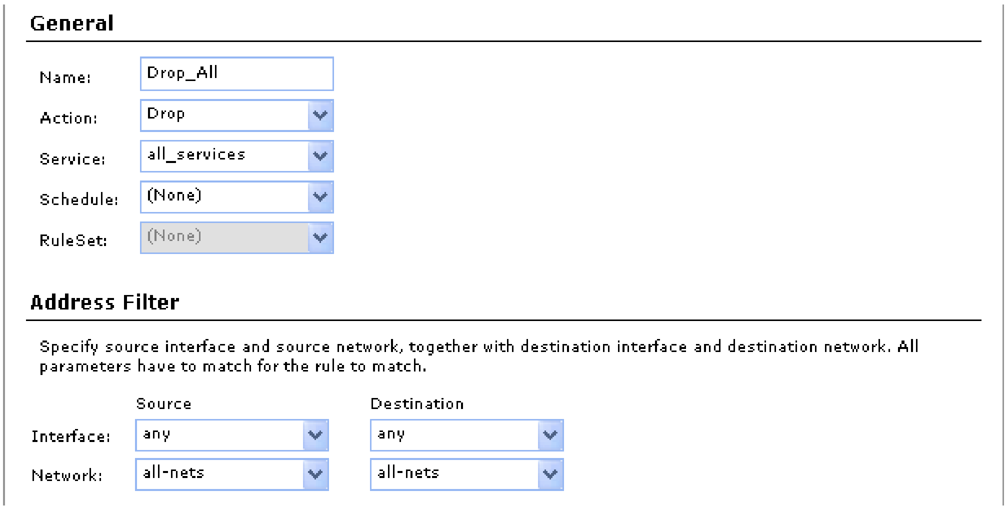
The IP rule again has the *NAT* action and this is necessary if the protected local hosts have private IP addresses. The ICMP requests will be sent out from the Clavister Security Gateway with the IP address of the interface connected to the ISP as the source interface. Responding hosts will send back ICMP repsonses to this single IP and CorePlus will then forward the response to the correct private IP address.

Adding a Drop All Rule

The top-down nature of the IP rule set scanning has already been discussed earlier. If **no** matching IP rule is found for a new connection then the *default rule* is triggered. This rule is hidden and cannot be changed and its action is to drop all such traffic as well as generate a log message for the drop.

In order to gain control over the logging of dropped traffic, it is recommended to create a drop all rule as the last rule in the *main* IP rule set. This rule has an *Action* of *Drop* with the source and destination network set to *all-nets* and the source and destination interface set to *any*.

The service for this rule must also be specified and this should be set to *all_services* in order to capture all types of traffic.



General

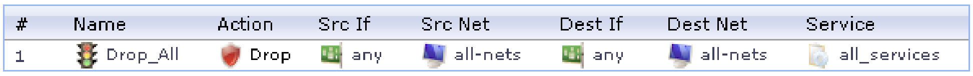
Name:	Drop_All
Action:	Drop
Service:	all_services
Schedule:	(None)
RuleSet:	(None)

Address Filter

Specify source interface and source network, together with destination interface and destination network. All parameters have to match for the rule to match.

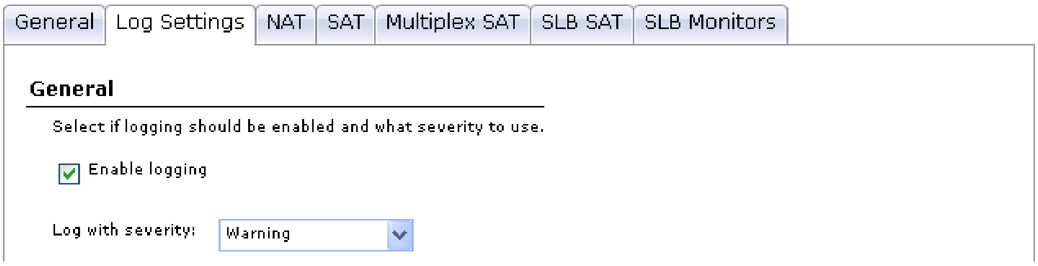
	Source	Destination
Interface:	any	any
Network:	all-nets	all-nets

If the this rule us the only one defined, displaying the *main* IP rule set will be as shown below.



#	Name	Action	Src If	Src Net	Dest If	Dest Net	Service
1	Drop_All	Drop	any	all-nets	any	all-nets	all_services

Logging can now be enabled on this rule with the desired severity. Click the **Log Settings** tab, and click the **Enable logging** box. All log messages generated by this rule will be given the selected severity and which will appear in the text of the log messages. It is up to the administrator to choose the severity and depends on how they would like to classify the messages.



General

Select if logging should be enabled and what severity to use.

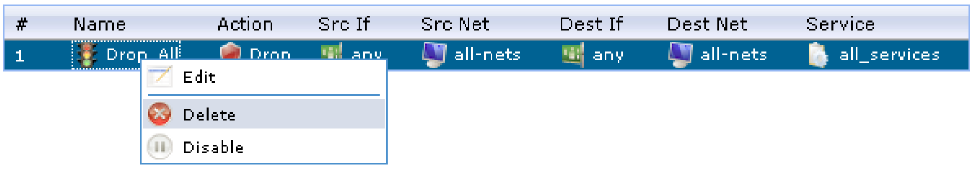
☑ Enable logging

Log with severity: Warning

Deleting Configuration Objects

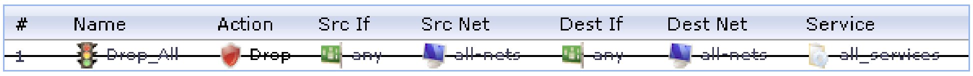
If information is deleted from a configuration during editing then these deletes are indicated by a line scored through the list entry while the configuration is still not yet activated. The deleted entry only disappears completely when the changes are activated.

For example, we can delete the drop all IP rule created in the previous paragraph by right clicking the rule and selecting *Delete* in the context menu.



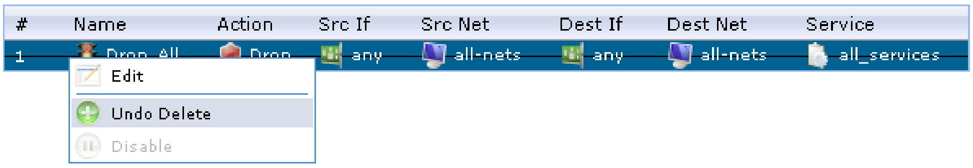
#	Name	Action	Src If	Src Net	Dest If	Dest Net	Service
1	Drop_All	Drop	any	all-nets	any	all-nets	all_services

The rule now appears with a line scored through it.



#	Name	Action	Src If	Src Net	Dest If	Dest Net	Service
~~1~~	~~Drop_All~~	~~Drop~~	~~any~~	~~all-nets~~	~~any~~	~~all-nets~~	~~all_services~~

We can reverse the delete by right clicking the rule again and choosing *Undo Delete*.

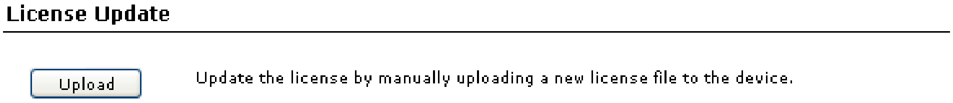


#	Name	Action	Src If	Src Net	Dest If	Dest Net	Service
1	Drop_All	Drop	any	all-nets	any	all-nets	all_services

Uploading a License

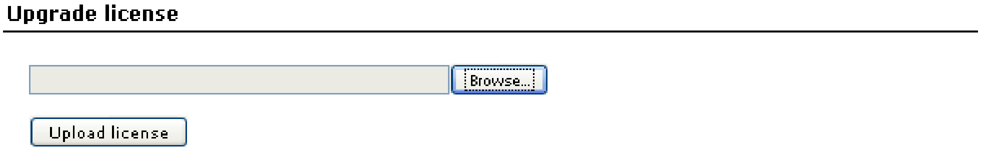
Without a valid license loaded, CorePlus operates in *demonstration mode* which means it will cease operations after 2 hours from startup. To remove this restriction, a valid license must be uploaded to the Clavister Security Gateway.

To do this, download a license as described in the last part of *Chapter 3, Web Interface and Wizard Setup*. This license can then be uploaded directly to CorePlus by selecting the **License** option from the **Maintenance** menu and then pressing the **Upload** button.



Update the license by manually uploading a new license file to the device.

Now press the **Browse** button to select the file from the load file system and then the **Upload License** button to send it to CorePlus.



As soon as upload of the license is complete, the 2 hour restriction will be removed and CorePlus will be restricted only by the restrictions of the license.

Chapter 5: CLI Setup

This chapter describes the setup steps using CLI commands instead of the setup wizard.

The CLI is accessible in two ways:

- Across the local network at default IP address *192.168.1.1* using an SSH (Secure Shell) client. The network connection setup is the same as that described in *Chapter 3, Web Interface and Wizard Setup* as is the way the workstation interface's static IP address must be set up so it is on the same network as the Clavister Security Gateway's interface.

  If there is a problem with workstation connection, a help checklist can be found in *Appendix A, Troubleshooting Setup*.

- Using a terminal or computer running a console emulator connected directly to the local RS-232 console port of the Clavister Security Gateway hardware.

The CLI commands listed below are grouped so that they mirror the options available in the setup wizard.

Confirming the Connection

Once connection is made to the CLI, pressing the **Enter** key will cause CorePlus to respond. The response will be a normal CLI prompt if connecting locally through the RS-232 console port and a username/password combination will not be required (a password for this console can be set later).

```
Device:/>
```

If connecting remotely through an SSH (Secure Shell) client, an administration username/password must first be entered and the initial default values for these are username *admin* and password *admin*. When these are accepted by CorePlus, a normal CLI prompt will appear and CLI commands can be entered.

Changing the Password

To change the administration username or password, use the *set* command to change the current CLI object category (sometimes refered to as the *object context*) to be the *LocalUserDatabase* called *AdminUsers*.

```
Device:/> cc LocalUserDatabase AdminUsers
Device:/AdminUsers>
```

Tip: Using tab completion with the CLI

The tab key can be pressed at any time so that CorePlus gives a list of possible options in a command.

Now set the username/password, which are case sensitive, to be the new chosen values for the user called *admin*. In the example below, we change to the username *new_name* and password *new_pass*.

```
Device:/AdminUsers> set User Admin Name=new_name Password=new_pass
```

The new username/password combination should be remembered and the password should be composed in a way which makes it difficult to guess. The next step is to return the CLI to the default top level of object categories.

```
Device:/AdminUsers> cc
Device:/>
```

Setting the Date and Time

Many CorePlus functions rely on an accurate date and time, so it is important that this is set correctly using the *time* command. A typical usage might be:

```
Device:/> time -set 2008-06-24 14:43:00
```

Notice that the date is entered in *yyyy-mm-dd* format and the time is stated in 24 hour *hh:mm:ss* format.

Ethernet Interfaces

The connection of external networks to the Clavister Security Gateway is via the various *Ethernet interfaces* which are provided by the hardware platform. On first-time startup, CorePlus scans for these interfaces and determines which are available and allocates their names. The first interface detected in the scan always becomes the initial default management interface and this cannot be changed beforehand.

All CorePlus interfaces are logically equal for CorePlus and although their physical capabilities may be different, any interface can perform any logical function. With the Clavister Software Series, the first interface is called *If1* and is always the management interface. We will assume that the hardware used has 3 Ethernet interfaces so the other two will be given the names *If2* and *If3* by CorePlus. For the sake of example, we will assume that the *If2* interface will be used for connection to the public Internet and the *If3* interface will be used for connection to a protected, local network.

Setting Up Internet Access

Next, we shall look at how to set up public Internet access with the CLI. The setup wizard described previously, provides the following four options:

A. Static - manual configuration.

B. DHCP - automatic configuration.

C. PPPoE setup

D. PPTP setup

The individual manual steps to configure these connection alternatives with the CLI are discussed next.

A. Static - manual configuration

We first must set or create a number of IP address objects. It's assumed here that the interface used for Internet connection is *If2*, the ISP gateway IP address is *10.5.4.1*, the IP address for the connecting interface will be *10.5.4.35* and the network to which they belong is *10.5.4.0/24*.

Note: Private IP addresses are used for example only

Each installation's IP addresses will be different from these IP addresses but they are used here only to illustrate how setup is done. Also, these addresses are private IP addresses and in reality an ISP would use public IP addresses instead.

We first add the gateway IP address object which we will call *wan_gw*:

```
Device:/> add Address IP4Address wan_gw Address=10.5.4.1
```

This is the address of the ISP's gateway which is the first router hop towards the public Internet. If this IP object already exists, it can be given the IP address with the command:

```
Device:/> set Address IP4Address wan_gw Address=10.5.4.1
```

Now use this object to set the gateway on the *If2* interface which is connected to the ISP:

```
Device:/> set Interface Ethernet If2 DefaultGateway=wan_gw
```

Next, set the IP object *If2_ip* which will be the IP address of the interface connected to the ISP:

```
Device:/> set IP4Address If2_ip Address=10.5.4.35
```

Now set the IP object *If2_net* which will be the IP network of the connecting interface:

```
Device:/> set IP4Address If2_net Address=10.5.4.0/24
```

It is recommended to verify the properties of the *If2* interface with the command:

```
Device:/> show Interface Ethernet If2
```

The typical output from this will be similar to the following:

```
                 Property  Value
--------------------------  --------------------------
                     Name:  If2
                       IP:  If2_ip
                  Network:  If2_net
           DefaultGateway:  wan_gw
                Broadcast:  10.5.4.255
                PrivateIP:  <empty>
                    NOCHB:  <empty>
                      MTU:  1500
                   Metric:  100
              DHCPEnabled:  No
           EthernetDevice:  0:If2  1:<empty>
          AutoSwitchRoute:  No
AutoInterfaceNetworkRoute:  Yes
  AutoDefaultGatewayRoute:  Yes
```

```
   ReceiveMulticastTraffic:  Auto
      MemberOfRoutingTable:  All
                  Comments:  <empty>
```

Setting the default gateway on the interface has the additional effect that CorePlus automatically creates a route in the default *main* routing table that has the network *all-nets* routed on the interface. This means that we do not need to explicitly create this route.

Even though an *all-nets* route is automatically added, no traffic can flow without the addition of an *IP rule* which explicitly allows traffic to flow. Let us assume we want to allow web surfing from the protected network *If3_net*. on the interface *If3*. A simple rule to do this would have an *Action* of *Allow* and would be defined with the following commands.

Firstly, we must change the current CLI context to be the default *IPRuleSet* called *main* using the command:

```
Device:/> cc IPRuleSet main
```

Additional IP rulesets can be defined which is why we do this, with the rule set *main* existing by default. Notice that the CLI prompt changes to reflect the current context:

```
Device:/main>
```

Now add an IP rule called *lan_to_wan* to allows the traffic through to the public Internet:

```
Device:/main> add IPRule name=lan_to_wan
                Action=Allow SourceInterface=If3
                SourceNetwork=If3_net
                DestinationInterface=If2
                DestinationNetwork=all-nets
                Service=http-all
```

This IP rule would be correct if the internal network hosts have public IP addresses but in most scenarios this will not be true and internal hosts will have private IP addresses. In that case, we must use NAT to send out traffic so that the apparent source IP address is the IP of the interface connected to the ISP. To do this we simply change the *Action* of the above command from *Allow* to *NAT*:

```
Device:/main> add IPRule name=lan_to_wan
                Action=NAT SourceInterface=If3
                SourceNetwork=If3_net
                DestinationInterface=If2
                DestinationNetwork=all-nets
                Service=http-all
```

The service used in the IP rule is *http-all* which will allow most web surfing but does not include the DNS protocol to resolve URLs into IP addresses. To solve this problem, a custom service could be used in the above rule which combines *http-all* with the *dns-all* service. However, the recommended method which provides the most clarity to a configuration is to create a separate IP rule for DNS:

```
Device:/main> add IPRule name=lan_to_wan_dns
                Action=NAT SourceInterface=If3
                SourceNetwork=If3_net
                DestinationInterface=If2
                DestinationNetwork=all-nets
                Service=dns-all
```

It is recommended that at least one DNS server is also defined in CorePlus. This DSN server or servers (a maximum of three can be configured) will be used when CorePlus itself needs to resolve URLs which is the case when a URL is specified in a configuration instead of an IP address.

If we assume an IP address object called *dns1_address* has already been defined for the first DNS server, the command to specify the first DNS server is:

```
Device:/> set DNS DNSServer1=dns1_address
```

Assuming a second IP object called *dns2_address* has been defined, the second DNS server is specified with:

```
Device:/> set DNS DNSServer2=dns2_address
```

B. DHCP - automatic configuration

All required IP addresses can alternatively be automatically retrieved from the ISP's DHCP server by enabling DHCP on the interface connected to the ISP. If the interface on which DHCP is to be enabled is *If2* then the command is:

```
Device:/> set Interface Ethernet If2 DHCPEnabled=Yes
```

Once the required IP addresses are retrieved with DHCP, CorePlus automatically sets the relevant address objects in the address book with this information.

For CorePlus to know on which interface to find the public Internet, a *route* has to be added to the *main* CorePlus routing table which specifies that the network *all-nets* can be found on the interface connected to the ISP and this route must also have the correct *Default Gateway* IP address specified. This *all-nets* route is added automatically by CorePlus during the DHCP address retrieval process. Automatic route generation is a setting for each interface that can be manually enabled and disabled.

After all IP addresses are set via DHCP and an *all-nets* route is added, the connection to the Internet is configured but no traffic can flow to or from the Internet since there is no IP rule defined that allows it. As was done in the previous option (**A**) above, we must therefore manually define an IP rule that will allow traffic from a designated source interface and source network. (in this example, the network *If3_net* and interface *If3*) to flow to the destination network *all-nets* and the destination interface *If2*.

C. PPPoE setup

For PPPoE connection, create the PPPoE tunnel interface on the interface connected to the ISP. The interface *If2* is assumed to be connected to the ISP in the command shown below which creates a PPPoE tunnel object called *wan_ppoe*:

```
Device:/> add Interface PPPoETunnel wan_ppoe
                EthernetInterface=If2 username=pppoe_username
                Password=pppoe_password Network=all-nets
```

Your ISP will supply the correct values for *pppoe_username* and *pppoe_password*.

Your ISP will supply the correct values for *pppoe_username* and *pppoe_password* in the dialog above.

The PPPoE tunnel interface can now be treated exactly like a physical interface by the policies defined in CorePlus rule sets.

There also has to be a route associated with the PPPoE tunnel to allow traffic to flow through it, and this is automatically created in the *main* routing table when the tunnel is defined. If the PPPoE tunnel object is deleted, this route is also automatically deleted.

At this point, no traffic can flow through the tunnel since there is no IP rule defined that allows it. As was done in option **A** above, we must define an IP rule that will allow traffic from a designated source interface and source network (in this example, the network *If3_net* and interface *If3*) to flow to the destination network *all-nets* and the destination interface which is the PPPoE tunnel that we have defined.

D. PPTP setup

For PPTP connection, first create the PPTP tunnel interface. It is assumed below that we will create a PPTP tunnel object called *wan_pptp* with the remote endpoint *10.5.4.1*:

```
Device:/> add Interface L2TPClient wan_pptp Network=all-nets
                username=pptp_username Password=pptp_password
                RemoteEndpoint=10.5.4.1 TunnelProtocol=PPTP
```

Your ISP will supply the correct values for *pptp_username*, *pptp_password* and the remote endpoint.

Your ISP will supply the correct values for *pptp_username*, *pptp_password* and the remote endpoint. An interface is not specified when defining the tunnel because this is determined by CorePlus looking up the *Remote Endpoint* IP address in its routing tables.

The PPTP client tunnel interface can now be treated exactly like a physical interface by the policies defined in CorePlus rule sets.

There also has to be an associated route with the PPTP tunnel to allow traffic to flow through it, and this is automatically created in the *main* routing table when the tunnel is defined. The destination network for this route is the *Remote Network* specified for the tunnel and for the public Internet this should be *all-nets*.

As with all automatically added routes, if the PPTP tunnel object is deleted then this route is also automatically deleted.

At this point, no traffic can flow through the tunnel since there is no IP rule defined that allows it. As was done in option **A** above, we must define an IP rule that will allow traffic from a designated source interface and source network (in this example, the network *If3_net* and interface *If3*) to flow to the destination network *all-nets* and the destination interface which is the PPTP tunnel that we have defined.

Activating and Committing Changes

After any changes are made to a CorePlus configuration, they will be saved as a new configuration but will not yet be activated. To activate all the configuration changes made since the last activation of a new configuration, the following command must be issued:

```
Device:/> activate
```

Although the new configuration is now activated, it does not become permanently activated until the following command is issued within 30 seconds following the *activate*:

```
Device:/> commit
```

The reason for two commands is to prevent a configuration accidentally locking out the administrator. If a lock-out occurs then the second command will not be received and CorePlus will revert back to the original configuration after the 30 second time period (this time period is a setting that can be changed).

DHCP Server Setup

If the Clavister Security Gateway is to act as a DHCP server then this can be set up in the following way:

First define an IP address object which has the address range that can be handed out. Here, we will use the IP range *192.168.1.10-192.168.1.20* as an example and this will be available on the *If3* interface which is connected to the protected internal network *If3_net*.

```
Device:/> add Address IP4Address dhcp_range
                Address=192.168.1.10-192.168.1.20
```

The DHCP server is then configured with this IP address object on the appropriate interface. In this case we will call the created DHCP server object *dhcp_lan* and assume the DHCP server will be available on the *If3* interface:

```
Device:/> add DHCPServer dhcp_lan IPAddressPool=dhcp_range
                Interface=If3 Netmask=255.255.255.0
                DefaultGateway=If3_ip
                DNS1=dns1_address
```

It is important to specify the *Default gateway* for the DHCP server since this will be handed out to DHCP clients on the internal network so that they know where to find the public Internet. The default gateway is always the IP address of the interface on which the DHCP server is configured. In this case, *If3_ip*.

NTP Server Setup

Network Time Protocol (NTP) servers can optionally be configured to maintain the accuracy of the system date and time. The command below sets up synchronization with the two NTP servers at hostname *pool.ntp.org* and IP address *10.5.4.76*:

```
Device:/> set DateTime TimeSyncEnable=Yes
                TimeSyncServer1=dns:pool.ntp.org
                TimeSyncServer2=10.5.4.76
```

The prefix *dns:* is added to the hostname to identify that it must resolved to an IP address by a DNS server (this is a convention used in the CLI with some commands).

Syslog Server Setup

Although logging may be enabled, no log messages are captured unless a server is set up to receive them and *Syslog* is the most common server type. If the Syslog server's address is *195.11.22.55* then the command to create a log receiver object called *my_syslog* which enables logging is:

```
Device:/> add LogReceiverSyslog my_syslog IPAddress=195.11.22.55
```

Allowing ICMP *Ping* Requests

As a further example of setting up IP rules, it can be useful to allow ICMP *Ping* requests to flow through the Clavister Security Gateway. As discussed earlier, the CorePlus will drop any traffic unless an IP rule explicitly allows it. Let us suppose that we wish to allow the pinging of external hosts with the ICMP protocol by computers on the internal *If3_net* network. The commands to allow this are as follows.

Firstly, we must change the current CLI context to be the *IPRuleSet* called *main* using the command:

```
Device:/> cc IPRuleSet main
```

Now add an IP rule called *allow_ping_outbound* to allow ICMP pings to pass:

```
Device:/main> add IPRule name=allow_ping_outbound
                Action=NAT SourceInterface=If3
                SourceNetwork=If3_net
                DestinationInterface=If2
                DestinationNetwork=all-nets
                Service=ping-outbound
```

The IP rule again has the *NAT* action and this is necessary if the protected local hosts have private IP addresses. The ICMP requests will be sent out from the Clavister Security Gateway with the IP address of the interface connected to the ISP as the source interface. Responding hosts will send back ICMP repsonses to this single IP and CorePlus will then forward the response to the correct private IP address.

Adding a Drop All Rule

Scanning of the IP rule set is done in a top-down fashion. If **no** matching IP rule is found for a new connection then the *default rule* is triggered. This rule is hidden and cannot be changed and its action is to drop all such traffic as well as generate a log message for the drop.

In order to gain control over the logging of dropped traffic, it is recommended to create a drop all rule as the last rule in the *main* IP rule set. This rule has an *Action* of *Drop* with the source and destination network set to *all-nets* and the source and destination interface set to *any*.

The service for this rule must also be specified and this should be set to *all_services* in order to capture all types of traffic. The command for creating this rule is:

```
Device:/main> add IPRule name=drop_all
                Action=Drop SourceInterface=any
                SourceNetwork=any
                DestinationInterface=any
                DestinationNetwork=all-nets
                Service=all_services
```

Uploading a License

Without a valid license loaded, CorePlus operates in *demonstration mode* which means it will cease operations after 2 hours from startup. To remove this restriction, a valid license must be uploaded to the Clavister Security Gateway.

To do this, download a license as described in the last part of *Chapter 3, Web Interface and Wizard Setup*. This license can then be uploaded directly to CorePlus using a *Secure Copy* (SCP) client (see the CorePlus Administrators Guide for more details of using SCP). As soon as upload of the license is complete, the 2 hour restriction will be removed and CorePlus will be restricted only by the restrictions of the license.

Appendix A: Troubleshooting Setup

This appendix deals with connection problems that might occur when connecting a management workstation to a Clavister Security Gateway.

If the management interface does not respond after the Clavister Security Gateway has powered up and CorePlus has started, there are a number of simple steps to trouble shoot basic connection problems:

1. Check that the correct interface is being used.

The most obvious problem is that the wrong Clavister Security Gateway interface has been used for the initial connection. Only the first interface found by CorePlus is activated for the initial connection from a browser after CorePlus starts for the first time.

2. Check that interface characteristics match.

If a Clavister Security Gateway's interface characteristics are configured manually then the interface on a switch to which it is connected should be configured with the same characteristics. For instance, the link speeds and half/full duplex settings must match. If they don't, communication will fail. This problem will not occur if the interfaces are set for automatic configuration on both sides and automatic is always the Clavister factory default setting.

3. Check that the workstation IP is configured correctly.

The second most obvious problem is if the IP address of the workstation running the web browser is not configured correctly.

4. Is the management interface properly connected?

Check the link indicator lights on the management interface. If they are dark then there may be a cable problem.

5. Check the cable type connected to the management interface.

Is the management interface connected directly to the management workstation or another router or host? In this case, an Ethernet "cross-over" cable may be needed for the connection, depending on the capabilities of the interface.

6. Using the *ifstat* CLI command.

To investigate a connection problem further, connect the a console to the RS-232 port on the Clavister Security Gateway after CorePlus starts. When you press the enter key, CorePlus should respond with the a standard CLI prompt. Now enter the following command a number of times:

```
Device:/> ifstat <if-name>
```

Where *<if-name>* is the name of the management interface. This will display a number of counters for that interface. The *ifstat* command on its own can list the names of all the interfaces.

If the *Input* counters in the hardware section of the output are not increasing then the error is likely to be in the cabling. However, it may simply be that the packets are not getting to the Clavister Security Gateway in the first place. This can be confirmed with a packet sniffer if it is available.

If the *Input* counters are increasing, the management interface may not be attached to the correct physical network. There may also be a problem with the routing information in any connected hosts or routers.

7. Using the *arpsnoop* CLI command.

A final diagnostic test is to try using the console command:

```
Device:/> arpsnoop -all
```

This will show the *ARP* packets being received on the different interfaces and confirm that the correct cables are connected to the correct interfaces.

Chapter 6: Going Further

After initial setup is complete, the administrator is ready to go further with configuring CorePlus to suit the requirements of a particular scenario. The manuals that will help with this are:

- The CorePlus Administrators Guide
- The CLI Reference Guide
- The Log Reference Guide

The CorePlus Administrators Guide

This guide is a comprehensive description of CorePlus features and includes a detailed table of contents and comprehensive index to quickly locate a particular topic.

Examples of the setup for various scenarios are included but screenshots are kept to a minimum since the user has a variety of management interfaces to choose from, including SNMP.

At minimum, the new administrator should first aquaint themselves with the CorePlus *Address Book* for defining IP address objects and with the CorePlus *IP rule set* for defining IP rules which can allow or block traffic types and which are also used to set up NAT address translation.

IP rules also demonstrate the way *Security Policies* are set up in CorePlus by identifying the targeted traffic through combinations of the source/destination interface/network combined with protocol type.

ALGs

Once the address book and IP rules are understood, the various ALGs will probably be of interest for managing higher level protocols such as HTTP. For instance, for management of web surfing, the HTTP ALG provides a number of important features such as content filtering.

VPN Setup

A common requirement is to quickly setup VPN networks based on Clavister Security Gateways. The CorePlus Administrators Guide includes an extensive VPN section and as part of this, a *VPN Quick Start* section which goes through a checklist of setup steps for nearly all types of VPN scenarios.

Included with the quick start section is a checklist for trouble shooting and advice on how best to deal with the networking complications that can arise with certificates.

Logging

By default, certain events will generate log messages and at least one log server should be configured to capture these messages although a *memlog* feature is provided which captures recent log messages in hardware memory. The administrator should review what events are important to them and at what severity.

CorePlus Education Courses

For details about classroom and online CorePlus education as well as CorePlus certification, visit the Clavister company website at *http://www.clavister.com* or contact your local sales representative.

Staying Informed

Clavister maintains an RSS feed of announcements that can be subscribed to at https://forums.clavister.com/rss-feeds/announcements/. It is recommended to subscribe to this feed so that you receive notifications when new releases of CorePlus versions are available for download and installation. Alternatively, announcements can be read directly from the Clavister forums which can be found at https://forums.clavister.com/.

Appendix B: Vista IP Setup

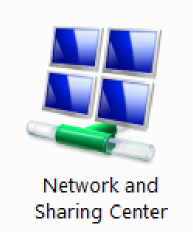
If a PC running Microsoft Vista is being used as the CorePlus management workstation, the computer's Ethernet interface connected to the Clavister Security Gateway must be configured with an IP address which belongs to the network *192.168.1.0/24* and is different from the security gateway's address of *192.168.1.1*.

The IP address *192.168.1.30* will be used for this purpose and the steps to set this up with Vista are as follows:

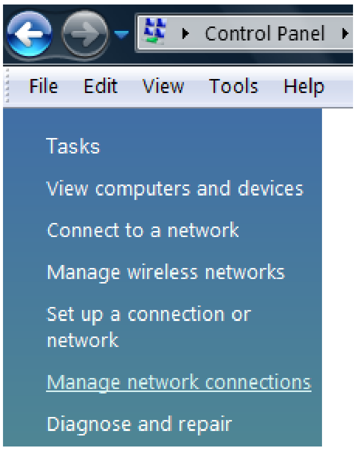
1. Press the Windows **Start** button.

2. Select the **Control Panel** from the start menu.

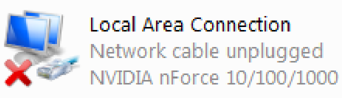
3. Select **Network & Sharing Center** from the control panel.



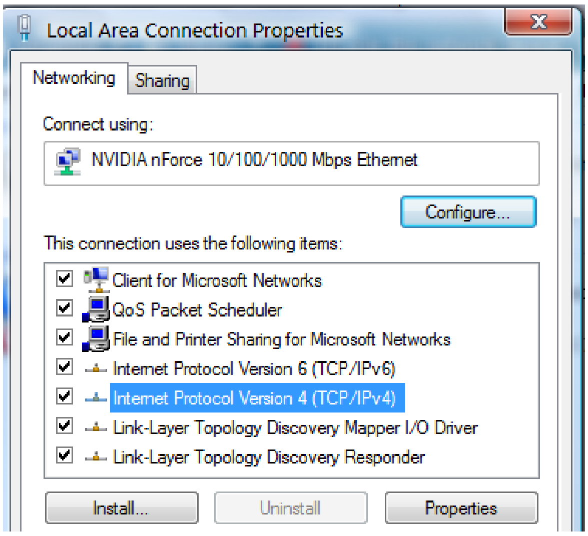
4. Select the **Manage network connections** option.



5. A list of the Ethernet interface connections will appear. Select the interface that will connect to the security gateway.



6. The properties for the selected interface will appear.



Local Area Connection Properties

Networking | Sharing

Connect using:

NVIDIA nForce 10/100/1000 Mbps Ethernet

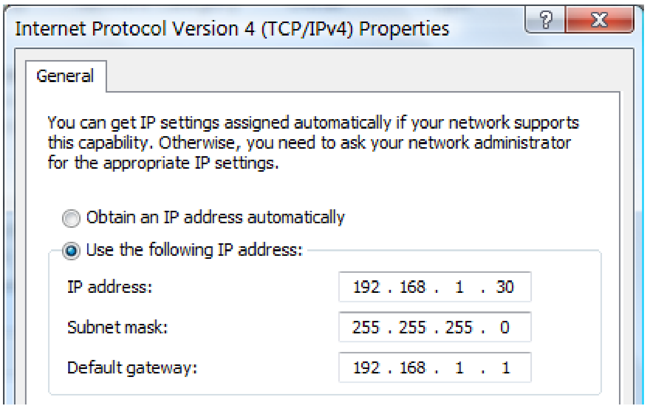
This connection uses the following items:

☑ Client for Microsoft Networks
☑ QoS Packet Scheduler
☑ File and Printer Sharing for Microsoft Networks
☑ Internet Protocol Version 6 (TCP/IPv6)
☑ Internet Protocol Version 4 (TCP/IPv4)
☑ Link-Layer Topology Discovery Mapper I/O Driver
☑ Link-Layer Topology Discovery Responder

Select and display the properties for *Internet Protocol Version 4 (TCP/IPv4).*

7. In the properties dialog, select the option **Use the following IP address** and enter the following values:

- **IP Address:** *192.168.1.30*
- **Subnet mask:** *255.255.255.0*
- **Default gateway:** *192.168.1.1*



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:

IP address: 192 . 168 . 1 . 30
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 192 . 168 . 1 . 1

DNS addresses can be entered later once Internet access is established.

8. Click **OK** to close this dialog and close all the other dialogs opened since step **(1)**.

Appendix C: Windows 7 IP Setup

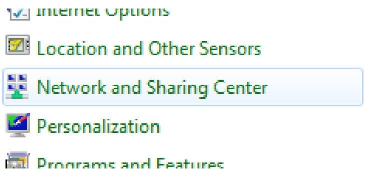
If a PC running Microsoft Windows 7 is being used as the CorePlus management workstation, the computer's Ethernet interface connected to the Clavister Security Gateway must be configured with an IP address which belongs to the network *192.168.1.0/24* and is different from the security gateway's address of *192.168.1.1*.

The IP address *192.168.1.30* will be used for this purpose and the steps to set this up with Windows 7 are as follows:

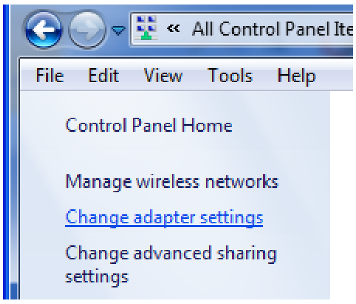
1. Press the Windows **Start** button.

2. Select the **Control Panel** from the start menu.

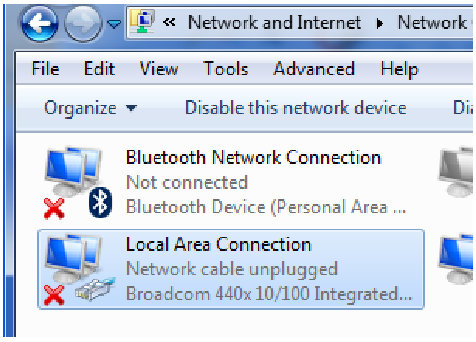
3. Select **Network & Sharing Center** from the control panel.



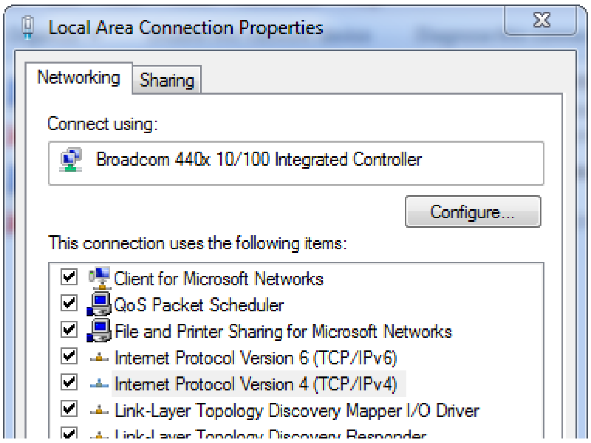
4. Select the **Change adapter settings** option.



5. A list of adapters will appear and will include the Ethernet interfaces. Select the interface that will connect to the security gateway.


« Network and Internet ▸ Network
File Edit View Tools Advanced Help
Organize ▾ Disable this network device Di
Bluetooth Network Connection
Not connected
Bluetooth Device (Personal Area ...
Local Area Connection
Network cable unplugged
Broadcom 440x 10/100 Integrated...

6. The properties for the selected interface will appear.



Local Area Connection Properties

Networking | Sharing

Connect using:

Broadcom 440x 10/100 Integrated Controller

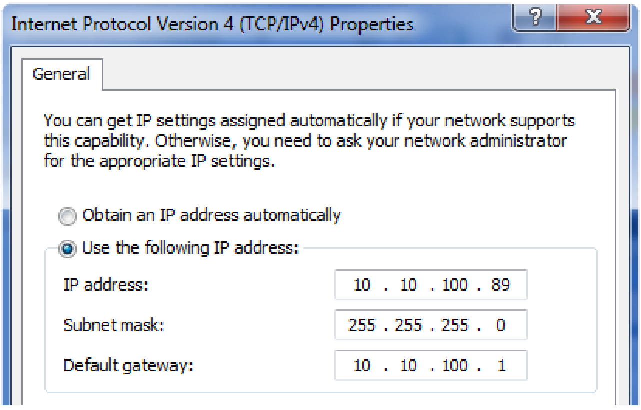
This connection uses the following items:

☑ Client for Microsoft Networks
☑ QoS Packet Scheduler
☑ File and Printer Sharing for Microsoft Networks
☑ Internet Protocol Version 6 (TCP/IPv6)
☑ Internet Protocol Version 4 (TCP/IPv4)
☑ Link-Layer Topology Discovery Mapper I/O Driver
☑ Link-Layer Topology Discovery Responder

Select and display the properties for *Internet Protocol Version 4 (TCP/IPv4).*

7. In the properties dialog, select the option **Use the following IP address** and enter the following values:

    - **IP Address:** *192.168.1.30*
    - **Subnet mask:** *255.255.255.0*
    - **Default gateway:** *192.168.1.1*



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:

IP address: 10 . 10 . 100 . 89
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 10 . 10 . 100 . 1

DNS addresses can be entered later once Internet access is established.

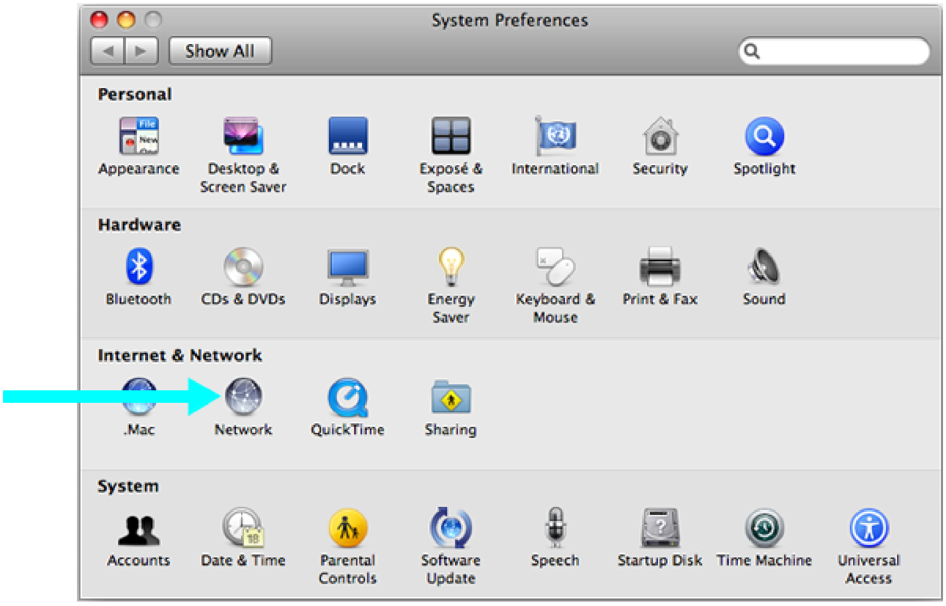
8. Click **OK** to close this dialog and close all the other dialogs opened since step **(1)**.

Appendix D: Apple Mac IP Setup

An Apple Mac can be used as the management workstation for initial setup of a Clavister Security Gateway. To do this, a selected Ethernet interface on the Mac must be configured correctly with a static IP. The setup steps for this with Mac OS X are:

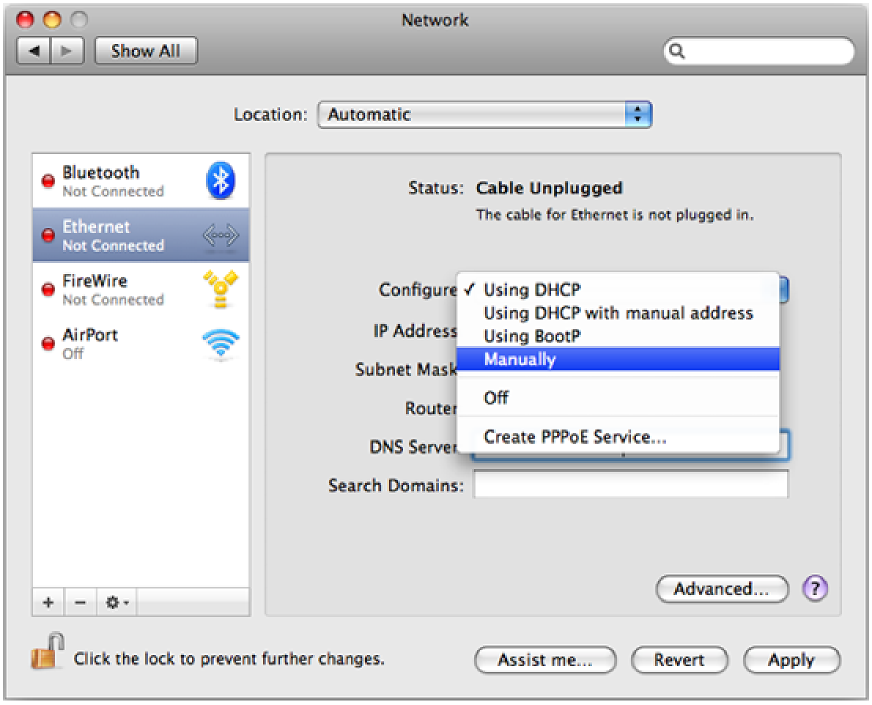
1. Go to the **Apple Menu** and select **System Preferences**.

2. Click on **Network**.



3. Select **Ethernet** from the left sidebar menu.

4. Select **Manually** in the **Configure** pull down menu.



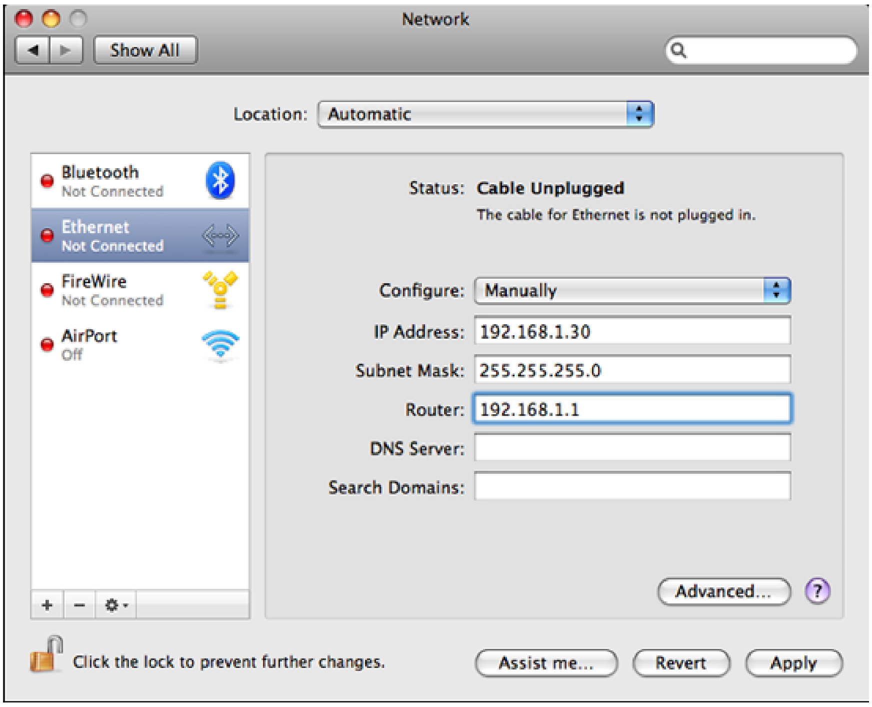
Location: Automatic

Status: Cable Unplugged

The cable for Ethernet is not plugged in.

Configure ✓ Using DHCP
Using DHCP with manual address
Using BootP
Manually
Off
Create PPPoE Service...

5. Now set the following values:
   - **IP Address:** *192.168.1.30*
   - **Subnet Mask:** *255.255.255.0*
   - **Router:** *192.168.1.1*



Network

Location: Automatic

Bluetooth Not Connected

Ethernet Not Connected

FireWire Not Connected

AirPort Off

Status: **Cable Unplugged**

The cable for Ethernet is not plugged in.

Configure: Manually

IP Address: 192.168.1.30

Subnet Mask: 255.255.255.0

Router: 192.168.1.1

DNS Server:

Search Domains:

Click the lock to prevent further changes.

6. Click **Apply** to complete the static IP setup.

Clavister AB
Sjögatan 6J
SE-89160 Örnsköldsvik
SWEDEN

Phone: +46-660-299200
Fax: +46-660-12250

www.clavister.com